ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA MEGADATOS S.A. EN LA CIUDAD DE QUITO, APLICANDO LAS NORMAS ISO 27001 E ISO 27002

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

FLORES ESTÉVEZ FANNY PAULINA
(fannyflores23@yahoo.es)

JIMÉNEZ NÚÑEZ DIANA CAROLINA
(dj_lagata@yahoo.es)

DIRECTOR: ING. PABLO HIDALGO
(phidalgo@ieee.com)

Quito, Agosto 2010

DECLARACIÓN

Nosotros, Fanny Paulina Flores Estévez y Diana Carolina Jiménez Núñez, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____ _____

Fanny Flores Diana Jiménez

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Fanny Paulina Flores Estévez y Diana Carolina Jiménez Núñez, bajo mi supervisión.

_____

Ing. Pablo Hidalgo

DIRECTOR DE PROYECTO

AGRADECIMIENTO

Agradecemos al Ingeniero Pablo Hidalgo, por su permanente colaboración en la realización del presente Proyecto de Titulación; su guía ha sido uno de los elementos fundamentales para el desarrollo y culminación exitosa del mismo.

A los integrantes del Departamento de Operaciones de la Empresa Megadatos S.A., especialmente a los Ingenieros Juan Francisco Yépez y Marco Logacho, por su colaboración y excelente predisposición.

A nuestros profesores, que durante toda la Carrera nos han preparado e impartido sus conocimientos, formándonos profesionalmente.

Fanny Flores
Diana Jiménez

DEDICATORIA

A Dios, por su inmensa generosidad y amor.

A mis padres, Juan y Fanny, mis mejores amigos, las personas a quienes más admiro y quiero; me han amado incondicionalmente y han hecho de mi la persona que ahora soy. A ustedes debo mis valores y principios; gracias por sus cuidados, esfuerzo, ejemplo, confianza y dedicación. Su presencia y apoyo me han alentado a dar mi mayor esfuerzo y finalmente ver culminada una de mis metas.

A mis hermanos, Juan y Evelyn, que han sido mis compañeros, amigos incondicionales, ejemplo a seguir. Gracias por su amistad, consejos y apoyo.

Fanny Flores

DEDICATORIA

A Dios, mi madre y mi hermano, quienes representan el pilar fundamental de mi vida y que con su amor y paciencia me han encaminado hacia la culminación de uno de mis sueños.

De manera especial dedico este Proyecto de Titulación a mi Padre, quien con su bendición desde el cielo ha guiado y cuidado mis pasos.

Diana Jiménez

ÍNDICE DE CONTENIDOS

CONTENIDO

TOMO I

CAPÍTULO 1

INTRODUCCIÓN A LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

CAPÍTULO 2

FUNDAMENTOS DE LOS ESTÁNDARES ISO 27001 E ISO 27002

CAPÍTULO 3

SITUACIÓN ACTUAL DE MEGADATOS S.A.

TOMO II

CAPÍTULO 4

PROPUESTA DEL DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA MEGADATOS S.A.

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El diseño del Sistema de Gestión de Seguridad de la Información (SGSI) para la Empresa ECUANET (MEGADATOS S.A.), se desarrolló en base a la Norma ISO 27001, y se consideraron las recomendaciones proporcionadas en la Norma ISO 27002. El punto de partida para el diseño fue el reconocimiento de los activos que contribuyen a la entrega de los servicios a los usuarios, así como las amenazas a las que están expuestos dichos activos; finalmente se realizó una evaluación de los riesgos, analizando el impacto de cada amenaza de acuerdo al número de clientes que se verían afectados. En base al estudio realizado, se desarrolló la propuesta para la Empresa, incluyendo políticas a seguir por parte del personal y soluciones técnicas que contribuyan a garantizar la seguridad de la información.

Este trabajo se divide en cinco capítulos, además de anexos en los que se incluye un Documento de procedimientos y evaluación de costos.

En el capítulo 1 se realiza un estudio sobre la seguridad de la información, amenazas y ataques a los que se expone y soluciones técnicas para contrarrestar dichos riesgos.

En el capítulo 2 se presenta la normativa concerniente a la seguridad de la información, enfocado en el análisis de las Normas ISO 27001 e ISO 27002.

En el capítulo 3 se presenta la situación actual de la Empresa, así como la descripción de la red a través de la cual se provee los servicios a los clientes y los activos que la conforman.

En el capítulo 4 se desarrolla el SGSI, se establecen los lineamientos de evaluación, se desarrolla la matriz de Riesgo, se seleccionan los objetivos de control y controles y se presenta la propuesta en base a la normativa ISO.

El capítulo 5 contiene las conclusiones y recomendaciones del presente proyecto.

PRESENTACIÓN

El presente Proyecto de Titulación tiene como objetivo el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI), en base a las Normas ISO 27001 e ISO 27002, dada la necesidad de proteger a la información, que constituye uno de los activos más importantes y de mayor valor para toda empresa.

Actualmente es común escuchar sobre el espionaje industrial, robo cibernético, “hackeo”, corrupción de la información, virus, pérdida, fuga de información, fallas en los sistemas, interrupción de servicios, etc.; lo cual indica que la información se encuentra expuesta a múltiples riesgos provocados o accidentales. Ante tal situación, es indispensable detectar las vulnerabilidades y tomar acciones que contrarresten dichos riesgos para la información.

ECUANET (MEGADATOS S.A.) requiere un plan estratégico, tal que facilite la implementación futura de las Normas ISO 27001 e ISO 27002 aplicadas a los servicios en la ciudad de Quito, garantizando así la confidencialidad, integridad y disponibilidad de la información. En base al modelo *Plan – Do – Check – Act* (PDCA), se presenta la propuesta a la Empresa, realizando previamente la identificación de los activos involucrados y una evaluación de los riesgos a los que se expone la información. Se contemplan soluciones a nivel técnico y a nivel de políticas de comportamiento por parte de los usuarios.

El estudio realizado en el presente Proyecto de Titulación, ha sido desarrollado en base a la situación actual y necesidades de la Empresa ECUANET (MEGADATOS S.A.); sin embargo, la metodología aplicada durante la ejecución del Sistema de Gestión de Seguridad de la Información (SGSI), así como las propuestas planteadas a la Empresa, podrían ser útiles para futuros estudios aplicados en otras Empresas que estén interesadas en obtener la Certificación ISO 27001.

CAPÍTULO 1

INTRODUCCIÓN A LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

1.1 PRINCIPIOS GENERALES DE LA SEGURIDAD DE LA INFORMACIÓN

1.1.1 INTRODUCCIÓN

En un mundo en el que la tecnología avanza a una velocidad vertiginosa y las comunicaciones requieren alcanzar distancias cada vez mayores, es prioritario contar con redes de información con un alto índice de confiabilidad, con el fin de resguardar la información que se desea transmitir o recibir.

El Internet, constituido por un conjunto de redes de comunicación interconectadas, representa actualmente el principal medio de comunicación, gestión y entretenimiento a nivel mundial.

Según el U.S. Census Bureau, el Ecuador cuenta con 14’573.101 habitantes; el índice de penetración de Internet según *Internet World Stats* (IWS), hasta Junio del 2009 es del 11,2%, que corresponde a 1’634.828 usuarios. Además, se proyecta que para fines del año 2010, de cada 10 ecuatorianos, 2 dispondrán del servicio de Internet. [1]

Resulta evidente que el Internet es el medio de comunicación más utilizado a nivel mundial; sin embargo se debe tomar en cuenta que también representa una de las vías principales, a través de la cual una red está expuesta a posibles amenazas. Hoy en día, los virus, intrusiones y ataques son muy comunes dentro de las redes; de modo que se debe tomar medidas adecuadas con el fin de proteger la información contenida en las mismas.

1.1.2 DEFINICIÓN DE SEGURIDAD DE LA INFORMACIÓN

La información puede presentarse en distintas formas: impresa, almacenada electrónicamente, escrita, video, audio; cualquiera sea su forma, la información requiere ser conservada y utilizada de manera segura.

La seguridad de la información hace referencia a cualquier método utilizado para proteger los datos almacenados en los dispositivos de almacenamiento externo contra el acceso de personas no autorizadas [2]. Es decir, consiste en la protección de la información contra amenazas internas y/o externas a las que podría estar expuesta una organización. La mitigación de las vulnerabilidades del sistema de seguridad de la información, con el cual opera la organización, garantizará mayores oportunidades, prestigio y credibilidad.

Se debe destacar que la seguridad de la información total no existe, pues diariamente se presentan nuevos riesgos que la amenazan; de modo que se debe trabajar para reducir dichos riesgos a niveles aceptables. Se evidencia así, que la seguridad de la información es un proceso que debe ser mejorado continuamente.

1.1.3 NECESIDAD DE SEGURIDAD

Para toda empresa o institución, su información constituye uno de los activos[1] más importantes y de mayor valor. Gracias a la correcta administración de la misma, una empresa puede mejorar su desempeño y ofrecer a los clientes un servicio de calidad, con el que se sientan seguros y satisfechos.

Actualmente es común escuchar sobre el espionaje industrial, robo cibernético, “hackeo”, virus, pérdida, fuga de información, fallas en los sistemas, interrupción de servicios, incendios, inundaciones, etc.; lo cual indica que la información se encuentra expuesta a múltiples riesgos provocados o accidentales. Ante tal

[1] Conjunto de todos los bienes y derechos con valor monetario que son propiedad de una empresa, institución o individuo, y que se reflejan en su contabilidad.

situación, es indispensable detectar las vulnerabilidades de las redes, tomar acciones que contrarresten los riesgos y salvaguardar la información.

Cisco, en base al desarrollo y a la seguridad, diferencia dos tipos de redes [3]:

- Red Cerrada: Consiste en una red diseñada e implementada en un ambiente corporativo, que provee conectividad solo a lugares conocidos, sin conexión a redes públicas.

- Red Abierta: Comprendida por una red diseñada para permitir la conectividad con redes públicas, inclusive con lugares desconocidos. Ésta se ha desarrollado debido al avance de las comunicaciones y del Internet.

En la Figura 1.1., se puede observar la diferencia entre ambas redes y la necesidad de implementar seguridades, principalmente en una red abierta.

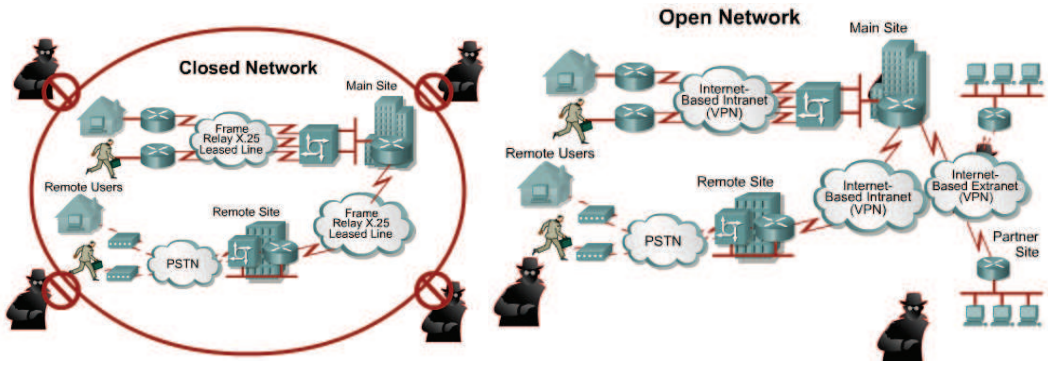


Figura 1.1: Red Cerrada y Red Abierta [3]

No es recomendable esperar a que un ataque se presente para tomar acciones al respecto. Resulta óptimo contar con planes estratégicos que sirvan para prever y evitar que la información de una organización se exponga a las amenazas. A más de planes de prevención, se debe contar con estrategias que mitiguen un ataque en el menor tiempo posible, en caso de presentarse.

Se deben implementar métodos que brinden seguridad a toda la información de una organización, tanto aquella referente con el personal, clientes, equipos, como la relacionada con métodos y procesos. Sin embargo, dependerá de la actividad a

la cual se dedique la empresa, el tipo de seguridad que se debe dar a la información.

Dada la necesidad de contar con una gestión de seguridad para la información en una organización, resulta imprescindible disponer de personal encargado de garantizar la utilización, disponibilidad y sobre todo la seguridad de la información.

1.1.4 COMPONENTES DE LA SEGURIDAD DE LA INFORMACIÓN

Para cumplir con el propósito de un sistema, que garantice la seguridad de la información, se deben integrar métodos que conserven la confidencialidad, integridad y disponibilidad.

- Confidencialidad: La información solo debe ser usada por personas autorizadas; de ninguna manera, una persona no autorizada debe tener acceso a la información, inclusive si no es intencional.

- Integridad: La información debe conservarse exacta y completa, sin modificaciones.

- Disponibilidad: El personal, entidad o procesos autorizados pueden acceder a la información y utilizarla en el momento que lo requieran.

1.2 VULNERABILIDADES, AMENAZAS Y ATAQUES

1.2.1 DEFINICIONES

Una vulnerabilidad es una debilidad inherente a toda red y dispositivo, incluyendo *routers*[2], *switches*[3], computadoras de escritorio, servidores e inclusive los propios dispositivos de seguridad.

---

[2] Dispositivo de capa 3. Útil en la conexión de redes para asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos. Trabaja en base a direcciones IP.

[3] Dispositivo de capa 2. Permite dividir dominios de colisión, envía la información a un usuario específico sin ser retransmitido al resto de los puertos. Su funcionamiento se basa en direcciones MAC.

Una amenaza se produce cuando ciertas personas interesadas y capacitadas, toman ventaja de debilidades de la seguridad para realizar acciones no permitidas. Las amenazas utilizan distintas herramientas y programas para atacar a redes y dispositivos de red, que generalmente son los puntos finales, tales como servidores o *hosts*[4].

Un ataque consiste en aprovechar una vulnerabilidad de un sistema informático, con propósitos desconocidos por el operador del sistema y que, por lo general, causan daño.

El objetivo principal de un Sistema de Gestión de Seguridad de la Información (SGSI) consiste en evitar o minimizar los ataques a los que una red podría estar expuesta, garantizando así que ninguna amenaza ponga en riesgo la seguridad de la información.

1.2.2 CLASIFICACIÓN DE LAS AMENAZAS

1.2.2.1 Amenazas no estructuradas

Son generalmente desarrolladas por personas que no tienen mucha experiencia en la ejecución de ataques a redes; se basan en herramientas básicas y sencillas. Sin embargo, este tipo de amenaza podría ser utilizada por el atacante para probar que tan segura es una red y cuán bien ésta es administrada.

1.2.2.2 Amenazas estructuradas

Son ejecutadas por personas capacitadas y conocedoras del tema. Desarrollan códigos, programas y técnicas sofisticadas para realizar ataques a las redes.

[4] En informática, se refiere a los computadores conectados a la red, que proveen o utilizan servicios de la misma.

1.2.2.3 Amenazas externas

Son desarrolladas por personas que no trabajan en la compañía cuya red es amenazada, de modo que no tienen acceso autorizado a las redes o sistemas. Los atacantes consiguen el ingreso a través del Internet o de servidores.

1.2.2.4 Amenazas internas

Se produce cuando cierto individuo de la compañía, que dispone de acceso autorizado a la red, tiene una cuenta en el servidor o acceso físico a la red, realiza un ataque al sistema informático o a la red de la compañía.

1.2.3 CLASIFICACIÓN DE LOS ATAQUES

1.2.3.1 Reconocimiento

Se basa en el descubrimiento no autorizado de información como: mapeo de sistemas, servicios e inclusive vulnerabilidades que presenta la red.

1.2.3.2 Acceso

Se produce cuando el atacante logra acceder a un dispositivo, a pesar de no disponer de una cuenta o contraseña para hacerlo, a través de herramientas que descubren alguna vulnerabilidad que permite el acceso.

1.2.3.3 Negación de servicio (DoS)

El atacante deshabilita o manipula la red o el sistema, con el propósito de impedir el uso de cierto servicio; en consecuencia, el sistema cae o se presenta considerablemente lento. Para este tipo de ataque, no es necesario que el atacante acceda al objetivo; es el ataque más común.

1.2.3.4 Gusanos, virus y troyanos

Un gusano ejecuta, de manera arbitraria, un código e instala una copia de sí mismo en la memoria de la computadora.

Un virus es un software malicioso, que se encuentra adjunto a otro programa para ejecutar una función no deseada, afectando a la computadora del usuario.

Un caballo troyano se diferencia del virus en que la aplicación entera fue realizada para presentarse como algo más, cuando en realidad se trata de una herramienta que ataca al equipo.

1.2.4 TIPOS DE ATACANTES

Se considera atacante al individuo que utiliza sus conocimientos, junto con diferentes medios informáticos, para afectar sistemas y obtener beneficios de manera ilícita. A continuación, se especifican los tipos de atacantes más comunes.

1.2.4.1 *Hacker*

Experto programador en computadoras que accede sin autorización a los recursos de una red, con intenciones maliciosas.

1.2.4.2 *Craker*

Individuo que tras romper la seguridad de un sistema, modifica el software original, eliminando la protección de anticopia.

1.2.4.3 *Phreaker*

Es un individuo que manipula la red telefónica para conseguir un funcionamiento que normalmente no es permitido; por ejemplo, hacer que el costo de una llamada de larga distancia sea igual al de una llamada nacional.

1.2.4.4 *Spammers*

Son individuos que envían una gran cantidad de mensajes de correo no solicitados. Usualmente, los *spammers* utilizan virus para tomar el control de un computador y enviar desde éste los mensajes.

1.2.4.5 *Carders*

También conocidos como piratas de tarjetas. Su objetivo principal son los sistemas con tarjetas con chip, especialmente tarjetas bancarias; para lo cual estudian el funcionamiento de dichos sistemas, determinando sus falencias.

1.2.4.6 *Script kiddies*

Son usuarios no muy experimentados que, por diversión, utilizan programas encontrados en Internet para ocasionar daños en los sistemas.

1.2.4.7 *Phisher*

Utiliza mensajes de correo electrónico o un medio similar para tratar de adquirir información sensible, como números de tarjetas de crédito o contraseñas.

1.3 ALTERNATIVAS CISCO PARA SEGURIDAD EN REDES

1.3.1 GENERALIDADES DE LOS DISPOSITIVOS Y SISTEMAS

Cisco presenta una amplia gama de opciones en cuanto a seguridad en redes: *Cisco IOS Firewall, Cisco Private Internet Exchange Security Appliance (PIX)* y *Cisco Adaptive Security Appliance* (*ASA*). Además presenta aplicaciones para administrar la seguridad como *Security Device Manager* (*SDM)* y *Adaptive Security Device Manager* (*ASDM)*.

1.3.1.1 Dispositivos y sistemas

1.3.1.1.1 Cisco IOS Firewall

El dispositivo de seguridad más conocido es el *firewall*. Un *firewall* es un sistema o grupo de sistemas que generan políticas de control de acceso entre dos o más redes.

Cisco IOS Firewall es una opción para software Cisco IOS que permite añadir mayor flexibilidad y mejorar capacidades existentes de soluciones de seguridad Cisco IOS.

Bloquea ataques, evita que individuos no autorizados accedan a la red y permite el acceso a usuarios autorizados. Integra funcionalidades de *firewall*, autenticación *proxy* y prevención de intrusiones; añade estado de red, filtrado, autenticación y autorización, bloqueo Java, alertas en tiempo real, monitoreo, entre otras.

Al configurar *Cisco IOS Firewall* en un *router* Cisco, se convierte en un *firewall* con aplicaciones como: listas de acceso, intercepción *Transmission Control Protocol* (TCP)[5], control de acceso, *Intrusion Prevention System* (IPS), mapeo de puertos, soporte de servidor de seguridad, traducción de direcciones de red, seguridad de red *Internet Protocol Security* (IPSec).

1.3.1.1.2 PIX Security Appliance

El PIX es un dispositivo de seguridad basado en hardware y software que provee filtrado de paquetes y tecnologías de servidor *Proxy*[6].

La serie de *Cisco PIX Security Appliance* 500 ofrece inspección de estado de *firewall*, acceso remoto *Virtual Path Network*[7] (VPN) y Punto-Punto, detección y

---

[5] Es un protocolo de comunicación orientado a conexión y fiable de la capa de transporte.

[6] Equipo intermediario entre el sistema del usuario e Internet. Usado para registrar el uso de Internet o para bloquear el acceso a ciertas páginas Web.

[7] Tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como el Internet.

prevención de intrusiones. Las aplicaciones varían dependiendo del modelo, que puede ser: PIX 501, PIX 506E, PIX 515E, PIX 525 y PIX 535.

a. PIX 501

- Recomendable para oficinas pequeñas. Conveniente para el uso de varias computadoras que comparten una única conexión.
- Capacidades de *Internet Key Exchange* (IKE)/IPSec VPN.
- Puede actuar como un *Dynamic Host Configuration Protocol* (DHCP) para asignar automáticamente direcciones de red a las computadoras.
- Dos tipos de encriptación[8] VPN: DES y 3DES.

b. PIX 506E

- Recomendable para oficinas remotas con redes pequeñas o medianas.
- Dos interfaces *Fast Ethernet* y 2 interfaces virtuales basadas en 802.1q.
- Dos tipos de encriptación VPN: DES y 3DES.

c. PIX 515E

- Recomendable para redes pequeñas o medianas.
- Soporta hasta 6 puertos Ethernet 10/100.
- Aceleración IPSec, proporcionada por una tarjeta integrada *PIX Firewall VPN Accelerator Plus (VAC+)* o por PIX *Security Appliance VAC.*

d. PIX 525

- Aconsejable para redes medianas o grandes.
- Dos interfaces Fast Ethernet 10/100 y soporta una combinación adicional de interfaces Fast Ethernet o Gigabit Ethernet.

[8] Proceso para volver ilegible información considerada importante. Para leer la información encriptada, se requiere una clave.

- Ofrece provisión de energía (AC o 48 DC) y redundancia con una segunda fuente.

e. PIX 535

- Recomendado para redes grandes o para proveedores.
- Soporta combinación de interfaces 10⁄100 Fast Ethernet o Gigabit Ethernet.
- Tarjeta integrada aceleradora para VPN.
- Redundancia en provisión de energía.
- *Throughput*[9] de 1.7 Gbps. Hasta 500000 conexiones simultáneas.

1.3.1.1.3 Adaptive Security Appliance (ASA)

Un ASA es un dispositivo que provee una defensa multicapa, a través de servicios integrados de seguridad como inspección de estado de *firewall*, acceso remoto VPN y Punto-punto, WebVPN y prevención de intrusiones.

Cisco desarrolló la familia 5500 en tres modelos disponibles: ASA 5510, ASA 5520 y ASA 5540.

a. ASA 5510

- Aconsejable para negocios pequeños o medianos.
- Hasta 5 interfaces Fast Ethernet 10⁄100.
- Soporta un *slot Security Services Module* (SSM) opcional que provee IPSec.
- *Throughput* de 100 Mbps. Hasta 64000 conexiones concurrentes.

b. ASA 5520

- Se recomienda para negocios pequeños o medianos.
- Cuatro Interfaces Gigabit Ethernet 10⁄100⁄1000.
- Soporta un *slot* SSM que provee IPSec.

[9] Conocido también como rendimiento. Se refiere a la cantidad de datos que se transmiten durante un tiempo determinado.

- *Throughput* de 200 Mbps. Hasta 130000 conexiones concurrentes.

c. ASA 5540

a. Recomendable para redes grandes.
b. Incorpora 4 interfaces Gigabit Ethernet 10/100/1000. 1 interfaz de administración Fast Ethernet 10/100.
c. *Slot* Opcional SSM que prove IPSec.
d. *Throughput* de 400 Mbps. Hasta 280000 conexiones concurrentes.

Los comandos y usos del PIX y de ASA son los mismos, excepto por la aplicación de VPN mediante *Secure Sockets Layer* (SSL) o WebVPN, que solo está disponible para ASA. Adicionalmente estos dos dispositivos pueden mejorar sustancialmente sus características al añadir módulos y tarjetas.

1.3.1.1.4 Finesse Operation System

Es el sistema operativo de Cisco que "corre" directamente sobre el hardware de *PIX Security Appliance* o *ASA Adaptive Security Appliance*.

1.3.1.1.5 ASA Adaptive Security Algorithm

Es la base de *Security Appliance*. El algoritmo ASA es orientado a conexión. Se crean sesiones basadas en direcciones origen y destino. Cuando una conexión TCP se establece, la información de direcciones IP y puertos se inserta en una tabla de estado de sesión. Se comparan los paquetes con los objetos de sesión, permitiendo el flujo solo si una conexión se encuentra en la tabla.

1.3.1.1.6 FWSM Firewall Services Module

Es un módulo integrado basado en la tecnología de *PIX*, que provee funcionalidades de *firewall* en los *switches* y *routers*.[10]

[10] Se aplica para los *Switches* Cisco Catalyst 6500 y *Routers* Cisco 7600.

FWSM provee 5 Gbps de *throughput* por módulo. Soporta VLANs y ofrece enrutamiento dinámico. Por defecto, todo el tráfico es denegado en un FWSM.

FWSM ocupa 1 *slot* en el *switch* y se puede instalar hasta 4 módulos. No puede funcionar independientemente, a diferencia del PIX. Antes de configurar una política de seguridad en un FWSM, se debe inicializar el FWSM, configurar las VLANs del *switch* y asociar VLANs con el FWSM.

1.3.1.1.7 Security Device Manager (SDM)

Útil para *routers* que incorporan el software Cisco IOS. SDM simplifica la configuración del *router* y de la seguridad. Guía paso a paso en la configuración de interfaces *Local Area Network* (LAN) y *Wide Area Network* (WAN), *firewall*, IPs, IPSec VPNs. Detecta configuraciones erradas y propone soluciones.

La ventana inicial provee información básica sobre el hardware, software y configuración del *router*. En la Figura 1.2 se observan las cuatro secciones de la ventana inicial: información sobre el router, revisión de la configuración, barra de herramientas y barra de menú.

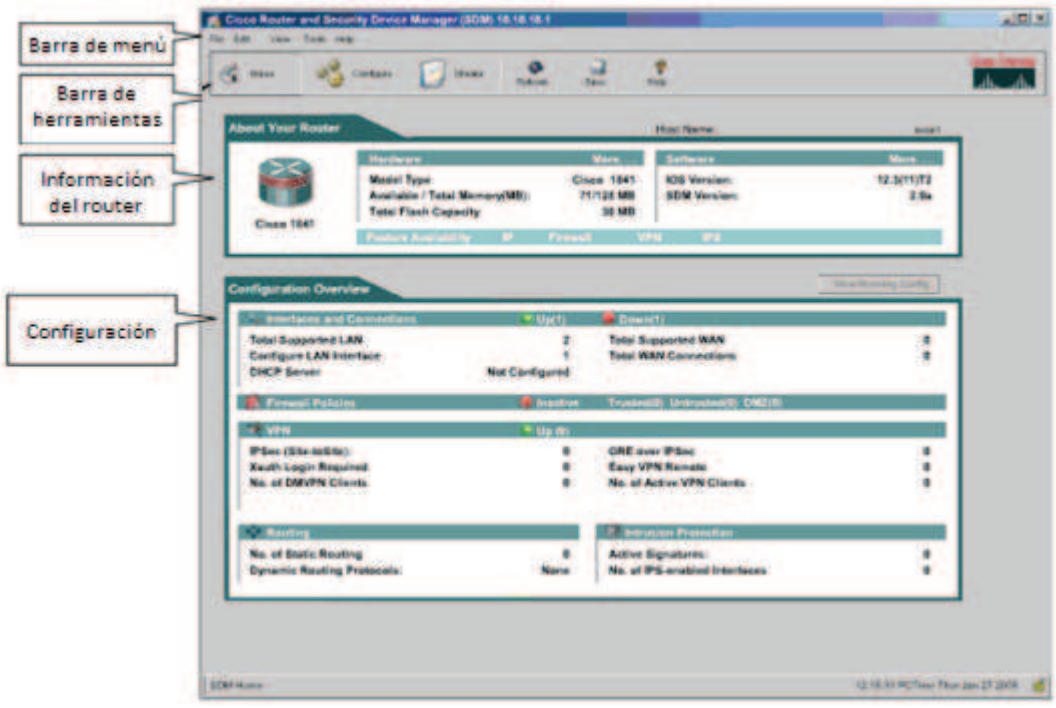


Figura 1.2: Ventana de inicio de SDM [4]

Adaptive Security Device Manager (ASDM) es una herramienta de configuración basada en *browser*. Diseñada para levantar, configurar y monitorear remotamente un PIX, sin requerir un conocimiento extenso del *Command Line Interface* (CLI).

1.3.1.2 Licencias para aplicaciones de seguridad

La licencia del PIX determina el nivel de servicio que provee, sus funciones en una red, el número máximo de interfaces y su memoria. Con cada licencia, Cisco provee una llave de activación basada en el tipo de licencia y número serial del PIX. Para habilitar los beneficios de la licencia, se debe ingresar la llave de activación en la configuración del PIX.

PIX *Security Appliance* 515E, 525, 535 con licencia sin restricciones, así como el ASA *Security Appliance*, pueden ser divididos en múltiples *firewalls* virtuales, conocidos como contextos de seguridad. Cada contexto es un *firewall* independiente con sus propias políticas de seguridad, interfaces y administradores.

1.3.1.3 Configuración básica del PIX *Security Appliance*

PIX Security Appliance contiene un grupo de comandos basados en Cisco IOS, por lo que la configuración será muy similar a la realizada en un *router*.

1.3.1.3.1 Modos

El PIX provee de 3 modos de acceso administrativo, tales como:

- Modo no privilegiado: Disponible cuando se accede al PIX. El *prompt* o indicador es >. Este modo provee una vista restringida y limitada de los parámetros del PIX.

- Modo privilegiado: Despliega el *prompt* #. Permite a los usuarios cambiar los parámetros actuales. Cualquier comando no privilegiado trabaja también en modo privilegiado.

- Modo de configuración: Despliega el *prompt* (config) #. Permite a los usuarios cambiar configuraciones del sistema. Todos los comandos privilegiados, no privilegiados trabajan en este modo.

Al acceder a un dispositivo de seguridad, se presenta el *prompt* **pixfirewall>** cuando se usa un PIX, o **ciscoasa>** si se usa un ASA. Estos indicadores corresponden al modo no privilegiado.

El comando **enable** permite ingresar al modo privilegiado. El PIX generalmente solicita al usuario una contraseña. El comando **enable password** habilita la contraseña en modo privilegiado.

Se usa el comando **configure terminal** para cambiar de modo privilegiado a modo de configuración. El comando **exit** o **quit** se utiliza para salir o retornar al modo anterior.

1.3.1.3.2 Niveles de Seguridad

El nivel de seguridad indica si una interfaz es más confiable y protegida con respecto a otra. El rango de niveles de seguridad va de 0 a 100, siendo 100 el nivel de mayor seguridad.

La regla primaria de los niveles de seguridad consiste en que una interfaz con un nivel de seguridad mayor puede acceder a otra con un nivel de seguridad inferior. Una interfaz con un nivel de seguridad inferior no puede acceder a otra con un nivel de seguridad superior sin constar en una *Access Control List* (ACL). No existe flujo de tráfico entre 2 interfaces con el mismo nivel de seguridad.

Cuando se configuran múltiples interfaces, el nivel de seguridad designa si una interfaz es interna o externa relativa a otra interfaz. Una interfaz es considerada interna en relación a otra si su nivel de seguridad es mayor y es considerada externa si su nivel de seguridad es inferior.

1.3.1.3.3 Comandos básicos de configuración para PIX

Por defecto, el *hostname* del PIX es *pixfirewall* y del ASA es *ciscoasa*. Con el comando **hostname**, se cambia el nombre del equipo.

El comando **interface** configura el tipo y capacidad de cada interfaz**.** Las interfaces del PIX están numeradas de 0 a x y las del ASA son 0⁄0, 0⁄1, 0⁄2, etc. Luego de ingresar el comando **interface**, el *prompt* cambia al nivel de sub-comando de configuración de la interfaz. En la configuración de la interfaz se puede establecer sub-comandos como velocidad, nombre de la interfaz, nivel de seguridad, dirección IP y otros parámetros.

El comando **nameif** asigna un nombre a cada interfaz del PIX. Con **ip address** cada interfaz del PIX puede ser configurada con una dirección IP específica; mientras que si se cuenta con un servidor DHCP[11], se puede usar el comando **ip address dhcp.** El comando **security level** especifica el nivel de seguridad de las interfaces y **speed** asigna la velocidad de la conexión en la interfaz**.**

1.3.1.3.4 Tiempo

Clock maneja el reloj del PIX**,** habilitando hora, mes, día y año.

El PIX genera mensajes *Syslog* para eventos del sistema como alertas. El comando **show logging** sirve para ver la configuración *log* y cualquier mensaje almacenado internamente. El comando **clear logging** borra el *buffer*[12] para evitar exceso de mensajes. El comando **logging timestamp** es usado para añadir un

[11] Servidor que asigna direcciones IP dinámicamente.

[12] Espacio de memoria, en que se almacenan datos para evitar que la aplicación que los requiera, se quede sin datos en algún momento. A diferencia de la caché, los datos del *buffer* siempre serán utilizados.

indicador de tiempo a estos mensajes. Se usa **clock set** para asegurar que la hora correcta aparezca en los mensajes *Syslog*.

1.3.1.4 Traducciones y conexiones de PIX

1.3.1.4.1 Network Address Translation (NAT)

Con **nat-control** habilitado, cuando un paquete IP[13] es enviado desde la red al PIX, la dirección origen es extraída y comparada con una tabla de traducciones existentes. Si la dirección aún no está en la tabla, se traduce; una nueva entrada se crea y se asigna una dirección IP de un grupo global de direcciones. El grupo global es configurado con el comando **global**. Tras la traducción, la tabla se actualiza y el paquete IP es enviado al destino.

El PIX soporta 2 tipos de traducciones de dirección: dinámica y estática. En la traducción dinámica, se traducen direcciones de *hosts* a un grupo de direcciones IP. En la traducción estática (comando **static**) se provee un mapeo permanente uno-a-uno entre dos direcciones IP.

El comando **nat 0** permite deshabilitar la traducción de dirección, de tal forma que las direcciones IP internas son visibles en el exterior sin traducción de dirección. Generalmente este proceso es aplicado para escenarios que cuentan con Virtual Private Networks (VPN).

1.3.1.4.2 Port Address Translation (PAT)

Normalmente, una red recibe solo un pequeño número de direcciones enrutables de su *Internet Service Provider* (ISP), mientras el número de *hosts* es mucho mayor. Para solucionar esta situación, puede usarse PAT. Con PAT, múltiples conexiones originadas desde *hosts* diferentes pueden ser traducidas en una dirección IP global.

---

[13] Unidad fundamental de la capa Internet del modelo TCP/IP. Conocido también como PDU de capa 2.

1.3.1.5 Capacidades de enrutamiento del PIX

1.3.1.5.1 LANs Virtuales

Con el PIX Versión 6.3 y superiores, se pueden asignar VLANs a las interfaces físicas del PIX o configurar múltiples interfaces lógicas en una única interfaz física y asignar cada interfaz lógica a una VLAN. El PIX soporta solo VLANs 802.1Q[14].

Con el comando **vlan_id** se asigna un VLAN ID a una subinterfaz. Se aplica el comando **no shutdown** a la interfaz principal para habilitar las subinterfaces. Con el comando **nameif** se define un nombre para cada VLAN. El comando **ip address** asigna direcciones IP a las VLANs. Para configurar un nivel de seguridad en una subinterfaz, se usa el comando **security-level *number***.

1.3.1.5.2 Enrutamiento estático y RIP

A pesar de que el PIX no es un *router*, éste tiene ciertas capacidades de enrutamiento. El comando **route** crea rutas estáticas. La mayoría de rutas pueden ser eliminadas con el comando **clear configure route**. Otra manera para construir la tabla de enrutamiento del PIX es habilitando el comando **rip**, que le permite aprender dinámicamente las rutas. Pese a que el PIX usa rutas aprendidas dinámicamente para llevar tráfico a sus destinos, éste no las propaga a otros dispositivos. El PIX no puede transmitir actualizaciones RIP entre interfaces, pero puede advertir a una de sus interfaces como ruta por defecto.

1.3.1.5.3 Open Shortest Path First (OSPF)

El software versión 6.3 de PIX, introduce soporte para enrutamiento dinámico con el protocolo de enrutamiento OSPF, ampliamente utilizado debido a su rápida convergencia después de cambios en la topología.

---

[14] Protocolo IEEE que permite a múltiples redes compartir el mismo medio físico, de forma transparente.

Se habilita OSPF con el comando **router ospf *pid***, luego se definen las redes del PIX en las que "corre" OSPF. Finalmente se definen las áreas OSPF. Para definir las redes y el área ID, se usa el subcomando **network area**.

1.3.1.5.4 Enrutamiento Multicast[15]

IP Multicasting consiste en la transmisión de un paquete IP a un grupo de *hosts*, identificados con una dirección de destino IP única.

Los *hosts* que desean recibir *multicasts*, deben unirse a un grupo *multicast* y los *routers* que transmiten datagramas *multicasts* deben conocer qué *hosts* pertenecen a cada grupo. Los *routers* encuentran la información enviando mensajes de petición *Internet Group Management Protocol* (IGMP). Los miembros de un grupo *multicast* responden con un mensaje IGMP, indicando el grupo *multicast* al que pertenecen.

El comando **igmp query-interval** configura la frecuencia con que los mensajes IGMP son enviados. La negación del comando retorna al tiempo por defecto de 60 segundos. Con **igmp query-max-response-time** se especifica el tiempo de respuesta máximo.

1.3.2 IDENTIDAD Y CONFIABILIDAD

AAA es el acrónimo de Autenticación, Autorización y Cuenta. AAA es esencial para proveer acceso remoto seguro a la red y administración remota de los dispositivos de la misma. Es un servicio que puede ser implementado localmente en un dispositivo o administrado desde un servidor central "corriendo" protocolos RADIUS o TACACS+.

[15] Envío simultáneo de la información de una red a múltiples destinos.

1.3.2.1 *Terminal Access Controller Access Control System plus* (TACACS+)

TACACS entrega el nombre y la contraseña de un usuario a un servidor centralizado. El servidor puede ser una base de datos TACACS o una base de datos similar.

TACACS+ es la versión mejorada de TACACS. Provee servicios de AAA independientemente. Cada servicio puede relacionarse con su propia base de datos o puede ser usado con otros servicios disponibles en el servidor o en la red.

1.3.2.2 *Remote Authentication Dial-In User Service* (RADIUS*)*

Es un protocolo AAA que asegura el acceso remoto a redes y las protege de accesos no autorizados. Se compone de un servidor, cliente y el protocolo con un formato que usa UDP/IP.

En la Figura 1.3 se distingue al servidor y cliente RADIUS. Un *Network Access Server* (NAS*)* opera como un cliente de RADIUS. El cliente envía información a los servidores RADIUS y actúa ante la respuesta que es retornada. Los servidores RADIUS reciben la solicitud de conexión del usuario para proporcionarle servicio.

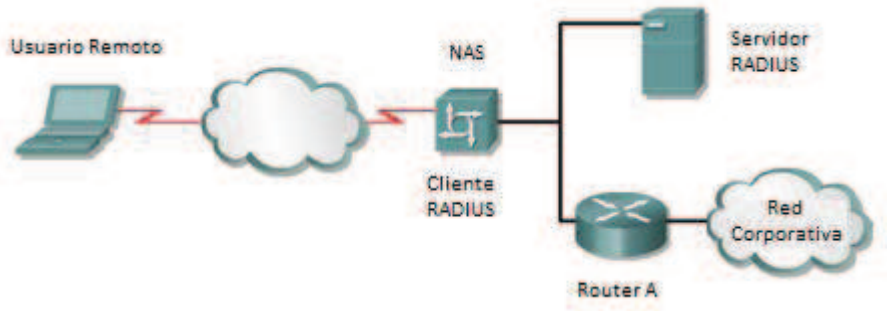


Figura 1.3: Topología de red usando un servidor RADIUS [5]

Las comunicaciones entre el cliente y servidor RADIUS son autenticadas usando un secreto compartido. Toda contraseña de usuario es encriptada en su envío.

1.3.2.3 TACACS+ vs. RADIUS

Las diferencias fundamentales entre TACACS+ y RADIUS se indican en la Figura 1.4.

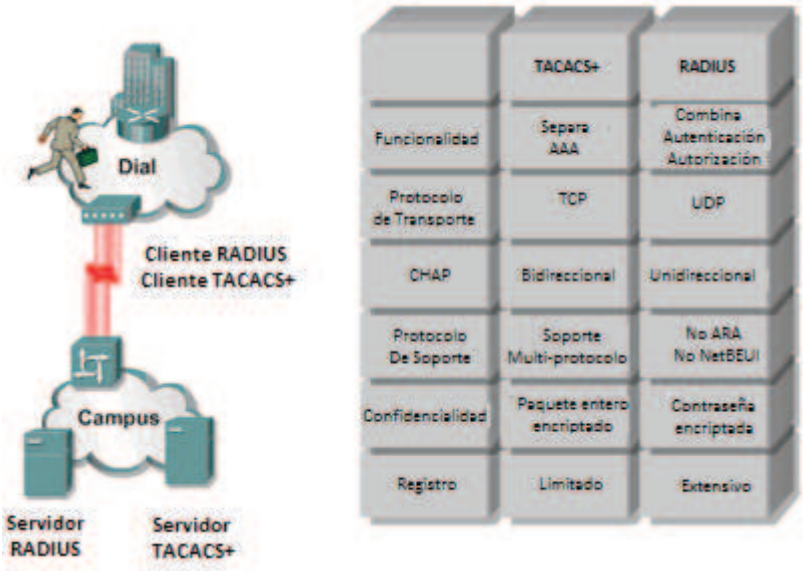


Figura 1.4: Comparación entre TACACS+ y RADIUS [5]

El hecho de que RADIUS combine autenticación y autorización, da menos flexibilidad; sin embargo utiliza *User Datagram Protocol* (UDP)[16] para simplificar la implementación del servidor y cliente, creándose la necesidad de métodos que mejoren la confiabilidad, como retransmisión de paquetes. Generalmente, se considera a TACACS+ superior a RADIUS, debido a que TACACS+ encripta el paquete entero, mientras que RADIUS solo encripta la porción de contraseña de secreto compartido.

1.3.2.4 Tecnologías de autenticación

1.3.2.4.1 Contraseñas Estáticas

Un método estático de autenticación de nombre de usuario/contraseña se conserva invariante hasta que el administrador del sistema o usuario lo cambie. Este método es susceptible a ataques, escuchas no deseadas o robo. La

[16] Protocolo del nivel de transporte, basado en el intercambio de datagramas. No es orientado a conexión y tampoco es confiable.

susceptibilidad se debe a que la contraseña no se cambia y los atacantes pueden ingresar varias veces con la contraseña descubierta.

Con el método cambiante de autenticación de nombre de usuario/contraseña, el usuario es obligado a cambiar la contraseña luego de un determinado tiempo. Este método es más seguro; sin embargo, aún es susceptible a ataques.

1.3.2.4.2 Contraseñas de "Una Vez" y Tarjetas Token

Una manera para crear contraseñas seguras para conexiones remotas consiste en usar algoritmos *hash*[17] de una vía, para crear un esquema de contraseña de "una vez"; esto es lo que hace *S/Key*. S/Key protege contra escuchas no deseadas sin modificación del software del cliente.

Los componentes de S/Key son: cliente, *host* y calculador de contraseña. El cliente provee la capa de acceso al usuario. El *host* procesa la solicitud y almacena la contraseña de "una vez". El calculador de contraseña es una función *hash* de una vía, definida para perder información cada vez que se aplica.

Otro método de autenticación de contraseña de "una vez" se basa en el uso de tarjetas *token* o inteligentes. Cada tarjeta es programada para un usuario específico y cada usuario tiene un PIN único que puede generar una contraseña cifrada estrictamente a la tarjeta correspondiente. El usuario genera una contraseña de "una vez" con la tarjeta usando un algoritmo de seguridad. El cliente remoto envía la contraseña de "una vez" al servidor *token*, que usa el mismo algoritmo para verificar que la contraseña es correcta.

1.3.2.4.3 Certificados digitales

Un certificado o firma digital es un *hash* encriptado que se añade al documento. Puede ser usado para confirmar la identidad del remitente y la integridad del

[17] Algoritmo que se utiliza para generar un valor de *hash* para algún dato, como por ejemplo claves. Un algoritmo *hash* hace que los cambios que se produzcan en los datos de entrada provoquen cambios en los bits del *hash*.

documento. Las firmas digitales están basadas en una combinación de encriptación de llave pública y algoritmos de función *hash* de una vía. Contiene información para identificar a un usuario o dispositivo, como el nombre, número serial, compañía o dirección IP. Además contiene una copia de la llave pública de identidad. Un *Certificate Authority* (CA) firma el certificado. El CA es un grupo confiable para el receptor, que valida identidades y crea certificados digitales.

Sin certificados, al añadir un dispositivo nuevo en la red, se debe cambiar la configuración de todos los dispositivos. Utilizando certificados digitales, cada dispositivo es enrolado con un CA. Cuando dos dispositivos desean comunicarse, intercambian certificados, sin necesidad de reconfigurar los dispositivos.

1.3.2.5 *Cisco Identity Based Networking Services* (IBNS)

Cisco IBNS es una solución integrada que combina varios productos Cisco de autenticación, control de acceso y políticas de usuario para asegurar la conectividad. Está administrada por un servidor RADIUS *Cisco Secure Access Control Server* (ACS). Combina control de acceso y perfiles de usuario a la conectividad segura de redes, servicios y aplicaciones. Se basa en RADIUS e implementaciones 802.1x.

Con Cisco IBNS se obtienen los siguientes beneficios:

- Adaptabilidad para ofrecer mayor flexibilidad y movilidad. Con la creación de perfiles de usuario o grupos con políticas que definen las relaciones entre usuario y recursos de la red se facilitan los procedimientos.

- Combinación de autenticación, control de acceso y políticas de usuario. Gracias a que las políticas de usuario están asociadas con los usuarios y no con los puertos, se ofrece más libertad a los usuarios.

1.3.2.5.1 802.1x

802.1x es una estructura estandarizada, definida por el *Institute of Electrical and Electronics Engineers* (IEEE). Es designada para proveer acceso a la red, basada en puertos. Este servicio es llamado autenticación puerto-nivel porque, por razones de seguridad, es ofrecido a un único equipo final para un puerto físico dado. Define tres roles en el proceso de autenticación, como se observa en la Figura 1.5.

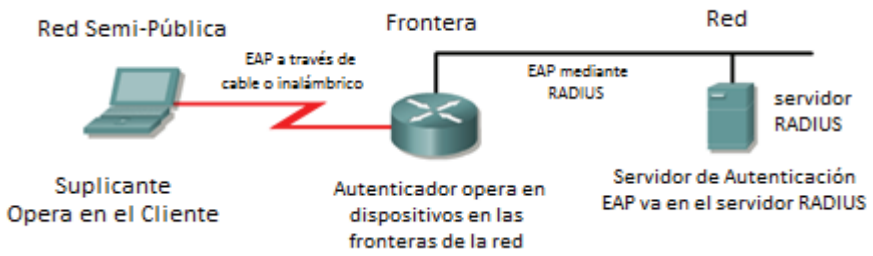


Figura 1.5: Componentes de 802.1x [5]

El equipo final que requiere acceso a la red es el suplicante. El dispositivo al que se conecta el suplicante y a través del cual obtiene permiso de acceso a la red es el autenticador. El servidor de autenticación es el responsable de la autenticación del suplicante. El proceso de autenticación, que consta de intercambios de mensajes *Extensible Authentication Protocol* (EAP*)* ocurre entre el suplicante y el servidor de autenticación.

Una alternativa para seguridad en *Wireless LAN* (WLAN)[18] es el desarrollo de una estructura que provee autenticación centralizada y distribución dinámica de llaves. Esta alternativa se basa en el uso de 802.1x y *Extensible Authentication Protocol* (EAP). Luego de la asociación de un cliente inalámbrico, el cliente y el servidor RADIUS intercambian mensajes EAP para una autenticación mutua. Se verifican las credenciales y si la autenticación mutua es satisfactoria, el servidor RADIUS y el cliente obtienen una llave *Wired Equivalent Privacy* (WEP) útil para el cliente.

[18] Sistema de comunicación de datos inalámbrico flexible, muy utilizado como alternativa a las redes LAN cableadas o como extensión de éstas.

1.3.2.5.2 Implementaciones alámbricas e inalámbricas

802.1x soporta dos topologías: punto a punto y LAN inalámbrica. En una configuración punto a punto, solo un cliente puede estar conectado al puerto 802.1x habilitado del *switch*. En una configuración inalámbrica, el puerto 802.1x configurado como *host* múltiple, al ser autorizado, todos los *hosts* adjuntos a ese puerto tienen acceso a la red. Si el puerto no es autorizado, el *switch* impide el acceso a la red a todos los clientes adjuntos.

1.3.2.6 *Network Admission Control* (NAC)

Usa la infraestructura de la red para reforzar el cumplimiento de las políticas de seguridad en todos los dispositivos que buscan acceder a los recursos de la red, reduciendo el riesgo de virus y gusanos. Las decisiones de acceso a la red pueden estar basadas en la información de estado de antivirus de los dispositivos en los equipos finales, en la versión del sistema operativo, nivel de parche del sistema operativo o componentes y versión de *Cisco Security Agent*.

NAC puede identificar dispositivos que no cumplan con las políticas de seguridad y denegarles el acceso, los ubica en un área de cuarentena o les permite un acceso restringido a los recursos de la red.

1.3.2.6.1 Componentes

NAC está conformado por 4 componentes, como se observa en la Figura 1.6.

Cisco y NAC integran *Cisco Trust Agent* (CTA). CTA recoge la información de estado de seguridad de varios software de seguridad de los clientes y comunica a la red Cisco conectada, donde las decisiones son tomadas.

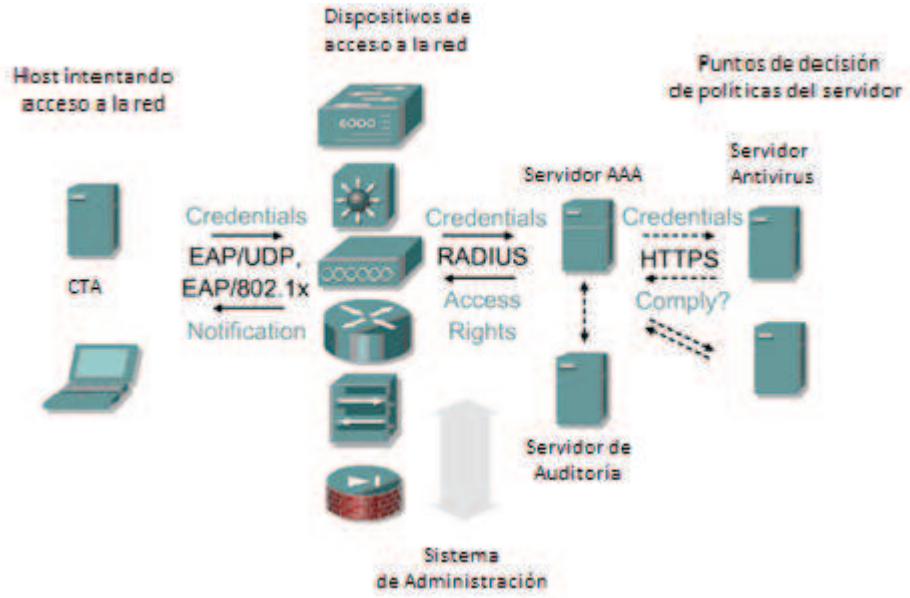


Figura 1.6: Componentes de NAC [5]

Los dispositivos que refuerzan las políticas de control de admisión son *routers*, *switches*, *access points* inalámbricos y aplicaciones de seguridad. Éstos demandan credenciales de *host* y envían la información a los servidores.

El servidor de políticas evalúa la información de seguridad del equipo final para determinar la política de acceso a aplicar. La base del sistema de servidor de políticas es *Cisco Secure* ACS aplicando RADIUS.

1.3.2.6.2 Operación

En la Figura 1.7, se resume la operación de NAC.

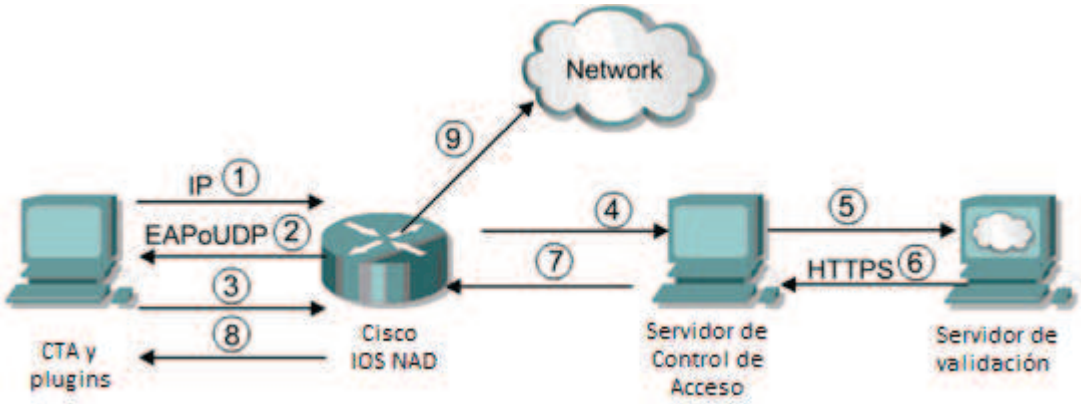


Figura 1.7: Operación de NAC [5]

En el proceso 1, el CTA indica que el cliente envía una solicitud para acceder a la red. Luego, en el proceso 2, NAD inicia el proceso de validación de postura. La identidad que recibe del CTA pasa por *Cisco Secure ACS* que luego inicia una sesión protegida EAP (PEAP) con el CTA. En el paso 3, CTA envía su credencial a NAD, que posteriormente la transfiere usando el protocolo RADIUS a *Cisco Secure ACS*. Las credenciales contienen atributos que conservan información acerca del estado actual del software de los clientes.

Cisco Secure ACS revisa y valida las credenciales, comparando los atributos contenidos en las mismas con su base de datos de políticas. *Cisco Secure ACS* puede además ser configurado para pasar estas credenciales a un servidor externo para validación, como se observa en el proceso 5.

Cisco Secure ACS ubica al cliente en un grupo, que puede ser Saludable, Revisado, Cuarentena o Desconocido. Envía la ACL apropiada para el grupo al NAD a ser aplicado al cliente, y posteriormente se envía la información al CTA.

1.3.3 CISCO SECURE ACS

1.3.3.1 Introducción a *Cisco Secure* ACS para Windows

ACS para el servidor Windows provee servicios AAA a dispositivos de la red como *routers*, servidores de acceso, PIX, concentradores VPN. Un cliente AAA es cualquier dispositivo que usa uno de los protocolos AAA soportado por *Cisco Secure ACS*. ACS utiliza los protocolos TACACS+ y RADIUS. El nivel de seguridad básico de *Cisco Secure ACS* es *Password Authentication Protocol* (PAP), con el que los usuarios se autentican una sola vez. *Challenge Handshake Authentication Protocol* (CHAP) permite un nivel de seguridad mayor, con contraseñas encriptadas cuando el cliente se comunica con el NAS.

Cisco Secure ACS combina autenticación, acceso de usuario o administrador y control de políticas. Esto permite mayor flexibilidad y movilidad para el usuario. Con una base de datos central para todas las cuentas de usuario, *Cisco Secure ACS* centraliza el control de los privilegios de usuario[19] y los distribuye a cientos o miles de puntos de acceso a lo largo de la red.

1.3.3.2 Autenticación y Bases de Datos de Usuarios

La autenticación determina la identidad del usuario y verifica la información. La autenticación tradicional utiliza un nombre y contraseña modificada. Métodos más modernos y seguros se basan en tecnologías como CHAP y *One-Time Passwords* (OTPs) contraseñas de "una vez". *Cisco Secure ACS* soporta varias soluciones OTP, incluyendo PAP para acceso de nodos remotos. Las tarjetas *token* son consideradas uno de los mecanismos OTP más poderosos.

Cisco Secure ACS autoriza el uso de la red, basado en un grupo de parámetros de una base de datos de usuario. Todos los usuarios autenticados por *Cisco Secure ACS* o bases externas, tienen una cuenta en la base de datos de usuario *Cisco Secure ACS*. A menos de que *Cisco Secure ACS* sea configurado para autenticar usuarios con una base de datos externa, se usa la base de datos *Cisco Secure ACS* durante la autenticación.

1.3.3.3 Arquitectura

Entre los servicios *Secure Cisco ACS*, se encuentran: CSAdmin que provee la interfaz HTML[20], CSAuth que provee servicios de autenticación, CSDBSync se encarga de la sincronización. Además se ofrece CSLog que provee servicios de acceso. CSMon provee monitoreo, recordatorio y notificación. CSTacacs provee comunicación entre clientes TACACS+ AAA y CSAuth. CSRadius permite comunicación entre clientes RADIUS AAA y el servicio CSAuth.

---

[19] Aplicaciones a las cuales un usuario podrá acceder dependiendo del área en la cual se desempeña.
[20] Siglas de *HyperText Markup Language*, es el lenguaje de marcado predominante para la elaboración de páginas web.

1.3.3.4 Funcionamiento de *Cisco Secure ACS*

1.3.3.4.1 Usando solo la Base de Datos ACS

Con los protocolos RADIUS o TACACS+, el NAS direcciona todas las solicitudes para acceder a la red, a *Cisco Secure ACS* para autenticación y autorización, verificándose el nombre de usuario y contraseña en la base de datos de *Cisco Secure ACS*. Se asignan autorizaciones y la información de la cuenta se ingresa al servicio de acceso de *Cisco Secure ACS*.

1.3.3.4.2 Usando Base de Datos Windows

El nombre de usuario y contraseña son enviados a la base de datos de usuario Windows 2000 para la autenticación. Si se aprueba, Windows 2000 concede el permiso como un usuario local, se envía respuesta a *Cisco Secure ACS* y la autorización es asignada.

1.3.3.4.3 Usando Base de Datos Externa de Usuario

Se puede configurar *Cisco Secure ACS* para solicitar autenticación de usuarios a una o más bases de datos externas. Para que *Cisco Secure ACS* pueda interactuar con una base de datos externa, se utiliza una *Application Programming Interface* (API), que permite el desarrollo rápido de nuevas extensiones.

1.3.3.4.4 Tarjetas Token

Para muchos servidores *token*, *Cisco Secure ACS* actúa como cliente. Para otros, se usa la interfaz RADIUS del servidor *token* para las solicitudes de autenticación. Después de que el nombre de usuario es ingresado en la base de datos de *Cisco Secure ACS*, CSAuth revisa al servidor *token* para verificar el nombre de usuario y contraseña de la tarjeta. El servidor aprueba o niega la validación.

1.3.3.4.5 Contraseñas Cambiantes de Usuario

Con *Cisco Secure ACS* para Windows Server 3.2, se puede habilitar *User-Changeable Password* (UCP). UCP es una aplicación que permite a los usuarios cambiar sus contraseñas *Cisco Secure ACS*.

1.3.3.5 Configuración de RADIUS y TACACS+ con *Cisco Secure ACS*

1.3.3.5.1 Instalación

Si *Cisco Secure ACS* es utilizado para autenticar usuarios con una base de datos de dominio de Windows, se debe asegurar que a más de instalar *Cisco Secure ACS*, se necesita configuración Windows.

Para el primer cliente AAA que será configurado para usar servicios AAA provistos por *Cisco Secure ACS*, se determina cuál protocolo AAA y proveedor se implementará. Luego de grabar el nombre del cliente AAA, se graba la dirección IP del cliente AAA, así como la dirección IP de la computadora donde *Cisco Secure* ACS será instalado. Finalmente, se graba la llave TACACS+ o RADIUS.

1.3.3.5.2 Configuración de TACACS+

Al configurar el *router*, se habilita TACACS+, se especifica la lista de servidores *Cisco Secure ACS* y se configura la llave de encriptación que se usará para la transmisión de datos entre el *router* y el servidor *Cisco Secure ACS*.

Con el comando **aaa new-model** se obliga al *router* a obviar cualquier método de autenticación configurado previamente. Como mínimo, se deberían ingresar los siguientes comandos:

Router(config)#**aaa new-model**
Router(config)#**aaa authentication login default group tacacs+ enable**

a. Comandos para TACACS+

En la configuración global, se ingresan los comandos mostrados en la Figura 1.8, con la dirección IP de los servidores *Cisco Secure ACS* y la llave de encriptación.

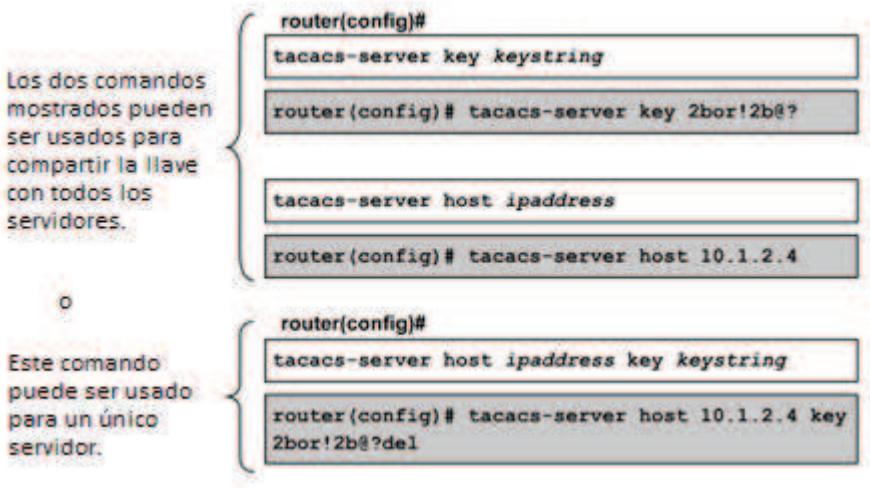


Figura 1.8: Comandos de configuración para TACACS+ [6]

El comando **tacacs-server key** es utilizado cuando dos o más servidores TACACS+ comparten la misma llave. Con el comando **tacacs-server host** varios servidores *Cisco Secure ACS* pueden ser especificados, cada uno con su propia llave.

b. Comandos para AAA

Después de habilitar AAA en el servidor de acceso, se definen las listas de métodos de autenticación. Las listas de métodos de autenticación son perfiles de seguridad que indican el protocolo y método de autenticación utilizado. Con el comando **aaa authentication** se habilitan los procesos de autenticación AAA.

1.3.3.5.3 Configuración de RADIUS

Para configurar RADIUS, se establece la comunicación entre el *router* y el servidor RADIUS. Se usan los comandos de configuración global AAA para definir listas de métodos de autenticación y autorización para crear la cuenta.

Los comandos **line** e **interface** se usan para configurar el *router* para comunicaciones hacia el servidor RADIUS. Se usa el comando **radius-server** para configurar el *router* para comunicaciones desde el servidor RADIUS.

1.3.4 *ADVANCED INSPECTION AND PREVENTION SECURITY SERVICES MODULE* (AIP-SSM)

1.3.4.1 Generalidades

El AIP-SSM es un módulo que se inserta en equipos de la serie ASA 5500, con el fin de desempeñar funciones de *Intrusion Prevention System* (IPS).

Se distinguen tres modelos de este módulo: AIP-SSM-10, AIP-SSM-20 y AIP-SSM-40. Los modelos de AIP-SSM se distinguen por el *throughput* que pueden soportar, al ser incorporados en los diferentes modelos de la serie ASA 5500; en la Tabla 1.1 se indican los valores correspondientes para cada caso.

ASA	AIP-SSM-10	AIP-SSM-20	AIP-SSM-40
	THROUGHPUT (Mbps)		
5510	150		
5520	225	375	450
5540		5540	650

Tabla 1.1: Modelos disponibles del módulo AIP-SSM

Los requisitos para el funcionamiento de un AIP-SSM son:

- Disponer de un ASA 5500, en el cual se incorpora el módulo.
- Disponer del software Cisco *Adaptive Security Appliance* 7.0 o superior.
- Encriptación DES o 3DES habilitada.

El ASA dispone de un *slot* para insertar el módulo AIP-SSM. Previo a su instalación, se debe apagar el ASA y retirar de su chasis los tornillos que resguardan el *slot*. Como se indica en la Figura 1.9, se debe introducir adecuadamente el módulo y cerrar nuevamente el sector.

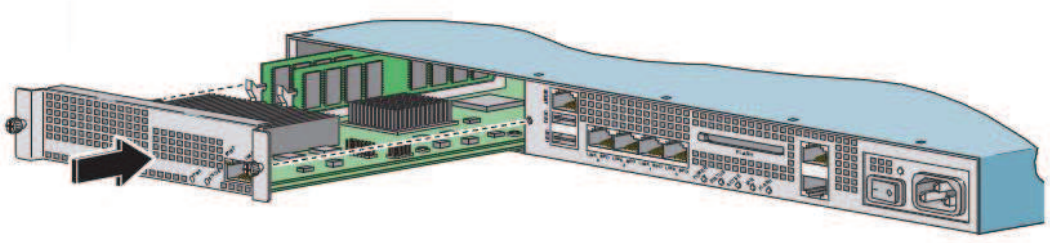


Figura 1.9: Incorporación del módulo AIP-SSM en el ASA [7]

Con el comando **asauio # show module 1** se visualiza si el módulo ha sido reconocido por el ASA y si se ha instalado apropiadamente.

1.3.4.2 IPS vs. IDS

El módulo AIP-SSM "corre" un software avanzado que provee inspección de seguridad en modo conectado o en modo promiscuo, según sean las necesidades de seguridad de la red.

Al configurar al módulo como un sensor en modo conectado o *Intrusion Prevention System* (IPS), la revisión del flujo de tráfico se realiza sobre los paquetes originales, por lo que se introduce latencia; sin embargo, este modo resulta conveniente si se desea impedir el ingreso de posibles amenazas a la red, pues es posible tomar acciones inmediatas. Con el modo promiscuo o *Intrusion Detection System* (IDS), la revisión se realiza sobre copias de los paquetes originales, por lo que no se incorpora una latencia adicional; sin embargo, dado que la revisión es efectuada sobre las copias de los paquetes, es posible que no se pueda detener inmediatamente a una posible amenaza.

1.3.4.3 Configuración

Para asignar un nombre determinado al módulo, los comandos a ingresar son:

sensor # configure Terminal
sensor (config) # service host
sensor (config-hos) # network-settings

sensor (config-hos-net) # host-name detector

Para asignar una dirección IP, máscara de subred y el default gateway del módulo, se ingresa:

sensor (config-hos-net) # host-ip x.x.x.x / y, z.z.z.z

Se especifica los hosts o redes que tendrán acceso al sensor, mediante listas de acceso; para ello se utiliza el comando:

sensor (config-hos-net) # access-list k.k.k.k/j

En el comando indicado, se establecen las direcciones de las redes con la máscara de subred correspondiente.

Con los siguientes comandos, se observan las estadísticas correspondientes de eventos ocurridos en el módulo: show statistics virtual-sensor, show statisticsanalysis-engine, show statistics authentication, show statistics denied-attackers, show statistics event-server, show statistics event-store, show statistics event host, show statistics logger, show statistics network-access, show statistics notification, show events.

Para conservar una copia de respaldo de la configuración, se utilizan los comandos:

sensor # copy current-config backup-config
sensor # more backup-config
sensor # copy backup-config current-config

Es necesario configurar la comunicación entre el ASA y el AIP-SSM, para ello se configura el ASA para que envíe tráfico al módulo, de la siguiente manera:

asauio(config) # access-list IPS permit ip any any

```
asauio(config) # class-map comunicacion
asauio(config-cmap) # match access-list IPS
asauio(config-cmap) # policy-map politica
asauio(config-pmap) # class comunicacion
asauio(config-pmap-c) # ips promiscuous fail-open
asauio(config-pmap-c) # service-policy politica global
```

Con los comandos indicados anteriormente, se configura la comunicación de tal forma que el sensor se comporte como IPS y que además en caso de falla no se detenga el flujo de paquetes. Otra alternativa es la configuración como IDS y también se podría variar el comportamiento en caso de falla, mediante el comando fail-close se conseguiría detener el flujo de paquetes si se produce una falla.

Es conveniente cuantificar el impacto de los riesgos; para ello se configura el módulo, de modo que se pueda dar un nivel de impacto (zerovalue, low, medium, high o misión-critical) a los riesgos asociados a determinada IP. Para ello se ingresa:

```
sensor (config) # service event-action-rules rules0
sensor (config-rul) # target-value target-value-setting high target address
b.b.b.b
```

Con los comandos indicados, se establece una regla que realiza el módulo, tal que se defina a cualquier evento de seguridad proveniente de la dirección ip b.b.b.b como de riesgo alto. Se debe definir como “critical-mission” a los eventos de seguridad ocurridos en las direcciones ip de los servidores y del *router* de borde.

Para negar el ingreso de paquetes de direcciones IP de un atacante:

```
sensor (config) # service event-action-rules rules0
sensor (config-rul) # overrides deny-attacker-primiscuous
```

Para no transmitir un paquete que genera alerta:

sensor (config-rul) # overrides deny-packet-primiscuous

Para no transmitir paquetes en la conexión TCP especificada:

sensor (config-rul) # overrides deny-connection-primiscuous

Para enviar paquetes TCP RST para terminar la conexión:

sensor (config-rul) # overrides reset-tcp-connection

Para solicitar un bloqueo de la conexión:

sensor (config-rul) # overrides request-block-connection

Para señalar los paquetes procedentes de la dirección IP del atacante:

sensor (config-rul) # overrides log-attacker-packets

Para señalar los paquetes de la dirección IP de la víctima:

sensor (config-rul) # overrides reset-victim-connection

Para escribir alertas en el Archivo de Eventos:

sensor (config-rul) # overrides produce-alert

Luego de ingresar cada uno de los comandos indicados anteriormente, se debe definir el rango de nivel de riesgo (RR) para cada caso; este valor se encuentra entre 0 y 100. El rango seleccionado dependerá del impacto del evento; el comando es:

sensor (config-rul-ove) # risk-rating-range 0-100

Para completar la ejecución adecuada de los comandos anteriores, se debe filtrar la información, de modo que el módulo disponga de los datos suficientes para detectar si se trata de un ataque e identificar a atacantes y víctimas. Para esto, se crea un filtro, estableciendo un nombre para el mismo y determinando dónde se desea insertar el filtro:

```
sensor (config-rul) # filters insert evento1 begin
sensor (config-rul-fil) # signature-id-range 1000-1005
sensor (config-rul-fil) # subsignature-id-range 1-5
sensor (config-rul-fil) # attacker-address-range c.c.c.c-d.d.d.d
sensor (config-rul-fil) # victim-address-range f.f.f.f-g.g.g.g
sensor (config-rul-fil) # victim-port-range h-j
sensor (config-rul-fil) # risk-rating-range k-l
sensor (config-rul-fil) # actions-to-remove-reset-tcp-connection
sensor (config-rul-fil) # deny-attacker-percentage m
sensor (config-rul-fil) # stop-on-match false
```

Es posible observar las estadísticas de los atacantes denegados, mediante el comando

```
sensor # show statistics denied-attackers
```

Con este comando se puede conocer las direcciones IP específicas, de donde provienen los ataques y el número de intentos asociados a cada dirección.

1.3.5 CONFIABILIDAD E IDENTIDAD EN CAPA 3

1.3.5.1 *Proxy* de Autenticación *Cisco IOS Firewall*

Permite aplicar políticas de seguridad específicas por usuario. Los usuarios pueden ser identificados y autorizados en base de sus propias políticas, y los privilegios de acceso pueden ser medidos en una base individual.

Con la aplicación del *proxy* de autenticación, los usuarios pueden ingresar a la red o al Internet vía HTTP, HTTPS, FTP o Telnet y sus perfiles de acceso serán supervisados por *Cisco Secure ACS* u otro servidor de autenticación.

Cuando un usuario inicia una sesión HTTP, HTTPS, FTP o Telnet a través del *firewall*, éste dispara el *proxy* de autenticación. El *proxy* revisa si el usuario ha sido autenticado.

Si una entrada de autenticación válida existe para el usuario, la sesión es permitida. Si no existe una entrada, el *proxy* responde a la solicitud de conexión del usuario con una petición de nombre de usuario y contraseña. Si la autenticación es exitosa, el perfil de autorización es otorgado desde el servidor AAA. Si la autenticación falla, el *proxy* reporta la falla al usuario.

El *proxy* de autenticación establece un tiempo máximo para cada perfil. Mientras existe actividad a través del *firewall*, el tráfico iniciado desde el host no "dispara" el *proxy* de autenticación y todo el tráfico autorizado es permitido. Si el tiempo configurado como máximo expira, el *proxy* remueve la información del perfil de usuario. Cuando esto ocurre, el tráfico desde el host es bloqueado y el usuario se ve obligado a iniciar otra conexión para "disparar" el *proxy*.

1.3.5.1.1 Configuración del Servidor AAA

El comando **aaa new-model** habilita el sistema de control de acceso AAA. Por defecto, el sistema no está habilitado.

Con los comandos **aaa authentication login** y **aaa authorization auth-proxy** se establecen parámetros de autenticación AAA. El primer comando define la lista de métodos de autenticación que pueden ser usados como TACACS+, RADIUS o ambos. Con el segundo se habilita al *proxy* de autorización para métodos AAA, como TACACS+, RADIUS o ambos.

Para especificar direcciones IP de servidores TACACS+ y RADIUS, se usan los comandos **tacacs-server host** y **radius-server host**, respectivamente. Los comandos **tacacs-server key** y **radius-server key** son útiles para definir la llave de encriptación para autenticación entre el *router* y el servidor AAA.

1.3.5.1.2 Tráfico AAA hacia el Router

Todo el tráfico que requiere autenticación y autorización debe ser revisado por el *router* usando ACLs extendidas. Tras una autenticación exitosa, las *Access Control Entries* (ACEs) dinámicas se insertan en las ACLs para permitir solo el tráfico autorizado por el perfil del usuario. El *proxy* de autenticación encubre cada ACE del perfil del usuario reemplazando la dirección IP origen en la ACL con la dirección IP origen del *host* autenticado.

Para permitir la comunicación del servidor AAA, se debe realizar una ACL extendida, creando una ACE donde la dirección origen es el servidor AAA y la dirección destino es la interfaz donde reside el servidor AAA. Luego se debería permitir cierto tráfico sin requerir autenticación como TACACS+, RADIUS e *Internet Control Message Protocol* (ICMP). Todo el tráfico restante se debería restringir. Las ACLs extendidas deben ser aplicadas a la interfaz en donde reside el servidor.

En caso de que el *proxy* se configure en la misma interfaz en donde reside el servidor AAA, la ACL se debe aplicar a la interfaz en donde el *proxy* está configurado.

Se utiliza el comando **ip http server** para usar el *proxy* de autenticación con HTTP. Con el comando **ip http authentication aaa** se solicita al servidor HTTP usar autenticación AAA.

1.3.5.1.3 Configuración de Proxy de Autenticación

El comando **inactivity-timer** especifica el tiempo máximo de inactividad y **absolute-timer** define el tiempo absoluto.

El *timer* de inactividad inicia después de que una conexión se libera. Si un usuario establece una conexión nueva antes de que se termine este *timer*, no se le solicita

reautenticarse. En caso de que el usuario establezca una nueva conexión después de que el *timer* de inactividad expire, el usuario se debe reautenticar.

El *timer* absoluto indica al usuario cuando inicia una nueva conexión. Permite configurar una ventana durante la cual el *proxy* de autenticación está activo en la interfaz habilitada.

Ambos *timers* pueden operar a la vez. Sin embargo, es recomendable que la duración del *timer* absoluto sea mayor que la del *timer* de inactividad; caso contrario, el *timer* de inactividad nunca sería invocado y se corre el riesgo de que si el usuario se ausentó de su máquina, otra persona haga uso de los servicios y acceda a la información. Por seguridad, conviene configurar los dos *timers*.

Para crear una regla del *proxy* de autenticación se usa el comando **ip auth-proxy name**. Una regla del *proxy* de autenticación puede ser asociada con una ACL, proveyendo control a los *hosts* que utilizan el *proxy* con la opción **list acl**.

1.3.5.2 Introducción a Componentes AAA de *PIX Security Appliance*

1.3.5.2.1 Autenticación de PIX Security Appliance

Existen tres tipos de autenticación disponibles en *PIX Security Appliance*.

- Autenticación de acceso
- Autenticación de *proxy cut-through*
- Autenticación de acceso túnel

El primer tipo de autenticación, permite solicitar verificación de autenticación al acceder al PIX. Está disponible para sesiones SSH, HTTP y Telnet.

Para la autenticación de *proxy cut-through*, el PIX puede ser configurado para solicitar autenticación para una sesión, como especifica el comando **aaa**

authentication. Solo las sesiones FTP, HTTPS y HTTP pueden ser interceptadas para autenticar usuarios.

Para la autenticación de acceso túnel, el PIX puede ser configurado para solicitar a un usuario de túnel remoto que se autentique. Si un usuario desea establecer un túnel IPSec, antes de que el túnel se establezca, el PIX solicitará al usuario un nombre de usuario y contraseña. Las credenciales se verifican antes de que el túnel de usuario esté completamente establecido.

1.3.5.2.2 Autorización de PIX Security Appliance

La autorización facilita y controla quién accede a las aplicaciones de seguridad y qué comandos puede ejecutar. El administrador crea cuentas de usuario y concede un nivel de privilegio a cada uno. Si se permite a todos los usuarios ejecutar HTTP, HTTPS, FTP y Telnet, la autenticación es suficiente y no es necesaria la autorización.

1.3.5.2.3 Soporte de Servidor AAA

PIX Security Appliance soporta autenticación y autorización usando su propio servidor local, una base de datos interna o un servidor AAA externo. El servicio de cuentas está ubicado en un servidor de cuentas externo.

El protocolo para comunicaciones entre el PIX y un servidor AAA externo varía por los componentes del AAA. En la Figura 1.10, se presentan los componentes de AAA, funciones y protocolos soportados. Para cada componente se tienen tres funciones.

Protocol	Authentication			Authorization			Accounting		
	Tunnel access	Console access	Cut-through Proxy	Tunnel access	Console access	Cut-through Proxy	Tunnel access	Console access	Cut-through Proxy
Local	×	×	×	×	×*				
RADIUS	×	×	×	×		×	×	×	×
TACACS+	×	×	×		×	×	×	×	×
SDI	×								
NT	×								
Kerberos	×								
LDAP				×					

Figura 1.10: Componentes, funciones y protocolos en AAA [8]

1.3.5.3 Configuración de AAA en *PIX Security Appliance*

1.3.5.3.1 Autenticación de Acceso de PIX Security Appliance

El comando **aaa authentication serial console** permite verificar la autenticación para acceder a la consola del PIX. La opciones **serial**, **telnet** y **ssh** solicitan un nombre de usuario y contraseña antes de la primera línea de comando.

1.3.5.3.2 Autenticación Interactiva de Usuario

Para configurar la autenticación interactiva de usuario, se especifica un grupo de servidor AAA con el comando **radius-server key**. Luego se designa un servidor de autenticación con **aaa-server**. Finalmente se habilita la autenticación de acceso a aplicaciones de seguridad con el comando **aaa authentication**.

Se pueden configurar hasta 15 grupos de hasta 16 servidores AAA cada uno. Cuando un usuario ingresa, los servidores son accesados uno a la vez, hasta que un servidor responda.

1.3.5.3.3 Base de Datos Local de Usuario

El comando **username** crea cuentas de usuario en la base de datos local del usuario. Con **privilege** se asigna un nivel de privilegio al usuario. Para borrar una

cuenta de usuario se usa el comando **no username**. Si se desea remover todas las entradas de la base de datos se ingresa el comando **clear config username**.

Para limitar el número de intentos se usa **aaa local authentication attempts max-fail**. Luego del número máximo de intentos, el acceso es bloqueado. Con el comando **show aaa local user** se observa los intentos fallidos de un usuario.

1.3.5.3.4 Prompts de Autenticación y Timeouts

El comando **auth-prompt** permite cambiar el texto de requerimiento AAA por acceso HTTP, FTP o Telnet a través del PIX. Éste es el texto que aparece abajo del nombre de usuario y contraseña cuando un usuario ingresa.

Con el comando **timeout uauth** se especifica la cantidad de memoria caché[21] que debería ser retenida después de que las conexiones del usuario se liberen.

1.3.5.3.5 Autenticación Forzada (Cut_Through) de Proxy

Es un método de verificación transparente de identidad de usuarios en el *firewall*. Permite o restringe el acceso a cualquier aplicación basada en TCP o UDP. El *proxy* forzado o *cut-through*, evalúa a un usuario inicialmente en la capa de aplicación y luego lo autentica con estándares TACACS+, RADIUS o bases de datos locales. Luego de que la política es revisada, el PIX desplaza el flujo de sesión y todo el tráfico fluye directamente entre el servidor y el cliente.

1.3.5.3.6 Configuración de Autorización

La autorización es esencial cuando se desea permitir a ciertos usuarios el uso de determinadas operaciones. Existen dos tipos de autorización: autorización de usuario clásica y descarga de cada usuario.

---

[21] Memoria en la que se almacenan datos para su rápido acceso. Es un tipo de memoria volátil, pero de gran velocidad.

En la autorización de usuario clásica, las reglas de acceso son configuradas en el servidor AAA TACACS+ y consultadas bajo demanda. El PIX es configurado con las reglas que especifican qué conexiones se necesitan para ser autorizado por el servidor AAA.

En la autorización por descarga, PIX *Security Appliance Software Version* 6.2, permite almacenar ACLSs completas en un servidor AAA y descargarlas al PIX. Una ACL es añadida al usuario o perfil de grupo en el servidor AAA. Después de que las credenciales son autenticadas, el servidor AAA retorna la ACL al PIX. La ACL retornada se modifica en base a la dirección IP origen del usuario autenticado.

El proceso de autorización consiste en configurar el PIX con el comando **aaa authorization {include | exclude}** o **aaa authorization match**. Posteriormente, se definen los parámetros de grupo del servidor AAA TACACS+ con ayuda del comando **per-group**.

1.3.5.3.7 Configuración de Cuentas

Para habilitar, deshabilitar o ver las cuentas de usuario en un servidor TACACS+ o RADIUS, se usa el comando **aaa accounting**. Los servicios de cuenta de usuario contienen los servicios de red a los que cada usuario tiene acceso. Esta información se conserva en el servidor AAA designado.

Para permitir la generación de un registro de cuenta, se identifica un flujo de tráfico con una ACL y se la aplica al comando **aaa accounting match**. Con el comando **aaa accounting console** se permite la generación de registros de cuenta para marcar el establecimiento y terminación del acceso a la consola del PIX. Cuando el comando **aaa accounting command** es configurado, cada comando ingresado por un usuario es almacenado y enviado al servidor de cuentas.

1.3.6 CONFIABILIDAD E IDENTIDAD EN CAPA 2

1.3.6.1 Relación de IBNS con 802.1x y EAP

Una alternativa para implementar confiabilidad e identidad en capa 2 es aplicar IBNS. Este servicio se explicó anteriormente; sin embargo se lo tratará más a detalle en esta sección.

1.3.6.1.1 Cómo Trabaja 802.1x

El *switch* o el cliente pueden iniciar la autenticación. Si la autenticación es habilitada en un puerto, con el comando de configuración de interfaz **dot1x port-control auto**, el *switch* inicia la autenticación cuando el estado del enlace del puerto cambie de *down* a *up*. Luego, envía al cliente una trama[22] EAP de solicitud de identidad. El cliente responde con una trama EAP de respuesta. Si el cliente no recibe la trama EAP de solicitud, puede iniciar la autenticación con una trama *EAP over LAN* (EAPOL) de inicio. Cuando el cliente indica su identidad, el *switch* pasa tramas EAP hasta que la autenticación sea exitosa o fallida.

El estado del puerto del *switch* determina si se concede o no acceso a la red. El puerto inicia en estado de no autorizado. Durante este estado, el puerto deshabilita todo flujo de tráfico, excepto los paquetes 802.1x. Cuando un cliente es autenticado, el puerto cambia a estado autorizado, permitiendo todo tráfico. Cuando un cliente se desconecta, envía un mensaje EAPOL de salida, provocando que el puerto del *switch* cambie nuevamente al estado de no autorizado.

1.3.6.1.2 IBNS y Cisco Secure ACS

La adición del soporte RADIUS a los *switches* Cisco Catalyst para controlar el acceso remoto de usuarios, significa que los esquemas de control de acceso basados en usuario, están ahora disponibles en los *links* de los *switches*.

[22] Unidad de información de la capa Enlace del model OSI.

EAP es la estructura tecnológica que hace posible desarrollar RADIUS en ambientes de red Ethernet. Se le atribuye además la adopción de esquemas AAA y ventajas de seguridad disponibles cuando se usan los servidores AAA. El estándar 802.1x, conocido como EAPOL provee un canal de comunicaciones entre un usuario final hasta el servidor AAA a través del *switch*. Con la adición de soporte AAA para el control de acceso, todas las conexiones LAN Ethernet pueden ser autenticadas con solicitudes individuales a cada usuario.

EAP facilita las demandas de autenticación basadas en usuario, tanto para esquemas de autenticación de contraseña *hashed* de una vía como PAP o esquemas más avanzados como certificados digitales.

Las políticas de acceso a la red definen cómo los usuarios pueden conectarse a la red y qué servicios pueden obtener cuando se conectan. *Cisco Secure ACS* provee control utilizando autenticación centralizada y autorización de usuarios.

1.3.6.1.3 Consideraciones de Despliegue ACS

a. Ambiente LAN Pequeño

Un único *Cisco Secure ACS* usualmente es colocado cerca al *switch*. La base de datos del usuario generalmente es pequeña porque pocos *switches* podrían requerir acceso al *Cisco Secure ACS*. Un segundo servidor podría ser implementado por cuestiones de redundancia.

b. Ambiente de red Grande

En una red grande que está dispersa geográficamente, la velocidad, redundancia y fiabilidad son importantes para determinar si utilizar un servidor *Cisco Secure ACS* centralizado o varios servidores dispersos. Los retardos en la autenticación introducidos por la red podrían ser considerables. Se recomienda tener mínimo un

Cisco Secure ACS implementado en cada región geográfica; de esta manera actuaría como *backup*[23] para los servidores de las demás regiones.

1.3.6.1.4 Configuración de perfil RADIUS de Cisco Secure ACS

Después de que un usuario completa satisfactoriamente el proceso de autenticación EAP, el ACS responde al *switch* con un paquete RADIUS de aceptación de la autenticación. Una vez recibidos por el *switch*, los atributos son procesados junto con el RADIUS RFC. El perfil de acceso contiene generalmente información de la autorización de un usuario específico, como ACLs a ser aplicadas o la VLAN ID a ser asignada.

1.3.6.2 Configurando Autenticación 802.1x Basada en Puerto

1.3.6.2.1 Habilitación de Autenticación 802.1x

Para habilitar autenticación 802.1x basada en puerto, debe estar habilitado AAA y se debe especificar una lista de métodos de autenticación.

Una lista de métodos describe los métodos de secuencia y autenticación para permitir el acceso a un usuario. El software utiliza el primer método enlistado para autenticar. Si el método falla, el software selecciona el siguiente método. El proceso continúa hasta que existe una comunicación satisfactoria o hasta que se agoten todos los métodos. Si la autenticación falla en cualquier punto del proceso, éste se detiene.

Iniciando en modo EXEC privilegiado, se usan los pasos indicados en la Figura 1.11 para configurar autenticación 802.1x basada en puertos.

[23] Respaldo o agente secundario que actúa en caso de que el primario falle.

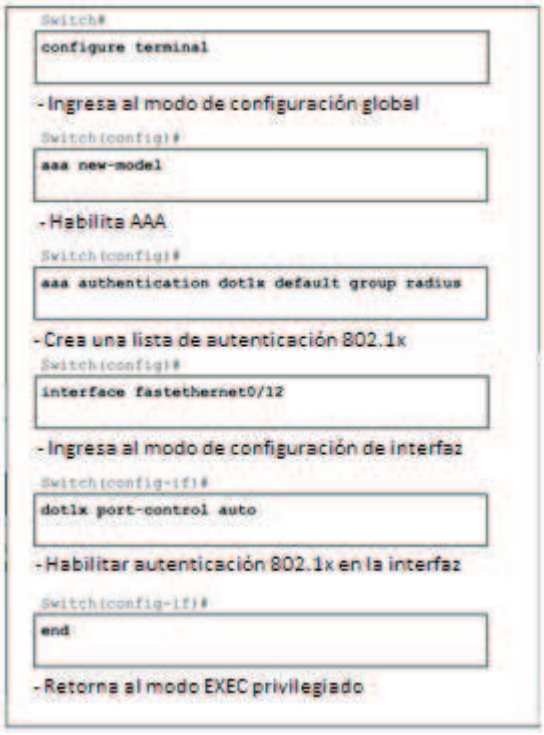


Figura 1.11: Configuración de autenticación 802.1x [9]

1.3.6.2.2 Configuración de la Comunicación entre el Switch y el Servidor RADIUS

Los servidores RADIUS son identificados por:

- Nombre de *host* o dirección IP.
- Nombre de *host* y números de puertos UDP.
- Dirección IP y números de puertos UDP (crea un identificador único que habilita solicitudes RADIUS a ser enviadas a múltiples puertos UDP en un servidor en la misma dirección IP).

Para configurar los parámetros del servidor RADIUS en el *switch*, se utiliza el comando **radius-server host {*hostname* | *ip-address*} auth-port *port-number* key *string***.

1.3.6.2.3 Habilitación de Re-Autenticación Periódica

Es posible configurar re-autenticación periódica y la frecuencia con la que puede ocurrir. En la Figura 1.12, se observan los comandos que permiten realizar estas configuraciones.

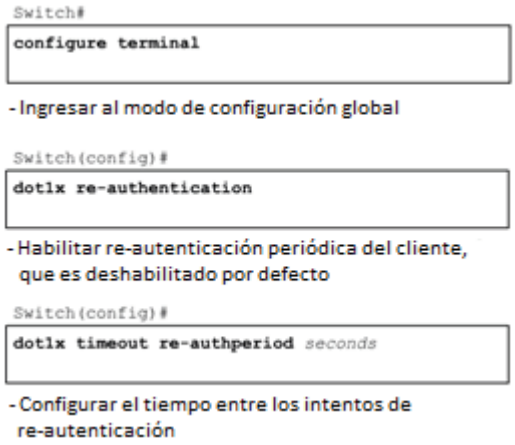


Figura 1.12: Configuración de re-autenticación [9]

La re-autenticación 802.1x automática no se puede utilizar para clientes conectados a puertos individuales.

1.3.7 FILTRADO EN UN *ROUTER*

La utilización del componente *Context-based Access Control* (CBAC) del paquete *Cisco IOS Firewall* en un *router*, permite dar un gran nivel de seguridad a las redes y gracias a sus características ser muy efectivo al ser usado como filtro.

Una ACL permite determinar en un *router* o *switch* cómo un paquete será manipulado (permitido o descartado), de acuerdo a las especificaciones dadas en ella. El CBAC es un tipo de ACL que provee un gran nivel de seguridad, mediante la inspección de tráfico de la capa 3, siempre y cuando el paquete haya sido previamente permitido de acuerdo a las especificaciones de la ACL de la interfaz.

1.3.7.1 *Cisco IOS Firewall Context-Based Access Control* (CBAC)

CBAC es un filtro inteligente que analiza el tráfico de sesiones que se han originado en cualquier interfaz del *router*. El análisis del tráfico que cursa a través del *firewall* permite almacenar información de las sesiones TCP y UDP. Esta información se usa para crear ACLs dinámicamente, con el fin de permitir el tráfico de retorno de sesiones permisibles.

CBAC, por ejemplo, analiza si el número de secuencia de una sesión TCP está dentro del rango esperado; si éste corresponde a un paquete sospechoso, CBAC lo descarta. Adicionalmente CBAC puede detectar un alto número de conexiones nuevas inusuales y emitir mensajes de alerta. CBAC mediante este análisis de información permite prevenir ciertos tipos de ataques, en especial los ataques DoS.

1.3.7.1.1 Funcionamiento de CBAC

Una vez que un paquete ha sido permitido por una ACL aplicada a una interfaz, comienza el análisis de CBAC.

CBAC especifica cuáles son los protocolos que deberán ser analizados, la interfaz, dirección de la interfaz (entrante o saliente) y en dónde se origina el análisis. El funcionamiento de CBAC se lo puede visualizar en la Figura 1.13.

Para CBAC, los datos o *payload* de cada paquete es transparente, pues el análisis solo se lo realizará en el canal de control.

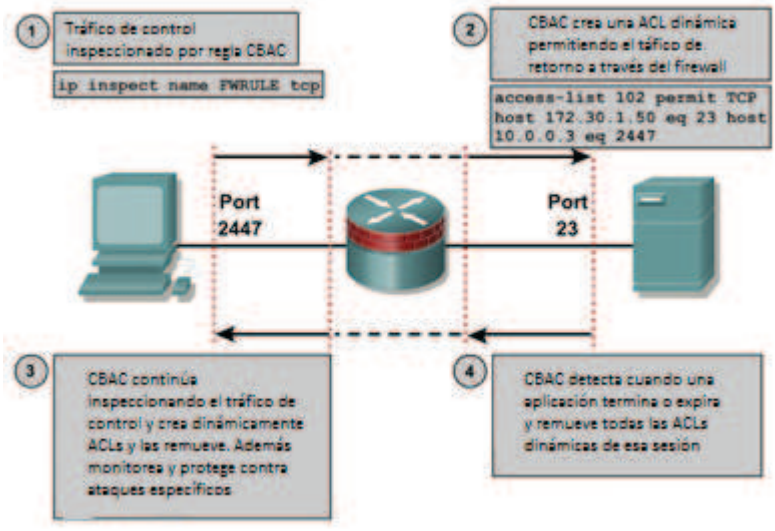


Figura 1.13: Funcionamiento de CBAC [10]

Una vez que se ha realizado el análisis, si se sospecha de un ataque con características de DoS, CBAC puede tomar las siguientes acciones:

- Genera mensajes de alerta.
- Protege los recursos del sistema que pudieran dificultar el rendimiento.
- Bloquea paquetes sospechosos.

Para el análisis y manejo de la información de estado de las sesiones, CBAC utiliza *timeout* y valores umbrales. El establecimiento de valores de *timeout* ayuda a prevenir ataques DoS, liberando recursos del sistema. CBAC logra esto descartando sesiones después de un tiempo específico. El establecimiento de valores umbrales ayuda a prevenir ataques DoS mediante el control del número de sesiones medio abiertas[24].

CBAC provee tres valores umbrales en contra de ataques DoS:

- El número total de sesiones TCP o UDP medio abiertas.
- El número de sesiones medio abiertas basadas en tiempo.
- El número de sesiones TCP medio abiertas por *host.*

Si el umbral es excedido, CBAC toma dos acciones:

- Envía un mensaje de *reset* a los puntos remotos de la sesión medio abierta más antigua, poniendo a disposición los recursos para la más nueva.

- Solo en caso de sesiones TCP medio abiertas, CBAC bloquea todos los paquetes SYN[25] temporalmente por un tiempo configurado en el valor umbral. Cuando el *router* bloquea un paquete SYN, la negociación TCP de tres vías (Figura 1.14) nunca se inicia. Esto evita que el *router* use memoria o procesamiento necesario para validar conexiones.

[24] Para sesiones TCP, una sesión medio abierta significa que la negociación de tres vías no se ha completado, es decir no se ha establecido la sesión. Para una sesión UDP, una sesión medio abierta significa que el *firewall* no ha detectado retorno de tráfico.
[25] Es el primer paquete que se envía para iniciar una sesión TCP.

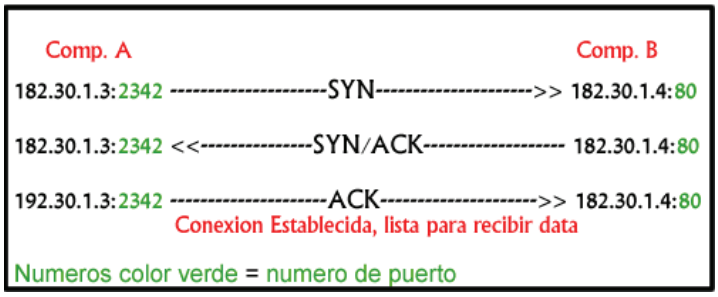


Figura 1.14: Negociación TCP de tres Vías [11]

Se deberá especificar los protocolos que se desean monitorear en contra de ataques DoS, mediante reglas de inspección aplicadas a una interfaz.

Cada vez que un paquete se analiza, la tabla de estado se actualiza para incluir información acerca del estado de la conexión del paquete. El retorno del tráfico solo será permitido a través del *firewall*, si la tabla de estados contiene información indicando que el paquete pertenece a una sesión permitida.

En las sesiones UDP el análisis es aproximado. Con UDP no hay sesiones actuales. El software aproxima una sesión, examinando la información del paquete y determina si éste es similar al paquete UDP anterior, en base a la similitud de la dirección fuente o destino y número de puerto. El software además revisa si el paquete está dentro del período configurado de *timeout* inactivo UDP.

Como se mencionó anteriormente, CBAC crea o borra dinámicamente ACLs en las interfaces del *firewall*, de acuerdo a la información mantenida en la tabla de estados; sin embargo estas ACLs nunca son almacenadas en la memoria NVRAM.

1.3.7.2 Configuración de *Cisco IOS Firewall* CBAC

Las siguientes tareas deberán ser realizadas para configurar CBAC:

- Seleccionar una interfaz interna o externa.
- Configurar ACLs a una interfaz.
- Establecer alertas.

- Establecer *timeouts* y valores umbrales.
- Definir *Port-to-Application Mapping* (PAM).
- Definir reglas de inspección.
- Aplicar reglas de inspección y ACLs a las interfaces.
- Probar y verificar.

Para que CBAC pueda funcionar correctamente, las ACLs deben ser configuradas apropiadamente en la interfaz.

Se asumirá que dentro de la red que se desea proteger no existen usuarios maliciosos, por lo que todo el tráfico que fluye desde la red protegida a través de la interfaz es permitido.

Es recomendable establecer las siguientes ACLs:

- Negar cualquier tráfico de una dirección fuente que pertenece a las direcciones de la red protegida, con el fin de evitar los ataques *spoofing*[26].

- Negar mensajes de *broadcast*[27] provenientes de una dirección fuente 255.255.255.255, con el fin de evitar ataques de *broadcast*.

Adicionalmente si CBAC es configurado en una interfaz externa, la ACL *oubound* puede ser estándar o extendida, mientras que la ACL *inbound* deberá ser extendida. Por el contrario si CBAC es configurado en una interfaz interna, la ACL *inbound* puede ser estándar o extendida, mientras que la ACL *oubound* deberá ser extendida.

1.3.7.2.1 Comandos de configuración

Para todos los comandos que se presenten a continuación, se utilizará el término **no** para establecer los parámetros por defecto en el *router*.

[26] Asumir la identidad de un dispositivo de la red protegida
[27] Transmisión de un paquete que será recibido por todos los dispositivos en una red.

a. Alertas

CBAC proporciona alertas en tiempo real y seguimiento basado en los eventos generados en el *firewall*, obteniendo información específica cuando se detecta una actividad sospechosa.

El comando **ip inspect alert-off** deshabilita los mensajes de alerta y el comando **ip inspect audit** permite habilitar mensajes de seguimiento.

b. Timeouts

Los *timeouts* determinarán cuánto tiempo se maneja la información de estado de una sesión y cuándo se descarta una sesión que no ha sido completamente establecida.

Para definir el tiempo de espera, para que una sesión TCP se establezca completamente antes de descartarla, se usa el comando **ip inspect tcp synwait-time** (tiempo por defecto 30 segundos).

Con el fin de definir cuánto tiempo será aún monitoreada una sesión TCP, después de detectar el fin de la sesión, se usa el comando **ip inspect tcp finwait-time** (tiempo por defecto 5 segundos).

Para determinar el tiempo que una sesión TCP o UDP será monitoreada después de no detectar actividad, se emplea el comando **ip inspect {tcp|udp} idle-time** (tiempo por defecto TCP: 3600 segundos UDP: 30 segundos).

c. Valores Umbrales

Para configurar los valores umbrales, que permitirán mitigar posibles ataques de DoS, mediante el establecimiento del número y velocidad de sesiones medio abiertas por minuto, se utilizarán los siguientes comandos:

- **ip inspect max-incomplete high *number:*** Define el número máximo de sesiones medio abiertas que inducen que el software comience a eliminarlas en un modo agresivo *(500 sesiones* por defecto).

- **ip inspect max-incomplete low *number:*** Define el número existente de sesiones medio abiertas que inducen que el software detenga la eliminación, se utiliza el comando (400 sesiones medio abiertas).

- **ip inspect one-minute high *number:*** Define el número máximo de intentos de establecimiento de sesión en un minuto, que inducen que el software comience a eliminar las sesiones medio abiertas (500 sesiones por defecto).

- **ip inspect one-minute low *number:*** Define mínimo de intentos de establecimiento de sesión en un minuto, que inducen que el software detenga la eliminación de sesiones medio abiertas (400 sesiones por defecto).

Cuando se tiene un alto número de peticiones con la misma dirección de *host* de destino, para el establecimiento de una sesión, es posible que se trate de un ataque de DoS. Para prevenir este tipo de ataques se utiliza:

- **ip inspect tcp max-incomplete host *number* block-time *minutes:*** Define el número de sesiones medio abiertas con el mismo *host* de destino, que son permitidas antes de que el software comience a eliminarlas y el tiempo en el que seguirán siendo eliminadas las nuevas peticiones de conexión al *host*. (50 sesiones y 0 minutos de tiempo de espera por defecto)

d. Port-to-application mapping (PAM)

Cada aplicación está asociada a un puerto previamente definido o estándar[28]. Si se desea relacionar una aplicación específica a un puerto diferente a los estándares, se deberá actualizar la tabla PAM. Esto podrá aplicarse a un *host*

[28] Las aplicaciones utilizan puertos TCP y UDP previamente definidos y estandarizados. Entre los más utilizados están: HTTP puerto 80, SMTP puerto 25, FTP puerto 21, TELNET puerto 23.

específico o un segmento de red, utilizando los siguientes comandos en la configuración global:

- **ip port-map *appl_name* port *port_num:*** Asocia un número de puerto con una aplicación específica.

- **access-list permit *acl_num ip_add* ip port-map *appl_name* port *port_num* list *acl_num:*** Asocia un número de puerto con una aplicación para un *host* específico.

- **access-list permit *acl_num ip_add wildcard_mask* ip port-map *appl_name* port *port_num* list *acl_num:*** Asocia un número de puerto con una aplicación para un segmento de red dado.

e. Reglas de inspección

e.1 Aplicación

Las reglas de inspección deben ser definidas para especificar qué tráfico IP y qué protocolos de la capa aplicación serán analizados por CBAC en la interfaz. Para generar una regla de inspección se utilizará el comando i**p inspect name *inspection_name protocol* [alert on|off] [audit-trail on|off].**

Se puede configurar reglas de inspección más específicas para JAVA, RPS o SMTP, sin embargo no se las mencionará en este documento, ya que el proyecto no busca el análisis de las mismas.

e.2. Fragmentación IP

Para evitar ataques DoS que involucran el envío de paquetes IP fragmentados[29], se utilizará el comando **ip inspect name *inspection-name* fragment max *number* timeout *seconds.***

[29] La fragmentación IP denota la distribución de un paquete IP en varios bloques de datos, si su tamaño sobrepasa la unidad máxima de transferencia.

e.3. ICMP

Para habilitar solo los paquetes ICMP que permiten dar un *troubleshooting*[30] en el análisis de la red se utilizará el comando **ip inspect name *inspection-name* icmp [timeout *seconds*].**

Una vez que se han configurado las reglas de inspección, éstas deberán ser aplicadas a una interfaz. De acuerdo a las necesidades del usuario se aplicarán en interfaces internas y/o externas, ya sea en el tráfico saliente o entrante.

También se deberán aplicar las ACL a las interfaces, tomando en cuenta que únicamente los paquetes permitidos por las ACL serán analizados por CBAC.

1.3.8 FILTRADO EN UN *SWITCH*

Los dispositivos de capa dos, poseen características de seguridad que permiten defenderse contra ciertos tipos de ataques. Los ataques más comunes a nivel de capa enlace son: Desbordamiento de la tabla *Content-Addressable Memory* (CAM), VLAN *hopping*, manipulación del protocolo *Spanning-Tree*, *Media Access Control* (MAC) *Address spoofing* y DHCP *starvation*.

1.3.8.1 Mitigación del ataque de desbordamiento de la tabla CAM

El ataque de desbordamiento de la tabla CAM corresponde a un envío masivo de solicitudes de direcciones MAC inválidas al *switch*. En este caso la capacidad de la memoria ha alcanzado su límite, provocando que el *switch* actúe como un *hub*[31] enviando mensajes de *broadcast* a cada uno de los puertos correspondientes a una misma VLAN.

Para contrarrestar este ataque se puede configurar seguridad en el puerto del *switch*. Mediante esta opción se podrá especificar la dirección MAC asociada al

[30] Forma sistemática de buscar el origen de un problema para que éste pueda ser resuelto.
[31] Dispositivo de capa física, que permite centralizar el cableado de una red y poder ampliarla. Este dispositivo recibe una señal y la repite, emitiéndola por sus puertos.

puerto o el número máximo de direcciones MAC que pueden ser aprendidas por dicho puerto. Si una dirección MAC inválida es detectada, el *switch* podrá bloquear a dicha dirección MAC o a su vez apagar el puerto. Dentro de la configuración de la interfaz, se configurará de la siguiente manera:

Para habilitar la configuración para puerto seguro se usará el comando **switchport mode access**, pues por defecto no es posible.

Para especificar la o las direcciones MAC asociadas al puerto, se empleará **switchport port-security mac-address *mac_addr***; mientras que para definir el número máximo de direcciones MAC que pueden ser aprendidas por el puerto se utilizará el comando **switchport port-security maximum <1-132>.**

El comando **switchport port-security violation <protect | restrict | shutdown>** indicará qué acción tomará el puerto en caso de violación de la seguridad.

1.3.8.2 Mitigación del ataque MAC *spoofing*

El ataque de MAC *spoofing* utiliza una dirección MAC válida de un *host*, para transmitir información (tramas), de tal forma que el *switch* aprenda esta dirección MAC por otro puerto y lo sobrescriba en la tabla CAM. Con ello el atacante podrá recibir la información que está destinada para el host cuya dirección MAC es válida, pues ahora el *switch* enviará las tramas por el otro puerto.

El ataque ARP *spoofing* consiste en aprovechar el ARP gratuito[32] para falsificar la identidad de una dirección IP de un segmento de red. Todos los *hosts* de la red e incluso el *switch*, asociarán la dirección IP válida con la dirección MAC del atacante. Todos los paquetes que se envíen al host atacado, serán interceptados.

Para proporcionar una solución a estos ataques ARP se utiliza DHCP *snooping*, el cual consiste en filtrar mensajes DHCP confiables y usarlos para construir una

[32] Se produce cuando un *host* envía un mensaje de *broadcast* , con el fin de que los otros *hosts* almacenen su dirección MAC en la cache ARP

tabla DHCP *snooping.* DHCP *snooping* permite a la infraestructura de red conocer donde están (*switch*/puerto) los servidores corporativos y no permitir que se instalen otros servidores falsos. La tabla DHCP *snooping* contiene las direcciones MAC, IP, tiempo de inactividad, número de VLAN, y la información correspondiente a la interfaz local no confiable del *switch*. La interfaz no confiable corresponderá a aquella que reciba mensajes de fuera de la red o *firewall*. Para habilitar esta opción se utilizarán los comandos:

En la configuración global se aplica **ip dhcp snooping** para habilitar el DHCP *snooping.* Posteriormente, se aplica **ip dhcp snooping vlan *vlan_id*** para habilitar el DHCP *snooping* para una VLAN específica.

En la configuración de una interfaz se ingresa **ip dhcp snooping trust** para configurar a una interfaz como confiable, para propósitos de DHCP *snooping.* Luego se ingresa el comando **ip dhcp snooping limit rate *rate*** para establecer la velocidad límite de DHCP *snooping*, es decir el número de paquetes DHCP que la interfaz puede recibir.

1.3.8.3 Mitigación del ataque DHCP *starvation*

Los ataques DHCP funcionan enviando requerimientos DHCP de direcciones MAC falsas, con el fin de acabar con las direcciones IP disponibles del servidor DHCP. De esta manera el atacante puede actuar como un servidor, respondiendo peticiones DHCP, e inmiscuirse en la red.

Para contrarrestar este tipo de ataques, se podrá limitar el número de direcciones MAC permitidas por cada interfaz del *switch*, o a su vez, activando la opción del DHCP *snooping*, como se indicó anteriormente.

1.3.8.4 Mitigación del ataque VLAN *hooping*

De manera general este tipo de ataque consiste en alcanzar redes pertenecientes a una VLAN a la cual el atacante no pertenece. Para ello existen dos formas:

- Falsificación de *Switch*: consiste en que la red del atacante actúe como un *switch* con un puerto troncalizado[33], de tal forma que tenga acceso a todas las VLAN.

- Doble etiqueta: en este caso el atacante envía una trama con dos cabeceras, de tal forma que el primer *switch* lee la trama, la desencapsula, la envía al puerto correspondiente y también al puerto troncalizado. Esta trama llega al segundo *switch*, detecta el segundo encabezado y vuelve a desencapsular, generando que la trama se dirija a otra VLAN distinta a la que pertenece el atacante.

Para mitigar este tipo de ataques se deberán realizar varias modificaciones en la configuración de las VLAN, utilizando las siguientes recomendaciones:

- Utilizar VLAN ID dedicadas para todos los puertos troncalizados.
- Deshabilitar los puertos que no se utilizan e identificarlos como VLAN sin uso.
- No utilizar la VLAN nativa[34] por defecto (VLAN 1) para ninguna aplicación.
- Establecer a todos los puertos destinados para usuarios en el modo no troncalizado, deshabilitando el *Dynamic Trunk Protocol* (DTP).

1.3.8.5 Prevención de la manipulación del *Spanning-Tree protocol* (STP)

El protocolo STP es utilizado para lograr topologías libres de bucles en infraestructuras redundantes de capa 2, de tal forma que se evite las tormentas de *broadcast*. Para este tipo de topologías, los *switches* identifican a un *switch* como *root* y bloquean todos los otros caminos de datos redundantes.

La manipulación del protocolo STP consiste en el envío de paquetes *Bridge Protocol Data Units* (BPDU)[35] por parte del atacante. Estos paquetes obligan el recálculo del protocolo STP, y permiten que el atacante se convierta en el nuevo

[33] Puerto que transmite información de varias VLANs a través de un enlace punto a punto.
[34] También conocida como VLAN por defecto. Lleva la información de estado de los puertos. Es la VLAN a la que pertenecía un puerto en un *switch* antes de ser configurado como troncal. Se puede tener una VLAN nativa por puerto.
[35] Tramas que contienen información del protocolo STP. Los switches envían BPDUs usando una única dirección MAC de su puerto como MAC de origen y una dirección de *multicast* como MAC de destino.

root de la topología. De esta manera el atacante tendrá acceso a la información de las tramas que son enviadas y pasan por los otros *switches*.

Para contrarrestar este tipo de ataques se activará en la configuración global el comando **spanning-tree guard (loop | none | root)**, con el fin de establecer la interfaz que es permitida para ser *root*.

Adicionalmente se utilizará el comando **spanning-tree portfast,** con el fin de habilitar o deshabilitar el envío o recepción de mensajes BPDU.

1.3.9 FILTRADO EN UN PIX

La configuración de un PIX es muy similar a la que se realizaría en un *router*, por lo que en este capítulo se mencionarán los cambios o nuevos parámetros que se deberá tomar en cuenta para la configuración de un PIX.

1.3.9.1 Configuración de ACLs en un PIX

Por defecto, en un PIX, una interfaz interna tiene un mayor nivel de seguridad que una interfaz externa. Adicionalmente por defecto se tiene que todo el tráfico que fluye desde una interfaz interna a una externa está permitido. Por el contrario el tráfico proveniente de una interfaz externa hacia una interna es bloqueado.

Para permitir el tráfico deseado o descartar el tráfico no deseado en el PIX, se aplicarán las ACLs. Las ACLs serán configuradas de la misma manera que en un *router*, con la diferencia de que ahora todas serán extendidas y que se utiliza la máscara de subred regular, en lugar de la *wildcard*.

Cuando un paquete ingresa a un PIX o *router*, éste será analizado por las ACLs existentes, verificando línea por línea si el paquete es permitido o no.

El PIX tiene la opción de agregar una ACE en una ACL ya creada en el orden deseado.

1.3.9.1.1 Comando ICMP

Para que el PIX no sea detectado en la red, es importante deshabilitar el *ping* de la interfaz del PIX, es decir, se deberá especificar si el tráfico ICMP será permitido o no. Si el PIX descarta un paquete ICMP, éste envía un mensaje en el Syslog.

1.3.9.1.2 Agrupación de objetos

El PIX presenta una característica para simplificar la creación y aplicación de ACLs, mediante la agrupación de objetos de red de tipo similar. Con esta agrupación se podrá relacionar a todos los objetos del grupo con una sola ACL.

Los tipos de grupos de objetos que pueden ser creados, son los siguientes:

- Red (*network*): permite agrupar *host*, servidores o subredes.
- Protocolo (*protocol*): permite agrupar protocolos del tipo ICMP, TCP, UDP, IP.
- Servicio (*service*): agrupa números de puertos TCP o UDP asignados a diferentes servicios.
- Tipo de ICMP (*ICMP-type*): agrupa tipos de mensajes ICMP que son permitidos o negados.

Para la creación de grupos de objetos se utilizará el comando **object-group [network | service | protocol | icmp-type]** ***name-id.***

Se ingresa a la configuración del grupo y se especificará qué objetos serán agrupados mediante la aplicación del comando **[network | port | protocol | icmp]-object** ***type.***

1.3.9.1.3 Reunión de grupos de objetos

Permite la reunión de grupos de objetos del mismo tipo, por ejemplo dos o más grupos de objetos de protocolo.

Para reunir grupos de objetos se utilizará el comando de configuración **object-group [network | service | protocol | icmp-type]** ***name-id***.

Se ingresa a la configuración del grupo y se especificará qué grupos de objetos se reunirán mediante el siguiente comando: **group-object** ***name id_grupo de objeto_1***.

1.3.9.2 Filtrado de códigos maliciosos

Los atacantes de redes generalmente insertan *applets*[36] maliciosos dentro de una aplicación aparentemente inofensiva. Una de las posibilidades para contrarrestar este tipo de ataque es bloquear las aplicaciones que posiblemente pueden ocultar estos *applets* maliciosos.

Las aplicaciones que pueden ser bloqueadas son las siguientes:

- Aplicaciones Java
- Aplicaciones Active X
- *User Request Line* (URL)
- HTTPS y FTP

1.3.9.3 Configuración de políticas modulares de un dispositivo de seguridad

El PIX permite identificar el tipo de tráfico que está cursando por él y determinar la prioridad que tendrá, mediante la utilización de *Modular Policy Framework* (MPF). Con MPF el administrador de la red podrá especificar las clases de tráfico y las acciones o políticas aplicados a ellas.

MPF es configurado usando los siguientes comandos:

- **class-map**: Este comando es usado para identificar el tráfico, mediante el análisis del contenido del paquete.

[36] Componente de una aplicación que se ejecuta en el contexto de otro programa, por ejemplo un navegador web.

- **policy-map**: Permite asociar una o más acciones con una clase específica de tráfico.
- **service-policy**: Permite habilitar un conjunto de políticas en una interfaz.

Por defecto, el análisis de protocolos y número de puertos es habilitado en el PIX. En la Figura 1.15 se muestra el *class map* que el PIX tiene por defecto, mientras que en la Figura 1.16 se indican las políticas que son tomadas por el PIX.

```
pixfirewall(config)# class-map insepction_default
pixfirewall(config)# match ?
default-inspection-traffic  Match default inspection traffic:
                            otiqbe-----top--2748        ouseeme-----udp--7648
                            dns--------udp--53          ftp---------top--21
                            gtp--------udp--2123, 3386  h323-h225---top--1720
                            h323--ras--udp--1718-1719   http--------top--80
                            iomp-------iomp             ils---------top--389
                            ngcp-------udp--2427,2727   netbios-----udp--137-138
                            rpc--------udp--111         rsh---------top--514
                            rtsp-------top---554        sip---------top-=5060
                            sip--------udp-5060         skinny------top--2000
                            smtp-------top--25          sqlnet------top--1521
                            xdmop------udp---177
```

Figura 1.15: *Class Map* por defecto del PIX [12]

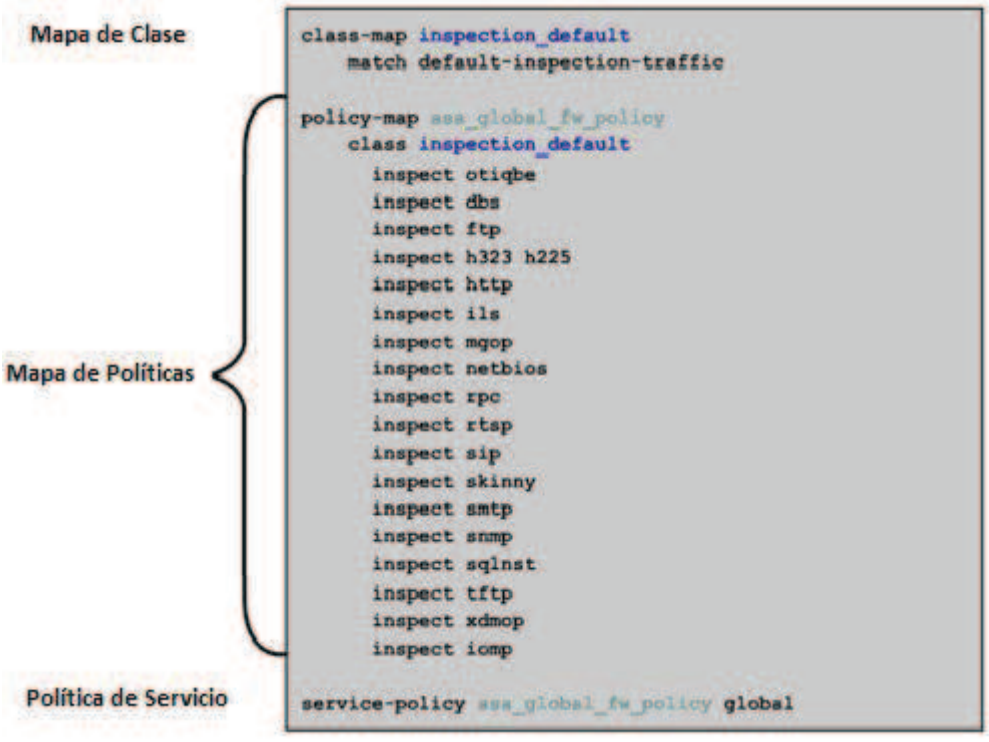


Figura 1.16: *Policy-Map* por defecto del PIX [12]

CAPÍTULO 2

FUNDAMENTOS DE LOS ESTÁNDARES ISO 27001 E ISO 27002

2.1 NORMATIVA INTERNACIONAL SOBRE SEGURIDAD DE LA INFORMACIÓN

2.1.1 NORMAS INTERNACIONALES PUBLICADAS

Dada la necesidad de las organizaciones para demostrar una adecuada gestión en seguridad de la información, se han creado normas o estándares con el fin de establecer o mejorar un sistema que permita garantizarla. Varios organismos internacionales han desarrollado estándares, facilitando y garantizando el cumplimiento de la seguridad de la información. Algunos de los estándares más conocidos son:

- ISO 17.799: Publicado por *Internacional Standard Organization* (ISO). Establece recomendaciones para administrar adecuadamente la seguridad de la información, que ha de ser documentada.

- COBIT: *Control Objectives for Information and related Technology*. Desarrollado por *Information Systems Audit and Control Association* (ISACA). Centra su interés en la gobernabilidad, aseguramiento, control y auditoría para Tecnologías de la Información y Comunicación (TIC).

- ITIL: *Information Technology Infrastructure Library*. Recoge las mejores prácticas para administrar los servicios de Tecnología de la Información (TI).

- Ley SOX: Obliga a las empresas públicas de Estados Unidos a mantener un control y almacenamiento informático de todas sus actividades.

- COSO: *Committee of Sponsoring Organizations*. Conserva el control contable y financiero de las organizaciones.

- ISO Serie 27000: Integra un conjunto de normas sobre Sistemas de Gestión de Seguridad de la Información (SGSI), que a través de su aplicación, permite administrar la información mediante el modelo *Plan – Do – Check – Act* (PDCA[37]).

2.1.2 CORRESPONDENCIA ENTRE NORMAS

Las normas de la ISO Serie 27000 son correspondientes con otras normas que comúnmente se aplican en las organizaciones, como las normas ISO 9001 e ISO 14001. Resulta fiable y sencilla la integración del SGSI, planteado en la ISO Serie 27000, con sistemas de gestión ya existentes, como los indicados.

La correspondencia entre la Norma ISO 9001 y la ISO Serie 27000, radica en que la primera especifica los requisitos para administrar un buen sistema de gestión de calidad, mientras que la segunda detalla el establecimiento de un SGSI. El establecimiento de un SGSI junto a un sistema de gestión de calidad permite garantizar un servicio organizado, seguro y de mejor calidad.

La Norma ISO 14001 establece las especificaciones y elementos para implementar un Sistema de Gestión Ambiental. Una de las consideraciones para un SGSI es prever posibles desastres naturales que pudieran afectar a la información de la empresa. Además la norma considera contraproducente el almacenamiento de información no actualizada, con lo que se podría reciclar la información impresa innecesaria. Al relacionar ambas normativas, se considera ciertos parámetros del SGSI como elementos favorecedores para la conservación del medio ambiente, factor principal para la Norma ISO 14001.

[37] Acrónimo en español de Planificar – Hacer – Revisar – Actuar

2.2 INTRODUCCIÓN A LAS NORMAS ISO 27000

2.2.1 ORIGEN Y DESARROLLO

Las Normas ISO/IEC 27000 constituyen una familia de estándares, desarrolladas por la ISO y por la *International Electrotechnical Commission* (IEC); son comúnmente conocidas como Normas ISO 27000. Esta familia de estándares se publicó ante la necesidad de contar con una base para la gestión de la seguridad de la información, especificando los requisitos para establecer, implementar, controlar, mantener e innovar un SGSI, conocido en inglés como *Information Security Management System* (ISMS).

British Standards Institution (BSI) desarrolló la norma BS 7799. La primera parte de la norma, denominada BS 7799-1, se publicó en 1995; a través de la cual se proporcionaba a las empresas británicas una serie de buenas prácticas con respecto a la gestión de la seguridad de la información. La segunda parte de la norma, BS 7799-2, se publicó en 1998; en ella se especifican los requisitos necesarios para que un SGSI pueda ser certificado.

ISO adoptó la norma BS 7799-1 en el año 2000, sin cambios significativos, denominándola ISO 17799. En cuanto a la segunda parte de la norma fue adoptada y publicada por la ISO en el año 2005 como ISO 27001; posteriormente, en el año 2007, se renombró a la norma ISO 17799 como ISO 27002. En la Figura 2.1, se resume el desarrollo de las normas ISO 27001 e ISO 27002, desde sus orígenes, como BS 7799 Parte 2 y BS 7799 Parte 1, respectivamente.

2.2.2 OBJETIVOS Y CAMPO DE ACCIÓN

Cada día, más empresas deciden adoptar las normas ISO 27000 como base y guía para su funcionamiento. Los objetivos que persigue la directiva de una empresa que implementa el estándar ISO 27000, son principalmente los siguientes:

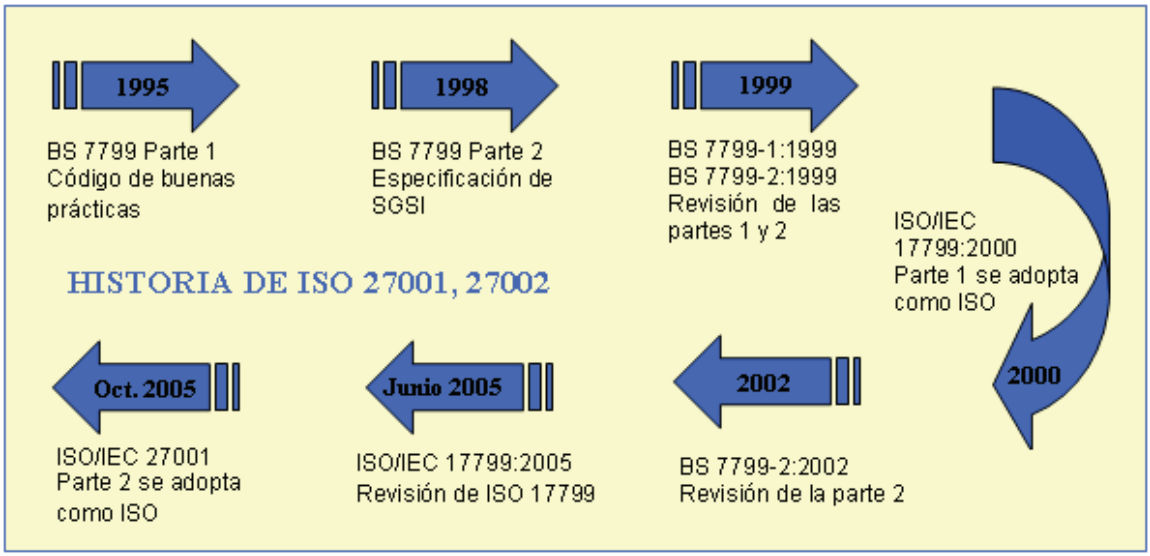


Figura 2.1: Evolución de normas ISO 27001 y 27002 [1]

- Contar con recomendaciones útiles para las personas encargadas de la proyección, implementación y control de la seguridad de la información.

- Mantener y mejorar los niveles de seguridad de sistemas, redes, equipos, información de la empresa, datos de los clientes y empleados, mediante la utilización de controles y análisis de riesgos.

- Elaborar planes de contingencia estratégicos que den solución en caso de posibles problemas o ataques detectados, de modo que el tiempo para solventar el incidente sea el mínimo posible.

- Concientizar a todo el personal acerca de la importancia de la seguridad de la información que maneja la empresa. Incentivar a que se informen y manejen las recomendaciones elaboradas en base a la normativa ISO 27000.

- Conservar documentada toda la información relacionada con los procedimientos a llevarse a cabo, para garantizar la seguridad de la información.

- Mantener un monitoreo y revisión constante de que las recomendaciones elaboradas en base a las Normas ISO 27000 están siendo aplicadas adecuadamente. En caso de ser necesario, mejorarlas.

Considerando que las recomendaciones de las Normas ISO 27000 son genéricas, esta normativa es aplicable a cualquier organización, independientemente del tipo, tamaño y naturaleza.

2.2.3 BENEFICIOS

La inversión y el trabajo involucrado en la implementación de procedimientos que garanticen la seguridad de la información, son recompensados con los beneficios que se obtienen. Algunos de los beneficios que se evidencian, se listan a continuación:

- Disminuye el riesgo de alteración, pérdida, robo o mal uso de la información, garantizando la confidencialidad, integridad y disponibilidad de la misma.

- Permite establecer procedimientos bien diseñados, claros y ordenados que permitan administrar eficientemente la seguridad de la información.

- Posibilita la integración de las Normas ISO 27000 con otros sistemas de gestión. Es común que dichas normas se integren con las normas ISO 9001 e ISO 14001.

- Permite garantizar seguridad y confidencialidad a los usuarios cuando acceden a la información, captando así su confianza.

- Se renueva la imagen de la empresa al contar con un elemento diferenciador con respecto a la competencia. Este factor podría ser decisivo en el mercado.

- Brinda confianza al personal de la empresa con respecto a la organización, normativa, recomendaciones, procedimientos a seguir.

- Disminuye tiempos fuera de servicio, luego de presentarse incidentes.

- Simplifica el monitoreo constante del sistema ante posibles riesgos, de modo que se lleve a cabo procedimientos que mitiguen las amenazas.

- Facilita la detección de las vulnerabilidades del sistema de administración de seguridad para tomar acciones de mejora.

2.3 INTRODUCCIÓN A LA FAMILIA DE ESTÁNDARES ISO 27000

La serie ISO 27000 está formada por varias normas. Son consideradas como normas base: ISO 27001 e ISO 27002, mientras que las Normas complementarias son principalmente: ISO 27003, ISO 27004, ISO 27005.

Es posible aplicar solo algunas normas de la familia y no todas, pues podría resultar innecesaria la implementación de toda la familia, en ciertos casos.

A continuación se presenta un resumen de las Normas ISO 27000, de modo que sea posible identificar las normas útiles para determinada organización; cabe recalcar que dentro de la serie de normas ISO 27000, la primera norma lleva el mismo nombre de la familia.

- ISO/IEC 27000

Fue publicada en Noviembre de 2008. Esta norma contiene un glosario de los términos que se utiliza en toda la serie de normas ISO 27000, con sus definiciones; gracias a esta norma, se evita posibles interpretaciones erradas de ciertos términos aplicados en la serie de normas.

- ISO/IEC 27001

Esta norma, certificable, se publicó en Octubre de 2005. Por contener los requisitos para la generación del SGSI, es considerada la norma más importante de la serie. En su Anexo A, presenta el resumen de los objetivos de control y controles expuestos en la norma ISO 27002, que pueden ser seleccionados por

los encargados de generar el SGSI de la organización. No es necesario que se apliquen todos los controles; sin embargo, se deben indicar las razones por las cuales no es necesaria la implementación de los controles obviados.

- ISO/IEC 27002

La norma adquirió este nombre a partir de Julio de 2007; anteriormente, se la conocía como ISO 17799:2005. En esta norma, no certificable, se presenta una guía de buenas prácticas que detalla al Anexo A de la norma ISO 27001, con respecto a los objetivos de control y controles recomendables para la seguridad de la información.

- ISO/IEC 27003

Esta norma aún no ha sido publicada, pese a que ésta haya sido prevista para Mayo de 2009. Se basará en el Anexo B de la norma BS 7799-2 y en algunas recomendaciones y guías, publicadas por la BSI. Básicamente consistirá de dos partes fundamentales: una guía de implementación del SGSI y la información sobre la aplicación y requerimientos del modelo PDCA.

- ISO/IEC 27004

Norma publicada en Diciembre de 2009. Con el fin de facilitar la medición de los componentes de la fase “Hacer”, del modelo PDCA, se especifican métricas y técnicas de medida que permiten determinar qué tan eficaz es el SGSI y qué tan eficaces resultan ser los controles.

- ISO/IEC 27005

Se publicó en Junio de 2008. Sirve como apoyo a la aplicación favorable de la seguridad de la información, otorgándole un enfoque de gestión de riesgos.

- ISO/IEC 27006

Publicada en Febrero de 2007. Detalla los requerimientos para la acreditación de entidades de auditoría y certificación de SGSI. No es considerada como una norma de acreditación por sí sola; se podría decir que facilita la interpretación de

ISO/IEC 17021, en cuanto a criterios de acreditación, cuando éstos se adaptan a entidades de certificación de ISO 27001.

- ISO/IEC 27007

Esta norma se encuentra en desarrollo; se estima su publicación a fines de 2010. Se fundamentará en una guía para la auditoría de un SGSI.

- ISO/IEC 27011

Esta norma fue elaborada en conjunto con la Unión Internacional de Telecomunicaciones (UIT); fue publicada en Diciembre de 2008. Comprende una guía de gestión de seguridad de la información, exclusiva para telecomunicaciones.

- ISO/IEC 27031

Aún se encuentran trabajando sobre esta norma; se espera que su publicación sea a finales del 2010. Contendrá una guía de continuidad de negocio, con respecto a tecnologías de la información y comunicaciones.

- ISO/IEC 27032

Su fecha de publicación se estimaba para Febrero de 2009; sin embargo aún no ha sido publicada. En este estándar, se facilitará una guía con respecto a la "ciberseguridad".

- ISO/IEC 27033

Publicada recientemente, en Diciembre de 2009. Consta de siete partes: gestión de seguridad de redes, arquitectura de seguridad de redes, escenarios de redes de referencia, aseguramiento de las comunicaciones en redes mediante *gateways*, acceso remoto, aseguramiento de comunicaciones en redes mediante VPNs y diseño e implementación de seguridad en redes.

- ISO/IEC 27034

Este estándar aún no ha sido publicado. Consistirá de una guía de seguridad en aplicaciones.

- ISO/IEC 27799

Norma publicada en Junio de 2008. Este estándar trata sobre la gestión de seguridad de la información en el sector sanitario, empleando la norma ISO 27002. Contiene una serie de recomendaciones para la gestión de la salud y seguridad de la información para organizaciones sanitarias y otros relacionados con la información sanitaria.

2.4 ESTÁNDAR INTERNACIONAL ISO/IEC 27001

2.4.1 INTRODUCCIÓN

La norma ISO 27001 ha sido elaborada con el fin de que empresas de cualquier tipo, tamaño y naturaleza puedan establecer, operar, monitorear, revisar, mantener y mejorar un SGSI.

El SGSI es el concepto sobre el que se construye la norma ISO 27001. Un SGSI establecerá el diseño, implantación y mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad a la información. Busca asegurar la confidencialidad, integridad y disponibilidad de los activos de la información, minimizando a la vez los riesgos de seguridad de la información.

Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.

En la Figura 2.2 se esquematiza el impacto de los riesgos en una organización, evidenciándose la necesidad de implementar un SGSI.

Figura 2.2: Impacto de los riegos [2]

2.4.1.1 Terminología [3]

En la norma ISO 27001 se aplican los términos y definiciones que se presentan a continuación, los cuales deben estar claramente entendidos, con el fin de no interpretar de forma errónea las cláusulas de la norma:

- Activo: cualquier cosa que tenga valor para la organización.

- Disponibilidad: la propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada.

- Confidencialidad: la propiedad que esa información esté disponible y no sea divulgada a personas entidades o procesos no autorizados.

- Seguridad de la información: preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no repudio y confiabilidad.

- Evento de seguridad de la información: una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible violación de la política de la seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad.

- Incidente de seguridad de la información: un solo o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones comerciales u amenazan la seguridad de la información.

- Sistema de gestión de seguridad de la información SGSI: esta parte del sistema gerencial general, está basada en un enfoque de riesgo comercial, para establecer, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

- Integridad: la propiedad de salvaguardar la exactitud e integridad de los activos.

- Riesgo residual: el riesgo remanente después del tratamiento del riesgo.

- Aceptación del riesgo: decisión de aceptar el riesgo.

- Análisis de riesgo: uso sistemático de la información para identificar fuentes y para estimar el riesgo.

- Valuación del riesgo: proceso general de análisis de riesgo y evaluación de riesgo.

- Evaluación del riesgo: proceso de comparar el riesgo estimado con el criterio de riesgo dado para determinar la importancia del riesgo.

- Gestión de riesgo: actividades coordinadas para dirigir y controlar una organización con relación al riesgo.

- Tratamiento de riesgo: proceso de tratamiento de la selección e implementación de medidas para modificar el riego.

- Enunciado de aplicabilidad: enunciado documentado que describe los objetivos de control y controles que son relevantes y aplicables al SGSI de la organización.

2.4.2 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Este estándar internacional adopta el modelo del proceso PDCA, el cual se puede aplicar a todos los procesos SGSI, tal como se muestra en la Figura 2.3

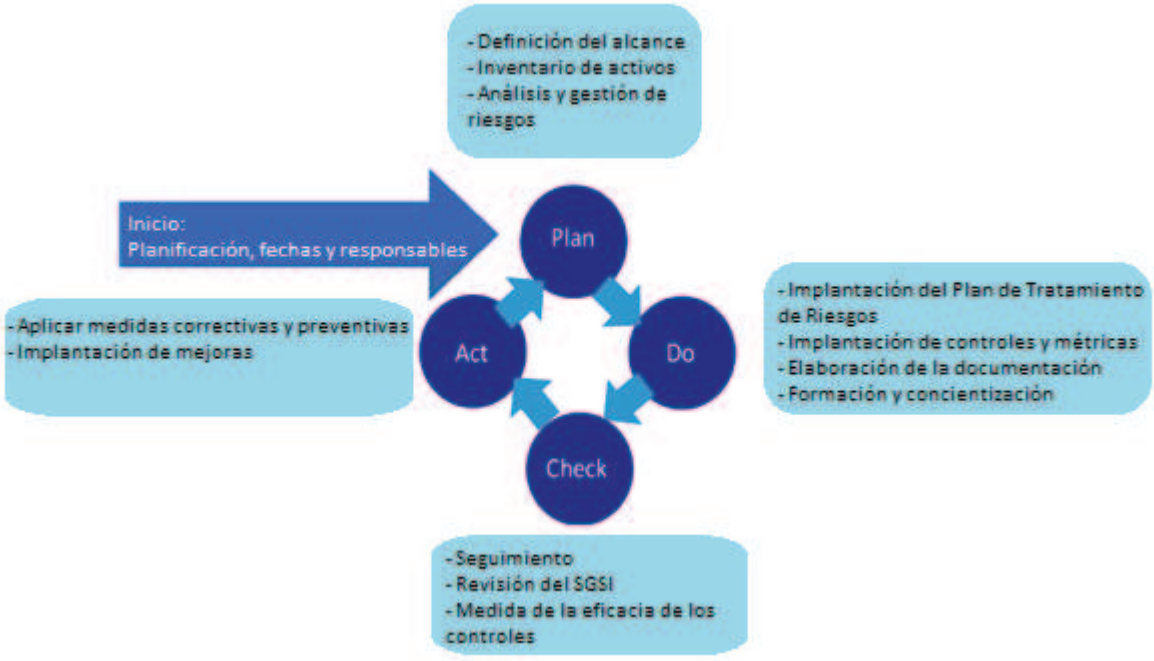


Figura 2.3: Modelo PDCA aplicado a los procesos SGSI [4]

2.4.2.1 Establecer el SGSI (Fase PLANIFICAR)

Es la fase de diseño del SGSI, donde se realiza la evaluación de riesgos de seguridad de la información y se seleccionan los controles adecuados.

Dentro de las especificaciones de la norma, la fase Planificar menciona lo siguiente:

- Definir el alcance y los límites del SGSI. Incluir además los detalles y la justificación de cualquier exclusión del alcance.

- Definir una política SGSI[38], que sea aprobada por la gerencia y que establezca principalmente la forma en la cual se evaluará el riesgo.

- Definir el enfoque de valuación del riesgo, identificando una metodología de cálculo del riesgo[39] y estableciendo niveles de riesgo adecuados.

- Identificar los riesgos que afecten los activos involucrados en el alcance del SGSI, detectando las vulnerabilidades y posibles amenazas relacionadas con ellos. Además se deben identificar los impactos que pueden tener las pérdidas de confiabilidad, integridad y disponibilidad sobre los activos.

- Analizar y evaluar los riesgos, calculando el impacto que provocaría un fallo de seguridad en el negocio.

- Identificar y evaluar las opciones para el tratamiento de riesgos. La Figura 2.4 muestra las diferentes opciones del tratamiento de riesgos.

- Seleccionar de acuerdo a lo descrito en la norma ISO 27002, los objetivos de control y controles para el tratamiento de riesgos.

- La gerencia deberá aprobar la implementación y operación del SGSI, además de aceptar los riesgos residuales propuestos.

- Preparar un enunciado de Aplicabilidad, el cual proporciona un resumen de las decisiones concernientes con el tratamiento de riesgos. En éste se indican los objetivos de control y controles seleccionados, las razones por las cuales fueron seleccionados y la justificación de la exclusión de algún control.

---

[38] La política SGSI es considerada como un super-conjunto de la política de seguridad de la información.

[39] Existen metodologías de cálculo de riesgo estandarizadas como la ISO/IEC TR 13335-3, sin embargo es aceptable definir una metodología propia.

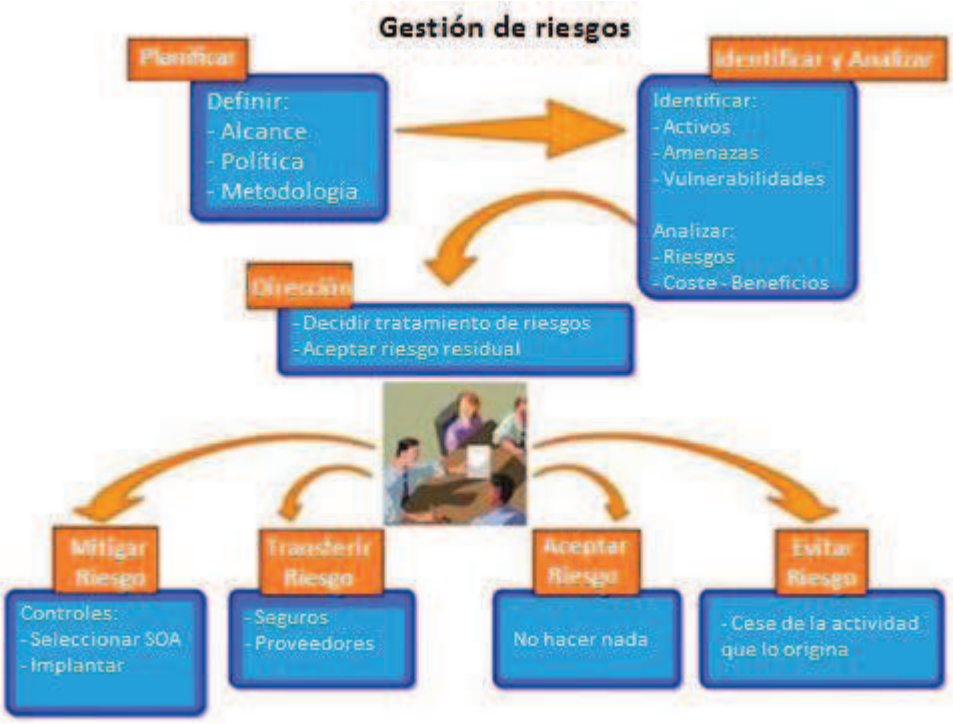


Figura 2.4: Tratamiento de riesgos [5]

2.4.2.2 Implementar y operar el SGSI (Fase HACER)

Es una fase del modelo PDCA que envuelve la implantación y operación de los controles.

Dentro de las especificaciones de la norma, la fase Hacer menciona lo siguiente:

- Definir e implementar el plan de tratamiento de riesgos, incluyendo la asignación de recursos, responsabilidades y prioridades.

- Implementar los controles seleccionados y definir cómo medir la efectividad de los mismos.

- Procurar programas de formación y concientización en relación a la seguridad de la información a todo el personal.

- Gestionar las operaciones del SGSI.

- Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información.

- Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.

2.4.2.3 Monitorear y revisar el SGSI (Fase CONTROLAR)

Es la fase que tiene como objetivo revisar y evaluar el desempeño (eficiencia y eficacia) del SGSI.

Dentro de las especificaciones de la norma, la fase Controlar menciona lo siguiente:

- Ejecutar procedimientos de monitoreo y revisión del SGSI, con el fin de verificar si las acciones realizadas para resolver ataques fueron efectivas.

- Revisar regularmente la efectividad del SGSI, aplicando correctivos en caso de que fuera necesario.

- Medir la efectividad de los controles para verificar que se hayan cumplido los requerimientos de seguridad.

- Revisar regularmente, en intervalos planificados, las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que hayan podido producirse en la organización, la tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior.

- Realizar periódicamente auditorías internas del SGSI en intervalos planificados.

- Revisar periódicamente el SGSI por parte de la Dirección, para garantizar que el alcance definido siga siendo el adecuado y que las mejoras en el proceso del SGSI sean evidentes.

- Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.

- Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI.

2.4.2.4 Mantener y mejorar el SGSI (Fase ACTUAR)

La fase Actuar del modelo PDCA permite realizar cambios cuando sea necesario, para llevar de vuelta el SGSI al máximo rendimiento.

Dentro de las especificaciones de la norma, la fase Actuar menciona lo siguiente:

- Aplicar correctivos que permitan mejorar falencias detectadas en el SGSI, estableciendo acciones correctivas aprendidas de las experiencias de seguridad propias y/o de otras organizaciones.

2.4.3 NORMATIVA

2.4.3.1 Documentación de la norma

Todas las decisiones tomadas por parte de la Gerencia, en relación a cada fase del modelo PDCA, deberán ser debidamente documentadas. Dichos documentos deben ser protegidos y controlados una vez que han sido aprobados.

Adicionalmente los documentos requeridos por el SGSI deben estar actualizados (en caso de haberse realizado alguna modificación) y disponibles para aquellos que los necesitan.

2.4.3.2 Responsabilidad de la Gerencia

El SGSI afecta fundamentalmente a la gestión del negocio, por lo que la responsabilidad del sistema está directamente relacionada con la Gerencia.

La norma ISO 27001 asigna a la Dirección algunas de las tareas fundamentales del SGSI, las cuales permitirán cumplir las cuatro fases del modelo PDCA.

Dentro de las responsabilidades de la Gerencia que menciona la norma se presentan las siguientes:

- Generar el documento donde se establezca la política de seguridad, planteando los objetivos del SGSI y delimitando el alcance

- Proveer los recursos necesarios para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI de acuerdo a los controles aplicados.

- Designar responsables que estén a cargo de realizar las tareas requeridas por el SGSI, siendo éstos adecuadamente capacitados para ejecutarlas competentemente.

2.4.3.3 Auditorías internas SGSI

La organización debe realizar auditorías internas SGSI a intervalos planeados, con el fin de determinar si los objetivos de control, controles, procesos y procedimientos se cumplen según lo planificado.

El procedimiento para realizar dichas auditorías también deberá ser documentado y los resultados de éstas deben ser considerados para eliminar las no conformidades.

2.5 ESTÁNDAR INTERNACIONAL ISO/IEC 27002 [6]

Se conoce a este estándar como: “Tecnología de la Información. Técnicas de Seguridad. Código de Práctica para la Gestión de la Seguridad de la Información”.

2.5.1 OBJETIVO

Esta norma se presenta como una guía práctica para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información dentro de una organización. Tras una evaluación de riesgos, la norma recomienda una serie de objetivos de control y controles a implementarse.

2.5.2 TERMINOLOGÍA

- Control: medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

- Directriz: descripción que aclara lo que se debería hacer y cómo hacerlo, para alcanzar los objetivos establecidos en las políticas.

- Servicios de procesamiento de información: cualquier servicio, infraestructura o sistema de procesamiento de información o los sitios físicos que los albergan.

- Política: toda intención y directriz expresada formalmente por la Dirección.

- Riesgo: combinación de la probabilidad de un evento y sus consecuencias.

- Valoración del riesgo: proceso de comparación del riesgo estimado frente a criterios de riesgo establecidos para determinar la importancia del riesgo.

- Gestión del riesgo: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

- Tercera parte: persona u organismo reconocido por ser independiente de las partes involucradas, con relación al asunto en cuestión.

- Amenaza: causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización.

- Vulnerabilidad: debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas.

2.5.3 ESTRUCTURA

La norma está formada por 11 cláusulas o secciones correspondientes a controles de seguridad. Las cláusulas tienen 39 categorías principales de seguridad en total.

En la Tabla 2.1 se presenta un resumen de las cláusulas que conforman la norma y la cantidad de categorías principales de seguridad de cada una.

CLÁUSULA		CATEGORÍAS PRINCIPALES
1	Política de seguridad	1
2	Organización de la seguridad de la información	2
3	Gestión de activos	2
4	Seguridad de los recursos humanos	3
5	Seguridad física y del entorno	2
6	Gestión de operaciones y comunicaciones	10
7	Control del acceso	7
8	Adquisición, desarrollo y mantenimiento de sistemas de información	6
9	Gestión de los incidentes de seguridad de la información	2
10	Gestión de la continuidad del negocio	1
11	Cumplimiento	3

Tabla 2.1: Cláusulas y Categorías Principales de la Norma ISO 27002

Cada categoría principal de seguridad está formada por un objetivo de control, que determina lo que se desea lograr y por uno o más controles que se pueden aplicar para lograr el objetivo de control.

Para describir cada control se definen tres campos:

- Control: Especifica el control para cumplir el objetivo de control.

- Guía de implementación Detalla la información para la implementación del control y satisfacción del objetivo de control. Podría resultar conveniente, no utilizar toda la guía o realizar modificaciones, en ciertos casos.

- Información adicional: Presenta información que podría ser necesaria, como consideraciones legales.

2.5.4 ESTABLECIMIENTO DE LOS REQUISITOS DE SEGURIDAD

Las tres fuentes principales de requisitos de seguridad son:

- Derivada de la evaluación de riesgos, considerando la estrategia y objetivos generales del negocio. Mediante la evaluación de riesgos, se identifican amenazas, se evalúa la vulnerabilidad y probabilidad de ocurrencia para estimar su impacto.

- La segunda fuente son los requisitos legales, estatutarios, reglamentarios y contractuales para la organización, socios, contratistas, proveedores de servicios y su entorno socio cultural.

- La última fuente es el conjunto de principios, objetivos y requisitos del negocio para el procesamiento de la información para sus operaciones.

2.5.5 EVALUACIÓN DE LOS RIESGOS DE SEGURIDAD Y TRATAMIENTO

Los requisitos de seguridad son identificados a través de una evaluación de riesgos de seguridad. La evaluación de riesgos permite identificarlos, cuantificarlos y priorizarlos. Dependiendo de sus resultados, se toman acciones que permitan implementar los controles para el tratamiento de los riesgos.

Se recomienda incluir estimaciones de la magnitud de los riesgos. Es conveniente realizarla de manera periódica. Una vez realizada la evaluación de cada uno de los riesgos, se toma una decisión para su tratamiento. Existen cuatro posibles decisiones, como se presentó en la Figura 2.4:

- Aplicación de los controles apropiados para reducir los riesgos. Pueden seleccionarse de esta norma, de otro grupo de controles o pueden ser diseñados, dependiendo las necesidades.

- Aceptación objetiva y con conocimiento de los riesgos.

- Impedimento de riesgos al evadir acciones que pudieran hacer que éstos se presenten.

- Transferencia de riesgos asociados a otras partes.

2.5.6 SELECCIÓN DE CONTROLES

Una vez que se han identificado los requisitos y riesgos de seguridad y se han tomado las decisiones para el tratamiento de los riesgos, se selecciona e implementa los controles que garanticen la reducción de los riesgos. Debe existir un equilibrio de la inversión frente a la probabilidad del daño. En esta norma constan tres controles, considerados los principios guía para la gestión de la seguridad de la información:

- Protección de datos y privacidad de la información personal.

- Protección de los registros de la organización.
- Derechos de propiedad intelectual.

2.5.7 CLÁUSULAS

2.5.7.1 Política de Seguridad

2.5.7.1.1 Política de Seguridad de la Información

Su objetivo es apoyar y orientar a la Gerencia de la organización en la gestión de seguridad de la información. Dependiendo de los objetivos del negocio, la directiva establece una dirección clara de la política y apoya en su cumplimiento.

a. Documento de la política de seguridad de la información

- Control

Un documento de política de seguridad de la información debería ser aprobado y comunicado a los empleados y a las partes externas necesarias.

- Resumen de la guía de implementación

El documento contiene la definición de seguridad de la información, objetivos, alcance, la intención de la dirección y su compromiso con la gestión. Se incorpora la estructura para el establecimiento de los objetivos de control y controles, así como la estructura de la evaluación de riesgos y gestión del riesgo. Se presenta una explicación breve sobre las normas, políticas y requisitos de cumplimiento. Define las responsabilidades para la gestión. Podría incluir información adicional que pudiera dar soporte a la política.

b. Revisión de la política de seguridad de la información

- Control

La revisión de la política de seguridad de la información debería realizarse de manera periódica o cuando se produzcan cambios significativos.

- Resumen de la guía de implementación

Un responsable desarrolla, revisa y valora la política. Durante la revisión se debe considerar la retroalimentación de las partes interesadas, resultados de revisiones independientes y previas, estados de acciones preventivas y correctivas, desempeño del proceso y cumplimiento de la política, cambios que pudieran afectar a la gestión de la seguridad de la organización. Además se deben tomar en cuenta las amenazas y vulnerabilidades, incidentes reportados y recomendaciones de las autoridades.

2.5.7.2 Organización de la Seguridad de la Información

2.5.7.2.1 Organización Interna

Su objetivo es gestionar la seguridad de la información de la organización. Se requiere la aprobación de la política de seguridad, asignación de funciones, coordinación y revisión de la implementación, por parte de la dirección. Conviene contar con una fuente asesora especializada en seguridad de la información.

a) Compromiso de la Dirección con la seguridad de la información

- Control

La Dirección debería apoyar a la seguridad dentro de la organización, comprometiéndose y conociendo todas las responsabilidades.

- Resumen de la guía de implementación

La Dirección es responsable de asegurar que las metas identificadas, satisfacen los requisitos de la organización. Debe formular, revisar y aprobar la política de seguridad de la información; además revisar la eficacia de su implementación y proporcionar los recursos necesarios para la misma. Se debe encargar de aprobar la asignación de funciones y responsabilidades e iniciar planes para concientizar sobre la seguridad de la información. Es imprescindible que se encargue de la coordinación para la implementación de los controles.

b) Coordinación de la seguridad de la información

- Control

Los representantes de todas las áreas de la organización deberían coordinar las actividades de la seguridad de la información.

- Resumen de la guía de implementación

La Coordinación involucra la colaboración de directores, usuarios, administradores, diseñadores de aplicación, auditores y personal de seguridad. Garantiza que las actividades de seguridad se realicen conforme la política; identifica y maneja los incumplimientos. Aprueba metodologías para la evaluación de riesgos y clasificación de la información. Identifica cambios significativos y amenazas; evalúa la idoneidad y coordina la implementación de los controles. Evalúa la información recibida del monitoreo y la revisión de los incidentes para recomendar las acciones apropiadas.

c) Asignación de responsabilidades para la seguridad de la información

- Control

Definir claramente las responsabilidades de la seguridad de la información.

- Resumen de la guía de implementación

Definir las responsabilidades para la protección de activos y para la realización de procesos específicos de seguridad. Los individuos con responsabilidades de seguridad asignadas, pueden delegar labores de seguridad a otros; sin embargo, deben dar seguimiento a la ejecución correcta de la tarea delegada.

d) Proceso de autorización para los servicios de procesamiento de información

- Control

Establecer un proceso de autorización de la Dirección para servicios nuevos de procesamiento de la información.

- Resumen de la guía de implementación

La autorización para servicios nuevos es concedida por el Director responsable del sistema de información local y la dirección general. Verificar que el hardware y software sean compatibles con otros componentes del sistema. Identificar servicios personales o privados en el procesamiento de información de la organización, pues podrían introducir nuevas vulnerabilidades.

e) Acuerdos sobre confidencialidad

- Control

Identificar y revisar regularmente los requisitos de confidencialidad o acuerdos de no-divulgación, para mantener la seguridad de la información.

- Resumen de la guía de implementación

Los acuerdos deberían contener los requisitos para asegurar la información confidencial. Para identificar dichos requisitos, se consideran los siguientes elementos: definición de la información, duración del acuerdo, acciones al término del acuerdo, responsabilidades y acciones de los suscriptores, propiedad de la información, secretos comerciales, uso permitido de la información. El derecho de auditar y monitorear los procesos, así como el proceso de notificación en caso de violación o incumplimiento del acuerdo.

f) Contacto con las autoridades

- Control

Conservar contacto con las autoridades pertinentes.

- Resumen de la guía de implementación

Establecer procedimientos que indiquen el momento y la autoridad encargada[40] a la que se le debería reportar algún incidente de seguridad de la información identificado. Es posible que organizaciones víctimas de ataques, requieran de terceras partes, para tomar acciones y contrarrestar los ataques.

[40] La autoridad encargada podría ser policía, bomberos, autoridades de supervisión.

g) Contactos con grupos de interés especiales

- Control

Mantener contacto con grupos de interés especiales, foros especializados en seguridad de la información y asociaciones de profesionales.

- Resumen de la guía de implementación

Es conveniente pertenecer a un grupo de interés especial, para mejorar y actualizar los conocimientos de seguridad, recibir alertas sobre ataques y vulnerabilidades, acceder a asesoría especializada. Sin embargo, se debe tener cuidado con la información compartida, por cuestiones de sensibilidad.

h) Revisión independiente de la seguridad de la información

- Control

Revisar de manera independiente el enfoque de la organización para la gestión de la seguridad de la información y su implementación, a intervalos planificados o cuando ocurran cambios considerables.

- Resumen de la guía de implementación

La revisión debería ser realizada por personas independientes del área revisada. Esta revisión[41] es necesaria para asegurar la eficacia e idoneidad del enfoque de la organización para la gestión de la seguridad de la información.

2.5.7.2.2 Partes Externas[42]

Su objetivo es conservar la seguridad de la información de la organización a la cual tienen acceso partes externas o que es procesada por éstas.

[41] La revisión podría incluir entrevistas de la Dirección, verificación de registros o revisión de los documentos de la política de seguridad.

[42] Se considera como parte externa a: proveedores, clientes, asesores, auditores, limpieza, alimentación, personal temporal, etc.

a) Identificación de los riesgos relacionados con las partes externas

- Control

Identificar los riesgos para la información y servicios de procesamiento de la información, si éstos van a ser utilizados por partes externas.

- Resumen de la guía de implementación

Para identificar los riesgos, se consideran los servicios a los que la parte externa tendrá acceso, el tipo de acceso[43], la importancia y sensibilidad de la información involucrada y controles para proteger la información a la que no tendrá acceso. Se deberá conocer al personal externo que manejará la información; el impacto de acceso denegado o acceso a información inexacta, las condiciones para la continuación del acceso en caso de un incidente. También se tomarán en cuenta los requisitos reglamentarios y obligaciones de la parte externa.

b) Abordaje de la seguridad cuando se trata con los clientes

- Control

Antes de permitir el acceso a los clientes a activos o información, se deberían considerar todos los requisitos de seguridad identificados.

- Resumen de la guía de implementación

Considerar factores como: protección de activos[44], descripción del producto o servicio, requisitos y beneficios del acceso, política de control de acceso[45]. Notificación e investigación de inexactitudes, incidentes y violaciones de la seguridad. Nivel aceptable e inaceptable del servicio, derecho a monitorear y revocación de acciones relacionadas con los activos. Responsabilidades civiles y legales del cliente y de la organización. Derechos de propiedad intelectual, asignación de derechos de copia y protección de trabajo en colaboración.

---

[43] El tipo de acceso puede ser físico, lógico o conexión de red.

[44] Procedimientos para proteger información y software, determinar si se han puesto en peligro los activos, integridad y restricciones a la copia o divulgación de la información.

[45] Control y uso de identificadores únicos (ID) y contraseña, autorización para los privilegios, declaración de prohibición de acceso no autorizado, revocación de derechos de acceso.

c) Abordaje de la seguridad en los acuerdos con terceras partes

- Control

En los acuerdos con terceras partes que impliquen el acceso o uso de la información o servicios de procesamiento de la información, se deberían considerar todos los requisitos de seguridad pertinentes.

- Resumen de la guía de implementación

En el acuerdo se incluye la política de seguridad de la información, controles para proteger activos[46], responsabilidades del usuario y del administrador. Disposiciones en caso de transferencia de personal, formatos para presentación de informes, procesos en gestión de cambios, política de control de acceso. Investigación de incidentes, descripción de cada servicio e información disponible, nivel aceptable e inaceptable del servicio. Derecho a monitorear, auditar y revocar acciones, proceso de escalada para solucionar incidentes. Responsabilidades civiles y legales del acuerdo, derechos de propiedad intelectual, participación de tercera parte con subcontratistas y sus controles. Condiciones para renegociación o término del acuerdo[47].

2.5.7.3 Gestión de Activos

2.5.7.3.1 Responsabilidad por los Activos

Su objetivo es conseguir una protección adecuada de los activos de la organización.

a) Inventario de activos

- Control

Identificar todos los activos. Mantener un inventario de los activos importantes.

---

[46] Protección de hardware y software, protección física, protección contra software malicioso, determinación si los activos han estado en peligro, devolución o destrucción de la información cuando termine el acuerdo. Confidencialidad, integridad y disponibilidad, restricciones a la copia, divulgación de la información y acuerdos de confidencialidad.

[47] Plan de contingencia en caso de que una de las partes termine antes el acuerdo, renegociación si cambian los requisitos de seguridad y documentación vigente de activos, licencias, acuerdos y derechos.

- Resumen de la guía de implementación

El inventario debería tener información del tipo de activo, formato, ubicación, información de soporte, licencias y el valor para el negocio. Para cada activo es necesario documentar su propiedad y clasificación de la información. Se recomienda identificar niveles de protección, en base a la importancia del activo, su valor para el negocio y su clasificación de seguridad.

b) Propietario de los activos

- Control

Toda la información y los activos asociados con los servicios de procesamiento de la información deberían ligarse a un propietario[48].

- Resumen de la guía de implementación

El propietario del activo es responsable de garantizar que la información y los activos asociados con los servicios de procesamiento de la información se clasifiquen adecuadamente, definir y revisar periódicamente las restricciones y clasificaciones de acceso. Además es el responsable de la entrega del servicio y funcionamiento de activos.

c) Uso aceptable de los activos

- Control

Identificar, documentar e implementar reglas sobre el uso aceptable de la información y sus activos asociados.

- Resumen de la guía de implementación

Los empleados, contratistas y usuarios por tercera parte deben seguir las reglas sobre el uso aceptable de la información, suministradas por el Director correspondiente. Incluyen el uso del correo electrónico e Internet y directrices para el uso de dispositivos móviles, especialmente fuera de la organización.

---

[48] Propietario hace referencia a un individuo o entidad con la responsabilidad aprobada de la dirección para el control, desarrollo, mantenimiento y uso de la seguridad de los activos. No implica derechos de propiedad.

2.5.7.3.2 Clasificación de la Información

Su objetivo es asegurar que la información reciba el nivel adecuado de protección, pues cierta información requiere un grado de protección adicional.

a) Directrices de clasificación

- Control

Clasificar la información de acuerdo a su valor, requisitos legales, sensibilidad e importancia para la organización.

- Resumen de la guía de implementación

Las clasificaciones y controles deben considerar las necesidades de compartir o restringir la información, así como el impacto de tales acciones. El propietario del activo es responsable de definir su clasificación, revisarlo y asegurar de que se encuentre en el nivel adecuado.

b) Etiquetado y manejo de la información

- Control

Utilizar procedimientos para el etiquetado y manejo de la información, de acuerdo al esquema de clasificación.

- Resumen de la guía de implementación

Tanto los activos en formato físico como electrónico deben estar sujetos a etiquetamiento. La etiqueta refleja la clasificación de la información, especialmente si se trata de información crítica. En caso de ser necesario, contar con procedimientos para identificar la clasificación de información de otras organizaciones e interpretar sus etiquetas.

2.5.7.4 Seguridad de los Recursos Humanos

2.5.7.4.1 Antes de la Contratación Laboral

Su objetivo es asegurar que empleados, contratistas y usuarios de terceras partes comprendan sus responsabilidades y sean aptos para las funciones a las que han sido asignados.

a) Roles y responsabilidades

- Control

Definir y documentar los roles y responsabilidades de seguridad de empleados, contratistas y usuarios de terceras partes.

- Resumen de la guía de implementación

Incluir como funciones y responsabilidades: actuar de acuerdo con las políticas de seguridad de la información, proteger los activos contra incidentes, ejecutar procesos de seguridad e informar eventos y riesgos de seguridad.

b) Selección

- Control

Verificar los antecedentes de los candidatos a ser empleados, contratistas o usuarios de terceras partes, de acuerdo con los reglamentos.

- Resumen de la guía de implementación

Para la verificación se requiere referencias de comportamiento satisfactorio, verificación de la identidad y hoja de vida, confirmación de las calificaciones profesionales y otros detalles adicionales[49].

[49] Se considera como detalle adicional un antecedente criminal o información de crédito.

c) Términos y condiciones laborales

- Control

Los empleados, contratistas y usuarios de terceras partes deben estar de acuerdo y firmar los términos y condiciones laborales. El contrato debe especificar las responsabilidades de las partes, en cuanto a seguridad.

- Resumen de la guía de implementación

Los términos laborales deben incluir un acuerdo de confidencialidad si se requiere acceso a información sensible, derechos y responsabilidades legales, responsabilidades para la clasificación de información y gestión de activos asociados, responsabilidades para el manejo de información recibida, responsabilidades fuera de las instalaciones y horas laborales, y acciones en caso de omitir los requisitos de seguridad.

2.5.7.4.2 Durante la Vigencia del Contrato Laboral

a) Responsabilidades de la Dirección

- Control

Exigir que empleados, contratistas y usuarios de terceras partes apliquen la seguridad de la información, según las políticas de la organización.

- Resumen de la guía de implementación

La Dirección debería garantizar que los entes mencionados en el control, estén informados sobre sus responsabilidades y funciones respecto a seguridad.

b) Educación, formación y concientización sobre la seguridad de la información

- Control

Instruir a los individuos que manejan la información, sobre la concientización y actualización de políticas y procedimientos de seguridad de la información.

- Resumen de la guía de implementación

Antes de otorgar el acceso a la información o a los servicios, presentar las políticas de seguridad de la organización y sus expectativas. También se debe establecer los requisitos de seguridad, uso correcto de la información, responsabilidades legales y controles. Instruir sobre las posibles amenazas y a quién contactar para reportar incidentes.

c) Proceso disciplinario

- Control

En caso de violación de la seguridad, debería existir un proceso disciplinario.

- Resumen de la guía de implementación

Analizar la naturaleza y gravedad de la violación, su impacto, si es la primera ofensa o si se repite, si fue intencional o por falta de capacitación. En casos graves de mala conducta, permitir el retiro de las funciones, derechos de acceso y privilegios. No iniciar el proceso, sin antes verificar la violación de la seguridad.

2.5.7.4.3 Terminación o Cambio de la Contratación Laboral

Su objetivo es asegurar que una salida o cambio en la organización, sea de forma ordenada.

a) Responsabilidades en la terminación

- Control

Definir y asignar responsabilidades durante la terminación o cambio de contratación laboral.

- Resumen de la guía de implementación

Las responsabilidades en la terminación deben incluir los requisitos permanentes de seguridad, responsabilidades legales, responsabilidades de acuerdos de

confidencialidad. Los términos y condiciones laborales deberían continuar durante cierto periodo después de terminado el contrato laboral.

b) Devolución de activos

- Control

Los entes deben devolver todos los activos que estén en su poder, al finalizar su contratación laboral, contrato o acuerdo.

- Resumen de la guía de implementación

Los activos a devolver incluyen software, documentos corporativos, equipos, dispositivos de cómputo, tarjetas de crédito y de acceso, manuales, información almacenada electrónicamente. Incluso se debe documentar y transferir conocimiento importante para la continuación de las operaciones.

c) Retiro de los derechos de acceso

- Control

Una vez finalizada la contratación laboral, contrato o acuerdo, retirar o modificar los derechos de acceso a la información y servicios.

- Resumen de la guía de implementación

Los derechos de acceso a retirar o modificar incluyen acceso físico, lógico, claves, servicios de procesamiento de información, suscripciones, documentación que lo identifique como miembro de la organización. Una vez que se retira a una persona de las listas de acceso, notificar a los demás empleados, contratistas o usuarios de terceras partes que ya no compartirán información con dicha persona.

2.5.7.5 Seguridad Física y del Entorno

2.5.7.5.1 Áreas Seguras

Su objetivo es evitar el acceso físico no autorizado, daño o interferencia a las instalaciones y a la información de la organización.

a) Perímetro de seguridad física

- Control

Utilizar perímetros de seguridad[50] para proteger las áreas en donde se tiene información y servicios de procesamiento de información.

- Resumen de la guía de implementación

Definir los perímetros de seguridad, su ubicación y fortaleza. Los perímetros de una edificación que contengan servicios de procesamiento de información, deberían ser robustos físicamente, con paredes sólidas, puertas externas con protección contra acceso no autorizado. Puertas y paredes a prueba de incendio, alarma, sistemas de detección de intrusos. Los servicios de procesamiento de información dirigidos por la organización deberían estar separados físicamente de los dirigidos por terceras partes.

b) Controles de acceso físico

- Control

Proteger las áreas seguras con controles de acceso para permitir el ingreso solo a personal autorizado.

- Resumen de la guía de implementación

Registrar la fecha y hora de entrada y salida de los visitantes, los cuales deben ser supervisados e informados sobre los requisitos de seguridad. Exigir la utilización de una identificación visible, restringir el acceso a áreas seguras al personal.

c) Seguridad de oficinas, recintos e instalaciones

- Control

Implementar seguridad física en oficinas, recintos e instalaciones.

---

[50] Perímetros de seguridad incluye a paredes, puertas de acceso controladas con tarjeta, mostradores de recepción atendidos, etc.

- Resumen de la guía de implementación

Considerar los reglamentos y normas de seguridad y salud; ubicar las instalaciones claves en lugares que eviten el acceso al público. Evitar la señalización de áreas en donde se procese información, así como su ubicación en directorios y listados telefónicos, que pudieran ser accesibles al público.

d) Protección contra amenazas externas y ambientales

- Control

Implementar protecciones físicas contra desastres naturales y artificiales[51].

- Resumen de la guía de implementación

Para evitar daños, colocar los materiales combustibles o peligrosos lejos del área de seguridad, evitar colocar materiales de oficina en un área segura. Ubicar los equipos de repuesto y medios de soporte de seguridad a una distancia prudente; suministrar equipo contra incendios.

e) Trabajo en áreas seguras

- Control

Diseñar y aplicar la protección física para trabajar en áreas seguras.

- Resumen de la guía de implementación

El personal solo debe conocer la existencia de un área segura si fuera necesario, evitar el trabajo no supervisado en áreas seguras. Las áreas seguras vacías deben ser bloqueadas físicamente y revisadas periódicamente. No se debe permitir equipo fotográfico, de video o audio, a menos que sea autorizado.

[51] Se incluye en desastres naturales y artificiales a incendios, inundaciones, terremotos, explosiones, manifestaciones sociales, etc.

f) Área de carga, despacho y acceso público

- Control

Controlar los puntos por donde pudiera ingresar personal no autorizado, como áreas de carga o despacho.

- Resumen de la guía de implementación

Restringir el acceso al área de carga y despacho desde el exterior del edificio; dicha área debe ubicarse en donde el personal no tenga acceso a otras áreas. Inspeccionar y registrar el material entrante antes de llevarlo al punto de uso.

2.5.7.5.2 Seguridad de los Equipos

Su objetivo es evitar la pérdida, daño o robo de los activos, así como la interrupción de las actividades de la organización.

a) Ubicación y protección de los equipos

- Control

Ubicar y proteger los equipos para reducir el riesgo de amenazas.

- Resumen de la guía de implementación

Ubicar los equipos y servicios de procesamiento, de modo que se minimice el acceso innecesario a áreas de trabajo. Colocar elementos que requieran protección especial en lugares especiales; adoptar controles que minimicen el riesgo de amenazas físicas[52]. Restricción de comer, beber y fumar cerca de servicios de procesamiento de información. Protección contra rayos y filtros protectores a las fuentes de energía y a las líneas de comunicaciones.

[52] Robo, incendio, explosión, humo, agua, polvo, vibración, efectos químicos, interferencia con el suministro eléctrico, interferencia con las comunicaciones, radiación electromagnética y vandalismo.

b) Servicios de suministro

- Control

Los equipos deben ser protegidos contra fallas en los servicios de suministro.

- Resumen de la guía de implementación

Los servicios de suministro[53] deben ser adecuados para los sistemas a los que sirven. Es recomendable el uso de UPS[54] para garantizar el funcionamiento continuo de equipos que soportan operaciones críticas; se recomienda iluminación de emergencia. El suministro de agua debe ser adecuado para alimentar el aire acondicionado, equipo de humidificación y sistemas de extinción de incendios. El equipo de telecomunicaciones debería conectarse al servidor mediante dos rutas distintas, por cuestiones de redundancia.

c) Seguridad del cableado

- Control

Tanto el cableado de energía eléctrica como el de telecomunicaciones deben estar protegidos contra daños o intercepciones.

- Resumen de la guía de implementación

Las líneas de energía y de telecomunicaciones en los servicios de procesamiento de información, deben ser subterráneas o tener protección. Para evitar interferencia, separar los cables de energía de los de comunicaciones. Emplear un plano del cableado y etiquetar los equipos y cables.

d) Mantenimiento de los equipos

- Control

Los equipos deben recibir mantenimiento para asegurar su disponibilidad e integridad.

---

[53] Se considera servicios de suministro a: electricidad, agua, alcantarillado, calefacción, ventilación y aire acondicionado.
[54] UPS hace referencia al suministro de energía sin interrupción, en caso de una falla del servicio eléctrico.

- Resumen de la guía de implementación

El mantenimiento debe ser acorde con las especificaciones e intervalos recomendados por el proveedor. Las reparaciones deben ser realizadas por el personal de mantenimiento. Es recomendable conservar registros de las fallas reales o sospechadas, así como el mantenimiento preventivo y correctivo.

e) Seguridad de los equipos fuera de las instalaciones

- Control

Garantizar seguridad a los equipos fuera de las instalaciones.

- Resumen de la guía de implementación

La Dirección autoriza el uso de equipos fuera de la organización. No dejar solos los equipos en lugares públicos; las *laptops* deben ser llevadas como equipaje de mano y camufladas. Si se realiza trabajos en casa, definir controles que aseguren a la información.

f) Seguridad en la reutilización o eliminación de los equipos

- Control

Antes de la reutilización o eliminación de un equipo, verificar que la información crítica almacenada, haya sido eliminada o sobrescrita de forma segura.

- Resumen de la guía de implementación

Destruir los dispositivos que contienen información sensible. Destruir, borrar o sobrescribir la información con técnicas que no permitan recuperarla.

g) Retiro de activos

- Control

No retirar sin autorización previa equipos, información o software.

- Resumen de la guía de implementación

Identificar a aquellos con la autoridad para permitir el retiro de activos. Se recomienda establecer registros y límite de tiempo para el retiro de equipos.

2.5.7.6 Gestión de Comunicaciones y Operaciones

2.5.7.6.1 Procedimientos Operacionales y Responsabilidades

Su objetivo es asegurar la operación correcta y segura de los servicios de procesamiento de información.

a) Documentación de los procedimientos de operación

- Control

Establecer responsabilidades y procedimientos para la gestión y operación de los servicios de procesamiento de información.

- Resumen de la guía de implementación

Documentar: instrucciones de procesamiento y manejo de información, copias de respaldo, requisitos de programación, manejo de errores, restricciones al uso del sistema, contactos de soporte, instrucciones de manejo de medios e informes especiales, uso de papelería especial, informes confidenciales, reinicio y recuperación del sistema en caso de falla, registros de auditoría.

b) Gestión del cambio

- Control

Controlar cambios en los servicios y sistemas de procesamiento de información.

- Resumen de la guía de implementación

Controlar estrictamente los sistemas operativos y software en la gestión de cambio. Los cambios deben ser aprobados, identificados, registrados, planificados, probados, evaluados y comunicados.

c) Distribución (segregación) de funciones

- Control

Distribuir las funciones y áreas de responsabilidad para reducir las posibilidades de modificación no autorizada o el uso inadecuado de los activos.

- Resumen de la guía de implementación

Al distribuir las funciones se reduce el riesgo del uso inadecuado del sistema. Si resulta difícil la distribución de funciones, la Dirección debería monitorear, registrar y supervisar las actividades.

d) Separación de las instalaciones de desarrollo, ensayo y operación

- Control

Separar a las instalaciones de desarrollo, ensayo y operación para reducir los riesgos de acceso o cambios no autorizados.

- Resumen de la guía de implementación

Establecer reglas para la transferencia de software del estado de desarrollo al operativo, que debería estar bajo diferentes sistemas, dominios y cuentas. Las herramientas de desarrollo no deberían ser accesibles en otros estados.

2.5.7.6.2 Gestión de la Prestación del Servicio por Terceras Partes

a) Prestación del servicio

- Control

Garantizar que los controles de seguridad, definiciones del servicio y niveles de prestación sean implementados, mantenidos y operados por el tercero.

- Resumen de la guía de implementación

Incluir acuerdos sobre disposiciones de seguridad, definiciones y gestión del servicio. Si la contratación es externa, se planifican las transiciones[55] seguras necesarias. El tercero debe contar con planes que garanticen la continuidad del servicio después de desastres o fallas.

b) Monitoreo y revisión de los servicios por terceros

- Control

Controlar y revisar regularmente los servicios, reportes y registros suministrados por terceras partes. Realizar auditorías a intervalos regulares.

- Resumen de la guía de implementación

Monitorear los niveles de desempeño del servicio, revisar reportes con formato acordado y mantener reuniones periódicas. Suministrar información sobre incidentes y revisión por ambas partes. Revisar registros y pruebas de auditoría sobre incidentes del tercero. Tener cuidado con la información sensible de la organización que pudiera requerir el tercero.

c) Gestión de los cambios en los servicios por terceras partes

- Control

Gestionar los cambios en la prestación de servicios, considerando la importancia de los sistemas y procesos involucrados, así como la reevaluación de riesgos.

- Resumen de la guía de implementación

Los cambios podrían ser por parte de la organización o del tercero. Dichos cambios pueden ser: mejoras en los servicios o redes, desarrollo de nuevas tecnologías y aplicaciones, modificaciones de las políticas y controles, cambio de ubicación física y cambio de proveedores.

[55] Transiciones involucra a información, servicios de procesamiento de información y todo aquello que se deba transferir.

2.5.7.6.3 Planificación y Aceptación del Sistema

Su objetivo es minimizar el riesgo de fallas en los sistemas.

a) Gestión de la capacidad

- Control

Realizar seguimiento y adaptación del uso de los recursos, proyecciones de requisitos de la capacidad futura.

- Resumen de la guía de implementación

Identificar los requisitos de la capacidad para actividades existentes y nuevas; monitorear el sistema, mejorar su capacidad y eficacia, controles que indiquen problemas en el momento oportuno. Poner atención a recursos cuya adquisición toma mucho tiempo o de costos altos, identificar las tendencias del uso.

b) Aceptación del sistema

- Control

Aceptar sistemas de información nuevos, actualizaciones y versiones nuevas. Realizar las pruebas adecuadas durante el desarrollo y antes de la aceptación.

- Resumen de la guía de implementación

Antes de la aceptación, son necesarios requisitos de desempeño y capacidad de computadores, procedimiento de reinicio y recuperación de errores, planes de contingencia, pruebas, establecimiento de controles, evidencia de que la instalación no afectará a los sistemas existentes, capacitación para la utilización de los sistemas.

2.5.7.6.4 Protección contra Códigos Maliciosos y Móviles[56]

Su objetivo es proteger la integridad del software y de la información.

a) Controles contra códigos maliciosos

- Control

Detección, prevención y recuperación contra códigos maliciosos.

- Resumen de la guía de implementación

Prohibir el uso de software no autorizado, proteger contra riesgos en la obtención de archivos y software. Instalar y actualizar regularmente el software de detección y reparación, revisar la posible presencia de códigos maliciosos en archivos, descargas de correo electrónico y páginas web. Definir procedimientos de gestión en caso de ataques. Mantener información actualizada, de fuentes confiables, sobre códigos maliciosos.

b) Controles contra códigos móviles

- Control

La configuración asegura que los códigos móviles operen de acuerdo con la política de seguridad. Evitar la ejecución de códigos móviles no autorizados.

- Resumen de la guía de implementación

Permitir la ejecución de códigos móviles en entornos con aislamiento lógico. De preferencia, se bloquea el uso y recepción de códigos móviles. Activar medidas técnicas para garantizar la gestión del código móvil, usar controles criptográficos para autenticación del código móvil.

[56] Código de software que se transfiere de un computador a otro y luego se ejecuta automáticamente y lleva a cabo una función específica con poca o ninguna interacción del usuario.

2.5.7.6.5 Respaldo

Su objetivo es mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de información.

a) Respaldo de la información

- Control

Hacer copias de respaldo de la información y del software y ponerlas a prueba.

- Resumen de la guía de implementación

Definir el nivel de respaldo de la información, registrar las copias de respaldo, definir su extensión y frecuencia. Almacenarlos distantes a lugares en donde pudieran sufrir daño. Probar regularmente los medios de respaldo y procedimientos de restauración. Es importante la confidencialidad, por lo que los respaldos deben ser encriptados.

2.5.7.6.6 Gestión de la Seguridad de las Redes

Su objetivo es asegurar la protección de la información en las redes.

a) Controles de las redes[57]

- Control

Mantener y controlar las redes para protegerlas de amenazas. Mantener la seguridad de los sistemas y aplicaciones que usa la red.

- Resumen de la guía de implementación

Separar la responsabilidad operativa por las redes y las operaciones de computador. Establecer responsabilidades y procedimientos para la gestión de equipos remotos; usar controles especiales para la información que pasa por redes públicas o inalámbricas, registrar y monitorear las acciones de seguridad.

[57] Mayor información sobre seguridad de la red, se encuentra en la norma ISO/IEC 18028.

b) Seguridad de los servicios de red

- Control

Identificar e incluir las características de seguridad, niveles de servicio y requisitos de los servicios de la red[58].

- Resumen de la guía de implementación

Determinar, monitorear y auditar la capacidad del proveedor del servicio de red. Identificar las disposiciones y características de seguridad, así como los niveles de servicio y requisitos de gestión.

2.5.7.6.7 Manejo de los Medios

Su objetivo es evitar la divulgación, modificación, retiro, destrucción de activos e interrupción de las actividades sin autorización.

a) Gestión de los medios removibles

- Control

Establecer procedimientos para la gestión de los medios removibles[59].

- Resumen de la guía de implementación

Hacer irrecuperables los contenidos de los medios reutilizables, exigiendo una autorización y registro para el retiro. Almacenar los medios en un ambiente seguro, almacenar información en otro medio para evitar pérdida por deterioro.

b) Eliminación de los medios

- Control

Eliminar de forma segura y sin riesgo los medios que ya no sean requeridos.

---

[58] Los servicios de red incluyen la provisión de conexiones, servicios de red privada y redes con valor agregado, soluciones de seguridad de red administrada y sistemas de detección de intrusión.

[59] Los medios removibles incluyen cintas, discos, memorias de almacenamiento, unidades de almacenamiento removibles, discos compactos, discos de video digital y medios impresos.

- Resumen de la guía de implementación

Identificar los medios que contienen información sensible, almacenarlos y eliminarlos de forma segura[60], registrando el hecho. Seleccionar un contratista con controles y experiencia para la recolección y eliminación de papel y equipos.

c) Procedimientos para el manejo de la información

- Control

Proteger la información manejada y almacenada contra divulgación no autorizada y uso inadecuado.

- Resumen de la guía de implementación

Para todo procedimiento que involucre información se considera: etiquetado de los medios, restricciones de acceso, integridad de datos y de procesamiento. Protección según el nivel de sensibilidad, almacenamiento de los medios de acuerdo a especificaciones del fabricante, rotulado claro de todas las copias de los medios, revisión de las listas de distribución y de receptores autorizados.

d) Seguridad de la documentación del sistema

- Control

Proteger la documentación del sistema[61] contra acceso no autorizado.

- Resumen de la guía de implementación

Almacenar con seguridad la documentación del sistema, mantener mínima y autorizada su lista de acceso, protegerla en la red pública.

2.5.7.6.8 Intercambio de la Información

Su objetivo es mantener la seguridad de la información y del software que se intercambian dentro de la organización y con otras entidades externas.

[60] Mediante incineración, trituración o borrado de los datos.

[61] La documentación del sistema podría contener descripciones de procesos de aplicación, procedimientos, estructuras de datos y procesos de autorización.

a) Políticas y procedimientos para el intercambio de información

- Control

Establecer políticas, procedimientos y controles de intercambio para proteger la información que se intercambia.

- Resumen de la guía de implementación

Proteger la información intercambiada, de intercepción, copiado, modificación, enrutamiento inadecuado y destrucción. Detectar códigos maliciosos, establecer procedimientos para comunicaciones inalámbricas. Usar técnicas criptográficas para proteger la confidencialidad, integridad y autenticidad. Recordar al personal no revelar información sensible, dejarla en un contestador automático o en dispositivos de impresión; no registrar datos en ningún software, evitar conversaciones confidenciales en áreas que no sean destinadas para tal fin.

b) Acuerdos para el intercambio

- Control

Definir acuerdos para el intercambio de información y software entre la organización y las partes externas.

- Resumen de la guía de implementación

Controlar y notificar la transmisión, despacho y recepción. Contar con normas para identificar a los servicios de mensajería, establecer responsabilidades en caso de incidentes, etiquetar la información sensible. Establecer normas técnicas para registrar y leer la información, así como las responsabilidades para la protección de datos, derechos de copia y conformidad de licencias.

c) Medios físicos en tránsito

- Control

Proteger los medios que contienen información, de acceso no autorizado, uso inadecuado o corrupción durante su transporte.

- Resumen de la guía de implementación

Utilizar transporte o servicios de mensajería confiables, de los que se verifique su identificación. Usar el embalaje adecuado y suficiente para proteger el contenido, considerando las especificaciones del fabricante. Si se trata de información sensible, se deben usar controles más estrictos[62].

d) Mensajería electrónica

- Control

Proteger adecuadamente la información contenida en mensajería electrónica.

- Resumen de la guía de implementación

Proteger los mensajes de acceso no autorizado, modificación o negación de servicio. Garantizar confiabilidad, disponibilidad del servicio y que la dirección y transporte del mensaje sean correctos. Si se involucran redes públicas, se requerirá aprobación, así como niveles más sólidos de autenticación.

e) Sistemas de información del negocio

- Control

Manejar políticas y procedimientos para proteger la información relacionada con la interconexión de los sistemas de información del negocio.

- Resumen de la guía de implementación

Se deben considerar: vulnerabilidades conocidas en los sistemas administrativos y de contaduría, así como en los sistemas de comunicación. Establecer políticas para gestionar la forma en que se comparte la información, restricción de acceso, creación de categorías del personal, retención y copias de respaldo.

[62] Controles estrictos como el uso de contenedores cerrados con llave, entrega en la mano, embalajes con sello de seguridad, división de la remesa en varias entregas o uso de rutas diferentes.

2.5.7.6.9 Servicios de Comercio Electrónico

Su objetivo es garantizar la seguridad de los servicios de comercio electrónico y su utilización.

a) Comercio electrónico

- Control

Proteger de incidentes la información asociada con el comercio electrónico que se transmite a través de redes públicas.

- Resumen de la guía de implementación

Elaborar procesos de autenticación y autorización de la persona que establece precios, emite o firma documentos. Conservar la confidencialidad de datos, y de las transacciones. Establecer convenios de forma de pago y comprobarlos. Evitar la pérdida o duplicidad de las transacciones y considerar las responsabilidades asociadas con transacciones fraudulentas.

b) Transacciones en línea

- Control

Proteger la información asociada con las transacciones en línea para evitar su alteración, divulgación, transmisión incompleta, duplicación no autorizada.

- Resumen de la guía de implementación

Usar firmas electrónicas, credenciales de usuario válidas y verificadas. Conservar la confidencialidad y privacidad. Utilizar encriptación de la ruta y seguridad de los protocolos utilizados. Si se utiliza una autoridad confiable[63], la seguridad se incorpora durante todo el proceso de gestión certificado-firma.

[63] Una autoridad confiable se utiliza para emitir y mantener firmas digitales y/o certificados digitales.

c) Información disponible al público

- Control

Proteger la integridad de la información disponible en un sistema de acceso público para evitar la modificación no autorizada.

- Resumen de la guía de implementación

Utilizar mecanismos apropiados, como firmas digitales, para otorgar un nivel alto de integridad. Antes de que la información esté disponible, probar los sistemas de acceso público y aprobarlos. Cada entrada al sistema, se verifica y aprueba.

2.5.7.6.10 Monitoreo

Su objetivo es detectar actividades no autorizadas de procesamiento de la información, registrar eventos y verificar la eficacia de los controles adoptados.

a) Registro de auditorías

- Control

Conservar las grabaciones de registros para auditoría de las actividades de los usuarios y eventos de seguridad para facilitar futuras investigaciones.

- Resumen de la guía de implementación

Los registros deben incluir: identificación de usuario, fecha, hora, detalles de los eventos, intentos aceptados y rechazados de acceso, cambios de configuración, uso de privilegios y de aplicaciones del sistema, archivos accesados y tipo de acceso, direcciones y protocolos de red, alarmas originadas, activación y desactivación de los sistemas de protección.

b) Monitoreo del uso del sistema

- Control

Determinar procedimientos para monitorear el uso de los servicios de procesamiento de información y revisar regularmente los resultados.

- Resumen de la guía de implementación

El nivel de monitoreo depende de la evaluación de riesgos. Se debería considerar: acceso autorizado, operaciones privilegiadas, intentos de acceso no autorizado, alertas o fallas del sistema, cambios o intentos de cambio en la configuración y los controles de seguridad del sistema.

c) Protección de la información del registro

- Control

Proteger la información de la actividad de registro contra el acceso no autorizado o manipulación.

- Resumen de la guía de implementación

Detectar y superar alteraciones en los mensajes registrados, eliminación o edición de archivos de registro y capacidad de almacenamiento de los medios de archivo de registro al límite, que podrían ocasionar la pérdida de información.

d) Registros del administrador y del operador

- Control

Registrar las actividades del operador y del administrador del sistema.

- Resumen de la guía de implementación

Los registros deberían contener: la hora, información o falla del evento, la cuenta y el administrador u operador involucrado y los procesos implicados.

e) Registro de fallas

- Control

Registrar y analizar las fallas para tomar acciones correctivas.

- Resumen de la guía de implementación

Registrar fallas reportadas por usuarios y programas del sistema. Revisar los registros de fallas y comprobar que han sido resueltas, así como las medidas correctivas tomadas.

f) Sincronización de relojes

- Control

Sincronizar los relojes de todos los sistemas de procesamiento de información de la organización, en base a un reloj maestro.

- Resumen de la guía de implementación

Establecer un reloj como estándar en un computador o dispositivo que opere un reloj en tiempo real. Es indispensable la sincronización para garantizar la exactitud de los registros.

2.5.7.7 Control de Acceso

2.5.7.7.1 Requisitos del Negocio para el Control del Acceso

Su objetivo es controlar el acceso a la información.

a) Política de control de acceso

- Control

Establecer, documentar y revisar la política de control de acceso, en base a los requisitos de la organización y de la seguridad para el acceso.

- Resumen de la guía de implementación

Establecer reglas y derechos para el control de acceso. La política considera requisitos de seguridad de las aplicaciones individuales, identificación de la información y riesgos, reglas para distribución y autorización de la información, obligaciones contractuales. La red debe reconocer todos los tipos de conexiones

posibles, distribución de las funciones de acceso[64], retiro de derechos de acceso, además de requisitos para la autorización de solicitudes de acceso y para la revisión periódica de los controles de acceso.

2.5.7.7.2 Gestión del Acceso a Usuarios

Su objetivo es asegurar el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas de información.

a) Registro de usuarios

- Control

Conceder y revocar el acceso a todos los sistemas y servicio para el registro y cancelación de usuarios.

- Resumen de la guía de implementación

Incluir el uso de identificación de usuario ID o ID de grupo, verificar que el usuario tenga autorización y que el nivel de acceso otorgado sea el adecuado. Entregar a los usuarios una declaración de sus derechos de acceso, que debe ser firmada. No otorgar el acceso hasta terminar la autorización, mantener un registro de las personas que usarán el servicio, retirar o bloquear los derechos de acceso cuando un usuario ha cambiado su función. Verificar periódicamente las ID y garantizar que las ID redundantes no sean otorgadas a otros usuarios.

b) Gestión de privilegios

- Control

Restringir y controlar la asignación y el uso de privilegios.

- Resumen de la guía de implementación

La asignación de privilegios se realiza mediante autorización. Asignar el privilegio a un ID diferente al utilizado para el uso normal; identificar a los usuarios y

[64] Distribución de las funciones de acceso involucra: solicitud, autorización y administración del acceso.

privilegios de acceso asociados con cada producto del sistema, asignar privilegios a los usuarios sobre los principios de necesidad de uso y evento por evento.

c) Gestión de contraseñas para usuarios

- Control

Controlar la asignación de contraseñas mediante un proceso formal de gestión.

- Resumen de la guía de implementación

Exigir la firma de una declaración de confidencialidad de contraseñas personales y conservación de contraseñas de grupo entre miembros. Los usuarios deben cambiar las contraseñas suministradas inicialmente y las predeterminadas por el proveedor. Verificar identidad antes de proporcionar una contraseña temporal, que debe ser única y no descifrable. Los usuarios deben confirmar la entrega de contraseñas y no almacenarlas en computadores en formato no protegido.

d) Revisión de los derechos de acceso de los usuarios

- Control

La gerencia debe revisar periódicamente los derechos de acceso.

- Resumen de la guía de implementación

Revisar los derechos de acceso periódicamente y después de cambios de cargos. Revisar las autorizaciones de acceso privilegiado más frecuentemente, y registrar los cambios de cuentas privilegiadas.

2.5.7.7.3 Responsabilidades de los Usuarios

Su objetivo es evitar el acceso de usuarios no autorizados, robo y compromiso de la información y de los servicios de procesamiento de información.

a) Uso de contraseñas

- Control

Exigir a los usuarios el uso de buenas prácticas de seguridad en la selección y uso de contraseñas.

- Resumen de la guía de implementación

Los usuarios deben conservar la confidencialidad de sus contraseñas, evitar su registro y cambiarlas regularmente. Seleccionar contraseñas de calidad[65] con longitud mínima suficiente, cambiar contraseñas temporales en el primer registro de inicio, no usar las mismas contraseñas de trabajo y las personales.

b) Equipo de usuario desatendido

- Control

Asegurarse de dar protección adecuada a un equipo desatendido.

- Resumen de la guía de implementación

Terminar las sesiones activas o asegurarlas con un mecanismo de bloqueo[66], realizar el registro de cierre en servidores, computadoras principales y personales al terminar la sesión. Asegurar los computadores personales o terminales cuando no están en uso, mediante una clave de bloqueo por ejemplo.

c) Política de escritorio despejado y de pantalla despejada

- Control

Adoptar una política de escritorio despejado para reportes y medios de almacenamiento removibles y una política de pantalla despejada para servicios de procesamiento de información.

---

[65] Una contraseña de calidad es fácil de recordar y difícil de adivinar, no debe asociarse con información del usuario, no es vulnerable a ataque de diccionarios, no tiene caracteres idénticos consecutivos ni todos son numéricos o alfabéticos.

[66] El mecanismo de bloqueo más utilizado es un protector de pantalla protegido por contraseña.

- Resumen de la guía de implementación

Asegurar bajo llave la información sensible. Cerrar o proteger las sesiones desatendidas, usando un mecanismo de bloqueo que solicite autenticación. Proteger los puntos de entrada y salida de correo, evitar el uso no autorizado de tecnología de reproducción y retirar inmediatamente de las impresoras los documentos con información sensible.

2.5.7.7.4 Control de Acceso a las Redes

Su objetivo es evitar el acceso no autorizado a los servicios en red.

a) Política de uso de los servicios en red

- Control

Los usuarios sólo deben tener acceso a los servicios autorizados.

- Resumen de la guía de implementación

La política de uso de las redes y servicios de red incluye las redes y servicios a los que se permite el acceso, procedimientos de autorización, controles y procedimientos para proteger el acceso a las conexiones y los medios utilizados para el acceso.

b) Autenticación de usuarios para conexiones externas

- Control

Emplear métodos de autenticación para controlar el acceso de usuarios remotos.

- Resumen de la guía de implementación

Con una técnica criptográfica, *token* de hardware o protocolos de desafío / respuesta, se puede autenticar a usuarios remotos. También se pueden usar las líneas privadas dedicadas o los procedimientos y controles de devolución de

marcación[67]. Para grupos de usuarios, se puede usar la autenticación de nodo. Son necesarios controles adicionales para el acceso a redes inalámbricas.

c) Identificación de los equipos en las redes

- Control

Considerar la identificación automática del equipo como un medio para autenticar conexiones de equipos y ubicaciones específicas.

- Resumen de la guía de implementación

Si la comunicación se puede iniciar desde un equipo o lugar específico, se puede usar la identificación del equipo. El identificador indica a qué red o redes está permitido conectar el equipo y si las redes tienen sensibilidad diferente.

d) Protección de los puertos de configuración y diagnóstico remoto

- Control

Controlar el acceso físico y lógico a los puertos de configuración y diagnóstico.

- Resumen de la guía de implementación

Usar un bloqueo de clave y procedimientos de soporte[68] para controlar el acceso físico al puerto. Retirar o inhabilitar los puertos, servicios y prestaciones que no se requieren para la funcionalidad de la organización.

e) Separación en las redes

- Control

Separar grupos de servicios de información, usuarios y sistemas de información.

---

[67] La devolución de marcación autentica a los usuarios, tratando de establecer una conexión con una red de la organización desde sitios remotos.

[68] Un ejemplo de procedimiento de soporte es garantizar que los puertos de configuración y diagnóstico sólo sean accesibles mediante acuerdo entre el administrador del servicio y el personal de soporte.

- Resumen de la guía de implementación

Se puede dividir a las redes en dominios lógicos de red. Al instalar una puerta de enlace (*gateway*) seguro entre dos redes, se puede controlar el acceso y flujo entre dos dominios. Otra manera para apartar los dominios es restringir el acceso usando VPNs para grupos de usuarios. Se puede separar redes usando la funcionalidad del dispositivo de red, por ejemplo conmutación IP[69]. Implementar controles adicionales en la separación de redes inalámbricas.

f) Control de conexión a las redes

- Control

Restringir la capacidad de los usuarios para conectarse a redes compartidas, especialmente fuera de la organización.

- Resumen de la guía de implementación

La capacidad de conexión se puede restringir mediante *gateways* que filtren el tráfico en base a tablas predefinidas. Las restricciones se dan en cuanto a mensajería, transferencia de archivos, acceso interactivo y a aplicaciones.

g) Control del enrutamiento en la red

- Control

Implementar controles de enrutamiento en las redes, asegurar que las conexiones no incumplan la política de control de acceso.

- Resumen de la guía de implementación

Basar los controles de enrutamiento en mecanismos de verificación para las direcciones fuente y destino. Se pueden usar *gateways* para validar la dirección en los puntos de control de las redes interna y externa si se usa *proxy* o NAT.

[69] Los dominios separados se pueden implementar controlando los flujos de datos de la red, usando las capacidades de enrutamiento / conmutación, como por ejemplo las ACLs.

2.5.7.7.5 Control de Acceso al Sistema Operativo

Su objetivo es evitar el acceso no autorizado a los sistemas operativos.

a) Procedimiento de registro de inicio seguro

- Control

Controlar el acceso a los sistemas operativos a través de un procedimiento de registro de inicio seguro.

- Resumen de la guía de implementación

No mostrar identificadores de aplicación, de sistema ni mensajes de ayuda, hasta que el proceso de registro de inicio se complete. Mostar una advertencia de que sólo deberían acceder usuarios autorizados. Limitar el número de intentos permitidos, registrar intentos exitosos y fallidos, establecer un tiempo antes de permitir intentos adicionales y enviar mensajes de alarma. Al finalizar un registro de inicio exitoso, el sistema debe mostrar la fecha y hora del inicio exitoso previo y detalles de intentos fallidos. No se debe mostrar la contraseña en texto claro en la red o esconderla mediante símbolos.

b) Identificación y autenticación de usuarios

- Control

Todos los usuarios deben tener un ID para su uso personal. Es necesario el uso de una técnica de autenticación para comprobar la identidad.

- Resumen de la guía de implementación

Utilizar una ID para rastrear las actividades de usuario; en el caso de requerir un ID compartido, se necesita de su aprobación y documentación. Los ID genéricos son usados para individuos cuyas actividades no requieren rastreo.

c) Sistemas de gestión de contraseñas

- Control

Los sistemas de manejo de contraseñas deben ser interactivos y asegurar la calidad de las mismas.

- Resumen de la guía de implementación

Usar IDs y contraseñas para conservar la responsabilidad. Permitir la selección y cambio de contraseñas, que deben ser de calidad; forzar a los usuarios a cambiar contraseñas temporales en el primer registro de inicio. Conservar un registro de contraseñas previas para evitar su reutilización. No mostrar contraseñas en pantalla y almacenarlas en formato protegido.

d) Uso de las utilidades del sistema

- Control

Restringir y controlar el uso de programas utilitarios que podrían anular los controles del sistema y de la aplicación.

- Resumen de la guía de implementación

Usar identificación, autenticación y autorización para las utilidades del sistema, que deben ser separadas del software de aplicaciones. Limitar el uso y disponibilidad de las utilidades del sistema, autorizar su uso *ad hoc* y registrarlo. Definir y documentar niveles de autorización para las utilidades del sistema, retirar o inhabilitar utilidades basadas en software innecesario.

e) Tiempo de inactividad de la sesión

- Control

Suspender las sesiones inactivas después de cierto tiempo de inactividad.

- Resumen de la guía de implementación

Despejar la pantalla de sesión; se podría cerrar la sesión de la aplicación y la de red después de cierto periodo de inactividad, que dependerá de los riesgos de seguridad del área, clasificación de la información y aplicaciones que utilizan.

f) Limitación del tiempo de conexión

- Control

Utilizar restricciones en los tiempos de conexión para brindar más seguridad a las aplicaciones de alto riesgo.

- Resumen de la guía de implementación

Usar espacios de tiempo predeterminados para ciertas funciones, restringir los tiempos de conexión a las horas normales de oficina y repetir la autenticación a determinados intervalos.

2.5.7.7.6 Control de Acceso a las Aplicaciones y a la Información

Su objetivo es evitar el acceso no autorizado a la información contenida en los sistemas de aplicación.

a) Restricción de acceso a la información

- Control

Restringir el acceso a la información y a funciones del sistema de aplicación por parte de usuarios y del personal de soporte.

- Resumen de la guía de implementación

Proporcionar menús para controlar el acceso a las funciones del sistema de aplicación; controlar derechos de acceso de los usuarios y de otras aplicaciones. Para datos salientes de sistemas que manejen información sensible, garantizar que se envíe a sitios autorizados solo la información necesaria.

b) Aislamiento de sistemas sensibles

- Control

Los sistemas sensibles deben tener un entorno informático dedicado o aislado.

- Resumen de la guía de implementación

El dueño de una aplicación identifica y documenta la sensibilidad de la misma; además identifica y acepta a los sistemas de aplicación con los que compartirá recursos y riesgos, en caso de que se ejecute en un entorno compartido.

2.5.7.7.7 Computación Móvil y Trabajo Remoto

Su objetivo es garantizar la seguridad de la información cuando se utilizan dispositivos de computación móviles y de trabajo remoto.

a) Computación y comunicaciones móviles

- Control

Establecer una política y adoptar medidas para la protección contra los riesgos debidos al uso de dispositivos de computación y comunicaciones móviles[70].

- Resumen de la guía de implementación

Considerar los requisitos para la protección física, controles de acceso, técnicas criptográficas, copias de respaldo, identificación, autenticación, protección contra virus y controles extras para conexiones inalámbricas. Los usuarios deben evitar ser observados por personas no autorizadas. Manejar la protección adecuada en caso de pérdida o robo de información o de servicios de computación móvil.

[70] Dispositivos de computación y comunicaciones móviles, incluyen a *notebooks*, *palmtops*, *laptops*, tarjetas inteligentes y teléfonos móviles.

b) Trabajo remoto

- Control

Manejar políticas, planes operativos y procedimientos para actividades de trabajo remoto.

- Resumen de la guía de implementación

Disponer de seguridad física, equipo adecuado y medios de almacenamiento, bajo el control de la organización. Definir el trabajo que se permite realizar remotamente, horas laborables, confidencialidad, sistemas y servicios a los que el usuario tiene acceso, reglas sobre el acceso de terceros a la información, disposición de soporte y de pólizas de seguro, auditoría, monitoreo, revocación de autoridad y derechos de acceso y devolución del equipo.

2.5.7.8 Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

2.5.7.8.1 Requisitos de Seguridad de los Sistemas de Información

Su objetivo es garantizar que la seguridad sea parte integral de los sistemas de información.

a) Análisis y especificación de los requisitos de seguridad

- Control

Especificar requisitos para los controles de seguridad en las declaraciones sobre requisitos de la organización para nuevos sistemas de información o mejoras.

- Resumen de la guía de implementación

Considerar controles manuales de apoyo y automatizados para los requisitos de control. Los requisitos reflejan el valor de los activos de información y el daño potencial en caso de falla. Es más económico introducir controles en la etapa de diseño que durante o después de la implementación. Seguir un proceso formal de adquisición y prueba, con contrato, si se adquieren productos; si el producto

proporciona funcionalidades adicionales, evaluar si se introducirían más riesgos o si se puede obtener beneficios de tal funcionalidad.

2.5.7.8.2 Procesamiento Correcto en las Aplicaciones

Su objetivo es evitar errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones.

a) Validación de los datos de entrada

- Control

Validar los datos de entrada a las aplicaciones, asegurando que sean correctos y apropiados.

- Resumen de la guía de implementación

Realizar verificaciones de entradas para detectar valores fuera de rango, caracteres inválidos, datos incompletos y datos de control inconsistentes. Revisar periódicamente el contenido de los campos clave o de archivos de datos, inspeccionar documentos de entrada impresos para determinar cambios no autorizados. Elaborar procedimientos ante errores de validación y para probar credibilidad de los datos entrantes. Definir responsabilidades para el personal del proceso de entrada de datos y crear un registro de actividades.

b) Control de procesamiento interno

- Control

Incorporar verificaciones de validación en las aplicaciones para detectar corrupción de la información por errores de procesamiento o actos deliberados.

- Resumen de la guía de implementación

Revisar que los programas se ejecuten en el orden y momento correctos, y que terminen en caso de falla. Utilizar programas para recuperación después de fallas,

proteger contra ataques por desbordamiento o exceso en el *buffer*[71] y documentar las actividades. Validar los datos de entrada generados por el sistema, verificar la integridad y autenticidad de los datos o software.

c) Integridad del mensaje

- Control

Identificar los requisitos para asegurar la autenticidad y proteger la integridad del mensaje en las aplicaciones.

- Resumen de la guía de implementación

Realizar una evaluación de los riesgos de seguridad, determinando si es necesaria la integridad del mensaje e identificando el método más apropiado.

d) Validación de los datos de salida

- Control

Validar los datos de salida de una aplicación para asegurar que el procesamiento de la información almacenada sea adecuado.

- Resumen de la guía de implementación

Verificar que los datos de salida sean razonables. Usar cuentas de control de conciliación, asegurando el procesamiento de todos los datos. Garantizar el suministro de información suficiente, procedimientos para responder las pruebas de validación. Definir responsabilidades en el proceso y registrar las actividades.

2.5.7.8.3 Controles Criptográficos

Su objetivo es proteger la confidencialidad, autenticidad o integridad de la información, mediante medios criptográficos.

[71] Ubicación de la memoria en una computadora o en un instrumento digital reservada para el almacenamiento temporal de información digital, mientras que está esperando ser procesada.

a) Política sobre el uso de controles criptográficos

- Control

Manejar una política para el uso de controles criptográfico que protejan la información.

- Resumen de la guía de implementación

La política debe considerar: posición de la gerencia con respecto a los controles criptográficos, nivel de protección considerando el tipo, fortaleza y calidad del algoritmo de encriptación. Proteger la información sensible contenida en medios móviles o removibles. Gestión de claves, incluyendo la protección de claves criptográficas y recuperación de información encriptada en caso de incidente.

b) Gestión de claves

- Control

Establecer la gestión de claves para apoyar el uso de técnicas criptográficas en la organización.

- Resumen de la guía de implementación

Proteger las claves criptográficas, privadas y secretas contra incidentes. Resguardar el equipo que genera, almacena y archiva las claves. El sistema de gestión de claves debe generar claves para diferentes sistemas criptográficos y aplicaciones, generar y obtener certificados de claves públicas, distribuir claves a los usuarios, almacenar claves, cambiar o actualizarlas, tratar las claves perdidas y revocarlas o desactivarlas.

2.5.7.8.4 Seguridad de los Archivos del Sistema

Garantizar la seguridad de los archivos del sistema.

a) Control del software operativo

- Control

Controlar la instalación de software en los sistemas operativos.

- Resumen de la guía de implementación

Solo administradores autorizados actualizan el software operativo, aplicaciones y librerías de programas. Los sistemas operativos solo contienen códigos ejecutables aprobados. Solo después de un ensayo exhaustivo exitoso, se implementa el software. Usar control de configuración y documentarlo, conservar y archivar las versiones anteriores del software. El uso de parches de software es útil para eliminar debilidades del sistema, pero deben ser probados antes.

b) Protección de los datos de prueba del sistema

- Control

Seleccionar, proteger y controlar cuidadosamente los datos de prueba.

- Resumen de la guía de implementación

Evitar el uso de bases de datos operativas con información personal o sensible, para pruebas, aplicar procedimientos de control de acceso a los sistemas de aplicación de pruebas. Cada vez que se copia información operativa en un sistema de prueba se requiere autorización. Al terminar la prueba, borrar la información operativa del sistema de prueba, registrando la acción.

c) Control de acceso al código fuente de los programas

- Control

Restringir el acceso al código fuente[72] de los programas

- Resumen de la guía de implementación

No mantener librerías fuente de programas en los sistemas operativos, restringir su acceso. Solo después de recibir la autorización, actualizar las librerías fuente

[72] El código fuente de programas es un código escrito por los programadores, compilado para crear ejecutables.

de programas y elementos asociados. Mantener los listados de programas en un entorno seguro, registrar los accesos a las librerías fuente de programas.

2.5.7.8.5 Seguridad en los Procesos de Desarrollo y Soporte

Mantener la seguridad del software e información del sistema de aplicaciones.

a) Procedimientos de control de cambios

- Control

Controlar la implementación de cambios con procedimientos de control.

- Resumen de la guía de implementación

Documentar los procedimientos de control de cambios[73] que podrían incluir evaluación de riesgos, análisis de impacto, controles de seguridad, registro de niveles de autorización, garantía de que los cambios se realizan por usuarios autorizados en el momento oportuno sin causar perturbación, documentación actualizada tras cambios y manejo de documentación antigua, identificación de elementos que requieren mejora, mantenimiento de una versión de control.

b) Revisión técnica de las aplicaciones después de los cambios en el sistema operativo

- Control

Revisar y someter a prueba las aplicaciones críticas cuando se cambian sistemas operativos, asegurando que no hay impacto adverso.

- Resumen de la guía de implementación

Revisar procedimientos de integridad y control de la aplicación luego de los cambios, garantizar que el plan y presupuesto de soporte cubrirá revisiones y pruebas. Asegurar la notificación oportuna sobre cambios en el sistema operativo, monitorear vulnerabilidades y nuevas versiones de parches y arreglos.

[73] Un cambio podría ser la introducción de sistemas nuevos o de cambios importantes en los sistemas existentes.

c) Restricciones en los cambios a los paquetes de software

- Control

Desalentar las modificaciones a los paquetes de software, limitarlas a los cambios necesarios y controlarlas estrictamente.

- Resumen de la guía de implementación

Preferir el uso de paquetes de software sin modificaciones. Si es necesaria la modificación, considerar el riesgo de que los procesos de integridad y control se vean comprometidos, consentimiento del vendedor o posibilidad de solicitar los cambios, el impacto si la organización se hace responsable del futuro mantenimiento. Conservar el software original y aplicar los cambios a una copia.

d) Fuga de información

- Control

Evitar oportunidades para que se produzca fuga de información.

- Resumen de la guía de implementación

Explorar los medios y comunicaciones de salida para determinar información oculta, así como el comportamiento de las comunicaciones y del sistema de modulación y enmascaramiento. Utilizar sistemas y software con integridad alta, monitorear las actividades del personal, sistema y sus recursos.

e) Desarrollo de software contratado externamente

- Control

Supervisar y monitorear el desarrollo de software contratado externamente.

- Resumen de la guía de implementación

Considerar acuerdos sobre licencias, propiedad de códigos y derechos de propiedad intelectual. Certificación y derechos de acceso para auditar la calidad y

exactitud del trabajo, convenios de fideicomiso, requisitos contractuales para la seguridad del código y pruebas antes de la instalación.

2.5.7.8.6 Gestión de la Vulnerabilidad Técnica

Su objetivo es reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas.

a) Control de las vulnerabilidades técnicas

- Control

Obtener información sobre vulnerabilidades técnicas de los sistemas de información en uso, evaluar la exposición a las vulnerabilidades y tomar acciones para tratar los riesgos asociados.

- Resumen de la guía de implementación

Establecer funciones y responsabilidades para la gestión de las vulnerabilidades técnicas[74], identificar los recursos de información para identificar las vulnerabilidades técnicas, definir el tiempo de reacción, riesgos y acciones ante notificaciones de las vulnerabilidades. Evaluar los riesgos asociados con la instalación de parches y probarlos. Si no hay parche disponible, "apagar" los servicios asociados a la vulnerabilidad, agregar controles de acceso y aumentar monitoreo. Registrar los procedimientos efectuados.

2.5.7.9 Gestión de los Incidentes de Seguridad de la Información

2.5.7.9.1 Reporte sobre los Eventos y las Debilidades de la Seguridad de la Información

Su objetivo es asegurar que los eventos y debilidades de seguridad de la información se comuniquen oportunamente para tomar las acciones correctivas.

[74] La gestión de vulnerabilidades técnicas incluye monitoreo, evaluación de riesgos, uso de parches, rastreo de activos y coordinación.

a) Reporte sobre los eventos de seguridad de la información

- Control

Informar sobre eventos de seguridad de la información, mediante canales de gestión apropiados, lo antes posible.

- Resumen de la guía de implementación

Establecer un procedimiento para el reporte de eventos de seguridad de la información[75] y otro de escalada y respuesta ante el incidente, establecer las acciones a tomar al recibir un reporte. Determinar un punto de contacto para el reporte. Los procedimientos de reporte deben incluir: procesos de retroalimentación para que el que reporta reciba los resultados y verifique su solución, formatos para el reporte, comportamiento ante un evento y el proceso disciplinario en caso de violación de la seguridad.

b) Reporte sobre las debilidades en la seguridad

- Control

Exigir a los empleados, contratistas y usuarios de terceras partes que observen y reporten las debilidades observadas o sospechadas en los sistemas o servicios.

- Resumen de la guía de implementación

Informar inmediatamente al responsable sobre debilidades para evitar incidentes en la seguridad de la información. Los mecanismos de reporte deben ser fáciles, accesibles y disponibles. No intentar probar una debilidad sospechada.

2.5.7.9.2 Gestión de los Incidentes y las Mejoras en la Seguridad de la Información

Su objetivo es asegurar la aplicación de un enfoque consistente y eficaz en la gestión de incidentes de seguridad de la información.

[75] Los eventos incluyen: pérdida de servicio o equipo, mal funcionamiento del sistema o software o hardware, errores humanos, incumplimiento de políticas, violaciones de seguridad física o de acceso, cambios no controlados.

a) Responsabilidades y procedimientos

- Control

Establecer responsabilidades y procedimientos para asegurar una respuesta adecuada a los incidentes.

- Resumen de la guía de implementación

Emplear reportes de eventos y debilidades de la seguridad de la información, monitoreo de sistemas, vulnerabilidades y alertas para detectar incidentes. Los procedimientos incluyen: manejo de diferentes tipos de incidentes[76], planes de contingencia, análisis de la causa del incidente, acciones correctivas para evitar recurrencia, comunicación con afectados, reporte de la acción, recolección y aseguramiento de evidencia, acción para la recuperación y corrección de fallas.

b) Aprendizaje debido a los incidentes de seguridad de la información

- Control

Utilizar mecanismos para cuantificar y monitorear el tipo, volumen y costo de los incidentes de seguridad de la información.

- Resumen de la guía de implementación

Utilizar la información obtenida de la evaluación de incidentes de seguridad de la información, para identificar los incidentes recurrentes o de alto impacto.

c) Recolección de evidencias

- Control

Recolectar, retener y presentar evidencia cuando una acción de seguimiento contra una persona u organización tras un incidente de seguridad de la información, implica acciones legales.

[76] Algunos tipos de incidentes son: fallas en el sistema, pérdida del servicio, códigos maliciosos, negación del servicio, errores por datos inexactos, uso inadecuado de sistemas.

- Resumen de la guía de implementación

Manejar procedimientos internos para recolectar y presentar evidencia con propósito disciplinario. Las reglas para la evidencia son la admisibilidad, es decir si la evidencia se puede o no utilizar en la corte y su peso, es decir la calidad y cabalidad de la evidencia.

2.5.7.10 Gestión de la Continuidad del Negocio

2.5.7.10.1 Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio

Su objetivo es contrarrestar interrupciones en las actividades de la organización y proteger sus procesos críticos de fallas en los sistemas de información o desastres, asegurando la recuperación oportuna.

a) Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio

- Control

Establecer un proceso de gestión para la continuidad del negocio en la organización, tratando los requisitos de seguridad de la información.

- Resumen de la guía de implementación

Los elementos del proceso son: comprensión de los riesgos con identificación de prioridad de los procesos críticos y activos involucrados; comprensión del impacto de interrupciones; adquisición de pólizas de seguros; controles preventivos y mitigantes; identificación de recursos[77] para tratar los requisitos identificados; seguridad del personal y servicios; planes de continuidad del negocio; pruebas y actualizaciones regulares de planes y procesos.

[77] Los recursos abarca: financieros, organizacionales, técnicos y ambientales.

b) Continuidad del negocio y evaluación de riesgos

- Control

Identificar eventos que pudieran ocasionar interrupciones en los procesos del negocio, junto con la probabilidad e impacto de la interrupción.

- Resumen de la guía de implementación

Identificar todos los eventos y realizar evaluaciones de riesgos para determinar la probabilidad e impacto de posibles interrupciones, considerando el tiempo, escala de daño y periodo de recuperación. En la evaluación de riesgos, tomando en cuenta todos los procesos de la organización, debe participar el dueño de los recursos y procesos. Una vez creada la estrategia, la Dirección la aprueba.

c) Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información

- Control

Manejar planes para mantener o recuperar las operaciones y asegurar la disponibilidad de la información, después de una interrupción o falla.

- Resumen de la guía de implementación

Establecer responsabilidades y procedimientos para la continuidad, identificar la pérdida aceptable de información y servicios, desarrollar procedimientos para recuperar operaciones y disponibilidad en el tiempo requerido. Establecer los procedimientos operativos mientras se termina la recuperación, documentar los procesos, formar al personal y realizar pruebas y actualizaciones de los planes, cuyos recursos deben identificarse. Conservar copias de los planes de continuidad en lugares seguros.

d) Estructura para la planificación de la continuidad del negocio

- Control

Mantener una sola estructura de los planes de continuidad, asegurando su consistencia e identificando prioridades para pruebas de mantenimiento.

- Resumen de la guía de implementación

Cada plan de continuidad debe contener su enfoque para la continuidad, el plan de escalada y las condiciones para su activación, las personas responsables de cada componente, un dueño específico. Una estructura para la planificación de la continuidad del negocio aborda los requisitos de seguridad de la información y considera: procedimientos de emergencia, respaldo, operativos temporales, de reanudación, además condiciones para la activación del plan, programación de mantenimiento, actividades de concientización, responsabilidades de las personas y suplentes y los activos y recursos para los procedimientos.

e) Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio

- Control

Someter a pruebas y revisiones periódicas los planes de continuidad del negocio, asegurando su eficacia y actualización.

- Resumen de la guía de implementación

Las pruebas programadas de cada elemento del plan, aseguran que los miembros del equipo sean conscientes de los planes, sus responsabilidades y funciones. Registrar los resultados para tomar acciones de mejora. En caso de cambios[78], se debería considerar la actualización de los planes de continuidad.

[78] Los cambios se presentan en: personal, direcciones o número telefónicos, estrategia del negocio, lugares, dispositivos y recursos, legislación, contratistas, proveedores, clientes, procesos existentes, procesos nuevos o retirados, riesgos.

2.5.7.11 Cumplimiento

2.5.7.11.1 Cumplimiento de los Requisitos Legales

Su objetivo es evitar el incumplimiento de cualquier ley, obligación estatutaria, reglamentaria o contractual y de cualquier requisito de seguridad.

a) Identificación de la legislación aplicable

- Control

Definir, documentar y actualizar los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos.

- Resumen de la guía de implementación

Definir y documentar controles y responsabilidades para cumplir estos requisitos.

b) Derechos de propiedad intelectual (DPI)

- Control

Asegurar el cumplimiento de registros legales, reglamentarios y contractuales sobre el uso de material con DPI y software patentado.

- Resumen de la guía de implementación

Para proteger material con DPI, publicar una política de cumplimiento de los DPI que defina el uso legal de información y software que no viole derechos de copia. Concientizar sobre las políticas para proteger los DPI y las acciones en caso de ser violados, mantener registros de los activos, conservar prueba y evidencia sobre propiedad de licencias, discos maestros, manuales. No exceder el número máximo de usuarios permitidos, verificar que se instale software autorizado y productos con licencia, cumplir los términos para software obtenido de redes públicas. No duplicar, convertir en otro formato ni copiar total o parcialmente documentos que no lo permita la ley de derechos de copia.

c) Protección de los registros de la organización

- Control

Proteger los registros importantes de pérdida, destrucción y falsificación.

- Resumen de la guía de implementación

Cada registro debe contener detalles de los periodos de retención y los medios de almacenamiento. Almacenar el material relacionado con claves criptográficas, encriptación o firmas digitales, de modo que se permita el descifrado de los registros durante el periodo de retención. Considerar el posible deterioro de los medios utilizados para almacenar los registros; si se utiliza medios electrónicos, garantizar la capacidad de acceso a los datos.

d) Protección de los datos y privacidad de la información personal

- Control

Garantizar la protección de los datos y la privacidad, conforme la legislación, reglamentos y cláusulas del contrato.

- Resumen de la guía de implementación

Manejar una política de protección y privacidad de los datos, que debe ser comunicada a todos los involucrados en el procesamiento de información personal. Se podría responsabilizar a una persona para tal labor.

e) Prevención del uso inadecuado de los servicios de procesamiento de información

- Control

Persuadir a los usuarios no utilizar servicios de procesamiento de información para fines no autorizados.

- Resumen de la guía de implementación

La Dirección aprueba el uso de los servicios de procesamiento de información, si detecta el uso no autorizado de cierto servicio, debe tomar la acción disciplinaria

adecuada. Todos los usuarios deben conocer el alcance de su acceso permitido y del monitoreo. Conviene que en el registro de inicio, se presente un mensaje de advertencia sobre el acceso no autorizado.

f) Reglamentación de los controles criptográficos

- Control

Utilizar controles criptográficos que cumplan los acuerdos, leyes y reglamentos.

- Resumen de la guía de implementación

Considerar restricciones de importaciones y/o exportaciones de hardware y software diseñados para adicionarles funciones criptográficas o para ejecución de las mismas, restricciones al uso de encriptación.

2.5.7.11.2 Cumplimiento de las Políticas y las Normas de Seguridad y Cumplimiento Técnico

Su objetivo es asegurar que los sistemas cumplan con las normas y políticas de seguridad de la organización.

a) Cumplimiento con las políticas y las normas de seguridad

- Control

Garantizar que los procedimientos de seguridad se llevan a cabo correctamente para lograr el cumplimiento de las políticas y normas de seguridad.

- Resumen de la guía de implementación

Revisar y registrar regularmente el cumplimiento del procesamiento de información con las políticas de seguridad, normas y requisitos. Al hallar algún incumplimiento, se determina la causa y acción correctiva apropiada.

b) Verificación del cumplimiento técnico

- Control

Verificar periódicamente los sistemas de información para determinar el cumplimiento con las normas de implementación de la seguridad.

- Resumen de la guía de implementación

Realizar la verificación del cumplimiento técnico, manualmente y/o con ayuda de herramientas automáticas que generan un informe técnico. Tener precaución si se utilizan evaluaciones de vulnerabilidad o pruebas de penetración[79], pues podrían poner en peligro la seguridad del sistema.

2.5.7.11.3 Consideraciones de Auditoría de los Sistemas de Información

Su objetivo es maximizar la eficacia de los procesos de auditoría de los sistemas de información y minimizar su interferencia.

a) Controles de auditoría de los sistemas de información

- Control

Planificar y acordar los requisitos y actividades de auditoría que implican verificaciones de los sistemas operativos, minimizando el riesgo de interrupciones.

- Resumen de la guía de implementación

Acordar los requisitos de auditoría con la Dirección, acordar y controlar el alcance de las verificaciones. Limitar las verificaciones al acceso de sólo lectura, permitir acceso diferente a sólo lectura para copias aisladas de archivos del sistema. Identificar los recursos para las verificaciones, monitorear y registrar todo acceso, documentando procedimientos, requisitos y responsabilidades. El auditor debe ser independiente de las actividades auditadas.

[79] Las pruebas de penetración y las evaluaciones de vulnerabilidad proveen una visión instantánea de un sistema en un estado específico en un momento específico.

b) Protección de las herramientas de auditoría de los sistemas de información

- Control

Proteger el acceso a herramientas de auditoría de los sistemas de información para evitar su uso inadecuado.

- Resumen de la guía de implementación

Separar las herramientas de auditoría de sistemas de información y los sistemas operativos o de desarrollo. No mantener las herramientas de auditoría en librerías de cinta, a menos que tengan un nivel adecuado de seguridad.

CAPÍTULO 3

SITUACIÓN ACTUAL DE MEGADATOS S.A.

3.1 GENERALIDADES DE LA EMPRESA

3.1.1 HISTORIA

La empresa ACCESS INTERNET con razón social MEGADATOS S.A. inició su labor en el campo de las telecomunicaciones en el año 1995 en la ciudad de Quito para prestar servicios de Internet. Posteriormente en septiembre del año 2002 adquirió el negocio de RAMTELECOM Telecomunicaciones S.A. convirtiéndose en la empresa ACCESSRAM, manteniendo el nombre de MEGADATOS S.A. como razón social.

En el 2004 comienza el proceso de fusión con ECUANET manteniéndose dicho nombre como marca comercial y MEGADATOS S.A. como razón social, conservándose de esta manera hasta la actualidad. En la Figura 3.1 se resume la evolución de la empresa.

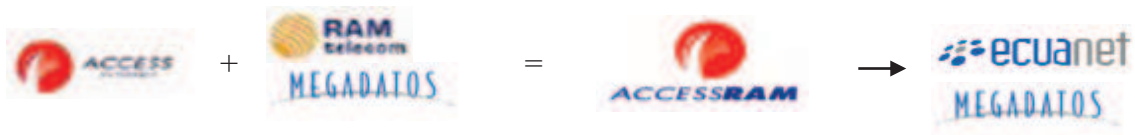


Figura 3.1: Evolución de la empresa MEGADATOS S.A.

3.1.2 MISIÓN Y VISIÓN

- **Misión [1]**

"Facilitamos el acceso a la información por medio del asesoramiento y provisión de soluciones integrales de calidad con un recurso humano altamente calificado y

motivado. Fomentamos relaciones a largo plazo contribuyendo con el crecimiento de nuestros clientes, colaboradores, accionistas y de esta forma al desarrollo de la Sociedad de la Información, el país y la organización."

- **Visión [1]**

"Ser reconocidos como:
- La mejor corporación facilitadora del acceso a la información y conocimiento.
- Líder en calidad de soluciones integrales en telecomunicaciones.
- Socios estratégicos de nuestros clientes.
- Una organización de calidad y excelencia, producto del compromiso de su gente."

3.1.3 ESTRUCTURA

La Empresa MEGADATOS S.A. está estructurada en cinco niveles. Cada integrante de la Empresa pertenece a un nivel, dependiendo de las funciones que lleva a cabo. Los niveles que se maneja son:

- Alta Dirección
- Nivel Directivo
- Nivel Ejecutivo
- Nivel Ejecutor
- Nivel Operativo

Se puede observar, en detalle, la estructura de la Empresa MEGADATOS S.A. en el Organigrama que se presenta en la Figura 3.2.

3.1.4 OFICINAS PRINCIPALES Y FILIALES

Las oficinas principales se encuentran en Quito, Guayaquil y Cuenca, en las siguientes direcciones:

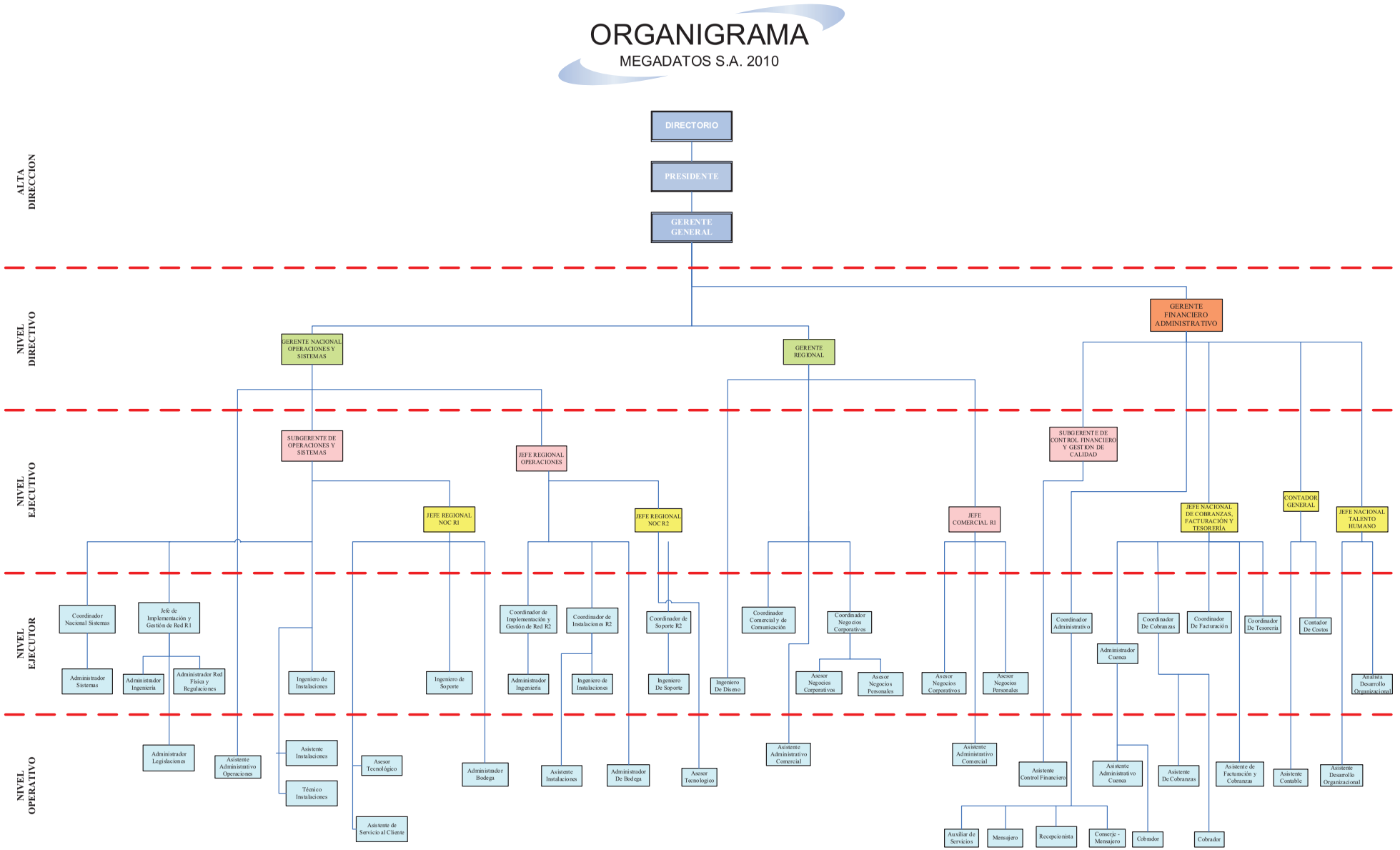


Figura 3.2: Organigrama de la Empresa MEGADATOS S.A. [2]

- Quito: Av. Núñez de Vela E 3-13 y Atahualpa, Edificio Torre del Puente, Pisos 2, 3 y 8.
- Guayaquil: Urb. Kennedy Norte Av. Miguel Alcívar, Edificio Torres del Norte B, Piso 4.
- Cuenca: Av. Del Estadio entre Manuel J. Calle y Roberto Crespo, Edificio del Estadio, Piso 4.

La empresa, además cuenta con oficinas filiales en Manta, Machala, Puerto Ayora, Ambato, Ibarra, Riobamba y Macas.

3.1.5 SERVICIOS BRINDADOS

ECUANET, para satisfacer las necesidades de sus clientes, considerando el desarrollo tecnológico acelerado y la creciente ola de las comunicaciones, brinda una gran variedad de servicios.

3.1.5.1 Internet

3.1.5.1.1 Banda Ancha Empresarial (Dedicado)

a. ISP

Este servicio es apropiado para ISP's, Cyber Cafés, *Call Centers* (VoIP), empresas de telecomunicaciones, empresas internacionales y grandes industrias. El acceso a Internet es proporcionado desde los nodos de Quito, Guayaquil o Cuenca. Algunas de las especificaciones del servicio brindado se presentan en la Tabla 3.1.

Garantía (*performance*) al POP USA	100%
Garantía (*performance*) al POP Local	100%
Disponibilidad	99,80%
Retardo de transmisión (ping)	Menor a 120 ms
Alojamiento de *hosting* de hasta	25 MB

Tabla 3.1: Especificaciones principales del servicio para ISP [3]

b. Corporativo

Este servicio fue diseñado para industrias florícolas, petroleras, gobierno, empresas internacionales Se proporciona el acceso a Internet a través de cualquier nodo de la empresa. Algunas de las especificaciones del servicio brindado se presentan en la Tabla 3.2.

Garantía (*performance*) al POP USA	60%
Garantía (*performance*) al POP Local	100%
Disponibilidad	99,80%
Retardo de transmisión (ping)	Menor a 120 ms
Alojamiento de *hosting* de hasta	25 MB

Tabla 3.2: Especificaciones principales del servicio Corporativo [3]

c. Small Office

Diseñado para empresas medianas. Cualquier nodo de ECUANET proporciona el servicio de Internet. Las especificaciones más importantes del servicio brindado se presentan en la Tabla 3.3.

Garantía (*performance*) al POP USA	35%
Garantía (*performance*) al POP Local	100%
Disponibilidad	99,60%
Retardo de transmisión (ping)	Aprox. 150 ms
Alojamiento de hosting de hasta	25 MB

Tabla 3.3: Especificaciones principales del servicio Small Office [3]

3.1.5.1.2 Banda Ancha Personal (Dedicado)

a. Banda Ancha Alámbrica

El servicio se provee a través de un módem DSL, entregando Internet dedicado con infraestructura simétrica o asimétrica. Se ofrecen tres velocidades,

dependiendo las necesidades del cliente y el contrato que desee: 128/64 kbps, 256/128 kbps y 512/128 kbps.

b. Banda Ancha Inalámbrica

Se provee Internet dedicado con infraestructura WIMAX o WIFI, llegando a cualquier lugar del país, inclusive a sitios en donde otros proveedores no llegan. Las velocidades disponibles son: 192 kbps, 256 kbps, 320 kbps y 512 kbps.

3.1.5.1.3 Dial Up (Conmutado)

Se ofrece conexión al Internet, a través de la línea telefónica, con instalación inmediata del servicio. Se ofrece este servicio en dos planes: ilimitado y por horas.

3.1.5.1.4 Internet Móvil (Conmutado)

Permite al usuario navegar en Internet, desde su computador personal, en cualquier lugar y en movimiento. Dentro de este servicio, ECUANET, ofrece tres opciones de Internet Móvil: 300 MB, 1000 MB y 2000 MB[80].

3.1.5.2 Servicios Informáticos

3.1.5.2.1 Diseño y Posicionamiento de Sitios Web

La tendencia del comercio por Internet, es cada vez más popular entre las empresas que encuentran en este medio una alternativa poderosa para ofrecer sus productos o servicios. A su vez, los clientes están optando por esta tendencia, que les ofrece mayor comodidad y facilidad.

ECUANET, ofrece el diseño y posicionamiento de sitios Web, facilitando así el desempeño de las empresas que optan por usar este servicio.

[80] Cantidad de información mensual que puede ser descargada de Internet.

3.1.5.2.2 Web Conference

Es una herramienta que facilita la comunicación entre individuos que no se encuentran en el mismo lugar; otorga mayores beneficios que el servicio telefónico pues emula presencia física a través de video. No se requiere de equipos costosos, representando así una herramienta muy conveniente si se considera el factor costo – beneficio.

3.1.5.2.3 E-Learning

Actualmente, un aliado que ha tomado mayor fuerza en la capacitación del personal, educación superior y de postgrado, es el *e-learning* o aprendizaje en línea. Con esta herramienta, se ahorran costos y tiempo.

ECUANET, ofrece este servicio como el instrumento ideal para la capacitación del personal en empresas que buscan su constante desarrollo y mejoramiento; a través de un personal altamente capacitado con conocimientos innovadores.

3.1.5.3 Servicios Adicionales

3.1.5.3.1 Voz IP

A través de este servicio, la voz viaja digitalmente en forma de paquetes, a través del Internet.

Este servicio es ofrecido por ECUANET, con el propósito de brindar mayores aplicaciones a los clientes y un ahorro en sus comunicaciones.

3.1.5.3.2 Soporte Linux

ECUANET, ofrece la configuración, instalación y soporte para servidores LINUX. Además garantiza asesoría, capacitación, actualizaciones, etc.

3.1.5.3.3 VPN

Las redes privadas virtuales facilitan el acceso remoto de datos, servidores, aplicaciones; constituyen una opción ideal para la construcción de intranets o redes corporativas.

Este servicio es ofrecido por ECUANET, como una excelente alternativa para empresas que requieren comunicarse con sus sucursales nacionales o internacionales.

3.2 INFRAESTRUCTURA DE LAS REDES UTILIZADAS PARA LOS SERVICIOS DE TELECOMUNICACIONES EN QUITO

El presente Proyecto de Titulación está enfocado a la seguridad de la información correspondiente a las aplicaciones brindadas por la Empresa en la ciudad de Quito, por lo que se trabajará únicamente con las redes correspondientes.

Las redes que brindan servicio a los clientes en la ciudad de Quito están conformadas, a nivel de capas 2 y 3 únicamente por equipos Cisco; razón por la cual se realizó el análisis de los equipos de seguridad que ofrece dicho proveedor, en el Capítulo 1.

Para un mejor análisis, se ha dividido a las redes de la empresa en tres partes:

- Centro de Datos.
- MEGARED[81] alámbrica.
- MEGARED inalámbrica.

En la Figura 3.3, se presenta la infraestructura para proveer los servicios en la ciudad de Quito.

[81] Se considera MEGARED debido a que es una infraestructura que solo utiliza extensores de redes LAN y la prestación de servicios es únicamente a nivel de capa 2 (VLANs).

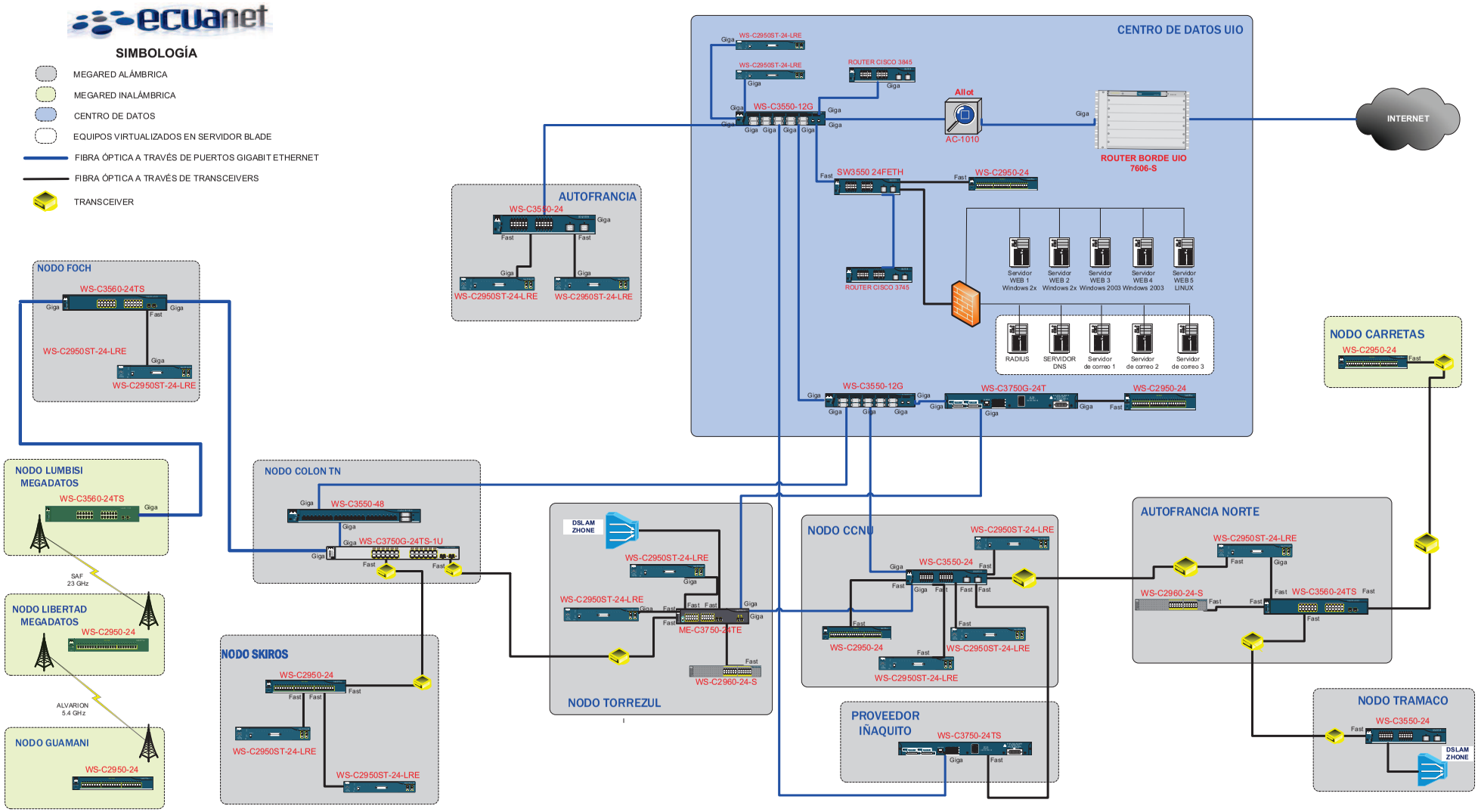


Figura 3.3: Diagrama de red ECUANET Quito [4]

3.2.1 CENTRO DE DATOS

Está ubicado en el piso 8 de las oficinas de la ciudad de Quito. Es el lugar en el cual se concentran todos los equipos de *backbone*[82].

El servicio entregado por los proveedores se concentra en el *router* de borde, el cual permite el enrutamiento hacia los diferentes destinos; posteriormente la información se dirige al Allot, el cual se encarga de limitar el ancho de banda asignado a cada uno de los clientes. La información se propaga a través de cada uno de los *switches*, cuyos puertos permiten el paso de VLANs específicas, de modo que la información se transmita adecuadamente.

3.2.1.1 Servidores

Para brindar los servicios informáticos, se cuenta con los diferentes servidores WEB, en los cuales están alojadas las páginas de los clientes y de la empresa.

Para la autenticación de los clientes *dial-up* y aquellos que poseen cuentas de correo, se utiliza el servidor Radius, el cual valida el nombre de usuario y contraseña ingresados.

El servidor *Domain Name Server* (DNS) asocia un nombre a una dirección IP y viceversa, de tal forma que los clientes puedan navegar por Internet sin inconvenientes.

Los diferentes servidores de correo alojan todos los correos que han sido enviados o recibidos por cuentas que pertenecen a los dominios de Ecuanet; además conservan un respaldo de los mismos hasta que el cliente se los descargue.

[82] Es la infraestructura de la transmisión de datos en una red o un conjunto de ellas en Internet.

3.2.2 MEGARED ALÁMBRICA

Está formada por 9 nodos, en donde se encuentran los equipos a los cuales se conectan las últimas millas hacia los clientes, siendo éstos de capa 2. En los equipos se han configurado los puertos, de tal forma que permitan la propagación de las VLANs desde el Centro de Datos hacia el cliente final.

Todas la conexiones entre nodos se realizan con fibra óptica, ya sea a través de puertos *Gigabit Ethernet* o *Fast Ethernet*; mientras que en las últimas millas, se utiliza cobre o fibra óptica a través de puertos *Fast Ethernet* o *Long Reach Ethernet*[83].

Los equipos de última milla utilizados para los clientes son: Cisco LRE 575, Módems Loop o *transceivers* TP-Link.

3.2.3 MEGARED INALÁMBRICA

Está formado por 4 nodos, cuyas últimas millas son enlaces de radio. En cada nodo se manejan *switches* de capa 2 que tienen el mismo concepto de MEGARED alámbrica, es decir la propagación de VLANs para la transmisión de datos.

Los enlaces hacia los clientes pueden ser punto – punto o punto – multipunto, utilizando como equipos de última milla: radios Alvarion, radios MTI, radios Tranceo y radios Teletronics. Las frecuencias utilizadas para los enlaces son en bandas no licenciadas[84], siendo 5.4 GHz, 5.8 GHz y 900 MHz las utilizadas.

---

[83] *Long Reach Ethernet* es un protocolo de red propietario desarrollado por Cisco, el cual permite velocidades de 5 a 15 Mbps.

[84] Se considera banda no licenciada a aquellas frecuencias que pueden ser utilizadas libremente, sin requerir el pago por el uso del espectro.

3.3 ACTIVOS RELACIONADOS CON LOS SERVICIOS DE TELECOMUNICACIONES EN QUITO

3.3.1 RECURSO HUMANO

El personal del Departamento de Operaciones que está a cargo y tiene acceso a los equipos de *backbone* de la ciudad es:

- 1 Jefe Regional NOC R1
- 2 Asesores Tecnológicos
- 6 Ingenieros de Soporte
- 3 Ingenieros de Instalaciones
- 2 Asistentes de Instalaciones
- 1 Técnico de Instalaciones
- 1 Jefe de Implementación y Gestión de Red R1
- 2 Administradores de Ingeniería
- 1 Administrador de Red Física y Regulaciones
- 1 Administrador de Legislaciones
- 1 Coordinador Nacional de Sistemas

3.3.2 BIENES MATERIALES

Se identifican los equipos que conforman las redes que permiten entregar los servicios a los clientes, tanto en el Centro de Datos como en los nodos.

En las Tablas 3.4 y 3.5, se especifica el modelo, cantidad y precio unitario de cada uno de los equipos.

Las características técnicas de los equipos identificados en el inventario, se detallan en la Tabla 3.6.

3.3.2.1 Inventario [85]

CENTRO DE DATOS			
EQUIPO	**MODELO / SISTEMA OPERATIVO**	**CANTIDAD**	**PRECIO UNITARIO APROXIMADO ($)**
Switch Cisco	WS-C3550-24FETH	1	2.995
Switch Cisco	WS-C2950-24	2	795
Switch Cisco	WS-C2950ST-24-LRE	2	750
Switch Cisco	WS-C3550-12G	2	11.990
Router Cisco	7606-S	1	38.000
Switch Cisco	WS-C3750G-24T	1	5.995
Router Cisco	3845	1	13.000
Router Cisco	3745	1	6.480
ALLOT	AC-1010	1	40.000
Servidor DNS	LINUX	1	60.000 [86]
RADIUS	LINUX	1	
Servidor de Correo	LINUX	3	
Servidor WEB	Windows 2000	2	3.500
Servidor WEB	Windows 2003	2	4.100
Servidor WEB	LINUX	1	3.300

Tabla 3.4: Inventario de Equipos Centro de Datos

MEGARED				
NODO	**EQUIPO**	**MODELO**	**CANTIDAD**	**PRECIO UNITARIO APROXIMADO ($)**
FOCH	*Switch* Cisco	WS-C3560-24TS	1	2.995
	Switch Cisco	WS-C2950ST-24-LRE	2	750
LUMBISÍ	*Switch* Cisco	WS-C3560-24TS	1	2.995
	Radio SAF	CFM-22-LM	1	12.500
LIBERTAD	*Switch* Cisco	WS-C2950-24	1	795
	Radio SAF	CFM-22-LM	1	12.500
	Radio Alvarion	BU/RB-B100-5.4	1	3.995
COLON	*Switch* Cisco	WS-C3550-48	1	4.995
	Switch Cisco	WS-C3750G-24TS-1U	1	5.995
SKIROS	*Switch* Cisco	WS-C2950-24	1	795
	Switch Cisco	WS-C2950ST-24-LRE	2	750
AUTOFRANCIA	*Switch* Cisco	WS-C3550-24	1	2.995

[85] Precios cotizados por la Empresa SISTELNET.
[86] Equipos virtualizados en el servidor Blade

	Switch Cisco	WS-C2950ST-24-LRE	2	750
TORREZUL	*Switch* Cisco	WS-C2950ST-24-LRE	2	750
	Switch Cisco	ME-C3750-24TE	1	5.995
	Switch Cisco	WS-C2960-24-S	1	795
	Dslam Zhone	2600	1	1.930
CCNU	*Switch* Cisco	WS-C2950-24	1	795
	Switch Cisco	WS-C3550-24	1	2.995
	Switch Cisco	WS-C2950ST-24-LRE	3	750
CARRETAS	*Switch* Cisco	WS-C2950-24	1	795
AUTOFRANCIA NORTE	*Switch* Cisco	WS-C2950ST-24-LRE	1	750
	Switch Cisco	WS-C2960-24-S	1	795
	Switch Cisco	WS-C3560-24TS	1	2.995
TRAMACO	*Switch* Cisco	WS-C3550-24	1	2.995
	Dslam Zhone	2600	1	1.930
PROVEEDOR IÑAQUITO	*Switch* Cisco	WS-C3750-24TS	1	3.995
GUAMANÍ	*Switch* Cisco	WS-C2950-24	1	795
	Radio Alvarion	BU/RB-B100-5.4	1	3.995

Tabla 3.5: Inventario de Equipos MEGARED

3.3.2.2 Características Técnicas [5]

EQUIPO	DESCRIPCIÓN		
SWITCH	**Marca**	CISCO	
	Modelo	WS-C3560-24TS	
	Puertos	(24) Ethernet 10/100	
		(2) SFP Gigabit Ethernet	1000 BASE-T
			1000 BASE-SX
			1000 BASE-LX
			1000 BASE-ZX
	Velocidad de transmisión máxima	32 Gbps	
	Velocidad basada en paquetes de 64 bytes	6.5 Mpps	
	Memoria flash	32 MB	
	DRAM	128 MB	
	Direcciones MAC	Hasta 12000	
	Potencia máxima	45 W	
	Voltaje AC	100-240 VAC	
	Voltaje DC	+12 V (5 A)	
	Corriente AC	450-190 mA	

	Configuración	Por *web browser*
	Aportes	QoS automático.
		Autonegociación para selección de half o full dúplex.
		Servidor DHCP.
		Spanning Tree rápido.
		Facilita redundancia.
		Se permite autenticación.
		Seguridad para cada puerto.
		Multinivel de seguridades en la consola.
	Protocolos más utilizados	DTP (*Dynamic Trunking Protocol*)
		PagP (*Port Aggregation Protocol*)
		LACP (*Link Aggregation Control Protocol*)
		HSRP (*Hot Standby Router Protocol*)
		RIPv1, 2 (*Routing Internet Protocol*)
		OSPF (*Open Shortest Path First*)
		IGRP (*Interior Gateway Routing Protocol*)
		BGP (*Border Gateway Protocol*)
SWITCH	**Marca**	CISCO
	Modelo	WS-C2950ST-24-LRE
	Puertos	(24) LRE
		(2) 10/100/1000 BASE-T
		(2) SFP
	Velocidad de transmisión máxima	4.7 Gbps
	Velocidad basada en paquetes de 64 bytes	3.5 Mpps
	Memoria flash	8 MB
	SDRAM	32 MB
	Direcciones MAC	Hasta 8000
	Potencia máxima	45 W
	Voltaje AC	100-240 VAC
	Configuración	Por *web browser*
	Aportes	Protección de contraseñas y configuraciones.
		Detección de intrusiones.
		Encriptación.
		Rechaza paquetes en base a direcciones MAC, IP o puertos.
		Multinivel de seguridades en la consola.
		Clasificación de paquetes en base a QoS.
	Protocolos más utilizados	SNMPv3 (*Simple Network Management Protocol*)
		ARP (*Address Resolution Protocol*)
		SSH (*Secure Shell Protocol*)
		DTP (*Dynamic Trunking Protocol*)
SWITCH	**Marca**	CISCO
	Modelo	WS-C2950-24
	Puertos	(24) 10/100 Mbps

	Velocidad De transmisión máxima	13.6 Gbps	
	Velocidad basada en paquetes De 64 bytes	3.6 Mpps	
	Memoria flash	8 MB	
	DRAM	16 MB	
	Direcciones MAC	Hasta 8000	
	Potencia máxima	30 W	
	Voltaje AC	100-240 VAC	
	Voltaje DC	12 V (4.5 A)	
	Configuración	Por *web browser*	
	Aportes	Seguridad mejorada de datos, en base a usuarios o direcciones MAC.	
		Autenticación de usuarios con servidores TACACS o RADIUS, por puertos.	
		Tramas clasificadas según CoS (Calidad del Servicio).	
		Sistemas de detección de intrusiones.	
	Protocolos más utilizados	SNMP (*Simple Network Management Protocol*)	
		IGMP (*Internet Group Management Protocol*)	
		STP (*Spanning Tree Protocol*)	
		PagP (*Port Aggregation Protocol*)	
		TFTP (*Trivial File Transfer Protocol*)	
SWITCH	**Marca**	CISCO	
	Modelo	WS-C3550-24	
	Puertos	(24) 10/100	
		(2) Gigabit Ethernet	1000 BASE-T
			1000 BASE-SX
			1000 BASE-LX/LH
			1000 BASE-ZX
	Velocidad de transmisión máxima	8.8 Gbps	
	Velocidad basada en paquetes de 64 bytes	6.6 Mpps	
	Memoria flash	16 MB	
	DRAM	64 MB	
	Direcciones MAC	Hasta 8000	
	Potencia máxima	65 W	
	Voltaje AC	100-240 VAC	
	Voltaje DC	12 V (8.3 A)	
	Configuración	Por *web browser* y CLI	
	Aportes	Balanceo de carga.	
		Limitador de velocidad.	
		Listas de control de acceso.	
		Identifica flujos de tráfico o grupos de paquetes en base al campo de diferenciación de servicios o a CoS.	
		Facilita la construcción de una red redundante.	
		Altos niveles de seguridad de consola.	

		Facilita la escalabilidad.	
	Protocolos más utilizados	STP (*Spanning Tree Protocol*)	
		RIP (*Routing Information Protocol*)	
		WCCP (*Web Cache Communication Protocol*)	
		OSPF (*Open Shortest Path First*)	
		IGRP (*Interior Gateway Routing Protocol*)	
		BGP (*Border Gateway Protocol*)	
SWITCH	**Marca**	CISCO	
	Modelo	WS-C3550-48	
	Puertos	(48) 10/100	
		(2) Gigabit Ethernet	1000 BASE-T
			1000 BASE-SX
			1000 BASE-LX/LH
			1000 BASE-ZX
	Velocidad de transmisión máxima	13.6 Gbps	
	Velocidad basada en paquetes de 64 bytes	10.1 Mpps	
	Memoria flash	16 MB	
	DRAM	64 MB	
	Direcciones MAC	Hasta 8000	
	Potencia máxima	110 W	
	Voltaje AC	100-240 VAC	
	Voltaje DC	+12 V (13 A)	
	Configuración	Por *web browser* y CLI	
	Aportes	Configuración simultánea de varios *switches*.	
		Limitador de velocidad.	
		Listas de control de acceso.	
		Posibilidad de múltiples aplicaciones a la vez.	
		Identifica flujos de tráfico o grupos de paquetes en base al campo de diferenciación de servicios o a CoS.	
		Facilita la construcción de una red redundante.	
		Altos niveles de seguridad de consola.	
	Protocolos más utilizados	RIP (*Routing Information Protocol*)	
		SMTP (*Simple Mail Transfer Protocol*)	
		IGMP (*Internet Group Management Protocol*)	
		STP (*Spanning Tree Protocol*)	
		OSPF (*Open Shortest Path First*)	
		EIGRP (*Enhanced Interior Gateway Routing Protocol*)	
		SNMP (*Simple Network Management Protocol*)	
		BGP (*Border Gateway Protocol*)	
SWITCH	**Marca**	CISCO	
	Modelo	WS-CE500-24	
	Puertos	(24) conectividad para desktop 10/100	
		(2) servidores o uplink	10
			100
			1000 BASE-T

	Velocidad de transmisión máxima	8.8 Gbps	
	Velocidad basada en paquetes de 64 bytes	6.6 Mpps	
	Memoria flash	16 MB	
	DRAM	32 MB	
	Direcciones MAC	Hasta 8000	
	Potencia máxima	30 W	
	Voltaje AC	100-240 VAC	
	Configuración	Por administrador GUI del dispositivo	
	Aportes	Posibilidad de conectar diferentes dispositivos.	
		Capaz de detectar dispositivos conectados a través de *Cisco Smartports Advisor.*	
		Protege a la red de virus y gusanos a través de NAC.	
		Con *Cisco Troubleshooting Advisor*, se identifica problemas con los cables y de configuración.	
		Minimiza tiempos fuera de servicio.	
	Protocolos más utilizados	SNMP (*Simple Network Management Protocol*)	
		STP (*Spanning Tree Protocol*)	
		IGMP (*Internet Group Management Protocol*)	
		LACP (*Link Aggregation Control Protocol*)	
		VTP (*VLAN Trunking Protocol*)	
SWITCH	**Marca**	CISCO	
	Modelo	ME-C3750-24TE	
	Puertos	(24) 10/100	
		(2) SFP Gigabit Ethernet (2) SFP Servicios Mejorados	1000 BASE-T
			1000 BASE-SX
			1000 BASE-EX
			1000 BASE-LX/LH
			1000 BASE-ZX
			1000 BASE-BX
	Velocidad basada en paquetes de 64 bytes	8.5 Mpps	
	Memoria flash	32 MB	
	DRAM	128 MB	
	Direcciones MAC	Hasta 12000	
	Potencia máxima	110 W	
	Voltaje AC	100-240 VAC	
	Configuración	Por CLI	
	Aportes	Mitiga riesgos mediante TIS (*Cisco Total Implementation Solutions*).	
		Minimiza tiempos fuera de servicio.	
		Permite creación de tablas con direcciones IP, MAC, puertos y VLAN para prevenir acceso de usuarios no deseados.	
		Control avanzado del flujo de tráfico.	
	Protocolos	MPLS (*Multiprotocol Label Switching*)	
		RIP (*Routing Information Protocol*)	

	más utilizados	SNMP (*Simple Network Management Protocol*)
		REP (*Resilient Ethernet Protocol*)
		EIGRP (*Enhanced Interior Gateway Routing Protocol*)
		OSPF (*Open Shortest Path First*)
		BGP (*Border Gateway Protocol*)
SWITCH	**Marca**	CISCO
	Modelo	WS-C2960-24-S
	Puertos	(24) Ehernet 10/100
	Velocidad de transmisión máxima	16 Gbps
	Velocidad basada en paquetes de 64 bytes	3.6 Mpps
	Memoria flash	32 MB
	DRAM	64 MB
	Direcciones MAC	Hasta 8000
	Potencia máxima	30 W
	Voltaje AC	100-240 VAC
	Configuración	Por *web browser*
	Aportes	Facilita migración de *hubs* no inteligentes o *switches* no administrables a una red totalmente administrable.
		Permite conexión de cobre o fibra para Gigabit Ethernet.
		Administración escalable y segura de la red.
		Control de admisión basada en usuarios, puertos y direcciones MAC.
		Calidad de servicio QoS
		Autoconfiguración, usando puertos inteligentes.
	Protocolos más utilizados	STP (*Spanning Tree Protocol*)
		BDPU (*Bridge Protocol Data Unit*)
		DTP (*Dynamic Trunking Protocol*)
		PagP (*Port Aggregation Protocol*)
		LACP (*Link Aggregation Control Protocol*)
		TFTP (*Trivial File Transfer Protocol*)
		NTP (*Network Timing Protocol*)
SWITCH	**Marca**	CISCO
	Modelo	WS-C3750G-24TS-1U
	Puertos	(24) Ethernet 10/100/1000
		(4) SFP Gigabit Ethernet
	Velocidad de transmisión máxima	32 Gbps
	Velocidad basada en paquetes de 64 bytes	38.7 Mpps
	Memoria flash	32 MB
	DRAM	128 MB
	Direcciones MAC	Hasta 12000
	Potencia máxima	94 W

	Voltaje AC	100-240 VAC
	Configuración	Por *web browser* y CLI
	Aportes	Flexibilidad en la configuración.
		Disponible con *Cross-stack*, que permite contar con QoS, limitación de velocidad, listad de control de acceso; mediante el IP *Base Image*.
		Stackwise permite realizar cambios o eliminaciones sin interrupción del servicio.
		EnergyWise permite el ahorro en el consumo de energía.
		SSH, Kerberos y SNMPv3, proveen seguridad, mediante encriptación del tráfico.
		ARP Dinámico asegura la integridad de los usuarios, previniendo que usuarios no deseados exploten la inseguridad natural del protocolo ARP.
	Protocolos más utilizados	VTP (*VLAN Trunking Protocol*)
		TFTP (*Trivial File Transfer Protocol*)
		NTP (*Network Timing Protocol*)
		STP (*Spanning Tree Protocol*)
		RIP (*Routing Information Protocol*)
		DHCP (*Dynamic Host Configuration Protocol*)
		DTP (*Dynamic Trunking Protocol*)
		PagP (*Port Aggregation Protocol*)
		LACP (*Link Aggregation Control Protocol*)
		IGRP (*Interior Gateway Routing Protocol*)
		BGP (*Border Gateway Protocol*)
		ARP (*Address Resolution Protocol*)
SWITCH	**Marca**	CISCO
	Modelo	WS-C3750-24TS
	Puertos	(24) Ethernet 10/100/1000
		(4) SFP Gigabit Ethernet
	Velocidad de transmisión máxima	32 Gbps
	Velocidad basada en paquetes de 64 bytes	38.7 Mpps
	Memoria flash	16 MB
	DRAM	128 MB
	Direcciones MAC	Hasta 12000
	Potencia máxima	94 W
	Voltaje AC	100-240 VAC
	Configuración	Por *web browser* y CLI
	Aportes	Flexibilidad en la configuración.
		Disponible con *Cross-stack*, que permite contar con QoS, limitación de velocidad, listas de control de acceso.
		Stackwise permite realizar cambios o eliminaciones sin interrupción del servicio.
		EnergyWise permite el ahorro en el consumo de energía.
		SSH, Kerberos y SNMPv3, proveen seguridad,

		mediante encriptación del tráfico.
		ARP Dinámico asegura la integridad de los usuarios, previniendo que usuarios no deseados exploten la inseguridad natural del protocolo ARP.
	Protocolos más utilizados	VTP (*VLAN Trunking Protocol*)
		TFTP (*Trivial File Transfer Protocol*)
		NTP (*Network Timing Protocol*)
		STP (*Spanning Tree Protocol*)
		RIP (*Routing Information Protocol*)
		DHCP (*Dynamic Host Configuration Protocol*)
		DTP (*Dynamic Trunking Protocol*)
		PagP (*Port Aggregation Protocol*)
		LACP (*Link Aggregation Control Protocol*)
		IGRP (*Interior Gateway Routing Protocol*)
		BGP (*Border Gateway Protocol*)
		ARP (*Address Resolution Protocol*)
SWITCH	**Marca**	CISCO
	Modelo	WS-C3550-12G
	Puertos	(10) 1000 BaseX
		(2) 10/100/1000 BaseT
	Velocidad de transmisión máxima	24 Gbps
	Velocidad basada en paquetes de 64 bytes	17 Mpps
	Memoria flash	16 MB
	DRAM	64 MB
	Direcciones MAC	Hasta 12000
	Potencia máxima	190 W
	Voltaje AC	100-240 VAC
	Configuración	Por *web browser* y CLI
	Aportes	*Weighted Round Robin* asegura la administración para priorización del flujo de paquetes.
		Limitador de velocidad.
		Switch Database Manager maneja acceso, enrutamiento y escenarios para VLAN.
		Embedded Remote Monitoring (RMON) provee de 4 grupos: historia, estadísticas, alarmas y eventos.
	Protocolos más utilizados	SNMP (*Simple Network Management Protocol*)
		TFTP (*Trivial File Transfer Protocol*)
		NTP (*Network Timing Protocol*)
		STP (*Spanning Tree Protocol*)
		VTP (*VLAN Trunking Protocol*)
		BGP (*Border Gateway Protocol*)
		IGRP (*Interior Gateway Routing Protocol*)
		BGP (*Border Gateway Protocol*)
		RIP (*Routing Information Protocol*)
		BPDU (*Bridge Protocol Data Unit*)

		ARP (*Address Resolution Protocol*)
SWITCH	**Marca**	CISCO
	Modelo	WS-C3750G-24T
	Puertos	(24) 10/100/1000
		(4) SFP Gigabit Ethernet
	Velocidad de transmisión máxima	32 Gbps
	Velocidad basada en paquetes de 64 bytes	35.7 Mpps
	Memoria flash	16 MB
	DRAM	128 MB
	Direcciones MAC	Hasta 12000
	Potencia máxima	98 W
	Voltaje AC	100-240 VAC
	Configuración	Por *web browser* y CLI
	Aportes	Mitiga riesgos mediante TIS (*Cisco Total Implementation Solutions*).
		Minimiza tiempos fuera de servicio.
		Permite creación de tablas con direcciones IP, MAC, puertos y VLAN para prevenir acceso de usuarios no deseados.
		Control avanzado del flujo de tráfico.
	Protocolos más utilizados	VTP (*VLAN Trunking Protocol*)
		TFTP (*Trivial File Transfer Protocol*)
		NTP (*Network Timing Protocol*)
		STP (*Spanning Tree Protocol*)
		RIP (*Routing Information Protocol*)
		DHCP (*Dynamic Host Configuration Protocol*)
		DTP (*Dynamic Trunking Protocol*)
SWITCH	**Marca**	CISCO
	Modelo	SW3550 24FETH
	Puertos	(10) 1000 BaseX
		(2) 10/100/1000 BaseT
	Velocidad de transmisión máxima	24 Gbps
	Velocidad basada en paquetes de 64 bytes	17 Mpps
	Memoria flash	16 MB
	DRAM	64 MB
	Direcciones MAC	Hasta 12000
	Potencia máxima	190 W
	Voltaje AC	100-240 VAC
	Configuración	Por *web browser* y CLI
	Aportes	*Weighted Round Robin* asegura la administración para priorización del flujo de paquetes.
		Limitador de velocidad.
		Switch Database Manager maneja acceso, enrutamiento y escenarios para VLAN.

		Embedded Remote Monitoring (RMON) provee de 4 grupos: historia, estadísticas, alarmas y eventos.
	Protocolos más utilizados	SNMP (*Simple Network Management Protocol*)
		TFTP (*Trivial File Transfer Protocol*)
		NTP (*Network Timing Protocol*)
		STP (*Spanning Tree Protocol*)
		VTP (*VLAN Trunking Protocol*)
		BGP (*Border Gateway Protocol*)
		IGRP (*Interior Gateway Routing Protocol*)
		BGP (*Border Gateway Protocol*)
		RIP (*Routing Information Protocol*)
		BPDU (*Bridge Protocol Data Unit*)
		ARP (*Address Resolution Protocol*)
DISPOSITIVO ADMINISTRADOR	**Marca**	Allot
	Modelo	NetEnforcer AC-1010
	Suscritos	Hasta 100000
	Velocidad de transmisión máxima	2 Gbps
	Interfaz de administración	10 / 100 BASE-T
	Interfaces de red	(2) 1000 BASE-T/SX/LX
	Puerto de consola	Serial, Conector RJ45
	Voltaje	100-240 VAC; -48 VDC
	Configuración	
	Aportes	Administra tráfico de Internet sobre enlaces Ethernet de alta velocidad, de hasta 2 Gbps.
		Inspección profunda de paquetes con políticas de QoS.
		Monitoreo y control del uso de la red.
	Protocolos más utilizados	BitTorrent
		Gnutella
		Ares
		EDonkey
		Warez
		Skype
		H.323
		SIP (*Session Initiation Protocol*)
		RTP (*Real-Time Transport Protocol*)
ROUTER	**Marca**	CISCO
	Modelo	7606-S
	Slots	6 por chasis
	Throughput	480 Gbps
	Voltaje	208 a 240 VAC
		- 48 a – 60 VDC
	Aportes	Soporta aplicaciones de voz, video y datos.
		Opciones para procesos de ruta redundantes y energía.
		Módulos de servicios Ethernet de alta densidad: 10/100 Mbps, Gigabit Ethernet y 10 Gigabit Ethernet.

		Módulos de servicios: Ipsec, firewall, detección de intrusión, análisis de red.
	Protocolos	MPLS (*Multiprotocol Label Switching*)
DSLAM	**Marca**	ZHONE
	Modelo	2600
	Voltaje	90 a 265 VAC
	Aportes	Provee funciones para entregar aplicaciones de video IP, voz IP y datos HSIA simultáneamente.
		Soporta servicios triple-play.
	Protocolos	IGMPv2 (*Internet Group Management Protocol* versión 2) SNMP (*Simple Network Management Protocol*)
SISTEMA DE RADIO	**Marca**	SAF
	Modelo	CFM-22-LM
	Frecuencia de Operación	22 – 23.6 GHz
	Velocidad de transmisión	8, 16, 34 Mbps (dependiendo de la configuración del IDU[87]).
	Componentes	Unidad interior (IDU)
		Unidad exterior (ODU) [87]
	Conexión IDU – ODU	Cable coaxial de 50 Ω.
	Aportes	Satisface requerimientos de velocidades altas (superiores a 2 Mbps). Monitoreo del desempeño del radio. Pruebas de *loopback*[88]. Parámetros de IDU y ODU controlados por software.
	Tecnología utilizada	Modulación: 4FSK
SISTEMA DE RADIO	**Marca**	ALVARION
	Modelo	BU/RB-B100-5.4
	Frecuencia de Operación	5.4 GHz
	Velocidad de transmisión	108 Mbps
	Componentes	Unidad interior (IDU)
		Unidad exterior (ODU)
	Conexión IDU – ODU	Cable en banda base.
	Aportes	Alternativa para proveer conectividad remota. Provee gran capacidad, conectividad punto a punto de alta velocidad. Opera en banda de frecuencia no licenciada. No es necesaria línea de vista. Soporta VLANs, permitiendo operación secura y servicios VPN.
	Tecnología utilizada	Modo: *Time Division Duplex* (TDD) Modulación: *Orthogonal Frequency Division*

[87] La unidad interior (IDU) es el módulo interno de un sistema de radio. La IDU es el componente mandatario del sistema radial de microonda, se encarga de la interconexión de la unidad exterior (ODU) con el equipo de usuario, administración local y remota y de proveer voltaje a la ODU; mientras que la parte externa está formada por la (ODU) y la antena, encargándose de transmitir y recibir señales de radio.

[88] Prueba en la que las señales se envían y luego se dirigen de vuelta al origen a lo largo de la ruta de comunicaciones; se utilizan para probar la disponibilidad de la interfaz de red.

		Multiplexing (OFDM) con *Forward Error Correction* (FEC)
SERVIDOR DNS	**Nombre del modelo**	Intel(R) Xeon(R) CPU E5506 @ 2.13GHz
	Caché	4096 KB
	Memoria RAM	1035,244 MB
	Disco duro	17201 MB
SERVIDOR RADIUS	**Nombre del modelo**	Intel(R) Xeon(R) CPU E5506 @ 2.13GHz
	Caché	4096 KB
	Memoria RAM	1035,244 MB
	Disco duro	17201 MB
SERVIDOR DE CORREO 1	**Nombre del modelo**	Intel(R) Xeon(R) CPU E5520 @ 2.27GHz
	Caché	8,192 MB
	Memoria RAM	1035,244 MB
	Disco duro	46799 MB
SERVIDOR DE CORREO 2	**Nombre del modelo**	Intel(R) Xeon(R) CPU E5520 @ 2.27GHz
	Caché	8,192 MB
	Memoria RAM	1035,244 MB
	Disco duro	37801 MB
SERVIDOR DE CORREO 3	**Nombre del modelo**	Intel(R) Xeon(R) CPU E5506 @ 2.13GHz
	Caché	4,096 MB
	Memoria RAM	1035,244 MB
	Disco duro	37801 MB
SERVIDOR WEB LINUX	**Nombre del modelo**	Intel(R) Core(TM)2 Duo CPU E4600 @ 2.40GHz
	Caché	2,048 MB
	Memoria RAM	1932,416 MB
	Disco duro	210043 MB

Tabla 3.6: Características Técnicas de equipos

3.4 INCIDENTES DE SEGURIDAD DETECTADOS

A continuación se presentan algunos de los incidentes que han afectado la Seguridad de la Información de la Empresa:

- Desconfiguracion involuntaria de los equipos por parte de personal en inducción[89], dejando sin operación a varios clientes.

- Desconexión de equipos alojados en el Centro de Datos y nodos por parte del personal de Operaciones.

- Desconexión de todos los equipos de un *rack* de la toma eléctrica, debido a fallo humano al manipular los fusibles del UPS.

- Falla en el funcionamiento del equipo de borde, debido al incremento del procesamiento del mismo, afectando a la totalidad de los clientes.

- Acceso de un *hacker* a uno de los servidores web, eliminando todos los archivos *index* de las páginas web allí alojadas.

- Modificaciones en la configuración de los equipos por parte de personal que ha dejado sus funciones en la empresa, afectando el servicio a ciertos clientes.

- Acceso a la configuración de los equipos desde cualquier sitio, incluso desde redes que no pertenecen a la empresa.

- Robo de los equipos del nodo Libertad, debido a la mala calidad de los candados.

- Falla de los UPS de los nodos Colón y Lumbisí cuando no existía servicio eléctrico, afectando el servicio de varios clientes.

- Quema de equipos en el nodo Autofrancia, debido a filtraciones de agua.

- Indisponibilidad del servicio, debido a corte o falla en el medio de transmisión de los nodos que no cuentan con enlaces de *backup.*

[89] Personal en inducción hace referencia a trabajadores que laboran pocos días en la empresa y que no cuentan con el suficiente conocimiento para realizar cambios.

- Interfencia de frecuencias en las últimas millas de clientes radiales, debido a saturación del espectro en bandas no licenciadas.

3.5 SEGURIDAD DE LA INFORMACIÓN IMPLEMENTADA ACTUALMENTE EN LA EMPRESA

3.5.1 POLÍTICA DE SEGURIDAD

La empresa actualmente no cuenta con un documento que registre las políticas de seguridad a ser cumplidas por los empleados o entidades externas. Se dispone únicamente de ciertos lineamientos, que han sido dados a conocer verbalmente por parte de la Gerencia del área de Operaciones, en los cuales se determina ciertas medidas de seguridad referentes a permisos de ingresos, acciones a ser tomadas en caso de desastres naturales, etc.

3.5.2 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La empresa no dispone de un departamento dedicado específicamente a la seguridad de la información. No se han designado responsabilidades referentes al tema a ningún miembro del área; sin embargo si alguna persona detecta alguna actividad que pueda afectar la seguridad de la información, es libre de tomar acciones al respecto o informar al jefe del área respectiva.

Únicamente se ha estipulado que cada uno de los miembros de la empresa debe firmar un acuerdo de confidencialidad, en el cual se especifica que no se deberá divulgar información sensible de la empresa a entidades externas. Este acuerdo es renovado cada año, tiene una vigencia de 5 años después de la salida del empleado de la empresa y el Gerente de la empresa es la persona responsable de aprobar este documento.

De igual manera, cuando han existido cambios significativos en cuanto a seguridad, por ejemplo, cambio de claves para equipos de *backbone* o cambio de

llaves para el acceso a los nodos, se notifica formalmente mediante un correo electrónico a todo el personal del Departamento de Operaciones. Sin embargo estas actividades no son revisadas a períodos regulares o planeados.

Para entidades externas tampoco se dispone de un procedimiento de control específico.

En el caso de proveedores, se ha dado libre acceso hacia los equipos físicos ubicados en el centro de datos o en los nodos, sin requerir de un control adicional o supervisión de personal de la Empresa.

Para el caso de clientes, que disponen de equipos ubicados en el Centro de Datos, el acceso exige la presentación de la credencial y la supervisión de una persona de la empresa que verifique que los trabajos y manipulación de información sea únicamente sobre los equipos que les pertenece.

De manera general los clientes no tienen acceso a la información de la empresa, únicamente a la de sus enlaces, sin tener la opción de manipularla.

3.5.3 GESTIÓN DE ACTIVOS

La empresa cuenta con el inventario respectivo de todos los activos que permiten brindar servicio en la ciudad de Quito. Se posee una base de datos, en la cual constan los números seriales y etiquetas contables[90] de los equipos que se encuentran en los nodos, instalados donde los clientes, y los almacenados en bodega.

Se tienen además identificados los propietarios de cada uno de los activos de la empresa; sin embargo esto no se encuentra documentado.

En el caso de equipos de *backbone,* el propietario que vela por su seguridad física es el Administrador de Red Física y Regulaciones; mientras que la administración

[90] Un equipo posee una etiqueta contable cuando su valor supera los 100 dólares.

de la información que contienen los equipos de *backbone* tiene dos “propietarios”. Uno de los administradores de Ingeniería, el cual es responsable de los equipos pertenecientes a la red alámbrica, mientras que el otro administrador de Ingeniería tiene a cargo los equipos correspondientes a la red inalámbrica. Adicionalmente el “propietario” de los servidores (tanto de clientes como de la empresa) es el Coordinador Nacional de Sistemas.

La clasificación de la información no está definida. Para esta clasificación se debería considerar el valor, confidencialidad y grado crítico para la organización de la información.

3.5.4 SEGURIDAD DE LOS RECURSOS HUMANOS

En este punto, el Departamento de Operaciones se apoya en el área de Recursos Humanos. Antes de que un empleado sea contratado, se solicitan documentos que certifiquen la integridad de la persona, tales como record policial, certificados de honorabilidad y cartas de recomendación. Los antecedentes de la persona son verificados y evaluados, con el fin de determinar si cumple el perfil solicitado.

La persona que ingresa a la empresa debe aceptar las condiciones contractuales y firmar el acuerdo de confidencialidad.

Una vez que el empleado se integra a sus actividades, el Jefe de cada área está en la obligación de indicarle cuáles son sus responsabilidades en cuanto a la seguridad de la información.

Una vez que el empleado haya culminado su contrato o a su vez haya sido retirado de sus funciones, está en la obligación de entregar todos los activos que manejaba. Adicionalmente la empresa retira todos los derechos de ingreso y permisos para la manipulación de la información.

3.5.5 SEGURIDAD FÍSICA Y AMBIENTAL

El Departamento de Operaciones tiene un piso independiente en el edificio, el cual cuenta con una puerta de ingreso controlada mediante una tarjeta magnética, la cual dispone únicamente el personal de la empresa. Adicionalmente existe una recepcionista que permite el ingreso de proveedores o clientes al lugar, previa verificación de su identidad.

El Centro de Datos, ubicado dentro del departamento de Operaciones, también tiene control de acceso del personal mediante tarjeta magnética. Estas tarjetas poseen únicamente el Jefe Regional NOC R1, el Jefe de Implementación y Gestión de Red R1, el Coordinador Nacional de Sistemas, los dos Administradores de Ingeniería, una tarjeta para toda el área de Soporte y otra para toda el área de Instalaciones. El ingreso a este lugar debe ser registrado en una hoja, en la cual se indicará la hora de entrada, la hora de salida, el trabajo realizado y la firma de la persona.

Para el acceso a los nodos se requiere una llave, pues éstos se encuentran cerrados con cadena y candado. Existen dos copias de las llaves de cada nodo, las cuales son administradas por uno de los ingenieros de soporte y por el Administrador de Red Física y Regulaciones. Cada uno de ellos lleva un registro de qué llaves han sido solicitadas, el día de entrega, día de recepción y la firma.

A nivel de seguridad física, cada uno de los puntos cuenta con un sistema de ventilación, respaldo de energía y sistema contra incendio.

Dentro de cada nodo, el cableado tanto de energía como de telecomunicaciones se encuentra protegido contra daño o intercepciones. Sin embargo el cableado que permite la interconexión de los nodos o que corresponden a últimas millas de clientes es vulnerable a daños, cortes accidentales o provocados, robos, etc., pues éste se encuentra tendido en la calle (postes) y no es posible ningún tipo de protección.

Todo equipo que sea retirado o que haya sido dado de baja es registrado y almacenado en bodega. Estos equipos son sacados previa autorización del propietario del equipo.

3.5.6 GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES

La empresa no cuenta con documentos que registren los procedimientos de operación de la información que deben llevarse a cabo. Únicamente cuando se realiza un cambio significativo, éste es notificado al jefe del área respectiva y él decidirá si es necesario comunicar o no a todo el personal de Operaciones.

Cuando planificadamente se va a realizar un cambio, como por ejemplo incorporar un equipo nuevo o retirar alguno, esto es notificado formalmente mediante un correo electrónico al personal del Departamento y a los clientes que han de ser afectados por dicho cambio.

En cuanto a la gestión de la entrega del servicio de terceros, se realiza un continuo monitoreo del mismo. El Departamento de Operaciones cuenta con personal que realiza el monitoreo de todos los enlaces a nivel de *backbone* y de clientes, el cual permite determinar si se ha visto interrumpido o presenta inconvenientes el servicio. Mediante este procedimiento se verifica si el daño es generado del lado de la empresa o del servicio brindado por el tercero.

El sistema que maneja el Departamento de Operaciones para la prestación de servicios, ha sido dimensionado correctamente con el fin de minimizar el riesgo de fallas. El ancho de banda total, tendido de últimas millas, capacidad de equipos, espacio físico, etc. han sido diseñados con proyección a crecimiento futuro.

Actualmente la empresa cuenta con un ancho de banda de 400 MHz, los cuales están utilizados en un 95% aproximadamente. Se ha previsto el crecimiento de la empresa, por lo que se tiene disponibilidad inmediata de incrementar este valor, en caso de que se lo requiera.

En cuanto a la capacidad física de los nodos, se dispone de unidades libres en los *racks* e inclusive espacio disponible para *racks* nuevos; por lo que se reservó espacio en caso de requerir la instalación de un equipo adicional.

En cuanto a la protección contra códigos maliciosos, de manera general la red no restringe el flujo de información hacia los clientes, pues se les otorga libertad para la navegación por Internet; solo se generan restricciones cuando un cliente solicita una configuración específica. Únicamente se protege contra códigos maliciosos a los servidores que se encuentran tras el *firewall*, como se presentó en la Figura 3.3, debido a que éstos manejan información sensible de la empresa y de los clientes.

Toda la información de la configuración de los equipos se encuentra respaldada por parte de los Administradores de Ingeniería, de modo que si un equipo falla pueda ser reemplazado y cargado con la configuración, disminuyendo así el tiempo de indisponibilidad. Adicionalmente, se cuenta con rutas de *backup* en los nodos principales[91], las cuales son habilitadas provisionalmente hasta la reparación del enlace principal.

En cuanto a la protección de la seguridad en redes e infraestructura de soporte, no se dispone de equipos (a excepción del *firewall*) ni software que permitan brindar seguridad; tan solo se cuenta con ciertos controles básicos que bloquean el acceso a posibles atacantes, por ejemplo a nivel de autenticación, que será tratado más adelante.

No existe una gestión establecida de los medios removibles. Se utilizan discos, memorias de almacenamiento y medios impresos en base al criterio del personal.

No se dispone de un sistema de monitoreo que detecte actividades de procesamiento de la información no autorizadas. Únicamente se cuenta con los controles de acceso al Centro de Datos y a los nodos, como se explicó anteriormente.

[91] Se consideran nodos principales a aquellos cuya falla involucraría indisponibilidad de un gran número de clientes.

En caso de existir alguna violación de la seguridad que afecta a la información disponible en algún equipo de la empresa, se toman las acciones correctivas necesarias para solventar el incidente; no se documentan estos eventos.

3.5.7 CONTROL DE ACCESO

La empresa cuenta con una política de control de acceso a la información, que es de conocimiento de todos los empleados; sin embargo, ocasionalmente no se realizan ciertas acciones en base a ésta, pues no se encuentra documentada y además no es sometida a revisión con regularidad.

En cuanto a la gestión del acceso, el Departamento de Sistemas conserva un listado de los usuarios que requieren ingresar a las diferentes aplicaciones y los privilegios que tienen. Las claves asignadas para ello son exclusivas para cada empleado. Esto es revisado mensualmente y modificado en caso de ser requerido, por ejemplo cuando un empleado abandona sus funciones dentro de la empresa.

Cada asesor del Departamento de Operaciones, tiene acceso a las claves que le permiten ingresar y gestionar los equipos de *backbone* para la entrega de servicios a los clientes. Adicionalmente, se cuenta con privilegios especiales de acuerdo al área a la cual pertenece el asesor. Estas claves y privilegios son otorgados por uno de los Administradores de Ingeniería, quien las modifica cuando lo considera conveniente.

Para el caso de la administración de servidores, las claves y privilegios son otorgadas por el Coordinador Nacional de Sistemas.

Para el control de acceso al sistema de operación, se utilizan contraseñas compartidas por los usuarios autorizados. No se manejan identificadores singulares de uso personal y exclusivo.

De forma general, las contraseñas utilizadas para el control de acceso son consideradas seguras, pues incluyen caracteres alfanuméricos y especiales. Sin embargo no existe un proceso formal, ni la protección necesaria para conservar dichas claves.

Para el caso de los clientes que disponen de un *router* de la empresa en sus instalaciones, éste se configura con una clave que es general para todos, la cual no es modificada ni conocida por el cliente.

En cuanto a las contraseñas de clientes, correspondientes a conexiones *dial-up* y cuentas de correo, son asignadas inicialmente por la empresa, pero pueden ser modificadas si el cliente lo solicita; de modo que en su mayoría no son contraseñas seguras, sino fáciles de recordar para el cliente.

Se dispone de políticas de confidencialidad, en cuanto a la revelación de contraseñas de las cuentas de correo de los clientes. En caso de que un cliente solicite su contraseña, se debe comprobar la autenticidad del mismo, solicitándole su cédula de identidad o RUC, dirección del domicilio u otro dato. Para los clientes con cuentas *dial-up*, se registra en el sistema[92] cada ingreso, con el nombre de usuario y contraseña digitados.

No se observan acciones adecuadas para proteger los equipos desatendidos; en su mayoría, la única protección con que cuentan los equipos es la contraseña de inicio de sesión y el temporizador de inactividad.

Para identificar un equipo en la red, se maneja direcciones IPs y nombres de equipo. La segregación de la red se basa únicamente en las claves de ingreso a los equipos y para el caso del concentrador, adicional a la clave, se habilita un puerto distinto a *telnet.*

Para proteger los medios de computación y comunicación móviles, se cuenta con una política que establece la obligatoriedad de registro de equipo en caso de

[92] El sistema para la autentificación de los clientes dial-up es el servidor Radius.

sacarlo de la empresa y el momento de su devolución; dicho registro incluye al equipo en mención, usuario, fecha de salida y de retorno, motivo y firmas del usuario y del asesor tecnológico responsable del equipo. Para el caso de medios de comunicación móviles, se establece la responsabilidad por calendario de forma rotativa, entre los técnicos del departamento.

3.5.8 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE LA INFORMACIÓN

No se ha realizado el análisis necesario con respecto a los requerimientos de seguridad de los sistemas; sin embargo, este análisis se lo realizará en el presente Proyecto de Titulación, durante la evaluación de riesgos.

Con respecto al procesamiento correcto en las aplicaciones, se revisa regularmente los servidores de correo y web.

Los procedimientos para el control de cambios, no se encuentran definidos formalmente; cada vez que es necesario un cambio, se determinan al momento los procedimientos que se deben llevar a cabo para ese cambio en particular. Tras cambios en los sistemas operativos, se revisan y prueban las aplicaciones críticas; además, todo cambio se controla de manera estricta, pese a no contar con una política formal.

El control que se maneja en el caso de vulnerabilidades técnicas, es el uso de redes de *backup* o respaldo, en caso de disponerlas.

3.5.9 GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

Generalmente, los reportes de eventos en la seguridad de la información son reportados a nivel del Departamento de Operaciones. Cualquier integrante del Departamento, al observar o sospechar de alguna debilidad, lo reporta al jefe del área respectiva, el cual tomará acciones en caso de que las considere necesarias.

Con el fin de asegurar la disponibilidad de información, la empresa cuenta con un sistema de monitoreo de los equipos de *backbone* y enlaces de clientes, en el cual se registran los eventos ocurridos y el tiempo fuera de servicio. A pesar de ello no se dispone de un archivo, en base al cual sea posible ejecutar acciones correctivas para evitar posibles reincidencias.

3.5.10 GESTIÓN DE LA CONTINUIDAD COMERCIAL

Para garantizar la continuidad del negocio, en caso de presentarse un incidente, para la mayoría de sus redes la empresa cuenta con *backups* que permiten que la suspensión del servicio sea imperceptible para los clientes; y en casos donde no se cuenta con *backups*, se gestiona la solución del incidente de modo inmediato. No se cuenta con planes diseñados ante incidentes; el área de Operaciones toma las acciones pertinentes cuando se presenta un incidente en particular.

3.5.11 CUMPLIMIENTO

La empresa define, documenta y actualiza los requerimientos estatutarios, reguladores y contractuales de manera general, más no para cada sistema de información. Los registros importantes de la empresa, así como la información personal se encuentran protegidos de pérdida y destrucción; sin embargo, resultaría conveniente incrementar las medidas al respecto.

Dado que la empresa no cuenta con una política de seguridad de la información, la gerencia de cada área no puede verificar su cumplimiento; sin embargo, una vez que se implemente la política, cada gerencia se encargará de hacerlo. Pese a no contar con tal política aún, se chequean regularmente los sistemas de información para garantizar su adecuado funcionamiento.

Previo a auditorías de recertificación de la Norma ISO 9001, la empresa se asegura de contar con todos los registros e información necesarios, así como de que todos los procedimientos de los sistemas de información se estén ejecutando adecuadamente.

CAPÍTULO 4

PROPUESTA DEL DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA MEGADATOS S.A.

4.1 REQUERIMIENTOS Y EXPECTATIVAS DE SEGURIDAD DE LA INFORMACIÓN DE MEGADATOS S.A.

Los requerimientos de seguridad de la empresa son:

- "Documentación de política": Se requiere que todo lineamiento sobre seguridad de la información, se especifique en una política o normativa que debe ser revisada periódicamente y mejorada en caso de ser necesario. Dicha política debe satisfacer a los requerimientos de seguridad de la Empresa y debe ser cumplida a cabalidad.

- "Apoyo de la Gerencia": Todo hecho relacionado con la Seguridad de la Información, debe ser de conocimiento de la Gerencia del Departamento de Operaciones, la que se compromete a apoyar al desarrollo y cumplimiento del SGSI.

- "Coordinación y participación": Todos los integrantes del Departamento de Operaciones deben ser informados sobre sus responsabilidades y participar en el desarrollo del SGSI, garantizando el cumplimiento del mismo.

- "Uso autorizado de hardware y software": Se requieren directrices para la utilización autorizada de hardware y software; no se debe permitir el uso deliberado de éstos, pues podrían afectar en la entrega normal de los servicios.

- “Compromiso del personal”: Se precisa contar con el compromiso del personal en resguardar la seguridad de la información, concerniente a la entrega de los servicios; esto implica su confidencialidad, integridad y seguridad, aún cuando ya no pertenezca a la Empresa.

- “Formación en Seguridad de la Información”: Se requiere contar con un personal instruido en Seguridad de la información, que esté actualizado sobre posibles amenazas y que se encuentre capacitado para desarrollar sus responsabilidades.

- “Revisión periódica de cumplimiento”: El funcionamiento del SGSI debe ser revisado continuamente, así como todos los procedimientos que garantizan la seguridad de la información en la entrega de los servicios. Dicha revisión podría ser llevada a cabo a nivel de auditoría, en cuyo caso se requiere la seguridad apropiada.

- “Medidas con entidades externas”: La detección de amenazas, debe también incluir a aquellas que podrían ser generadas por la interacción de actividades laborales con entidades externas para proveer los servicios; ante esta situación, es necesario proteger la seguridad de la información que pudiera ser compartida con dichas entidades.

- “Privilegios de acceso”: Los privilegios de acceso físico y lógico deben ser establecidos adecuadamente, de manera segura y deben ser revisados con regularidad.

- “Seguridad de los activos de información”: Los activos de información utilizados para proveer los servicios, deben ser organizados y resguardados física y lógicamente, atribuyéndolos un responsable y evitando amenazas humanas, tecnológicas y ambientales. Además, se debe establecer el uso adecuado de los mismos.

- “Proceso disciplinario”: En caso de poner en peligro la seguridad de la información, se deberá sancionar al infractor con lo estipulado en una política de proceso disciplinario.

- “Documentación y registro de eventos”: Documentación adecuada y registro seguro de todos los procedimientos de operación, así como de cualquier eventualidad de la seguridad de la información y de los sistemas.

- “Procedimientos”: Elaboración de lineamientos sobre los procedimientos para realizar cambios, utilizar la información, manejo de mensajes electrónicos

- “Aislamiento de aplicaciones”: Es indispensable separar o aislar aplicaciones, cuyo mal manejo pudiera afectar en el funcionamiento normal de otras.

- “Diseño adecuado de los sistemas de información”: No se pueden presentar fallas por un diseño mal realizado o mal planificado, ni por un procesamiento incorrecto de las aplicaciones; éste debe ser revisado continuamente y corregido en caso de ser necesario.

- “Prevención de ataques”: Se requieren controles que permitan detectar y eliminar amenazas provenientes de la red, como virus, gusanos, troyanos, ataque de diccionario, negación del servicio, entre otros.

- “Respaldo de la información”: Respaldo seguro de toda la información utilizada para proveer los servicios, tanto de configuración como de usuarios.

- “Planes para la continuidad”: Establecer planes para la continuidad, en caso de presentarse algún incidente de la seguridad de la información asociada a la entrega de los servicios, considerando tiempos de solución mínimos y soluciones óptimas.

- “Cumplimiento con legislación”: Todos los controles aplicados deberán ir acorde con el cumplimiento de los requerimientos legales; bajo ningún

concepto se deberá generar conflicto entre los controles para el desarrollo del SGSI y los requerimientos legales que la Empresa debe cumplir.

- "Concordancia entre ISO 9001 e ISO 27000": El marco referencial del Sistema de Gestión de Seguridad de la información, basado en las Normas ISO 27001 e ISO 27002, debe guardar relación y correspondencia con la Norma ISO 9001, que actualmente se encuentra implementada en la empresa. Los contenidos del SGSI y de la Gestión de Calidad, deben ser acordes y en lo posible complementarios.

- "Análisis económico": La aplicación de controles para garantizar la seguridad de la información, debe considerar un análisis económico, de tal forma que las inversiones no superen el valor de los activos protegidos.

Las expectativas de seguridad de la empresa son:

- Si ocurriera una violación en la seguridad de la información, por parte de algún empleado de la empresa o terceros, se debería contar con la capacidad tecnológica de detectar al responsable.

- Si se presentara una falla en la prestación de servicios, que imposibilite su entrega, se debería disponer de *backups*, de modo que el tiempo de indisponibilidad sea prácticamente imperceptible para los clientes.

- En caso de que ocurriera la pérdida o robo de información, sea impresa o electrónica, se debería contar con información de respaldo que sirva como sustento.

- Si se presentaran ataques externos a las redes encargadas de proporcionar servicios, se debería contar con el personal que detecte dichos ataques, su procedencia y los mitigue mediante controles adecuados. Lo óptimo sería detectar las vulnerabilidades que podrían ser aprovechadas por las amenazas y disminuirlas para evitar posibles ataques.

- Si alguno de los equipos que permiten la entrega de los servicios, sufriera daño o robo, se debería contar con el respaldo de configuración del mismo, tal que sea factible una reconfiguración inmediata.

- En caso de ocurrir algún hecho que esté en contra de la política de seguridad de la información de la empresa, se debería contar con una normativa que especifique la sanción correspondiente.

- Si algún proveedor, empleado o cliente de la empresa, solicitara cierta información, se debería contar con una normativa que indique a quién y qué tipo de información puede ser proporcionada.

4.2 PROCESO PARA EL DISEÑO DEL SGSI

En la Figura 4.1 se indican las actividades y documentos a desarrollarse, en cada una de las etapas del modelo PDCA, aplicado al diseño de un Sistema de Gestión de Seguridad de la Información de los servicios de telecomunicaciones ofrecidos a los usuarios de la ciudad de Quito de la Empresa MEGADATOS S.A.

El Proyecto de Titulación abarca la definición del alcance del SGSI, la Política y objetivos, la identificación y valuación de riesgos, la selección de los objetivos de control y de los controles, el desarrollo del Plan de tratamiento de riesgos y del Enunciado de aplicabilidad. Finalmente contempla el desarrollo de las políticas, en base a los controles seleccionados.

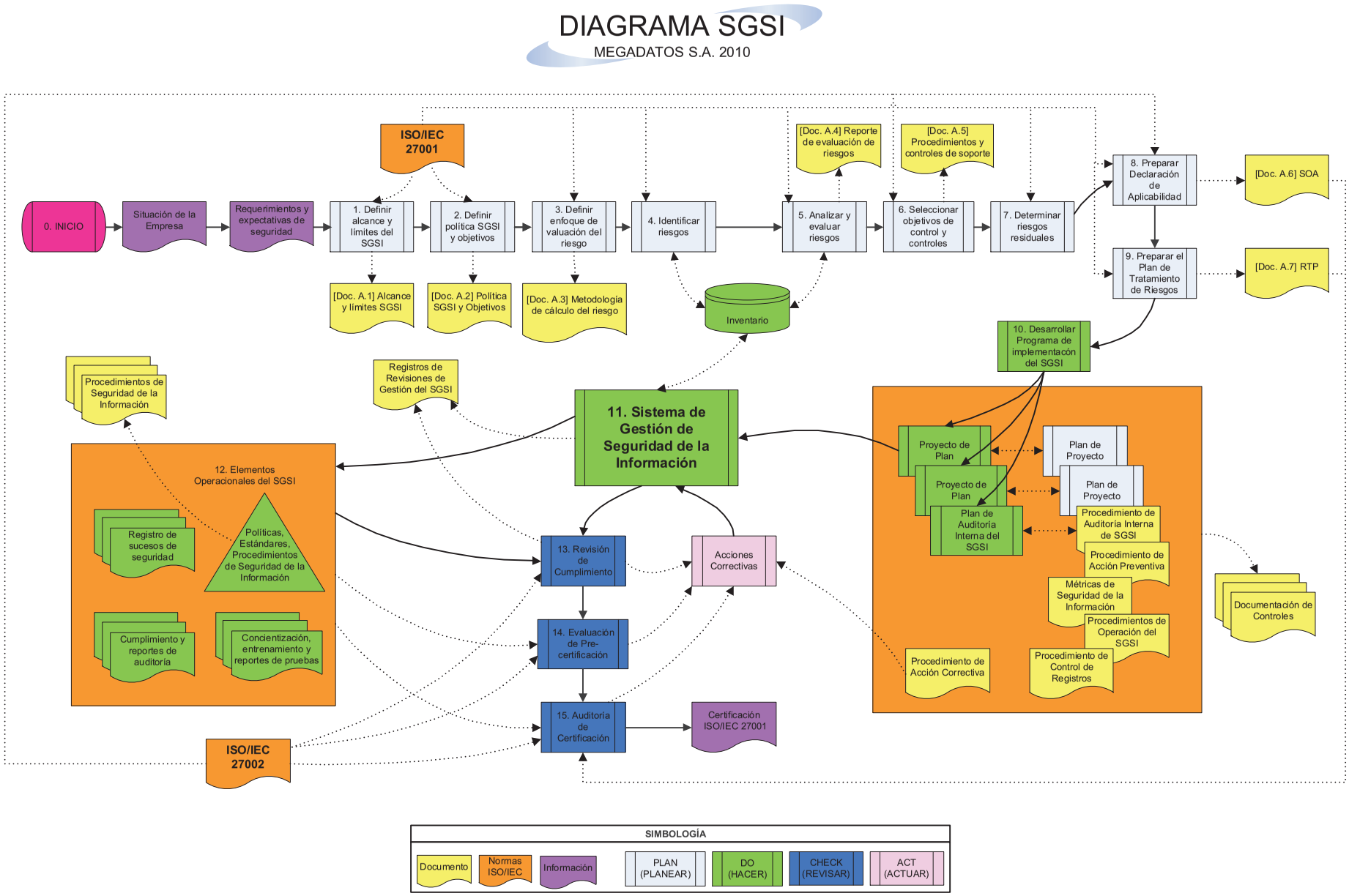


Figura 4.1: Diagrama de Actividades y Documentos para Implementación de SGSI, basado en el modelo PDCA

4.3 ESTABLECIMIENTO DEL SGSI

4.3.1 DEFINICIÓN DEL ALCANCE Y LÍMITES DEL SGSI

Documento A.1

La empresa MEGADATOS S.A. pretende especificar los lineamientos que debe llevar a cabo el personal del Departamento de Operaciones y proveedores para prever, corregir y actuar ante un evento que podría poner en riesgo la confidencialidad, integridad y disponibilidad de la información de los servicios de telecomunicaciones ofrecidos a los usuarios de la ciudad de Quito.

Se considera únicamente los servicios proporcionados en Quito, puesto que es la ciudad en la que convergen la mayor cantidad de clientes y es una de las dos ciudades que está certificada con la Norma ISO 9001. Considerando que los servicios prestados por la empresa constituyen los activos más importantes de la misma, dado que es el producto final que percibe el cliente, se busca otorgar el mayor nivel de seguridad posible.

4.3.2 DEFINICIÓN DE LA POLÍTICA SGSI Y OBJETIVOS

Documento A.2

El Sistema de Gestión de Seguridad de la Información tiene como objetivo establecer los lineamientos que deberán ser realizados por cada uno de los miembros del Departamento de Operaciones, con el fin de preservar la seguridad de la información. Se pretende establecer al SGSI como la base para conservar y evaluar la seguridad de la información dentro de la empresa.

Se designará un responsable de Seguridad de la información, el cual deberá asegurar el mantenimiento permanente de los niveles de seguridad requeridos por la organización en cuanto a servicios. En consecuencia, tendrá el compromiso de prevenir la ocurrencia de acciones inapropiadas o comportamientos ilegales de

los distintos usuarios que utilizan los recursos informáticos, así como los usuarios externos que acceden a estos recursos.

Estas responsabilidades no sólo competen a la disposición de los intereses que persigue la organización, sino también a las obligaciones legales, reguladoras y éticas que conciernen al buen funcionamiento y privacidad de la información de la organización.

El personal encargado de la seguridad serán las personas responsables de documentar, actualizar e implantar las políticas contenidas en este documento. Asimismo deberá realizar evaluaciones periódicas acerca de la efectividad de las políticas y definir modificaciones cuando considere que sean necesarias para asegurar la protección de los activos de información de la organización.

Toda documentación acerca de las políticas de seguridad deberá ser revisada por el comité de Seguridad de la información y aprobada por el Gerente General. Adicionalmente, se deberá comunicar al personal del Departamento de Operaciones cualquier cambio realizado.

La política de seguridad sugerida a la Empresa se enuncia a continuación.

"Brindamos soluciones integrales seguras en Telecomunicaciones e Internet, garantizando la confidencialidad, integridad y disponibilidad de la información. Se dispone de personal, infraestructura y dispositivos que permiten prever, corregir y actuar ante posibles riesgos."

4.3.3 ENFOQUE DE VALUACIÓN DEL RIESGO

Documento A.3

La metodología de cálculo del riesgo a ser utilizada se presenta a continuación.

Con el fin de determinar la importancia de los activos, la probabilidad de ocurrencia de una amenaza, su impacto, costo, tratamiento, es recomendable realizar la valorización de dichos parámetros.

Para el análisis de riesgo, se tomará en cuenta tanto la valorización cualitativa, en la cual se utilizan escalas descriptivas para evaluar el evento, así como la valorización cuantitativa, que utiliza valores numéricos o datos estadísticos para proporcionar una base más sólida en la toma de decisiones.

4.3.3.1 Activos de información

Para el caso de la valoración de los activos, se considerará el nivel de importancia de cada activo para garantizar la confidencialidad, integridad y disponibilidad de la información en la entrega de servicios a los clientes. Para tal efecto, se utilizará el criterio y escalas especificados en las Tablas 4.1, 4.2 y 4.3.

ACTIVOS DE INFORMACIÓN FACTOR CONFIDENCIALIDAD (Conf)		
NIVEL	**CATEGORÍA**	**DESCRIPCIÓN**
1	Bajo	Puede ser revelado o proporcionado. Si su contenido fuera revelado, las consecuencias en la entrega de los servicios podrían ser imperceptibles.
2	Moderado	Puede ser revelado o proporcionado únicamente a personal de la Empresa Megadatos S.A. Si su contenido fuera revelado, las consecuencias en la entrega de los servicios podrían ser moderadas.
3	Alto	Puede ser revelado o proporcionado únicamente al personal del Departamento de Operaciones. Si su contenido fuera revelado, las consecuencias en la entrega de los servicios podrían ser altas.
4	Muy Alto	Puede ser revelado o proporcionado únicamente al personal del Departamento de Operaciones de Megadatos S.A., que autorice el Gerente Nacional de dicho departamento. Si su contenido fuera revelado, las consecuencias en la entrega de los servicios podrían ser fatales.

Tabla 4.1: Valoración de Confidencialidad de Activos de Información

ACTIVOS DE INFORMACIÓN FACTOR INTEGRIDAD (Int)		
NIVEL	**CATEGORÍA**	**DESCRIPCIÓN**
1	Bajo	La modificación de su contenido no afectaría en la entrega de los servicios.
2	Moderado	La modificación de su contenido afectaría de manera moderada en la entrega de los servicios.
3	Alto	La modificación de su contenido afectaría considerablemente en la entrega de los servicios.
4	Muy Alto	La modificación de su contenido afectaría de manera muy relevante en la entrega de los servicios.

Tabla 4.2: Valoración de Integridad de Activos de Información

ACTIVOS DE INFORMACIÓN FACTOR DISPONIBILIDAD (Disp)		
NIVEL	**CATEGORÍA**	**DESCRIPCIÓN**
1	Bajo	Si su contenido no estuviera disponible, las consecuencias en la entrega de los servicios podrían ser reducidas.
2	Moderado	Si su contenido no estuviera disponible, las consecuencias en la entrega de los servicios podrían ser moderadas.
3	Alto	Si su contenido no estuviera disponible, las consecuencias en la entrega de los servicios podrían ser altas.
4	Muy Alto	Si su contenido no estuviera disponible, las consecuencias en la entrega de los servicios podrían ser fatales.

Tabla 4.3: Valoración de Disponibilidad de Activos de Información

Finalmente, se obtendrá el producto de los tres factores (confidencialidad, integridad y disponibilidad) considerados para cada activo, obteniendo su Nivel de Importancia en la entrega de servicios (NI) (de 1 a 64). Para dicho cálculo se considera la Fórmula 4.1.

$$Conf \times Int \times Disp = NI$$

Fórmula 4.1: Nivel de Importancia de Activo de Información

A partir de la categorización expresada en las Tablas 4.1 a 4.3, en la Tabla 4.4, se presenta una estimación de los niveles de importancia que se obtendrán.

RANGOS DE IMPORTANCIA DE LOS ACTIVOS DE INFORMACIÓN		
NIVEL	**CATEGORÍA**	**DESCRIPCIÓN**
1-4	**Bajo**	Activo de importancia baja para asegurar la confidencialidad, integridad y disponibilidad de la información asociada a la prestación de servicios a los clientes.
5-16	**Moderado**	Activo de importancia moderada para asegurar la confidencialidad, integridad y disponibilidad de la información asociada a la prestación de servicios a los clientes.
17-36	**Alto**	Activo de importancia alta para asegurar la confidencialidad, integridad y disponibilidad de la información asociada a la prestación de servicios a los clientes.
37-64	**Muy Alto**	Activo de importancia muy alta para asegurar la confidencialidad, integridad y disponibilidad de la información asociada a la prestación de servicios a los clientes.

Tabla 4.4: Rangos de Importancia de Activos de Información

4.3.3.2 Probabilidad e Impacto de Amenazas

En las Tablas 4.5 y 4.6, se presentan los niveles de probabilidad y niveles de impacto con los que se trabajará durante la valuación del riesgo.

PROBABILIDAD DE OCURRENCIA (Prob)		
NIVEL	**CATEGORÍA**	**DESCRIPCIÓN**
1	Muy improbable	Riesgo con probabilidad de ocurrencia muy baja; de 1% a 25% de que se presente.
2	Improbable	Riesgo con probabilidad baja de presentarse; de 26% a 50% de que se presente.
3	Moderado	Riesgo con probabilidad media de presentarse; de 51% a 74% de que se presente.
4	Probable	Riesgo con alta probabilidad de presentarse; de 75% a 95% de que se presente.
5	Casi Certeza	Riesgo con probabilidad muy alta de presentarse; 96% a 100% de probabilidad de que se presente.

Tabla 4.5: Valoración de la Probabilidad de Ocurrencia [1]

IMPACTO (Imp)		
NIVEL	**CATEGORÍA**	**DESCRIPCIÓN**
1	Insignificante	Riesgo que podría tener un impacto muy pequeño, imperceptible o nulo en la prestación de los servicios. Un usuario afectado.
2	Leve	Riesgo que podría tener un impacto pequeño en la prestación de los servicios; podría ser corregido en un tiempo corto. Número de afectados entre 2 y 10.
3	Moderado	Riesgo que podría tener un impacto importante en la prestación de los servicios; se requeriría de un tiempo considerable para ser corregido. Número de afectados entre 11 y 50.
4	Mayor	Riesgo que podría tener un impacto muy significativo en la prestación de los servicios; se requeriría de más tiempo para que el riesgo sea tratado. Número de afectados entre 51 y 140.
5	Catastrófico	Riesgo que podría tener un impacto que influiría directamente en la prestación de los servicios, implicando el no funcionamiento total de los mismos. El tiempo de tratamiento sería el máximo dentro de todos los impactos. Número de afectados mayor a 140.

Tabla 4.6: Valoración del Impacto [1]

En el documento no se realiza una categorización del impacto de acuerdo al tipo de servicio, pues se considera a todos con características similares (referente a ingresos a la empresa), salvo para el caso de clientes banda ancha personales y *dial up*, con los cuales se mantendrá una relación de 10:1[93].

Una vez elaboradas las Tablas de Probabilidad de ocurrencia e Impacto, se procederá a obtener el Nivel de Riesgo (NR). Para dicho cálculo se considera la Fórmula 4.2.

$$Prob \times Imp = NR$$

Fórmula 4.2: Nivel de Riesgo

Se analizará cada combinación posible de probabilidad e impacto para determinar el nivel de riesgo adecuado, como se presenta en la Tabla 4.7.

[93] La relación 10:1 hace referencia a que por cada 10 clientes banda ancha personales o *dial-up* se considera 1 cliente afectado para la asignación de impacto.

PROBABILIDAD		IMPACTO		NIVEL DE RIESGO
1	Muy improbable	1	Insignificante	Bajo
2	Improbable	1	Insignificante	Bajo
3	Moderado	1	Insignificante	Bajo
4	Probable	1	Insignificante	Moderado
5	Casi Certeza	1	Insignificante	Alto
1	Muy improbable	2	Leve	Bajo
2	Improbable	2	Leve	Bajo
3	Moderado	2	Leve	Moderado
4	Probable	2	Leve	Alto
5	Casi Certeza	2	Leve	Alto
1	Muy improbable	3	Moderado	Moderado
2	Improbable	3	Moderado	Moderado
3	Moderado	3	Moderado	Alto
4	Probable	3	Moderado	Alto
5	Casi Certeza	3	Moderado	Extremo
1	Muy improbable	4	Mayor	Alto
2	Improbable	4	Mayor	Alto
3	Moderado	4	Mayor	Exremo
4	Probable	4	Mayor	Exremo
5	Casi Certeza	4	Mayor	Extemo
1	Muy improbable	5	Catastrófico	Alto
2	Improbable	5	Catastrófico	Extremo
3	Moderado	5	Catastrófico	Extremo
4	Probable	5	Catastrófico	Extremo
5	Casi Certeza	5	Catastrófico	Extremo

Tabla 4.7: Determinación del Nivel de Riesgo [1]

En la Tabla 4.8 se detallan los posibles Niveles de Riesgo.

NIVEL DE RIESGO	DESCRIPCIÓN
Bajo	El nivel de riesgo es bajo, considerando la probabilidad de ocurrencia y el impacto que podría tener al presentarse. Se requiere de controles no urgentes.
Moderado	El nivel de riesgo es moderado, considerando la probabilidad de ocurrencia y el impacto que podría tener al presentarse. Dado el nivel, los controles se deben implementar de manera rápida.
Alto	El nivel de riesgo es alto, considerando la probabilidad de ocurrencia y el impacto que podría tener al presentarse. Se requiere la implementación urgente de controles.
Extremo	El nivel de riesgo es extremo, considerando la probabilidad de ocurrencia y el impacto que podría tener al presentarse. Los controles se deben implementar con suma urgencia.

Tabla 4.8: Rango de Niveles de Riesgo [1]

4.3.3.3 Costo de las Amenazas

Es importante considerar el costo que implicaría una amenaza, es decir las pérdidas económicas[94] a las que la empresa se enfrentaría en caso de presentarse cualquiera de las amenazas que serán identificadas más adelante. Para el análisis de dicho costo, se utilizará la Tabla 4.9, en base a la cotización de activos.

COSTO DE AMENAZAS (Cos)		
NIVEL	**CATEGORÍA**	**DESCRIPCIÓN**
1	Muy Bajo	En caso de presentarse cierta amenaza, su costo sería muy bajo. Se estima como este costo a los valores comprendidos entre $0 y $200.
2	Bajo	En caso de presentarse cierta amenaza, su costo sería bajo. Se estima como costo bajo a los valores comprendidos entre $200,01 y $2.000.
3	Moderado	En caso de presentarse cierta amenaza, su costo sería moderado. Se estima como costo moderado a los valores comprendidos entre $2000,01 y $10.000.
4	Alto	En caso de presentarse cierta amenaza, su costo sería alto. Se estima como costo alto a los valores comprendidos entre $10.000,01 y $30.000.
5	Muy Alto	En caso de presentarse cierta amenaza, su costo sería muy alto. Se estima como costo muy alto a valores superiores a $30.000.

Tabla 4.9: Valoración del Costo de Amenazas

4.3.3.4 Cálculo del Riesgo

Con la probabilidad de ocurrencia, impacto y costo de las amenazas, es posible calcular el Riesgo; para el cálculo se utiliza la Fórmula 4.3:

$$Prob \times Imp \times Cos = RIESGO$$

Fórmula 4.3: Cálculo del Riesgo en función de la Probabilidad, Impacto y Costo

[94] Se consideran costos por pérdidas económicas al valor de los equipos que pudiera verse afectado ante cierta amenaza, demandas por interrupción del servicio, o cualquier costo que implique pérdida para la Empresa. Dentro de estos gastos, no se incluye los costos de los controles.

Al reemplazar la Fórmula 4.2 en 4.3, se observa que ésta podría presentarse como indica la Fórmula 4.4:

$$NR \times Cos = RIESGO$$

Fórmula 4.4: Cálculo del Riesgo en función del Nivel de Riesgo y Costo

Los riesgos podrán variar entre 1 a 125. En la Tabla 4.10 se presentan las categorías asignadas para cada rango identificado. Se han seleccionado rangos de tamaños distintos, procurando que los niveles superiores abarquen la mayor cantidad de elementos, con el fin de asumir las condiciones más críticas y evitar que a algunas amenazas se les asigne riesgos más bajos a los que realmente deberían tener.

RANGOS DE RIESGO		
NIVEL	**CATEGORÍA**	**DESCRIPCIÓN**
1-15	**Leve**	El riesgo es leve, considerando la probabilidad de ocurrencia, impacto y costo que podría tener al presentarse. Su ocurrencia implicaría una pérdida prácticamente imperceptible de la seguridad de la información en la prestación de los servicios.
16-35	**Bajo**	El riesgo es bajo, considerando la probabilidad de ocurrencia, impacto y costo que podría tener al presentarse. Su ocurrencia implicaría una pérdida leve de la seguridad de la información en la prestación de los servicios.
36-60	**Moderado**	El riesgo es moderado, considerando la probabilidad de ocurrencia, impacto y costo que podría tener al presentarse. Su ocurrencia implicaría una pérdida moderada de la seguridad de la información en la prestación de los servicios.
61-90	**Alto**	El riesgo es alto, considerando la probabilidad de ocurrencia, impacto y costo que podría tener al presentarse. Su ocurrencia implicaría una pérdida alta de la seguridad de la información en la prestación de los servicios.
91-125	**Extremo**	El riesgo es extremo, considerando la probabilidad de ocurrencia, impacto y costo que podría tener al presentarse. Su ocurrencia implicaría la pérdida total de la seguridad de la información en la prestación de los servicios.

Tabla 4.10: Rangos de Riesgo

Se identifican niveles de tratamiento del riesgo, considerando las cuatro posibilidades especificadas en la norma ISO 27001: aplicar controles, aceptar el riesgo, evitar el riesgo y transferirlo. La categorización se la realizará en función de la probabilidad de ocurrencia y del impacto.

Pese a que existen cuatro posibilidades de acción, se considerarán tres de ellas como dependientes de los valores de probabilidad e impacto: aplicar controles, aceptar el riesgo y evitarlo. Se optará por transferir el riesgo, en caso de que éste sea producto de un factor externo; la determinación de la transferencia de un riesgo, será independiente de los valores de probabilidad e impacto del mismo. En la Tabla 4.11 se presenta la acción a tomar, dependiendo del Nivel de Riesgo.

NIVEL DE RIESGO	ACCIÓN
Bajo	Aceptar el riesgo
Moderado	Evitar el riesgo
Alto	Aplicar controles
Extremo	

Tabla 4.11: Tratamiento del Riesgo

4.3.4 IDENTIFICACIÓN DE RIESGOS

Para identificar los riesgos a los que se expone la información asociada con los servicios que ofrece MEGADATOS S.A. a los clientes de la ciudad de Quito, es necesario identificar los activos dentro del alcance del SGSI, sus propietarios, las amenazas a las que se exponen, las vulnerabilidades que podrían ser aprovechadas por las amenazas y el impacto que podría tener la pérdida de seguridad de la información de los activos analizados.

4.3.4.1 Activos de información

Considerando los activos de información detallados en el Capítulo 3, se aplica la metodología especificada en el Documento A.3. Se establece el nivel de importancia de cada activo para garantizar la seguridad de la información de los servicios proporcionados a los clientes, basándose en la confidencialidad,

integridad y disponibilidad de la misma. En la Tabla 4.12 se presentan los niveles de importancia (NI) obtenidos de cada activo.

4.3.4.1.1 Centro de Datos

Una vez realizado el análisis de valoración de los activos en el Centro de Datos, se observa que los activos más críticos en contribuir a la seguridad de la información son el *router* de borde, los *switches* y *routers* que permiten la conectividad con equipos que concentran la mayor cantidad de información, y los servidores DNS y Radius que se encuentran virtualizados en el servidor blade.

4.3.4.1.2 Megared Alámbrica

Los activos de información de Megared Alámbrica, considerados como elementos básicos para garantizar la seguridad de la información, son los *switches* de distribución, los cuales tienen conectados *switches* de acceso y en algunos casos permiten la existencia de *backups* para nodos vecinos.

4.3.4.1.3 Megared Inalámbrica

Los resultados obtenidos de la valoración de nivel de importancia de los activos de información, permiten determinar que los activos de la Megared Inalámbrica considerados como más importantes son los *switches* ubicados en Lumbisí, Libertad y Carretas, debido a la cantidad de enlaces hacia clientes, presentes en cada uno de ellos.

4.3.4.2 Amenazas, Vulnerabilidades e Impactos

Es necesario analizar las amenazas humanas, tecnológicas y ambientales a las que podrían estar expuestos los activos de información, peligrando así su seguridad. Además, se identifican las vulnerabilidades asociadas a cada amenaza y el impacto que representaría para la empresa si una de ellas se hace presente.

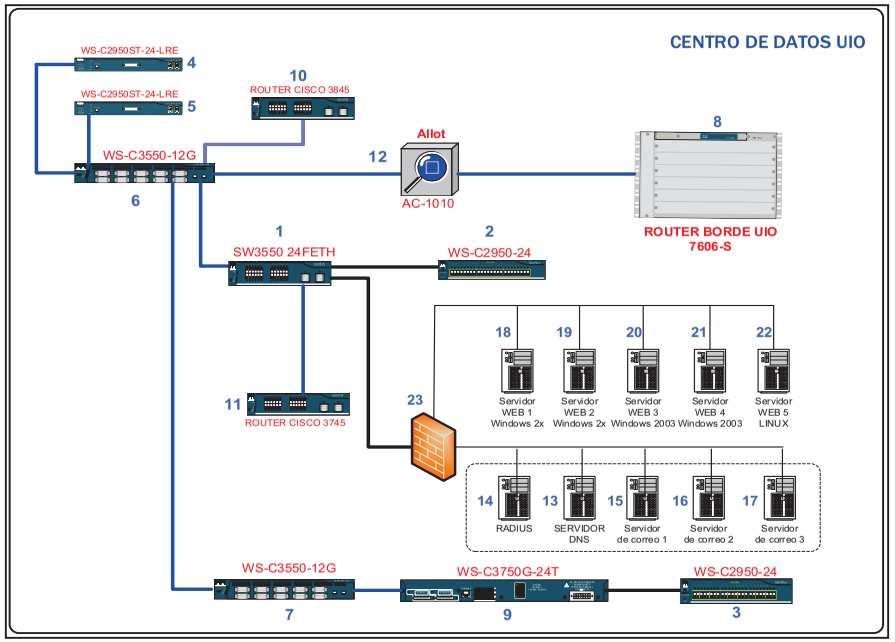
NODO	ACTIVO	Conf	Int	Disp	NI	PROPIETARIO	DIAGRAMA
CENTRO DE DATOS	1	3	4	4	48	Jefe de Implementación y Gestión de Red R1	
	2	3	3	2	18		
	3	3	3	2	18		
	4	2	3	2	12		
	5	2	3	2	12		
	6	4	4	4	64		
	7	3	4	4	48		
	8	4	4	4	64		
	9	3	4	4	48		
	10	2	3	3	18		
	11	2	3	3	18		
	12	3	4	2	24		
	13	4	4	4	64		
	14	4	4	3	48		
	15	3	4	3	36		
	16	3	4	3	36		
	17	3	4	3	36		
	18	2	4	3	24		
	19	2	4	3	24		
	20	2	4	3	24		
	21	2	4	3	24		
	22	2	4	3	24		
	23	4	4	3	48		

Tabla 4.12: Cálculo de Nivel de Importancia de activos de información para la Seguridad (Página 1 de 4)

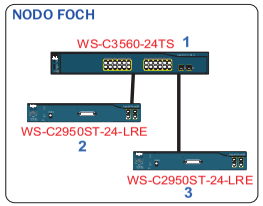
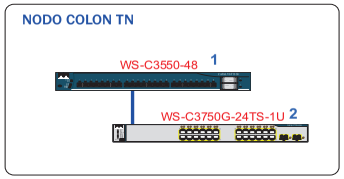
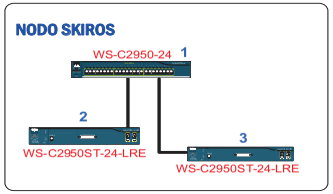
NODO	ACTIVO	Conf	Int	Disp	NI	PROPIETARIO	DIAGRAMA
FOCH	1	3	3	3	27	Administrador de Ingeniería (alámbrico) y Administrador de Red Física y Regulaciones	
	2	2	3	1	6		
	3	2	3	2	12		
LUMBISÍ	1	3	3	3	27	Administrador de Ingeniería (inalámbrico) y Administrador de Red Física y Regulaciones	
LIBERTAD	1	3	3	2	18	Administrador de Ingeniería (inalámbrico) y Administrador de Red Física y Regulaciones	
COLÓN	1	3	3	3	27	Administrador de Ingeniería (alámbrico) y Administrador de Red Física y Regulaciones	
	2	3	4	3	36		
SKIROS	1	3	3	3	27	Administrador de Ingeniería (alámbrico) y Administrador de Red Física y Regulaciones	
	2	2	3	2	12		
	3	2	3	2	12		

Tabla 4.12: Cálculo de Nivel de Importancia de activos de información para la Seguridad (Página 2 de 4)

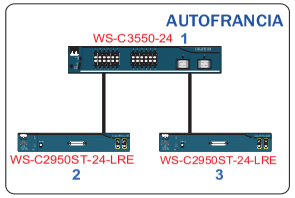
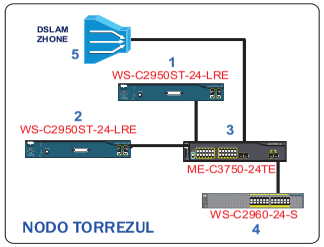
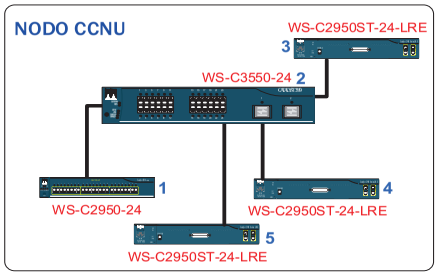
NODO	ACTIVO	Conf	Int	Disp	NI	PROPIETARIO	DIAGRAMA
AUTOFRANCIA	1	3	3	3	27	Administrador de Ingeniería (alámbrico) y Administrador de Red Física y Regulaciones	
	2	3	3	2	18		
	3	3	3	2	18		
TORREZUL	1	2	3	2	12	Administrador de Ingeniería (alámbrico) y Administrador de Red Física y Regulaciones	
	2	2	3	2	12		
	3	3	3	3	27		
	4	2	3	2	12		
	5	2	3	1	6		
CCNU	1	2	3	2	12	Administrador de Ingeniería (alámbrico) y Administrador de Red Física y Regulaciones	
	2	3	4	3	36		
	3	2	3	2	12		
	4	2	3	2	12		
	5	2	3	2	12		
CARRETAS	1	3	3	2	18	Administrador de Ingeniería (inalámbrico) y Administrador de Red Física y Regulaciones	

Tabla 4.12: Cálculo de Nivel de Importancia de activos de información para la Seguridad (Página 3 de 4)

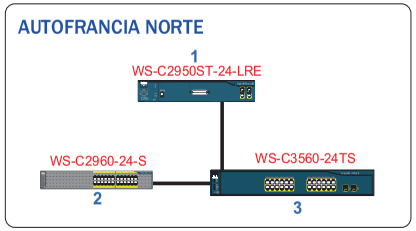
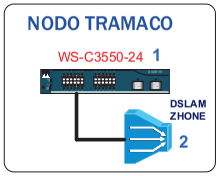
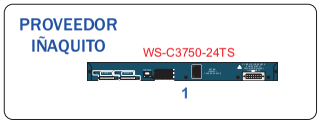
NODO	ACTIVO	Conf	Int	Disp	NI	PROPIETARIO	DIAGRAMA
AUTOFRACIA NORTE	1	3	3	3	27	Administrador de Ingeniería (alámbrico) y Administrador de Red Física y Regulaciones	
	2	3	3	1	9		
	3	3	3	2	18		
TRAMACO	1	3	3	1	9	Administrador de Ingeniería (alámbrico) y Administrador de Red Física y Regulaciones	
	2	3	3	1	9		
PROVEEDOR IÑAQUITO	1	3	3	3	27	Administrador de Ingeniería (alámbrico) y Administrador de Red Física y Regulaciones	
GUAMANÍ	1	2	3	1	6	Administrador de Ingeniería (inalámbrico) y Administrador de Red Física y Regulaciones	

Tabla 4.12: Cálculo de Nivel de Importancia de activos de información para la Seguridad (Página 4 de 4)

Para determinar los impactos, se considera el número de clientes asociados a los equipos; la información pertinente se presenta en la Tabla 4.13. Algunos equipos del Centro de Datos no almacenan en su configuración directamente a clientes; sin embargo, son considerados como fundamentales pues de éstos depende la distribución adecuada de los servicios hacia los nodos, constituyendo así el núcleo de la prestación de servicios, de modo que el impacto de posibles amenazas en dichos equipos será analizada de acuerdo a la importancia de la información que contienen.

Tabla 4.13: Clientes configurados en equipos

Documento A.4

En las Tablas 4.14, 4.15 y 4.16 se presenta la identificación de riesgos, en la que se describen las amenazas y vulnerabilidades que se ha detectado, junto al impacto que ellas generan.

4.3.5 ANÁLISIS Y EVALUACIÓN DEL RIESGO

Una vez identificadas las amenazas a las que se exponen los activos de información, se procede a analizarlas y evaluarlas; para ello se estiman sus probabilidades de ocurrencia, impactos comerciales y costos. La metodología utilizada es la indicada en el Documento A.3. Los resultados obtenidos se presentan en la Matriz de Riesgos de las Tablas 4.14, 4.15 y 4.16 junto a la identificación de riesgos.

Tras la evaluación de los resultados obtenidos en la Matriz de Riesgo, se derivan las siguientes observaciones:

4.3.5.1 Centro de Datos

Pese a que en el Centro de Datos, se cuenta con más seguridades físicas que en los nodos, no dejan de existir amenazas que ponen en riesgo la seguridad de la información. En este caso resultan más críticas las amenazas pues se trata del lugar en donde se concentran los equipos de *core*.

Las amenazas humanas con niveles de riesgo más elevados corresponden a la desconfiguración y desconexión involuntarias de equipos, ingreso no autorizado al Centro de Datos, suplantación de identidad, modificación de información y divulgación de información.

En cuanto a las amenazas tecnológicas, se observan altos niveles de riesgo en la falla de servicio de los proveedores, presencia de virus, troyanos, gusanos, ataques de diccionarios o negación de servicio.

Si bien los equipos que alberga el Centro de Datos representan los bienes más importantes de la Empresa para proporcionar servicios en Quito, los niveles de riesgo de las amenazas ambientales no llegan a ser máximos porque se cuenta con mayores seguridades físicas que en los nodos; aún así, los niveles obtenidos corresponden a la categoría de aplicación de controles.

4.3.5.1 Megared Alámbrica

Se considera más probable la ocurrencia de las amenazas en los nodos, que en el Centro de Datos. Existe más probabilidad porque es más sencillo ingresar a un equipo de acceso o de distribución que a uno de *core*. Además, las seguridades físicas en los nodos son muy inferiores a las del Centro de Datos.

La presencia de las amenazas analizadas, tendría un mayor impacto en los nodos que asocian a más clientes, que corresponden a Colón, CCNU y Autofrancia Norte; por ello se evidencia la necesidad de aplicar controles que aseguren la prestación del servicio ininterrumpido.

Los nodos Colón, Torrezul, CCNU y Foch son los que alojan los equipos más costosos, siendo así los nodos que deberían tener más seguridad, dada la pérdida económica que podría implicar su robo.

Los niveles de riesgo más altos de las amenazas humanas, corresponden al ingreso no autorizado al nodo, suplantación de identidad y divulgación de la información, en la mayoría de los casos.

Con respecto a las amenazas tecnológicas, se observa que los niveles de riesgo más elevados son: falla en el funcionamiento del *switch* de distribución, presencia de virus, troyanos, gusanos, ataques de diccionario y negación del servicio.

En el caso de los niveles de riesgo de las amenazas ambientales, se observa que la probabilidad de ocurrencia de dichas amenazas en los nodos es superior a la del Centro de Datos; debido a su ubicación geográfica, protecciones instaladas y

estructura de la edificación; sin embargo el impacto es inferior debido al número de clientes.

4.3.5.2 Megared Inalámbrica

La presencia de amenazas es más probable en los nodos pertenecientes a Megared Inalámbrica que en el Centro de Datos o en Megared Alámbrica; esto se debe a que el medio inalámbrico es inseguro y vulnerable.

Una cantidad considerable de clientes se encuentran asociados a los nodos de Megared Inalámbrica, lo que hace que el impacto de los riesgos sea alto. El nodo que implica el mayor impacto es Lumbisí, pues su caída ocasionaría también indisponibilidad en Libertad y Guamaní, dado que no se cuenta con *backups*.

Los nodos de Megared Inalámbrica abarcan equipos costosos, pues a más de los *switches* y radios principales de transmisión entre nodos, albergan los radios utilizados para clientes. Lumbisí y Libertad son los nodos con activos más costosos.

Los niveles de riesgo más altos, de amenazas humanas, corresponden al ingreso no autorizado al nodo, suplantación de identidad, divulgación de información y robo de equipos.

De las amenazas tecnológicas, los niveles de riesgo más altos pertenecen a virus, gusanos, troyanos, ataques de diccionario y negación del servicio.

En cuanto a las amenazas ambientales, los niveles de riesgo son elevados en todos los nodos, especialmente en los de mayor impacto. Así se observa que los nodos son muy vulnerables a todas las amenazas ambientales.

IDENTIFICACIÓN DE RIESGOS				ANÁLISIS Y EVALUACIÓN DEL RIESGO CENTRO DE DATOS					
	AMENAZAS	VULNERABILIDADES	IMPACTO	Prob	Imp	NR	Cos	RIESGO	ACCIÓN
Humanas	Desconfiguración involuntaria de *switch* o *router* con NI Muy Alto	No hay una gestión adecuada de claves para configuración, ni una política de privilegios de acceso. No hay un procedimiento formal de almacenamiento de configuraciones.	Podría verse afectado el direccionamiento, enrutamiento; esto incidirá en la entrega de servicios a una gran cantidad de clientes.	3	5	15	3	45	Aplicar controles
	Desconfiguración involuntaria de *switch* o *router* con NI Alto		Podría verse afectado el direccionamiento, enrutamiento; esto incidirá en la entrega de servicios a una cantidad considerable de clientes.	3	4	12	2	24	Aplicar controles
	Desconfiguración involuntaria de *switch* o *router* con NI Moderado		Podría verse afectado el direccionamiento, enrutamiento; esto incidirá en la entrega de servicios a una cantidad moderada de clientes.	3	3	9	2	18	Aplicar controles
	Desconexión de puertos, *switch* o *router* con NI Muy Alto	No hay suficiente control en el ingreso al Centro de Datos. No hay la protección física adecuada para evitar desconexión. No hay una normativa de instalación o cambio del cableado o de equipos.	Desconexión de servicio para una gran cantidad de clientes.	3	5	15	3	45	Aplicar controles
	Desconexión de puertos, *switch* o *router* con NI Alto		Desconexión de servicio para una cantidad considerable de clientes.	3	4	12	2	24	Aplicar controles
	Desconexión de puertos, *switch* o *router* con NI Moderado		Desconexión de servicio para una cantidad moderada de clientes.	3	3	9	2	18	Aplicar controles
	Ingreso a la configuración de equipos con NI Muy Alto, de personal no autorizado	No hay un sistema de monitoreo y registro de ingreso a equipos. No hay un bloqueo para el acceso a los equipos provenientes de segmentos de red diferentes a los de la Empresa. No existe una política formal de concesión de claves y privilegios de acceso.	Cambio no autorizado de configuración; se podría afectar en la entrega de servicios a una gran cantidad de clientes. Además podría implicar robo de información o probabilidad de ataques.	2	5	10	3	30	Aplicar controles
	Ingreso a la configuración de equipos con NI Alto, de personal no autorizado		Cambio no autorizado de configuración; se podria afectar en la entrega de servicios a una cantidad considerable de clientes. Además podría implicar robo de información o probabilidad de ataques.	2	4	8	2	16	Aplicar controles
	Ingreso a la configuración de equipos con NI Moderado, de personal no autorizado		Cambio no autorizado de configuración; se podría afectar en la entrega de servicios a una cantidad moderada de clientes. Además podría implicar robo de información o probabilidad de ataques.	2	2	4	1	4	Aceptar el riesgo

Tabla 4.14: Matriz de Riesgo del Centro de Datos (Página 1 de 5)

IDENTIFICACIÓN DE RIESGOS			ANALISIS Y EVALUACION DEL RIESGO CENTRO DE DATOS					
AMENAZAS	VULNERABILIDADES	IMPACTO	Prob	Imp	NR	Cos	RIESGO	ACCIÓN
Ingreso no autorizado a Centro de Datos	No hay suficiente control en el ingreso al Centro de Datos. No existe una política formal para el ingreso al Centro de Datos, tanto para el personal interno como de terceros. No existe un registro del ingreso o salida de equipos del Centro de Datos.	Acciones inapropiadas con los activos, como robo o desconexión.	5	3	15	3	45	Aplicar controles
Suplantación de identidad	No hay una gestión adecuada de claves de usuario, pues éste podría compartirlas o almacenarlas inadecuadamente. No existe monitoreo de conexión de usuario en puerto correspondiente.	Cambio no autorizado de configuraciones, violación en la confidencialidad de la información. Peligro de robo y ataques.	3	4	12	2	24	Aplicar controles
Modificación de información contenida en los equipos	No existe una política formal de autorización de cambios, migraciones o actualizaciones.	Cambios no autorizados; generación de conflictos entre el personal, por desconocimiento de los cambios.	5	3	15	3	45	Aplicar controles
Divulgación de información	A menudo no se pone en práctica el Acuerdo de Confidencialidad. No se aplican las sanciones especificadas en el Acuerdo de Confidencialidad. No se da seguimiento al personal que ha dejado de ejercer sus funciones en la Empresa.	Violación a la confidencialidad de la información, mal uso de la información por agentes externos.	4	5	20	3	60	Aplicar controles
Error de manejo de la información de activos	No se mantiene clasificada la información. No toda la información y equipos están etiquetados.	Información sensible podría verse afectada, pérdida de información crítica.	3	3	9	3	27	Aplicar controles
Daño de equipos por mantenimiento inadecuado	No se tiene una política de mantenimiento periódico de los equipos.	Daño de activos de información, afectando el servicio.	1	5	5	5	25	Aplicar controles
Robo o pérdida de equipos	No hay suficiente control en el ingreso al Centro de Datos. No hay un inventario completo de activos. **No se ha establecido de manera formal los propietarios de los activos.**	Pérdida económica y falla momentánea en la entrega de servicios.	1	5	5	4	20	Aplicar controles .

Tabla 4.14: Matriz de Riesgo del Centro de Datos (Página 2 de 5)

IDENTIFICACIÓN DE RIESGOS				ANALISIS Y EVALUACION DEL RIESGO CENTRO DE DATOS					
	AMENAZAS	VULNERABILIDADES	IMPACTO	Prob	Imp	NR	Cos	RIESGO	ACCIÓN
Tecnológicas	Falla de servicio de proveedores	No se cuenta con los *backups* necesarios en caso de que falle un proveedor.	Prescindir del servicio de un proveedor, ocasionaría la imposibilidad de entregar los servicios a los clientes, afectando la disponibilidad.	2	5	10	3	30	Aplicar controles *
	Falla en el funcionamiento de *switch* o *router* con NI Muy Alto	No hay un procedimiento formal de contingencia. No hay un procedimiento formal de almacenamiento de configuraciones.	Si falla un equipo del Centro de Datos, se afecta la distribución de los servicios hacia los nodos, implicando la pérdida del servicio para una gran cantidad de clientes.	1	5	5	5	25	Aplicar controles *
	Falla en el funcionamiento de *switch* o *router* con NI Alto		Si falla un equipo del Centro de Datos, se afecta la distribución de los servicios hacia los nodos, implicando la pérdida del servicio para una cantidad considerable de clientes.	1	4	4	4	16	Aplicar controles *
	Falla en el funcionamiento de *switch* o *router* con NI Moderado		Si falla un equipo del Centro de Datos, se afecta la distribución de los servicios hacia los nodos, implicando la pérdida del servicio para una cantidad moderada de clientes.	1	3	3	2	6	Evitar el riesgo *
	Falla de Allot	No hay un procedimiento formal de contingencia. No hay un procedimiento formal de almacenamiento de configuraciones.	Se afectaría la limitación del ancho de banda de los clientes, generando saturación.	1	3	3	5	15	Aplicar controles *
	Falla del Servidor Blade	No hay un procedimiento formal de contingencia. No hay un procedimiento formal de almacenamiento de configuraciones.	Indisponibilidad de la información asociada a los servidores de correo, servidor DNS y Radius. Se ven afectados todos los usuarios de correo e Internet.	1	5	5	5	25	Aplicar controles *
	Falla de Servidores WEB	No hay un procedimiento formal de contingencia. No hay un procedimiento formal de almacenamiento de configuraciones.	Indisponibilidad de la publicación de páginas web de usuarios.	2	4	8	3	24	Aplicar controles *
	Falla del *firewall*	No hay un procedimiento formal de contingencia. No hay un procedimiento formal de almacenamiento de configuraciones.	Caída momentánea de los servidores, mientras no se levante el *backup* . Aún así es riesgoso que los datos se transmitan sin atravesar el *firewall* .	2	4	8	3	24	Aplicar controles *

Tabla 4.14: Matriz de Riesgo del Centro de Datos (Página 3 de 5)

IDENTIFICACIÓN DE RIESGOS			ANALISIS Y EVALUACION DEL RIESGO CENTRO DE DATOS					
AMENAZAS	VULNERABILIDADES	IMPACTO	Prob	Imp	NR	Cos	RIESGO	ACCIÓN
Daño en medios de transmisión	No hay medios alternos o bakcups en todos los casos. Falta de aplicación de normas de Cableado Estructurado.	Corte de servicio para uno o más clientes.	2	3	6	1	6	Evitar el riesgo
Interferencia provocada entre cables de energía y de comunicaciones.	El cableado no ha sido realizado, considerando las distancias mínimas recomendadas para evitar interferencias.	La calidad en la entrega del servicio no sería óptima, debido a las interferencias; se presentarían pérdidas.	2	2	4	1	4	Aceptar el riesgo
Virus, caballos troyanos, gusanos, ataques de diccionario	No hay un sistema de detección y monitoreo de amenazas o ataques. No hay suficientes seguridades de bloqueo de amenazas. No se manejan claves seguras en todos los casos. No se instruye regularmente al personal sobre posibles amenazas.	Afectación en la entrega parcial o total de los servicios; violación a la seguridad de la información.	3	5	15	3	45	Aplicar controles
Negación de servicio (DoS)	No hay sistema de detección de ataques DoS. No existe una política en cuanto a configuración para resguardar los equipos.	Indisponibilidad en la entrega normal de los servicios a uno o varios clientes.	3	5	15	3	45	Aplicar controles
Inconvenientes de capacidad para proveer servicio	Pese a contar con un ancho de banda considerable, no existe un estudio y análisis al respecto. Número limitado de puertos físicos en los equipos. No hay un análisis actual sobre la capacidad en disco de los servidores	Incapacidad para proporcionar servicio a clientes nuevos o para incrementar la capacidad de los clientes actuales.	2	3	6	2	12	Evitar el riesgo
Falla de UPS	No se tiene conocimiento acerca de cortes de energía no programados. No se tiene una política de mantenimiento periódico de los equipos.	Corte de servicio para todos los clientes.	1	5	5	3	15	Aplicar controles
Daño de aire acondicionado	No se tiene una política de mantenimiento periódico de los equipos.	Sobrecalentamiento de los equipos y posible daño de los mismos.	2	3	6	3	18	Evitar el riesgo

Tabla 4.14: Matriz de Riesgo del Centro de Datos (Página 4 de 5)

IDENTIFICACIÓN DE RIESGOS				ANALISIS Y EVALUACION DEL RIESGO CENTRO DE DATOS					
	AMENAZAS	VULNERABILIDADES	IMPACTO	Prob	Imp	NR	Cos	RIESGO	ACCIÓN
Ambientales	Incendio	El sistema contra incendios no se somete regularmente a mantenimiento.	Daño parcial o total del Centro de Datos, junto a los equipos que alberga.	1	5	5	5	25	Aplicar controles *
		Falta de conocimiento del personal de cómo actuar frente a un incendio.							
	Filtraciones de agua	No se tiene una política de mantenimiento periódico del aire acondicionado.	Daño parcial o total del Centro de Datos, junto a los equipos que alberga.	1	4	4	4	16	Aplicar controles *
		No se conoce el estado de las tuberías del edificio.							
		Los S.S.H.H. se encuentran cercanos al Centro de Datos.							
	Terremoto	Quito está ubicada en una zona áltamente telúrica.	Daño parcial o total del Centro de Datos, junto a los equipos que alberga.	1	5	5	5	25	Aplicar controles *
		Falta de conocimiento del personal de cómo actuar frente a un terremoto.							
		No se dispone de una estructura antisísmica.							

Tabla 4. 14: Matriz de Riesgo del Centro de Datos (Página 5 de 5)

IDENTIFICACIÓN DE RIESGOS				ANÁLISIS Y EVALUACIÓN DEL RIESGO											
				NODO FOCH						NODO COLÓN					
AMENAZAS		VULNERABILIDADES	IMPACTO	Prob	Imp	NR	Cos	RIESGO	ACCIÓN	Prob	Imp	NR	Cos	RIESGO	ACCIÓN
Humanas	Desconfiguración involuntaria de *switch*	No hay una gestión adecuada de claves para configuración, ni una política de privilegios de acceso.	Podría verse afectado el direccionamiento, enrutamiento; incidiendo en la entrega de servicios.	3	3	9	2	18	Aplicar controles	3	3	9	2	18	Aplicar controles
		No hay un procedimiento formal de almacenamiento de configuraciones.													
	Desconexión de *switch* o de puertos	No hay control en el ingreso al nodo.	Desconexión de servicio para uno o más clientes.	3	3	9	2	18	Aplicar controles	3	3	9	2	18	Aplicar controles
		No hay la protección física adecuada para evitar desconexión.													
		No hay una normativa de instalación o cambio del cableado o de equipos.													
	Ingreso no autorizado al nodo	No hay suficiente control en el ingreso al nodo.	Acciones inapropiadas con los activos, como apagado o desconexión.	5	3	15	2	30	Aplicar controles	5	3	15	2	30	Aplicar controles
		No existe una política formal para el ingreso al nodo, tanto para el personal interno como de terceros.													
		No existe un registro del ingreso o salida de equipos del nodo.													
	Ingreso a la configuración de equipos, de personal no autorizado	No hay un sistema de monitoreo y registro de ingreso a equipos.	Cambio no autorizado de configuración; robo de información o probabilidad de ataques. Se podría afectar en la entrega de servicios a los clientes.	2	4	8	2	16	Aplicar controles	2	4	8	3	24	Aplicar controles
		No hay un bloqueo para el acceso a los equipos provenientes de segmentos de red diferentes a los de la Empresa.													
		No existe una política formal de concesión de claves y privilegios de acceso.													
		No existe una política para actualización periódica de claves.													

Tabla 4.15: Matriz de Riesgo de Megared Alámbrica (Página 1 de 20)

IDENTIFICACIÓN DE RIESGOS			ANÁLISIS Y EVALUACIÓN DEL RIESGO											
			NODO FOCH						NODO COLÓN					
AMENAZAS	VULNERABILIDADES	IMPACTO	Prob	Imp	NR	Cos	RIESGO	ACCIÓN	Prob	Imp	NR	Cos	RIESGO	ACCIÓN
Suplantación de identidad	No hay una gestión adecuada de claves de usuario, pues éste podría compartirlas o almacenarlas inadecuadamente. No existe monitoreo de conexión de usuario en puerto correspondiente.	Cambio no autorizado de configuraciones, violación en la confidencialidad de la información. Peligro de robo y ataques.	3	4	12	2	24	Aplicar controles	3	4	12	3	36	Aplicar controles
Modificación de información contenida en los equipos	No existe una política formal de autorización de cambios, migraciones o actualizaciones.	Cambios no autorizados; generación de conflictos entre el personal, por desconocimiento de los cambios.	5	2	10	1	10	Aplicar controles	5	2	10	1	10	Aplicar controles
Divulgación de información	A menudo no se pone en práctica el Acuerdo de Confidencialidad. No se aplican las sanciones especificadas en el Acuerdo de Confidencialidad. No se da seguimiento al personal que ha dejado de ejercer sus funciones en la Empresa.	Violación a la confidencialidad de la información, mal uso de la información por agentes externos.	3	4	12	2	24	Aplicar controles	3	4	12	3	36	Aplicar controles
Error de manejo de la información de activos	No se mantiene clasificada la información. No toda la información y equipos están etiquetados.	Información sensible podría verse afectada, pérdida de información crítica.	3	2	6	2	12	Evitar el riesgo	3	3	9	3	27	Aplicar controles
Daño de equipos por mantenimiento inadecuado	No se tiene una política de mantenimiento periódico de los equipos.	Daño de activos de información, afectando el servicio.	2	4	8	3	24	Aplicar controles	2	4	8	4	32	Aplicar controles
Robo o pérdida de equipos	No hay suficiente control en el ingreso al nodo. Bajo nivel de seguridad física No hay un inventario completo de activos. **No se ha establecido de manera formal los propietarios de los activos.**	Pérdida económica y falla momentánea en la entrega de servicios.	2	4	8	3	24	Aplicar controles -	2	4	8	4	32	Aplicar controles -

Tabla 4.15: Matriz de Riesgo de Megared Alámbrica (Página 2 de 20)

IDENTIFICACIÓN DE RIESGOS				ANÁLISIS Y EVALUACIÓN DEL RIESGO											
				NODO FOCH						NODO COLÓN					
AMENAZAS		VULNERABILIDADES	IMPACTO	Prob	Imp	NR	Cos	RIESGO	ACCIÓN	Prob	Imp	NR	Cos	RIESGO	ACCIÓN
Tecnológicas	Falla en el funcionamiento del *switch* de distribución	No hay un procedimiento formal de contingencia. No hay un procedimiento formal de almacenamiento de configuraciones. Falta de adecuaciones en las instalaciones del nodo.	Falla momentánea en la entrega de servicios a clientes, inoperabilidad de *switches* de acceso u otros *switches* de distribución.	1	4	4	3	12	Aplicar controles *	1	4	4	3	12	Aplicar controles *
	Falla en el funcionamiento de *switch* de acceso o DSLAM	No hay un procedimiento formal de contingencia. No hay un procedimiento formal de almacenamiento de configuraciones. Falta de adecuaciones en las instalaciones del nodo.	Falla momentánea en la entrega de servicios a clientes.	1	2	2	2	4	Aceptar el riesgo *	1	3	3	3	9	Evitar el riesgo *
	Interferencia provocada entre cables de energía y de comunicaciones	El cableado no ha sido realizado, considerando las separaciones mínimas recomendadas para evitar interferencias.	La calidad en la entrega del servicio no sería óptima, debido a las interferencias; se presentarían pérdidas.	2	2	4	1	4	Aceptar el riesgo	2	2	4	1	4	Aceptar el riesgo
	Virus, caballos troyanos, gusanos, ataques de diccionario	No hay un sistema de detección y monitoreo de amenazas o ataques. No hay suficientes seguridades de bloqueo de amenazas. No se manejan claves seguras en todos los casos. No se instruye regularmente al personal sobre posibles amenazas.	Afectación en la entrega parcial o total de los servicios; violación a la seguridad de la información.	3	4	12	2	24	Aplicar controles	3	4	12	2	24	Aplicar controles
	Negación de servicio (DoS)	No hay sistema de detección de ataques DoS. No existe una política en cuanto a configuración para resguardar los equipos.	Indisponibilidad en la entrega normal de los servicios a uno o varios clientes.	3	4	12	3	36	Aplicar controles	3	4	12	3	36	Aplicar controles

Tabla 4.15: Matriz de Riesgo de Megared Alámbrica (Página 3 de 20)

IDENTIFICACIÓN DE RIESGOS				ANÁLISIS Y EVALUACIÓN DEL RIESGO											
				NODO FOCH						NODO COLÓN					
AMENAZAS		VULNERABILIDADES	IMPACTO	Prob	Imp	NR	Cos	RIESGO	ACCIÓN	Prob	Imp	NR	Cos	RIESGO	ACCIÓN
	Inconvenientes de capacidad para proveer servicio	Pese a contar con un ancho de banda considerable, no existe un estudio y análisis al respecto. Número limitado de puertos físicos en los equipos. No hay un análisis actual sobre la capacidad en disco de los servidores	Incapacidad para proporcionar servicio a clientes nuevos o para incrementar la capacidad de los clientes actuales.	2	2	4	1	4	Aceptar el riesgo	2	2	4	1	4	Aceptar el riesgo
	Falla de UPS	No se tiene conocimiento acerca de cortes de energía no programados. No se tiene una política de mantenimiento periódico de los equipos.	Corte de servicio para todos los clientes.	2	4	8	3	24	Aplicar controles	2	4	8	3	24	Aplicar controles
	Daño en última milla	No se tiene la suficiente seguridad física en los enlaces. No se cuenta con *backups* para todos los enlaces. Accidentes de tránsito pueden afectar a los postes que sostienen el cableado.	Corte de servicio para uno o más clientes.	4	2	8	1	8	Aplicar controles	4	2	8	1	8	Aplicar controles
	Daño del equipo de última milla	No se da instructivos a clientes de cuidado de equipos. Falta de adecuaciones en las instalaciones del nodo. Malas condiciones eléctricas de las instalaciones del cliente.	Corte de servicio para un cliente.	2	1	2	1	2	Aceptar el riesgo	2	1	2	1	2	Aceptar el riesgo
Ambientales	Incendio	No se dispone de un sistema contra incendios. El nodo no se encuentra en un lugar aislado, puede verse afectado por daños externos.	Daño parcial o total del nodo, junto a los equipos que alberga.	1	4	4	3	12	Aplicar controles	1	4	4	4	16	Aplicar controles
	Filtraciones de agua	Falta de adecuaciones en las instalaciones del nodo.	Daño parcial de equipos.	1	2	2	2	4	Aceptar el riesgo	1	2	2	2	4	Aceptar el riesgo
	Terremoto	Quito está ubicada en una zona áltamente telúrica. No se dispone de una estructura antisísmica.	Daño parcial o total del nodo, junto a los equipos que alberga.	1	4	4	3	12	Aplicar controles	1	4	4	4	16	Aplicar controles

Tabla 4.15: Matriz de Riesgo de Megared Alámbrica (Página 4 de 20)

IDENTIFICACIÓN DE RIESGOS				ANÁLISIS Y EVALUACIÓN DEL RIESGO											
				NODO SKIROS						NODO AUTOFRANCIA					
AMENAZAS		VULNERABILIDADES	IMPACTO	Prob	Imp	NR	Cos	RIESGO	ACCIÓN	Prob	Imp	NR	Cos	RIESGO	ACCIÓN
Humanas	Desconfiguración involuntaria de *switch*	No hay una gestión adecuada de claves para configuración, ni una política de privilegios de acceso.	Podría verse afectado el direccionamiento, enrutamiento, incidiendo en la entrega de servicios.	3	2	6	1	6	Evitar el riesgo	3	2	6	1	6	Evitar el riesgo
		No hay un procedimiento formal de almacenamiento de configuraciones.													
	Desconexión de switch o de puertos	No hay control en el ingreso al nodo.	Desconexión de servicio para uno o más clientes.	3	2	6	1	6	Evitar el riesgo	3	2	6	1	6	Evitar el riesgo
		No hay la protección física adecuada para evitar desconexión.													
		No hay una normativa de instalación o cambio del cableado o de equipos.													
	Ingreso no autorizado al nodo	No hay suficiente control en el ingreso al nodo.	Acciones inapropiadas con los activos, como apagado o desconexión.	5	2	10	1	10	Aplicar controles	5	2	10	1	10	Aplicar controles
		No existe una política formal para el ingreso al nodo, tanto para el personal interno como de terceros.													
		No existe un registro del ingreso o salida de equipos del nodo.													
	Ingreso a la configuración de equipos, de personal no autorizado	No hay un sistema de monitoreo y registro de ingreso a equipos.	Cambio no autorizado de configuración; robo de información o probabilidad de ataques. Se podría afectar en la entrega de servicios a los clientes.	2	3	6	1	6	Evitar el riesgo	2	3	6	1	6	Evitar el riesgo
		No hay un bloqueo para el acceso a los equipos provenientes de segmentos de red diferentes a los de la Empresa.													
		No existe una política formal de concesión de claves y privilegios de acceso.													
		No existe una política para actualización periódica de claves.													

Tabla 4.15: Matriz de Riesgo de Megared Alámbrica (Página 5 de 20)

IDENTIFICACIÓN DE RIESGOS			ANÁLISIS Y EVALUACIÓN DEL RIESGO											
			NODO SKIROS						NODO AUTOFRANCIA					
AMENAZAS	VULNERABILIDADES	IMPACTO	Prob	Imp	NR	Cos	RIESGO	ACCIÓN	Prob	Imp	NR	Cos	RIESGO	ACCIÓN
Suplantación de identidad	No hay una gestión adecuada de claves de usuario, pues éste podría compartirlas o almacenarlas inadecuadamente. No existe monitoreo de conexión de usuario en puerto correspondiente.	Cambio no autorizado de configuraciones, violación en la confidencialidad de la información. Peligro de robo y ataques.	3	3	9	1	9	Aplicar controles	3	3	9	1	9	Aplicar controles
Modificación de información contenida en los equipos	No existe una política formal de autorización de cambios, migraciones o actualizaciones.	Cambios no autorizados; generación de conflictos entre el personal, por desconocimiento de los cambios.	5	1	5	1	5	Aplicar controles	5	1	5	1	5	Aplicar controles
Divulgación de información	A menudo no se pone en práctica el Acuerdo de Confidencialidad. No se aplican las sanciones especificadas en el Acuerdo de Confidencialidad. No se da seguimiento al personal que ha dejado de ejercer sus funciones en la Empresa.	Violación a la confidencialidad de la información, mal uso de la información por agentes externos.	3	3	9	2	18	Aplicar controles	3	3	9	2	18	Aplicar controles
Error de manejo de la información de activos	No se mantiene clasificada la información. No toda la información y equipos están etiquetados.	Información sensible podría verse afectada, pérdida de información crítica.	3	1	3	1	3	Aceptar el riesgo	3	2	6	2	12	Evitar el riesgo
Daño de equipos por mantenimiento inadecuado	No se tiene una política de mantenimiento periódico de los equipos.	Daño de activos de información, afectando el servicio.	2	3	6	2	12	Evitar el riesgo	2	3	6	3	18	Evitar el riesgo
Robo o pérdida de equipos	No hay suficiente control en el ingreso al nodo. Bajo nivel de seguridad física No hay un inventario completo de activos. **No se ha establecido de manera formal los propietarios de los activos.**	Pérdida económica y falla momentánea en la entrega de servicios.	2	3	6	2	12	Evitar el riesgo .	2	3	6	3	18	Evitar el riesgo .

Tabla 4.15: Matriz de Riesgo de Megared Alámbrica (Página 6 de 20)

IDENTIFICACIÓN DE RIESGOS				ANÁLISIS Y EVALUACIÓN DEL RIESGO											
				NODO SKIROS						NODO AUTOFRANCIA					
AMENAZAS		VULNERABILIDADES	IMPACTO	Prob	Imp	NR	Cos	RIESGO	ACCIÓN	Prob	Imp	NR	Cos	RIESGO	ACCIÓN
Tecnológicas	Falla en el funcionamiento del *switch* de distribución	No hay un procedimiento formal de contingencia.	Falla momentánea en la entrega de servicios a clientes, inoperabilidad de *switches* de acceso u otros *switches* de distribución.	1	3	3	2	6	Evitar el riesgo *	1	3	3	3	9	Evitar el riesgo *
		No hay un procedimiento formal de almacenamiento de configuraciones.													
		Falta de adecuaciones en las instalaciones del nodo.													
	Falla en el funcionamiento de *switch* de acceso o DSLAM	No hay un procedimiento formal de contingencia.	Falla momentánea en la entrega de servicios a clientes.	1	3	3	2	6	Evitar el riesgo *	1	3	3	2	6	Evitar el riesgo *
		No hay un procedimiento formal de almacenamiento de configuraciones.													
		Falta de adecuaciones en las instalaciones del nodo.													
	Interferencia provocada entre cables de energía y de comunicaciones	El cableado no ha sido realizado, considerando las separaciones mínimas recomendadas para evitar interferencias.	La calidad en la entrega del servicio no sería óptima, debido a las interferencias; se presentarían pérdidas.	2	2	4	1	4	Aceptar el riesgo	2	2	4	1	4	Aceptar el riesgo
	Virus, caballos troyanos, gusanos, ataques de diccionario	No hay un sistema de detección y monitoreo de amenazas o ataques.	Afectación en la entrega parcial o total de los servicios; violación a la seguridad de la información.	3	3	9	2	18	Aplicar controles	3	3	9	2	18	Aplicar controles
		No hay suficientes seguridades de bloqueo de amenazas.													
		No se manejan claves seguras en todos los casos.													
		No se instruye regularmente al personal sobre posibles amenazas.													
	Negación de servicio (DoS)	No hay sistema de detección de ataques DoS.	Indisponibilidad en la entrega normal de los servicios a uno o varios clientes.	3	3	9	2	18	Aplicar controles	3	3	9	2	18	Aplicar controles
		No existe una política en cuanto a configuración para resguardar los equipos.													

Tabla 4.15: Matriz de Riesgo de Megared Alámbrica (Página 7 de 20)

IDENTIFICACIÓN DE RIESGOS				ANÁLISIS Y EVALUACIÓN DEL RIESGO											
				NODO SKIROS						NODO AUTOFRANCIA					
AMENAZAS		VULNERABILIDADES	IMPACTO	Prob	Imp	NR	Cos	RIESGO	ACCIÓN	Prob	Imp	NR	Cos	RIESGO	ACCIÓN
	Inconvenientes de capacidad para proveer servicio	Pese a contar con un ancho de banda considerable, no existe un estudio y análisis al respecto. Número limitado de puertos físicos en los equipos. No hay un análisis actual sobre la capacidad en disco de los servidores	Incapacidad para proporcionar servicio a clientes nuevos o para incrementar la capacidad de los clientes actuales.	2	1	2	1	2	Aceptar el riesgo	2	1	2	1	2	Aceptar el riesgo
	Falla de UPS	No se tiene conocimiento acerca de cortes de energía no programados. No se tiene una política de mantenimiento periódico de los equipos.	Corte de servicio para todos los clientes.	2	3	6	2	12	Evitar el riesgo	2	3	6	2	12	Evitar el riesgo
	Daño en última milla	No se tiene la suficiente seguridad física en los enlaces. No se cuenta con *backups* para todos los enlaces. Accidentes de tránsito pueden afectar a los postes que sostienen el cableado.	Corte de servicio para uno o más clientes.	4	2	8	1	8	Aplicar controles	4	2	8	1	8	Aplicar controles
	Daño del equipo de última milla	No se da instructivos a clientes de conservación de equipos. Falta de adecuaciones en las instalaciones del nodo. Malas condiciones eléctricas de las instalaciones del cliente.	Corte de servicio para un cliente.	2	1	2	1	2	Aceptar el riesgo	2	1	2	1	2	Aceptar el riesgo
Ambientales	Incendio	No se dispone de un sistema contra incendios. El nodo no se encuentra en un lugar aislado, por lo que puede verse afectado por daños externos.	Daño parcial o total del nodo, junto a los equipos que alberga.	1	3	3	2	6	Evitar el riesgo	1	3	3	3	9	Evitar el riesgo
	Filtraciones de agua	Falta de adecuaciones en las instalaciones del nodo.	Daño parcial de equipos.	1	2	2	1	2	Aceptar el riesgo	1	2	2	1	2	Aceptar el riesgo
	Terremoto	Quito está ubicada en una zona áltamente telúrica. No se dispone de una estructura antisísmica.	Daño parcial o total del nodo, junto a los equipos que alberga.	1	3	3	2	6	Evitar el riesgo	1	3	3	3	9	Evitar el riesgo

Tabla 4.15: Matriz de Riesgo de Megared Alámbrica (Página 8 de 20)

IDENTIFICACIÓN DE RIESGOS				ANALISIS Y EVALUACION DEL RIESGO											
				NODO TORREZUL						NODO CCNU					
AMENAZAS		VULNERABILIDADES	IMPACTO	Prob	Imp	NR	Cos	RIESGO	ACCIÓN	Prob	Imp	NR	Cos	RIESGO	ACCIÓN
Humanas	Desconfiguración involuntaria de *switch*	No hay una gestión adecuada de claves para configuración, ni una política de privilegios de acceso.	Podría verse afectado el direccionamiento, enrutamiento, incidiendo en la entrega de servicios.	3	3	9	2	18	Aplicar controles	3	3	9	2	18	Aplicar controles
		No hay un procedimiento formal de almacenamiento de configuraciones.													
	Desconexión de *switch* o de puertos	No hay control en el ingreso al nodo.	Desconexión de servicio para uno o más clientes.	3	3	9	2	18	Aplicar controles	3	3	9	2	18	Aplicar controles
		No hay la protección física adecuada para evitar desconexión.													
		No hay una normativa de instalación o cambio del cableado o de equipos.													
	Ingreso no autorizado al nodo	No hay suficiente control en el ingreso al nodo.	Acciones inapropiadas con los activos, como apagado o desconexión.	4	3	12	2	24	Aplicar controles	5	3	15	2	30	Aplicar controles
		No existe una política formal para el ingreso al nodo, tanto para el personal interno como de terceros.													
		No existe un registro del ingreso o salida de equipos del nodo.													
	Ingreso a la configuración de equipos, de personal no autorizado	No hay un sistema de monitoreo y registro de ingreso a equipos.	Cambio no autorizado de configuración; robo de información o probabilidad de ataques. Se podría afectar en la entrega de servicios a los clientes.	2	4	8	2	16	Aplicar controles	2	4	8	2	16	Aplicar controles
		No hay un bloqueo para el acceso a los equipos provenientes de segmentos de red diferentes a los de la Empresa.													
		No existe una política formal de concesión de claves y privilegios de acceso.													
		No existe una política para actualización periódica de claves.													

Tabla 4.15: Matriz de Riesgo de Megared Alámbrica (Página 9 de 20)

IDENTIFICACIÓN DE RIESGOS			ANÁLISIS Y EVALUACIÓN DEL RIESGO											
			NODO TORREZUL						NODO CCNU					
AMENAZAS	VULNERABILIDADES	IMPACTO	Prob	Imp	NR	Cos	RIESGO	ACCIÓN	Prob	Imp	NR	Cos	RIESGO	ACCIÓN
Suplantación de identidad	No hay una gestión adecuada de claves de usuario, pues éste podría compartirlas o almacenarlas inadecuadamente. No existe monitoreo de conexión de usuario en puerto correspondiente.	Cambio no autorizado de configuraciones, violación en la confidencialidad de la información. Peligro de robo y ataques.	3	4	12	2	24	Aplicar controles	3	4	12	2	24	Aplicar controles
Modificación de información contenida en los equipos	No existe una política formal de autorización de cambios, migraciones o actualizaciones.	Cambios no autorizados; generación de conflictos entre el personal, por desconocimiento de los cambios.	5	2	10	1	10	Aplicar controles	5	2	10	1	10	Aplicar controles
Divulgación de información	A menudo no se pone en práctica el Acuerdo de Confidencialidad. No se aplican las sanciones especificadas en el Acuerdo de Confidencialidad. No se da seguimiento al personal que ha dejado de ejercer sus funciones en la Empresa.	Violación a la confidencialidad de la información, mal uso de la información por agentes externos.	3	4	12	2	24	Aplicar controles	3	4	12	2	24	Aplicar controles
Error de manejo de la información de activos	No se mantiene clasificada la información. No toda la información y equipos están etiquetados.	Información sensible podría verse afectada, pérdida de información crítica.	3	3	9	2	18	Aplicar controles	3	3	9	2	18	Aplicar controles
Daño de equipos por mantenimiento inadecuado	No se tiene una política de mantenimiento periódico de los equipos.	Daño de activos de información, afectando el servicio.	2	4	8	3	24	Aplicar controles	2	4	8	3	24	Aplicar controles
Robo o pérdida de equipos	No hay suficiente control en el ingreso al nodo. Bajo nivel de seguridad física No hay un inventario completo de activos. **No se ha establecido de manera formal los propietarios de los activos.**	Pérdida económica y falla momentánea en la entrega de servicios.	1	4	4	3	12	Aplicar controles -	2	4	8	3	24	Aplicar controles -

Tabla 4.15: Matriz de Riesgo de Megared Alámbrica (Página 10 de 20)

IDENTIFICACIÓN DE RIESGOS				ANÁLISIS Y EVALUACIÓN DEL RIESGO											
				NODO TORREZUL						NODO CCNU					
AMENAZAS		VULNERABILIDADES	IMPACTO	Prob	Imp	NR	Cos	RIESGO	ACCIÓN	Prob	Imp	NR	Cos	RIESGO	ACCIÓN
Tecnológicas	Falla en el funcionamiento del *switch* de distribución	No hay un procedimiento formal de contingencia. No hay un procedimiento formal de almacenamiento de configuraciones. Falta de adecuaciones en las instalaciones del nodo.	Falla momentánea en la entrega de servicios a clientes, inoperabilidad de *switches* de acceso u otros *switches* de distribución.	1	4	4	3	12	Aplicar controles *	1	4	4	3	12	Aplicar controles *
	Falla en el funcionamiento de *switch* de acceso o DSLAM	No hay un procedimiento formal de contingencia. No hay un procedimiento formal de almacenamiento de configuraciones. Falta de adecuaciones en las instalaciones del nodo.	Falla momentánea en la entrega de servicios a clientes.	1	3	3	2	6	Evitar el riesgo *	1	3	3	2	6	Evitar el riesgo *
	Interferencia provocada entre cables de energía y de comunicaciones	El cableado no ha sido realizado, considerando las separaciones mínimas recomendadas para evitar interferencias.	La calidad en la entrega del servicio no sería óptima, debido a las interferencias; se presentarían pérdidas.	1	2	2	1	2	Aceptar el riesgo	2	2	4	1	4	Aceptar el riesgo
	Virus, caballos troyanos, gusanos, ataques de diccionario	No hay un sistema de detección y monitoreo de amenazas o ataques. No hay suficientes seguridades de bloqueo de amenazas. No se manejan claves seguras en todos los casos. No se instruye regularmente al personal sobre posibles amenazas.	Afectación en la entrega parcial o total de los servicios; violación a la seguridad de la información.	3	4	12	2	24	Aplicar controles	3	4	12	2	24	Aplicar controles
	Negación de servicio (DoS)	No hay sistema de detección de ataques DoS. No existe una política en cuanto a configuración para resguardar los equipos.	Indisponibilidad en la entrega normal de los servicios a uno o varios clientes.	3	4	12	3	36	Aplicar controles	3	4	12	3	36	Aplicar controles

Tabla 4.15: Matriz de Riesgo de Megared Alámbrica (Página 11 de 20)

IDENTIFICACIÓN DE RIESGOS				ANÁLISIS Y EVALUACIÓN DEL RIESGO											
				NODO TORREZUL						NODO CCNU					
AMENAZAS		VULNERABILIDADES	IMPACTO	Prob	Imp	NR	Cos	RIESGO	ACCIÓN	Prob	Imp	NR	Cos	RIESGO	ACCIÓN
	Inconvenientes de capacidad para proveer servicio	Pese a contar con un ancho de banda considerable, no existe un estudio y análisis al respecto. Número limitado de puertos físicos en los equipos. No hay un análisis actual sobre la capacidad en disco de los servidores	Incapacidad para proporcionar servicio a clientes nuevos o para incrementar la capacidad de los clientes actuales.	2	2	4	1	4	Aceptar el riesgo	2	2	4	1	4	Aceptar el riesgo
	Falla de UPS	No se tiene conocimiento acerca de cortes de energía no programados. No se tiene una política de mantenimiento periódico de los equipos.	Corte de servicio para todos los clientes.	1	4	4	2	8	Aplicar controles	2	4	8	3	24	Aplicar controles
	Daño en última milla	No se tiene la suficiente seguridad física en los enlaces. No se cuenta con *backups* para todos los enlaces. Accidentes de tránsito pueden afectar a los postes que sostienen el cableado.	Corte de servicio para uno o más clientes.	4	2	8	1	8	Aplicar controles	4	2	8	1	8	Aplicar controles
	Daño del equipo de última milla	No se da instructivos a clientes de conservación de equipos. Falta de adecuaciones en las instalaciones del nodo. Malas condiciones eléctricas de las instalaciones del cliente.	Corte de servicio para un cliente.	2	1	2	1	2	Aceptar el riesgo	2	1	2	1	2	Aceptar el riesgo
Ambientales	Incendio	No se dispone de un sistema contra incendios. El nodo no se encuentra en un lugar aislado, puede verse afectado por daños externos.	Daño parcial o total del nodo, junto a los equipos que alberga.	1	4	4	3	12	Aplicar controles	1	4	4	3	12	Aplicar controles
	Filtraciones de agua	Falta de adecuaciones en las instalaciones del nodo.	Daño parcial de equipos.	1	2	2	2	4	Aceptar el riesgo	1	2	2	2	4	Aceptar el riesgo
	Terremoto	Quito está ubicada en una zona áltamente telúrica. No se dispone de una estructura antisísmica.	Daño parcial o total del nodo, junto a los equipos que alberga.	1	4	4	3	12	Aplicar controles	1	4	4	3	12	Aplicar controles

Tabla 4.15: Matriz de Riesgo de Megared Alámbrica (Página 12 de 20)

IDENTIFICACIÓN DE RIESGOS				ANÁLISIS Y EVALUACIÓN DEL RIESGO											
				NODO AUTOFRANCIA NORTE						NODO TRAMACO					
AMENAZAS		VULNERABILIDADES	IMPACTO	Prob	Imp	NR	Cos	RIESGO	ACCIÓN	Prob	Imp	NR	Cos	RIESGO	ACCIÓN
Humanas	Desconfiguración involuntaria de *switch*	No hay una gestión adecuada de claves para configuración, ni una política de privilegios de acceso.	Podría verse afectado el direccionamiento, enrutamiento, incidiendo en la entrega de servicios.	3	3	9	2	18	Aplicar controles	3	1	3	1	3	Aceptar el riesgo
		No hay un procedimiento formal de almacenamiento de configuraciones.													
	Desconexión de *switch* o de puertos	No hay control en el ingreso al nodo.	Desconexión de servicio para uno o más clientes.	3	3	9	2	18	Aplicar controles	3	1	3	1	3	Aceptar el riesgo
		No hay la protección física adecuada para evitar desconexión.													
		No hay una normativa de instalación o cambio del cableado o de equipos.													
	Ingreso no autorizado al nodo	No hay suficiente control en el ingreso al nodo.	Acciones inapropiadas con los activos, como apagado o desconexión.	5	3	15	2	30	Aplicar controles	5	1	5	1	5	Aplicar controles
		No existe una política formal para el ingreso al nodo, tanto para el personal interno como de terceros.													
		No existe un registro del ingreso o salida de equipos del nodo.													
	Ingreso a la configuración de equipos, de personal no autorizado	No hay un sistema de monitoreo y registro de ingreso a equipos.	Cambio no autorizado de configuración; robo de información o probabilidad de ataques. Se podría afectar en la entrega de servicios a los clientes.	2	4	8	2	16	Aplicar controles	2	1	2	1	2	Aceptar el riesgo
		No hay un bloqueo para el acceso a los equipos provenientes de segmentos de red diferentes a los de la Empresa.													
		No existe una política formal de concesión de claves y privilegios de acceso.													
		No existe una política para actualización periódica de claves.													

Tabla 4.15: Matriz de Riesgo de Megared Alámbrica (Página 13 de 20)

IDENTIFICACIÓN DE RIESGOS				ANÁLISIS Y EVALUACIÓN DEL RIESGO											
				NODO AUTOFRANCIA NORTE						NODO TRAMACO					
AMENAZAS	VULNERABILIDADES	IMPACTO		Prob	Imp	NR	Cos	RIESGO	ACCIÓN	Prob	Imp	NR	Cos	RIESGO	ACCIÓN
Suplantación de identidad	No hay una gestión adecuada de claves de usuario, pues éste podría compartirlas o almacenarlas inadecuadamente.	Cambio no autorizado de configuraciones, violación en la confidencialidad de la información. Peligro de robo y ataques.		3	4	12	2	24	Aplicar controles	3	1	3	1	3	Aceptar el riesgo
	No existe monitoreo de conexión de usuario en puerto correspondiente.														
Modificación de información contenida en los equipos	No existe una política formal de autorización de cambios, migraciones o actualizaciones.	Cambios no autorizados; generación de conflictos entre el personal, por desconocimiento de los cambios.		5	2	10	1	10	Aplicar controles	5	1	5	1	5	Aplicar controles
Divulgación de información	A menudo no se pone en práctica el Acuerdo de Confidencialidad.	Violación a la confidencialidad de la información, mal uso de la información por agentes externos.		3	4	12	2	24	Aplicar controles	3	1	3	2	6	Aceptar el riesgo
	No se aplican las sanciones especificadas en el Acuerdo de Confidencialidad.														
	No se da seguimiento al personal que ha dejado de ejercer sus funciones en la Empresa.														
Error de manejo de la información de activos	No se mantiene clasificada la información.	Información sensible podría verse afectada, pérdida de información crítica.		3	2	6	2	12	Evitar el riesgo	3	1	3	2	6	Aceptar el riesgo
	No toda la información y equipos están etiquetados.														
Daño de equipos por mantenimiento inadecuado	No se tiene una política de mantenimiento periódico de los equipos.	Daño de activos de información, afectando el servicio.		2	4	8	3	24	Aplicar controles	2	1	2	3	6	Aceptar el riesgo
Robo o pérdida de equipos	No hay suficiente control en el ingreso al nodo.	Pérdida económica y falla momentánea en la entrega de servicios.		2	4	8	3	24	Aplicar controles -	2	1	2	3	6	Aceptar el riesgo -
	Bajo nivel de seguridad física														
	No hay un inventario completo de activos.														
	No se ha establecido de manera formal los propietarios de los activos.														

Tabla 4.15: Matriz de Riesgo de Megared Alámbrica (Página 14 de 20)

IDENTIFICACIÓN DE RIESGOS				ANÁLISIS Y EVALUACIÓN DEL RIESGO											
				NODO AUTOFRANCIA NORTE						NODO TRAMACO					
AMENAZAS		VULNERABILIDADES	IMPACTO	Prob	Imp	NR	Cos	RIESGO	ACCIÓN	Prob	Imp	NR	Cos	RIESGO	ACCIÓN
Tecnológicas	Falla en el funcionamiento del *switch* de distribución	No hay un procedimiento formal de contingencia. No hay un procedimiento formal de almacenamiento de configuraciones. Falta de adecuaciones en las instalaciones del nodo.	Falla momentánea en la entrega de servicios a clientes, inoperabilidad de *switches* de acceso u otros *switches* de distribución.	1	4	4	3	12	Aplicar controles *	1	1	1	3	3	Aceptar el riesgo *
	Falla en el funcionamiento de *switch* de acceso o DSLAM	No hay un procedimiento formal de contingencia. No hay un procedimiento formal de almacenamiento de configuraciones. Falta de adecuaciones en las instalaciones del nodo.	Falla momentánea en la entrega de servicios a clientes.	1	4	4	2	8	Aplicar controles *	1	1	1	2	2	Aceptar el riesgo *
	Interferencia provocada entre cables de energía y de comunicaciones	El cableado no ha sido realizado, considerando las separaciones mínimas recomendadas para evitar interferencias.	La calidad en la entrega del servicio no sería óptima, debido a las interferencias; se presentarían pérdidas.	2	2	4	1	4	Aceptar el riesgo	2	1	2	1	2	Aceptar el riesgo
	Virus, caballos troyanos, gusanos, ataques de diccionario	No hay un sistema de detección y monitoreo de amenazas o ataques. No hay suficientes seguridades de bloqueo de amenazas. No se manejan claves seguras en todos los casos. No se instruye regularmente al personal sobre posibles amenazas.	Afectación en la entrega parcial o total de los servicios; violación a la seguridad de la información.	3	4	12	2	24	Aplicar controles	3	1	3	2	6	Aceptar el riesgo
	Negación de servicio (DoS)	No hay sistema de detección de ataques DoS. No existe una política en cuanto a configuración para resguardar los equipos.	Indisponibilidad en la entrega normal de los servicios a uno o varios clientes.	3	4	12	3	36	Aplicar controles	3	1	3	2	6	Aceptar el riesgo

Tabla 4.15: Matriz de Riesgo de Megared Alámbrica (Página 15 de 20)

IDENTIFICACIÓN DE RIESGOS				ANÁLISIS Y EVALUACIÓN DEL RIESGO											
				NODO AUTOFRANCIA NORTE						NODO TRAMACO					
AMENAZAS		VULNERABILIDADES	IMPACTO	Prob	Imp	NR	Cos	RIESGO	ACCIÓN	Prob	Imp	NR	Cos	RIESGO	ACCIÓN
	Inconvenientes de capacidad para proveer servicio	Pese a contar con un ancho de banda considerable, no existe un estudio y análisis al respecto. Número limitado de puertos físicos en los equipos. No hay un análisis actual sobre la capacidad en disco de los servidores	Incapacidad para proporcionar servicio a clientes nuevos o para incrementar la capacidad de los clientes actuales.	2	2	4	1	4	Aceptar el riesgo	2	1	2	1	2	Aceptar el riesgo
	Falla de UPS	No se tiene conocimiento acerca de cortes energéticos no programados. No se tiene una política de mantenimiento periódico de los equipos.	Corte de servicio para todos los clientes.	2	4	8	3	24	Aplicar controles	2	1	2	2	4	Aceptar el riesgo
	Daño en última milla	No se tiene la suficiente seguridad física en los enlaces. No se cuenta con *backups* para todos los enlaces. Accidentes de tránsito pueden afectar a los postes que sostienen el cableado.	Corte de servicio para uno o más clientes.	4	2	8	1	8	Aplicar controles	4	1	4	1	4	Evitar el riesgo
	Daño del equipo de última milla	No se da instructivos a clientes de conservación de equipos. Falta de adecuaciones en las instalaciones del nodo. Malas condiciones eléctricas de las instalaciones del cliente.	Corte de servicio para un cliente.	2	1	2	1	2	Aceptar el riesgo	2	1	2	1	2	Aceptar el riesgo
Ambientales	Incendio	No se dispone de un sistema contra incendios. El nodo no se encuentra en un lugar aislado, puede verse afectado por daños externos.	Daño parcial o total del nodo, junto a los equipos que alberga.	1	4	4	3	12	Aplicar controles	1	1	1	3	3	Aceptar el riesgo
	Filtraciones de agua	Falta de adecuaciones en las instalaciones del nodo.	Daño parcial de equipos.	1	2	2	2	4	Aceptar el riesgo	1	1	1	1	1	Aceptar el riesgo
	Terremoto	Quito está ubicada en una zona áltamente telúrica. No se dispone de una estructura antisísmica.	Daño parcial o total del nodo, junto a los equipos que alberga.	1	4	4	3	12	Aplicar controles	1	1	1	3	3	Aceptar el riesgo

Tabla 4.15: Matriz de Riesgo de Megared Alámbrica (Página 16 de 20)

IDENTIFICACIÓN DE RIESGOS				ANÁLISIS Y EVALUACIÓN NODO PROVEEDOR IÑAQUITO					
AMENAZAS		VULNERABILIDADES	IMPACTO	Prob	Imp	NR	Cos	RIESGO	ACCIÓN
Humanas	Desconfiguración involuntaria de *switch*	No hay una gestión adecuada de claves para configuración, ni una política de privilegios de acceso.	Podría verse afectado el direccionamiento, enrutamiento; incidiendo en la entrega de servicios.	3	2	6	2	12	Evitar el riesgo
		No hay un procedimiento formal de almacenamiento de configuraciones.							
	Desconexión de *switch* o de puertos	No hay control en el ingreso al nodo.	Desconexión de servicio para uno o más clientes.	3	2	6	2	12	Evitar el riesgo
		No hay la protección física adecuada para evitar desconexión.							
		No hay una normativa de instalación o cambio del cableado o de equipos.							
	Ingreso no autorizado al nodo	No hay suficiente control en el ingreso al nodo.	Acciones inapropiadas con los activos, como apagado o desconexión.	4	2	8	2	16	Aplicar controles
		No existe una política formal para el ingreso al nodo, tanto para el personal interno como de terceros.							
		No existe un registro del ingreso o salida de equipos del nodo.							
	Ingreso a la configuración de equipos, de personal no autorizado	No hay un sistema de monitoreo y registro de ingreso a equipos.	Cambio no autorizado de configuración; robo de información o probabilidad de ataques. Se podría afectar en la entrega de servicios a los clientes.	2	3	6	2	12	Evitar el riesgo
		No hay un bloqueo para el acceso a los equipos provenientes de segmentos de red diferentes a los de la Empresa.							
		No existe una política formal de concesión de claves y privilegios de acceso.							
		No existe una política para actualización periódica de claves.							

Tabla 4.15: Matriz de Riesgo de Megared Alámbrica (Página 17 de 20)

IDENTIFICACIÓN DE RIESGOS				ANÁLISIS Y EVALUACIÓN					
				NODO PROVEEDOR IÑAQUITO					
AMENAZAS		VULNERABILIDADES	IMPACTO	Prob	Imp	NR	Cos	RIESGO	ACCIÓN
	Suplantación de identidad	No hay una gestión adecuada de claves de usuario, pues éste podría compartirlas o almacenarlas inadecuadamente. No existe monitoreo de conexión de usuario en puerto correspondiente.	Cambio no autorizado de configuraciones, violación en la confidencialidad de la información. Peligro de robo y ataques.	3	3	9	2	18	Aplicar controles
	Modificación de información contenida en los equipos	No existe una política formal de autorización de cambios, migraciones o actualizaciones.	Cambios no autorizados; generación de conflictos entre el personal, por desconocimiento de los cambios.	5	2	10	1	10	Aplicar controles
	Divulgación de información	A menudo no se pone en práctica el Acuerdo de Confidencialidad. No se aplican las sanciones especificadas en el Acuerdo de Confidencialidad. No se da seguimiento al personal que ha dejado de ejercer sus funciones en la Empresa.	Violación a la confidencialidad de la información, mal uso de la información por agentes externos.	3	3	9	2	18	Aplicar controles
	Error de manejo de la información de activos	No se mantiene clasificada la información. No toda la información y equipos están etiquetados.	Información sensible podría verse afectada, pérdida de información crítica.	1	1	1	2	2	Aceptar el riesgo
	Daño de equipos por mantenimiento inadecuado	No se tiene una política de mantenimiento periódico de los equipos.	Daño de activos de información, afectando el servicio.	2	3	6	3	18	Evitar el riesgo
	Robo o pérdida de equipos	No hay suficiente control en el ingreso al nodo. Bajo nivel de seguridad física No hay un inventario completo de activos. **No se ha establecido de manera formal los propietarios de los activos.**	Pérdida económica y falla momentánea en la entrega de servicios.	1	3	3	3	9	Evitar el riesgo.

Tabla 4.15: Matriz de Riesgo de Megared Alámbrica (Página 18 de 20)

IDENTIFICACIÓN DE RIESGOS				ANÁLISIS Y EVALUACIÓN					
				NODO PROVEEDOR IÑAQUITO					
AMENAZAS		VULNERABILIDADES	IMPACTO	Prob	Imp	NR	Cos	RIESGO	ACCIÓN
Tecnológicas	Falla en el funcionamiento del *switch* de distribución	No hay un procedimiento formal de contingencia. No hay un procedimiento formal de almacenamiento de configuraciones. Falta de adecuaciones en las instalaciones del nodo.	**Falla momentánea en la entrega de servicios a clientes, inoperabilidad de *switches* de acceso u otros *switches* de distribución.**	1	3	3	3	9	Evitar el riesgo -
	Interferencia provocada entre cables de energía y de comunicaciones	El cableado no ha sido realizado, considerando las separaciones mínimas recomendadas para evitar interferencias.	La calidad en la entrega del servicio no sería óptima, debido a las interferencias; se presentarían pérdidas.	1	2	2	1	2	Aceptar el riesgo -
	Virus, caballos troyanos, gusanos, ataques de diccionario	No hay un sistema de detección y monitoreo de amenazas o ataques. No hay suficientes seguridades de bloqueo de amenazas. No se manejan claves seguras en todos los casos. No se instruye regularmente al personal sobre posibles amenazas.	Afectación en la entrega parcial o total de los servicios; violación a la seguridad de la información.	3	3	9	2	18	Aplicar controles
	Negación de servicio (DoS)	No hay sistema de detección de ataques DoS. No existe una política en cuanto a configuración para resguardar los equipos.	Indisponibilidad en la entrega normal de los servicios a uno o varios clientes.	3	3	9	2	18	Aplicar controles
	Inconvenientes de capacidad para proveer servicio	Pese a contar con un ancho de banda considerable, no existe un estudio y análisis al respecto. Número limitado de puertos físicos en los equipos. No hay un análisis actual sobre la capacidad en disco de los servidores	Incapacidad para proporcionar servicio a clientes nuevos o para incrementar la capacidad de los clientes actuales.	1	1	1	1	1	Aceptar el riesgo

Tabla 4.15: Matriz de Riesgo de Megared Alámbrica (Página 19 de 20)

IDENTIFICACIÓN DE RIESGOS				ANÁLISIS Y EVALUACIÓN NODO PROVEEDOR IÑAQUITO					
AMENAZAS		VULNERABILIDADES	IMPACTO	Prob	Imp	NR	Cos	RIESGO	ACCIÓN
	Falla de UPS	No se tiene conocimiento acerca de cortes de energía no programados. No se tiene una política de mantenimiento periódico de los equipos.	Corte de servicio para todos los clientes.	1	3	3	2	6	Evitar el riesgo *
	Daño en última milla	No se tiene la suficiente seguridad física en los enlaces. *No se cuenta con backups para todos los enlaces.* Accidentes de tránsito pueden afectar a los postes que sostienen el cableado.	Corte de servicio para uno o más clientes.	4	1	4	1	4	Evitar el riesgo
	Daño del equipo de última milla	No se da instructivos a clientes de conservación de equipos. Falta de adecuaciones en las instalaciones del nodo. Malas condiciones eléctricas de las instalaciones del cliente.	Corte de servicio para un cliente.	2	1	2	1	2	Aceptar el riesgo *
Ambientales	Incendio	No se dispone de un sistema contra incendios. El nodo no se encuentra en un lugar aislado, puede verse afectado por daños externos.	Daño parcial o total del nodo, junto a los equipos que alberga.	1	3	3	3	9	Evitar el riesgo *
	Filtraciones de agua	Falta de adecuaciones en las instalaciones del nodo.	Daño parcial de equipos.	1	2	2	2	4	Aceptar el riesgo *
	Terremoto	Quito está ubicada en una zona áltamente telúrica. No se dispone de una estructura antisísmica.	Daño parcial o total del nodo, junto a los equipos que alberga.	1	3	3	3	9	Evitar el riesgo *

Tabla 4.15: Matriz de Riesgo de Megared Alámbrica (Página 20 de 20)

IDENTIFICACIÓN DE RIESGOS				ANÁLISIS Y EVALUACIÓN DEL RIESGO											
				NODO LUMBISI						NODO LIBERTAD					
AMENAZAS		VULNERABILIDADES	IMPACTO	Prob	Imp	NR	Cos	RIESGO	ACCIÓN	Prob	Imp	NR	Cos	RIESGO	ACCIÓN
Humanas	Desconfiguración involuntaria del *switch* o radios	No hay una gestión adecuada de claves para configuración, ni una política de privilegios de acceso.	Podría verse afectado el direccionamiento, enrutamiento, incidiendo en la entrega de servicios.	3	3	9	2	18	Aplicar controles	3	2	6	2	12	Evitar el riesgo
		No hay un procedimiento formal de almacenamiento de configuraciones.													
	Desconexión de *switch*, radio o de puertos	No hay control en el ingreso al nodo.	Desconexión de servicio para uno o más clientes.	3	3	9	2	18	Aplicar controles	3	2	6	2	12	Evitar el riesgo
		No hay la protección física adecuada para evitar desconexión.													
		No hay una normativa de instalación o cambio del cableado o de equipos.													
	Ingreso no autorizado al nodo	No hay suficiente control en el ingreso al nodo.	Acciones inapropiadas con los activos, como apagado o desconexión.	5	3	15	2	30	Aplicar controles	5	2	10	2	20	Aplicar controles
		No existe una política formal para el ingreso al nodo, tanto para el personal interno como de terceros.													
		No existe un registro del ingreso o salida de equipos del nodo.													
	Ingreso a la configuración de equipos, de personal no autorizado	No hay un sistema de monitoreo y registro de ingreso a equipos.	Cambio no autorizado de configuración; robo de información o probabilidad de ataques. Se podría afectar en la entrega de servicios a los clientes.	2	4	8	2	16	Aplicar controles	2	3	6	2	12	Evitar el riesgo
		No hay un bloqueo para el acceso a los equipos provenientes de segmentos de red diferentes a los de la Empresa.													
		No existe una política formal de concesión de claves y privilegios de acceso.													
		No existe una política para actualización periódica de claves.													

Tabla 4.16: Matriz de Riesgo de Megared Inalámbrica (Página 1 de 10)

IDENTIFICACIÓN DE RIESGOS			ANÁLISIS Y EVALUACIÓN DEL RIESGO											
			NODO LUMBISI						NODO LIBERTAD					
AMENAZAS	VULNERABILIDADES	IMPACTO	Prob	Imp	NR	Cos	RIESGO	ACCIÓN	Prob	Imp	NR	Cos	RIESGO	ACCIÓN
Suplantación de identidad	No hay una gestión adecuada de claves de usuario, pues éste podría compartirlas o almacenarlas inadecuadamente. No existe monitoreo de conexión de usuario en puerto correspondiente.	Cambio no autorizado de configuraciones, violación en la confidencialidad de la información. Peligro de robo y ataques.	3	4	12	2	24	Aplicar controles	3	3	9	2	18	Aplicar controles
Modificación de información contenida en los equipos	No existe una política formal de autorización de cambios, migraciones o actualizaciones.	Cambios no autorizados; generación de conflictos entre el personal, por desconocimiento de los cambios.	5	2	10	1	10	Aplicar controles	5	1	5	1	5	Aplicar controles
Divulgación de información	A menudo no se pone en práctica el Acuerdo de Confidencialidad. No se aplican las sanciones especificadas en el Acuerdo de Confidencialidad. No se da seguimiento al personal que ha dejado de ejercer sus funciones en la Empresa.	Violación a la confidencialidad de la información, mal uso de la información por agentes externos.	3	4	12	2	24	Aplicar controles	3	3	9	2	18	Aplicar controles
Error de manejo de la información de activos	No se mantiene clasificada la información. No toda la información y equipos están etiquetados.	Información sensible podría verse afectada, pérdida de información crítica.	3	2	6	2	12	Evitar el riesgo	3	1	3	2	6	Aceptar el riesgo
Incumplimiento con la legislación	No se realiza una revisión periódica en cuanto a la regularización de los enlaces. No existe una política formal de autorización de cambios, migraciones o actualizaciones.	Corte de servicio para los clientes asociados al nodo, debido al no cumplimiento de leyes.	2	3	6	2	12	Evitar el riesgo	2	3	6	2	12	Evitar el riesgo
Daño de equipos por mantenimiento inadecuado	No se tiene una política de mantenimiento periódico de los equipos.	Daño de activos de información, afectando el servicio.	2	4	8	4	32	Aplicar controles	2	4	8	4	32	Aplicar controles

Tabla 4.16: Matriz de Riesgo de Megared Inalámbrica (Página 2 de 10)

IDENTIFICACIÓN DE RIESGOS				ANÁLISIS Y EVALUACIÓN DEL RIESGO											
				NODO LUMBISI						NODO LIBERTAD					
AMENAZAS		VULNERABILIDADES	IMPACTO	Prob	Imp	NR	Cos	RIESGO	ACCIÓN	Prob	Imp	NR	Cos	RIESGO	ACCIÓN
	Robo o pérdida de equipos	No hay suficiente control en el ingreso al nodo. Bajo nivel de seguridad física. Debido al tipo de enlace, los equipos (radios y antenas) se encuentran en la parte externa del nodo. No hay un inventario completo de activos. **No se ha establecido de manera formal los propietarios de los activos.**	Pérdida económica y falla momentánea en la entrega de servicios.	3	4	12	4	48	Aplicar controles	3	3	9	4	36	Aplicar controles
Tecnológicas	Falla en el funcionamiento del switch	No hay un procedimiento formal de contingencia. No hay un procedimiento formal de almacenamiento de configuraciones. Falta de adecuaciones en las instalaciones del nodo.	**Falla momentánea en la entrega de servicios a clientes, inoperabilidad de otros *switches* de distribución, debido a la falla del enlace radial.**	1	4	4	3	12	Aplicar controles	1	3	3	2	6	Evitar el riesgo
	Falla en el funcionamiento del radio principal	No hay un procedimiento formal de contingencia. No hay un procedimiento formal de almacenamiento de configuraciones. Debido a la ubicación de los equipos (radios y antenas), éstos se encuentran expuestos a las condiciones atmosféricas.	**Falla momentánea en la entrega de servicios a clientes, inoperabilidad de otros *switches* de distribución, debido a la falla del enlace radial.**	1	4	4	4	16	Aplicar controles	2	3	6	4	24	Evitar el riesgo
	Interferencia en la frecuencia utilizada	Se utilizan bandas de frecuencia no licenciadas para la mayoría de enlaces. No se realiza un barrido de frecuencias periódicamente, para determinar enlaces que trabajen en frecuencias cercanas. Espectro de frecuencia saturado.	Transmisión no óptima de la señal, pérdidas.	3	2	6	2	12	Evitar el riesgo	3	2	6	2	12	Evitar el riesgo

Tabla 4.16: Matriz de Riesgo de Megared Inalámbrica (Página 3 de 10)

IDENTIFICACIÓN DE RIESGOS			ANÁLISIS Y EVALUACIÓN DEL RIESGO											
			NODO LUMBISI						NODO LIBERTAD					
AMENAZAS	VULNERABILIDADES	IMPACTO	Prob	Imp	NR	Cos	RIESGO	ACCIÓN	Prob	Imp	NR	Cos	RIESGO	ACCIÓN
Interferencia provocada entre cables de energía y de comunicaciones	El cableado no ha sido realizado, considerando las separaciones mínimas recomendadas para evitar interferencias.	La calidad en la entrega del servicio no sería óptima, debido a las interferencias; se presentarían pérdidas.	2	2	4	1	4	Aceptar el riesgo	2	2	4	1	4	Aceptar el riesgo
Virus, caballos troyanos, gusanos, ataques de diccionario	No hay un sistema de detección y monitoreo de amenazas o ataques.	Afectación en la entrega parcial o total de los servicios; violación a la seguridad de la información.	3	4	12	2	24	Aplicar controles	3	3	9	2	18	Aplicar controles
	No hay suficientes seguridades de bloqueo de amenazas.													
	No se manejan claves seguras en todos los casos.													
	No se instruye regularmente al personal sobre posibles amenazas.													
Negación de servicio (DoS)	No hay sistema de detección de ataques DoS.	Indisponibilidad en la entrega normal de los servicios a uno o varios clientes.	3	4	12	2	24	Aplicar controles	3	3	9	2	18	Aplicar controles
	No existe una política en cuanto a configuración para resguardar los equipos.													
Inconvenientes de capacidad para proveer servicio	Pese a contar con un ancho de banda considerable, no existe un estudio y análisis al respecto.	Incapacidad para proporcionar servicio a posibles clientes nuevos o para incrementar la capacidad actual de los clientes.	2	2	4	1	4	Aceptar el riesgo	2	2	4	1	4	Aceptar el riesgo
	Número limitado de puertos físicos en los equipos.													
	Espectro de frecuencia saturado.													
	No hay un análisis actual sobre la capacidad en disco de los servidores													

Tabla 4.16: Matriz de Riesgo de Megared Inalámbrica (Página 4 de 10)

IDENTIFICACIÓN DE RIESGOS				ANÁLISIS Y EVALUACIÓN DEL RIESGO											
				NODO LUMBISI						NODO LIBERTAD					
AMENAZAS		VULNERABILIDADES	IMPACTO	Prob	Imp	NR	Cos	RIESGO	ACCIÓN	Prob	Imp	NR	Cos	RIESGO	ACCIÓN
	Falla de UPS	No se tiene conocimiento acerca de cortes de energía no programados. Dificultad en el acceso para el ingreso de un generador. No se tiene una política de mantenimiento periódico de los equipos.	Corte de servicio para todos los clientes.	2	4	8	3	24	Aplicar controles.	2	3	6	3	18	Evitar el riesgo.
	Daño del equipo de última milla	No se da instructivos a los clientes de cómo cuidar los equipos. Debido a la ubicación de los equipos (radios y antenas), éstos se encuentran expustos a las condiciones atmosféricas. Malas condiciones eléctricas de las instalaciones del cliente.	Corte de servicio para un cliente.	2	1	2	2	4	Aceptar el riesgo.	2	1	2	2	4	Aceptar el riesgo.
Ambientales	Incendio	No se dispone de un sistema contra incendios. Puede ser afectado por incendios provocados.	Daño parcial o total del nodo, junto a los equipos que alberga.	1	4	4	4	16	Aplicar controles.	1	3	3	4	12	Evitar el riesgo.
	Filtraciones de agua	Falta de adecuaciones en las instalaciones del nodo.	Daño parcial de equipos.	2	2	4	3	12	Aceptar el riesgo.	2	2	4	2	8	Aceptar el riesgo.
	Terremoto	Quito está ubicada en una zona altamente telúrica. No se dispone de una estructura antisísmica.	Daño parcial o total del nodo, junto a los equipos que alberga.	1	4	4	4	16	Aplicar controles.	1	3	3	4	12	Evitar el riesgo.
	Deslaves	Ubicación geográfica del nodo (lomas o montañas)	Daño parcial o total del nodo, junto a los equipos que alberga.	1	4	4	4	16	Aplicar controles.	1	3	3	4	12	Evitar el riesgo.
	Tormentas eléctricas	No se da una revisión periódica del funcionamiento del pararayos. Se desconoce sobre el estado del sistema de puesta a tierra.	Daño parcial o total del nodo, junto a los equipos que alberga.	1	4	4	4	16	Aplicar controles.	1	3	3	4	12	Evitar el riesgo.

Tabla 4.16: Matriz de Riesgo de Megared Inalámbrica (Página 5 de 10)

IDENTIFICACIÓN DE RIESGOS				ANÁLISIS Y EVALUACIÓN DEL RIESGO											
				NODO CARRETAS						NODO GUAMANÍ					
AMENAZAS		VULNERABILIDADES	IMPACTO	Prob	Imp	NR	Cos	RIESGO	ACCIÓN	Prob	Imp	NR	Cos	RIESGO	ACCIÓN
Humanas	Desconfiguración involuntaria del *switch* o radios	No hay una gestión adecuada de claves para configuración, ni una política de privilegios de acceso.	Podría verse afectado el direccionamiento, enrutamiento, incidiendo en la entrega de servicios.	3	2	6	2	12	Evitar el riesgo	3	1	3	1	3	Aceptar el riesgo
		No hay un procedimiento formal de almacenamiento de configuraciones.													
	Desconexión de *switch*, radio o de puertos	No hay control en el ingreso al nodo.	Desconexión de servicio para uno o más clientes.	3	2	6	2	12	Evitar el riesgo	3	1	3	1	3	Aceptar el riesgo
		No hay la protección física adecuada para evitar desconexión.													
		No hay una normativa de instalación o cambio del cableado o de equipos.													
	Ingreso no autorizado al nodo	No hay suficiente control en el ingreso al nodo.	Acciones inapropiadas con los activos, como apagado o desconexión.	5	2	10	2	20	Aplicar controles	5	1	5	1	5	Aplicar controles
		No existe una política formal para el ingreso al nodo, tanto para el personal interno como de terceros.													
		No existe un registro del ingreso o salida de equipos del nodo.													
	Ingreso a la configuración de equipos, de personal no autorizado	No hay un sistema de monitoreo y registro de ingreso a equipos.	Cambio no autorizado de configuración; robo de información o probabilidad de ataques. Se podría afectar en la entrega de servicios a los clientes.	2	3	6	2	12	Evitar el riesgo	2	2	4	1	4	Aceptar el riesgo
		No hay un bloqueo para el acceso a los equipos provenientes de segmentos de red diferentes a los de la Empresa.													
		No existe una política formal de concesión de claves y privilegios de acceso.													
		No existe una política para actualización periódica de claves.													

Tabla 4.16: Matriz de Riesgo de Megared Inalámbrica (Página 6 de 10)

IDENTIFICACIÓN DE RIESGOS			ANÁLISIS Y EVALUACIÓN DEL RIESGO											
			NODO CARRETAS						NODO GUAMANÍ					
AMENAZAS	VULNERABILIDADES	IMPACTO	Prob	Imp	NR	Cos	RIESGO	ACCIÓN	Prob	Imp	NR	Cos	RIESGO	ACCIÓN
Suplantación de identidad	No hay una gestión adecuada de claves de usuario, pues éste podría compartirlas o almacenarlas inadecuadamente. No existe monitoreo de conexión de usuario en puerto correspondiente.	Cambio no autorizado de configuraciones, violación en la confidencialidad de la información. Peligro de robo y ataques.	3	3	9	2	18	Aplicar controles	3	2	6	1	6	Evitar el riesgo
Modificación de información contenida en los equipos	No existe una política formal de autorización de cambios, migraciones o actualizaciones.	Cambios no autorizados; generación de conflictos entre el personal, por desconocimiento de los cambios.	5	1	5	1	5	Aplicar controles	5	1	5	1	5	Aplicar controles
Divulgación de información	A menudo no se pone en práctica el Acuerdo de Confidencialidad. No se aplican las sanciones especificadas en el Acuerdo de Confidencialidad. No se da seguimiento al personal que ha dejado de ejercer sus funciones en la Empresa.	Violación a la confidencialidad de la información, mal uso de la información por agentes externos.	3	3	9	2	18	Aplicar controles	3	2	6	1	6	Evitar el riesgo
Error de manejo de la información de activos	No se mantiene clasificada la información. No toda la información y equipos están etiquetados.	Información sensible podría verse afectada, pérdida de información crítica.	2	1	2	2	4	Aceptar el riesgo	2	1	2	2	4	Aceptar el riesgo
Incumplimiento con la legislación	No se realiza una revisión periódica en cuanto a la regularización de los enlaces. No existe una política formal de autorización de cambios, migraciones o actualizaciones.	Corte de servicio para los clientes asociados al nodo, debido al no cumplimiento de leyes.	2	3	6	2	12	Evitar el riesgo	2	2	4	2	8	Aceptar el riesgo
Daño de equipos por mantenimiento inadecuado	No se tiene una política de mantenimiento periódico de los equipos.	Daño de activos de información, afectando el servicio.	2	3	6	2	12	Evitar el riesgo	2	2	4	3	12	Aceptar el riesgo

Tabla 4.16: Matriz de Riesgo de Megared Inalámbrica (Página 7 de 10)

IDENTIFICACIÓN DE RIESGOS				ANÁLISIS Y EVALUACIÓN DEL RIESGO											
				NODO CARRETAS						NODO GUAMANÍ					
AMENAZAS		VULNERABILIDADES	IMPACTO	Prob	Imp	NR	Cos	RIESGO	ACCIÓN	Prob	Imp	NR	Cos	RIESGO	ACCIÓN
Tecnológicas	Robo o pérdida de equipos	No hay suficiente control en el ingreso al nodo.	Pérdida económica y falla momentánea en la entrega de servicios.	2	3	6	2	12	Evitar el riesgo	3	2	6	3	18	Evitar el riesgo
		Bajo nivel de seguridad física.													
		Debido al tipo de enlace, los equipos (radios y antenas) se encuentran en la parte externa del nodo.													
		No hay un inventario completo de activos.													
		No se ha establecido de manera formal los propietarios de los activos.													
	Falla en el funcionamiento del switch	No hay un procedimiento formal de contingencia.	**Falla momentánea en la entrega de servicios a clientes, inoperabilidad de otros *switches* de distribución, debido a la falla del enlace radial.**	1	3	3	2	6	Evitar el riesgo	1	2	2	2	4	Aceptar el riesgo
		No hay un procedimiento formal de almacenamiento de configuraciones.													
		Falta de adecuaciones en las instalaciones del nodo.													
	Falla en el funcionamiento del radio principal	No hay un procedimiento formal de contingencia.	**Falla momentánea en la entrega de servicios a clientes, inoperabilidad de otros *switches* de distribución, debido a la falla del enlace radial.**	2	3	6	3	18	Evitar el riesgo	-	-	-	-	-	
		No hay un procedimiento formal de almacenamiento de configuraciones.													
		Debido a la ubicación de los equipos (radios y antenas), éstos se encuentran expuestos a las condiciones atmosféricas.													
	Interferencia en la frecuencia utilizada	Se utilizan bandas de frecuencia no licenciadas para la mayoría de enlaces.	Transmisión no óptima de la señal, pérdidas.	3	2	6	2	12	Evitar el riesgo	2	2	4	2	8	Aceptar el riesgo
		No se realiza un barrido de frecuencias periódicamente, para determinar enlaces que trabajen en frecuencias cercanas.													
		Espectro de frecuencia saturado.													

Tabla 4.16: Matriz de Riesgo de Megared Inalámbrica (Página 8 de 10)

IDENTIFICACIÓN DE RIESGOS			ANÁLISIS Y EVALUACIÓN DEL RIESGO											
			NODO CARRETAS						NODO GUAMANÍ					
AMENAZAS	VULNERABILIDADES	IMPACTO	Prob	Imp	NR	Cos	RIESGO	ACCIÓN	Prob	Imp	NR	Cos	RIESGO	ACCIÓN
Interferencia provocada entre cables de energía y de comunicaciones	El cableado no ha sido realizado, considerando las separaciones mínimas recomendadas para evitar interferencias.	La calidad en la entrega del servicio no sería óptima, debido a las interferencias; se presentarían pérdidas.	2	2	4	1	4	Aceptar el riesgo	2	2	4	1	4	Aceptar el riesgo
Virus, caballos troyanos, gusanos, ataques de diccionario	No hay un sistema de detección y monitoreo de amenazas o ataques.	Afectación en la entrega parcial o total de los servicios; violación a la seguridad de la información.	3	3	9	2	18	Aplicar controles	3	2	6	2	12	Evitar el riesgo
	No hay suficientes seguridades de bloqueo de amenazas.													
	No se manejan claves seguras en todos los casos.													
	No se instruye regularmente al personal sobre posibles amenazas.													
Negación de servicio (DoS)	No hay sistema de detección de ataques DoS.	Indisponibilidad en la entrega normal de los servicios a uno o varios clientes.	3	3	9	2	18	Aplicar controles	3	2	6	2	12	Evitar el riesgo
	No existe una política en cuanto a configuración para resguardar los equipos.													
Inconvenientes de capacidad para proveer servicio	Pese a contar con un ancho de banda considerable, no existe un estudio y análisis al respecto.	Incapacidad para proporcionar servicio a posibles clientes nuevos o para incrementar la capacidad actual de los clientes.	2	2	4	1	4	Aceptar el riesgo	2	1	2	1	2	Aceptar el riesgo
	Número limitado de puertos físicos en los equipos.													
	Espectro de frecuencia saturado.													
	No hay un análisis actual sobre la capacidad en disco de los servidores													

Tabla 4.16: Matriz de Riesgo de Megared Inalámbrica (Página 9 de 10)

IDENTIFICACIÓN DE RIESGOS				ANÁLISIS Y EVALUACIÓN DEL RIESGO											
				NODO CARRETAS						NODO GUAMANÍ					
AMENAZAS		VULNERABILIDADES	IMPACTO	Prob	Imp	NR	Cos	RIESGO	ACCIÓN	Prob	Imp	NR	Cos	RIESGO	ACCIÓN
	Falla de UPS	No se tiene conocimiento acerca de cortes de energía no programados.	Corte de servicio para todos los clientes.	2	3	6	2	12	Evitar el riesgo.	2	2	4	2	8	Aceptar el riesgo.
		Difilcultad en el acceso para el ingreso de un generador.													
		No se tiene una política de mantenimiento periódico de los equipos.													
	Daño del equipo de última milla	No se da instructivos a los clientes de cómo cuidar los equipos.	Corte de servicio para un cliente.	2	1	2	2	4	Aceptar el riesgo.	2	1	2	2	4	Aceptar el riesgo.
		Debido a la ubicación de los equipos (radios y antenas), éstos se encuentran expuestos a las condiciones atmosféricas.													
		Malas condiciones eléctricas de las instalaciones del cliente.													
Ambientales	Incendio	No se dispone de un sistema contra incendios.	Daño parcial o total del nodo, junto a los equipos que alberga.	1	3	3	2	6	Evitar el riesgo.	1	2	2	3	6	Aceptar el riesgo.
		Puede ser afectado por incendios provocados.													
	Filtraciones de agua	Falta de adecuaciones en las instalaciones del nodo.	Daño parcial de equipos.	2	2	4	2	8	Aceptar el riesgo.	2	1	2	2	4	Aceptar el riesgo.
	Terremoto	Quito está ubicada en una zona altamente telúrica.	Daño parcial o total del nodo, junto a los equipos que alberga.	1	3	3	2	6	Evitar el riesgo.	1	2	2	3	6	Aceptar el riesgo.
		No se dispone de una estructura antisísmica.													
	Deslaves	Ubicación geográfica del nodo (lomas o montañas)	Daño parcial o total del nodo, junto a los equipos que alberga.	1	3	3	2	6	Evitar el riesgo.	1	2	2	3	6	Aceptar el riesgo.
	Tormentas eléctricas	No se da una revisión periódica del funcionamiento del pararrayos.	Daño parcial o total del nodo, junto a los equipos que alberga.	1	3	3	3	9	Evitar el riesgo.	1	2	2	2	4	Aceptar el riesgo.
		Se desconoce sobre el estado del sistema de puesta a tierra.													

Tabla 4.16: Matriz de Riesgo de Megared Inalámbrica (Página 10 de 10)

* Amenazas que dependiendo el caso, podrían corresponder a Transferir el Riesgo. La transferencia se produciría a los proveedores o aseguradoras.

4.3.6 TRATAMIENTO DE LOS RIESGOS

En la parte final de las Tablas 4.14, 4.15 y 4.16, en base a la metodología presentada en el Documento A.3, se determina el tratamiento de cada riesgo o acción a tomar en caso de que éste se presente.

4.3.6.1 Centro de Datos

Como se puede observar, en la mayoría de casos se requiere la aplicación de controles, pues en general se detectan altos niveles de impacto.

En los casos que implican activos con NI Moderado, se obtiene como tratamiento, la evitación o aceptación de los riesgos.

4.3.6.2 Megared Alámbrica

Los resultados obtenidos, señalan que las amenazas en los nodos de Megared Alámbrica, deberían ser tratadas con aplicación de controles, evitación de riesgos y aceptación de riesgos; sin embargo, debido a que la mayoría de activos corresponden a NI Moderado, se observa más presencia de evitación o aceptación de riesgos que en el Centro de Datos.

Al igual que en el Centro de Datos, se debe optar por transferir el riesgo, en caso de que la amenaza sea responsabilidad de entes externos, como proveedores o aseguradoras.

4.3.6.3 Megared Inalámbrica

Se observa mayor necesidad de aplicación de controles que en Megared Alámbrica; esto se debe principalmente a que la probabilidad de ocurrencia de las amenazas es superior, dado que el medio inalámbrico es más vulnerable que el alámbrico. La razón para obtener evitación o aceptación de controles, se debe

principalmente a que el impacto es bajo, pues se asocia a menos clientes que en el Centro de Datos o en Megared Alámbrica.

Se debe transferir el riesgo cuando el compromiso de la amenaza esté bajo la responsabilidad de entes externos.

4.3.7 SELECCIÓN DE OBJETIVOS DE CONTROL Y CONTROLES

Documento A.5

Una vez obtenido el tratamiento de riesgo para cada amenaza identificada, se procede a seleccionar los objetivos de control y controles más adecuados de la Norma ISO 27001.

Se presentan los objetivos de control y controles seleccionados en la Tabla 4.17.

El mismo objetivo de control y los mismos controles, son adecuados para el tratamiento de distintas amenazas, como se observa en la Tabla 4.17. Además, se observa que para el tratamiento de una amenaza existen varios objetivos de control y controles que eficazmente contribuirían a su mitigación; por esta razón se considerarán varios controles para una misma amenaza.

En la Tabla 4.18 se presentan más objetivos de control y controles, considerados como fundamentales, una vez que se aplique el Sistema de Gestión de Seguridad de la Información. Dichos controles podrían ser aplicables para el tratamiento de todas las amenazas identificadas.

SELECCIÓN DE OBJETIVOS DE CONTROL Y CONTROLES						
AMENAZA		**ACCIÓN**	**OBJETIVO DE CONTROL**		**CONTROL**	
Humana	Desconfiguración involuntaria de *switch* o *router*	Aplicar controles Evitar el riesgo	7,1	Responsabilidad por los activos.	7.1.3	Uso aceptable de los recursos.
			9,2	Seguridad del equipo.	9.2.3	Seguridad en el cableado.
			10,1	Procedimientos y responsabilidades operacionales.	10.1.4	Separación de los medios de desarrollo y operacionales.
			10,5	Respaldo (*backup*).	10.5.1	*Backup* o respaldo de la información.
			10,6	Gestión de seguridad de redes.	10.6.1	Controles de red.
			11,2	Gestión del acceso del usuario.	11.2.3	Gestión de la clave del usuario.
			11,3	Responsabilidades del usuario.	11.3.2	Equipo de usuario desatendido.
					11.3.3	Política de pantalla y escritorio limpio.
			11,4	Control de acceso a redes.	11.4.3	Identificación del equipo en red.
					11.4.4	Protección del puerto de diagnóstico remoto.
					11.4.5	Segregación en redes.
					11.4.6	Control de conexión de redes.
			12,2	Procesamiento correcto en las aplicaciones.	12.2.1	Validación de data de Insumo.
			12,3	Controles criptográficos.	12.3.1	Política sobre el uso de controles criptográficos.
					12.3.2	Gestión de claves.
			15,1	Cumplimiento con requerimientos legales.	15.1.6	Regulación de controles criptográficos.
	Desconexión de puertos, *switch* o *router*	Aplicar controles Evitar el riesgo	9,1	Áreas seguras.	9.1.1	Perímetro de seguridad física.
					9.1.2	Controles físicos de entrada.
					9.1.3	Seguridad de oficinas, habitaciones y medios.
			9,2	Seguridad del equipo.	9.2.3	Seguridad en el cableado.

Tabla 4.17: Selección de Objetivos de Control y Controles (Página 1 de 14)

SELECCIÓN DE OBJETIVOS DE CONTROL Y CONTROLES						
AMENAZA		ACCIÓN	OBJETIVO DE CONTROL		CONTROL	
	Ingreso a la configuración de equipos, de personal no autorizado	Aplicar controles Evitar el riesgo Aceptar el riesgo	6,2	Entidades externas.	6.2.2	Tratamiento de riesgos relacionados con entidades externas.
			7,1	Responsabilidades por los activos.	7.1.3	Uso aceptable de los activos.
			8,3	Terminación o cambio del empleo.	8.3.3	Eliminación de derechos de acceso.
			9,2	Seguridad del equipo.	9.2.3	Seguridad en el cableado.
			10,1	Procesamiento y responsabilidades operacionales.	10.1.1	Procedimientos de operación documentados.
			10,6	Gestión de seguridad de redes.	10.6.1	Controles de red.
			10,7	Gestión de medios.	10.7.4	Seguridad de documentación del sistema.
			10,8	Intercambio de información.	10.8.1	Procedimientos y políticas de información y software.
			11,1	Requerimiento comercial para el control del acceso.	11.1.1	Política de control de acceso.
			11,2	Gestión del acceso del usuario.	11.2.1	Inscripción del usuario.
					11.2.2	Gestión de privilegios.
					11.2.3	Gestión de la clave del usuario.
					11.2.4	Revisión de los derechos de acceso del usuario.
			11,3	Responsabilidades del usuario.	11.3.1	Uso de clave.
					11.3.2	Equipo de usuario desatendido.
					11.3.3	Política de pantalla y escritorio limpio.
			11,4	Control de acceso a redes.	11.4.1	Política sobre el uso de servicios en red.
					11.4.2	Autenticación del usuario para conexiones externas.
					11.4.3	Identificación del equipo en red.
					11.4.4	Protección del puerto de diagnóstico remoto.
					11.4.5	Segregación en redes.
					11.4.6	Control de conexión de redes.
					11.4.7	Control de *routing* de redes.

Tabla 4.17: Selección de Objetivos de Control y Controles (Página 2 de 14)

SELECCIÓN DE OBJETIVOS DE CONTROL Y CONTROLES						
AMENAZA		ACCIÓN	OBJETIVO DE CONTROL		CONTROL	
			11,5	Control de acceso al sistema de operación.	11.5.1	Procedimientos de registro en el terminal.
					11.5.2	Identificación y autenticación del usuario.
					11.5.3	Sistema de gestión de claves.
					11.5.5	Sesión inactiva.
					11.5.6	Limitación de tiempo de conexión.
			11,6	Control de acceso a la aplicación e información.	11.6.1	Restricción al acceso a la información.
			12,2	Procesamiento correcto en las aplicaciones.	12.2.3	Integridad del mensaje.
			12,3	Controles criptográficos.	12.3.1	Política sobre el uso de controles criptográficos.
					12.3.2	Gestión de claves.
			12,4	Seguridad de los archivos del sistema.	12.4.3	Control de acceso al código fuente del programa
	Ingreso no autorizado a Centro de Datos	Aplicar controles	6,2	Entidades externas.	6.2.1	Identificación de riesgos relacionados con entidades externas.
					6.2.3	Tratamiento de la seguridad en contratos con terceras partes.
			8,2	Durante el empleo.	8.2.1	Gestión de responsabilidades.
					8.2.3	Proceso disciplinario.
			8,3	Terminación o cambio del empleo.	8.3.3	Eliminación de derechos de acceso.
			9,1	Áreas seguras.	9.1.1	Perímetro de seguridad física.
					9.1.2	Controles de entrada físicos.
					9.1.3	Seguridad de oficinas, habitaciones y medios.
					9.1.5	Trabajo en áreas seguras.
					9.1.6	Áreas de acceso público, entrega y carga.
			9,2	Seguridad del equipo.	9.2.1	Ubicación y protección del equipo.
					9.2.3	Seguridad en el cableado.

Tabla 4.17: Selección de Objetivos de Control y Controles (Página 3 de 14)

SELECCIÓN DE OBJETIVOS DE CONTROL Y CONTROLES						
AMENAZA		ACCIÓN	OBJETIVO DE CONTROL		CONTROL	
			11,1	Requerimiento comercial para el control del acceso.	11.1.1	Política de control de acceso.
			11,2	Gestión del acceso del usuario.	11.2.4	Revisión de los derechos de acceso del usuario.
			11,5	Control de acceso al sistema de operación.	11.5.2	Identificación y autenticación del usuario.
			11,6	Control de acceso a la aplicación e información.	11.6.2	Aislamiento del sistema sensible.
	Ingreso no autorizado al nodo	Aplicar controles	6,2	Entidades externas.	6.2.1	Identificación de riesgos relacionados con entidades externas.
					6.2.3	Tratamiento de la seguridad en contratos con terceras partes.
			8,2	Durante el empleo.	8.2.1	Gestión de responsabilidades.
					8.2.3	Proceso disciplinario.
			8,3	Terminación o cambio del empleo.	8.3.3	Eliminación de derechos de acceso.
			9,1	Áreas seguras.	9.1.1	Perímetro de seguridad física.
					9.1.2	Controles de entrada físicos.
					9.1.3	Seguridad de oficinas, habitaciones y medios.
					9.1.5	Trabajo en áreas seguras.
					9.1.6	Áreas de acceso público, entrega y carga.
			9,2	Seguridad del equipo.	9.2.1	Ubicación y protección del equipo.
					9.2.3	Seguridad en el cableado.
			11,1	Requerimiento comercial para el control del acceso.	11.1.1	Política de control de acceso.
			11,2	Gestión del acceso del usuario.	11.2.4	Revisión de los derechos de acceso del usuario.
			11,5	Control de acceso al sistema de operación.	11.5.2	Identificación y autenticación del usuario.
			11,6	Control de acceso a la aplicación e información.	11.6.2	Aislamiento del sistema sensible.

Tabla 4.17: Selección de Objetivos de Control y Controles (Página 4 de 14)

SELECCIÓN DE OBJETIVOS DE CONTROL Y CONTROLES						
AMENAZA		ACCIÓN	OBJETIVO DE CONTROL		CONTROL	
	Suplantación de identidad	Aplicar controles Evitar el riesgo Aceptar el riesgo	8,2	Durante el empleo.	8.2.3	Proceso disciplinario.
			10,6	Gestión de seguridad de redes.	10.6.1	Controles de red.
			10,8	Intercambio de información.	10.8.1	Procedimientos y políticas de información y software.
			11,2	Gestión del acceso del usuario.	11.2.3	Gestión de la clave del usuario.
			11,3	Responsabilidades del usuario.	11.3.1	Uso de clave.
					11.3.2	Equipo de usuario desatendido.
					11.3.3	Política de pantalla y escritorio limpio.
			11,4	Control de acceso a redes.	11.4.2	Autenticación del usuario para conexiones externas.
					11.4.7	Control de *routing* de redes.
			11,5	Control de acceso al sistema de operación.	11.5.2	Identificación y autenticación del usuario.
					11.5.3	Sistema de gestión de claves.
	Modificación de información contenida en los equipos	Aplicar controles	6,1	Organización interna.	6.1.4	Proceso de autorización para los medios de procesamiento de información.
			7,1	Responsabilidad por los activos.	7.1.3	Uso aceptable de los activos.
			8,2	Durante el empleo.	8.2.3	Proceso disciplinario.
			9,2	Seguridad del equipo.	9.2.7	Traslado de propiedad.
			10,1	Procedimientos y responsabilidades operacionales.	10.1.1	Procedimientos de operación documentados.
					10.1.2	Gestión de cambio.
					10.1.3	Segregación de deberes.
			10,3	Planeación y aceptación del sistema.	10.3.2	Aceptación del sistema
			10,8	Intercambio de información.	10.8.1	Procedimientos y políticas de información y software.
					10.8.4	Mensajes electrónicos.
			10.10	Monitoreo.	10.10.3	Protección de la información del registro.

Tabla 4.17: Selección de Objetivos de Control y Controles (Página 5 de 14)

SELECCIÓN DE OBJETIVOS DE CONTROL Y CONTROLES						
AMENAZA		ACCIÓN	OBJETIVO DE CONTROL		CONTROL	
			11.4	Control de acceso a redes.	11.4.1	Política sobre el uso de servicios en red.
					11.4.4	Protección del puerto de diagnóstico remoto.
			11.5	Control de acceso al sistema de operación.	11.5.2	Identificación y autenticación del usuario.
					11.5.3	Sistema de gestión de claves.
					11.5.4	Uso de utilidades del sistema.
					11.5.5	Sesión inactiva.
					11.5.6	Limitación de tiempo de conexión.
			11.6	Control de acceso a la aplicación e información.	11.6.1	Restricción al acceso a la información.
			12.4	Seguridad de los archivos del sistema.	12.4.1	Control de software operacional.
					12.4.2	Protección de la data de prueba del sistema.
					12.4.3	Control de acceso al código fuente del programa.
			12.5	Seguridad en los procesos de desarrollo y soporte.	12.5.1	Procedimientos de control de cambio.
					12.5.2	Revisión técnica de aplicaciones después de cambios en el sistema operativo.
					12.5.3	Restricciones sobre los cambios en los paquetes de software.
	Divulgación de información	Aplicar controles Evitar el riesgo Aceptar el riesgo	6.1	Organización interna.	6.1.5	Acuerdos de confidencialidad.
			8.1	Antes del empleo.	8.1.2	Selección
			8.2	Durante el empleo.	8.2.1	Gestión de responsabilidades.
					8.2.2	Capacitación y educación en seguridad de la información.
					8.2.3	Proceso disciplinario.
			8.3	Terminación o cambio del empleo.	8.3.1	Responsabilidades de terminación.
			9.2	Seguridad del equipo.	9.2.6	Eliminación segura o re-uso de equipo.

Tabla 4.17: Selección de Objetivos de Control y Controles (Página 6 de 14)

SELECCIÓN DE OBJETIVOS DE CONTROL Y CONTROLES						
AMENAZA		ACCIÓN	OBJETIVO DE CONTROL		CONTROL	
			10,7	Gestión de medios.	10.7.1	Gestión de los medios removibles.
					10.7.2	Eliminación de medios.
					10.7.3	Procedimientos de manejo de la información.
					10.7.4	Seguridad de documentación del sistema.
			10,8	Intercambio de información.	10.8.1	Procedimientos y políticas de información y software.
					10.8.2	Acuerdos de intercambio.
					10.8.4	Mensajes electrónicos.
			10.10	Monitoreo.	10.10.3	Protección de la información del registro.
			11.2	Gestión del acceso del usuario.	11.2.3	Gestión de la clave del usuario.
			11.3	Responsabilidades del usuario.	11.3.1	Uso de clave.
			12.3	Controles criptográficos.	12.3.1	Política sobre el uso de controles criptográficos.
			12.5	Seguridad en los procesos de desarrollo y soporte.	12.5.4	Filtración de información.
	Error de manejo de la información de activos	Aplicar controles Evitar el riesgo Aceptar el riesgo	7.2	Clasificación de la información.	7.2.1	Lineamientos de clasificación.
					7.2.2	Etiquetado y manejo de la información.
			9.2	Seguridad del equipo.	9.2.1	Ubicación y protección del equipo.
					9.2.3	Seguridad en el cableado.
					9.2.6	Eliminación segura o re-uso de equipo.
			10.7	Gestión de medios.	10.7.1	Gestión de los medios removibles.
					10.7.3	Procedimientos de manejo de la información.
			10.8	Intercambio de información.	10.8.1	Procedimientos y políticas de información y software.
			12.2	Procesamiento correcto en las aplicaciones.	12.2.1	Validación de data de Insumo.
					12.2.2	Control de procesamiento interno.
					12.2.4	Validación de data de *output*.

Tabla 4.17: Selección de Objetivos de Control y Controles (Página 7 de 14)

SELECCIÓN DE OBJETIVOS DE CONTROL Y CONTROLES						
AMENAZA		ACCIÓN	OBJETIVO DE CONTROL		CONTROL	
			15.1	Cumplimiento con requerimientos legales.	15.1.5	Prevención de mal uso de medios de procesamiento de información.
	Daño de equipos por mantenimiento inadecuado	Aplicar controles Evitar el riesgo Aceptar el riesgo	9.2	Seguridad del equipo.	9.2.4	Mantenimiento de equipo.
	Incumplimiento con la legislación	Evitar el riesgo Aceptar el riesgo	6.1	Organización interna.	6.1.3	Asignación de responsabilidades de la S.I.
			6.2	Entidades externas.	6.2.1	Identificación de riesgos relacionados con entidades externas.
					6.2.3	Tratamiento de la seguridad en contratos con terceras partes.
			8.2	Durante el empleo.	8.2.1	Gestión de responsabilidades.
			12.2	Procesamiento correcto en las aplicaciones.	12.2.4	Validación de data de output.
			15.1	Cumplimiento con requerimientos legales.	15.1.1	Identificación de legislación aplicable.
	Robo o pérdida de equipos e información	Aplicar controles Evitar el riesgo Aceptar el riesgo *	7.1	Responsabilidades por los activos.	7.1.1	Inventarios de activos.
					7.1.2	Propiedad de los activos.
			8.1	Antes del empleo.	8.1.1	Roles y responsabilidades.
					8.1.3	Términos y condiciones de empleo.
			8.2	Durante el empleo.	8.2.3	Proceso disciplinario.
			8.3	Terminación o cambio del empleo.	8.3.2	Devolución de activos.
			10.5	Respaldo (*backup*).	10.5.1	Backup o respaldo de la información.
			10.7	Gestión de medios.	10.7.1	Gestión de los medios removibles.
					10.7.2	Eliminación de medios.
					10.7.3	Procedimientos de manejo de la información.

Tabla 4.17: Selección de Objetivos de Control y Controles (Página 8 de 14)

SELECCIÓN DE OBJETIVOS DE CONTROL Y CONTROLES						
AMENAZA		ACCIÓN	OBJETIVO DE CONTROL		CONTROL	
			10.8	Intercambio de información.	10.8.1	Procedimientos y políticas de información y software.
					10.8.4	Mensajes electrónicos.
			11.3	Responsabilidades del usuario.	11.3.1	Uso de clave.
			12.3	Controles criptográficos.	12.3.1	Política sobre el uso de controles criptográficos.
			12.5	Seguridad en los procesos de desarrollo y soporte.	12.5.4	Filtración de información.
			14.1	Aspectos de la seguridad de la información de la gestión de la continuidad comercial.	14.1.1	Incluir S.I. en el proceso de gestión de continuidad comercial.
					14.1.2	Continuidad comercial y evaluación del riesgo.
					14.1.3	Desarrollar e implementar planes de continuidad incluyendo S.I.
					14.1.4	Marco referencial para la planeación de la continuidad comercial.
					14.1.5	Prueba, mantenimiento y re-evaluación de planes de continuidad comerciales.
			15.1	Cumplimiento con requerimientos legales.	15.1.3	Protección de los registros organizacionales.
					15.1.4	Protección de data y privacidad de información personal.
					15.1.6	Regulación de controles criptográficos.
Tecnológica	Falla de servicio de proveedores	Aplicar controles *	10.2	Gestión de la entrega del servicio de terceros.	10.2.1	Entrega del servicio.
					10.2.2	Monitoreo y revisión de los servicios de terceros.
					10.2.3	Manejar los cambios en los servicios de terceros.
			10.6	Gestión de seguridad de redes.	10.6.2	Seguridad de los servicios de red.
			12.5	Seguridad en los procesos de desarrollo y soporte.	12.5.5	Desarrollo de software contratado externamente.
			12.6	Gestión de vulnerabilidad técnica.	12.6.1	Control de vulnerabilidades técnicas.
			15.1	Cumplimiento con requerimientos legales.	15.1.1	Identificación de legislación aplicable.

Tabla 4.17: Selección de Objetivos de Control y Controles (Página 9 de 14)

SELECCIÓN DE OBJETIVOS DE CONTROL Y CONTROLES						
AMENAZA	ACCIÓN	OBJETIVO DE CONTROL			CONTROL	
Falla en el funcionamiento de *switch, router* o DSLAM	Aplicar controles Evitar el riesgo Aceptar el riesgo *	9.2	Seguridad del equipo.	9.2.4	Mantenimiento de equipo.
		10.1	Gestión de las comunicaciones y operaciones.	10.1.1	Procedimientos de operación documentados.
		10.5	Respaldo (*backup*).	10.5.1	*Backup* o respaldo de la información.
		10.6	Gestión de seguridad de redes.	10.6.1	Controles de red.
		12.6	Gestión de vulnerabilidad técnica.	12.6.1	Control de vulnerabilidades técnicas.
Falla del *firewall*	Aplicar controles *	9.2	Seguridad del equipo.	9.2.4	Mantenimiento de equipo.
		10.1	Gestión de las comunicaciones y operaciones.	10.1.1	Procedimientos de operación documentados.
		10.5	Respaldo (*backup*).	10.5.1	*Backup* o respaldo de la información.
		10.6	Gestión de seguridad de redes.	10.6.1	Controles de red.
		12.6	Gestión de vulnerabilidad técnica.	12.6.1	Control de vulnerabilidades técnicas.
Falla de Allot	Aplicar controles *	9.2	Seguridad del equipo.	9.2.4	Mantenimiento de equipo.
		10.1	Gestión de las comunicaciones y operaciones.	10.1.1	Procedimientos de operación documentados.
		10.5	Respaldo (*backup*).	10.5.1	*Backup* o respaldo de la información.
		10.6	Gestión de seguridad de redes.	10.6.1	Controles de red.
		12.6	Gestión de vulnerabilidad técnica.	12.6.1	Control de vulnerabilidades técnicas.
Falla de Servidores WEB	Aplicar controles *	9.2	Seguridad del equipo.	9.2.4	Mantenimiento de equipo.
		10.1	Gestión de las comunicaciones y operaciones.	10.1.1	Procedimientos de operación documentados.
		10.5	Respaldo (*backup*).	10.5.1	*Backup* o respaldo de la información.
		10.6	Gestión de seguridad de redes.	10.6.1	Controles de red.
		12.6	Gestión de vulnerabilidad técnica.	12.6.1	Control de vulnerabilidades técnicas.

Tabla 4.17: Selección de Objetivos de Control y Controles (Página 10 de 14)

SELECCIÓN DE OBJETIVOS DE CONTROL Y CONTROLES						
AMENAZA	ACCIÓN	OBJETIVO DE CONTROL		CONTROL		
Falla del Servidor Blade	Aplicar controles *	9.2	Seguridad del equipo.	9.2.4	Mantenimiento de equipo.	
		10.1	Gestión de las comunicaciones y operaciones.	10.1.1	Procedimientos de operación documentados.	
		10.5	Respaldo (backup).	10.5.1	*Backup* o respaldo de la información.	
		10.6	Gestión de seguridad de redes.	10.6.1	Controles de red.	
		10.8	Intercambio de información.	10.8.4	Mensajes electrónicos.	
		12.6	Gestión de vulnerabilidad técnica.	12.6.1	Control de vulnerabilidades técnicas.	
Daño en medios de transmisión	Evitar el riesgo	RECOMENDACIONES BASADAS EN:				
		9.2	Seguridad del equipo.	9.2.3	Seguridad en el cableado.	
		10.1	Procedimientos y responsabilidades operacionales.	10.1.1	Procedimientos de operación documentados.	
		10.6	Gestión de seguridad de redes.	10.6.1	Controles de red.	
Daño en última milla	Aplicar controles Evitar el riesgo	9.2	Seguridad del equipo.	9.2.3	Seguridad en el cableado.	
				9.2.5	Seguridad del equipo fuera del local.	
		10.5	Respaldo (*backup*).	10.5.1	*Backup* o respaldo de la información.	
Daño en equipo de última milla	Aceptar el riesgo *	TRANSFERENCIA DE RIESGO A ASEGURADORA				
Falla en el funcionamiento de radio principal	Aceptar el riesgo *	TRANSFERENCIA DE RIESGO A ASEGURADORA				
Interferencia provocada entre cables de energía y de comunicaciones	Aplicar controles Aceptar el riesgo	9.2	Seguridad del equipo.	9.2.3	Seguridad en el cableado.	

Tabla 4.17: Selección de Objetivos de Control y Controles (Página 11 de 14)

SELECCIÓN DE OBJETIVOS DE CONTROL Y CONTROLES					
AMENAZA	**ACCIÓN**	**OBJETIVO DE CONTROL**		**CONTROL**	
Interferencia en la frecuencia utilizada	Evitar el riesgo Aceptar el riesgo *	RECOMENDACIONES BASADAS EN:			
		10.2	Gestión de la entrega del servicio de terceros.	10.2.1	Entrega del servicio.
				10.2.2	Monitoreo y revisión de los servicios de terceros.
Virus, troyanos, gusanos, ataques de diccionario	Aplicar controles Evitar el riesgo Aceptar el riesgo	6.1	Organización de la seguridad de la información.	6.1.7	Contacto con grupos de interés especial.
		10.1	Procedimientos y responsabilidades operacionales.	10.1.1	Procedimientos de operación documentados.
		10.4	Protección contra software malicioso y código móvil.	10.4.1	Controles contra software malicioso.
				10.4.2	Controles contra códigos móviles.
		10.6	Gestión de seguridad de redes.	10.6.1	Controles de red.
		12.2	Procesamiento correcto en las aplicaciones.	12.2.1	Validación de data de Insumo.
				12.2.2	Control de procesamiento interno.
				12.2.3	Integridad del mensaje.
Negación de servicio (DoS)	Aplicar controles Evitar el riesgo Aceptar el riesgo	10.1	Procedimientos y responsabilidades operacionales.	10.1.1	Procedimientos de operación documentados.
		10.6	Gestión de seguridad de redes.	10.6.1	Controles de red.
		10.8	Intercambio de información.	10.8.4	Mensajes electrónicos.
		12.2	Procesamiento correcto en las aplicaciones.	12.2.1	Validación de data de Insumo.
				12.2.2	Control de procesamiento interno.
				12.2.3	Integridad del mensaje.
Inconvenientes de capacidad para proveer servicio	Evitar el riesgo Aceptar el riesgo	RECOMENDACIONES BASADAS EN:			
		10.3	Planeación y aceptación del sistema.	10.3.1	Gestión de capacidad.

Tabla 4.17: Selección de Objetivos de Control y Controles (Página 12 de 14)

SELECCIÓN DE OBJETIVOS DE CONTROL Y CONTROLES						
AMENAZA		ACCIÓN	OBJETIVO DE CONTROL		CONTROL	
	Falla de UPS	Aplicar controles Evitar el riesgo Aceptar el riesgo *	9.2	Seguridad del equipo.	9.2.2	Servicios públicos.
			10.1	Procedimientos y responsabilidades operacionales.	10.1.1	Procedimientos de operación documentados.
	Daño de aire acondicionado	Evitar el riesgo *	RECOMENDACIONES BASADAS EN:			
			9.2	Seguridad del equipo.	9.2.2	Servicios públicos.
					9.2.4	Mantenimiento de equipo.
			10.1	Procedimientos y responsabilidades operacionales.	10.1.1	Procedimientos de operación documentados.
Ambiental	Incendio	Aplicar controles Evitar el riesgo Aceptar el riesgo *	9.1	Áreas seguras.	9.1.4	Protección contra amenazas externas y ambientales
					9.1.5	Trabajo en áreas seguras.
			9.2	Seguridad del equipo.	9.2.1	Ubicación y protección del equipo.
					9.2.2	Servicios públicos
			10.5	Respaldo (*backup*).	10.5.1	*Backup* o respaldo de la información.
	Filtraciones de agua	Aplicar controles Evitar e riesgo Aceptar el riesgo *	9.1	Áreas seguras.	9.1.4	Protección contra amenazas externas y ambientales
					9.1.5	Trabajo en áreas seguras.
			9.2	Seguridad del equipo.	9.2.1	Ubicación y protección del equipo.
					9.2.2	Servicios públicos
			10.5	Respaldo (*backup*).	10.5.1	*Backup* o respaldo de la información.

Tabla 4.17: Selección de Objetivos de Control y Controles (Página 13 de 14)

SELECCIÓN DE OBJETIVOS DE CONTROL Y CONTROLES						
AMENAZA		ACCIÓN	OBJETIVO DE CONTROL		CONTROL	
	Terremoto	Aplicar controles Evitar e riesgo Aceptar el riesgo *	9.1	Áreas seguras.	9.1.4	Protección contra amenazas externas y ambientales
					9.1.5	Trabajo en áreas seguras.
			9.2	Seguridad del equipo.	9.2.1	Ubicación y protección del equipo.
					9.2.2	Servicios públicos
			10.5	Respaldo (*backup*).	10.5.1	*Backup* o respaldo de la información.
	Deslaves	Aplicar controles Evitar el riesgo Aceptar el riesgo *	9.1	Áreas seguras.	9.1.4	Protección contra amenazas externas y ambientales
					9.1.5	Trabajo en áreas seguras.
			9.2	Seguridad del equipo.	9.2.1	Ubicación y protección del equipo.
					9.2.2	Servicios públicos
			10.5	Respaldo (*backup*).	10.5.1	*Backup* o respaldo de la información.
	Tormentas eléctricas	Aplicar controles Evitar el riesgo Aceptar el riesgo *	9.1	Áreas seguras.	9.1.4	Protección contra amenazas externas y ambientales
					9.1.5	Trabajo en áreas seguras.
			9.2	Seguridad del equipo.	9.2.1	Ubicación y protección del equipo.
					9.2.2	Servicios públicos
			10.5	Respaldo (*backup*).	10.5.1	*Backup* o respaldo de la información.

Tabla 4.17: Selección de Objetivos de Control y Controles (Página 14 de 14)

APLICABLES PARA TODAS LAS AMENAZAS			
OBJETIVO DE CONTROL		**CONTROL**	
5.1	Política de S.I.	5.1.1	Documentar política de S.I.
		5.1.2	Revisión de la política de S.I.
6.1	Organización interna.	6.1.1	Compromiso de la gerencia con la S.I.
		6.1.2	Coordinación de la S.I.
		6.1.3	Asignación de responsabilidades de la S.I.
		6.1.4	Proceso de autorización para los medios de procesamiento de información.
		6.1.6	Contacto con autoridades.
		6.1.8	Revisión independiente de la S.I.
10.10	Monitoreo.	10.10.1	Registro de auditoría.
		10.10.2	Uso del sistema de monitoreo.
		10.10.4	Registro del administrador y operador.
		10.10.5	Registro de fallas.
		10.10.6	Sincronización de relojes.
12.1	Requerimientos de seguridad de los sistemas.	12.1.1	Análisis y especificación de los requerimientos de seguridad.
13.1	Reporte de eventos y debilidades en la S.I.	13.1.1	Reporte de eventos en la S.I.
		13.1.2	Reporte de debilidades en la seguridad.
13.2	Gestión de incidentes y mejoras en la S.I.	13.2.1	Responsabilidades y procedimientos.
		13.2.2	Aprendizaje de los incidentes en la S.I.
		13.2.3	Recolección de evidencia.
15.2	Cumplimiento con las políticas y estándares de seguridad, y el cumplimiento técnico.	15.2.1	Cumplimiento con las políticas y estándares de seguridad.
		15.2.2	Chequeo de cumplimiento técnico.
15.3	Consideraciones de auditoría de los sistemas de información.	15.3.1	Controles de auditoría de sistemas de información.
		15.3.2	Protección de las herramientas de auditoría de los sistemas de información.

Tabla 4.18: Selección de Objetivos de Control y Controles Generales

4.3.8 ENUNCIADO DE APLICABILIDAD

Documento A.6

A continuación se analiza la aplicabilidad de los controles seleccionados, así como las razones para no utilizar determinados controles.

ENUNCIADO DE APLICABILIDAD (SOA)					
SELECCIONADOS					
OBJETIVO DE CONTROL		CONTROL		RAZÓN DE SELECCIÓN	APLICABILIDAD
5.1	Política de S.I.	5.1.1	Documentar política de S.I.	Necesidad de un documento que contenga los lineamientos de la S.I.	Sí, requisito de “Documentación de política”
		5.1.2	Revisión de la política de S.I.	Una vez implementado el SGSI, será necesario evaluar su funcionamiento, así como la política.	Sí, requisito de “Documentación de política”
6.1	Organización interna.	6.1.1	Compromiso de la Gerencia con la S.I.	El apoyo de la Gerencia proporciona credibilidad y cumplimiento por parte de todos los involucrados.	Sí, requisito de “Apoyo de la Gerencia”
		6.1.2	Coordinación de la S.I.	Necesidad de participación conjunta del personal.	Sí, requisito de "Coordinación y participación"
		6.1.3	Asignación de responsabilidades de la S.I.	Definir la asignación de tareas, implica la no concentración de responsabilidades en un solo encargado.	Sí, requisito de "Coordinación y participación"
		6.1.4	Proceso de autorización para los servicios de procesamiento de información.	Necesidad de contar con una política de autorización para el uso de hardware o software.	Sí, requisito de “Uso autorizado de hardware y software”
		6.1.5	Acuerdos de confidencialidad.	Evitar la divulgación de la información referente a la entrega de servicios.	Sí, requisito de “Compromiso del personal”
		6.1.6	Contacto con autoridades.	Necesidad de participación conjunta del personal.	Sí, requisito de “Apoyo de la gerencia”
		6.1.7	Contacto con grupos de interés especial.	Necesidad de mantener informado y capacitado al personal.	Sí, requisito de “Formación en Seguridad de la Información”
		6.1.8	Revisión independiente de la S.I.	Una vez implementado el SGSI, será necesario evaluar su funcionamiento, así como la política.	Sí, requisito de “Revisión periódica de cumplimiento”
6.2	Entidades externas.	6.2.1	Identificación de riesgos relacionados con entidades externas.	Identificar riesgos ocasionados por el trabajo con entidades externas.	Sí, requisito de “Medidas con entidades externas”

Tabla 4.19: Enunciado de Aplicabilidad (SOA) (Página 1 de 14)

SELECCIONADOS					
OBJETIVO DE CONTROL		CONTROL		RAZÓN DE SELECCIÓN	APLICABILIDAD
		6.2.2	Tratamiento de la seguridad cuando se trabaja con clientes.	La provisión de servicios a los clientes, implica la consideración de confidencialidad, integridad y disponibilidad.	Sí, requisitos de “Privilegios de acceso”
		6.2.3	Tratamiento de la seguridad en contratos con terceras personas.	La Empresa se relaciona con varias entidades externas, para proveer los servicios.	Sí, requisito de “Medidas con entidades externas”
7.1	Responsabilidad por los activos.	7.1.1	Inventarios de activos.	Indispensable para el manejo adecuado y seguro de la información asociada a los activos.	Sí, requisito de “Seguridad de los activos de información”
		7.1.2	Propiedad de los activos.	Definir la propiedad de los activos, implica la no concentración de responsabilidades en un solo encargado.	Sí, requisito de “Seguridad de los activos de información”
		7.1.3	Uso aceptable de los activos.	Indispensable para el manejo adecuado y seguro de la información asociada a los activos.	Sí, requisito de “Seguridad de los activos de información”
7.2	Clasificación de la información.	7.2.1	Lineamientos de clasificación.	Indispensable para el manejo adecuado y seguro de la información asociada a los activos.	Sí, requisito de “Seguridad de los activos de información”
		7.2.2	Etiquetado y manejo de la información.	Indispensable para el manejo adecuado y seguro de la información asociada a los activos.	Sí, requisito de “Seguridad de los activos de información”
8.1	Antes del empleo.	8.1.1	Roles y responsabilidades.	Definir las responsabilidades y tareas, antes de que inicie sus actividades, evitando malos entendidos.	Sí, requisito de "Coordinación y participación"
		8.1.2	Selección.	Necesidad de indentificar si el personal es capaz de realizar las actividades asignadas y confirmar que no tenga antecedentes, que pudieran afectar a la S.I.	Sí, requisito de “Compromiso del personal”
		8.1.3	Términos y condiciones de empleo.	Definir las responsabilidades y tareas, antes de que inicie sus actividades, evitando malos entendidos.	Sí, requisito de "Coordinación y participación"

Tabla 4.19: Enunciado de Aplicabilidad (SOA) (Página 2 de 14)

SELECCIONADOS					
OBJETIVO DE CONTROL		CONTROL		RAZÓN DE SELECCIÓN	APLICABILIDAD
8.2	Durante el empleo.	8.2.1	Responsabilidades de la dirección.	Establecer la gestión de la dirección, en el cumplimiento de la S.I.	Sí, requisito de “Apoyo de la Gerencia”
		8.2.2	Capacitación y educación en S.I.	El conocimiento permitirá la aplicación eficaz del SGSI.	Sí, requisito de “Formación en Seguridad de la Información”
		8.2.3	Proceso disciplinario.	Necesidad de establecer sanciones, en caso de cometer actos que pongan en peligro al SGSI.	Sí, requisito de "Proceso disciplinario"
8.3	Terminación o cambio del empleo.	8.3.1	Responsabilidades de terminación.	Resguardar la S.I., de posible divulgación, de personal que termine sus funciones en la Empresa.	Sí, requisito de “Compromiso del personal”
		8.3.2	Devolución de activos.	Resguardar la seguridad de los activos de información, evitando su pérdida o robo.	Sí, requisito de “Seguridad de los activos de información”
		8.3.3	Eliminación de derechos de acceso.	Evitar posible mal uso de los servicios de información.	Sí, requisitos de “Privilegios de acceso”
9.1	Áreas seguras.	9.1.1	Perímetro de seguridad física.	Garantizar la seguridad de los activos de información, aislándolos en lugares seguros.	Sí, requisito de “Seguridad de los activos de información”
		9.1.2	Controles de entrada físicos.	Evitar el ingreso no autorizado.	Sí, requisito de “Seguridad de los activos de información”
		9.1.3	Seguridad de oficinas, habitaciones y medios.	Garantizar la seguridad de los activos de información.	Sí, requisito de “Seguridad de los activos de información”
		9.1.4	Protección contra amenazas externas y ambientales.	Garantizar la seguridad de los activos de información.	Sí, requisito de “Seguridad de los activos de información”
		9.1.5	Trabajo en áreas seguras.	Ambientar los lugares que requieran seguridad, dada la importancia de los procesos de información que en éstos se realizan.	Sí, requisito de “Seguridad de los activos de información”
		9.1.6	Áreas de acceso público, entrega y carga.	Evitar posibles riesgos de la información, en lugares con afluencia de varias personas.	Sí, requisito de “Seguridad de los activos de información”

Tabla 4.19: Enunciado de Aplicabilidad (SOA) (Página 3 de 14)

SELECCIONADOS					
OBJETIVO DE CONTROL		CONTROL		RAZÓN DE SELECCIÓN	APLICABILIDAD
9.2	Seguridad del equipo.	9.2.1	Ubicación y protección del equipo.	Resguardar los activos de información.	Sí, requisito de “Seguridad de los activos de información”
		9.2.2	Servicios públicos.	Tomar precauciones de riesgos asociados a los servicios públicos.	Sí, requisito de “Medidas con entidades externas”
		9.2.3	Seguridad en el cableado.	Evitar riesgos asociados a un cableado inadecuado.	Sí, requisito de “Seguridad de los activos de información”
		9.2.4	Mantenimiento de equipo.	Tomar las medidas adecuadas para realizar mantenimientos periódicos a los equipos.	Sí, requisito de “Seguridad de los activos de información”
		9.2.5	Seguridad del equipo fuera del local.	Evitar riesgos que impliquen la inseguridad de los equipos que se encuentren fuera de la Empresa.	Sí, requisito de “Seguridad de los activos de información”
		9.2.6	Eliminación segura o re-uso del equipo.	Resguardar la información almacenada en los equipos, de posible divulgación o mal uso.	Sí, requisito de “Seguridad de los activos de información”
		9.2.7	Retiro de activos.	Establecer procesos de autorización para el retiro de equipos.	Sí, requisito de “Seguridad de los activos de información”
10.1	Procedimientos y responsabilidades operacionales.	10.1.1	Procedimientos documentados de operación	Necesidad de contar con documentos que almacenen información sobre los procedimiemtos de operación.	Sí, requisito de “Documentación y registro de eventos”
		10.1.2	Gestión de cambios.	Controlar los cambios que se realicen para la entrega de servicios.	Sí, requisito de "Procedimientos"
		10.1.3	Distribución de funciones.	Distribuir funciones, implica la no concentración de responsabilidades en un solo encargado.	Sí, requisito de “Compromiso del personal”
		10.1.4	Separación de los medios de desarrollo y operacionales.	Evitar cambios inapropiados o contraproducentes para la entrega de los servicios.	Si, requisito de "Aislamiento de aplicaciones"
10.2	Gestión de la entrega del servicio de terceros.	10.2.1	Entrega del servicio.	Constatar que los servicios que se reciben de los proveedores, se encuentren dentro de lo estipulado.	Sí, requisito de “Medidas con entidades externas”
		10.2.2	Monitoreo y revisión de los servicios de terceros.	Constatar que los servicios que se recibe de los proveedores, se encuentren dentro de lo estipulado.	Sí, requisito de “Medidas con entidades externas”

Tabla 4.19: Enunciado de Aplicabilidad (SOA) (Página 4 de 14)

SELECCIONADOS					
OBJETIVO DE CONTROL		CONTROL		RAZÓN DE SELECCIÓN	APLICABILIDAD
		10.2.3	Gestión de los cambios en los servicios por tercercas partes.	Dirigir los cambios en los servicios por terceros, teniendo en cuenta la importancia de los sistemas y procesos involucrados.	Sí, requisito de “Medidas con entidades externas”
10.3	Planeación y aceptación del sistema.	10.3.1	Gestión de la capacidad.	Necesidad de controlar el uso de los recursos, así como las proyecciones a futuro.	Sí, requisito de “Diseño adecuado de los sistemas de información”
		10.3.2	Aceptación del sistema.	Necesidad de procedimiento para aceptar a sistemas nuevos.	Sí, requisito de “Diseño adecuado de los sistemas de información”
10.4	Protección contra software malicioso y código móvil.	10.4.1	Controles contra software malicioso.	Incorporar controles de detección y mitigación de software que pudiera poner en peligro la S.I.	Sí, requisito de “Prevención de ataques”
		10.4.2	Controles contra códigos móviles.	Incorporar controles para evitar procedimientos indeseados o daños por la ejecución de códigos móviles.	Sí, requisito de “Prevención de ataques”
10.5	Respaldo *backup.*	10.5.1	*Backup* o respaldo de la información.	Contar con respaldos de toda la información asociada a los activos de información que permiten entregar los servicios.	Sí, requisito de “Respaldo de la información”
10.6	Gestión de seguridad de redes.	10.6.1	Controles de las redes.	Necesidad de implementar controles que protejan a la red de posibles amenazas, así como los sistemas que se encuentran en la red.	Sí, requisito de “Prevención de ataques”
		10.6.2	Seguridad de los servicios de la red.	Identificar las caracterísiticas de seguridad, niveles de servicio y requisitos de gestión para los servicios de la red.	Sí, requisito de “Prevención de ataques”
10.7	Gestión de medios.	10.7.1	Gestión de los medios removibles.	Incorporar normativas sobre el uso de los medios removibles, que pudieran poner en riesgo a la seguridad de la información de los servicios.	Sí, requisito de “Seguridad de los activos de información”

Tabla 4.19: Enunciado de Aplicabilidad (SOA) (Página 5 de 14)

SELECCIONADOS					
OBJETIVO DE CONTROL		CONTROL		RAZÓN DE SELECCIÓN	APLICABILIDAD
		10.7.2	Eliminación de medios.	Resguardar la información almacenada en los medios, de posible divulgación o mal uso.	Sí, requisito de “Seguridad de los activos de información”
		10.7.3	Procedimientos de manejo de la información.	Resguardar la información de posible divulgación o mal uso.	Sí, requisito de "Procedimientos"
		10.7.4	Seguridad de documentación del sistema.	Necesidad de documentar el sistema, de manera segura, para su utilización y mejora.	Sí, requisito de “Documentación y registro de eventos”
10.8	Intercambio de información.	10.8.1	Procedimientos y políticas de información y software.	Necesidad de contar con una política que establezca procedimientos y políticas para el uso adecuado de información y software, sin uso deliberado.	Sí, requisito de “Medidas con entidades externas”
		10.8.2	Acuerdos de intercambio.	Se requiere contar con acuerdos documentados y detallados de intercambio de información.	Sí, requisito de “Medidas con entidades externas”
		10.8.3	Medios físicos en tránsito.	Necesidad de fijar lineamientos seguros para el tránsito de activos de la información.	Sí, requisito de “Medidas con entidades externas”
		10.8.4	Mensajes electrónicos.	Necesidad de establecer reglas para el uso general de mensajes electrónicos.	Sí, requisito de "Procedimientos"
10.10	Monitoreo.	10.10.1	Registro de auditorías.	Necesidad de establecer una política de documentación y archivo de las actividades de los usuarios, con fines de auditoría.	Sí, requisito de “Documentación y registro de eventos”
		10.10.2	Monitoreo del uso del sistema.	Se requiere establecer procedimientos para monitorear el uso de los servicios de procesamiento de información, evitando así posibles incidentes.	Sí, requisito de “Revisión periódica de cumplimiento”
		10.10.3	Protección de la información del registro.	Necesidad de proteger la información de registro de la Empresa, evitando posible fuga de información.	Sí, requisito de “Documentación y registro de eventos”

Tabla 4.19: Enunciado de Aplicabilidad (SOA) (Página 6 de 14)

SELECCIONADOS					
OBJETIVO DE CONTROL		CONTROL		RAZÓN DE SELECCIÓN	APLICABILIDAD
		10.10.4	Registros del administrador y del operador.	Sería conveniente registrar las actividades realizadas por el adiministrador y los operadores, controlando así los eventos o fallas.	Sí, requisito de “Revisión periódica de cumplimiento”
		10.10.5	Registro de fallas.	Necesidad de documentar y almacenar las fallas de los sistemas que permiten proveer los servicios.	Sí, requisito de “Documentación y registro de eventos”
		10.10.6	Sincronización de relojes.	Los sistemas de información deben estar sincronizados para que controles se ejecuten y la información se almacene con indicadores correctos.	Sí, requisito de “Documentación y registro de eventos”
11.1	Requerimiento comercial para el control del acceso.	11.1.1	Política de control de acceso.	Necesidad de establecer políticas para controlar los privilegios y acceso a la información y servicios.	Sí, requisitos de “Privilegios de acceso”
11.2	Gestión del acceso del usuario.	11.2.1	Registro de usuarios.	Necesidad de implementar controles que restrinjan o autoricen el uso de la información a los usuarios.	Sí, requisitos de “Privilegios de acceso”
		11.2.2	Gestión de privilegios.	Se requiere un análisis de los privilegios que se debe otorgar a los diferentes usuarios, para desarrollar una política asociada a los privilegios.	Sí, requisitos de “Privilegios de acceso”
		11.2.3	Gestión de contraseñas para usuario.	Implementar procedimientos que garanticen la seguridad de las contraseñas de usuario, evitando fuga de información o su mal uso.	Sí, requisitos de “Privilegios de acceso”
		11.2.4	Revisión de los derechos de acceso del usuario.	Necesidad de revisar y cambiar los derechos de acceso del usuario, dada la inseguridad que se evidencia.	Sí, requisitos de “Privilegios de acceso”
11.3	Responsabilidades del usuario.	11.3.1	Uso de contraseñas.	Implementar procedimientos que garanticen la seguridad de las contraseñas de usuario, evitando fuga de información o su mal uso.	Sí, requisito de “Compromiso del personal”

Tabla 4.19: Enunciado de Aplicabilidad (SOA) (Página 7 de 14)

SELECCIONADOS					
OBJETIVO DE CONTROL		CONTROL		RAZÓN DE SELECCIÓN	APLICABILIDAD
		11.3.2	Equipo de usuario desatendido.	Evitar ingreso no autorizado a configuración de equipos u otras aplicaciones.	Sí, requisito de “Compromiso del personal”
		11.3.3	Política de pantalla y escritorio limpio.	Evitar el acceso no autorizado a información que pudiera estar disponible sin seguridad.	Sí, requisito de “Compromiso del personal”
11.4	Control de acceo a redes.	11.4.1	Política de uso de los servicios en red.	Necesidad de establecer la forma en que se utilizan los servicios en red y la autorización de acceso.	Sí, requisitos de “Privilegios de acceso”
		11.4.2	Autenticación de usuarios para conexiones externas.	Se requiere controlar el acceso de usuarios remotos, mediante métodos seguros de autenticación.	Sí, requisitos de “Privilegios de acceso”
		11.4.3	Identificación de los equipos en las redes.	Se requieren métodos para identificar automáticamente a los equipos, autenticar conexiones y determinar ubicaciones.	Sí, requisitos de “Privilegios de acceso”
		11.4.4	Protección de los puertos de configuración y diagnóstico remoto.	Necesidad de controlar el acceso físico y lógico a los puertos de configuración y de diagnóstico, para evitar posibles amenazas.	Sí, requisitos de “Privilegios de acceso”
		11.4.5	Separación en las redes.	Se requiere implementar la separación de los servicios de información, usuarios y sistemas de información para resguardar la seguridad de información sensible.	Si, requisito de "Aislamiento de aplicaciones"
		11.4.6	Control de conexión a las redes.	Necesidad de controles para restringir la conexión de los usuarios, de acuerdo al control de acceso.	Sí, requisitos de “Privilegios de acceso”
		11.4.7	Control del enrutamiento en la red.	Necesidad de controles de enrutamiento en las redes, protegiendo el cumplimiento de la política de control de acceso.	Sí, requisitos de “Privilegios de acceso”

Tabla 4.19: Enunciado de Aplicabilidad (SOA) (Página 8 de 14)

SELECCIONADOS					
OBJETIVO DE CONTROL		CONTROL		RAZÓN DE SELECCIÓN	APLICABILIDAD
11.5	Control de acceso al sistema de operación.	11.5.1	Procedimientos de registro de inicio seguro.	Asegurar que solo los usuarios autorizadas ingresen en el sistema, resgistrándose de manera segura.	Sí, requisitos de “Privilegios de acceso”
		11.5.2	Identificación y autenticación del usuario.	Necesidad de controles para identificar y autenticar solo a los usuarios autorizados.	Sí, requisitos de “Privilegios de acceso”
		11.5.3	Sistema de gestión de contraseñas.	Implementar un sistema que administre de manera segura las contraseñas y evite el mal uso de las mismas.	Sí, requisitos de “Privilegios de acceso”
		11.5.4	Uso de utilidades del sistema.	Se requiere establecer normas que regulen el uso de programas utilitarios que pudieran anular los controles del sistema y de la aplicación.	Sí, requisitos de “Privilegios de acceso”
		11.5.5	Sesión inactiva.	Necesidad de suspender las sesiones que después de un tiempo determinado se encuentren inactivas, evitando mal uso de la información.	Sí, requisitos de “Privilegios de acceso”
		11.5.6	Limitación de tiempo de conexión.	Se requiere implementar límites de tiempo en las aplicaciones de alto riesgo, incorporando mayor seguridad.	Sí, requisitos de “Privilegios de acceso”
11.6	Control de acceso a la aplicación e información.	11.6.1	Restricción del acceso a la información.	Necesidad de limitar el acceso a la información al personal, procurando que ésta esté disponible solo para aquellos que realmente la requieran.	Sí, requisitos de “Privilegios de acceso”
		11.6.2	Aislamiento de sistemas sensibles.	Se necesita aislar a todos los sistemas sensibles en su propio entorno informático, limitando su acceso al máximo.	Si, requisito de "Aislamiento de aplicaciones"
12.1	Requerimientos de seguridad de los sistemas.	12.1.1	Análisis y especificación de los requisitos de seguridad.	Necesidad de que la Empresa determine los requisitos para los controles de seguridad a aplicarse en un futuro.	Sí, requisitos de “Documentación de política”

Tabla 4.19: Enunciado de Aplicabilidad (SOA) (Página 9 de 14)

SELECCIONADOS					
OBJETIVO DE CONTROL		CONTROL		RAZÓN DE SELECCIÓN	APLICABILIDAD
12.2	Procesamiento correcto en las aplicaciones.	12.2.1	Validación de los datos de entrada.	Se requiere garantizar que los datos de entrada sean correctos y apropiados, de modo que se ofrezcan eficazmente los servicios.	Sí, requisito de “Diseño adecuado de los sistemas de información”
		12.2.2	Control de procesamiento interno.	Necesidad de verificar la validación de las aplicaciones y así detectar posibles incidentes.	Sí, requisito de “Diseño adecuado de los sistemas de información”
		12.2.3	Integridad del mensaje.	Se requieren controles que permitan garantizar la autenticidad e integridad de los mensajes.	Sí, requisito de “Diseño adecuado de los sistemas de información”
		12.2.4	Validación de los datos de salida.	Se requiere garantizar que los datos de salida sean correctos y apropiados, de modo que se ofrezcan eficazmente los servicios.	Sí, requisito de “Diseño adecuado de los sistemas de información”
12.3	Controles criptográficos	12.3.1	Política sobre el uso de controles criptográficos.	Necesidad de implementar controles criptográficos que aseguren a la información en su transmisión o almacenamiento.	Sí, requisitos de “Privilegios de acceso”
		12.3.2	Gestión de claves.	Se necesita un sistema encargado de administrar las claves de usuarios, garantizando su seguridad.	Sí, requisitos de “Privilegios de acceso”
12.4	Seguridad de los archivos del sistema.	12.4.1	Control de software operativo.	Es necesario controlar y restringir la instalación de software.	Sí, requisito de “Uso autorizado de hardware y software”
		12.4.2	Protección de los datos de prueba del sistema.	Se requiere establecer una normativa sobre la selección y uso de los datos que se utilizan para realizar pruebas.	Sí, requisito de “Documentación y registro de eventos”
		12.4.3	Control de acceso al código fuente de los programas.	Es necesario restringir el acceso al código fuente de los programas, enfocando el acceso tan solo al encargado del Departamento de Sistemas.	Sí, requisitos de “Privilegios de acceso”

Tabla 4.19: Enunciado de Aplicabilidad (SOA) (Página 10 de 14)

SELECCIONADOS					
OBJETIVO DE CONTROL		CONTROL		RAZÓN DE SELECCIÓN	APLICABILIDAD
12.5	Seguridad en los procesos de desarrollo y soporte.	12.5.1	Procedimientos de control de cambio.	Establecer los procedimientos que se deben realizar para cualquier modificación o cambio, pues éstas son muy frecuentes y no siguen lineamiemtos.	Sí, requisito de "Procedimientos"
		12.5.2	Revisión técnica de las aplicaciones después de cambios en el sistema operativo.	Se requiere someter a revisión las aplicaciones luego de cambios, inclusive deben ser sometidas a pruebas para verificar el éxito del cambio.	Sí, requisito de “Revisión periódica de cumplimiento”
		12.5.3	Restricciones sobre los cambios en los paquetes de software.	No se pueden realizar cambios a nivel de software, sin un análisis inicial; para ello se requiere de restricciones.	Sí, requisito de “Uso autorizado de hardware y software”
		12.5.4	Fuga de información.	Se debe evitar la fuga de información asociada a los procesos de desarrollo y soporte, mediante los controles apropiados.	Sí, requisito de “Uso autorizado de hardware y software”
		12.5.5	Desarrollo de software contratado externamente.	Es necesario revisar continuamente el desarrollo de software que se contrata, considerando acuerdos, convenios, requisitos.	Sí, requisito de “Medidas con entidades externas”
12.6	Gestión de vulnerabilidad técnica.	12.6.1	Control de las vulnerabilidades técnicas.	Es necesario que la Empresa se informe sobre las vulnerabilidades técnicas que presentan sus sistemas de información, para tomar acciones correctivas.	Sí, requisito de “Formación en Seguridad de la Información”
13.1	Reporte de eventos en la S.I.	13.1.1	Reporte de eventos en la S.I.	Se requiere establecer la obligatoriedad en el aviso sobre los eventos de seguridad de la información, a los encargados.	Sí, requisito de “Documentación y registro de eventos”
		13.1.2	Reporte de debilidades en la seguridad.	Es necesario que el personal de aviso en caso de que detecte o presuma la presencia de alguna amenaza para la seguridad de la información.	Sí, requisito de “Documentación y registro de eventos”

Tabla 4.19: Enunciado de Aplicabilidad (SOA) (Página 11 de 14)

SELECCIONADOS					
OBJETIVO DE CONTROL		CONTROL		RAZÓN DE SELECCIÓN	APLICABILIDAD
13.2	Gestión de incidentes y mejoras en la S.I.	13.2.1	Responsabilidades y procedimientos.	Es imprescindible establecer las responsabilidades y los procedimientos a cargo de cada integrante del Departamento, para resolver de forma eficiente cualquier incidente.	Sí, requisito de "Coordinación y participación"
		13.2.2	Aprendizaje debido a los incidentes de S.I.	Se requieren mecanismos que cuantifiquen y monitoreen el tipo, volumen y costo de los incidentes de seguridad; para utilizar la información a futuro si se requiere.	Sí, requisito de “Formación en Seguridad de la Información”
		13.2.3	Recolección de evidencia.	Es necesario conservar la evidencia de todo incidente de S.I.; podría ser requerida en caso de llevar el caso a lo penal.	Sí, requisito de “Documentación y registro de eventos”
14.1	Aspectos de la S.I. de la gestión de la continuidad comercial.	14.1.1	Incluir S.I. en el proceso de gestión de continuidad del negocio.	Para que la continuidad comercial persista, se requiere la entrega óptima de servicios.	Sí, requisito de "Planes para la continuidad"
		14.1.2	Continuidad comercial y evaluación del riesgo.	Para que la continuidad comercial persista, se requiere la entrega óptima de servicios, de modo que se debe evaluar cualquier riesgo que se identifique.	Sí, requisito de "Planes para la continuidad"
		14.1.3	Desarrollar e implementar planes de continuidad incluyendo S.I.	Se necesita establecer planes que garanticen la continuidad en la entrega de los servicios, en caso de presentarse alguna falla.	Sí, requisito de "Planes para la continuidad"
		14.1.4	Estructura para la planificación de la continuidad comercial.	Se requiere de una estructura única de los planes de continuidad, que deben ser consistentes.	Sí, requisito de "Planes para la continuidad"
		14.1.5	Prueba, mantenimiento y reevaluación de planes de continuidad comercial.	Es necesario que los planes de continuidad se sometan a pruebas de manera periódica, así es posible evaluarlos y mejorarlos.	Sí, requisito de "Planes para la continuidad"

Tabla 4.19: Enunciado de Aplicabilidad (SOA) (Página 12 de 14)

SELECCIONADOS					
OBJETIVO DE CONTROL		CONTROL		RAZÓN DE SELECCIÓN	APLICABILIDAD
15.1	Cumplimiento con requerimientos legales.	15.1.1	Identificación de legislación aplicable.	Para la entrega eficaz de los servicios, la Empresa debe definir y revisar los requisitos legales correspondientes.	Sí, requisito de “Cumplimiento con legislación”
		15.1.2	Derechos de propiedad intelectual (IPR)	Se requiere verificar el uso de software autorizado y licenciado en la entrega de los servicios.	Sí, requisito de “Cumplimiento con legislación”
		15.1.3	Protección de los registros de la organización.	Es indispensable resguardar los registros, de posibles amenazas humanas, tecnológicas o ambientales; pues éstas podrían afectar en la entrega de los servicios.	Sí, requisito de “Cumplimiento con legislación”
		15.1.4	Protección de los datos y privacidad de información personal.	Se necesita seguridad para conservar los datos asociados a información personal, garantizando su confidencialidad e integridad.	Sí, requisito de “Cumplimiento con legislación”
		15.1.5	Prevención del uso inadecuado de los servicios de procesamiento de información.	Se requiere alertar al personal sobre la no utilización de los servicios de procesamiento de información para fines no autorizados.	Sí, requisito de “Cumplimiento con legislación”
		15.1.6	Regulación de controles criptográficos.	Para la transmisión y almacenamiento seguro de información se requerirán controles criptográficos, que deben ser utilizados bajo cierta regulación que se especifique.	Sí, requisito de “Cumplimiento con legislación”
15.2	Cumplimiento con las políticas y estándares de seguridad, y el cumplimiento técnico.	15.2.1	Cumplimiento con las políticas y estándares de seguridad.	Una vez implementado el SGSI, será necesario evaluar su funcionamiento, así como la política.	Sí, requisitos de “Documentación de política”
		15.2.2	Verificación del cumplimiento técnico.	Es necesario que se verifique periódicamente el cumplimiento de los sistemas de información.	Sí, requisito de “Revisión periódica de cumplimiento”

Tabla 4.19: Enunciado de Aplicabilidad (SOA) (Página 13 de 14)

SELECCIONADOS					
OBJETIVO DE CONTROL		**CONTROL**		**RAZÓN DE SELECCIÓN**	**APLICABILIDAD**
15.3	Consideraciones de auditoría de los sistemas de información.	15.3.1	Controles de auditoría de sistemas de información.	Se requiere planificar cuidadosamente las auditorías en las que se verifiquen los sistemas operativos, para evitar posibles incidentes.	Sí, requisito de “Revisión periódica de cumplimiento”
		15.3.2	Protección de las herramientas de auditoría de los sistemas de información.	Es necesario aislar a las herramientas de auditoría de los sistemas de información, pues podrían ser alteradas y entregar resultados incorrectos.	Sí, requisito de “Revisión periódica de cumplimiento”
EXCLUÍDOS					
OBJETIVO DE CONTROL		**CONTROL**		**RAZÓN DE EXLUSIÓN**	
10.8	Intercambio de información.	10.8.5	Sistemas de información comercial.	La Empresa no presenta en su página web información comercial; además ésta no forma parte de los servicios finales que se ofrecen a los clientes.	
10.9	Servicios de comercio electrónico.	10.9.1	Comercio electrónico.	Se excluye a toda la Categoría Principal 10.9 porque la Empresa no ofrece actualmente servicios de comercio electrónico.	
		10.9.2	Transacciones en línea.		
		10.9.3	Información disponible públicamente.		

Tabla 4.19: Enunciado de Aplicabilidad (SOA) (Página 14 de 14)

4.3.9 PROCESOS PROPUESTOS

Documento A.7

En base a la Norma ISO 27002, se establecen los siguientes procesos, garantizando la confidencialidad, integridad y disponibilidad de la información. La nomenclatura utilizada para identificar cada cláusula, se basa en función de su nombre y del orden correspondiente.

1. Procesos de Política de Seguridad: PR-POLSEG-01 (4 Páginas)

2. Procesos de la Organización de la Seguridad de la Información: PR-ORGSEGINF-02 (9 Páginas)

3. Procesos de Gestión de Activos: PR-GESACT-03 (10 Páginas)

4. Procesos de Seguridad de los Recursos Humanos: PR-SEGRECHUM-04 (13 Páginas)

5. Procesos de Seguridad Física y del Entorno: PR-SEGFISENT-05 (11 Páginas)

6. Procesos de Gestión de Operaciones y Comunicaciones: PR-GESOPCOM-06 (26 Páginas)

7. Procesos de Control de Acceso: PR-CONACC-07 (18 Páginas)

8. Procesos de Adquisición, Desarrollo y Mantenimiento de Sistemas de Información: PR-ADDEMASI-08 (23 Páginas)

9. Procesos de Gestión de los Incidentes de Seguridad de la Información: PR-GESINCSI-09 (5 Páginas)

10. Procesos de Gestión de la Continuidad del Negocio: PR-GESCONEG-10 (5 Páginas)

11. Procesos de Cumplimiento: PR-CUMPL-11 (12 Páginas)

ecuanet Pionero y Líder en Soluciones Corporativas	PROCESOS DE POLÍTICA DE SEGURIDAD PR-POLSEG-01	Página 1 de 4
ELABORADO POR: FANNY FLORES DIANA JIMÉNEZ	REVISADO POR: ING. PABLO HIDALGO	APROBADO POR:

1.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Objetivo:

Dar a conocer al personal la importancia de la Seguridad de la Información y la necesidad de implementar un Sistema de Gestión de Seguridad de la Información (SGSI), que debe ser revisado periódicamente, garantizando la confidencialidad, integridad y disponibilidad de la información.

1.1.1 DOCUMENTO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Seguridad de la Información hace referencia a los métodos utilizados para proteger a la información, de amenazas internas y/o externas a las que podría estar expuesta.

Los objetivos generales que se persigue con la seguridad de la información, son:

- Asegurar una calidad óptima de los servicios, en cuanto a la confidencialidad, integridad y disponibilidad de la información asociada a éstos.

- Garantizar mayores oportunidades, prestigio y credibilidad para la Empresa.

- Detectar y mitigar las amenazas que pudieran poner en riesgo a la seguridad de la información.

- Trabajar en conjunto para el cumplimiento del SGSI.

El alcance de la seguridad de la información, es la protección del activo más importante de toda organización: su información, orientándose así a la cooperación de todo el personal por el cumplimiento del SGSI, para resguardar a la información de cualquier amenaza a la cual podría exponerse.

La importancia de la seguridad de la información radica en que actualmente la información se encuentra expuesta a un sinnúmero de amenazas, y siendo ésta uno de los activos más trascendentales para el funcionamiento de una organización, resulta indispensable tomar iniciativas que permitan garantizar la seguridad de la misma.

El Gerente Nacional de Operaciones y Sistemas apoyará activamente en el desarrollo y cumplimiento del SGSI.

La estructura que se utiliza para establecer la evaluación de riesgos, incluye la consideración de la probabilidad de ocurrencia, impacto y costos de los mismos, determinando así los Niveles de Riesgo, utilizados para determinar la gestión de riesgo. Para el establecimiento de los objetivos de control y controles se analizan éstos de la Norma ISO 27001, determinando cuáles son los más apropiados, dependiendo de los resultados de la gestión de riesgo.

Se establecen políticas y principios de seguridad, orientados a facilitar la coordinación de las actividades entre el personal de la Empresa y entidades externas, gestionar adecuadamente el uso de activos de información, establecer seguridad para los equipos y lugares, incorporar controles que aseguren los accesos, sancionar en caso de infracción a la seguridad de la información, capacitar y concienciar al personal acerca de la seguridad, revisar

periódicamente el cumplimiento del SGSI, documentar y archivar la información de eventos, cumplir con la legislación.

Se definen las responsabilidades generales del Departamento de Operaciones en la consecución del desarrollo del SGSI, su cumplimiento y revisión; además se establecen las responsabilidades personales de los encargados de determinadas funciones de seguridad. De manera general, las responsabilidades son respetar los privilegios de acceso, usar adecuadamente los activos de información, no divulgar información, registrar actividades e incidentes detectados.

La política de seguridad encuentra sus fundamentos en la valuación de riesgos desarrollada en base al Documento A3, en el establecimiento del Nivel de Importancia de los activos, en el Enunciado de Aplicabilidad desarrollado y en las Normas ISO 27001 e ISO 27002.

1.1.2 REVISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La política del SGSI deberá ser revisada anualmente por parte del Encargado de Seguridad de la Información; así también el Gerente Nacional de Operaciones y Sistemas deberá participar de esta actividad y aprobar el nuevo documento.

En esta revisión, se deberá realizar una evaluación de los resultados obtenidos, con el fin de calificar la efectividad de los controles implementados y tomar decisiones para actualizar o establecer nuevos controles. En esta evaluación se deberá tomar en cuenta la confidencialidad, integridad y disponibilidad de la información mantenida durante dicho período, las amenazas que dieron lugar a

incidentes de seguridad y las vulnerabilidades que participaron en dicha amenaza.

Adicionalmente se deberá hacer un análisis de nuevas amenazas y vulnerabilidades que pudieran presentarse en la empresa, para ser tomadas en cuenta en los cambios de la política.

Los correctivos a considerarse en la política de seguridad de la información serán especificados en un nuevo documento, el cual será dado a conocer a todo el personal del Departamento de Operaciones y Sistemas en un lapso máximo de 24 horas, una vez recibida la aprobación del Gerente del Departamento.

En caso de presentarse un cambio representativo en las operaciones de la empresa, que implique la prestación de servicios brindados en la ciudad de Quito, tales como: implementación o cambio de ubicación de un nodo, implementación de equipos de seguridad, modificación de la legislación de telecomunicaciones, etc., se deberá realizar la revisión de la política de Seguridad de la Información de manera extraordinaria, sin que ésta afecte la revisión anual planificada.

2.1 ORGANIZACIÓN INTERNA

Objetivo:

Definir las directrices que deberán llevarse a cabo para iniciar y controlar la implementación de la seguridad dentro de la organización.

2.1.1 COMPROMISO DE LA DIRECCIÓN CON LA SEGURIDAD DE LA INFORMACIÓN

La Dirección estará comprometida con el correcto desarrollo del Sistema de Gestión de Seguridad de la Información, de tal forma que se involucre desde el planeamiento, determinando si los objetivos de la seguridad de la información satisfacen las necesidades de la organización.

La política de seguridad de la información, será elaborada por el Encargado de Seguridad, siendo ésta revisada y aprobada por el Gerente Nacional de Operaciones y Sistemas, el mismo que dará el seguimiento respectivo para verificar la eficacia de la política en la implementación.

Adicionalmente la Gerencia se encargará de coordinar en la organización la implementación de los controles de seguridad de la información y aprobar la asignación de funciones y responsabilidades específicas.

La Gerencia a más de proporcionar los recursos necesarios para la implementación del SGSI, deberá comprometerse a capacitar al personal sobre la importancia de la seguridad de la información, de tal forma que éstos participen activamente y generen opciones para el mejoramiento del sistema.

2.1.2 COORDINACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Para la coordinación de la seguridad de la información se tomarán en cuenta los siguientes lineamientos:

a) Todo el personal del Departamento de Operaciones deberá participar activamente para garantizar el cumplimiento de la política, para lo cual la Gerencia ejecutará planes de concientización de la importancia de la seguridad de la información.

b) La política de seguridad de la información, una vez aprobada, será dada a conocer al personal del Departamento de Operaciones y a cada persona que se incorpore al grupo de trabajo en el momento de su ingreso, de tal manera que se tenga conocimiento de las actividades que deberán ser efectuadas. En caso de no cumplirse las estipulaciones mencionadas en la política se aplicará la Política de proceso disciplinario.

c) Se manejarán las metodologías de evaluación de riesgos y de clasificación de la información descritas en el Documento A3; sin embargo se podrá recibir sugerencias de mejora u otras alternativas, las cuales serán analizadas y evaluadas por el Encargado de Seguridad.

2.1.3 ASIGNACIÓN DE RESPONSABILIDADES PARA LA SEGURIDAD DE LA INFORMACIÓN

El Encargado de Seguridad será responsable del desarrollo e implementación de la seguridad, además será quien designe, bajo un criterio de equidad y

tomando en cuenta las funciones que desempeña cada trabajador, las diferentes tareas y responsabilidades.

De manera general se asignarán responsables de los activos, de acuerdo a lo indicado en la Tabla de Cálculo de Nivel de Importancia de activos de información para la Seguridad, los cuales serán los encargados de velar por la seguridad física de cada uno de los equipos, así como resguardar la seguridad de la información que éstos almacenan.

Adicionalmente las responsabilidades de cada uno de los trabajadores se mencionarán en cada una de las políticas descritas en este documento.

2.1.4 PROCESO DE AUTORIZACIÓN PARA LOS SERVICIOS DE PROCESAMIENTO DE INFORMACIÓN

La implementación de nuevos elementos (hardware o software) que se relacionen con la entrega de los servicios en la ciudad de Quito, deberán ser previamente supervisados por el responsable de seguridad, de tal manera que éste pueda verificar que la puesta en marcha del elemento cumple con los requisitos de seguridad correspondientes para su aprobación. En caso de que sea totalmente necesario el ingreso del elemento, el Encargado de Seguridad deberá analizar posibles amenazas y vulnerabilidades que conllevaría la implementación, para actualizar la Matriz de riesgo correspondiente.

Una vez que el Encargado de Seguridad ha supervisado el ingreso, el Gerente Nacional de Operaciones y Sistemas deberá dar la aprobación final para la implementación del nuevo elemento.

2.1.5 ACUERDOS SOBRE CONFIDENCIALIDAD

El documento “Acuerdo de Confidencialidad” deberá ser revisado e incluirá los siguientes puntos:

a) La información que será considerada como confidencial y que no podrá ser divulgada bajo ningún concepto será la siguiente:

- Usuario y contraseña utilizados para el acceso a configuraciones de los equipos.
- Activos de la empresa
- Configuración de los equipos y direcciones IP.
- Claves de cuentas de clientes.
- Ubicación de nodos y acceso a ellos.
- Horario del personal de trabajo.

b) El acuerdo de confidencialidad se mantendrá vigente durante el período durante el cual el trabajador ejerza sus funciones en la empresa y se prolongará hasta 3 años después de su separación de la empresa.

c) Se tendrá derecho a realizar auditorías no planificadas y monitorear las actividades que involucran a la información considerada como confidencial.

d) Las sanciones a ejecutarse en caso de incumplimiento serán las especificadas en la Política de Proceso disciplinario.

2.1.6 CONTACTO CON LAS AUTORIDADES

Internamente se mantendrá el siguiente nivel de escalamiento en caso de ser detectado algún incidente de seguridad de la información:

- Jefe de Implementación y Gestión de Red R1 / Coordinador Nacional de Sistemas
- Jefe Regional NOC R1
- Encargado de seguridad
- Gerente nacional de Operaciones y Sistemas.

Ellos a su vez contarán con el listado de contactos, que contenga los datos y nivel de escalamiento de bomberos, policía, proveedores, etc., el cual será elaborado por el Encargado de Seguridad.

2.1.7 CONTACTOS CON GRUPOS DE INTERÉS ESPECIALES

El Encargado de Seguridad deberá mantenerse en la vanguardia en cuanto a la seguridad de la información, para lo cual la empresa le brindará la capacitación en cursos especiales o foros por lo menos una vez al año.

Con ello se permitirá que el Encargado de Seguridad esté en continua relación con gente externa, con la cual se podrá compartir conocimiento sobre mejores prácticas, advertencias oportunas de nuevos ataques y vulnerabilidades, asesoría, entre otras.

2.1.8 REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN

Se llevará a cabo revisiones independientes anualmente, ejecutadas por una organización de tercera parte especializada en el tema de seguridad de la información.

Los resultados emitidos por la organización a cargo, serán entregados al Gerente Nacional de Operaciones y Sistemas para que, en conjunto con el Encargado de Seguridad, se realice el análisis y verificación de las políticas que están siendo ejecutadas correctamente y cuales no.

Dichos resultados y correctivos deberán ser documentados y almacenados por el Encargado de Seguridad, con el fin de comparar en la siguiente revisión los aciertos obtenidos y mejoras logradas.

2.2 PARTES EXTERNAS

Objetivo:

Definir los riesgos relacionados con las partes externas, especificando las directrices que se tomarán en cuenta en caso de detectar incidentes de seguridad relacionados con ellos.

2.2.1 IDENTIFICACIÓN DE LOS RIESGOS RELACIONADOS CON LAS PARTE EXTERNAS

Para la identificación de riesgos relacionados con el acceso de partes externas se deberá considerar lo siguiente:

a) Las partes externas tendrán acceso únicamente a nivel físico al Centro de Datos y nodos. Bajo ningún concepto serán portadores de claves que les permita el acceso a nivel lógico.

b) El valor de la información involucrada será correspondiente a lo estipulado en la evaluación de riesgos.

c) El ingreso al Centro de Datos y nodos de partes externas será controlado y supervisado por una persona del Departamento de Operaciones.

d) El personal perteneciente a partes externas deberá portar su identificación correspondiente para que le sea autorizado el ingreso.

e) En caso de producirse un incidente de seguridad durante la realización de trabajos por personal de partes externas, dicho trabajo será suspendido, hasta detectarse el origen del incidente. En caso de que el origen provenga de una mala práctica de las partes externas, se aplicarán las sanciones respectivas estipuladas en el contrato.

2.2.2 ABORDAJE DE LA SEGURIDAD CUANDO SE TRATA CON LOS CLIENTES

Antes de proporcionar el acceso a clientes a los activos de la información se considerarán los siguientes términos:

a) Determinación de la confiabilidad, disponibilidad e integración de la información otorgada al cliente. La empresa manejará una disponibilidad del 99.8 % en cuanto al servicio otorgado.

b) Prácticas utilizadas para protección de activos, incluyendo los procedimientos para detectar incidentes de seguridad.

c) Se otorgará información sensible, únicamente si se ha confirmado la identidad del cliente.

d) Se proporcionarán reportes, en caso de detectarse incidentes de seguridad que hayan involucrado información sensible.

e) El cliente tiene derecho a realizar un monitoreo de las actividades relacionadas con los activos de la organización.

2.2.3 ABORDAJE DE LA SEGURIDAD EN LOS ACUERDOS CON TERCERAS PARTES

Se deberán expresar de manera clara los términos que se manejarán con terceras partes, de tal forma que no existan malos entendidos entre las organizaciones, para lo cual se tomarán en cuenta los siguientes requisitos:

a) Se deberá informar de la política de seguridad de la información con la cual se rige a la empresa.

b) Las actividades que se llevan a cabo para la protección de cada activo, tanto a nivel físico como lógico.

3.1 RESPONSABILIDAD POR LOS ACTIVOS

Objetivo:

Identificar los activos que contribuyen a la entrega de los servicios, establecer su importancia y propiedad, para ser considerados en la aplicación y cumplimiento de los controles.

3.1.1 INVENTARIO DE ACTIVOS

La realización de un inventario implica identificar los activos de información asociados a la entrega de los servicios y documentar su importancia; dado que un prerrequisito para la gestión de riesgos es la realización de un inventario, éste fue desarrollado y está especificado en “Cálculo de Nivel de Importancia de activos de información para la Seguridad” (Tabla 4.12). En el inventario desarrollado, junto a la determinación del Nivel de Importancia, se establece la información necesaria de cada activo.

La importancia de los activos se establece en función de cuán substancial es el activo para garantizar la confidencialidad, integridad y disponibilidad de los servicios, así se determina su nivel de importancia (NI), como se especifica en el Documento A3 y sus resultados se presentan en la Tabla 4.12.

En base a la importancia de los activos, se identifican los niveles de protección que se les debe otorgar. Para cada nivel de importancia identificado, se establece un nivel de protección. Para aquellos activos con NI bajo, la protección será baja; para los activos con NI moderado, la protección que se les dará será moderada. En el caso de los activos con NI alto, se requerirá de un nivel de protección alto y

finalmente para los activos con NI Muy Alto, el nivel de protección debe ser igualmente muy alto.

Pese a que se considera como activos a: información, software, equipos, personas y a bienes intangibles, la presente política se concentra en los activos de información que corresponden a los equipos que permiten proporcionar los servicios a los clientes de Quito, puesto que el alcance del SGSI planteado abarca tan solo a la seguridad en la prestación de los servicios.

3.1.2 PROPIETARIO DE LOS ACTIVOS

Se designan propietarios de los activos de información, a los individuos con la responsabilidad aprobada de la dirección por el control de la producción, desarrollo, mantenimiento, uso y seguridad de los activos.

La propiedad de los activos, se designa de la siguiente manera:

a) Activos que conforman el Centro de Datos, corresponden al Jefe de Implementación y Gestión de Red R1.

b) El Administrador de Ingeniería (Alámbrico) y el Administrador de Red Física y Regulaciones son los propietarios de los activos de información de Megared Alámbrica.

c) Para los activos de Megared Inalámbrica, se asigna la propiedad al Administrador de Ingeniería (Inalámbrico) y al Administrador de Red Física y Regulaciones.

El propietario de un activo será el responsable de garantizar que la información y los activos se clasifiquen adecuadamente; además deberá definir y revisar las restricciones y clasificaciones del acceso periódicamente, en base a las políticas de control de acceso.

A más de los equipos, la propiedad puede ser asignada a los procesos, actividades, aplicaciones o a los datos. Por ello, se realiza la siguiente designación:

a) El propietario de los procesos y actividades asociadas a la seguridad de la información de los servicios entregados, es el Gerente Nacional de Operaciones y Sistemas.

b) En cuanto a las aplicaciones, se designa su propiedad al Coordinador Nacional de Sistemas.

c) El Jefe Regional NOC R1 es designado propietario de los datos que implican la entrega de los servicios.

3.1.3 USO ACEPTABLE DE LOS ACTIVOS

Megadatos S.A. proporciona varios servicios de transmisión de datos por la red, facilitando a sus clientes el acceso a la información. La empresa, se compromete a exigir a los usuarios el cumplimiento del uso aceptable de los servicios, mediante sus condiciones contractuales.

La empresa incluirá en sus contratos las siguientes condiciones generales de "Política de uso aceptable de los Servicios de Internet y Correo electrónico" a todos sus usuarios, tanto al personal como a sus clientes:

a) Los usuarios deben acceder a los servicios, de conformidad con la ley, la moral y con lo estipulado por la "Política de uso aceptable de los activos", incluida en el contrato.

b) El usuario se abstendrá de utilizar los servicios con fines ilícitos, perjudiciales, violentos, denigrantes a los derechos e intereses de terceros; o que puedan deteriorar, inutilizar o sobrecargar los servicios, equipos informáticos, documentos o archivos de otros usuarios de la red. Además se prohíbe promover pensamientos discriminatorios por raza, sexo, religión, creencias, condición física o psíquica. La empresa se compromete a informar a las autoridades pertinentes y colaborar en todo lo necesario para sancionar estas actividades.

c) Están prohibidas las acciones que pongan en riesgo el secreto de las comunicaciones, considerándose así las actividades que violen los derechos de intimidad personal, distribución de información sin autorización de usuarios, obtención engañosa de datos personales como cuentas y claves de acceso. La empresa actuará inmediatamente si se detecta o reporta algún caso de violación al secreto de comunicaciones.

d) No se permiten actividades que violenten los derechos de propiedad intelectual, como marcas registradas, secretos comerciales, piratería de software, patentes.

e) Se prohíben acciones de *hacking*, *cracking*, *phreaking*, *carding*, *phising*; así como el acceso no autorizado, robo, bloqueo o daño de la información, sobrecarga o deterioro de los servicios, sistemas, redes y equipos. Además está prohibida la distribución de información por Internet, sobre procedimientos de creación de virus, gusanos, caballos troyanos, ataques de diccionario o negación del servicio, con fines maliciosos.

f) Los usuarios de correo electrónico no enviarán publicidad o comunicaciones a una cantidad considerable de personas, sin su autorización. Además, no enviarán cadenas de mensajes electrónicos no solicitados ni autorizados por los receptores. Con el fin de evitar esta acción, la empresa implementará servidores *antispam* y se dará seguimiento a posibles generadores de *spam*.

Los siguientes literales se aplican exclusivamente para el personal.

g) Se prohíbe el uso del Internet para actividades que no correspondan exclusivamente al ámbito laboral, como por ejemplo navegación en páginas de redes sociales, descarga de música, videos, juegos, páginas para adultos, entre otras. Se procede a bloquear las páginas de Internet de la intranet de la empresa, que no contribuyen con el desarrollo laboral de la misma y que por el contrario, ponen en riesgo a la seguridad de la información de los servicios de procesamiento.

h) El correo electrónico debe ser utilizado únicamente con propósitos relativos al trabajo. La información que se ponga a disposición en este servicio, deberá ajustarse a la seguridad necesaria, que se especifica en la “Política de control de acceso”, así como el manejo de contraseñas. Durante horas

laborables, los usuarios no podrán acceder a cuentas de correo electrónico distintas a las cuentas oficiales de la empresa, a menos que estén autorizados. La información recibida de partes externas, debe ser sometida a revisión antes de su utilización.

i) Tan solo el personal del Departamento de Operaciones y el Coordinador Nacional de Sistemas tendrán acceso a la configuración de los equipos que conforman la red, a través de la cual se proporcionan los servicios a los clientes.

j) Cuando sea necesario realizar cambios en la configuración de los equipos, se deberá tomar las medidas necesarias para no cometer errores y afectar a la entrega normal de los servicios; además se deberá obtener la autorización documentada del Gerente Nacional de Operaciones y Sistemas para cualquier modificación.

En caso de que la empresa lo considere oportuno, podrá tomar medidas que, cumpliendo con la legislación, minimicen el impacto ocasionado en el servicio prestado a sus usuarios.

3.2 CLASIFICACIÓN DE LA INFORMACIÓN

Objetivo:

Garantizar que la información reciba el nivel de protección adecuado, considerando su valor, requisitos legales, sensibilidad e importancia, además de estar debidamente identificada.

3.2.1 DIRECTRICES DE CLASIFICACIÓN

La clasificación de la información debe ser realizada en base a su valor, requisitos legales, sensibilidad e importancia para la empresa.

Dicha clasificación debe considerar la posibilidad de compartir o restringir la información, analizando el impacto que tendrían estos hechos. Se utilizan cuatro niveles de clasificación de la información:

a) Pública: Podrá ser compartida o transmitida libremente, sin la necesidad de autorización o controles de seguridad, pues su divulgación no podría afectar en la entrega normal de los servicios ni en el funcionamiento de la empresa.

b) Moderadamente sensible: Su compartición requiere la aprobación del Jefe Regional NOC R1.

c) Muy Sensible: Para ser compartida o transmitida, se necesita de la aprobación del Gerente Nacional de Operaciones y Sistemas; además se requerirá la aplicación de controles técnicos, como encriptación y almacenamiento seguro.

d) Extremadamente Sensible: Su compartición implica la aprobación del Gerente Nacional de Operaciones y Sistemas, el uso de controles criptográficos y almacenamiento seguro. El mal manejo de esta información podría ocasionar incidentes con graves consecuencias en la entrega de los servicios, por lo que su prioridad es la máxima.

Es responsabilidad de los propietarios de los activos, definir la clasificación de éstos y revisarla de forma periódica, asegurándose que el nivel de clasificación sea el apropiado.

En "Cálculo de Nivel de Importancia de activos de información para la Seguridad" (Tabla 4.12), se presenta información que podría servir a los propietarios para clasificar a los activos, considerando su importancia en la confidencialidad, integridad y disponibilidad de la información. Se recomienda a los propietarios que consideren a los activos de mayor NI como los que requieren un mayor grado de protección o manejo especial.

Para realizar inicialmente la clasificación, se debe considerar el inventario de activos de información, asegurándose que esté completo.

Para la revisión periódica de la clasificación, se consideran los incidentes detectados, modificaciones físicas o lógicas en la red, cambios en los privilegios de acceso. Dicha revisión debe ser realizada semestralmente, es decir dos veces durante la vigencia de la Política de Seguridad de la Información, antes de su revisión.

Se debe evitar la superclasificación, pues se podría originar la implementación de controles innecesarios, ocasionado costos adicionales.

3.2.2 ETIQUETADO Y MANEJO DE LA INFORMACIÓN

Los lineamientos a seguir para el etiquetado de la información son los siguientes:

a) Se etiquetarán todos los activos de información que permiten la entrega de los servicios; considerando activos en formatos físicos y electrónicos.

b) Todos los equipos ubicados en el Centro de Datos y en los nodos, contarán con etiquetas físicas impresas directamente en los equipos, que contengan la siguiente información:

- Nombre de la empresa.
- Nombre del nodo o si se encuentra en el Centro de Datos.
- Distintivo particular del equipo, según el código del inventario manejado por el propietario de los equipos y de bodega.
- Distintivo de la clasificación de la información involucrada en el activo, reflejándose así las directrices de clasificación; este indicador solo debe ser de entendimiento para la empresa. Por ejemplo, para la clasificación Pública, se podría utilizar el distintivo (1), para la clasificación Moderadamente Sensible el distintivo (2), (3) para Muy Sensible y (4) para Extremadamente Sensible.

c) En la configuración de los equipos, también se incluirá la etiqueta, como parte de la configuración del *banner* de cada equipo, como se muestra en el Documento B1.

d) En el caso de compartición de información, ésta debe incluir como etiqueta electrónica, el distintivo de la clasificación de la información involucrada en el archivo, siguiendo la convención adoptada en el literal b).

e) En los acuerdos con otras organizaciones, que impliquen la compartición de información, se deberá incluir los procedimientos para identificar e interpretar la clasificación de la información y sus etiquetas.

4.1 ANTES DE LA CONTRATACIÓN LABORAL

Objetivo:

Asegurar que el personal sea apto para desempeñar sus funciones y que comprenda sus responsabilidades. Reducir el riesgo de posibles amenazas humanas, como divulgación, robo o mal uso de los activos.

4.1.1 ROLES Y RESPONSABILIDADES

Antes de la contratación laboral, se deben establecer las responsabilidades y funciones que tendrá a cargo la persona que se desea contratar, en cuanto a la seguridad de la información. Se debe considerar:

Comunicar al aspirante sobre la existencia de las políticas de seguridad de la información en la empresa, haciéndole conocer que su gestión debe ir acorde con las mismas.

Informar sobre la importancia de resguardar los activos contra acceso, divulgación, modificación, destrucción o interferencia no autorizados.

Informar sobre los procesos de seguridad que debería llevar a cabo, y de los cuales sería responsable. Además se debe indicar al aspirante sobre su obligación en comunicar cualquier evento de seguridad, o riesgos que detecte.

4.1.2 SELECCIÓN

Se realizarán revisiones de verificación, garantizando la privacidad y la protección de datos personales. Para la selección se seguirá el procedimiento establecido en el diagrama de la Figura PR1.

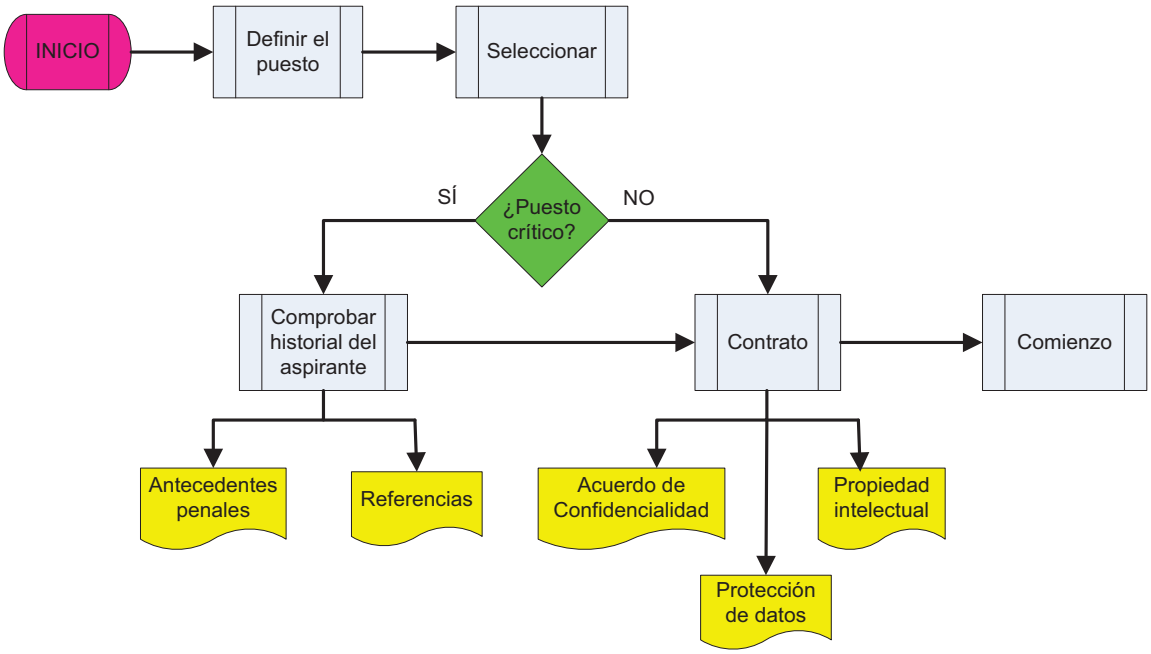


Figura PR1: Diagrama de selección del candidato

Para el caso de candidatos del Departamento de Operaciones y Sistemas, todos los puestos son considerados como críticos, dada la sensibilidad de la información que se maneja. El Departamento de Recursos Humanos será responsable de:

Informar a los candidatos sobre todas las actividades de selección, incluidas las verificaciones.

Solicitar a todos los candidatos una referencia personal, que no sea familiar, de preferencia docente; y dos referencias laborales. En caso de que el aspirante no haya trabajado anteriormente, se requerirán dos referencias personales.

Verificar la identidad del candidato, en base a su Cédula de Identidad o Pasaporte.

En caso de que el puesto a ocupar, implique el acceso a información extremadamente sensible, se verificará la hoja de vida del candidato; constatando su totalidad y exactitud. La determinación del nivel de información a ser utilizada, será realizada por el Jefe Regional NOC R1.

En caso de que no se tenga certeza sobre las calificaciones académicas declaradas por el candidato, y que éstas fueran necesarias, se acudirá a la Institución Académica, solicitando la confirmación de la información.

Verificar datos adicionales, dependiendo del puesto a ocupar; como antecedentes penales mediante el Récord policial, evasión o antecedentes de deuda mediante un informe en la Central de Riesgos.

Una vez seleccionados los candidatos que presenten el perfil más seguro para la empresa, el Departamento de Recursos Humanos comunicará al de Operaciones y Sistemas los resultados. El Jefe Regional NOC R1 será el encargado de la selección final, mediante una entrevista personal y una prueba de conocimientos.

En caso de que la selección se llevara a cabo con intervención de una agencia, el contrato con la agencia debe especificar sus responsabilidades para la selección y los procedimientos a seguir en caso de que la selección entregue resultados dudosos. De preferencia, la agencia debe seguir el mismo procedimiento que Megadatos S.A. para la selección del personal.

4.1.3 TÉRMINOS Y CONDICIONES LABORALES

Todos los empleados, contratistas y terceras partes, con acceso a información sensible, deben firmar un acuerdo de confidencialidad antes de tener acceso a los servicios de procesamiento de información.

De manera general, los derechos legales de los empleados y contratistas están sujetos al Artículo 42 del Capítulo IV del Código de Trabajo, referente a las Obligaciones del Empleador. Las responsabilidades legales se sujetan a los artículos 45 y 46 del Capítulo IV del Código de Trabajo, que hacen referencia a las Obligaciones y Prohibiciones del trabajador, respectivamente.

Como políticas internas de la Empresa, se concede al personal el derecho de utilizar la información, en base a la política de seguridad de la información; acceder a las aplicaciones o lugares de la empresa que requiera, siempre y cuando sus privilegios de acceso lo permitan. Derecho a realizar copias autorizadas de información, formar parte de los talleres de concientización y capacitación de seguridad de la información. Además podrán disponer de la información de los controles de seguridad implementados, si es que demuestra la necesidad de dicha información y está autorizado. Trabajar en áreas seguras, que no solo resguarden a los bienes materiales, sino también a los bienes humanos.

Son responsabilidades legales, establecidas por la empresa, velar por el cumplimiento de la política de seguridad de la información, respetar los privilegios de acceso, no divulgar información, seguir los lineamientos para el tratamiento de incidentes de la información, registrar sus actividades, hacer buen uso de los activos, prevenir al Departamento de Operaciones y Sistemas sobre cualquier riesgo detectado que pudiera afectar a la entrega de los servicios.

El personal que maneja determinado sistema o servicio de información, será el responsable de la gestión de los activos asociados a éstos; además debe colaborar con el propietario de los activos, durante la clasificación de la información y en las revisiones periódicas, sugiriendo correcciones o cambios de clasificación.

Para el tratamiento de información recibida de partes externas, es responsabilidad del personal, cumplir con la “Política de uso aceptable de los activos”, garantizando así que dicha información sea confiable y no nociva. Dependiendo de su contenido, la información deberá ser tratada por una persona en particular; siendo así el caso, la información proveniente de clientes debe ser tratada por los Asesores Tecnológicos o Ingenieros de Soporte. La información proveniente de proveedores, debe ser tratada por el Jefe Regional NOC R1 o por la Gerencia o Subgerencia del Departamento de Operaciones y Sistemas, dependiendo el caso. Si la procedencia de la información fuera desconocida, el responsable de tratarla será el Encargado de Seguridad de la Información.

En caso de ser necesario, los integrantes del Departamento de Operaciones y Sistemas, deberán trabajar en horarios fuera de lo establecido, con las mismas

responsabilidades, garantizando así el máximo esfuerzo para que la disponibilidad de los servicios sea ininterrumpida. De igual manera, cuando el personal realice trabajo de campo, se conservan las mismas responsabilidades.

En caso de que alguna persona incumpla con la “Política de seguridad de la información” o con los requisitos de seguridad de la empresa, será sometida a la “Política de proceso disciplinario”, una vez se haya verificado el incumplimiento.

4.2 DURANTE LA VIGENCIA DEL CONTRATO LABORAL

Objetivo:

Minimizar el riesgo de error humano, mediante la instrucción y concientización adecuadas. Garantizar el conocimiento del personal, referente al cumplimiento de las políticas de seguridad y las consecuencias de su no aplicación.

4.2.1 RESPONSABILIDADES DE LA DIRECCIÓN

a) Informar al personal acerca de sus responsabilidades y funciones, respecto a la seguridad de la información, antes de que tenga acceso a información o sistemas sensibles.

b) Proporcionar al personal las expectativas de seguridad de las funciones que tendrá a su cargo.

c) Asegurarse de que el personal esté de acuerdo con los términos y condiciones laborales, incluyendo a la Política de seguridad; mediante la firma de un documento que contenga los lineamientos de todos los términos.

d) Motivar al personal para el cumplimiento de las políticas de seguridad y concienciar sobre la importancia de la seguridad de la información, en las funciones que realiza, a través de talleres y cursos que deben ser realizados trimestralmente, y que evidencien la necesidad e importancia de la seguridad de la información.

e) Asegurarse que el personal tenga las calificaciones y habilidades adecuadas.

4.2.2 EDUCACIÓN, FORMACIÓN Y CONCIENTIZACIÓN SOBRE LA SEGURIDAD DE LA INFORMACIÓN

Una vez desarrolladas todas las políticas de seguridad de la información, se procede a la preparación, por parte del Encargado de Seguridad de la Información de la Empresa y de sus dos asesores, de un curso con duración de dos semanas.

En el curso se expondrá a los Departamentos de Operaciones y Sistemas, contratistas y terceras partes, acerca de las políticas de seguridad de la información desarrolladas para la empresa y las expectativas que se tiene de las mismas. El contenido del curso deberá estar documentado y dicho material deberá ser entregado a cada asistente. Los instructores deberán cerciorarse de

que todos los temas tratados hayan sido comprendidos, resolviendo las inquietudes y sometiendo a una evaluación a los asistentes.

Se desarrollarán cursos y talleres periódicamente, en los que se capacitará al personal sobre posibles modificaciones en las políticas de la empresa e innovaciones tecnológicas en seguridad de la información. Dichos cursos serán organizados por el Encargado de Seguridad de la Información de la Empresa, posibilitando la oportunidad de contar con instructores externos.

En el caso de personal nuevo, durante el tiempo de acoplamiento e instrucción sobre las tareas a realizar, también deberá ser capacitado en seguridad de la información y las políticas concernientes.

La capacitación debe incluir también la información sobre amenazas conocidas y su procedimiento de mitigación, detección de nuevas amenazas y el procedimiento de información sobre eventos de seguridad a los encargados, que deben ser los propietarios de los activos y el Encargado de la seguridad de la información de la Empresa.

4.2.3 PROCESO DISCIPLINARIO

En caso de presentarse algún incumplimiento con la seguridad de la información, los responsables serán sancionados de acuerdo a los siguientes literales:

a) El proceso disciplinario procede, una vez que la Gerencia o Subgerencia Nacional de Operaciones y Sistemas verifiquen la violación de la seguridad.

b) El proceso disciplinario será llevado a cabo de manera imparcial y en las mismas condiciones, sin privilegios ni exclusiones.

c) El Encargado de la seguridad de la información de la Empresa, junto al Gerente o Subgerente Nacional de Operaciones y Sistemas, analizarán la naturaleza, gravedad e impacto de la violación; además se deberá considerar si se trata de una reincidencia y si la infracción fue involuntaria o no.

d) Si se determina que la infracción no tuvo un impacto grave y que fue involuntaria, se precede al envío de un memorando al responsable del incumplimiento.

e) Se procede al retiro inmediato de las funciones, derechos de acceso físico y lógico, acompañamiento inmediato fuera de las instalaciones, si es necesario; en caso grave y de mala conducta. Dependiendo de los resultados del análisis, el retiro se realizará mediante despido, conforme al Artículo 188 del Capítulo X del Código de Trabajo; o a través de la solicitud del visto bueno al Ministerio de Trabajo, dependiendo el caso.

4.3 TERMINACIÓN O CAMBIO DE LA CONTRATACIÓN LABORAL

Objetivo:

Asegurar que la culminación o cambio del contrato laboral de un empleado, contratista o tercera parte, sea adecuada, estableciendo procedimientos que garanticen la seguridad de la información, aún cuando alguna persona termine con sus funciones en la empresa.

4.3.1 RESPONSABILIDADES EN LA TERMINACIÓN

En caso de terminación o cambio del contrato laboral, el Departamento de Recursos Humanos con la coparticipación del Jefe Regional NOC R1 y el Encargado de seguridad de la información de la Empresa, gestionarán el procedimiento. Se debe comunicar al implicado acerca de sus responsabilidades:

a) Conservar el compromiso permanentemente de no atentar contra la seguridad de la información de la Empresa; ya sea mediante divulgación, o en general la utilización inapropiada de la información. Para ello, en el acuerdo de confidencialidad que todo el personal acepta inicialmente, se debe incluir la permanencia de su vigencia.

b) Aceptar la terminación de las funciones, junto con los privilegios de acceso.

c) Entregar todo activo de información de la Empresa; incluso documentos de su autoría, al Encargado de seguridad de la información, quien se cerciorará que ha recibido el archivo original y las copias, en caso de existir. El Encargado de seguridad deberá recibir el activo con firmas de entregado y recibido, la fecha y los detalles de dicho evento. Dependiendo de la información contenida en el material, el Encargado procederá a eliminarla de manera segura o entregarla a un nuevo responsable.

d) En caso de ser necesario, el Jefe Regional NOC R1, podría solicitar la continuidad de los términos y condiciones laborales por un período no mayor a un mes. Esto podría ocurrir si es que en alguna cláusula del contrato laboral se incluyó la culminación de determinada actividad.

El cambio en la contratación laboral, debe ser gestionado de la misma forma que la culminación. Una vez terminado el proceso de culminación del contrato laboral, se procederá con el proceso detallado en la “Política Antes de la Contratación laboral”.

El Departamento de Recursos Humanos tendrá la responsabilidad de informar a los demás empleados, contratistas y terceras partes sobre los cambios en los acuerdos operativos y de personal.

4.3.2 DEVOLUCIÓN DE ACTIVOS

Los asesores del Encargado de la seguridad de la información de la Empresa, deben conservar un inventario de todos los activos, bajo la responsabilidad de cada uno de los empleados, incluyendo: software, documentos corporativos, equipos, dispositivos de cómputo, tarjetas de acceso, manuales e información almacenada en medios electrónicos.

Dicho inventario debe ser revisado semestralmente y los asesores deberán documentar el procedimiento, con las firmas correspondientes de cada responsable de activos.

En caso de que se produzca la culminación o cambio del contrato laboral, los asesores y el Encargado de seguridad de la información, recibirán los activos, conforme al último inventario. En este punto, el procedimiento continúa como se detalla en el literal c) de Responsabilidades en la terminación.

Cuando un empleado, contratista o tercera parte tenga un conocimiento importante para la continuación de las operaciones, el Encargado de la seguridad de la información deberá solicitar la documentación y transferencia de la información a la empresa.

4.3.3 RETIRO DE LOS DERECHOS DE ACCESO

Antes de la culminación o cambio de la contratación laboral, el Encargado de seguridad de la información y el Jefe Regional NOC R1, reconsiderarán los derechos de acceso de la persona a los activos asociados con los sistemas y servicios de información; determinando así la necesidad o no del retiro de los derechos de acceso.

Los derechos de acceso que deben ser considerados, incluyen acceso físico, lógico, contraseñas, tarjetas de identificación, servicios de procesamiento de información, suscripciones y retiro de toda documentación que identifique al implicado como miembro de la empresa.

Para la determinación del cambio o no de derechos de acceso, se considerarán tres aspectos fundamentales:

a) El motivo de la culminación o el cambio y si la iniciativa fue del empleado o de la dirección.

b) Las responsabilidades y funciones que desempeña el empleado.

c) El valor de los activos a los que tiene acceso.

En caso de que el implicado disponga de contraseñas colectivas, se procederá al cambio inmediato. Además el Departamento de Recursos Humanos procederá a informar a los demás empleados, contratistas y terceras partes sobre los cambios en los acuerdos operativos y de personal.

5.1 ÁREAS SEGURAS

Objetivo:

Especificar las áreas que alojan activos con información crítica para la empresa, para otorgar el acceso únicamente a personal autorizado, evitando de esta manera daño o interferencia de la información.

5.1.1 PERÍMETRO DE SEGURIDAD FÍSICA

Para la aplicación de las posteriores normas del perímetro de seguridad física, se deberá considerar la Tabla de Inventario de activos, en la cual constan los costos correspondientes y las Matrices de Riesgo, de tal forma que:

a) Se establece que el Centro de Datos esté ubicado dentro de las oficinas del Departamento de Operaciones y que la puerta de acceso a éste será controlada con tarjeta magnética. Adicionalmente, para el caso de personas externas, el Centro de Datos estará protegido con mostradores de recepción atendidos.

b) En el caso de los nodos, la infraestructura en donde se encuentran ubicados, deberá ser revisada por el Administrador de Red Física y Regulaciones, de tal forma que se cumplan los siguientes requisitos:

- Las cerraduras de las puertas deberán encontrarse en buen estado; en caso de detectarse que éstas se encuentran forzadas, oxidadas, etc, se deberá cambiarlas inmediatamente.

- Las ventanas deberán ser selladas, de tal forma que no puedan ser abiertas por ningún motivo. Adicionalmente se deberán colocar cortinas opacas en los nodos, con el fin de que no se exponga a la vista los dispositivos que se encuentran dentro.

- Se deberá tener por lo menos dos barreras físicas de protección para el ingreso al nodo, es decir se tendrá que contar con dos cerraduras independientes, o una cerradura y un candado.

c) Se deberá implementar un sistema de alarma en cada uno de los nodos, cuyas claves serán otorgadas únicamente al personal de operaciones y serán controladas por el Administrador de Red Física y Regulaciones.

5.1.2 CONTROLES DE ACCESO FÍSICO

Para el acceso al Centro de Datos y a los diferentes nodos, se determina lo siguiente:

Cada área del Departamento de Operaciones dispondrá de una tarjeta magnética para el acceso al Centro de Datos.

El área de soporte administrará y será custodio de los juegos de llaves de acceso a los nodos. El Jefe Regional NOC R1 será responsable del almacenamiento de todas las llaves en un lugar seguro y al que solo tenga acceso el personal del área.

Para el caso de ingresos planificados, el personal deberá notificar vía correo electrónico al Jefe Regional NOC R1, con 24 horas de anterioridad, la solicitud

de ingreso al sitio, indicando los trabajos que se realizarán, fecha, hora, y personal responsable. Sin una autorización escrita no se permitirá el ingreso. Adicionalmente, antes del ingreso al Centro de Datos o a los nodos, se deberá llenar un registro.

Para el caso de ingresos emergentes, una vez que se ha solventado el incidente, se deberá enviar un correo electrónico al Jefe Regional NOC R1 indicando el trabajo realizado.

Para el caso de partes externas o clientes, la solicitud de ingreso deberá ser enviada al Jefe Regional NOC R1, con 24 horas de antelación, especificando el personal que ingresará, cédula de identidad y los trabajos a realizarse. El ingreso deberá ser autorizado de forma escrita y en él se especificará el personal a cargo del Departamento de Operaciones que supervisará el trabajo y se responsabilizará de cualquier incidente de seguridad que se pudiera producir.

5.1.3 SEGURIDAD DE OFICINAS, RECINTOS E INSTALACIONES

Para mantener la seguridad de las instalaciones se consideran los siguientes estatutos:

a) El Centro de Datos será aquel que nunca estará expuesto al acceso público; se lo conservará siempre funcionando dentro de las instalaciones del Departamento de Operaciones.

b) Se determina que no se pondrá ningún tipo de señalización en los nodos que hagan referencia a la presencia de equipos de procesamiento de Información, con el fin de mantener la discreción en estas áreas.

c) Por ningún motivo se proporcionará la ubicación física de los nodos a personas externas, salvo el caso que exista una autorización del Gerente Nacional de Operaciones y Sistemas.

5.1.4 PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y AMBIENTALES

Para la minimización del impacto en caso de amenazas para la seguridad externas o ambientales, se deberán tomar en consideración los siguientes puntos:

Mantener copias de respaldo de la información en lugares alejados a los nodos y el Centro de Datos, de modo que si éstos se viesen afectados por algún desastre, se pueda actuar con rapidez para minimizar el tiempo de indisponibilidad.

Para el Centro de Datos y nodos se deberá instalar un sistema de ventilación adecuado, con el fin de evitar el sobrecalentamiento de equipos que den inicio a un incendio.

Los equipos deberán estar correctamente adaptados y sujetos en los *racks*, de tal forma que en caso de presentarse un temblor, éstos no tengan la posibilidad de caerse o verse afectados.

En el caso de los nodos, no se almacenará el combustible para los generadores de respaldo dentro del lugar; de ser requerido se deberá adquirir en dicho momento, utilizarlo y retirarlo cuando ya no sea necesario.

El Centro de Datos contará con un extinguidor contra incendios para combatir fuegos clase C, el mismo que será verificado periódicamente y renovado de acuerdo a lo indicado por el fabricante. Además se deberá publicar el instructivo de forma clara y en un lugar visible, de manera que el personal se encuentre preparado para actuar en caso de emergencia.

5.1.5 TRABAJO EN ÁREAS SEGURAS

Los trabajos a realizarse dentro de áreas que contengan información crítica para la empresa deberán cumplir los siguientes puntos:

a) Todos los trabajos en el Centro de Datos y en los nodos deberán ser autorizados y supervisados de acuerdo a lo especificado en los controles de acceso físico.

b) No se permitirá que se obtengan imágenes (fotos o filmaciones) del interior de los nodos o Centro de Datos, salvo que exista la autorización escrita del Gerente Nacional de Operaciones y Sistemas, en la cual se mencione el objetivo de dichas imágenes.

5.1.6 ÁREAS DE CARGA, DESPACHO Y ACCESO PÚBLICO

a) El personal de despacho deberá identificarse con la recepcionista de la Empresa y una vez que esté autorizado podrá pasar al Departamento de Operaciones para realizar su entrega formal en la sala de reuniones del Departamento de Operaciones.

b) Los activos que ingresan serán etiquetados y probados por la persona a cargo del equipo, la cual deberá verificar que éste no genere ninguna amenaza a su entrada, ni durante su operación.

c) El personal de despacho ingresará únicamente a la sala de reuniones para hacer la entrega del equipo, salvo el caso de que éste deba ser instalado en el lugar de operación; en dicho caso se aplicarán los controles de acceso físico.

5.2 SEGURIDAD DE LOS EQUIPOS

Objetivo:

Proteger a los activos de daños físicos y ambientales, tomando en cuenta el costo económico que tiene cada uno.

5.2.1 UBICACIÓN Y PROTECCIÓN DE LOS EQUIPOS

Todos los trabajadores deberán seguir los siguientes estatutos, con el fin de proteger los equipos utilizados para la prestación de servicios en la ciudad de Quito:

a) Los equipos de *core* serán ubicados en el Centro de Datos; mientras que los de equipos de distribución y acceso serán adecuados en los nodos o el Centro de Datos, de acuerdo a lo requerido. En estos lugares se mantendrán las directrices estipuladas en los controles de acceso físico.

b) Tanto en el Centro de Datos, como en los nodos está prohibido el ingreso o consumo de alimentos y bebidas.

c) El Administrador de Red Física y Regulaciones deberá implementar protección contra rayos en aquellos lugares donde no se dispone.

5.2.2 SERVICIO DE SUMINISTRO

Se deberán tomar en cuenta los lineamientos que se presentan a continuación, para mantener la seguridad de la información en caso de fallas en los servicios de suministro:

a) En caso de fallo a nivel eléctrico, los equipos del Centro de Datos y de los nodos estarán conectados a un UPS, el cual proporcionará un tiempo de respaldo de al menos 1 hora.

El Administrador de Red Física y Regulaciones será el encargado de realizar el análisis, en cada sitio, para dimensionar la carga que el UPS deberá soportar; así también tendrá la responsabilidad de proporcionar el respectivo mantenimiento cada 3 meses.

b) Se deberá contar con 3 generadores de energía (como mínimo), para dar continuidad a las operaciones del negocio, en caso de que se prolongue la falla del servicio. El área de soporte será la responsable de monitorear el estado de los nodos a nivel eléctrico y en caso de detectar que el respaldo del UPS no será suficiente, asignará a una persona para que se dirija al nodo y conecte el generador al UPS.

c) Se deberá verificar que el suministro de agua sea el adecuado para alimentar el aire acondicionado instalado en el Centro de Datos. El equipo de aire acondicionado deberá ser sometido a revisiones cada 6 meses.

5.2.3 SEGURIDAD EN EL CABLEADO

El cableado instalado en el Centro de Datos y nodos deberá cumplir con las siguientes especificaciones:

a) Las líneas de energía y de telecomunicaciones serán subterráneas o aéreas, de acuerdo a la estructura física del lugar.

b) Se deberá separar el cableado utilizado para la parte eléctrica y el cableado de comunicaciones, con el fin de evitar interferencia.

c) El Centro de Datos y los nodos deberán contar con equipos que permitan la correcta organización del cableado, tales como ODFs y *patch pannels*.

d) Todos los cables deberán ser etiquetados correctamente en los dos extremos; así también los equipos a los cuales se conectan, deberán especificar la dirección IP, propietario, servicio que prestan y en cada puerto indicar el enlace asociado (cliente).

e) El Jefe de Implementación y Gestión de Red R1 deberá realizar planos del cableado del Centro de Datos y cada uno de los nodos, los cuales serán actualizados cada vez que se realiza una modificación.

5.2.4 MANTENIMIENTO DE LOS EQUIPOS

Se deberá realizar el mantenimiento de los equipos ubicados en el Centro de Datos y en los nodos, de acuerdo a las siguientes indicaciones:

a) Los mantenimientos de equipos administrados por la Empresa Megadatos serán efectuados únicamente por el personal del área de Infraestructura, previa autorización del Gerente Nacional de Operaciones y Sistemas.

b) Los mantenimientos a equipos de administración de terceras partes o clientes, deberán ser solicitados con 24 horas de antelación y una vez obtenida la aprobación, los trabajos serán supervisados por personal del área de soporte.

c) Se realizarán los mantenimientos de los equipos de acuerdo a lo especificado por los fabricantes; sin embargo se hará una revisión general del Centro de Datos y nodos una vez al mes.

d) En caso de registrarse un mantenimiento emergente debido a falla en la operación del equipo, se deberá notificar a todo el personal de operaciones el trabajo efectuado.

e) El Jefe de Implementación y Gestión de Red R1 deberá mantener un registro de los trabajos efectuados en cada uno de los equipos, especificando las fallas reales o sospechadas, la fecha del mantenimiento, personal a cargo y el mantenimiento preventivo o correctivo realizado.

5.2.5 SEGURIDAD DE LOS EQUIPOS FUERA DE LAS INSTALACIONES

Los equipos que se encuentran fuera de las instalaciones son los equipos de Radio de Megared Inalámbrica, debido a la necesidad de ubicarlos en los exteriores para la transmisión efectiva de los datos. Se procurará resguardar los nodos, de modo que los equipos externos no estén expuestos a riesgos como robo o mal uso.

En el caso del cableado que conduce los datos de los servicios, a lo largo de las redes, se procurará ubicarlos de modo que se minimicen los riesgos de corte accidental o intencional; de todos modos se contará con cableado de respaldo en bodega, que deberá ser reemplazo inmediatamente en caso de producirse algún incidente.

5.2.6 SEGURIDAD EN LA REUTILIZACIÓN O ELIMINACIÓN DE LOS EQUIPOS

Los equipos que sean dados de baja por deterioro o daño deberán ser sometidos a las siguientes ordenanzas:

a) Los equipos provenientes del Centro de Datos o de nodos, deberán ser revisados por el Administrador de Ingeniería, el que eliminará toda la información en él contenida. Posteriormente el equipo será revisado nuevamente por el Jefe de Implementación y Gestión de Red R1, el cual realizará un reseteo manual del equipo, para posteriormente enviarlo al seguro o a bodega.

b) En caso de ser equipos de última milla, éstos serán retirados y enviados sin ninguna revisión previa al seguro, debido a que en ellos no se dispone de información relevante.

5.2.7 RETIRO DE ACTIVOS

Para el retiro de activos se deberán seguir las siguientes directrices:

a) El Gerente de Operaciones y Sistemas deberá emitir una autorización para que un activo sea retirado del Centro de Datos o nodos.

b) El Jefe de Implementación y Gestión de Red R1 llevará un registro de los activos que hayan sido retirados, especificando la fecha, persona a cargo, tipo de equipo, número de serie y adjuntando la autorización respectiva.

6.1 PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES

Objetivo:

Garantizar que los procedimientos operacionales sean ejecutados adecuadamente, estableciéndose las responsabilidades para el personal del Área de Operaciones.

6.1.1 DOCUMENTACIÓN DE LOS PROCEDIMIENTOS DE OPERACIÓN

Para garantizar que los procedimientos de operación sean manejados adecuadamente, se establecen las siguientes directrices:

a) En caso de que se requiera modificar la configuración de un equipo que permite la entrega de servicios, se deberá solicitar la autorización respectiva y documentar todos los cambios realizados y entregar dicha información al Jefe de Implementación y Gestión de Red R1. Adicionalmente, una vez que se concluyan los trabajos en los equipos, se deberán cerrar las sesiones adecuadamente, de modo que ninguna persona no autorizada pueda ingresar a una sesión no concluida.

b) El Jefe de Implementación y Gestión de Red R1 deberá mantener una copia de respaldo de la configuración de cada uno de los equipos y actualizar la información en caso de que se hayan generado cambios. La información respaldada será almacenada en formato electrónico, bajo la política de controles de encriptación; además se mantendrá una copia impresa que estará disponible únicamente para personal autorizado.

c) Para la realización de mantenimientos de los equipos, configuraciones o migraciones, se deberá planificar en horarios no laborables, de tal forma que se reduzca el impacto de afectación a los clientes. Además éstos deberán ser notificados oportunamente con 48 horas de anticipación.

d) Si se cometiera un error durante la ejecución del trabajo, se procederá a detenerlo e inmediatamente analizar el impacto del error. Si se tratara de un error leve y de fácil solución, el involucrado deberá solventarlo y documentar el evento. Si el error fuera grave o de solución compleja, se informará al Jefe de Implementación y Gestión de Red R1 acerca del incidente, quien se encargará de la solución y documentación respectiva; además deberá cerciorarse de que el servicio afectado se haya recuperado.

e) En caso de producirse dificultades técnicas u operativas inesperadas, se deberá contactar al Jefe de Implementación y Gestión de Red R1; sin embargo, si éstas tuvieran un origen externo se deberá contactar al respectivo proveedor, a través de la intranet de la empresa.

6.1.2 GESTIÓN DEL CAMBIO

Se establecerá un control estricto de la gestión del cambio de los sistemas que están involucrados en la prestación de servicios. Para ello se deberán llevar a cabo las siguientes actividades:

a) Para todo cambio a realizarse en los sistemas que permiten la entrega de los servicios, se deberán realizar pruebas previas, con el fin de medir la efectividad del cambio y asegurarse de no producir impactos negativos en la prestación de los servicios, incluyendo la seguridad de la información.

b) Se establecerá un documento de control de cambios, en el cual se estipulará el responsable del trabajo, el tipo de mantenimiento a realizarse, la fecha y hora de ejecución y los clientes afectados. Este documento deberá ser aprobado por el Jefe de Implementación y Gestión de Red R1 y por el Gerente Nacional de Operaciones y Sistemas. Posteriormente, la información deberá ser entregada al Jefe Regional NOC R1, quien estará a cargo de la notificación respectiva a los clientes, con 48 horas de anticipación. En caso de ser un mantenimiento emergente, el procedimiento será similar; sin embargo la notificación no tendrá un tiempo de antelación estipulado.

c) Una vez concluidos los cambios, se deberá documentar y registrar los procedimientos realizados y los resultados obtenidos. Dicha información, junto al documento aprobado de control de cambios, serán almacenados por el Gerente General de Operaciones y Sistemas.

6.1.3 DISTRIBUCIÓN DE FUNCIONES

Para reducir el riesgo de uso inadecuado de los sistemas utilizados en la prestación de los servicios, se procederá a distribuir las funciones entre todo el personal del Departamento de Operaciones, de la siguiente manera:

a) El Nivel Directivo será el responsable de promover el cumplimiento de la Política de Seguridad de la información establecida en el Departamento, además se encargará de aprobar y revisar periódicamente dicha política. El Encargado de seguridad de la información pertenecerá a este nivel y supervisará el funcionamiento adecuado del SGSI.

b) El Nivel Ejecutivo tomará las responsabilidades del Nivel Directivo, en caso de que éste no se encuentre presente. Además se encargará del seguimiento de la solución de los incidentes detectados.

c) El Nivel Ejecutor será el encargado de solventar los incidentes detectados, documentando y registrando todos los eventos.

d) El Nivel Operativo tendrá a su cargo la utilización adecuada y segura, a nivel físico, de los activos.

6.1.4 SEPARACIÓN DE LAS INSTALACIONES DE DESARROLLO, ENSAYO Y OPERACIÓN

Se establece la presente política, ante la necesidad de garantizar que se realicen pruebas previas a la implementación de determinada aplicación o equipos, de manera aislada.

Las personas encargadas del desarrollo y ensayo de nuevas aplicaciones o equipos, serán el Jefe de Implementación y Gestión de Red R1, los Administradores de Ingeniería y los Ingenieros de Instalaciones.

Se utilizará un sistema aislado al de operación, mediante contraseñas distintas, para la ejecución de las pruebas. Una vez confirmado el funcionamiento correcto, se asignarán las contraseñas al personal del Departamento de Operaciones.

6.2 GESTIÓN DE LA PRESTACIÓN DEL SERVICIO POR TERCERAS PARTES

Objetivo:

Definir las responsabilidades de la prestación de los servicios por terceros, dando énfasis a la seguridad de la información.

6.2.1 PRESTACIÓN DEL SERVICIO

La prestación de servicios por terceros, deberá garantizar la confidencialidad, integridad y disponibilidad de la información. Se deberá incluir en el contrato, una cláusula que especifique que la información de la empresa manejada por el proveedor, no será divulgada ni usada inadecuadamente; y en caso de incumplimiento, se establecerán las sanciones respectivas.

Se deberá confirmar que el proveedor cuente con los controles necesarios, que garanticen la seguridad y continuidad de la prestación de los servicios, en caso de presentarse desastres o fallas significativas.

6.2.2 MONITOREO Y REVISIÓN DE LOS SERVICIOS POR TERCEROS

Para garantizar el cumplimiento de los términos y condiciones de seguridad de la información con terceros, se establecerán los siguientes lineamientos:

a) Mediante el sistema de monitoreo, administrado por un Ingeniero de Soporte designado, se llevará un registro de los indicadores de disponibilidad de cada uno de los proveedores, en el cual se determinará si la entrega del servicio está conforme al contrato.

b) Se deberá incluir en los contratos, la obligación del envío de reportes mensuales, que incluyan análisis de la confidencialidad, integridad y disponibilidad de la información mantenida en ese período; así también estipular que trimestralmente se realicen reuniones para verificar los registros y pruebas de auditoría con respecto a eventos de seguridad.

c) El Encargado de seguridad de la información deberá dar seguimiento a cada uno de los problemas identificados, que deberán ser registrados.

6.2.3 GESTIÓN DE LOS CAMBIOS EN LOS SERVICIOS POR TERCERAS PARTES

Cuando se planeen cambios en los servicios por terceras partes, será necesario recibir una notificación que detalle los trabajos, con 72 horas de anticipación, con el fin de que el Encargado de seguridad de la información evalúe los riesgos, impacto y nuevos requerimientos que conllevaría el cambio.

Si el Encargado de seguridad de la información determina que el cambio notificado es factible y que no tendrá impacto negativo para la empresa, enviará una aprobación firmada por el Gerente Nacional de Operaciones y Sistemas a la tercera parte. En caso de detectar algún inconveniente o conflicto, se convocará a una reunión para acordar los detalles.

6.3 PLANIFICACIÓN Y ACEPTACIÓN DEL SISTEMA

Objetivo:

Especificar los recursos requeridos que permiten garantizar la disponibilidad de la capacidad de los sistemas.

6.3.1 GESTIÓN DE LA CAPACIDAD

Para dar seguimiento al uso de los recursos y planificar adecuadamente con proyecciones a futuro, se deberá realizar un análisis de la capacidad. Los propietarios de los activos serán responsables de mantener el 10% de la capacidad total, libre, de tal forma que un crecimiento sea factible. En caso de que la capacidad disponible estipulada anteriormente, se reduzca, los propietarios deberán solicitar los recursos para conservar el mínimo establecido.

Se realizará la asignación de responsabilidades, conforme a la Política de Distribución de funciones, de modo que no se centralice la información.

6.3.2 ACEPTACIÓN DEL SISTEMA

Para que un sistema sea implementado, con el fin de servir a la entrega de los servicios, el Jefe de Implementación y Gestión de Red R1 deberá presentar un documento en el cual se justifique la necesidad de tal sistema, las pruebas realizadas, resultados obtenidos y la autorización del Gerente Nacional de Operaciones y Sistemas. Adicionalmente, el nuevo sistema deberá estar sujeto a las Políticas de Gestión del cambio y Separación de las instalaciones de desarrollo, ensayo y operación.

La persona encargada de la implementación de determinado sistema, será responsable de poner en conocimiento del personal las nociones sobre el funcionamiento de éste; en caso de ser necesario deberá enviar el manual respectivo.

6.4 PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS Y MÓVILES

Objetivo:

Prevenir y detectar ataques a la red que proporciona los servicios, incluyendo virus, gusanos, troyanos, ataques DoS, entre otros; mediante la implementación de políticas, software y hardware.

6.4.1 CONTROLES CONTRA CÓDIGOS MALICIOSOS

Con el fin de proteger a la red que provee servicios, contra códigos maliciosos, se configurarán seguridades a nivel de capa 2. Además se propone la

implementación del dispositivo de seguridad ASA 5540 incorporando el módulo AIP-SSM. Los beneficios se detallan en el Documento B1.

A parte de la propuesta técnica mencionada anteriormente, se deberán seguir los siguientes lineamientos:

El uso de software no autorizado está estrictamente prohibido. El Coordinador Nacional de Sistemas, junto al Encargado de Seguridad de la información, son los únicos autorizados en aprobar el uso de determinado software, una vez se haya evaluado su funcionamiento e impacto.

Todo archivo recibido, deberá ser sometido al análisis correspondiente, eliminando la posibilidad de que contenga paquetes maliciosos. Todo software detector y eliminador de amenazas, deberá ser actualizado regularmente; siendo confiable y seguro.

Los asesores del Encargado de seguridad de la información, deberán investigar la presencia de archivos no aprobados o modificaciones no autorizadas; en caso de detectar algún incidente, comunicarán de inmediato a su supervisor para proceder a la aplicación de la Política de proceso disciplinario.

El Encargado de seguridad de la información y sus asesores, deberán estar informados e instruidos acerca de innovaciones en ataques a redes y códigos maliciosos, así como métodos para eliminarlos; además deberán revisar quincenalmente los sistemas, garantizando que no hayan accedido códigos maliciosos a los mismos. En caso de detectarlos, se procederá inmediatamente

a un plan de mitigación, procurando no afectar en la disponibilidad de los servicios; se incorporarán los controles que sean necesarios, sometidos previamente a pruebas. Una vez superado el incidente, se verificará que éste haya sido solventado y que ningún sistema haya sido afectado durante los trabajos realizados. Todos los procedimientos deberán ser documentados.

En el Documento B1 (ver Anexos), se propone la implementación del módulo AIP-SSM; a través de éste será posible obtener información periódica sobre los intentos de ataque o introducción de códigos maliciosos a la red. Los asesores del Encargado de seguridad de la información deberán analizar estas estadísticas quincenalmente y elaborar los reportes adecuados; posteriormente el Encargado de seguridad de la información y el Coordinador Nacional de Sistemas deberán tomar acciones que superen cualquier intento de ataque.

6.4.2 CONTROLES CONTRA CÓDIGOS MÓVILES

Debido a que el uso de códigos móviles no es imprescindible en el Departamento de Operaciones y Sistemas para proveer los servicios a los clientes, se prohibirá la ejecución o recepción de los mismos. Si existiera la necesidad de utilizar un código móvil, se deberá solicitar al Encargado de seguridad de la información la autorización correspondiente con los motivos para tal petición.

6.5 RESPALDO

Objetivo:

Contar con respaldo de toda la información relacionada con la entrega de los servicios; dichos respaldos serán elaborados periódicamente y en base al nivel de sensibilidad de la información involucrada.

6.5.1 RESPALDO DE LA INFORMACIÓN

Toda la información y software necesarios en la entrega de los servicios, deberán contar con un respaldo, de modo que puedan ser recuperados después de un desastre o falla. Para ello, se determina:

a) Toda la información clasificada como pública, tendrá una copia de respaldo, como archivo de Word, Excel, Power Point o Visio. El respaldo de la información moderadamente sensible, será en archivo de Word, Excel, Power Point o Visio, pero con restricción de acceso. Para las clasificaciones muy sensible y extremadamente sensible, el respaldo será conservado en formato pdf con restricción de copia. Todos los respaldos sin protección estarán bajo la responsabilidad del Encargado de seguridad de la información.

b) Toda la información deberá ser respaldada al menos una vez cada seis meses, excepto aquella información que varía con mayor frecuencia. Se deberá documentar el procedimiento, cuando se realice el respaldo de la información.

c) Se incorporarán medios criptográficos, en base al Documento B1, para proteger la información sensible que requiera mayor seguridad.

6.6 GESTIÓN DE LA SEGURIDAD DE LAS REDES

Objetivo:

Proteger a los servicios proporcionados a los clientes, en el trayecto a lo largo de las redes; además incorporar controles que garanticen la confidencialidad, integridad y disponibilidad de los servicios.

6.6.1 CONTROLES DE LAS REDES

Se deberá garantizar la seguridad de la información sobre las redes y proteger los servicios contra el acceso no autorizado; para ello se establece:

a) Tan solo los computadores del Área de Operaciones y del Coordinador Nacional de Sistemas, tendrán acceso a la operatividad de las redes que proporcionan los servicios a los clientes; inclusive el personal indicado tendrá restricciones para determinadas aplicaciones, dependiendo el caso.

b) El acceso remoto a todos los equipos, deberá realizarse vía ssh. Los equipos deberán tener al menos tres usuarios con contraseñas diferentes; dichos usuarios serán destinados a las Áreas de Infraestructura, Instalaciones y Soporte, siendo los jefes directamente responsables de comunicar al personal a su cargo de las mismas. Los permisos que contenga cada usuario estarán dados por los requisitos solicitados por los jefes departamentales y serán

validados por el Encargado de seguridad de la información.

c) De existir la sospecha de que una persona no autorizada tenga conocimiento de los nombre de usuario y contraseñas, el Encargado de seguridad de la información deberá proceder con el cambio inmediato de dichos parámetros.

d) Se deberán especificar las redes permitidas para acceder remotamente a los equipos, las mismas que deben ser comunicadas únicamente al personal autorizado. De requerirse la conexión desde otra red, se solicitará la autorización del Jefe de Infraestructura, así como de la Gerencia de Operaciones y Sistemas.

e) Al ingresar a cualquier equipo del *backbone*, se deberá presentar un *banner* advirtiendo sobre las restricciones de acceso; en el Documento B1 se presenta la configuración respectiva.

f) En caso de realizarse cambios en la configuración de los equipos, no se podrá grabar hasta que el responsable técnico tenga la seguridad que los cambios no afectarán al servicio.

g) Con la implementación del servidor Syslog y del ASA-5540, detallados en el Documento B1, será posible el registro y monitoreo de las acciones de seguridad con mayor facilidad.

6.6.2 SEGURIDAD DE LOS SERVICIOS DE LA RED

Dado que Megadatos S.A., es una empresa dedicada a la entrega de servicios a través de redes, resulta imprescindible contar con controles que garanticen la seguridad de los mismos. Se incorporarán enlaces de *backup* para asegurar la disponibilidad de los servicios en caso de falla del principal, como se detalla en el Documento B1.

En el caso de asegurar los servicios de Internet y correo electrónico, se proponen configuraciones básicas de los *routers* y *switches*, el tratamiento de ataques en capa 2 mediante filtrado; además se propone la implementación del dispositivo ASA 5540 y el módulo AIP-SSM, los cuales incorporan mayor seguridad en el acceso, detección de intrusiones, aviso de incidentes, entre otros. Todos estos controles, descritos en el Documento B1, proporcionarán mayor seguridad a los servicios que atraviesan las redes.

6.7 MANEJO DE LOS MEDIOS

Objetivo:

Garantizar que no se produzcan modificaciones, retiros, divulgación o destrucciones de activos, sin la autorización correspondiente. Controlar el mantenimiento y almacenamiento apropiado de los medios.

6.7.1 GESTIÓN DE LOS MEDIOS REMOVIBLES

Los asesores del Encargado de seguridad de la información, deberán encargarse del cumplimiento de las siguientes directrices:

a) Eliminar el contenido que no sea útil, de los medios (discos, memorias de almacenamiento, discos compactos, medios impresos), de modo que la información sea irrecuperable e inaccesible. Toda eliminación deberá ser autorizada por el Jefe de Implementación y Gestión R1, documentada y registrada. Una vez que se autorice el retiro, los asesores analizarán el contenido del medio y eliminarán la información correspondiente.

b) Se deberá asegurar que los medios que contengan información asociada a la entrega de servicios, se encuentren registrados, en un ambiente seguro y vigilado, en base a las especificaciones del fabricante y bajo la responsabilidad de los asesores y del Encargado de seguridad de la información.

6.7.2 ELIMINACIÓN DE LOS MEDIOS

Con el propósito de eliminar los medios, de manera segura, minimizando el riesgo de fuga de información, se deberán seguir los siguientes lineamientos:

a) El Encargado de seguridad de la información, con ayuda de los asesores, serán los responsables de almacenar y eliminar de forma segura los medios; dicha eliminación será realizada mediante borrado de los datos y trituración. Se analizará semestralmente los medios que deberían ser eliminados de forma segura, solicitando la autorización correspondiente al Jefe de Implementación y Gestión R1.

b) El Encargado de seguridad de la información y los asesores, serán los responsables de la eliminación de los datos; mientras que se solicitará el servicio de un contratista para la trituración respectiva. Para la selección del

contratista se deberá garantizar que éste sea idóneo, que cuente con controles y la experiencia adecuada.

c) Toda eliminación de elementos, deberá ser documentada y registrada adecuadamente.

6.7.3 PROCEDIMIENTOS PARA EL MANEJO DE LA INFORMACIÓN

Para evitar el uso inadecuado o divulgación de la información, se establecen los siguientes literales:

a) Se deberá garantizar que todos los medios que contengan información concerniente a la entrega de servicios, se encuentren sujetos a la Política de Control de activos; además se deberá asegurar que el etiquetado de cada medio, esté asociado adecuadamente a su nivel de clasificación. Para ello, se deberá realizar una revisión semestral, documentando los procedimientos realizados y cualquier evento anómalo detectado.

b) Todo el personal, así como los clientes, estarán sujetos a la Política de Control de Acceso; mediante las restricciones detalladas en la política indicada, se evitará el acceso de personal no autorizado

c) A través de las Políticas de Validación de los datos de entrada y de salida, se garantizará que los datos de entrada estén completos y que se aplique la validación de la salida.

d) Para la protección de los datos de la memoria temporal, se considerará el nivel de sensibilidad de la información. Se debería aplicar controles criptográficos, como los propuestos en el Documento B1, para el almacenamiento de información con niveles altos de sensibilidad. O se podría optar por la eliminación segura periódica de dicha información, si no es imprescindible su almacenamiento.

e) Para el almacenamiento de los medios, se deberá considerar las indicaciones del fabricante, evitando posibles daños por almacenaje inadecuado.

f) Todas las copias de los medios, deberán estar rotuladas adecuadamente e incluir la opción de autenticación para los usuarios, la cual deberá ser revisada o modificada, cada tres meses o si se presentara un cambio de funciones o salida de algún empleado.

6.7.4 SEGURIDAD DE LA DOCUMENTACIÓN DEL SISTEMA

La documentación de los sistemas que permiten la entrega de servicios, deberá ser almacenada físicamente con seguridad, bajo la responsabilidad del propietario del sistema respectivo; la seguridad también deberá existir para la documentación almacenada en archivo, bajo controles criptográficos y restricción de acceso.

El acceso a la documentación de los sistemas será restringido, de modo que solo el personal que realmente la necesita, tenga acceso a la misma. El propietario del sistema respectivo, determinará los privilegios de acceso.

6.8 INTERCAMBIO DE LA INFORMACIÓN

Objetivo:

Garantizar la seguridad de la información intercambiada entre el personal de la empresa y con terceras partes.

6.8.1 POLÍTICAS Y PROCEDIMIENTOS PARA EL INTERCAMBIO DE INFORMACIÓN

Se establecen las siguientes directrices para realizar intercambio de información vinculada a la entrega de servicios:

La información intercambiada será protegida contra intercepción, mediante controles incorporados a nivel de capa 2, autenticación, autorización, criptografía y aislamiento mediante listas de acceso; dichos controles se detallan en el Documento B1. Para evitar el copiado y modificación de la información que se intercambie, ésta deberá ser enviada de preferencia en formato pdf y restricción de copiado.

Toda la información intercambiada deberá seguir los lineamientos establecidos en la Política contra códigos maliciosos.

Toda información sensible que sea enviada como archivo adjunto, deberá ser encriptada mediante un algoritmo que ofrezca la seguridad adecuada; garantizando que solo los receptores autorizados tengan acceso a la misma.

En cuanto a la información intercambiada mediante servicios de comunicación electrónica, deberán estar sujetas a la Política de Uso aceptable de los activos.

Se deberá restringir el uso de comunicaciones inalámbricas, por parte de todo el personal de la empresa, dado que se podrían generar interferencias. El Encargado de seguridad de la información, deberá analizar el impacto de la utilización de los sistemas generadores de comunicaciones inalámbricas, considerando las frecuencias de operación de los mismos y las de los sistemas utilizados para proveer servicios a los clientes.

Se deberá obligar a los empleados, contratistas y terceras partes en no comprometer a la empresa, mediante la divulgación de información sensible, que pudiera poner en riesgo la confidencialidad, integridad y disponibilidad de los servicios. Para tal propósito se aplicará la Política de Roles y responsabilidades.

La responsabilidad del tratamiento de la correspondencia recibida, se establece en el literal d) de la Política de Términos y condiciones laborales; los responsables deberán determinar el tratamiento que requerirá la información recibida, tanto en su retención como en la eliminación. En caso de no tener seguridad total acerca del tratamiento, se solicitará apoyo al Encargado de seguridad de la información.

Se prohíbe el abandono de información, asociada a la entrega de los servicios, en medios de impresión. Cualquier empleado que requiriera imprimir dicha información, deberá hacerlo en la impresora asignada a su área y recogerla inmediatamente.

El personal deberá tomar precauciones como: evitar conversaciones telefónicas afuera de la empresa, que pudieran proveer información de la entrega de los servicios; no tratar información sensible mediante llamadas telefónicas ni dejarla en contestadoras automáticas, utilizar correctamente el fax y las fotocopiadoras.

6.8.2 ACUERDOS PARA EL INTERCAMBIO

Los siguientes parámetros se deberán incluir en los acuerdos para el intercambio de la información y software entre la empresa y las partes externas:

La Gerencia de Operaciones y Sistemas tendrá la responsabilidad de controlar y notificar la transmisión, despacho y recepción de todo intercambio, al encargado de la parte externa. A su vez, el encargado de la parte externa tendrá la obligación de controlar y notificar la transmisión, despacho y recepción del intercambio.

Con el fin de garantizar el no-repudio de la información intercambiada, se deberá tener conocimiento previo de que se realizará dicho intercambio y garantizar que éste se efectúe satisfactoriamente.

Si se requiriera el servicio de un contratista de mensajería, se deberá garantizar que éste sea confiable e idóneo para la entrega; de ser posible, se deberá solicitar el servicio de mensajería que normalmente utiliza la empresa.

Si se presentara cualquier tipo de incidente, como la pérdida de información, será responsabilidad de la persona que la envió, pues no habrá tomado las medidas adecuadas para el envío. Ante tal situación, se aplicará la Política de proceso disciplinario. Además, será responsabilidad del implicado, solventar el incidente.

Se utilizarán etiquetas en la información, especificando su nivel de sensibilidad. Para la comprensión de las etiquetas, por parte del receptor, éste deberá ser informado previamente acerca de las mismas. Además se podrán utilizar controles criptográficos para el intercambio, con previo conocimiento y consentimiento de las partes implicadas.

Será responsabilidad de los propietarios, proteger los datos durante el intercambio. En cuanto a los derechos de copia y licencias de software, se designarán responsables al Encargado de seguridad de la información y al Coordinador Nacional de Sistemas.

6.8.3 MEDIOS FÍSICOS EN TRÁNSITO

Será responsabilidad de la persona que envíe un medio, asociado a la entrega de los servicios: utilizar transporte o servicios de mensajería confiables que estén incluidos en la lista de contratistas autorizados, exigir la utilización de paquetes y cintas apropiados para no sufrir deterioro durante el trayecto.

Si el medio involucrara información considerada como sensible para la entrega de los servicios, se deberán adoptar controles como el uso de contenedores cerrados con llave, entrega personal y sellos de seguridad.

6.8.4 MENSAJERÍA ELECTRÓNICA

Para garantizar la protección adecuada a los mensajes electrónicos dentro de la empresa, se aplicará la Política de Uso aceptable de los activos. Para los usuarios del servicio de correo electrónico que ofrece la empresa, los mensajes serán protegidos mediante la incorporación de un Servidor TACACS+, que trabajará en conjunto con el dispositivo de seguridad ASA-5540 para proporcionar autenticación segura a los usuarios; los detalles de este control se especifican en el Documento B1.

Con el control propuesto, se podrá garantizar la protección de los mensajes contra acceso no autorizado, el transporte correcto, confiabilidad y disponibilidad del servicio.

6.9 MONITOREO

Objetivo:

Supervisar el funcionamiento y uso adecuado de los sistemas de información y aplicaciones necesarias para la entrega de los servicios. Disminuir el riesgo de actividades no autorizadas y verificar la eficacia de los controles adoptados.

6.9.1 REGISTRO DE AUDITORÍAS

Deberán ser conservados los registros de las actividades de los usuarios y de eventos de seguridad de la información, por cuestiones de auditoría. En los registros deberán incluir:

Identificación del usuario involucrado en la actividad o evento, incluyendo su nombre de usuario y área a la que pertenece.

La fecha, hora y detalles necesarios sobre la actividad o evento.

Listas de intentos aceptados y rechazados de acceso al sistema y a los datos; para ello se utilizarán los comandos correspondientes del ASA-5540, para observar las estadísticas de los eventos ocurridos; también se utilizarán los indicadores de los servidores RADIUS y TACACS+ con dicho fin. Se deberá realizar la revisión indicada, al menos 2 veces al mes.

Deberá existir constancia de todo cambio realizado en los sistemas, configuraciones, red, privilegios de acceso, mediante registros.

Se deberán conservar los registros de todas las alarmas originadas por el sistema de monitoreo con que actualmente cuenta la empresa, de los mensajes Syslog originados por el ASA, sistemas antivirus, cualquier eventualidad registrada por el servidor de autenticación, autorización y registro.

6.9.2 MONITOREO DE USO DEL SISTEMA

Para el monitoreo de uso de los sistemas, se deberá incluir:

En el monitoreo de acceso autorizado, se considerará la identificación de usuario, fecha y hora de los eventos, el tipo de evento; además de los datos y programas a los que se ha tenido acceso durante la sesión. Para dicho monitoreo se manejarán las utilidades que ofrece el dispositivo de seguridad ASA.

El monitoreo de las operaciones privilegiadas incluirán el uso de cuentas y el inicio o detención de los sistemas que permiten la entrega de los servicios.

Para el monitoreo de intentos de acceso no autorizados, incluyendo acciones fallidas, rechazadas, violaciones a la política de acceso y detección de intrusión, se aplicarán las funcionalidades descritas en el literal a) de la presente política, detalladas en el Documento B1; también será utilizado el literal e) de la Política de Registro de auditorías. Si se detectaran anomalías por parte del personal, se procederá con la aplicación de la Política de Proceso disciplinario.

En el monitoreo de alertas, alarmas o fallas del sistema, serán considerados los mensajes obtenidos en el servidor Syslog, los mensajes proporcionados por el sistema de monitoreo y los resultados obtenidos de los comandos correspondientes en el ASA.

La frecuencia del monitoreo dependerá del nivel de sensibilidad asociado al sistema y de su utilización; así por ejemplo, el sistema de monitoreo con que actualmente cuenta la empresa deberá ser atendido de manera permanente. Los mensajes Syslog deberán ser revisados diariamente; en cuanto a la revisión correspondiente del dispositivo de seguridad ASA, deberá ser realizada al menos dos veces al mes.

6.9.3 PROTECCIÓN DE LA INFORMACIÓN DEL REGISTRO

La información contenida en los registros deberá ser protegida de alteraciones; para ello deberá estar al alcance de un número reducido de personas que realmente necesiten dicha información. Si fuera necesario editar o eliminar un

archivo de registro, se deberá indicar las razones para hacerlo y solicitar la autorización correspondiente al Encargado de seguridad de la información.

Para evitar la sobrecarga de almacenamiento de los medios de archivo de registro, se dispondrá de particiones en disco exclusivas para conservar los registros. Se revisará periódicamente el estado de la capacidad disponible de almacenamiento; de ser necesario, se deberá suprimir registros no necesarios, siguiendo el procedimiento descrito en el literal a) de la Política de Gestión de los medios removibles; o solicitar mayor capacidad en disco para los registros.

6.9.4 REGISTROS DEL ADMINISTRADOR Y DEL OPERADOR

Todas las actividades de operadores o propietarios de los sistemas, deberán incluir en sus registros los responsables, fecha, hora, detalles del evento, si se trató de una falla o mantenimiento.

Si se trató de un ingreso a los sistemas, se deberá especificar la cuenta de usuario utilizada para la actividad; además se incluirán los procesos que se vieron implicados y las actividades realizadas durante el trabajo.

Estos registros deberán ser realizados por los asesores del Encargado de seguridad de la información, junto al responsable de la actividad que se esté registrando, con soporte de los indicadores del sistema. Una vez terminado el registro, deberá ser revisado por el Encargado de seguridad de la información, quien se encargará de su almacenamiento.

6.9.5 REGISTRO DE FALLAS

Todas las fallas de los sistemas de información que permiten la entrega de los servicios, deberán estar sujetas a registro. El Encargado de seguridad de la información, junto al propietario del sistema o aplicación involucrada, deberá dar seguimiento al evento, en base a la información del registro; finalmente se deberá garantizar que la falla ha sido superada satisfactoriamente y mediante autorización del Jefe de Implementación y Gestión de Red R1.

Una vez superada la falla, el propietario del sistema o aplicación, deberá revisar las medidas correctivas; garantizando que no se hayan puesto en peligro los controles u otros sistemas.

6.9.6 SINCRONIZACIÓN DE RELOJES

Se requerirá que todos los sistemas de información que permiten la entrega, revisión o monitoreo de los servicios se encuentren sincronizados, de modo que se igualarán los relojes de todos los servidores y demás equipos, con el reloj configurado en el ASA.

La sincronización garantizará la exactitud de los registros y será necesaria para el análisis de eventos, investigaciones o evidencia en casos de procesos disciplinarios.

7.1 REQUISITOS DEL NEGOCIO PARA EL CONTROL DEL ACCESO

Objetivo:

Definir las reglas generales para controlar el acceso lógico y físico a los sistemas, aplicaciones e infraestructura necesaria para proveer los servicios, minimizando la probabilidad de acceso no autorizado y mal uso de la información.

7.1.1 POLÍTICA DE CONTROL DE ACCESO

Para controlar el acceso lógico y físico de los usuarios, se procederá a determinar los siguientes parámetros:

a) Deberán ser considerados los requisitos de seguridad de todas las aplicaciones y sistemas utilizados para brindar los servicios a los clientes. En el caso de todos los procedimientos de operación, se considerará como requisito fundamental la utilización y acceso exclusivo por parte del personal autorizado, la realización de pruebas previo a toda implementación y la no afectación de la confidencialidad, integridad y disponibilidad de la información. Para la entrega de los servicios, los tres requisitos fundamentales serán la confidencialidad, integridad y disponibilidad de la información asociadas a los mismos.

b) Toda la información involucrada en las aplicaciones y sistemas que permiten proporcionar los servicios, deberá ser identificada, así también como los riesgos a los que podría enfrentarse. Para la identificación de riesgos, se deberá considerar el Análisis y evaluación del riesgo desarrollado y sus posibles modificaciones.

c) Los jefes de cada Área, serán los encargados de determinar el acceso a la información que tendrá cada empleado, en base a sus funciones y responsabilidades dentro de la empresa. Deberá comunicarle sobre sus privilegios de acceso, otorgarle los recursos necesarios e informarle sobre la confidencialidad y uso personal de los mismos. Se deberá incluir en el contrato laboral dichas obligaciones.

d) Existirán perfiles estándar de acceso de usuario para funciones laborales comunes; de modo que determinadas actividades no dependan exclusivamente de una persona. Para ello se aplicará el literal b) de la Política de Controles de las redes. Cuando se realicen cambios en dichas cuentas, se deberá informar oportunamente a los usuarios con acceso autorizado a la aplicación correspondiente.

e) Los derechos de acceso deberán ser comunicados, junto a la sanciones por incumplimiento. Para controlar el acceso lógico, se utilizarán los datos proporcionados por el dispositivo de seguridad ASA y por los servidores de acceso, que se encargarán de la autenticación, autorización y registro de las solicitudes.

f) Cada jefe de Área será el encargado de analizar las necesidades de acceso y autorizar la incorporación o retiro de privilegios, con previa información al Encargado de seguridad de la información. Además tendrá la responsabilidad de revisar periódicamente los controles de acceso utilizados por los sistemas y aplicaciones manejadas en su Área.

7.2 GESTIÓN DEL ACCESO DE USUARIOS

Objetivo:

Garantizar que solo los usuarios autorizados tengan acceso a los sistemas de información y aplicaciones; y que además el acceso sea negado a usuarios no autorizados.

7.2.1 REGISTRO DE USUARIOS

Para controlar el registro de usuarios, se procederá a:

a) Establecer el uso de identificadores únicos de usuario e identificadores de grupo tan solo en los casos establecidos por el literal b) de la Política de Controles de las redes. Todo identificador debe ser aprobado y documentado por el propietario correspondiente.

b) Los propietarios de los activos, sistemas y aplicaciones deberán verificar que todos los usuarios de éstos, tengan su autorización y que no se esté dando mal uso de los privilegios de acceso. Además tendrán la obligación de mantener un registro de los usuarios autorizados.

c) Los usuarios deberán recibir una declaración escrita de sus derechos de acceso, que tendrá que ser firmada y acatada en su totalidad, sin acceder a sistemas o aplicaciones que no consten en la declaración.

d) No se concederá ningún derecho de acceso hasta que el proceso de autorización haya culminado.

e) Será necesaria la revisión de los privilegios de acceso, por parte del propietario del activo, sistema o aplicación, de modo que se generen cambios en los privilegios si se han producido cambios de funciones o retiro del trabajo.

7.2.2 GESTIÓN DE PRIVILEGIOS

Para el manejo eficaz de los privilegios de acceso, se establecen las siguientes directrices:

a) En base al literal f) de la Política de Control de acceso, se identificarán los usuarios y sus privilegios de acceso; además se definirá la asignación de privilegios, en función de la necesidad, bajo el criterio del Jefe de Área.

b) El Jefe de Área conservará el proceso de autorización y el registro de todos los privilegios asignados.

c) Se asignarán los privilegios a identificadores de usuario, diferentes a los utilizados para el uso normal.

7.2.3 GESTIÓN DE CONTRASEÑAS PARA USUARIOS

Para la gestión de contraseñas, se procederá con los siguientes parámetros:

a) Durante los términos y condiciones laborales, se exigirá a los usuarios la firma de una declaración de su compromiso por mantener la confidencialidad de las contraseñas personales y de conservar las contraseñas de grupo únicamente entre los miembros.

b) Para las aplicaciones y sistemas utilizados en la entrega de servicios, que manejen contraseñas personales, se suministrará una contraseña temporal segura; dicha contraseña deberá ser cambiada por el usuario en un plazo máximo de 48 horas.

c) Todas las contraseñas predeterminadas por el proveedor, deberán ser cambiadas una vez se instale el sistema, equipo o software. Para el caso de los *switches* y *routers* que conforman la red, en el Documento B1 se establecen los comandos para realizar el procedimiento.

d) Se prohíbe el almacenamiento de las contraseñas en sistemas de computador en formato no protegido; para el almacenamiento se deberán utilizar controles criptográficos. Los asesores del Encargado de seguridad de la información tendrán la responsabilidad de verificar que se esté cumpliendo con este control.

7.2.4 REVISIÓN DE LOS DERECHOS DE ACCESO DE LOS USUARIOS

La revisión de los derechos de acceso de los usuarios se realizará trimestralmente y después de cada cambio; mientras que la revisión de los derechos de acceso privilegiado deberá realizarse al menos bimestralmente. Todos los cambios en las cuentas, deberán ser registrados para la revisión.

7.3 RESPONSABILIDADES DE LOS USUARIOS

Objetivo:

Definir las responsabilidades de los usuarios; de modo que se minimicen los riesgos de acceso no autorizado, divulgación o robo.

7.3.1 USO DE CONTRASEÑAS

Las contraseñas deberán estar sujetas a las siguientes condiciones:

a) Mantenerse bajo confidencialidad. Solo deberán ser de conocimiento del usuario a quien se le haya asignado el acceso a la aplicación o sistema asociado a la contraseña; para controlar el cumplimiento de este literal, deberá ser incluido en los contratos laborales del personal.

b) No se deberán almacenar las contraseñas en papel, archivos de software o dispositivos sin autorización. El Encargado de seguridad de la información será la persona que podrá autorizar el almacenamiento de contraseñas, de forma segura y mediante un método aprobado.

c) Se procederá al cambio de contraseñas cuando éstas sean puestas en peligro, cuando existan cambios en los privilegios de acceso, cuando algún empleado del Departamento termine sus funciones en la empresa. También se procederá al cambio de contraseñas de manera periódica, sin necesidad de que ocurra algún evento de los especificados anteriormente; de preferencia se deberá realizar el cambio dependiendo el grado de sensibilidad de la aplicación o sistema.

d) Las contraseñas deberán ser de calidad, no guardar relación con los usuarios. Además no deben ser palabras de diccionario, su longitud deberá ser mínimo de 10 caracteres alfanuméricos y especiales, por ejemplo: anTi$_aTaque34#. No deberán ser fáciles de recordar y se deberá evitar el uso de caracteres idénticos consecutivos o de únicamente caracteres numéricos o alfabéticos. Los usuarios no deberán utilizar para sus labores en la empresa, las contraseñas que dispongan en aplicaciones ajenas al trabajo.

e) Todas las contraseñas temporales deberán ser cambiadas en un tiempo máximo de 48 horas; será responsabilidad del usuario que utilizará la contraseña realizar el cambio.

f) Ningún usuario podrá compartir sus contraseñas individuales con otras personas. Los asesores del Encargado de seguridad de la información deberán supervisar el cumplimiento de esta política; en caso de que se detectara su incumplimiento, se procederá con la Política de proceso disciplinario.

g) De preferencia, los usuarios a quienes se les asigne varias cuentas para el acceso a diferentes sistemas o aplicaciones, deberán utilizar claves distintas.

7.3.2 EQUIPO DE USUARIO DESATENDIDO

Un equipo desatendido en el Departamento de Operaciones y Sistemas, podría implicar modificaciones no autorizadas, acceso no autorizado, divulgación o robo de información. Dado el impacto que ocasionaría tal incidente, todos los

usuarios responsables de las aplicaciones y sistemas que permiten proveer los servicios, deberán terminar las sesiones activas cuando finalicen los trabajos.

Se configurarán los equipos, de modo que se presenten protectores de pantalla protegidos por contraseña, si es que existiera inactividad por más de 10 minutos. Además se deberá asegurar los computadores y terminales contra el uso no autorizado, mediante el acceso por contraseña personal.

Todo el personal del Departamento deberá apagar sus computadores, en cuanto termine su jornada laboral; a menos que se requiera la ejecución de monitoreo, en cuyo caso se deberá comunicar al jefe del Área correspondiente.

7.3.3 POLÍTICA DE ESCRITORIO DESPEJADO Y DE PANTALLA DESPEJADA

El abandono de información sensible relacionada con la entrega de los servicios, en pantalla o en un escritorio, podría ocasionar la utilización inadecuada, divulgación y robo de la información. Para evitar tales riesgos, se procederá a adoptar la política de escritorio y pantalla despejados. Se considerarán la Política de Clasificación de la información, los requisitos legales y los riesgos asociados.

Toda información considerada como crítica, deberá ser guardada en caja fuerte y bajo llave. Para reforzar este control, se aplicará la Política de Equipo desatendido, mediante el bloqueo de sesiones inactivas. También se aplicará el literal h) de las Políticas y procedimientos para el intercambio de información, evitando así el abandono de información en medios de impresión; para tal propósito se podrían adquirir impresoras con función de código de pines.

7.4 CONTROL DE ACCESO A LAS REDES

Objetivo:

Controlar el acceso a los sistemas, aplicaciones y servicios, tanto internos como externos, evitando el acceso no autorizado.

7.4.1 POLÍTICA DE USO DE LOS SERVICIOS EN RED

Para garantizar que los usuarios accedan únicamente a los servicios a los cuales están autorizados, se establecen los siguientes lineamientos:

a) Los jefes de cada Área del Departamento de Operaciones y Sistemas analizarán sobre las redes y servicios a los que cada usuario de su Área debería tener acceso. Para el caso de los clientes, el Jefe Regional NOC R1 será el encargado de dicho análisis. Una vez concluidos los análisis, se procederá a solicitar la autorización del Gerente Nacional del Departamento; entonces se procederá a la asignación correspondiente.

b) Se incorporarán controles automáticos, que verifiquen el cumplimiento de la presente política. El dispositivo de seguridad ASA, permitirá crear listas de acceso y grupos de autenticación; además facilitará la autorización y registro de las actividades.

c) Para acceder a las redes, se utilizarán los medios proporcionados y autorizados por la empresa; bajo ningún concepto se deberá duplicar o

utilizar recursos de los clientes. Para reforzar la presente política se aplicará la Política de controles de las redes.

7.4.2 AUTENTICACIÓN DE USUARIOS PARA CONEXIONES EXTERNAS

Se incorporará autenticación para todos los usuarios del servicio de Internet y de correo electrónico. Como se plantea en el Documento B1, para los usuarios de los servicios *dial-up* y correo electrónico, se utilizará un servidor TACACS+; mientras que los usuarios de los servicios de banda ancha y corporativo, estarán asociados a un servidor RADIUS, que deberá realizar una autenticación transparente para el usuario. Los servidores, además permitirán el bloqueo de conexiones no deseadas o no autorizadas.

Ambos servidores utilizan controles criptográficos, de modo que la información asociada en la autenticación se transmitirá de manera segura.

Para controlar el acceso de los clientes asociados a nodos de Megared inalámbrica, cualquiera sea el servicio proporcionado, se debería optar por el servidor TACACS+, que incorpora mayor seguridad, necesaria para el intercambio de información en un medio inseguro como lo es el inalámbrico.

7.4.3 IDENTIFICACIÓN DE LOS EQUIPOS EN LAS REDES

Con el propósito de autenticar conexiones de equipos y ubicaciones específicas, se identificarán todos los equipos en las redes.

De manera lógica, se procederá a configurar los equipos, con nombres adecuados, que especifiquen con claridad de qué equipo se trata y qué nivel de importancia tiene. La configuración se detalla en el Documento B1.

Para la identificación física, se deberá incorporar al equipo, una etiqueta que contenga información sobre las redes a las cuales puede ser conectado, y la sensibilidad de dichas redes.

7.4.4 PROTECCIÓN DE LOS PUERTOS DE CONFIGURACIÓN Y DIAGNÓSTICO REMOTO

Para proteger los puertos de configuración y diagnóstico remoto, se utilizarán las cuentas asignadas con contraseñas proporcionadas al personal con acceso autorizado a la configuración y diagnóstico de las redes. Se aplicará la Política de Controles de las redes.

Se deberá inhabilitar o retirar los puertos, servicios, aplicaciones que no sean necesarias para la entrega y revisión de los servicios.

7.4.5 SEPARACIÓN EN LAS REDES

Se requerirá separar los entornos de seguridad de la red; para ello se propone la creación de servidores de autenticación diferentes para el personal y los empleados dentro del grupo de autenticación. Tan solo el personal debería tener acceso al dispositivo de seguridad, por ello se plantea la respuesta exclusiva al personal para solicitudes de acceso serial, privilegiado y telnet. Los demás equipos que conforman la red, restringirán el acceso no autorizado, mediante contraseñas.

Existirán entornos de red aislados para la realización de pruebas y desarrollo de sistemas y aplicaciones, eliminando el riesgo de cambios no autorizados e incorporación de fallas.

Se deberán separar las redes inalámbricas, a través de controles adicionales como los descritos en la Política de Autenticación de usuarios para conexiones externas.

7.4.6 CONTROL DE CONEXIÓN A LAS REDES

Conforme a la Política de Control de acceso, se deberán mantener y actualizar los derechos de acceso a la red. Los controles propuestos se detallan en el Documento B1; dichos controles deberán ser aplicados a la mensajería, transferencia de archivos, acceso interactivo, acceso a las aplicaciones. Además se deberán revisar las conexiones establecidas y fallidas, mediante los servidores de autenticación y el dispositivo de seguridad incorporado.

7.4.7 CONTROL DEL ENRUTAMIENTO EN LA RED

Para controlar el enrutamiento correcto en la red, se cuenta con protocolos de capa 3 que proporcionan un nivel confiable de enrutamiento, verificándose las direcciones fuente y destino. El dispositivo de seguridad generará mensajes Syslog en caso de detectar errores en el envío o recepción de información, sospechando un posible ataque o riesgo.

7.5 CONTROL DE ACCESO AL SISTEMA OPERATIVO

Objetivo:

Evitar que usuarios no autorizados accedan a los sistemas operativos que permiten proporcionar los servicios a los clientes.

7.5.1 PROCEDIMIENTOS DE REGISTRO DE INICIO SEGURO

Para garantizar un buen procedimiento de registro de inicio, los encargados de su mantenimiento deberán evitar la publicación de información hasta que el proceso de registro de inicio se haya completado satisfactoriamente; además se deberá mostrar una advertencia sobre la restricción del acceso.

No se deberán suministrar mensajes de ayuda durante el registro de inicio, pues usuarios no autorizados podrían beneficiarse de ellos y lograr el acceso. La validación de la información de registro deberá ser efectuada una vez que se hayan terminado todos los datos de entrada; en caso de que el sistema detectara un error, no se deberá indicar al usuario qué información fue correcta e incorrecta.

Para el acceso, se limitará la cantidad de intentos permitidos a 3; los servidores de autenticación serán los encargados de esta función. Para ello, se detalla en el Documento B1, la configuración correspondiente. Resultaría conveniente establecer en los servidores, tiempos de dilación antes de permitir intentos adicionales de registro de inicio. También convendría utilizar el sistema de contraseñas ocultas mediante símbolos y la criptografía para transmitir las contraseñas por la red.

Dado que el dispositivo de seguridad ASA trabaja en conjunto con los servidores de autenticación, será posible que se almacenen los registros exitosos y fallidos, junto a los detalles respectivos, posibilitando a los administradores del sistema acceder a dicha información.

7.5.2 IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS

Cada jefe de Área concederá identificadores de usuario (ID) a los empleados de los cuales es responsable; para ello deberá aplicar el literal c) de la Política de Control de acceso. Los identificadores serán utilizados por el jefe del Área para controlar el acceso físico y lógico de los usuarios; además servirán para rastrear y monitorear sus actividades.

Solo en el caso descrito en el literal b) de la Política de Controles en la redes, se utilizarán identificadores de usuario compartido; lo que evitará la dependencia de un solo usuario en determinadas funciones en el Departamento de Operaciones.
Los servidores de autenticación TACACS+ y RADIUS proporcionan verificación sólida de autenticidad, pues emplean al protocolo CHAP durante el proceso de autenticación. Para reforzar la seguridad de la autenticación en el acceso físico a los nodos y al Centro de Datos, será conveniente implementar medios biométricos, como un lector de huellas digitales que contenga almacenada la información del personal con acceso autorizado; de modo que cuando se registre un acceso, se registren también los detalles del mismo.

7.5.3 SISTEMA DE GESTIÓN DE CONTRASEÑAS

El sistema de gestión de contraseñas, con el fin de monitorear las actividades de los usuarios y conservar responsabilidades, se basará en identificadores de usuario (ID) y contraseñas.

El sistema deberá permitir el cambio de contraseñas de los usuarios, imponiendo que éstas sean contraseñas de calidad, como se describe en el literal d) de la Política de Uso de contraseñas. En caso de que se detectara la intención de utilizar una contraseña que no cumpla con las condiciones requeridas, el sistema deberá indicar al usuario que la contraseña ingresada no cumple con las condiciones y que deberá utilizar otra.

Se deberá incorporar un *timer* de validez de contraseñas de los sistemas empleados por el personal para la entrega de los servicios; de manera que cada dos meses el sistema obligue a los usuarios a cambiar de contraseñas. El sistema deberá conservar un registro de las contraseñas empleadas.

Para el almacenamiento de las contraseñas, se deberán utilizar controles criptográficos y localidades de disco diferentes a las que contengan los datos del sistema de aplicación.

7.5.4 USO DE LAS UTILIDADES DEL SISTEMA

Para acceder a las utilidades del sistema, se deberán seguir las siguientes directrices:

a) Atravesar por un procedimiento de autenticación y autorización, mediante el uso de identificadores de usuario y contraseña, los cuales deberán ser limitados a una cantidad mínima de usuarios, de preferencia.

b) Todo uso de las utilidades del sistema, deberá ser registrado; dicho registro servirá para verificar que los niveles de autorización para las utilidades del sistema sean los adecuados y que estén siendo empleadas adecuadamente.

c) Todas las utilidades o software del sistema que sea innecesario para la prestación o revisión de los servicios, deberá ser retirado, puesto que podrían representar una vulnerabilidad para que se presenten amenazas.

7.5.5 TIEMPO DE INACTIVIDAD DE LA SESIÓN

En base a la sensibilidad de la información asociada a los sistemas o aplicaciones utilizadas para la entrega de los servicios, se determinará el tiempo de dilación adecuado para suspender las sesiones inactivas.

En el documento B1, se detallan los comandos a utilizar para la configuración de los equipos de la red y del dispositivo de seguridad, de modo que se establezcan tiempos de espera agotados que permitan el cierre de las sesiones.

7.5.6 LIMITACIÓN DEL TIEMPO DE CONEXIÓN

Se deberá limitar el tiempo de conexión para las aplicaciones consideradas como de alto riesgo. Los trabajos efectuados en el dispositivo de seguridad

ASA, deberán ser considerados como de alto riesgo, para lo cual se establece el tiempo agotado absoluto, descrito en el Documento B1.

Será conveniente conservar los tiempos límite de conexión, con que actualmente cuentan los equipos que conforman la red.

Se procederá a restringir los tiempos de conexión a las horas normales de oficina, a menos que se requiera tiempo extra u operaciones de horario prolongado; para ello, el jefe del Área que requiera la prolongación de tiempo, será el responsable de la autorización respectiva.

No se utilizará repetición de autenticación a intervalos determinados, excepto si el sistema detectara inactividad en la sesión, en cuyo caso se aplicará el tiempo agotado de inactividad.

7.6 CONTROL DE ACCESO A LAS APLICACIONES Y A LA INFORMACIÓN

Objetivo:

Evitar que usuarios no autorizados accedan a la información de los sistemas de aplicación.

7.6.1 RESTRICCIÓN DEL ACCESO A LA INFORMACIÓN

En base a la Política de Control de acceso, se restringirá el ingreso de los usuarios a la información. Para controlar el acceso a las funciones del sistema de aplicación, se deberá proporcionar menús a los usuarios, de modo que sea más sencillo ingresar a la función necesaria y evitar errores involuntarios.

Además se deberá restringir los derechos de acceso, como leer, escribir, eliminar y ejecutar, dependiente del usuario que haya accedido al sistema.

La información generada por los sistemas de aplicación, deberá ser manejada adecuadamente, evitando que sea enviada a terminales o sitios no autorizados.

7.6.2 AISLAMIENTO DE SISTEMAS SENSIBLES

Será necesario aislar los sistemas sensibles, en un entorno dedicado. Una vez que los propietarios de los sistemas y aplicaciones evalúen sus sensibilidades y los riesgos a los cuales se exponen, deberán determinar si se requiere o no aislamiento.

Se deberá proceder al aislamiento del ingreso a los equipos de *backbone* y al dispositivo de seguridad, de forma que solo el personal autorizado del Departamento de Operaciones y Sistemas pueda acceder a los mismos. Además se propone la determinación de niveles de seguridad diferentes en las interfaces del ASA, creando un aislamiento en las interfaces; de modo que toda la red de la empresa quede aislada de las redes externas, y se posibilite la comunicación solo para las redes especificadas como permitidas.

Mediante medios biométricos se podrá incorporar aislamiento físico en los lugares en los que se procesen sistemas sensibles.

8.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

Objetivo:

Incorporar a la seguridad como parte esencial de los sistemas de información.

8.1.1 ANÁLISIS Y ESPECIFICACIÓN DE LOS REQUISITOS DE SEGURIDAD

Los requisitos de seguridad que persigue la empresa son los siguientes:

a) El Encargado de la Seguridad de la Información de la Empresa, con respaldo de la Gerencia y Subgerencia del Departamento, analizarán y supervisarán la implementación de los controles necesarios que garanticen la seguridad de los sistemas de información. Se considerarán controles automatizados y manuales, según sea conveniente.

b) Se requieren directrices para la utilización autorizada de hardware y software; no se debe permitir el uso deliberado de éstos, pues podrían afectar en la entrega normal de los servicios.

c) Se requiere contar con un personal instruido en cuestión de Seguridad de la Información, que esté actualizado sobre posibles amenazas y que se encuentre capacitado para desarrollar sus responsabilidades.

d) El funcionamiento de todos los procedimientos que garantizan la seguridad de los sistemas de información, debe ser revisado periódicamente. Dicha revisión podría ser llevada a cabo a nivel de auditoría, en cuyo caso se requiere la seguridad apropiada.

e) La detección de amenazas, debe también incluir a aquellas que podrían ser generadas por la interacción de actividades laborales con entidades externas para proveer los servicios.

f) Los privilegios de acceso físico y lógico deben ser establecidos adecuadamente, de manera segura y deben ser revisados con regularidad. De preferencia se procurará establecer el uso de métodos biométricos, para el acceso físico, evitando así el uso no autorizado de las tarjetas de acceso. Para el acceso lógico, un elemento esencial serán las listas de acceso y la criptografía.

g) En caso de poner en peligro la seguridad de los sistemas de información, se deberá sancionar al infractor con lo estipulado la Política de proceso disciplinario.

h) Es indispensable separar o aislar aplicaciones, cuyo mal manejo pudiera afectar en el funcionamiento normal de otras.

i) No se pueden presentar fallas por un diseño mal realizado o planificado, ni por un procesamiento incorrecto de las aplicaciones; éste debe ser revisado continuamente y corregido en caso de ser necesario.

j) Se requieren controles que permitan detectar y eliminar amenazas provenientes de la red, como virus, gusanos, troyanos, ataque de diccionario, negación del servicio, entre otras.

k) Para la selección de controles, la empresa solicitará al menos a tres proveedores la cotización y detalle de los mismos. El Gerente y Subgerente Nacional de Operaciones y Sistemas determinarán la mejor opción, sometiéndola a prueba una vez adquirido; se analizarán los posibles riesgos introducidos y se tomarán medidas correctivas.

l) La aplicación de controles para garantizar la seguridad de la información, debe considerar un análisis económico, de tal forma que las inversiones no superen el valor de los activos protegidos.

8.2 PROCESAMIENTO CORRECTO EN LAS APLICACIONES

Objetivo:

Evitar posibles errores, pérdidas, uso inadecuado o modificaciones no autorizadas de la información en las aplicaciones.

8.2.1 VALIDACIÓN DE LOS DATOS DE ENTRADA

Todo dato que ingrese y sea un aporte para el funcionamiento y entrega normal de los servicios, será verificado. Las verificaciones que se realizarán son:

Verificaciones de entradas duales, de fronteras o campos limitantes, con el objetivo de detectar valores fuera de rango, exceso en los límites superiores e inferiores. Se procede a verificar que los anchos de banda contemplados en los contratos de los clientes, correspondan a los proporcionados por la aplicación HiperK[95]. Además se procederá a revisar si los recursos contratados a los proveedores son los que se estima en los contratos.

Los asesores del Encargado de la seguridad de la información, realizarán una revisión semestral, del contenido de los campos clave, archivos de datos, y documentos impresos, constatando su integridad.

Los sistemas de información deben incorporar un control de detección de caracteres inválidos, datos incompletos, datos de control inconsistentes, de modo que presenten al usuario el aviso correspondiente.

Se realizará la verificación de los procedimientos de respuesta ante errores de validación. Todo el personal tendrá la obligación de verificar los sistemas de acceso por contraseña, realizando cuatro pruebas, al menos una vez al mes:

- Ingresar el nombre de usuario correcto y una contraseña incorrecta.
- Ingresar el nombre de usuario incorrecto y la contraseña correcta.
- Ingresar tanto el nombre de usuario y de contraseña incorrectos.
- Ingresar tanto el nombre de usuario y de contraseña correctos.

[95] Aplicación utilizada en la Empresa para la gestión de contratos, ingreso de incidentes y revisión de indicadores de los requerimientos atendidos por los técnicos.

En caso de obtener una respuesta inesperada del sistema, informará inmediatamente al Encargado de seguridad de la información de la empresa, quien a su vez documentará el evento y lo reportará al Coordinador Nacional de Sistemas.

Para verificar la credibilidad de los datos de entrada, el receptor tendrá la obligación de realizar los procedimientos necesarios, como recálculo, ingreso a las configuraciones, envío de correo electrónico solicitando una confirmación, llamada telefónica; se debería utilizar cualquier método que, sin violentar en contra de la Política de seguridad de la información de la empresa, garantice la credibilidad de los datos.

Todo el personal participará en el proceso de entrada de datos; aquel que reciba información de clientes y proveedores, tendrá la obligación de validarla. Tan solo en el caso de una procedencia dudosa, se reenviará la información al Encargado de seguridad de la información de la empresa.

Todas las actividades implicadas en el proceso de entrada de datos, deberán ser registradas; esta información estará bajo en control del Encargado de la seguridad de la información de la empresa.

8.2.2 CONTROL DE PROCESAMIENTO INTERNO

Durante el diseño, implementación y revisión de las aplicaciones, se debe considerar que los riesgos de falla en el procesamiento deben ser prácticamente nulos; para ello, los desarrolladores de las aplicaciones deberán considerar los siguientes literales:

a) Las funciones “agregar”, “modificar” y “borrar” son críticas para realizar cambios en los datos. Los cambios podrían ser equívocos, por lo que se debe aplicar mayor seguridad a dichas funciones; se podría agregar una o dos ventanas de confirmación de la acción.

b) El Coordinador Nacional de Sistemas, incorporará las medidas necesarias para impedir que la ejecución de los programas se realice en un orden equivocado, afectando al funcionamiento adecuado de los sistemas de información.

c) Se utilizarán programas para la recuperación después de fallas. Si se ha perdido información importante para la entrega de los servicios, no se debe utilizar el computador, sino ejecutar inmediatamente programas de recuperación de datos y archivos, que realizan una prueba de diagnóstico del disco duro para descartar fallas físicas y luego proceden a la recuperación de datos borrados, dañados o perdidos. Algunos de los programas que podrían ser utilizados son: *Pcinspector*, *Smart Data Recovery*, *Smart Flash Recovery* o *Drive Rescue*. Una vez recuperada la información, se procederá a guardarla en una localidad distinta a la original, evitando sobrescribirla.

   Otra opción para la recuperación de fallas, es la utilización de hardware que garantiza la conectividad sin interrupciones, otorgando disponibilidad, redundancia de hardware y funciones de recuperación después de fallas. Un ejemplo son los *routers* de la serie Cisco 1900.

d) Los ataques por desbordamiento o exceso en el búfer, tienen por objeto la ejecución de un código arbitrario en un programa, al transmitir un flujo de datos mayor que el que se puede recibir. Para enfrentar estos ataques, se anexa propuestas en el Documento B1; además el personal deberá estar informado acerca de las alertas de seguridad y de las revisiones publicadas.

Se elaborarán listas de verificación de control de sesión de los usuarios, control de balance de cada ejecución y actualización de archivos. Además se verificará la validación de datos entregados por el sistema, la integridad y autenticidad de software descargado o actualizado. Se revisará que los programas de aplicación se ejecuten adecuadamente y terminen en caso de falla.

Se procederá a documentar todas las actividades y conservar seguros los resultados obtenidos.

8.2.3 INTEGRIDAD DEL MENSAJE

Se deben evaluar los riesgos de seguridad, determinando los casos en los que se requiere integridad del mensaje. La implementación de controles de integridad en todos los casos, resultaría innecesaria e involucraría costos superfluos.

Se aplicarán técnicas criptográficas para implementar la integridad del mensaje, en los casos en que la información involucrada sea muy sensible o extremadamente sensible. Para los demás casos, se utilizarán controles sencillos, como los establecidos en el literal e) de la Política de validación de los datos de entrada.

8.2.4 VALIDACIÓN DE LOS DATOS DE SALIDA

Para la validación de los datos de salida:

a) Todo el personal que maneje datos de salida, debe suministrar la información suficiente para su futura comprensión y determinación de exactitud, totalidad, precisión y clasificación.

b) Los asesores del Encargado de seguridad de la información, deben verificar la verosimilitud de la información de salida, constatando que sea razonable. Además, deben comprobar el procesamiento total de todos los datos de salida, realizando verificaciones en las aplicaciones y servidores necesarios. En caso de que se detectara alguna anomalía, deberán informar inmediatamente al Encargado de seguridad de la información de la empresa.

c) Se verificará que los anchos de banda que constan en los contratos, son los que se les proporciona a los clientes y que el servicio no es intermitente. La verificación para cada cliente, se llevará a cabo durante un día, mediante el monitoreo en el Allot, la constatación dentro de la configuración del *switch* y la ejecución de un *ping* extendido, garantizando así que los anchos de banda contratados, sean los que se les proporciona a los clientes y que el servicio sea continuo. Cada asesor tecnológico e ingeniero de soporte, será el encargado de verificar el ancho de banda proporcionado a los clientes de los cuales está a cargo. Si se detectara alguna anomalía, se documentará el evento y se informará al Encargado de seguridad de la información.

d) Se manejará un registro de todas las actividades del proceso de validación de la salida de los datos; esta información estará bajo el control del Encargado de la seguridad de la información de la empresa.

8.3 CONTROLES CRIPTOGRÁFICOS

Objetivo:

Utilizar medios criptográficos para proteger la confidencialidad, autenticidad e integridad de la información referente a la prestación de servicios.

8.3.1 POLÍTICA SOBRE EL USO DE CONTROLES CRIPTOGRÁFICOS

Con el fin de proteger la confidencialidad, integridad y autenticidad de la información, se establecen las siguientes directrices para la implementación de controles criptográficos[96].

a) La protección de la información, a través de controles criptográficos, deberá garantizar la seguridad de los servicios proporcionados, sin afectar en su funcionamiento y entrega normales.

b) En base a la evaluación de riesgos, es necesaria la implementación de controles criptográficos asociados a los servidores web y de correo, dado que el impacto en caso de falla sería muy alto. En el Documento B1, se presentan propuestas que incluyen encriptación en el flujo de tráfico, así como en las contraseñas.

[96] La encriptación permite cambiar los datos, de forma que solo el receptor pueda tener acceso a éstos. Para descifrar el mensaje, el destinatario debe tener la clave de desencriptación.

c) Se utilizarán programas para encriptar la información sensible almacenada en los dispositivos USB autorizados y en los discos duros; algunas propuestas se detallan en el Documento B1.

d) El Encargado de seguridad de la información será quien gestione las llaves privadas y públicas.

e) El Encargado de seguridad de la información, será el responsable de generar, proteger y manejar adecuadamente las claves criptográficas. En caso de pérdida de la información encriptada, se procederá a solicitar apoyo al Coordinador Nacional de Sistemas para la recuperación.

f) Para la implementación eficaz del control, se procederá a realizar pruebas previas, evitando la falla de los servicios y garantizando el funcionamiento eficaz del control. Una vez obtenidos los resultados esperados, el Gerente Nacional de Operaciones y Sistemas autorizará la implementación.

g) Para controles dependientes de la inspección del contenido, como el monitoreo de interfaces y de virus, no se aplicará encriptación de la información, ya que son eventos que requieren acciones correctivas inmediatas y al involucrar encriptación, aumentaría el tiempo de reacción debido al proceso de desencriptación.

8.3.2 GESTIÓN DE CLAVES

Para proteger las claves criptográficas, privadas y secretas se presenta la Política de gestión de claves:

a) Los diferentes sistemas criptográficos y aplicaciones empleadas, tendrán asociadas sus claves únicas e irrepetibles.

b) Los asesores del Encargado de seguridad de la información generarán y obtendrán certificados para las claves o llaves públicas necesarias.

c) El Encargado de seguridad de la información deberá entregar un documento a los futuros usuarios de claves; en él se solicita la firma de aceptación del uso de las mismas y se especifica la forma de activación de las claves. Una vez aceptadas las condiciones, el Encargado de seguridad de la información enviará la información de las claves en un correo electrónico, debiendo percatarse de que el archivo se encuentre encriptado y que las claves sean enviadas a los destinos correctos.

d) Las claves serán almacenadas por el Encargado de seguridad de la información, en archivos encriptados en la Intranet y con acceso exclusivo para cada usuario. Cuando un usuario autorizado, ingrese en su archivo correspondiente, solo él dispondrá de la llave, recibida previamente en el Documento de aceptación, permitiendo así su desencriptación. La selección de claves para cada caso, será realizada en base a la Política de privilegios de acceso. La llave de desencriptación no deberá ser almacenada electrónicamente, en lo posible debe ser recordada o registrada de manera segura.

e) Las claves serán cambiadas al menos trimestralmente. Si se presentara algún incidente por descubrimiento de alguna clave, todas deberán ser cambiadas inmediatamente. También se requerirá un cambio absoluto cuando algún empleado abandone sus funciones en la empresa.

Todo cambio deberá ser autorizado por el Encargado de seguridad de la información.

f) Los asesores del Encargado de seguridad de la información deberán archivar todas las claves, inclusive aquellas que ya no se utilicen. El archivo deberá ser protegido. Para la destrucción segura de claves, se verificará que no se encuentre almacenada en ningún dispositivo o configuración. Tan solo deberá permanecer en el archivo de claves.

g) Cada seis meses se realizará una revisión interna de la gestión de claves, garantizando que todas están siendo bien utilizadas, sin riesgos asociados. Además se revisarán los archivos y registros necesarios.

8.4 SEGURIDAD DE LOS ARCHIVOS DEL SISTEMA

Objetivo:

Evitar los riesgos que podrían amenazar la seguridad de los archivos del sistema.

8.4.1 CONTROL DEL SOFTWARE OPERATIVO

El Encargado de seguridad de la información, supervisará que se sigan los siguientes lineamientos para evitar los riesgos que podrían amenazar a los sistemas operativos:

a) Actualizar el software operativo, aplicaciones y las librerías de los programas que sirven como soporte en la provisión de los servicios.

Se dará un énfasis especial a la actualización de los diagramas de red, información de los clientes en el HiperK, actualizaciones requeridas en el Allot y en los archivos de direcciones IP. Dichos cambios serán efectuados por el personal de Operaciones, con la autorización correspondiente.

b) El Coordinador Nacional de Sistemas garantizará que los sistemas operativos contengan exclusivamente códigos ejecutables aprobados y no códigos en desarrollo ni compiladores. Además, garantizará que el software de las aplicaciones y del sistema operativo se implementa luego de atravesar por pruebas exhaustivas y exitosas, que deberán ser documentadas. Controlará periódicamente la configuración del software implementado y documentará todos los detalles necesarios.

c) El Departamento de Sistemas se encargará de conservar una política de restauración al estado anterior. Un día anterior a todo cambio en el sistema, se creará un punto de restauración, para que en caso de que el cambio genere un impacto negativo en el sistema, éste pueda retornar al estado anterior al cambio. Además se conservarán las versiones anteriores del software de aplicación, junto a la información necesaria para su configuración, parámetros, procedimientos; todo esto se podría utilizar en caso de contingencia.

d) Se conservará un registro de todas las actualizaciones de las librerías de los programas operativos utilizados para la entrega de los servicios; dicho registro contendrá información del responsable de la actualización, fecha, detalles de todos los cambios y sus motivos. Esta información será de gran utilidad para auditorías.

e) Si se deseara una actualización de versión de software, el Coordinador Nacional de Sistemas, será el encargado de analizar los requisitos de la empresa para el cambio y la seguridad de la nueva versión; determinándose la aplicabilidad o no de la actualización. La gerencia Nacional de Operaciones y Sistemas aprobará la actualización, una vez que reciba el informe correspondiente del Coordinador Nacional de Sistemas.

8.4.2 PROTECCIÓN DE LOS DATOS DE PRUEBA DEL SISTEMA

Con el fin de proteger los datos operativos para el desarrollo de pruebas, se seguirán las siguientes directrices:

a) No utilizar bases de datos que contengan información personal o sensible para la ejecución de pruebas.

b) Los sistemas de aplicación de pruebas tendrán acceso restringido. Tan solo el Coordinador Nacional de Sistemas y el Encargado de seguridad de la información tendrán acceso a las aplicaciones de pruebas, mediante cuentas y contraseñas preestablecidas y que sólo sea de su conocimiento. Además, se incorporará un tiempo de uso máximo por sesión, minimizando la posibilidad de uso no autorizado.

c) Cada vez que se requiera copiar la información operativa en un sistema de aplicación de prueba, el Encargado de seguridad de la información solicitará al Jefe de Operaciones NOC R1 la autorización para la copia, mediante un documento que señale las razones del requerimiento y el compromiso de

registrar el evento y borrar del sistema de aplicación de prueba la información operativa en un tiempo máximo de 48 horas, luego de terminada la prueba.

8.4.3 CONTROL DE ACCESO AL CÓDIGO FUENTE DE LOS PROGRAMAS

Es imperativo restringir el acceso al código fuente de programas, diseños, contenido de aplicaciones que permiten proporcionar los servicios, evitando el acceso y cambios nos autorizados. Se recomienda el almacenamiento central controlado del código de fuente de programas en las librerías fuente; para controlar el acceso dichas librerías, se seguirán las siguientes consideraciones:

a) No mantener las librerías fuente de programas en los sistemas operativos, de ser posible.

b) El Coordinador Nacional de Sistemas y una persona de su Departamento, designada por él, tendrán acceso a las librerías fuente de programas. Siendo así los únicos que podrán encargarse de actualizar las librerías fuente y adquirir la información asociada para programación, en cuanto hayan recibido la autorización documentada del Jefe Regional NOC R1.

c) Además, el Coordinador Nacional de Sistemas y la persona a quien haya designado, se encargarán de contar con los listados de programas, registrar todos los accesos a las librerías fuente de programas, mantener y copiar las librerías fuente; dichos procedimientos requerirán de total seguridad.

8.5 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE

Objetivo:

Garantizar la seguridad del software y de la información del sistema de aplicaciones que permita u optimice la entrega de los servicios.

8.5.1 PROCEDIMIENTOS DE CONTROL DE CAMBIOS

Para el desarrollo de todo cambio que involucre a los sistemas de información, aplicaciones y redes encargadas de proporcionar los servicios, se seguirán los siguientes lineamientos:

a) El Encargado de seguridad de la información deberá realizar un registro en el que se detallen los niveles acordados de autorización, para cada empleado, contratista o tercera parte. Dicho registro considerará las necesidades de cada ente para el desempeño de sus responsabilidades en la empresa, otorgándole el nivel de autorización adecuado. En el nivel de autorización, se reflejarán los privilegios ante cambios lógicos y físicos para cada aplicación o localidad.

b) Cualquier cambio será realizado tan solo por el usuario autorizado, quien previo al cambio deberá analizar el impacto que generará.

c) Se considerarán a software, información, entidades de bases de datos y hardware como unidades posibles para modificación o cambio.

Cada propietario de un activo realizará semestralmente una evaluación de necesidad de cambio; presentará los resultados obtenidos al Coordinador de Seguridad de la información, quien analizará la situación junto al propietario del activo, el Jefe Regional de Operaciones NOC R1 y el Subgerente de Operaciones y Sistemas.

El Gerente Nacional de Operaciones y Sistemas presentará la autorización formal para el cambio, que deberá ser ejecutado en no menos de 24 horas de recibida la aprobación.

d) La persona responsable del cambio, documentará todos los procedimientos desarrollados y entregará esta información al Encargado de seguridad de la información. Además, deberá actualizar toda la documentación al finalizar el cambio; se asegurará de que los cambios no perturben los procesos y que la información antigua sea archivada o eliminada, dependiendo de la necesidad.

e) De igual modo que en la Política de control del software operativo, se conservarán versiones antiguas, como medida de contingencia ante cualquier eventualidad que pudiera surgir después del cambio.

8.5.2 REVISIÓN TÉCNICA DE LAS APLICACIONES DESPUÉS DE LOS CAMBIOS EN EL SISTEMA OPERATIVO

Después de realizar cambios en los sistemas operativos, se revisarán y someterán a prueba las aplicaciones críticas que contribuyen a la entrega de los servicios, verificando que no se haya presentado impacto adverso.

Para las verificaciones correspondientes, se considerará:

a) El Coordinador Nacional de Sistemas revisará los procedimientos de integridad y control de la aplicación, asegurándose que no hayan sido puestos en peligro.

b) El Encargado de seguridad de la información, deberá cerciorarse de que el plan y presupuesto de soporte anual cubrirán las revisiones y pruebas necesarias después de los cambios en el sistema operativo y de que se hacen cambios en los planes de continuidad del negocio. Además deberá exigir al responsable del cambio, que se le notifique oportunamente sobre la implementación del cambio, para asignar previamente las responsabilidades del desarrollo de pruebas y revisiones al personal adecuado de Operaciones o Sistemas.

c) El Departamento de Sistemas deberá monitorear las vulnerabilidades del sistema y las nuevas versiones de parches y arreglos del distribuidor. El Coordinador Nacional de Sistemas entregará el reporte del monitoreo al Encargado de seguridad de la información, cada fin de mes, quienes discutirán sobre los resultados y analizarán las soluciones, en caso de ser requeridas.

8.5.3 RESTRICCIONES EN LOS CAMBIOS A LOS PAQUETES DE SOFTWARE

Los paquetes de software utilizados para la prestación o revisión de los servicios, no deberán ser modificados, en lo posible.

En caso de que requirieran modificaciones, se deberá tener precaución con que los procesos de integridad y de control incorporados se vean afectados, si se necesita el consentimiento del proveedor, si existe la posibilidad de obtener del mismo proveedor los cambios necesarios, o si a futuro la empresa será la responsable del mantenimiento del software, dado que el proveedor podría desentenderse tras los cambios.

Se conservará el software original, aplicando los cambios a una copia, como medida de contingencia ante cualquier eventualidad que pudiera surgir después del cambio. Todos los cambios se probarán y documentarán adecuadamente.

8.5.4 FUGA DE INFORMACIÓN

Para evitar la fuga de información, se deberán cumplir los siguientes aspectos:

a) Se prohíbe el almacenamiento de información referente a la prestación de los servicios, en medios no autorizados o de uso personal y sin seguridad, que pudieran ser objeto de robo o pérdida dentro o fuera de la empresa. Cada miembro del personal es responsable por el cumplimiento de esta obligación. El Coordinador de Seguridad de la Información, podrá en determinado momento, solicitar a cualquier persona del Departamento que le presente el contenido de sus dispositivos de almacenamiento para verificar que se esté cumpliendo con la política. En caso de detectar incumplimiento, se procederá a aplicar la Política de Proceso disciplinario.

b) El Encargado de seguridad de la información y sus dos asesores, analizarán permanentemente el comportamiento de las comunicaciones que involucren información de los servicios proporcionados a los clientes, percatándose de que no sea posible que un tercero deduzca información crítica para los servicios.

c) Los sistemas y software utilizados para la entrega de los servicios, deberán ser comprobados de integridad alta y deberán cumplir con los requisitos de seguridad de la empresa.

   El Coordinador Nacional de Sistemas o un delegado por éste, deberán realizar el análisis de los sistemas y software que se desee utilizar, previo a su implementación.

d) El Encargado de seguridad de la información monitoreará regularmente las actividades del personal y del sistema, asociadas a la entrega de los servicios. Se monitorearán los accesos físicos y lógicos, el uso adecuado de contraseñas, la no divulgación de información, el almacenamiento adecuado, la documentación y registro de todas las actividades, protección de los documentos, actividades y cambios en los sistemas y bajo qué usuario fueron realizadas. En caso de detectar algún incidente, se aplicará la Política de Proceso disciplinario.

8.5.5 DESARROLLO DE SOFTWARE CONTRATADO EXTERNAMENTE

Para la supervisión y monitoreo del software contratado externamente, se deberá considerar en el contrato las cláusulas necesarias que permitan dichos procedimientos; como por ejemplo: acuerdos sobre licencias, derechos de propiedad intelectual, certificación de la calidad y exactitud y derechos de acceso para auditarlas.

Se deben establecer los requisitos contractuales para la calidad y funcionalidad de la seguridad del código, incluyendo la realización de pruebas antes de la instalación. Es importante considerar que en caso de falla de la tercera parte, se cuente con convenios de fideicomiso.

Los encargados de asegurar un contrato adecuado del software, son el Gerente y Subgerente del Departamento de Operaciones y Sistemas, con asesoría del Encargado de seguridad de la información.

8.6 GESTIÓN DE LA VULNERABILIDAD TÉCNICA

Objetivo:

Evitar los riesgos ocasionados por la explotación de las vulnerabilidades técnicas de los sistemas de información que permiten prestar los servicios.

8.6.1 CONTROL DE LAS VULNERABILIDADES TÉCNICAS

La realización de un inventario completo de los activos de información es un prerrequisito para la gestión eficaz de la vulnerabilidad técnica asociada a la

entrega de los servicios. Para la realización de la evaluación de los riesgos, se desarrolló el inventario correspondiente, disponiéndose por tanto del mismo.

Con el fin de identificar vulnerabilidades técnicas, se seguirá el siguiente proceso de gestión:

a) El Encargado de seguridad de la información desarrollará y revisará periódicamente el inventario de activos de información, que a más de los equipos, considerará toda la información necesaria del software como su vendedor, versión, estado actual y las personas responsables del mismo. Esta información deberá ser entregada al Coordinador Nacional de Sistemas.

b) El Departamento de Sistemas, bajo la dirección de su Coordinador, será el responsable de monitorear la presencia de cualquier vulnerabilidad, evaluarla y buscar soluciones para mitigarla. Los recursos de información que se utilizarán para identificar las vulnerabilidades, serán también de responsabilidad del Departamento de Sistemas, tras una evaluación adecuada.

c) Cuando se detecte alguna vulnerabilidad técnica, la persona que lo haya hecho deberá documentar y notificar el evento, en un máximo de 3 horas, al Coordinador Nacional de Sistemas; quien reenviará la información correspondiente al Encargado de seguridad de la información. El Departamento de Sistemas deberá enviar reportes al Encargado de seguridad de la información, sobre los avances en el tratamiento de la vulnerabilidad reportada, que podría ser el uso de parches.

El Encargado de seguridad de la información deberá cerciorarse que la vulnerabilidad no tenga un impacto grave en la prestación de los servicios y que sea superada en 72 horas máximo luego de su identificación.

d) En caso de que la utilización de parches, sea una opción aparentemente útil, el Coordinador Nacional de Sistemas evaluará los riesgos asociados con su instalación; además probará y evaluará los parches antes de su instalación. En caso de no existir parches disponibles, se deberá considerar las siguientes opciones: apagar los servicios relacionados con la vulnerabilidad, adaptar controles de acceso, aumentar el monitoreo para detectar los ataques reales y concientizar acerca de la vulnerabilidad.

e) Todos los procedimientos deberán documentarse y sus registros deberán ser conservados.

9.1 REPORTE SOBRE LOS EVENTOS Y LAS DEBILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN

Objetivo:

Garantizar que los eventos de seguridad de la información detectados, que impliquen la entrega de los servicios, sean comunicados oportunamente y se tomen las acciones correctivas adecuadas.

9.1.1 REPORTE SOBRE LOS EVENTOS DE SEGURIDAD DE LA INFORMACIÓN

Todos los integrantes del Departamento de Operaciones y Sistemas serán responsables de revisar si se produce algún evento de seguridad sobre los sistemas, aplicaciones o activos con los que se asocian sus responsabilidades y funciones en la empresa. Serán considerados como eventos de seguridad: pérdida del servicio o equipo, mal funcionamiento de los sistemas, errores humanos, incumplimiento de las políticas. Si se detectara algún incidente, deberán registrarlo y comunicarlo inmediatamente al jefe de su área, sin ejecutar ninguna acción previa a la autorización respectiva.

Dependiendo del incidente que se presentara, el jefe de área y la persona que lo detectó, deberán encargarse de la mitigación del mismo. En caso de que se requiriera el apoyo del Encargado de seguridad de la información o del Coordinador Nacional de Sistemas, éstos deberán prestar la colaboración necesaria para el tratamiento del evento.

Cada proceso realizado para el tratamiento correspondiente, deberá ser documentado e informado al Jefe de área, conservando el formato de reporte que actualmente maneja la empresa, en donde se incluye el área, responsable, fecha, hora, detalles del incidente, avances del tratamiento y la solución. El Jefe de área utilizará el reporte para confirmar que el incidente haya sido solventado y que ningún otro sistema o aplicación haya sido puesto en peligro.

Si se detectara que el evento de seguridad fue producto de una falla de algún miembro del personal, se procederá a aplicar la Política de Proceso disciplinario.

9.1.2 REPORTE SOBRE LAS DEBILIDADES EN LA SEGURIDAD

En base a la Política de Reporte sobre los eventos de seguridad de la información, cualquier miembro del personal deberá informar lo antes posible al Jefe de área si detecta algún evento de seguridad. Si se trata de incidentes con responsabilidad de los proveedores, el Jefe de área deberá informar inmediatamente al proveedor respectivo, exigiendo la solución inmediata y el reporte continuo de los avances del tratamiento.

9.2 GESTIÓN DE LOS INCIDENTES Y LAS MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN

Objetivo:

Manejar una gestión adecuada para el tratamiento de los incidentes de seguridad de la información, garantizando que las responsabilidades establecidas se estén ejecutando en forma correcta y oportuna.

9.2.1 RESPONSABILIDADES Y PROCEDIMIENTOS

Como se establece en la Política de Reporte sobre los eventos de seguridad de la información, todos tendrán la responsabilidad de reportar los eventos y debilidades de la seguridad de la información que detecten. Además se deberá revisar periódicamente los reportes generados por el dispositivo de seguridad ASA; dicha función estará a cargo del Encargado de seguridad de la información y de sus asesores.

Los jefes de cada área serán los responsables de dirigir el tratamiento de los incidentes detectados en su área, teniendo la posibilidad de solicitar apoyo al Encargado de seguridad de la información, al Coordinador Nacional de Sistemas, o a otro jefe de área que anteriormente pudo haber estado a cargo de un incidente similar.

Los responsables del tratamiento del incidente deberán documentar todos los procedimientos; el jefe de área verificará que al final el incidente haya sido solventado y garantizará que se han tomado las medidas necesarias para evitar una reincidencia.

Los reportes deberán ser conservados por el jefe de área y por el Encargado de seguridad de la información; dichos reportes podrían ser utilizados para el tratamiento de futuros incidentes.

9.2.2 APRENDIZAJE DEBIDO A LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Los reportes de los incidentes de seguridad deberán incluir datos sobre el tipo de incidente, fecha, hora, el costo que implicó, sus consecuencias, el motivo que lo originó, el procedimiento llevado a cabo para su solución; en general toda información asociada al incidente, pues podría ser útil para la aplicación de controles y para el tratamiento de futuros incidentes.

9.2.3 RECOLECCIÓN DE EVIDENCIAS

Toda evidencia de los incidentes de seguridad de la información, será conservada por el jefe de área en la que se haya presentado el evento o por el Encargado de seguridad de la información.

Se deberá incluir en los contratos laborales, que en caso de ser necesario el sometimiento de la Política de proceso disciplinario, la evidencia presentada por el jefe de área tendrá validez para la determinación de las sanciones correspondientes.

Se utilizará el servicio de los abogados de la empresa para desarrollar los parámetros que debería contener la evidencia de un evento determinado, de modo que dicha evidencia sea admisible y aprobada en caso de requerir acciones penales.

La evidencia documentada en papel, será conservada por el Encargado de seguridad de la información, segura bajo llave. Para la información contenida

en medios de computador, se realizarán duplicados, documentado el procedimiento de copiado que deberá tener testigos.

10.1 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Objetivo:

Garantizar la continuidad de las operaciones para la prestación de servicios en la ciudad de Quito, mediante la definición de acciones y procedimientos a ejecutar en caso de fallas de los elementos que componen los servicios tecnológicos (informáticos y comunicaciones).

10.1.1 INCLUSIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN EL PROCESO DE GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

La gestión de la continuidad del negocio estará basada en los siguientes aspectos:

a) Se deberá realizar un análisis de la tabla de Cálculo de Nivel de Importancia de activos de información para la Seguridad y de las Matrices de riesgo, para determinar la prioridad de los procesos críticos del negocio y de los activos que en éstos intervienen.

b) De acuerdo a los árboles de impacto se determinará cuáles son los activos tolerables a fallos y cuáles afectan de manera significativa la continuidad de la operación del negocio, de manera que se tenga claro el impacto que puedan tener las interrupciones causadas por incidentes de seguridad.

c) Se adquirirán pólizas de seguro, que cubran los daños producidos por cualquier falla, en los equipos ubicados en el Centro de Datos y en los nodos.

d) Los controles preventivos y mitigantes a aplicarse serán los considerados en la Política de Gestión de la seguridad de las redes, en la cual se incluye la utilización de rutas alternas (*backup*) para mantener la continuidad de la operación del negocio. Dicha información deberá ser debidamente documentada y dada a conocer a todo el personal del Departamento de Operaciones, para que tenga conocimiento de cómo actuar en caso de presentarse algún incidente de seguridad.

e) El Jefe de Implementación y Gestión de Red R1 deberá mantener los planes y procesos de continuidad actualizados y deberá realizar pruebas para confirmar el correcto funcionamiento de los mismos.

10.1.2 CONTINUIDAD DEL NEGOCIO Y EVALUACIÓN DE RIESGOS

Es responsabilidad del encargado de seguridad, del Jefe de Implementación y Gestión de Red R1 y del Jefe Regional NOC R1, realizar la revisión periódica del documento de la evaluación de riesgos, con el propósito de identificar, cuantificar y priorizar los riesgos actuales y nuevos riesgos que pudiesen presentarse.

Adicionalmente se revisarán la tabla de Cálculo de Nivel de Importancia de activos de información para la Seguridad y los árboles de impacto, para determinar que éstos se encuentran en concordancia con los riesgos actuales y que se cumplen con los objetivos de la organización.

De manera preponderante, se deberá considerar que el tiempo de disponibilidad ofrecido a clientes, de acuerdo a lo especificado en los contratos, es de 99.8% (1 hora 26 minutos mensuales de indisponibilidad), para cualquier implementación y modificación a realizarse.

Basado en estos lineamientos se desarrollará la estrategia de continuidad, la cual será documentada y aprobada por la Gerencia.

10.1.3 DESARROLLO E IMPLEMENTACIÓN DE PLANES DE CONTINUIDAD QUE INCLUYAN LA SEGURIDAD DE LA INFORMACIÓN

Se deberán tomar en cuenta los siguientes lineamientos para el desarrollo del Plan de continuidad del negocio:

a) El encargado de seguridad junto con el área de infraestructura serán los responsables de desarrollar el Plan de continuidad del negocio, en el cual se especificarán las responsabilidades del personal en cada uno de los procesos. En caso de que las terceras partes deban intervenir, también deberá ser especificado.

b) Se definirá cuáles son los incidentes de seguridad que serán aceptables para la empresa, tal como se especifica en las Matrices de riesgo.

c) La Gerencia deberá brindar la capacitación necesaria al personal, para que éste pueda desenvolverse apropiadamente en caso de presentarse algún incidente de seguridad.

d) Se realizarán pruebas periódicas para determinar la efectividad de los planes de contingencia, siendo éstas efectuadas cada 6 meses.

e) La documentación de los planes de continuidad del negocio será administrada por el encargado de seguridad y por el Jefe de Implementación y Gestión de Red R1 únicamente, pues en ésta se especifican las vulnerabilidades de la organización.

10.1.4 ESTRUCTURA PARA LA PLANIFICACIÓN DE LA CONTINUIDAD DEL NEGOCIO

Para la planificación de la continuidad del negocio se tomarán en cuenta las siguientes directrices:

a) El personal a cargo de mantener la disponibilidad comprometida a nivel de *backbone* será el área de Infraestructura, para lo cual se implementarán rutas de *backup* hacia todos los nodos.

b) En el caso de clientes, el área de soporte será quien deberá detectar el incidente y tendrá la responsabilidad de solventarlo en el tiempo estipulado, manteniendo la disponibilidad comprometida. Para ello se respaldará en los proveedores en caso de ser necesario.

c) En caso de verse afectada la integridad y confiabilidad de la información, el personal responsable será el Encargado de seguridad y el Coordinador Nacional de Sistemas, quienes realizarán el análisis de las amenazas comprometidas en el incidente de seguridad.

10.1.5 PRUEBAS, MANTENIMIENTO Y REEVALUACIÓN DE LOS PLANES DE CONTINUIDAD DEL NEGOCIO

Para la ejecución de pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio se deberán tomar en cuenta los siguientes lineamientos:

a) Las pruebas a efectuarse deberán simularse lo más cercano a casos reales, de tal forma que se analice el comportamiento del personal asignado en el cumplimiento de sus responsabilidades. Estos trabajos deberán realizarse cada 3 meses y serán ejecutados bajo la supervisión del encargado de seguridad.

b) A nivel tecnológico se verificará la efectividad de las herramientas disponibles y se analizará la posibilidad de la adquisición de nuevas en caso de no darse los resultados esperados en los planes de continuidad del negocio.

c) Los proveedores deberán participar de los planes de continuidad del negocio sin objeción, siendo esta actividad parte de lo estipulado en el contrato.

d) Se deberán documentar los resultados obtenidos en cada una de las pruebas para mantener un registro de los objetivos alcanzados y de las fallas detectadas, con el fin de tomar acciones urgentes en caso de que se repitan continuamente las mismas fallas.

11.1 CUMPLIMIENTO DE LOS REQUISITOS LEGALES

Objetivo:

Evitar el incumplimiento de obligaciones estatutarias, reglamentarias o contractuales, en general de cualquier ley.

11.1.1 IDENTIFICACIÓN DE LA LEGISLACIÓN APLICABLE

Para garantizar el cumplimiento de los requisitos contractuales con los clientes, se procederá como se indica en el literal c) de la Política de Validación de los datos de salida.

En cuanto a los proveedores, la Gerencia y Subgerencia del Departamento de Operaciones y Sistemas, deberán asegurarse de que en los contratos se incluyan requisitos que garanticen la seguridad de la información, concerniente a su confidencialidad, integridad y disponibilidad. Se deberá incluir como requisito la mayor disponibilidad de los servicios, en lo posible el 99,8%; además se deberá solicitar la implementación de controles que garanticen la confidencialidad e integridad de la información y posteriormente se deberá monitorear que todos los requisitos se estén cumpliendo a cabalidad.

Para el caso de los contratistas, se deberán incluir requisitos similares a los indicados para los proveedores, otorgando la suficiente importancia a la seguridad de la información. Se podría incluir en los contratos, tiempos mínimos de reparación y de reporte del daño.

Toda la legislación que debe cumplir la empresa, en cuanto al pago de impuestos, presentación de documentación al SRI, regulación con el Senatel sobre el uso de recursos, permisos de funcionamiento, entre otros deberes, serán revisados bimestralmente por el Encargado de seguridad de la información y sus dos asesores. De las revisiones se realizarán informes, que serán registrados y almacenados; en caso de detectar error de manejo, se procederá a enviar el memorando correspondiente.

11.1.2 DERECHOS DE PROPIEDAD INTELECTUAL (DPI)

Para todo material que requiera protección, por ser considerado de propiedad intelectual, se considerarán las siguientes directrices:

a) Todo software, dada la propiedad intelectual, será adquirido de manera lícita, junto con las licencias necesarias y el respaldo del proveedor; además deberá ser utilizado conforme a las indicaciones del proveedor. Bajo ningún concepto, se adquirirá software de fuentes desconocidas ni poco confiables, que podrían violar los derechos de copia.

b) El Encargado de seguridad de la información, deberá incluir en los talleres y cursos que se dictarán periódicamente, el tema de la protección de los derechos de propiedad intelectual en la empresa y la política al respecto. En caso de violación a los derechos de propiedad intelectual, se procederá como lo estipula la Política de Proceso disciplinario.

c) Los asesores del Encargado de seguridad de la información, deberán realizar un registro de los activos que permiten entregar los servicios, con requisitos para proteger los derechos de propiedad intelectual.

Además serán los encargados de conservar la prueba y evidencia sobre la propiedad de licencias, manuales; se deberá asegurar que únicamente se instale software autorizado y productos con licencia.

d) Se dispondrá de controles para asegurar que no se exceda el número máximo de usuarios permitidos, como un limitador de licencias para determinado software en la intranet y las revisiones respectivas por parte de los asesores.

e) Si se necesitara transferir el software a otros, el Encargado de seguridad de la información, deberá verificar que el número máximo de usuarios permitidos no se haya completado aún. En caso de que aún sea posible, se procederá a la transferencia, registrando el evento y reduciendo la capacidad sobrante de usuarios. Si ya no fuera posible la adición de más usuarios, se procederá a adquirir más licencias del proveedor. De preferencia, se adquirirán más licencias de las que se requiera inicialmente, con planeación a futuro.

f) El personal que obtenga software e información de redes públicas, útiles para la prestación de los servicios, deberá solicitar autorización previa del Encargado de seguridad de la información; dicha solicitud deberá ser documentada y registrada. El Encargado de seguridad de la información dispondrá de 48 horas para analizar si es necesaria y segura la obtención. En caso de considerarla innecesaria o insegura, se negará la solicitud; si fuera necesaria y segura, será aprobada.

g) Está estrictamente prohibido duplicar, copiar total o parcialmente información, convertir en otro formato o extraer información si no es permitido por la ley de los derechos de copia. En caso de infracción de este literal, se procederá como lo estipula la Política de Proceso disciplinario, inclusive podría conducir a acciones legales.

11.1.3 PROTECCIÓN DE LOS REGISTROS DE LA ORGANIZACIÓN

Con el fin de proteger los registros importantes para la entrega de los servicios contra pérdida, destrucción y falsificación, se instaurará una política de clasificación de registros por tipo; así se identificarán registros de procedimientos operativos de los sistemas, registros de configuración, registros de cambios físicos, registros asociados al manejo de los activos. Cada registro constará de su período de retención, que dependerá del caso; además contendrá los tipos de medio de almacenamiento, dependiendo de la sensibilidad de la información.

Dada la posibilidad de deterioro de los medios utilizados para el almacenamiento, se utilizará un almacenamiento de *backup* en un medio distinto, bajo las recomendaciones del fabricante. En los casos en que se requiera almacenar por un plazo largo, se utilizará papel o microfichas, a parte de medios electrónicos seguros.

Cada integrante del personal, que realizara algún procedimiento que debería ser registrado, tendrá la obligación de hacerlo y entregar la información al Encargado de seguridad de la información.

Cada registro que se almacene en medios electrónicos, deberá ser entregado como archivo original de cualquier programa de *Office* y como archivo pdf, con seguridad de anticopia. Todos los registros serán guardados con clave, la cual será almacenada por el Encargado de seguridad de la información; cuando sea requerida, se solicitará al encargado su autorización, junto con la clave. El archivo original de *Office*, que estará bajo la responsabilidad del Encargado de Seguridad de la Información, no deberá ser entregado, a menos de que se tratara de un asunto sumamente necesario. El archivo que servirá de consulta o análisis será el pdf con seguridad.

En caso de que no se realizara un registro o de que no fuera entregado al Encargado de seguridad de la información, se procederá con la Política de Proceso disciplinario.

En general, se establecerá un período de retención de registros del Departamento de Operaciones, de cinco años. Se configurará este tiempo de expiración para cada registro, en el sistema de almacenamiento y manipulación. Transcurrido este tiempo, el Gerente y Subgerente de Operaciones y Sistemas, junto al Coordinador Nacional de Sistemas y el Encargado de seguridad de la información, analizarán si existe la necesidad de conservar o no cada uno de los registros.

Los registros innecesarios para la empresa, serán destruidos; tanto el archivo de programa de *Office*, como el pdf serán borrados totalmente de los discos duros y en caso de ser almacenados en cd o dvd, se procederá a su destrucción. El Coordinador Nacional de Sistemas tendrá la responsabilidad de garantizar que la información ya no esté disponible.

El Encargado de seguridad de la información tendrá la responsabilidad de destruir los registros conservados en papel, garantizando que finalmente la información sea ilegible, sin perjudicar al medio ambiente.

11.1.4 PROTECCIÓN DE LOS DATOS Y PRIVACIDAD DE LA INFORMACIÓN PERSONAL

Se instaura una Política de protección y privacidad de los datos asociados a la entrega de los servicios, en la cual se estipula lo siguiente:

a) Los asesores del Encargado de seguridad de la información tendrán la responsabilidad de guiar a todo el personal, proveedores, contratistas y terceras partes sobre sus responsabilidades para el cumplimiento de la Política de protección y seguridad de los datos.

b) Se considera a la información de los clientes como privada e inaccesible para personas que no sean autorizadas por ellos. Ningún Departamento de la empresa deberá facilitar información de ningún cliente, a menos de que se tratara del mismo cliente, que olvidó su nombre de usuario o contraseña; en tal caso se le solicitará información disponible en el *HiperK*, como cédula de identidad, RUC, teléfono o dirección, indicándole que se trata de una verificación de identidad por seguridad. Si se tratara de clientes que requieren sus direcciones IP, se les solicitará que envíen a la dirección electrónica de Soporte, un correo con los datos necesarios para verificar su identidad y el motivo de su solicitud.

c) Se aplicará la Política de directrices de clasificación, para determinar el nivel de sensibilidad de la información involucrada. En lo posible se deberá otorgar la categoría de Muy sensible a toda la información personal de los clientes; en el caso de las IPs, se debería optar por el nivel Extremadamente sensible. Para el tratamiento de dicha información, se aplicarán los controles, como se especifica en la política señalada.

11.1.5 PREVENCIÓN DEL USO INADECUADO DE LOS SERVICIOS DE PROCESAMIENTO DE INFORMACIÓN

Todo uso de los servicios de procesamiento de información con propósitos no autorizados, será considerado como uso inadecuado de los servicios. En la Política de Uso aceptable de los activos, se establecen los usos no autorizados de los servicios. En caso de detectar mediante monitoreo legal, el uso inadecuado de los servicios, sea por parte del personal, como de los clientes, se informará inmediatamente al Jefe Regional NOC R1, al Subgerente y Gerente de Operaciones y Sistemas, acerca del incidente.

Para evitar el uso inadecuado de los servicios de procesamiento de información, se presentarán mensajes de advertencia. En caso de que se tratara de una persona no autorizada intentando ingresar a un servicio de procesamiento de información de la empresa, se le desplegará en la pantalla un mensaje que indique que el servicio de procesamiento de información al cual está ingresando es de propiedad de la empresa y que no se permite acceso no autorizado.

Para restringir el acceso a información con fines ilícitos, perjudiciales, violentos, denigrantes a los derechos e intereses de terceros, el Encargado de seguridad de la información deberá estar informado acerca de estas páginas; de modo que cada vez que al servidor DNS se le solicite la traducción del nombre, se envíe al usuario un mensaje que le indique que el contenido de la página solicitada es restringido y preguntándole si desea ingresar. Tan solo si el usuario acepta, el servidor DNS procedería a realizar la traducción, pero bajo las condiciones estipuladas en la Política de uso aceptable de activos.

11.1.6 REGLAMENTACIÓN DE LOS CONTROLES CRIPTOGRÁFICOS

El Encargado de seguridad de la información y el Coordinador Nacional de Sistemas, mediante asesoría legal, antes de desplazar la información encriptada o controles criptográficos, desarrollarán la reglamentación de los controles criptográficos.

Para el cumplimiento con acuerdos, leyes y reglamentos pertinentes, se deberán considerar las restricciones de importaciones y/o exportaciones de hardware y software de computadores para la ejecución de funciones criptográficas; así también como las restricciones al uso de encriptación.

11.2 CUMPLIMIENTO DE LAS POLÍTICAS Y LAS NORMAS DE SEGURIDAD Y CUMPLIMIENTO TÉCNICO

Objetivo:

Revisar los sistemas de información que permiten la entrega de los servicios, garantizando así que cumplen con las políticas de seguridad del Departamento.

11.2.1 CUMPLIMIENTO CON LAS POLÍTICAS Y LAS NORMAS DE SEGURIDAD

Los responsables de garantizar que todos los procedimientos de seguridad de la información se están cumpliendo satisfactoriamente son el Gerente y Subgerente del Departamento de Operaciones y Sistemas, con asesoría del Encargado de seguridad de la información.

Se deberá comprobar que cada procedimiento sea revisado en el tiempo estipulado por la política correspondiente.

En caso de que se hallara un incumplimiento, el Encargado de seguridad de la información deberá determinar la causa, evaluará la necesidad de acciones que garanticen el cumplimiento futuro, determinará e implementará la acción correctiva y finalmente revisará la acción correctiva que se ejecutó.

Todos los resultados de las revisiones y de las acciones correctivas deberán ser registrados y conservados.

11.2.2 VERIFICACIÓN DEL CUMPLIMIENTO TÉCNICO

El Departamento de Sistemas, bajo la supervisión de su Coordinador Nacional y del Encargado de seguridad de la información, realizará la verificación semestral del cumplimiento técnico de los sistemas de información que permiten o facilitan la entrega de los servicios.

La verificación deberá ser manual, mediante herramientas de software; y automática, mediante herramientas que generen un informe técnico que deberá ser interpretado por los encargados de la verificación.

De preferencia no se deberán realizar evaluaciones de vulnerabilidad o pruebas de penetración, pues podrían poner en peligro la seguridad de los sistemas; en caso de que se justifique y sea necesaria y conveniente la realización de dichas pruebas, se deberá solicitar la autorización respectiva al Jefe Regional NOC R1, con al menos 72 horas de antelación.

11.3 CONSIDERACIONES DE LA AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN

Objetivo:

Mejorar la eficacia de los procesos de auditoría de los sistemas de información utilizados en la entrega de los servicios.

11.3.1 CONTROLES DE AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN

Cuando se realicen auditorías que impliquen verificaciones de los sistemas operativos, el Encargado de seguridad de la información, deberá planificar; minimizando el riesgo de interrupciones en la entrega de los servicios.

Previo a las actividades de auditoría se deberán considerar las siguientes directrices:

a) El Encargado de seguridad de la información, junto al Jefe Regional NOC R1 y el Subgerente de Operaciones y Sistemas, acordarán los requisitos de auditoría del Departamento; así como el alcance de las verificaciones y los requisitos para el procesamiento especial o adicional.

b) El Coordinador Nacional de Sistemas deberá garantizar que las verificaciones se limiten al acceso de sólo lectura del software y los datos. Se permitirá acceso diferente al de sólo lectura únicamente para copias aisladas de archivos del sistema que se puedan borrar al terminar la auditoría o darles la protección adecuada.

c) Se procurará que la persona encargada de realizar la auditoría, sea independiente de las actividades auditadas.

d) Se deberán monitorear y registrar inclusive los accesos por auditoría. Además se deberá documentar todos los procedimientos, requisitos y responsabilidades.

11.3.2 PROTECCIÓN DE LAS HERRAMIENTAS DE AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN

El Encargado de seguridad de la información será el responsable de que las herramientas de auditoría de los sistemas de información que permiten la entrega de los servicios a los clientes, como software o archivos de datos, estén separadas de los sistemas operativos y de desarrollo, y de que no sean almacenadas en medios accesibles para el personal.

El almacenamiento será realizado en base a la Política de Controles criptográficos y bajo el acceso del Encargado de seguridad de la información y del Gerente y Subgerente del Operaciones y Sistemas.

Se deberá manifestar al personal acerca de la prohibición de la manipulación de dichas herramientas, caso contrario se aplicará la Política de Proceso disciplinario.

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- Gracias a la Tecnología de la Información y Comunicación, los usuarios tienen acceso a mayores aplicaciones y privilegios que facilitan, aceleran y hacen más eficaces sus actividades. Pese a las notables ventajas de contar con sistemas de comunicación que permiten acortar distancias, enviar y recibir información valiosa para el funcionamiento de una organización, reducir gastos, etc., resulta necesario analizar las amenazas a las que se expone dicha organización al emplear ciertos sistemas informáticos. Es decir, el empleo de beneficios podría acarrear amenazas en el desempeño de una organización.

- A más del recurso humano, el activo más valioso de toda organización es su información, cualquiera sea su forma; por ello es necesario tomar medidas para asegurarla. La seguridad de la información implica seguridad en su confidencialidad, integridad y disponibilidad. Solo si se garantiza seguridad en los tres aspectos indicados, se puede afirmar que la información está segura.

- Incendios, inundaciones, terremotos son algunas de las amenazas a las que ha estado expuesta la información tradicionalmente; sin embargo, con el desarrollo de sistemas y tecnologías, han surgido nuevas amenazas, que resultan ser un peligro para la información, tales como el mapeo de sistemas, negación de servicio, gusanos, virus, troyanos, ataques de diccionario, hackeo, crackeo, entre otras.

- Dada la gran cantidad de ataques a la seguridad de la información de la que han sido víctimas un sinnúmero de organizaciones, se han desarrollado

alternativas que detecten, eviten y monitoreen posibles amenazas. Anteriormente bastaba con un *firewall* que restrinja el acceso a una red; actualmente, vista la necesidad de mayor protección, se presentan nuevas innovaciones a nivel de software y hardware. Algunas de las opciones más reconocidas y adquiridas en el mercado son: Cisco IOS *Firewall*, PIX, ASA, IDS e IPS.

- Para incorporar Cisco IOS *Firewall* como una solución de seguridad, se puede instalar el software en un *router* Cisco preexistente de la red. Si se desea mayores beneficios, PIX o ASA podrían ser una excelente opción. Algunos beneficios que presentan estas opciones de seguridad son: prevención de intrusiones, autenticación y autorización, alertas en tiempo real, monitoreo, uso de listas de acceso, entre otros.

- Uno de los conceptos básicos que manejan los equipos de seguridad para su funcionamiento es el uso de niveles de seguridad, los cuales permiten otorgar cierto nivel de seguridad a las interfaces. Una interfaz con un nivel de seguridad mayor puede acceder a una con un nivel inferior y ésta no podrá acceder a una interfaz con un nivel de seguridad superior. Otra herramienta fundamental para estos equipos son las listas de acceso, mediante las cuales se permite o restringe el acceso a determinado usuario.

- Con el fin de facilitar la planeación e implementación de controles que permitan garantizar la seguridad de la información, varios organismos han desarrollado Normas. Las más utilizadas actualmente, son las Normas ISO de la Serie 27000. Las Normas ISO 27001 y 27002 constituyen la base para el desarrollo de un Sistema de Gestión de Seguridad de la Información.

- La Norma ISO 27001 es el fundamento para el desarrollo del SGSI, en la que a través del modelo PDCA, se guía al usuario para la planeación, implementación, revisión y corrección del SGSI. Indica los análisis previos, documentos necesarios que deben ser desarrollados y las consideraciones para futuras revisiones. La Norma ISO 27002 contiene varios objetivos de

control y controles, útiles para evitar las amenazas detectadas durante la valuación de riesgos.

- Dentro de las vulnerabilidades analizadas en la Matriz de riesgo, se distingue la ausencia de una normativa que regule las actividades del Departamento de Operaciones para garantizar la seguridad de la información. Otra vulnerabilidad que se manifiesta repetidamente es la ausencia de una gestión adecuada para el acceso físico y lógico de los usuarios, incluyendo tarjetas de ingreso y claves seguras. No se presenta una gestión segura de los activos de información, ni se manifiesta preocupación suficiente en la inducción sobre seguridad de la información al personal.

- Los valores de los riesgos obtenidos en la Matriz, permiten confirmar algunas premisas que se intuían inicialmente. Se confirma que no se presta el cuidado suficiente en el mantenimiento de los equipos; además no se siguen lineamientos formales de acceso físico y lógico. Dada la ausencia de equipos de seguridad para redes, los riesgos que implicarían ataques, virus, gusanos, troyanos, negación de servicio, resultarían fatales. A más de seguridades lógicas, se evidencia la necesidad urgente de seguridades físicas, tanto en el Centro de Datos como en los nodos.

- En su mayoría, los controles detallados en la Norma ISO 27002, resultan de gran utilidad para el tratamiento de los riesgos detectados en la entrega de los servicios de la empresa.

- La implementación de una Política de seguridad permitirá controlar de mejor manera las actividades realizadas por los usuarios y garantizar la seguridad de la información asociada a la entrega de los servicios. Mediante la documentación y registro de todos los procedimientos será posible monitorear las actividades, disponer de información útil para futuros eventos y conservar la información necesaria para auditorías.

- Con la implementación de controles que permitan proteger a la información transmitida a través de las redes, como criptografía, autenticación, autorización, privilegios de acceso, se añadirá mayor seguridad a la confidencialidad, integridad y disponibilidad de los servicios. Dichos factores son esenciales en la percepción de los servicios por parte de los clientes.

- La participación activa de todo el personal en el desarrollo y mantenimiento del SGSI, será el elemento esencial para su éxito.

- Con la implementación del SGSI, la confidencialidad, integridad y disponibilidad de la información, estarán garantizadas; este factor resultará decisivo para los clientes en la selección de un proveedor, al ser un elemento fundamental y diferenciador en el mercado. Sin la implementación del SGSI, no se contará con el respaldo de garantizar la seguridad de la información para los clientes, ocasionando que éstos opten por otra opción que les ofrezca seguridad.

5.2 RECOMENDACIONES

- Se debe considerar que la información siempre está expuesta a posibles amenazas, sea humanas, tecnológicas o ambientales.

- Se debe tomar en cuenta que diariamente se desarrollan amenazas nuevas. Ante esta situación, se recomienda analizar la seguridad de la información de una organización y sus controles de seguridad con mucha regularidad; es recomendable realizar los análisis básicos al menos una vez a la semana, y los minuciosos al menos una vez trimestralmente.

- No esperar a que se produzca un ataque a la seguridad de la información, para tomar acciones correctivas para contrarrestarlo. Lo ideal es adoptar acciones preventivas antes que correctivas.

- Para seleccionar el equipo de seguridad adecuado, se recomienda considerar el tamaño de la red a la cual se desea proteger, las aplicaciones que en ésta se manejan y el análisis de costos correspondiente. Para el caso de un ISP, dado que su producto final es la entrega de servicios que atraviesan por redes, es recomendable adquirir un equipo o sistema que proporcione la mayor cantidad de seguridades posibles, procurando que el costo de la implementación tenga relación con el valor de los activos que se desea proteger.

- Si en una organización se desea implementar una normativa de seguridad de la información, es recomendable analizar las posibles opciones. Varias organizaciones en el Ecuador basan su funcionamiento en la Norma ISO 9001, sobre Gestión de Calidad; en este caso, resulta muy conveniente la utilización de las Normas ISO 27000, sobre seguridad de la información, pues éstas guardan relación.

- En caso de utilizar la Norma ISO 27002, como fuente para la selección de objetivos de control y controles, se recomienda considerar las 11 cláusulas y sus categorías principales; es posible que no todos los controles de las categorías principales sean útiles para determinado sistema, en tal caso conviene especificar los motivos de la exclusión de determinado control.

- Si dentro de los objetivos de control y controles presentados en la Norma ISO 27002, no se encontraron objetivos de control y controles que la organización considere importantes para contribuir con el mejoramiento del SGSI, se recomienda crearlos e incorporarlos dentro de la documentación de controles.

- Antes de desarrollar un SGSI en una organización, es necesario tener conocimiento de la misma. Es recomendable conocer su estructura, los productos o servicios que brinda, la infraestructura y funcionamiento de sus redes, los activos de información que posee. Una vez conocidos éstos, se debe proceder a realizar la valuación de riesgos para determinar qué acciones se deben tomar.

- Todos los controles deberían ser probados antes de ser implementados, puesto que podrían no funcionar como se espera, y por el contrario se podrían incorporar nuevas vulnerabilidades en los sistemas o aplicaciones.

- La implementación de todo control deberá considerar que al tratarse de una empresa proveedora de servicios mediante redes, no se deberán introducir tiempos de retardo importantes al incluirlo, puesto que uno de los factores más relevantes para los clientes es la rapidez de sus servicios.

- Una vez implementados los controles, se deberá dar fiel cumplimiento a las políticas de seguridad establecidas en la empresa; solo así se podrá garantizar el funcionamiento exitoso del SGSI.

- Considerando todos los factores analizados en el presente Estudio, se recomienda a la Empresa la implementación del SGSI propuesto para la ciudad de Quito, inicialmente. Una vez implementado el SGSI en Quito, se podría tomar como referencia el trabajo desarrollado para implementar el SGSI en las demás ciudades del país en las que opera la Empresa.

- La implementación del SGSI debería llevarse a cabo por etapas, en base al modelo PDCA descrito en el presente Proyecto. Los tiempos que se deberían utilizar para cada etapa no deberían ser limitados, pues se correría el riesgo de obviar acciones importantes ante la presión de los tiempos máximos; sin embargo, no debería ser superior a un año la culminación del trabajo, pues durante el desarrollo del SGSI podrían presentarse vulnerabilidades que afecten a los sistemas o aplicaciones.

- Una vez implementado el SGSI, como establecen los Procesos de Monitoreo, se deberán realizar revisiones periódicas del sistema, para verificar que su funcionamiento sea el adecuado y tomar acciones correctivas en caso de detectar algún inconveniente.

REFERENCIAS BIBLIOGRÁFICAS Y ELECTRÓNICAS

CAPÍTULO 1

[1] http://blog.formaciongerencial.com/tag/usuarios-internet-ecuador/
[2] Diccionario enciclopédico Océano Uno, Grupo editorial Océano, edición 1992
[3] CISCO Network Security Module 1
[4] CISCO Network Security Module 3
[5] CISCO Network Security Module 4
[6] CISCO Network Security Module 5
[7] CISCO Datasheet. Installing AIP-SSM Chapter 6
[8] CISCO Network Security Module 6
[9] CISCO Network Security Module 7
[10] CISCO Network Security Module 8
[11] http://www.wisedatasecurity.com/net-scanning.html
[12] CISCO Network Security Module 9

CAPÍTULO 2

[1] www.ISO27000.es
[2] http://www.iso27000.es/sgsi.html#section2b
[3] Norma ISO 27001
[4] http://www.seinhe.com/wp-content/uploads/2009/01/imagen_iso27001_12.png
[5] http://www.iso27000.es/sgsi.html#section2d
[6] NORMA ISO 27002

CAPÍTULO 3

[1] http://www.ecuanet.com/Quienessomos/tabid/67/Default.aspx
[2] Intranet de Ecuanet, página de Calidad
[3] www.ecuanet.com
[4] intranet de Ecuanet
[5] *Datasheets* de Cisco

CAPÍTULO 4

[1] http://www.corevalparaiso.cl/archivos_upload/EXPOSICION%20MATRIZ%20CORE.ppt