ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DESARROLLO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA E IMPLEMENTACIÓN DE TRES DOMINIOS EN BASE A LA NORMA 27002 PARA EL ÁREA DE HARDWARE EN LA EMPRESA UNIPLEX SYSTEMS S.A. EN QUITO

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

RICHARD EDUARDO POSSO GUERRERO
richardposso@hotmail.com

DIRECTOR: Ing. PABLO LÓPEZ MBA
pablo.lopez@epn.edu.ec

Quito, Marzo 2009

DECLARACIÓN

Yo, Richard Eduardo Posso Guerrero, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis 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.

Richard Eduardo Posso Guerrero

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por el señor Richard Eduardo Posso Guerrero, bajo mi supervisión.

Ing. Pablo López MBA
DIRECTOR DE PROYECTO

AGRADECIMIENTO

A mis padres, hermana y familiares por su comprensión y apoyo incondicional en mi vida académica.

Al Ing. Pablo López por ser mi guía y apoyo constante en la culminación de este proyecto.

A mis amigos por su apoyo durante todo este tiempo.

Y a todos aquellos que de una u otra forma ayudaron para la culminación de este proyecto.

Richard Eduardo

DEDICATORIA

A mis papitos Carlos y Luz, por su esfuerzo, apoyo, guía y comprensión durante toda mi vida.

A mi hermanita Isabel, por su cariño y apoyo.
Al amor de mi vida, mi chiquita hermosa.
A toda mi familia por su constante preocupación.

Y a todos quienes creyeron en mí.

Richard Eduardo

CONTENIDO

ÍNDICE DE CONTENIDOS

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

RESUMEN

En el presente proyecto se desarrolla un Plan Piloto de Políticas de Seguridad Informática para ser implementado en el área de Networking de la empresa Uniplex Systems S.A. Se realiza un análisis de las políticas precedentes del área y se mejoran y crean nuevas para abarcar tres dominios de la norma ISO /IEC 27002

En el Capítulo 1, se presenta un resumen de la historia de las normas ISO 27000 y se describe la norma de Seguridad de la Información ISO/IEC 27002.

En el Capítulo 2, se analizan tres dominios de la norma que tienen estrecha relación con la Seguridad Informática.

En el Capítulo 3, se analiza la situación de las políticas de Seguridad Informática instauradas previo a la implementación del Plan Piloto. Se describe la metodología para desarrollar un Sistema de Seguridad Informática y se desarrolla el Plan Piloto de Políticas de Seguridad Informática.

En el Capítulo 4, se desarrollan las nuevas políticas en base al procedimiento visto en el capítulo 3 y se procede a la implementación de las mismas.

En el Capítulo 5, se presentan las conclusiones y recomendaciones del presente proyecto.

Finalmente, en los anexos se dispone de conceptos importantes de este proyecto; se detalla la documentación e instructivos que se desarrollaron para implementar la norma, se indica la implementación de las políticas de Seguridad Informática y se dispone de una guía para que los usuarios la apliquen sin dificultades.

PRESENTACIÓN

La información en medios informáticos es altamente utilizada en todas las empresas, hogares, escuelas, universidades, etc. Por esta razón es importante determinar qué hacer para protegerla y evitar que caiga en manos de personas no autorizadas; esto se obtiene con la implementación de políticas de Seguridad Informática.

Este proyecto se basa en la Norma ISO/IEC 27002 que trata de las “Políticas de Seguridad de la Información”, se realiza un resumen de la norma y se analizan tres dominios que son aplicados a la Seguridad Informática.

Se analizan las políticas que se aplicaban antes del proyecto y se desarrollan nuevas acorde con la norma.

Se implementa las políticas desarrolladas en el área de hardware (Networking) de la empresa Uniplex Systems S.A.

De esta manera la información que ingresa y sale del área de Networking ya no queda desprotegida, y en lugar de ello se generan registros para conocer su estado.

CAPÍTULO I
MARCO TEÓRICO

CAPÍTULO I: MARCO TEÓRICO

1.1 INTRODUCCIÓN

En este mundo globalizado; las empresas, a más de estar en permanente evolución y desarrollo, requieren estar acorde con las regulaciones legales y técnicas del entorno, deben implementar normas que les permita cumplir estos preceptos, y desarrollar controles para evitar quedarse rezagadas de las demás.

Varias empresas piensan que disponen de una correcta Seguridad Informática y creen que sus "datos confidenciales" son inaccesibles a personal no autorizado; pero el hecho es que en la mayoría de casos, al fin de mes o de año, las empresas competidoras disponen en la Mesa de Reuniones los balances generales de estas "empresas con políticas de Seguridad Informática[1]" equívocamente implementadas. Las fuentes de las empresas competidoras en muchos casos es gente inescrupulosa que pertenece a la misma empresa pero que se dedica al tráfico de información para sacar lucro.

Otro caso no tan alejado de la realidad son las empresas que tienen la información para desarrollar proyectos, pero que no saben donde la tienen, disponen de todos los documentos de investigaciones previas regada por todos lados, sin clasificar y desordenada, teniendo en algunos casos más de diez veces la copia de una canción favorita que un desarrollo investigativo.

Existen peores circunstancias en que la empresa nunca ha reflexionado acerca de la continuidad del negocio.

Como todos sabemos, mucha información es vulnerable; puede perderse debido a fallas en elementos físicos, afectarle un virus informático, desastres naturales, etc.

[1] Ver Anexo 1

Es claro que la correcta aplicación de las Políticas de Seguridad de la Información mantiene la integridad, confidencialidad y disponibilidad de la misma; y por ello se aclara que este trabajo involucra un subconjunto de éstas, se habla de políticas de Seguridad Informática, que ayudan a establecer las Políticas de Seguridad de la Información.

Para facilidad del lector; se detallan algunos conceptos utilizados en este trabajo, ver Anexo 1.

1.2 NORMAS ISO 27000[2]

1.2.1 ORIGEN

Desde 1901, y como primera entidad de normalización a nivel mundial, el Instituto Británico de Estandarización (British Standards Institution BSI), fue responsable de la publicación de importantes normas como:

- Publicación BS 5750 - ahora ISO 9001 (Sistema de Gestión de Calidad)
- Publicación BS 7750 - ahora ISO 14001 (Especificaciones y elementos de cómo implementar un Sistema de Gestión Ambiental)
- Publicación BS 8800 - ahora OHSAS 18001 (Requisitos de Sistema de Gestión de Seguridad y Salud)

La norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa -británica o no- un conjunto de buenas prácticas para la gestión de la seguridad de su información.

La primera parte de la norma (BS 7799-1) es una guía de buenas prácticas, en la que no se establece un esquema de certificación. La segunda parte (BS 7799-2), publicada por primera vez en 1998, establece los requisitos de un sistema de

[2] http://www.iso27000.es/doc_iso27000_all.htm

Seguridad de la Información (SGSI) para ser certificable por una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000.
En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión.

En el Gráfico 1.1 se puede apreciar un resumen de la historia de la Norma.

GRÁFICO 1.1 HISTORIA DE LA NORMA

En 2005, con más de 1700 empresas certificadas en BS 7799-2, este esquema se publicó por ISO como estándar ISO 27001, al tiempo que se revisó y actualizó ISO 17799. Esta última norma se renombra como ISO 27002:2005 el 1 de Julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión.

En Marzo de 2006, posteriormente a la publicación de la ISO27001:2005, BSI publicó la BS7799-3:2006, centrada en la gestión del riesgo de los sistemas de información.

1.2.2 LA SERIE 27000

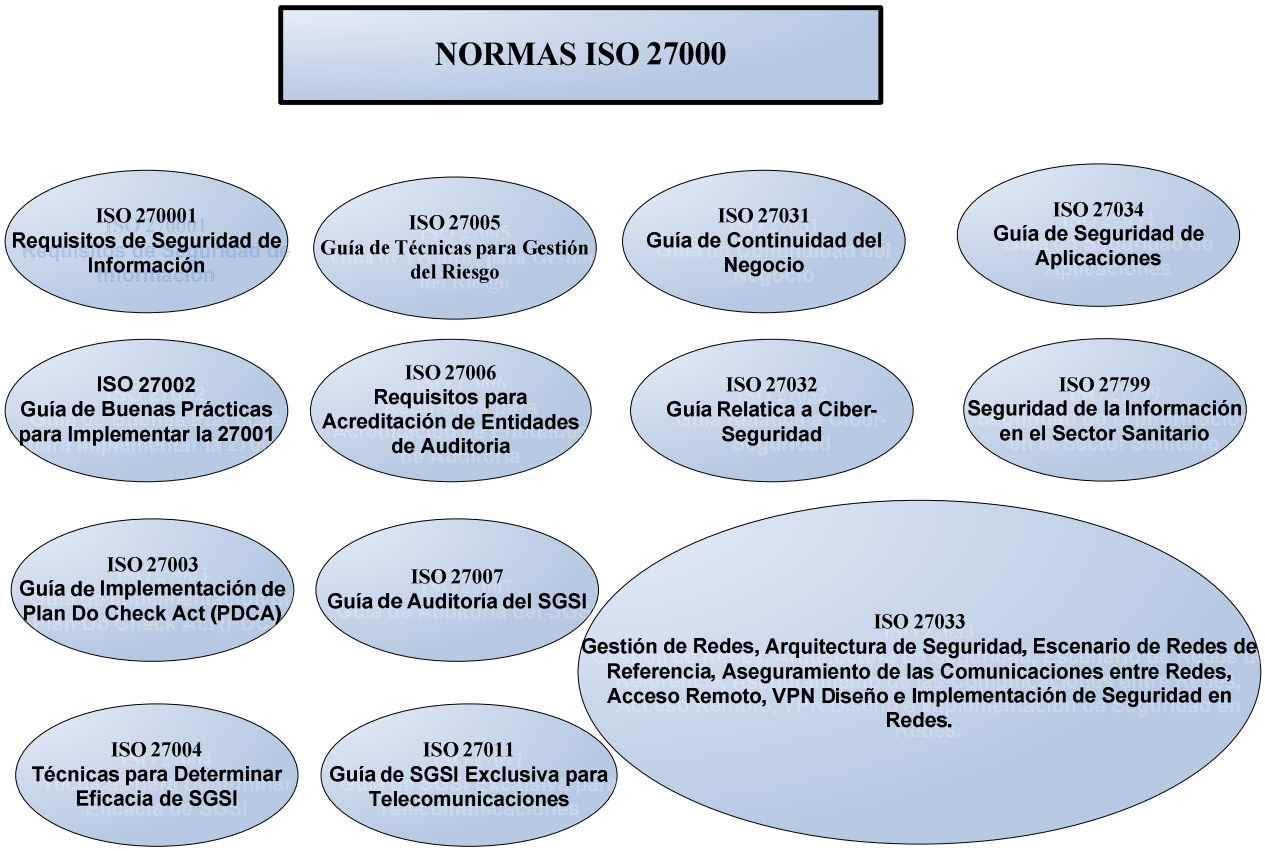


GRÁFICO 1.2 FAMILIA ISO 27000

En el gráfico 1.2 se presenta brevemente la familia ISO 27000

ISO 27000: En fase de desarrollo; su fecha prevista de publicación es Marzo de 2009. Contendrá términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión. Esta norma está previsto que sea gratuita.

ISO 27001: Publicada el 15 de Octubre de 2005. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de Seguridad de la Información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones. Sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas

empresas certificadas en esta última. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005 (nueva numeración de ISO 17799:2005 desde el 1 de Julio de 2007), para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI.

ISO 27002: Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a Seguridad de la Información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2005.

ISO 27003: En fase de desarrollo; su fecha prevista de publicación es Mayo de 2009. Consistirá en una guía de implementación de SGSI e información acerca del uso del modelo (Planear Hacer Chequear Actuar) (PDCA Plan Do Check Act) y de los requerimientos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.

ISO 27004: En fase de desarrollo; su fecha prevista de publicación es Marzo de 2009. Especificará las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase “Do” (Implementar y Utilizar) del ciclo PDCA (Plan, Do, Check Act).

ISO 27005: En fase de desarrollo; su fecha prevista de publicación es Mayo de 2009. Consistirá en una guía de técnicas para la gestión del riesgo de la Seguridad de la Información y servirá, por tanto, de apoyo a la ISO 27001 y a la implantación de un SGSI.

ISO 27006: Publicada el 1 de Marzo de 2007. Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de

Seguridad de la Información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSI) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001 y los SGSI.

ISO 27007: En fase de desarrollo; su fecha prevista de publicación es Mayo de 2010. Consistirá en una guía de auditoría de un SGSI.

ISO 27011: En fase de desarrollo; su fecha prevista de publicación es Marzo de 2009. Consistirá en una guía de gestión de Seguridad de la Información específica para telecomunicaciones, elaborada conjuntamente con la ITU (Unión Internacional de Telecomunicaciones).

ISO 27031: En fase de desarrollo; su fecha prevista de publicación es Mayo de 2010. Consistirá en una guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones.

ISO 27032: En fase de desarrollo; su fecha prevista de publicación es Marzo de 2009. Consistirá en una guía relativa a la ciber-seguridad.

ISO 27033: En fase de desarrollo; su fecha prevista de publicación es entre 2010 y 2011. Es una norma consistente en 7 partes: gestión de seguridad de redes, arquitectura de seguridad de redes, escenarios de redes de referencia, aseguramiento de las comunicaciones entre redes mediante puertas de salida (Gateway), acceso remoto, aseguramiento de comunicaciones en redes mediante Redes Privadas Virtuales (Virtual Private Network VPN) y diseño e implementación de seguridad en redes.

ISO 27034: En fase de desarrollo; su fecha prevista de publicación es Marzo de 2009. Consistirá en una guía de seguridad en aplicaciones.

ISO 27799: En fase de desarrollo; su fecha prevista de publicación es 2009. Es un estándar de gestión de Seguridad de la Información en el sector sanitario aplicando ISO 17799 (actual ISO 27002).

1.3 DESCRIPCIÓN DE LA NORMA 27002[3]

Esta Norma contiene 39 objetivos de control y 133 controles que se encuentran agrupados en 11 dominios principales. A continuación se presenta un resumen de la Norma ISO/IEC 27002.

1.3.1 POLÍTICA DE SEGURIDAD

1.3.1.1. Política de Seguridad de la Información

1.3.1.1.1 Documento de la Política de Seguridad de la Información

El documento de la Política de Seguridad de la Información debería enunciar el compromiso de la gerencia. En otras palabras, debería contener:

a) Una definición de la seguridad de la información, sus objetivos, alcances generales y la importancia.
b) La intención de la gerencia, sus objetivos y los principios de la Seguridad de la Información en línea con la estrategia y los objetivos comerciales.
c) Un marco referencial para establecer los objetivos de control y los controles incluyendo la estructura de la evaluación del riesgo y la gestión de riesgo.
d) Una explicación breve de las políticas, principios, estándares y requerimientos de conformidad de la seguridad.

[3] Norma ISO/IEC 27002

e) Una definición de las responsabilidades generales y específicas para la gestión de la Seguridad de la Información incluyendo el reporte de incidentes de Seguridad de la Información.
f) Referencias a la documentación que fundamenta la política; por ejemplo, políticas y procedimientos de seguridad más detallados para sistemas de información específicos o reglas de seguridad que los usuarios debieran observar y cumplir.

1.3.1.1.2 Revisión de la Política de Seguridad de la Información

Se debería revisar la Política de Seguridad de la Información a intervalos de tiempo planificados o cuando existen cambios significativos relacionados con la información, esta revisión debe estar enfocada al mejoramiento del documento.

1.3.2 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

1.3.2.1 Organización Interna

La gerencia debería establecer una gestión para iniciar y controlar la implementación de la Seguridad de la Información, se debería aprobar la política de Seguridad de la Información, asignar las funciones de seguridad, coordinar y revisar la implementación de la seguridad en toda la organización. Es conveniente desarrollar contactos con grupos o especialistas externos en seguridad, para ir al ritmo de las tendencias industriales.

1.3.2.1.1 Compromiso de la Dirección con la Seguridad de la Información

La dirección debería apoyar activamente la seguridad dentro de la organización con un rumbo claro, un compromiso demostrado y el conocimiento de las responsabilidades de la Seguridad de la Información. Las responsabilidades se podrían manejar a través de un comité de dirección dedicado a esta labor.

1.3.2.1.2 Coordinación de la Seguridad de la Información

Las actividades de la Seguridad de la Información deberían ser coordinadas por los representantes de todas las áreas de la organización, esta coordinación involucra la cooperación y colaboración de directores, usuarios, administradores, diseñadores de aplicación, auditores y personal de seguridad. La coordinación también debería identificar la forma en que se manejan los incumplimientos, evaluar la efectividad de los controles para recomendar acciones para responder a incidentes identificados.

1.3.2.1.3 Asignación de Responsabilidades para la Seguridad de la Información

La asignación de responsabilidades para la Seguridad de la Información se debería realizar de acuerdo con la política de Seguridad de la Información. Se deberían definir claramente las responsabilidades para la protección de activos[4] y para realizar procesos específicos de seguridad. Las personas con responsabilidades de seguridad asignadas pueden delegar las labores de seguridad a otros; pero continúan siendo responsables y deberían verificar la correcta ejecución de las tareas asignadas.

1.3.2.1.4 Proceso de Autorización para los Servicios de Procesamiento de Información

Se recomienda tener en cuenta las siguientes directrices[5] para el proceso de autorización:

a) Los servicios nuevos deberían tener autorización de la dirección para el usuario apropiado, autorizando su propósito y uso.
b) Cuando sea necesario, tanto hardware como software deberían ser verificados para asegurar que son compatibles con otros componentes del sistema;

[4] Ver ANEXO 1
[5] Ver ANEXO 1

c) Se deberían identificar e implementar controles necesarios contra posibles vulnerabilidades introducidas por equipos personales tales como laptops, computadores domésticos, PDA, Palms, u otros dispositivos manuales.

1.3.2.1.5 Acuerdos sobre Confidencialidad

Los acuerdos de confidencialidad deberían abordar los requisitos para proteger la información confidencial. Se deberían considerar los siguientes elementos para establecer los requisitos:

a) Definir la información que se ha de proteger (por ejemplo información confidencial)
b) Tiempo de duración esperada del acuerdo, incluyendo los casos en que puede ser necesario mantener la confidencialidad de manera indefinida.
c) Acciones requeridas cuando se termina un acuerdo
d) Responsabilidades y acciones de los que suscriben el acuerdo de confidencialidad para evitar la divulgación no autorizada de información (tal como “necesidad de conocer”).
e) Propiedad de la información, secretos comerciales y propiedad intelectual y como se relaciona con la protección de la información confidencial.
f) Derecho de auditar y monitorear las actividades que involucran a la información confidencial
g) Proceso para el reporte de divulgación no autorizada o violación de la información confidencial.
h) Términos para la devolución o la destrucción de la información al terminar el acuerdo.
i) Acciones esperadas a tomar en caso de incumplimiento de este acuerdo

Los requisitos para los acuerdos de confidencialidad o no-divulgación se deberían revisar periódicamente y cuando se produzcan cambios que influyan en estos requisitos.

1.3.2.1.6 Contacto con las Autoridades

Las empresas deberían tener procedimientos que especifiquen cuándo y a través de qué autoridades una persona se debería contactar y la forma en que se deberían reportar oportunamente los incidentes identificados de la Seguridad de la Información, o la sospecha de incumplimiento de la ley.

El contacto también implica relación con organismos de regulación, esto serviría para prepararse a los cambios futuros en la ley. Puede ser también incluir los servicios públicos, servicios de emergencia, seguridad, entre otros.

1.3.2.1.7 Contactos con Grupos de Intereses Especiales

La pertenencia a foros o grupos de intereses especiales se debería considerar un medio para:

a) Renovar el conocimiento sobre la información referente a la seguridad.
b) Garantizar que la comprensión del entorno de Seguridad de la Información es actual y completa.
c) Recibir advertencias oportunas de alertas, avisos y parches relacionados con ataques y vulnerabilidades.
d) Obtener acceso a asesoría especializada sobre Seguridad de la Información.
e) Compartir información acerca de nuevas tecnologías, productos, amenazas o vulnerabilidades.
f) Suministrar puntos adecuados de enlace cuando se trata de incidentes de Seguridad de la Información.

1.3.2.1.8 Revisión Independiente de la Seguridad de la Información

Esta revisión debe ser hecha por una persona ajena al área sometida a revisión; así se puede conseguir eficacia, idoneidad y propiedad del enfoque de la organización para la gestión de la Seguridad de la Información.

1.3.2.2. Partes Externas

Cuando existe una necesidad del negocio de trabajar con partes externas que pueden requerir acceso a la información de la organización y a sus *servicios de procesamiento de información*[6], se debería realizar una evaluación de riesgos para determinar las implicaciones para la Seguridad de la Información y los requisitos de control[7]. Los controles se deberían acordar y definir en un convenio con la parte externa.

1.3.2.2.1 Identificación de los Riesgos Relacionados con las Partes Externas

Cuando existe la necesidad de permitir el acceso de una parte externa a los servicios de procesamiento de información o a la información de la organización, se debería llevar a cabo una evaluación de riesgos, así se pueden identificar los controles necesarios. Se debería considerar:

a) Los servicios de procesamiento de información a los cuales requiere acceso la parte externa.
b) El tipo de acceso que tendrá la parte externa a la información y a los servicios de procesamiento de información (físico, lógico o conexión de red).
c) El valor y la sensibilidad de la información involucrada.
d) Los controles necesarios para que información no autorizada no esté disponible para la parte externa.
e) La forma en que se puede identificar al personal autorizado a tener acceso, la manera de verificar la autorización, y la forma de confirmar esta verificación.
f) Los medios y controles utilizados por la parte externa para almacenar, procesar, comunicar, compartir e intercambiar la información.
g) El impacto del acceso denegado a la parte externa cuando lo requiere y la recepción o el acceso de la parte externa a información engañosa.

[6] Ver ANEXO 1
[7] Ver ANEXO 1

h) Los procedimientos para tratar los incidentes de Seguridad de la Información, los daños potenciales y las condiciones para la continuación del acceso de la parte externa.
i) Los requisitos legales y otras obligaciones contractuales pertinentes a la parte externa que se debería tener en cuenta.

1.3.2.2.2 Abordaje de la Seguridad cuando se Trata con los clientes

Los siguientes términos se deberían considerar para abordar la seguridad antes de dar acceso a los clientes a cualquiera de los activos de la organización:

a) Protección de activos.
b) Descripción del producto o servicio que se va a proveer.
c) Las diversas razones, requisitos y beneficios del acceso del cliente.
d) Política del control de acceso (uso de ID, contraseñas, privilegios, o revocar derechos).
e) Convenios para el reporte, la notificación y la investigación de las inexactitudes de la información (por ejemplo de detalles personales), incidentes y violaciones de la seguridad de información.
f) Descripción de cada servicio que va a estar disponible
g) La meta del nivel de servicio y los niveles aceptables de servicio.
h) El derecho a monitorear y revocar cualquier actividad relacionada con los activos de la organización.
i) Las respectivas responsabilidades civiles de la organización y del cliente.
j) Derechos de propiedad intelectual (DPI) y asignación de derechos de copia y la protección de cualquier trabajo en colaboración.

1.3.2.2.3 Abordaje de la Seguridad en los Acuerdos con Terceras Partes

Se debería garantizar que no existen malos entendidos entre la organización y la tercera parte. Se recomienda tener en cuenta los siguientes puntos para la inclusión en el acuerdo con el objeto de cumplir los requisitos de seguridad identificados:

a) La política de Seguridad de la Información y los controles para asegurar la protección del activo.
b) Asegurar la concientización del usuario sobre responsabilidades y aspectos de la seguridad de la información.
c) Disposiciones para la transferencia de personal, cuando es apropiado.
d) Responsabilidades relacionadas con la instalación y el mantenimiento del software y el hardware.
e) La estructura clara y los formatos acordados para la presentación de los informes.
f) La política de control del acceso.
g) Disposiciones para la notificación y la investigación de incidentes, incumplimientos y violaciones de los requisitos establecidos en el acuerdo.
h) La descripción de cada servicio que va a estar disponible y los objetivos del servicio.
i) El derecho a monitorear y revocar cualquier actividad relacionada con los activos de la organización.
j) El derecho a auditar las responsabilidades definidas en el acuerdo, a que dichas auditorías sean realizadas por una tercera parte y a enumerar los derechos estatutarios de los auditores.
k) El establecimiento de un proceso de escalada para la solución de problemas.
l) Los requisitos de la continuidad del servicio, incluyendo las medidas para la disponibilidad y confiabilidad, de acuerdo con las prioridades de negocio de la organización.
m) Las responsabilidades civiles correspondientes de las partes del acuerdo.
n) Los derechos de propiedad intelectual (DPI) y asignación de derechos de copia y la protección de cualquier trabajo en colaboración.
o) La participación de la tercera parte con los subcontratistas y los controles de seguridad que estos subcontratistas necesiten implementar.
p) Las condiciones para la regeneración / terminación del acuerdo

1.3.3 GESTIÓN DE ACTIVOS

1.3.3.1 Responsabilidad por los Activos

Se deberían identificar los dueños para todos los activos y asignar la responsabilidad para el mantenimiento de los controles adecuados. La implementación de los controles específicos puede ser delegada por el dueño, pero éste sigue siendo responsable de la protección adecuada de los activos.

1.3.3.1.1 Inventario de Activos

La organización debería identificar todos los activos y documentar su importancia. El inventario de activos debería incluir toda la información necesaria para recuperarse de los desastres, incluyendo el tipo de activo, el formato, la ubicación, la información de soporte, la información sobre licencias y el valor para el negocio.

1.3.3.1.2 Propietario de los Activos

El propietario del activo debería ser responsable de:

a) Garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente.
b) Definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso.

1.3.3.1.3 Uso Aceptable de los Activos

Los empleados, contratistas y usuarios de tercera parte que tienen acceso a los activos de la organización deberían estar conscientes de los límites que existen para el uso que hagan de los recursos de procesamiento de información y de cualquier uso efectuado bajo su responsabilidad.

1.3.3.2 Clasificación de la Información

La información se debería clasificar para indicar la necesidad, las prioridades y el grado esperado de protección. Es recomendable utilizar un esquema de clasificación para definir un conjunto apropiado de niveles de protección y comunicar la necesidad de medidas especiales en caso que sea necesario.

1.3.3.2.1 Directrices de Clasificación

Las directrices de clasificación deberían incluir convenciones para la clasificación inicial y la reclasificación con el paso del tiempo, de acuerdo con alguna política predeterminada de control de acceso. Debería ser responsabilidad del propietario del activo definir la clasificación del activo, revisarlo periódicamente y asegurarse de que se mantiene actualizado y en el nivel adecuado.

1.3.3.2.2 Etiquetado y Manejo de la Información

Es necesario que los procedimientos para el etiquetado de la información comprendan los activos de información en formatos físico y electrónico. El etiquetado debería reflejar la clasificación según las reglas y directrices establecidas. Para la manipulación de la información es recomendable definir los procedimientos de manejo, incluyendo procesamiento, almacenamiento, transmisión, desclasificación y destrucción seguros.

1.3.4 SEGURIDAD DE LOS RECURSOS HUMANOS

1.3.4.1 Antes de la Contratación Laboral[8]

Las responsabilidades de la seguridad se deberían definir antes de iniciar la contratación laboral, describiendo adecuadamente el trabajo, los términos y condiciones del mismo. Los candidatos para el empleo, contratistas y usuarios de

[8] La palabra “contratación” cubre todas las siguientes situaciones: empleo de personas (temporal o a término indefinido), asignación de roles de trabajo, cambio de roles de trabajo, asignación de contratos, y la terminación de cualquiera de estos acuerdos.

terceras partes se deberían seleccionar adecuadamente, en especial cuando se trata de trabajos que sean de mucha importancia para la empresa.

1.3.4.1.1 Roles y Responsabilidades

Las funciones y responsabilidades deberían incluir los requisitos para:

a) Implementar y actuar de acuerdo con las políticas de Seguridad de la Información de la organización.
b) Proteger los activos contra acceso, divulgación, modificación, destrucción o interferencia no autorizados.
c) Ejecutar actividades particulares de seguridad.
d) Garantizar que se asigna la responsabilidad a la persona para que tome las acciones.
e) Informar los eventos de seguridad u otros riesgos de seguridad para la organización.

1.3.4.1.2 Selección

Para seguridad en la selección del personal se debería considerar, siempre y cuando se autorice en la legislación, lo siguiente:

a) Referencias de comportamiento satisfactorio.
b) Verificación de la hoja de vida del candidato.
c) Verificación de las calificaciones profesionales y académicas declaradas.
d) Verificación de la identidad.
e) Verificación de los detalles adicionales tales como créditos o antecedentes criminales.

1.3.4.1.3 Términos y condiciones laborales

Los términos y condiciones laborales deberían reflejar la política de seguridad de la organización, se debería tener en cuenta elementos como:

a) Todos los empleados, contratistas y usuarios de terceras partes que tengan acceso a información sensible deberían firmar un acuerdo de confidencialidad antes de tener acceso a la información.
b) Los derechos y responsabilidades legales de los empleados, los contratistas y cualquier otro usuario, por ejemplo con respecto a las leyes de derechos de copia o la legislación sobre protección de datos.
c) Responsabilidades para la clasificación de la información y la gestión de los activos de información manejados por el empleado, el contratista o el usuario de tercera parte.
d) Responsabilidades del empleado, el contratista o el usuario de tercera parte para el manejo de la información recibida de otras empresas o de partes externas.
e) Responsabilidades de la organización para el manejo de toda la información personal, durante el contrato laboral con la organización.
f) Responsabilidades que van más allá de las instalaciones de la organización y de las horas laborales, por ejemplo en el caso de trabajo en el domicilio.
g) Acciones a tomar si el empleado, el contratista o el usuario de tercera parte hace caso omiso de requisitos de seguridad de la organización.

1.3.4.2 Durante la Vigencia del Contrato Laboral

Se debería concientizar, educar y formar a todos los empleados para que apliquen correctamente las políticas de Seguridad de la Información y utilicen correctamente los servicios de procesamiento de información para minimizar los posibles riesgos de seguridad. Es conveniente establecer un proceso disciplinario formal para el manejo de las violaciones de la seguridad.

1.3.4.2.1 Responsabilidades de la Dirección

Las responsabilidades de la dirección deberían incluir el garantizar que los empleados, los contratistas y los usuarios de terceras partes:

a) Estén adecuadamente informados sobre las funciones y responsabilidades respecto a la Seguridad de la Información antes de que se les otorgue acceso a la información.
b) Tengan las directrices para establecer las expectativas de seguridad de sus funciones dentro de la organización.
c) Estén motivados para cumplir las políticas de seguridad de la organización.
d) Logren un grado de concientización sobre la seguridad correspondiente a sus funciones y responsabilidades dentro de la organización.
e) Estén de acuerdo con los términos y las condiciones laborales, las cuales incluyen la política de Seguridad de la Información de la organización y los métodos apropiados de trabajo.
f) Sigan teniendo las calificaciones y las habilidades apropiadas.

1.3.4.2.2 Educación y Concientización sobre la Seguridad de la Información

Se debería empezar con un proceso de introducción en el cual se presenten las políticas de seguridad de la organización y las expectativas, esto debería ser antes de otorgar el acceso a la información. En esta introducción se deberían incluir puntos como requisitos de seguridad, controles, proceso disciplinario.

1.3.4.2.3 Proceso Disciplinario

El proceso disciplinario debería garantizar la imparcialidad y el tratamiento correcto para los empleados de quienes se sospecha han cometido violaciones de la seguridad. El proceso disciplinario formal debería brindar una respuesta gradual, de tal forma que se sancione conforme a la mala conducta presentada y si es reiterado.

1.3.4.3 Terminación o Cambio de la Contratación Laboral

Se deberían establecer responsabilidades para asegurar la gestión de la salida de los empleados, contratistas o usuarios de terceras partes de la organización y que

se complete la devolución de todo el equipo y la cancelación de todos los derechos de acceso.

1.3.4.3.1 Responsabilidades en la Terminación

La comunicación de las responsabilidades en la terminación debería incluir las responsabilidades legales y las responsabilidades contenidas en cualquier acuerdo de confidencialidad, los términos y condiciones laborales deberían continuar durante un período definido después de terminar la contratación laboral del empleado, el contratista o el usuario de terceras partes.

1.3.4.3.2 Devolución de Activos

Se debería tener un proceso de terminación para incluir la devolución del software previamente publicado, los documentos corporativos, manuales y los equipos. También es necesaria la devolución de otros activos de la organización tales como los dispositivos móviles, tarjetas de crédito, tarjetas de acceso, y la información almacenada en medios electrónicos.

1.3.4.3.3 Retiro de los Derechos de Acceso

Después de la terminación del convenio con un empleado, se deberían considerar los derechos de acceso de la persona a los activos asociados con la información y de ser necesario retirarlos. Si un empleado, contratista o usuario de terceras partes que se retira tiene contraseñas conocidas para permanecer activo, éstas se deberían cambiar en la terminación o el cambio de empleo, contrato o acuerdo.

1.3.5 SEGURIDAD FÍSICA Y DEL ENTORNO

1.3.5.1 Áreas Seguras

La información crítica para la empresa debería estar ubicada en áreas seguras, protegidas por perímetros de seguridad definidos, con barreras de seguridad y

controles adecuados. Dichas áreas deberían estar protegidas físicamente contra acceso no autorizado, daño e interferencia.

1.3.5.1.1 Perímetro de Seguridad Física

*P*ara la seguridad física se deberían considerar:

a) Definir claramente los perímetros de seguridad; la ubicación y las fortalezas de cada perímetro deberían depender de los requisitos de seguridad de los activos.
b) Los perímetros de un lugar con servicios de procesamiento de información deberían ser robustos físicamente; las paredes sólidas y puertas externas deberían tener protección adecuada contra el acceso no autorizado; las puertas y ventanas deberían estar cerradas con llave cuando no están atendidas y se debería tener presente la protección externa para las ventanas, en especial cuando se está a nivel del suelo.
c) Se debería establecer un área de recepción con personal para controlar el acceso físico al lugar; el acceso debería estar permitido únicamente al personal autorizado.
d) Cuando sea posible se deberían construir barreras físicas para evitar el acceso no autorizado.
e) Las puertas de incendio en el perímetro de seguridad deberían tener alarma y someterse a pruebas para establecer el grado requerido de resistencia según las normas nacionales e internacionales; éstas deberían funcionar de manera segura de acuerdo con el código local de incendios.
f) Si es posible se debería instalar sistemas adecuados de detección de intrusos y someterlos a pruebas regularmente.
g) Los servicios de procesamiento de información dirigidos por la organización deberían estar físicamente separados de los dirigidos por terceras partes.

1.3.5.1.2 Controles de Acceso Físico

Se deberían tener en cuenta las siguientes directrices:

a) Se deberían registrar la fecha y la hora de entrada y salida de visitantes, todos los visitantes deberían estar supervisados, sólo se les debería dar acceso para propósitos específicos y autorizados.
b) Se debería controlar el acceso a áreas en donde se procesa o almacena información sensible y restringir el acceso a personas autorizadas; se podría utilizar controles de autenticación como las tarjetas de control de acceso.
c) Se debería exigir a todos los empleados, contratistas y usuarios de terceras partes la utilización de alguna forma de identificación visible y se debería notificar inmediatamente al personal de seguridad si se encuentran visitantes sin acompañante o sin identificación visible.
d) Al personal del servicio de soporte de terceras partes se le debería dar acceso restringido a las áreas seguras o a los servicios de procesamiento de información sensible únicamente cuando sea necesario.
e) Los derechos de acceso a áreas seguras se deberían revisar y actualizar con regularidad y revocarlos cuando sea necesario.

1.3.5.1.3 Seguridad de Oficinas, Recintos e Instalaciones

Se recomienda tener en cuenta las siguientes directrices para la seguridad de oficinas, recintos y servicios:

a) Tener presente los reglamentos y las normas pertinentes a la seguridad y la salud.
b) Las instalaciones claves se deberían ubicar de modo que se evite el acceso al público.
c) Cuando sea viable, las edificaciones deberían ser discretas y no tener indicaciones sobre su propósito, sin señales obvias que identifiquen la presencia de actividades de procesamiento de información.
d) Los directorios y los listados telefónicos internos que indican las ubicaciones de los servicios de procesamiento de información sensible no deberían ser de fácil acceso al público.

1.3.5.1.4 Protección contra Amenazas Externas y Ambientales

Se recomienda tener en mente las siguientes directrices para evitar daño debido a incendio, inundación, terremoto, explosión, malestar social, y otras formas de desastre natural o artificial.

a) Los materiales inflamables se deberían almacenar a una distancia prudente del área de seguridad.
b) Los equipos de backup y los medios de soporte de seguridad se deberían ubicar a una distancia prudente para evitar daño debido a algún desastre que afecte a las instalaciones principales.
c) Se debería suministrar equipo apropiado contra incendios y ubicarlo adecuadamente.

1.3.5.1.5 Trabajo en Áreas Seguras

Se debería considerar las siguientes directrices:

a) El personal sólo debería conocer la existencia del área segura según las necesidades de la empresa.
b) Se debería evitar el trabajo no supervisado en áreas seguras tanto por razones de seguridad como para evitar las oportunidades de actividades maliciosas.
c) Las áreas seguras vacías deberían tener bloqueo físico y se deberían revisar periódicamente.
d) No se debería permitir equipo de grabación fotográfica, de audio ni otro equipo de grabación como cámaras en dispositivos móviles, a menos que esté autorizado.

1.3.5.1.6 Áreas de Carga, Despacho y Acceso Público

Se recomienda considerar las siguientes directrices:

a) Se debería restringir el acceso al área de despacho y carga desde el exterior de la edificación a personal identificado y autorizado.
b) El área de despacho y carga se debería designar y diseñar para que los suministros se puedan descargar evitando que el personal de despacho tenga acceso a otras partes de la organización.
c) Las puertas externas del área de despacho y entrega deberían estar aseguradas mientras las puertas internas estén abiertas.
d) El material que llega se debería inspeccionar para determinar posibles amenazas antes de moverlo desde el área de despacho y carga hasta el punto de uso.
e) El material que llega se debería registrar de acuerdo con los procedimientos de gestión de activos a su entrada al lugar.
f) Cuando sea posible, los envíos entrantes y salientes se deberían separar físicamente.

1.3.5.2 Seguridad de los Equipos

La protección del equipo debe ser contra amenazas físicas y ambientales, esto ayuda a reducir el riesgo de acceso no autorizado a la información y para proteger contra pérdida o daño. También se debería considerar la ubicación de los equipos.

1.3.5.2.1 Ubicación y Protección de los Equipos

Se recomienda considerar las siguientes directrices para la protección de los equipos:

a) Los equipos se deberían ubicar de modo tal que se minimice el acceso innecesario a las áreas de trabajo.
b) Los servicios de procesamiento de información que manejan datos sensibles, deberían estar ubicados de tal forma que se reduzca el riesgo de visualización de la información por personas no autorizadas.

c) Los elementos que requieran protección especial deberían estar aislados para reducir el nivel general de protección requerida de los demás elementos.
d) Se recomienda adoptar controles para minimizar el riesgo de amenazas físicas potenciales (robo, explosión, falla en el suministro de agua, polvo, vibración, efectos químicos, falla en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo).
e) Se deberían establecer directrices para comer, beber y fumar en las cercanías de los servicios de procesamiento de información.
f) Es conveniente monitorear las condiciones ambientales, para determinar las condiciones que podrían afectar adversamente el funcionamiento de los servicios de procesamiento de información.
g) Se debería aplicar protección contra rayos a todas las edificaciones y adaptar filtros protectores a las fuentes de energía entrantes y a las líneas de comunicación.
h) Es recomendable considerar la utilización de métodos especiales de protección para equipos en ambientes industriales, tales como membranas para los teclados.
i) Los equipos de procesamiento de información sensible deberían estar protegidos para minimizar el riesgo de fuga de información.

1.3.5.2.2 Servicios de Suministro

Todos los servicios de suministro, tales como electricidad, agua, alcantarillado, calefacción, ventilación y aire acondicionado deberían ser adecuados para los sistemas a los que dan apoyo.
Se recomienda tener UPS (Uninterruptible Power Supply) para garantizar el funcionamiento de los servicios y equipos principales hasta que se pueda apagarlos normalmente; o de ser posible, un generador.

1.3.5.2.3 Seguridad del Cableado

Se recomienda tener en cuenta las siguientes directrices para la seguridad del cableado:

a) Las líneas de energía y de telecomunicaciones en los servicios de procesamiento de información deberían ser subterráneas, o tener protección alterna adecuada.
b) El cableado de la red debería estar protegido contra interceptación no autorizada o daño, por ejemplo utilizando conductos o evitando rutas a través de áreas públicas.
c) Los cables de energía deberían estar separados de los cables de comunicaciones para evitar interferencia.
d) Se deberían utilizar rótulos de equipo y de cables claramente identificables para minimizar los errores en las conexiones de cables.
e) Es recomendable emplear un plano del cableado para reducir la posibilidad de errores.
f) Para sistemas críticos se debería considerar la instalación de conductos blindados, uso de fibra, e inspecciones periódicas.

1.3.5.2.4 Mantenimiento de los Equipos

Se recomienda considerar las siguientes directrices para el mantenimiento de los equipos:

a) El mantenimiento de los equipos debería estar acorde con las especificaciones y los intervalos de servicio recomendados por el proveedor.
b) Solo personal autorizado debería realizar las reparaciones y el mantenimiento de los equipos.
c) Se recomienda conservar registros de todas las fallas y de todo el mantenimiento preventivo y correctivo.

d) Es recomendable implementar controles apropiados cuando se programa el mantenimiento para los equipos, si el mantenimiento lo realiza el personal dentro o fuera de la organización y la clase de información que tiene el equipo.
e) Se deberían cumplir todos los requisitos impuestos por las pólizas de seguros;

1.3.5.2.5 Seguridad de los Equipos Fuera de las Instalaciones

Se recomienda tener en cuenta las siguientes directrices para la protección del equipo por fuera de las instalaciones:

a) El equipo y los medios llevados fuera de las instalaciones no se deberían dejar solos en sitios públicos, los computadores portátiles se deberían llevar como equipaje de mano y camuflado.
b) Se deberían observar en todo momento las instrucciones del fabricante para la protección del equipo, por ejemplo, protección contra la exposición a campos electromagnéticos.
c) Se recomienda determinar controles para el trabajo que se realiza en casa mediante una evaluación de riesgos y controles adecuados, por ejemplo gabinetes de archivos con seguro, política de escritorio despejado, controles de acceso a los computadores y comunicaciones seguras con la oficina.
d) Se debería contratar un seguro para proteger el equipo fuera de las instalaciones.

1.3.5.2.6 Seguridad en la Reutilización o Eliminación de los Equipos

Los dispositivos que contienen información sensible se deberían destruir físicamente o su información se debería destruir o sobrescribir usando técnicas que permitan que la información original no se pueda recuperar.

1.3.5.2.7 Retiro de Activos

Se recomienda tener presentes las siguientes directrices:

a) Ni los equipos, ni la información, tampoco el software se deberían retirar sin autorización previa.
b) Los empleados, contratistas y usuarios de terceras partes que tengan autoridad para permitir retirar activos deberían estar claramente identificados.
c) Se recomienda establecer límites de tiempo para el retiro de equipos y verificar el cumplimiento en el momento de devolución.
d) Se debería registrar que el equipo ha sido retirado de la empresa y que ha sido devuelto.

1.3.6 GESTIÓN DE COMUNICACIONES Y OPERACIONES

1.3.6.1 Procedimientos Operacionales y Responsabilidades

Se debería establecer todas las responsabilidades y los procedimientos para la gestión y operación de todos los servicios de procesamiento de información.

1.3.6.1.1 Documentación de los Procedimientos de Operación

Los procedimientos de operación deberían especificar las instrucciones para la ejecución detallada de cada trabajo, incluyendo:

a) Procesamiento y manejo de información.
b) Copias de respaldo.
c) Instrucciones para el manejo de errores y otras condiciones que se pueden presentar durante la ejecución del trabajo, incluyendo las restricciones al uso de las utilidades del sistema.

d) Contactos de soporte en caso de dificultades técnicas u operativas inesperadas.
e) Instrucciones de manejo de los medios y los informes especiales, incluyendo los procedimientos para la eliminación segura de los informes de tareas fallidas.
f) Procedimientos para el reinicio y la recuperación del sistema que se ha de usar en caso de falla del sistema.
g) Gestión de los registros de auditoría y de la información de registro del sistema.

1.3.6.1.2 Gestión del Cambio

Los sistemas operativos y el software de aplicación deberían estar sujetos a un control estricto de la gestión del cambio; se deberían considerar los siguientes elementos:

a) Identificación y registro de los cambios significativos.
b) Planificación y pruebas de los cambios;
c) Evaluación de los impactos potenciales de tales cambios, incluyendo los impactos en la seguridad.
d) Procedimiento de aprobación formal para los cambios propuestos.
e) Comunicación de los detalles del cambio a todas las personas implicadas.
f) Procedimientos de emergencia, incluyendo los procedimientos y las responsabilidades de cancelar o recuperarse de cambios fallidos y eventos imprevistos.

1.3.6.1.3 Distribución (Segregación) de Funciones

La distribución de funciones es un método para reducir el riesgo de uso inadecuado deliberado o accidental del sistema. Se debería tener cuidado de que ninguna persona pueda tener acceso, modificar o utilizar los activos sin autorización o sin ser detectado.

1.3.6.1.4 Separación de las Instalaciones de Desarrollo, Ensayo y Operación

Se deberían tener presentes los siguientes elementos:

a) Se recomienda definir y documentar las reglas para la transferencia de software del estado de desarrollo al operativo.
b) El software de desarrollo y el operativo se deberían ejecutar en diferentes sistemas o procesadores de computación, dominios o directorios.
c) Los compiladores, editores, herramientas de desarrollo o utilidades del sistema no deberían ser accesibles desde los sistemas operativos cuando no se requiera.
d) El ambiente del sistema de prueba debería emular al ambiente del sistema operativo lo más estrechamente posible.
e) Los usuarios deberían emplear perfiles de usuario diferentes para los sistemas operativos y de prueba y los menús deberían desplegar mensajes de identificación adecuados para reducir el riesgo de error.
f) Los datos sensibles no se deberían copiar en el entorno del sistema de prueba.

1.3.6.2 Gestión de la Prestación del Servicio por Terceras Partes

La organización debería verificar la implementación de acuerdos, monitorear el cumplimiento de ellos y gestionar los cambios para asegurar que los servicios que se prestan cumplen los requisitos acordados con los terceros.

1.3.6.2.1 Prestación del Servicio

La prestación de servicios por terceros debería incluir los acuerdos sobre disposiciones de seguridad, definiciones del servicio y aspectos de la gestión del mismo. En el caso de contrataciones externas, la organización debería planificar las transiciones necesarias (de información, servicios de procesamiento de

información y todo lo demás que se deba transferir) y garantizar que la seguridad se mantiene durante todo el período de transición.

1.3.6.2.2 Monitoreo de Revisión de los Servicios por Terceros

El monitoreo y la revisión de los servicios por terceros deberían garantizar el cumplimiento de los términos y condiciones de Seguridad de la Información de los acuerdos y que los incidentes y problemas de la Seguridad de la Información se manejan adecuadamente. La organización debería garantizar que el tercero asigne responsabilidades para la verificación del cumplimiento y la aplicación de los requisitos de los acuerdos. Los servicios, reportes y registros suministrados por terceras partes se deberían controlar y revisar con regularidad y las auditorías se deberían llevar a cabo a intervalos regulares.

1.3.6.2.3 Gestión de los Cambios en los Servicios por Terceras Partes

Es necesario que el proceso de gestión de los cambios en el servicio prestado por el tercero tome en consideración:

a) Los cambios hechos por la organización para implementar mejoras en servicios tales como: desarrollo de aplicaciones nuevas, actualizaciones de la política, nuevos controles para mejorar la seguridad.
b) Cambios en los servicios por el tercero para implementar cambios en las redes, usar nuevas tecnologías, adquirir nuevos productos, nuevas herramientas de desarrollo, cambios en la ubicación física o cambio de proveedores.

1.3.6.3 Planificación y Aceptación del Sistema

Se requieren planificación y preparación para garantizar la disponibilidad de la capacidad y los recursos adecuados para entregar el desempeño requerido del sistema.

1.3.6.3.1 Gestión de la Capacidad

Se recomienda monitorear y adaptar el sistema para garantizar y mejorar la capacidad y la eficacia de los sistemas. Se deberían establecer controles de indagación para indicar los problemas en el momento oportuno. En las proyecciones de los requisitos de capacidad futura se deberían considerar los negocios nuevos y los requisitos del sistema, así como las tendencias actuales y proyectadas en la capacidad de procesamiento de información de la organización.

1.3.6.3.2 Aceptación del Sistema

Se debería garantizar que los requisitos para la aceptación de sistemas nuevos están definidos, acordados, documentados y probados claramente. Los sistemas de información nuevos, las actualizaciones deberían migrar a producción después de obtener la aceptación formal, en la que se deberían considerar:

a) Requisitos de desempeño y capacidad de los computadores.
b) Procedimientos de reinicio y de recuperación por errores, y planes de contingencia.
c) Preparación y prueba de procedimientos operativos de rutina para las normas definidas.
d) Establecimiento del conjunto de controles de seguridad acordados.
e) Procedimientos manuales eficaces.
f) Disposiciones para la continuidad del negocio.
g) Evidencia de que la instalación del sistema nuevo no afectará a los sistemas existentes, en especial en horas pico.
h) Evidencia de que se ha tenido en cuenta el efecto del sistema nuevo en toda la seguridad de la organización.
i) Formación en la utilización de los sistemas nuevos.
j) Facilidad de uso, en la medida en que afecte el desempeño del usuario y evite el error humano.

1.3.6.4 Protección contra Códigos Maliciosos y Móviles

El software y los servicios de procesamiento de información son vulnerables a códigos maliciosos tales como virus de computador, caballos troyanos, gusanos electrónicos. Los usuarios deberían ser conscientes de los peligros de estas vulnerabilidades. Se deberían introducir controles para evitar, detectar y retirar los códigos maliciosos de la organización.

1.3.6.4.1 Controles contra Códigos Maliciosos

La protección contra códigos maliciosos se debería basar en software de detección y reparación de códigos maliciosos, acceso apropiado al sistema y controles en la gestión de cambios. Se recomienda considerar las siguientes directrices:

a) Establecer una política formal que prohíba el uso de software no autorizado.
b) Establecer una política formal para la protección contra los riesgos ligados con la obtención de archivos y software, indicando las medidas de protección que se deberían tomar.
c) Llevar a cabo revisiones regulares del software y del contenido de los sistemas que dan soporte a los procesos críticos del negocio; se debería investigar la presencia de archivos no aprobados o modificaciones no autorizadas.
d) Instalación y actualización del software de detección y reparación de códigos maliciosos para explorar los computadores y los medios.
e) Definir responsabilidades y procedimientos de gestión para tratar la protección contra códigos maliciosos en los sistemas.
f) Preparación de planes adecuados para la continuidad del negocio con el fin de recuperarse de los ataques de códigos maliciosos.
g) Implementación de procedimientos para recolectar información periódicamente, como la suscripción a sitios Web y listados de correo que suministren información sobre los códigos maliciosos.

h) Implementación de procedimientos para verificar la información relacionada con códigos maliciosos y garantizar que los boletines de advertencia sean exactos e informativos.

1.3.6.4.2 Controles contra Códigos Móviles

Se recomienda tener en cuenta las siguientes consideraciones para la protección contra códigos móviles que ejecutan acciones no autorizadas:

a) Ejecución de los códigos móviles en un entorno con aislamiento lógico.
b) Bloqueo de cualquier uso de códigos móviles.
c) Bloqueo de la recepción de códigos móviles.
d) Activación de medidas técnicas en un sistema específico para garantizar la gestión del código móvil.
e) Control de recursos disponibles para el acceso a códigos móviles;
f) Controles criptográficos para autenticar de forma única el código móvil

1.3.6.5 Respaldo

Se deberían establecer procedimientos de rutina para implementar la política y la estrategia de respaldo, para hacer copias de seguridad de los datos y probar sus tiempos de restauración.

1.3.6.5.1 Respaldo de la Información

Es conveniente disponer de servicios de respaldo adecuados para garantizar que la información y el software esenciales se recuperan después de un desastre o una falla de los medios, se recomienda considerar los siguientes elementos:

a) Es recomendable definir el nivel necesario para la información de respaldo.
b) Se deberían hacer registros exactos y completos de las copias de respaldo y generar procedimientos documentados de restauración.

c) La extensión (por ejemplo respaldo completo o diferencial) y la frecuencia de los respaldos debería reflejar los requisitos del negocio de la organización, los requisitos de Seguridad de la Información involucrada y la importancia de la continuidad del negocio de la organización.
d) Los respaldos se deberían almacenar en un sitio lejano, a una distancia suficiente para escapar a cualquier daño debido a desastres en la sede principal.
e) A la información de respaldo se le debería dar un grado apropiado de protección física y ambiental.
f) Es conveniente probar con regularidad los medios de respaldo para garantizar que sean confiables para uso en emergencias.
g) Los procedimientos de restauración se deberían verificar y probar con regularidad para garantizar su eficacia y que se pueden completar dentro del tiempo designado en los procedimientos para la recuperación.
h) En situaciones donde es importante la confidencialidad, los respaldos se deberían proteger por medio de encriptación.

1.3.6.6 Gestión de la Seguridad de las Redes

La gestión segura de las redes, las cuales pueden sobrepasar las fronteras de la organización, exige la consideración del flujo de datos, las implicaciones legales, el monitoreo y la protección.

1.3.6.6.1 Controles de las Redes

Se debería implementar controles que garanticen la Seguridad de la Información en las redes y la protección de los servicios conectados contra el acceso no autorizado. Es conveniente tener en cuenta los siguientes elementos:

a) La responsabilidad operativa de las redes debería estar separada de las operaciones de computador, según sea el caso.

b) Es necesario establecer las responsabilidades y los procedimientos para la gestión de equipos remotos, incluyendo los equipos en áreas de usuarios.
c) Es conveniente establecer controles especiales para mantener la confidencialidad y la integridad de los datos que pasan por redes públicas o redes inalámbricas y para proteger los sistemas y las aplicaciones conectadas.
d) Se deberían aplicar el registro y el monitoreo adecuados para permitir y registrar las acciones de seguridad pertinentes.
e) Se recomienda coordinar las actividades de gestión para optimizar el servicio para la organización y para garantizar que los controles se aplican consistentemente en toda la infraestructura del procesamiento de información.

1.3.6.6.2 Seguridad de los Servicios de la Red

Se debería determinar y monitorear periódicamente la capacidad del proveedor del servicio de red para gestionar los servicios acordados de forma segura, y se debería acordar el derecho a auditoría. La organización debería garantizar que los proveedores de servicios de red implementan estas medidas.

1.3.6.7 Manejo de los Medios

Se deberían establecer procedimientos operativos adecuados para proteger documentos, medios de computador, datos de entrada/salida y documentación del sistema contra divulgación, modificación, remoción y destrucción no autorizadas.

1.3.6.7.1 Gestión de los Medios Removibles

Se recomienda tener presentes las siguientes directrices:

a) Si ya no son necesarios, los contenidos de los medios reutilizables que se van a retirar de la organización se deberían hacer irrecuperables.

b) Cuando sea necesario, se debería exigir autorización para los medios retirados de la organización y conservar un registro de tales retiros.
c) Los medios se deberían almacenar en un ambiente seguro y vigilado, según las especificaciones del fabricante.
d) La información almacenada en los medios que debe estar disponible por más tiempo del de la vida del medio, también se debería almacenar en otra parte para evitar la pérdida de información debido al deterioro de dichos medios.
e) Se debería tener en cuenta el registro de los medios removibles para evitar la oportunidad de que se presente pérdida de datos.
f) Las unidades de medios removibles solo se deberían habilitar si existen razones del negocio para hacerlo.

1.3.6.7.2 Eliminación de los Medios

Los procedimientos formales para la eliminación segura de los medios deberían minimizar el riesgo de fuga de información sensible. Se recomienda tener en cuenta los siguientes elementos.

a) Los medios que contienen información sensible se deberían eliminar de forma segura, por ejemplo mediante incineración.
b) Se deberían establecer procedimientos para identificar los elementos que pueden requerir eliminación segura.
c) Puede ser más fácil disponer de todos los elementos de los medios de almacenamiento que serán recogidos y liberados de forma segura, que tratar de disponer sólo de los elementos sensibles.
d) Muchas organizaciones ofrecen servicios de recolección y eliminación de equipos y medios; se debe tener cuidado en seleccionar un contratista idóneo con control y experiencia adecuados.
e) Se debería registrar la eliminación de los elementos sensibles.

1.3.6.7.3 Procedimientos para el Manejo de la Información

Se deberían elaborar procedimientos para manejar, procesar, almacenar y comunicar la información de acuerdo con su clasificación. Se deberían considerar los siguientes elementos:

a) Manejo y etiquetado de todos los medios hasta su nivel indicado de clasificación.
b) Restricciones de acceso para evitar el acceso de personal no autorizado.
c) Mantenimiento de un registro formal de los receptores autorizados de los datos.
d) Garantizar que los datos de entrada están completos, que el procesamiento se completa adecuadamente y que se aplica la validación de la salida.
e) Protección de los datos de la memoria temporal que esperan su ejecución.
f) Almacenamiento de los medios según las especificaciones del fabricante.
g) Mantenimiento de la distribución de datos en un mínimo.
h) Rotulado de todas las copias de los medios para la autenticación del receptor autorizado.
i) Revisión de las listas de distribución y las listas de receptores autorizados a intervalos regulares.

1.3.6.7.4 Seguridad de la Documentación del Sistema

Para asegurar la documentación del sistema, se deberían tener en cuenta los siguientes elementos:

a) La documentación del sistema se debería almacenar con seguridad.
b) La lista de acceso a la documentación del sistema se debería mantener mínima y debería estar autorizada por el dueño de la aplicación.
c) La documentación del sistema en la red pública o que se suministra a través de una red pública, debería tener protección adecuada.

1.3.6.8 Intercambio de la Información

Se deberían establecer procedimientos y normas para proteger la información y los medios físicos que contienen información en tránsito y que se van a compartir.

1.3.6.8.1 Políticas y Procedimientos para el Intercambio de Información

Los procedimientos y controles a seguir cuando se utilizan servicios de comunicación electrónica para el intercambio de información deberían considerar los siguientes elementos:

a) Procedimientos para proteger la información intercambiada contra interceptación, copiado, modificación, enrutamiento inadecuado y destrucción.
b) Procedimientos para detección y protección contra códigos maliciosos que se pueden transmitir con el uso de comunicaciones electrónicas.
c) Procedimientos para proteger la información electrónica sensible comunicada en forma de adjunto.
d) Directrices que enfaticen el uso aceptable de los servicios de comunicación electrónica.
e) Procedimientos para el uso de comunicaciones inalámbricas, pensando en los riesgos particulares involucrados.
f) Responsabilidades de empleados, contratistas y cualquier otro usuario de no comprometer a la organización.
g) Uso de técnicas criptográficas para proteger la confidencialidad, la integridad y la autenticidad de la información.
h) Directrices de retención y eliminación para toda la correspondencia, incluyendo mensajes, según la legislación y reglamentos locales y nacionales correspondientes.
i) No dejar información sensible en los dispositivos de impresión como copiadoras, impresoras y máquinas de facsímil.

j) Controles y restricciones asociados con el envío de servicios de comunicación, como el envío automático de correo electrónico a direcciones de correo externas;
k) Recordar al personal que deberían tomar precauciones adecuadas como no revelar información sensible.
l) No dejar mensajes que contengan información sensible en el contestador automático.
m) Recordar al personal sobre los problemas de usar máquinas de facsímil (envío a número erróneo, envío automático programado).
n) Recordar al personal no registrar datos demográficos, como direcciones de correo electrónico o información personal, en ningún software para evitar su recolección para uso no autorizado.
o) Recordar al personal que las máquinas modernas de facsímil y las fotocopiadoras tienen páginas de almacenamiento y caché, en caso de falla en el papel o en la transmisión, que se pueden imprimir una vez se ha solucionado la falla.

1.3.6.8.2 Acuerdos para el Intercambio de Información

En los acuerdos de intercambio de información se deberían tomar en consideración las siguientes condiciones de seguridad:

a) Responsabilidades de la dirección para controlar y notificar la transmisión, el despacho y la recepción;
b) Procedimientos para notificar a quien envía, la transmisión, el despacho y la recepción.
c) Procedimientos para garantizar la trazabilidad y el no-repudio.
d) Normas técnicas mínimas para el empaquetado y la transmisión.
e) Acuerdos de fideicomiso.
f) Normas para identificar los servicios de mensajería.
g) Responsabilidades y deberes en caso de incidentes de Seguridad de la Información, como pérdida de datos.

h) Uso de sistemas acordados de etiquetado de la información, garantizando que el significado de las etiquetas se entienda inmediatamente y que la información está protegida adecuadamente.
i) Propiedad y responsabilidades para la protección de datos, derechos de copia, conformidad de las licencias de software.
j) Normas técnicas para registrar y leer la información y el software;
k) Todos los controles especiales que se puedan requerir para proteger los elementos sensibles tales como las claves criptográficas.

1.3.6.8.3 Medios Físicos en Tránsito

Se recomienda tener en cuenta las siguientes directrices para la protección de los medios que se transportan entre los lugares:

a) Se recomienda utilizar transporte confiable o servicios de mensajería.
b) Se debería acordar con la dirección una lista de servicios de mensajería.
c) Se deberían desarrollar procedimientos para verificar la identificación de los servicios de mensajería.
d) El embalaje debería ser suficiente para proteger el contenido contra cualquier daño físico que se pueda producir durante el transporte, por ejemplo protección contra todos los factores ambientales que puedan reducir la eficacia de la restauración de los medios (datos de fabricante).
e) Cuando sea necesario, se deberían adoptar controles para proteger la información sensible contra divulgación o modificación no autorizada.

1.3.6.8.4 Mensajería Electrónica

Las consideraciones de seguridad para la mensajería electrónica deberían incluir las siguientes:

a) Proteger los mensajes contra acceso no autorizado, modificación o negación de los servicios.
b) Garantizar que la dirección y el transporte del mensaje son correctos.

c) Confiabilidad general y disponibilidad del servicio.
d) Consideraciones legales como, por ejemplo, los requisitos para las firmas electrónicas.
e) Obtención de aprobación antes de utilizar servicios públicos externos como la mensajería instantánea o el compartir archivos.
f) Niveles sólidos de autenticación que controlen el acceso desde redes accesibles al público.

1.3.6.8.5 Sistemas de Información del Negocio

Se deberían establecer, desarrollar e implementar políticas para proteger la información asociada con los sistemas de información del negocio, las consideraciones de tales servicios para la seguridad y para el negocio deberían incluir:

a) Vulnerabilidades conocidas en los sistemas administrativos y de contaduría en donde la información es compartida entre diferentes partes de la organización.
b) Vulnerabilidades de la información en los sistemas de comunicación del negocio, por ejemplo la grabación de llamadas telefónicas, almacenamiento de facsímiles, distribución del correo.
c) Políticas y controles adecuados para gestionar la forma en que se comparte la información.
d) Categorías excluyentes de información sensible, si los sistemas no brindan un nivel adecuado de protección.
e) Restricción del acceso a la información diaria, relacionada con individuos seleccionados, por ejemplo el personal de proyectos sensibles.
f) Categorías de personal, contratistas o socios del negocio a quienes se permite usar el sistema y los sitios desde los cuales pueden tener acceso.
g) Restricción de los servicios seleccionados para categorías de usuarios específicos.
h) Identificación del estado de los usuarios (empleados de la organización o contratistas) en los directorios para el beneficio de otros usuarios.

i) Retención y copias de respaldo de la información contenida en el sistema.
j) Requisitos y disposiciones para los recursos de emergencia.

1.3.6.9 Servicios de Comercio Electrónico

Es necesario considerar las implicaciones de seguridad asociadas al uso de servicios de comercio electrónico, incluyendo las transacciones en línea y los requisitos para los controles. También se deberían considerar la integridad y disponibilidad de la información publicada electrónicamente a través de sistemas disponibles al público.

1.3.6.9.1 Comercio Electrónico

Las consideraciones de seguridad para el comercio electrónico deberían incluir las siguientes:

a) El nivel de confianza que exige cada parte en la identidad declarada de las otras partes, por ejemplo por medio de autenticación.
b) Los procesos de autorización asociados con la persona que puede emitir o firmar documentos comerciales clave.
c) La garantía de que los socios comerciales están totalmente informados sobre sus autorizaciones.
d) La determinación y el cumplimiento de los requisitos de confidencialidad, integridad, prueba de despacho y recibo de documentos clave, y el no repudio de contratos, por ejemplo los asociados a los procesos de licitación.
e) El nivel de confianza exigido en la integridad de las listas de precios publicadas.
f) La confidencialidad de datos o información sensible.
g) La confidencialidad e integridad de las transacciones de orden de compra, información sobre pagos, detalles de las direcciones de entrega y confirmación de recibo.

h) El grado adecuado de verificación para comprobar la información sobre pagos suministrada por un cliente.
i) La selección del mejor convenio sobre la forma de pago más apropiada para evitar el fraude.
j) El nivel de protección exigido para mantener la confidencialidad e integridad de la información de orden de compra.
k) Evitar la pérdida o duplicación de la información sobre transacciones.
l) La responsabilidad asociada con transacciones fraudulentas.
m) Los requisitos de las pólizas de seguros.

1.3.6.9.2 Transacciones en Línea

Las consideraciones de seguridad para las transacciones en línea deberían incluir las siguientes:

a) Uso de firmas electrónicas por cada una de las partes implicadas en la transacción;
b) Todos los aspectos de la transacción (credenciales, transacción confidencial, privacidad).
c) Encriptación de la ruta para las comunicaciones entre todas las partes involucradas.
d) Seguridad de los protocolos utilizados para la comunicación entre todas las partes involucradas.
e) Garantizar que el almacenamiento de los detalles de la transacción está fuera de cualquier entorno de acceso público (Intranet), y que no se retiene ni expone en un medio de almacenamiento accesible directamente desde Internet.
f) Cuando se emplea una autoridad confiable (por ejemplo firmas digitales y/o certificados digitales) la seguridad se integra a través de todo el proceso completo de gestión del certificado/firma.

1.3.6.9.3 Información Disponible al Público

El software y otra información que requiere un nivel alto de integridad y que están en sistemas públicos se deberían proteger con mecanismos apropiados como firmas digitales. Los sistemas de acceso público se deberían probar frente a debilidades y fallas antes de que la información esté disponible, también se debe asegurar que:

a) La información se obtenga de conformidad con toda la legislación sobre protección de datos.
b) La entrada de información hacia el sistema editorial se procese completa y exactamente de forma oportuna.
c) La información sensible estará protegida durante la recolección, el procesamiento y el almacenamiento.
d) El acceso al sistema editorial no permite acceso involuntario a redes a las cuales se conecta el sistema.

1.3.6.10 Monitoreo

Se deberían monitorear los sistemas y registrar los eventos de Seguridad de la Información. Los registros de operador y la actividad de registro de fallas se deberían utilizar para garantizar la identificación de los problemas del sistema de información.

1.3.6.10.1 Registro de Auditorías

Los registros para auditoría deberían incluir, cuando corresponda.

a) Identificación (ID) de usuario.
b) Fecha, hora y detalles de los eventos clave (registro de inicio y registro de cierre).
c) Identidad o ubicación de la terminal.

d) Registros de los intentos aceptados y rechazados de acceso al sistema.
e) Registros de los intentos aceptados y rechazados de acceso a los datos y otros recursos.
f) Cambios en la configuración del sistema.
g) Uso de privilegios.
h) Uso de las utilidades y aplicaciones del sistema.
i) Archivos a los que se ha tenido acceso y tipo de acceso.
j) Direcciones y protocolo de red.
k) Alarmas originadas por el sistema de control de acceso.
l) Activación y desactivación de los sistemas de protección, como los sistemas antivirus y los sistemas de detección de intrusión.

1.3.6.10.2 Monitoreo del Uso del Sistema

El nivel de monitoreo necesario para servicios individuales se debería determinar mediante una evaluación de riesgos. La organización debería cumplir todos los requisitos legales que se apliquen a sus actividades de monitoreo. Las áreas que se deberían considerar incluyen:

a) Acceso autorizado.
b) Todas las operaciones privilegiadas.
c) Intentos de acceso no autorizado.
d) Alertas o fallas del sistema.
e) Cambios o intentos de cambio en la configuración y los controles de seguridad del sistema.

La frecuencia con la cual se revisan los resultados de las actividades de monitoreo debería depender de los riesgos involucrados. Los factores de riesgo que se deberían considerar incluyen:

a) Importancia de los procesos de aplicación.
b) Valor, sensibilidad e importancia de la información implicada.

c) Experiencia previa de infiltración o uso inadecuado del sistema, y frecuencia de aprovechamiento de las vulnerabilidades.
d) Extensión de la interconexión del sistema (particularmente en redes públicas).
e) Servicio de operación de registro que se desactiva.

1.3.6.10.3 Protección de la Información del Registro

Los servicios y la información de la actividad de registro se deberían proteger contra el acceso o la manipulación no autorizados. Los controles deberían tener como objeto la protección contra cambios no autorizados y problemas operativos con el servicio de registro incluyendo:

a) Alteraciones en los tipos de mensaje que se registran.
b) Archivos de registro que se editan o eliminan.
c) Capacidad de almacenamiento de los medios de archivo de registro que se exceden, lo que resulta en la falla para grabar eventos o sobre-escritura de eventos grabados anteriormente.

1.3.6.10.4 Registros del Administrador y del Operador

Se deberían registrar las actividades tanto del operador como del administrador del sistema. Los registros deberían incluir:

a) La hora en que ocurrió el evento.
b) Información sobre el evento (por ejemplo archivos manipulados) o la falla (por ejemplo errores que se presentaron y acciones correctivas que se tomaron).
c) Cuál cuenta y cuál administrador estuvo involucrado.
d) Cuáles procesos estuvieron implicados.

1.3.6.10.5 Registro de Fallas

Se deberían registrar las fallas reportadas por los usuarios o por los programas del sistema relacionadas con problemas de procesamiento de la información o con los sistemas de comunicación. Deberían existir reglas claras para el manejo de las fallas reportadas, incluyendo:

a) Revisión de los registros de fallas para garantizar que éstas se han resuelto satisfactoriamente.
b) Revisión de las medidas correctivas para garantizar que no se han puesto en peligro los controles y que la acción tomada está totalmente autorizada.

1.3.6.10.6 Sincronización de Relojes

Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de la organización o del dominio de seguridad deberían estar sincronizados con una fuente de tiempo exacta y acordada.

1.3.7 CONTROL DE ACCESO

1.3.7.1 Requisitos del Negocio para el Control del Acceso

El acceso a la información, a los servicios de procesamiento de información y a los procesos del negocio se debería controlar con base en los requisitos de seguridad y del negocio. Las reglas para el control del acceso deberían tener en cuenta las políticas de distribución y autorización de la información.

1.3.7.1.1 Política de Control de Acceso

Las reglas y los derechos para el control del acceso para los usuarios se deberían establecer con claridad en una política de control del acceso, los controles del

acceso son tanto lógicos como físicos y se deberían considerar en conjunto. La política debería considerar los siguientes aspectos:

a) Requisitos de seguridad de las aplicaciones individuales del negocio.
b) Identificación de toda la información relacionada con las aplicaciones del negocio y los riesgos a los que se enfrenta la información.
c) Políticas para la distribución y autorización de la información, por ejemplo la necesidad de conocer los principios, niveles de seguridad y clasificación de la información.
d) Consistencia entre el control del acceso y las políticas de clasificación de la información de sistemas y redes diferentes.
e) Legislación pertinente y obligaciones contractuales relacionadas con la protección del acceso a los datos o los servicios.
f) Perfiles estándar de acceso de usuario para funciones laborales comunes en la organización.
g) Gestión de los derechos de acceso en un entorno distribuido y con red que reconozca todos los tipos de conexiones posibles.
h) Distribución de las funciones de control de acceso, por ejemplo solicitud de acceso, autorización del acceso, administración del acceso.
i) Requisitos para la autorización formal de las solicitudes de acceso.
j) Requisitos para la revisión periódica de los controles de acceso.
k) Retiro de los derechos de acceso.

1.3.7.2 Gestión del Acceso de Usuarios

Se deberían establecer procedimientos para controlar el acceso a los sistemas y servicios de información, éstos deberían comprender desde el registro inicial de los usuarios nuevos hasta la cancelación final del registro de usuarios que ya no requieren acceso a los servicios y sistemas de información. Se debería poner atención especial con los usuarios con capacidad para modificar estos controles.

1.3.7.2.1 Registro de Usuarios

*D*ebería existir un procedimiento para el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de información. El procedimiento de control del acceso para el registro y cancelación de usuarios debería tener:

a) Uso de la identificación por usuario (ID) para permitir que los usuarios sean responsables de sus acciones; cuando se requieran ID's de grupo, se debería permitir por razones del negocio pero deberían estar aprobados y documentados.
b) Verificación de que el usuario tenga autorización del dueño del sistema para el uso del sistema o servicio de información.
c) Verificación de que el nivel de acceso otorgado sea adecuado para que los propósitos del negocio sean consistentes con la política de seguridad de la organización, es decir, no pone en peligro la distribución de funciones.
d) Dar a los usuarios una declaración escrita de sus derechos de acceso.
e) Exigir a los usuarios firmar declaraciones que indiquen que ellos entienden las condiciones del acceso.
f) Asegurar que los proveedores del servicio no otorguen el acceso hasta que se hayan terminado los procedimientos de autorización.
g) Mantenimiento de un registro formal de todas las personas registradas para usar el servicio.
h) Retirar o bloquear inmediatamente los derechos de acceso de los usuarios que han cambiado de función, de trabajo o que han dejado la organización.
i) Garantizar que las identificaciones (ID) de usuario no se otorgan a otros usuarios.

1.3.7.2.2 Gestión de Privilegios

Se debería controlar la asignación y el uso de privilegios. Los sistemas de usuario múltiple que requieren protección contra el acceso no autorizado deberían

controlar la asignación de privilegios a través de un proceso formal de autorización. Se recomienda tener en cuenta los siguientes elementos:

a) Se deberían identificar los usuarios y sus privilegios de acceso asociados con cada producto del sistema.
b) Se deberían asignar los privilegios a los usuarios sobre los principios de necesidad de uso, de manera acorde con la política de control de acceso.
c) Se debería conservar un registro de todos los privilegios asignados. Los privilegios no se deberían otorgar hasta que el proceso de autorización esté completo.
d) Es conveniente promover el desarrollo y empleo de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.
e) Se recomienda promover también el desarrollo y empleo de programas que eviten la necesidad de funcionar con privilegios.
f) Los privilegios se deberían asignar a un identificador de usuario (ID) diferente a los utilizados para el uso normal del negocio.

1.3.7.2.3 Gestión de Contraseñas para Usuarios

La asignación de contraseñas se debería controlar a través de un proceso formal de gestión. El proceso debería incluir los siguientes requisitos:

a) Se debería exigir a los usuarios la firma de una declaración para mantener confidenciales las contraseñas personales y conservar las contraseñas de grupo únicamente entre los miembros de éste.
b) Cuando se exige a los usuarios mantener sus propias contraseñas, inicialmente se les debería suministrar una contraseña temporal segura que estén forzados a cambiar inmediatamente.
c) Establecer procedimientos para verificar la identidad de un usuario antes de proporcionarle una contraseña temporal, nueva.
d) Las contraseñas temporales se deberían suministrar de forma segura a los usuarios; se recomienda evitar mensajes de correo electrónico de terceras partes o sin protección.

e) Las contraseñas temporales deberían ser únicas para un individuo y no ser descifrables;
f) Los usuarios deberían confirmar la entrega de las contraseñas;
g) Las contraseñas nunca se deberían almacenar en sistemas de computador en un formato no protegido;
h) Las contraseñas predeterminadas por el proveedor se deberían cambiar inmediatamente después de la instalación de los sistemas o del software.

1.3.7.2.4 Revisión de los Derechos de Acceso de los Usuarios

La dirección debería establecer un procedimiento formal de revisión periódica de los derechos de acceso de los usuarios. Se deberían considerar las siguientes directrices:

a) Los derechos de acceso de los usuarios se deberían revisar a intervalos regulares (cada cierto tiempo o después de cada cambio de funciones).
b) Los derechos de acceso de usuarios se deberían revisar y reasignar cuando hay cambios de un cargo a otro dentro de la misma organización.
c) Es recomendable revisar las autorizaciones para derechos de acceso privilegiado a intervalos frecuentes (tiempo menor a los derechos de acceso normales).
d) Se debería verificar la asignación de privilegios a intervalos regulares para garantizar que no se obtienen privilegios no autorizados.
e) Los cambios en las cuentas privilegiadas se deberían registrar para su revisión periódica.

1.3.7.3 Responsabilidades de los Usuarios

Se debería concientizar a los usuarios sobre sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular con relación al uso de contraseñas y a la seguridad del equipo del usuario.

1.3.7.3.1 Uso de Contraseñas

Se debería exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de contraseñas. Todos los usuarios deberían:

a) Mantener la confidencialidad de las contraseñas.
b) Evitar conservar registros de las contraseñas, a menos que éstas se puedan almacenar de forma segura y el método de almacenamiento esté aprobado.
c) Cambiar las contraseñas siempre que haya indicación de puesta en peligro del sistema o de la contraseña.
d) Seleccionar contraseñas de calidad (fáciles de recordar, con caracteres especiales, difíciles de adivinar, no sean vulnerables a diccionarios, no tengan caracteres idénticos consecutivos).
e) Cambiar las contraseñas a intervalos regulares o con base en el número de accesos y evitar la reutilización de contraseñas antiguas.
f) Cambiar las contraseñas temporales en el primer registro de inicio.
g) No incluir contraseñas en ningún proceso de registro automatizado, por ejemplo almacenadas en un macro o en una clave de función.
h) No compartir las contraseñas de usuarios individuales.
i) No utilizar la misma contraseña para propósitos del negocio y para los que no lo son.

1.3.7.3.2 Equipo de Usuario Desatendido

Se debería concientizar a los usuarios sobre los requisitos y los procedimientos de seguridad para proteger los equipos desatendidos, así como sobre sus responsabilidades en la implementación de dicha protección. Se debería advertir a los usuarios sobre:

a) Terminar las sesiones cuando finalice, a menos que se puedan asegurar por medio de un mecanismo de bloqueo (protector de pantalla con contraseña).

b) Realizar el registro de cierre en computadoras principales, servidores y computadores personales de oficina al terminar la sesión.
c) Cuando no están en uso, asegurar los terminales contra el uso no autorizado mediante una clave de bloqueo o una contraseña.

1.3.7.3.3 Política de Escritorio Despejado y de Pantalla Despejada

En la política de escritorio despejado y pantalla despejada se deberían considerar las clasificaciones de la información, los requisitos legales y contractuales, los riesgos correspondientes y los aspectos culturales de la organización. Es recomendable tener presentes las siguientes directrices:

a) Cuando no se requiere la información crítica del negocio, como por ejemplo los medios de almacenamiento electrónicos o en papel, se debería asegurarlos bajo llave (caja fuerte, gabinete).
b) Las sesiones de los terminales se deberían proteger con un mecanismo de bloqueo de pantalla y de teclado controlado por una contraseña, para que se activen automáticamente después de un lapso de inactividad.
c) Se deberían proteger los puntos de entrada y salida de correo y los fax desatendidos.
d) Es conveniente evitar el uso no autorizado de fotocopiadoras y otra tecnología de reproducción.
e) Los documentos que contengan información sensible se deberían retirar inmediatamente de las impresoras.

1.3.7.4 Control de Acceso a las Redes

Es recomendable controlar el acceso a los servicios en red. El acceso de los usuarios a las redes y a los servicios de red no debería comprometer la seguridad de los servicios de red garantizando que:

a) Existen interfaces apropiadas entre la red de la organización y las redes que pertenecen a otras organizaciones, y las redes públicas.
b) Se aplican mecanismos adecuados de autenticación para los usuarios y los equipos.
c) Se exige control de acceso de los usuarios a los servicios de información.

1.3.7.4.1 Política de Uso de los Servicios en Red

Los usuarios solo deberían tener acceso a los servicios para cuyo uso están específicamente autorizados. Se debería formular una política con respecto al uso de las redes y los servicios de red. Esta política debería abarcar:

a) Las redes y los servicios de red a los cuales se permite el acceso.
b) Los procedimientos de autorización para determinar a quién se le permite el acceso a qué redes y qué servicios en red.
c) Los controles y procedimientos de gestión para proteger el acceso a las conexiones de red y los servicios de red.
d) Los medios utilizados para el acceso a las redes y los servicios de red.

1.3.7.4.2 Autenticación de Usuarios para Conexiones Externas

Se deberían emplear métodos apropiados de autenticación para controlar el acceso de usuarios remotos. Se puede lograr usando técnicas con bases criptográficas, token de hardware o protocolos de desafío/respuesta. Las posibles implementaciones de dichas técnicas se pueden encontrar en diversas soluciones de red privada virtual (VPN).

Se deberían implementar controles de autenticación adicionales para controlar el acceso a redes inalámbricas debido a las grandes oportunidades para la interceptación y que no son detectadas en el tráfico de red.

1.3.7.4.3 Identificación de los Equipos en las Redes

En la identificación automática de los equipos se debería considerar un medio para autenticar conexiones de equipos y ubicaciones específicas. Un identificador en el equipo se puede usar para indicar si está permitido que este equipo se conecte a la red. Estos identificadores deberían indicar con claridad a qué red está permitido conectar el equipo, si existe más de una red y si estas tienen sensibilidad diferente.

1.3.7.4.4 Protección de los Puertos de Configuración y Diagnóstico Remoto

Los controles para el acceso a los puertos de diagnóstico y configuración, incluyen el uso de un bloqueo de clave y procedimientos de soporte para controlar el acceso físico al puerto. Un ejemplo de un procedimiento de soporte es garantizar que los puertos de diagnóstico y configuración sólo sean accesibles mediante acuerdo entre el administrador del servicio de computador y el personal de soporte de hardware/software que requiere el acceso.

1.3.7.4.5 Separación en las Redes

En las redes se deberían separar los grupos de servicios de información, usuarios y sistemas de información. Un método para el control en las redes grandes es dividirlas en dominios lógicos de red separados, cada uno protegido por un perímetro de seguridad. Se puede aplicar un conjunto graduado de controles en diferentes dominios lógicos de red para separar aún más los entornos de seguridad de la red, por ejemplo los sistemas de acceso público, las redes internas y los activos críticos.

Se puede implementar un perímetro de red instalando una puerta de enlace (Gateway) seguro entre las dos redes que se van a interconectar para controlar el acceso y el flujo de información entre los dos dominios. Esta puerta de enlace (Gateway) se debería configurar para filtrar el tráfico entre estos dominios y para bloquear el acceso no autorizado, este tipo de puerta de enlace es lo que se

conoce comúnmente como barrera de fuego (firewall). Otro método para apartar los dominios lógicos separados es restringir el acceso a la red usando redes privadas virtuales para grupos de usuarios dentro de la organización, o para las redes inalámbricas procedentes de redes internas y privadas.

1.3.7.4.6 Controles de Conexión a las Redes

Para redes compartidas, se debería restringir la capacidad de los usuarios para conectarse a la red, de acuerdo con la política de control de acceso y los requisitos de aplicación del negocio. Se puede restringir a través de puertas de enlace (Gateway) de red que filtren el tráfico por medio de reglas predefinidas. Los siguientes son algunos ejemplos de aplicaciones a las cuales se deberían aplicar restricciones:

a) mensajería, por ejemplo, el correo electrónico.
b) Transferencia de archivos.
c) Acceso interactivo.
d) Acceso a las aplicaciones.

1.3.7.4.7 Control del Enrutamiento en la Red

Se deberían implementar controles de enrutamiento en las redes con el fin de asegurar que las conexiones entre computadores y los flujos de información no incumplan la política de control de acceso de las aplicaciones del negocio. Las puertas de enlace (Gateway) de seguridad se pueden usar para validar la dirección fuente/destino en los puntos de control de las redes interna y externa.

1.3.7.5 Control de Acceso al Sistema Operativo

Se recomienda utilizar medios de seguridad para restringir el acceso de usuarios no autorizados a los sistemas operativos. Tales medios deberían tener la capacidad para:

a) Autenticar usuarios autorizados, de acuerdo con una política de control de acceso.
b) Registrar intentos exitosos y fallidos de autenticación del sistema.
c) Registrar el uso de privilegios especiales del sistema.
d) Emitir alarmas cuando se violan las políticas de seguridad del sistema.
e) Suministrar medios adecuados para la autenticación.
f) Cuando sea apropiado, restringir el tiempo de conexión de los usuarios.

1.3.7.5.1 Procedimiento de Registro de Inicio Seguro

El procedimiento de registro en un sistema operativo debería estar diseñado para minimizar la oportunidad de acceso no autorizado. Por ello, el procedimiento de registro de inicio debería divulgar información mínima sobre el sistema para evitar suministrar asistencia a un usuario no autorizado. Un buen procedimiento de registro de inicio debería cumplir los siguientes aspectos:

a) No mostrar identificadores de aplicación ni de sistema hasta que el proceso de registro de inicio se haya completado exitosamente.
b) Mostrar una advertencia de notificación general indicando que solo deberían tener acceso al computador los usuarios autorizados.
c) No suministrar mensajes de ayuda durante el procedimiento de registro de inicio que ayuden a un usuario no autorizado.
d) Validar la información de registro de inicio únicamente al terminar todos los datos de entrada. Si se presenta una condición de error, el sistema no debería indicar que parte de los datos es correcta o incorrecta.
e) Limitar la cantidad de intentos permitidos de registro de inicio.
f) Limitar el tiempo máximo permitido para el procedimiento de registro de inicio.
g) Mostrar información de fecha y hora de registro exitoso y el detalle de intentos fallidos.
h) No mostrar la contraseña que se introduce o esconder los caracteres mediante símbolos.

i) No transmitir contraseñas en texto claro en la red.

1.3.7.5.2 Identificación y Autenticación de Usuarios

Todos los usuarios deberían tener un identificador único (ID del usuario) para su uso personal, y se debería elegir una técnica de autenticación para comprobar la identidad de un usuario. Los identificadores de usuario (ID) se deberían utilizar para rastrear las actividades de la persona responsable.

1.3.7.5.3 Sistema de Gestión de Contraseñas

Los sistemas para la gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas. Un sistema de gestión de contraseñas debería:

a) Hacer cumplir el uso de identificadores de usuario (ID) individual y de contraseñas para conservar la responsabilidad.
b) Permitir a los usuarios la selección y el cambio de sus contraseñas e incluir un procedimiento de confirmación para tener en cuenta los errores en los ingresos.
c) Imponer una elección de contraseñas de calidad.
d) Imponer cambios de contraseña.
e) Forzar a los usuarios a cambiar las contraseñas temporales en el primer registro de inicio.
f) Conservar un registro de las contraseñas de usuario previas y evitar su reutilización.
g) No mostrar contraseñas en la pantalla cuando se hace su ingreso.
h) Almacenar los archivos de contraseñas separadamente de los datos del sistema de aplicación.
i) Almacenar y transmitir contraseñas en formatos protegidos (encriptadas o codificadas)

1.3.7.5.4 Uso de las Utilidades del Sistema

Se debería restringir y controlar estrictamente el uso de programas que pueden anular los controles del sistema de la aplicación. Se recomienda considerar las siguientes directrices:

a) Uso de procedimientos de identificación, autenticación y autorización para las utilidades del sistema.
b) Separación de las utilidades del sistema del software de aplicaciones.
c) Limitación del uso de las utilidades del sistema a la cantidad mínima viable de usuarios de confianza autorizados.
d) Autorización del uso ad hoc de las utilidades del sistema.
e) Limitación de la disponibilidad de las utilidades del sistema, por ejemplo para la duración de un cambio autorizado.
f) Registro de todo uso de las utilidades del sistema.
g) Definición y documentación de los niveles de autorización para las utilidades del sistema.
h) Retiro de todas las utilidades o el software del sistema basado en software innecesario.
i) No poner a disposición las utilidades del sistema a usuarios que tengan acceso a aplicaciones en sistemas en donde se requiere distribución de funciones.

1.3.7.5.5 Tiempo de Inactividad de la Sesión

Una utilidad de tiempo de inactividad debería despejar la pantalla de sesión y también cerrar la sesión de la aplicación y la de red después de un periodo definido de inactividad.

1.3.7.5.6 Limitación del Tiempo de Conexión

Se deberían tener en cuenta los controles de tiempo para las aplicaciones sensibles de computador, en especial las de lugares de alto riesgo, por ejemplo

áreas públicas que están fuera de la gestión de seguridad de la organización. Los siguientes son algunos ejemplos de estas restricciones:

a) Uso de conexiones por tiempo predeterminados.
b) Restricción de los tiempos de conexión a las horas normales de oficina, si no se requiere tiempo extra u operaciones de horario prolongado.
c) Considerar la repetición de la autenticación a intervalos determinados.

1.3.7.6 Control de Acceso a las Aplicaciones y a la Información

Se deberían usar medios de seguridad para restringir el acceso a los sistemas de aplicación. Los sistemas de aplicación deberían contener requerimientos como:

a) Controlar el acceso de usuarios a la información de acuerdo con una política definida de control de acceso.
b) Suministrar protección contra acceso no autorizado por una aplicación, el software del sistema operativo o software malicioso que pueda anular o desviar los controles del sistema o de la aplicación.
c) No poner en peligro otros sistemas con los que se comparten los recursos de información.

1.3.7.6.1 Restricción del Acceso a la Información

Se debería restringir el acceso a la información y a las funciones del sistema de aplicación por parte de los usuarios. Las restricciones del acceso se deberían basar en los requisitos de las aplicaciones del negocio. Se debería considerar la aplicación de las siguientes directrices:

a) Proporcionar menús para controlar el acceso a las funciones del sistema de aplicación.
b) Controlar los derechos de acceso de los usuarios (leer, escribir, eliminar y ejecutar).

c) Controlar los derechos de acceso de otras aplicaciones.
d) Garantizar que los datos de salida de los sistemas de aplicación que manejan información sensible sólo contienen la información pertinente para el uso de la salida y que se envía únicamente a terminales autorizados.

1.3.7.6.2 Aislamiento de Sistemas Sensibles

Los sistemas sensibles deberían tener un entorno informático aislado. Se deberían considerar los siguientes puntos para el aislamiento de los sistemas sensibles:

a) La sensibilidad de un sistema de aplicación se debería identificar y documentar por parte del dueño de la aplicación.
b) Cuando una aplicación se ejecute en un entorno compartido, los sistemas de aplicación con los cuales compartirá recursos y los riesgos de esta compartición deberían ser identificados y aceptados por el responsable de la aplicación sensible.

1.3.7.7 Computación Móvil y Trabajo Remoto

La protección debería estar acorde con los riesgos que originan estas formas específicas de trabajo. Cuando se usa la computación móvil, se deberían tener en cuenta los riesgos de trabajar en un entorno sin protección y aplicar la protección adecuada, cuando se trabaja desde un sitio remoto, la organización debería aplicar protección en el sitio del remoto y garantizar que se han establecido las disposiciones adecuadas para esta forma de trabajo.

1.3.7.7.1 Computación y Comunicaciones Móviles

Cuando se usan servicios de computación y de comunicaciones móviles (notebook, palmtop, laptop, tarjetas inteligentes y teléfonos móviles) se debería tener cuidado especial para asegurarse de que la información no se pone en

riesgo. Se deberían incluir los requisitos para la protección física, los controles de acceso, las técnicas criptográficas, las copias de respaldo y la protección contra virus.

El acceso remoto a la información del negocio a través de redes públicas usando servicios de computación móvil solo debería tener lugar después de la identificación y la autenticación exitosa. Los servicios de computación móvil también se deben proteger físicamente contra robo, especialmente cuando se deja, en automóviles y otros medios de transporte, habitaciones de hoteles, centros de conferencias y reuniones.

Es conveniente contratar un seguro para los casos de robo o pérdida de los servicios de computación móvil. El equipo que porta información sensible no se debería dejar desatendido y se debería bloquear con algún medio físico o cerraduras especiales para asegurar el equipo.
Se recomienda disponer la formación del personal que utiliza computación móvil para concientizar sobre los riesgos adicionales que se originan en este tipo de trabajo y los controles que se deberían implementar.

Como todos sabemos, la tecnología celular está aun en evolución, razón por la cual su sistema de seguridad tiene algunas vulnerabilidades conocidas que deberían ser tomadas en cuenta.

1.3.7.7.2 Trabajo Remoto

Se deberían implementar políticas, planes operativos y procedimientos para las actividades de trabajo remoto. Las organizaciones sólo deberían autorizar las actividades de trabajo remoto si están satisfechas las disposiciones de seguridad adecuadas y los controles establecidos. Se recomienda considerar los siguientes aspectos:

a) La seguridad física en el sitio de trabajo remoto (seguridad física y del entorno).

b) El entorno físico de trabajo remoto propuesto.
c) Los requisitos de seguridad de las comunicaciones, pensando en la necesidad de acceso remoto a los sistemas internos de la organización, la sensibilidad de la información a la cual se tendrá acceso.
d) La amenaza del acceso no autorizado a la información o los recursos por parte de otras personas que usan el mismo espacio (familia y amigos).
e) El uso de redes domésticas y los requisitos en la configuración de servicios de red inalámbrica.
f) Las políticas para evitar disputas con respecto a los derechos de propiedad intelectual desarrollados o al equipo de propiedad privada.
g) El acceso a equipo de propiedad privada (para verificar la seguridad de la maquina o durante una investigación), si es permitido por la ley.
h) Los acuerdos sobre licencias de software que permitan que la organización sea responsable de la licencia para software de clientes en estaciones de trabajo de propiedad privada de los empleados, contratistas o usuarios de terceras partes.
i) Protección antivirus y requisitos de barreras contra fuego (firewall).

1.3.8 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

1.3.8.1 Requisitos de Seguridad de los Sistemas de Información

Los sistemas de información incluyen sistemas operativos, infraestructura, aplicaciones del negocio, productos de vitrina, servicios y aplicaciones desarrolladas para usuarios. El diseño y la implementación del sistema de información que da soporte a los procesos del negocio pueden ser cruciales para la seguridad. Se deberían identificar los requisitos de seguridad antes del desarrollo y/o la implementación de los sistemas de información.

1.3.8.1.1 Análisis y Especificación de los Requisitos de Seguridad

En las especificaciones para los requisitos de control se deberían considerar los controles automatizados que se han de incorporar en el sistema de información y la necesidad de controles y manuales de apoyo. Los requisitos del sistema para la Seguridad de la Información y los procesos para implementarla se deberían integrar en las fases iniciales de los proyectos del sistema de información. Los controles introducidos en la etapa de diseño son significativamente más baratos de implementar y mantener que aquellos incluidos durante o después de la implementación.

Si se adquieren productos, se debería seguir un proceso formal de adquisición y prueba. Los contratos con el proveedor deberían abordar los requisitos de seguridad identificados. Cuando la funcionalidad de la seguridad de un producto determinado no satisface el requisito específico, entonces es conveniente considerar los controles de los riesgos, introducidos y asociados, antes de adquirir el producto.

1.3.8.2 Procesamiento Correcto en las Aplicaciones

Se debería diseñar controles apropiados en las aplicaciones, incluyendo las aplicaciones desarrolladas por el usuario para garantizar el procesamiento correcto. Estos controles deberían incluir la validación de los datos de entrada y de salida del procesamiento interno.

1.3.8.2.1 Validación de los Datos de Entrada

Se deberían validar los datos de entrada a las aplicaciones para asegurar que dichos datos son correctos y apropiados. Es recomendable realizar verificaciones de las entradas de las transacciones del negocio, de los datos permanentes (nombre y direcciones, limites de crédito, números de referencia del cliente) y de

las tablas de parámetros (precios de venta, tasas de conversión de divisas, tasas de impuestos). Se recomienda tomar en consideración:

a) Verificaciones de entradas de datos para determinar (valores fuera de rango, caracteres no validos, datos incompletos, datos inconsistentes).
b) revisión periódica del contenido de los campos clave o de los archivos de datos para confirmar su validez e integridad.
c) Inspección de los documentos de entrada impresos para determinar cambios no autorizados (todos los cambios en los datos de entrada deben estar autorizados).
d) Procedimientos de respuesta ante errores de validación.
e) Procedimientos para probar la credibilidad de los datos de entrada.
f) Definición de responsabilidades para todo el personal que participa en el proceso de entrada de datos.
g) Creación de un registro de las actividades implicadas en el proceso de entrada de datos.

1.3.8.2.2 Control de Procesamiento Interno

Se deberían incorporar verificaciones de validación en las aplicaciones para detectar cualquier corrupción de la información. El diseño y la implementación de las aplicaciones deberían garantizar que se minimizan los riesgos de falla en el procesamiento, los cuales originan pérdida de la integridad. Las áreas específicas que se han de considerar incluyen:

a) Utilización de las funciones agregar, modificar y borrar para implementar los cambios en los datos.
b) Procedimientos para evitar que los programas se ejecuten en orden erróneo o su ejecución después de falla previa del procesamiento.
c) Utilización de programas adecuados para la recuperación después de fallas con el fin de garantizar el procesamiento correcto de los datos.
d) Protección contra ataques empleando desbordamiento/exceso en el búfer.

1.3.8.2.3 Integridad del Mensaje

Se deberían identificar los requisitos para asegurar la autenticidad y proteger la integridad del mensaje en las aplicaciones, así como identificar e implementar los controles adecuados. Se debería realizar una evaluación de los riesgos de seguridad para determinar si se requiere integridad del mensaje y para identificar el método más apropiado de implementación.

1.3.8.2.4 Validación de los Datos de Salida

Se deberían validar los datos de salida de una aplicación para asegurar que el procesamiento de la información almacenada es correcto y adecuado a las circunstancias. La validación de los datos de salida puede incluir:

a) Verificaciones de la credibilidad para probar si los datos de salida son razonables.
b) Asegurar el procesamiento de todos los datos.
c) Suministro de información suficiente para que un lector o un sistema de procesamiento posterior determine la exactitud, precisión y clasificación de la información.
d) Procedimientos para responder las pruebas de validación de salidas.
e) Definición de las responsabilidades del personal que participa en el proceso de la salida de datos.
f) Creación de un registro de las actividades del proceso de validación de la salida de datos.

1.3.8.3 Controles Criptográficos

Proteger la confidencialidad, autenticidad o integridad de la información, por medios criptográficos. Se debería desarrollar una política sobre el uso de los controles criptográficos y establecer una gestión de claves para dar soporte al empleo de técnicas criptográficas.

1.3.8.3.1 Política sobre el Uso se Controles Criptográficos

Se debería implementar una política sobre el uso de controles criptográficos para la protección de la información. Se recomienda tomar en consideración los siguientes aspectos al desarrollar una política criptográfica:

a) El enfoque de la dirección para el uso de controles criptográficos en la organización, incluyendo los principios generales bajo los cuales se debería proteger la información del negocio.
b) La evaluación de riesgos deberían ayudar a identificar el nivel requerido de protección teniendo en cuenta tipo, fortaleza y calidad del algoritmo de encriptación requerido.
c) Uso de encriptación para la protección de la información transportada por medios móviles o removibles, por dispositivos o a través de líneas de comunicación.
d) Enfoque para la gestión de claves que incluya métodos para la protección de las claves criptográficas y la recuperación de información encriptada en caso de pérdida, amenaza o daño de las claves.
e) Funciones y responsabilidades, es decir, quien es encargado de la implementación de la política y de la gestión de claves.
f) Normas a adoptar para la implementación eficaz en toda la organización (qué solución se usa para cuáles procesos del negocio).
g) Impacto de la utilización de información encriptada sobre los controles que dependen de la inspección del contenido (por ejemplo, detección de virus).

Los controles criptográficos se utilizan para lograr diferentes objetivos de seguridad:

a) Confidencialidad.- Uso de encriptación de la información para proteger información sensible o crítica, bien sea almacenada o transmitida.
b) Integridad/autenticidad.- Uso de firmas digitales o códigos de autenticación de mensajes para proteger la autenticidad e integridad de información sensible o crítica transmitida o almacenada.

c) No repudio.- Uso de técnicas criptográficas para obtener prueba de la ocurrencia o no ocurrencia de un evento o acción.

Cuando se utilizan firmas digitales, se recomienda considerar toda la legislación pertinente, en particular la legislación que describe las condiciones bajo las cuales la firma digital es legalmente obligatoria (véase el numeral 15.1).

1.3.8.3.2 Gestión de Claves

Se debería establecer la gestión de claves para apoyar el uso de técnicas criptográficas en la organización. Todas las claves criptográficas deberían tener protección contra modificación, pérdida o destrucción.
El equipo usado para generar, almacenar y archivar las claves debería estar protegido por medios físicos. Un sistema de gestión de claves se debería basar en un conjunto acordado de normas, procedimientos y método seguros para:

a) Generar claves para diferentes sistemas criptográficos y diferentes aplicaciones.
b) Generar y obtener certificados de claves públicas.
c) Distribuir claves a los usuarios previstos, incluyendo la forma de activar y recibir las claves.
d) Almacenar las claves, incluyendo la forma en que los usuarios autorizados tendrán acceso a ellas.
e) Cambiar o actualizar las claves incluyendo reglas sobre cuándo cambiarlas y cómo hacerlo.
f) Tratar las claves perdidas.
g) Revocar las claves, incluyendo la forma de retirarlas o desactivarlas, por ejemplo cuando las claves se han puesto en peligro o cuando un usuario se retira de la organización (en cuyo caso las claves también se deberían archivar).
h) Recuperar las claves perdidas o corruptas como parte de la gestión de continuidad del negocio; por ejemplo, para la recuperación de información encriptada.

i) Archivar claves, por ejemplo para la información archivada o con copia de respaldo.
j) Destrucción de claves.
k) Registro y auditoría de las actividades relacionadas con la gestión de claves.

1.3.8.4 Seguridad de los Archivos del Sistema

Los accesos a los archivos del sistema y al código fuente del programa deberían estar protegidos, y los proyectos de tecnología de la información y las actividades de soporte se deberían efectuar de forma segura.

1.3.8.4.1 Control del Software Operativo

Se deberían establecer procedimientos para controlar la instalación de software en los sistemas operativos. Para minimizar los riesgos de corrupción de los sistemas operativos, se deberían tener en cuenta las siguientes directrices para controlar los cambios:

a) La actualización del software operativo, las librerías y los programas sólo deberían ser realizadas por administradores capacitados y con la debida autorización de la dirección.
b) Los sistemas operativos únicamente deberían contener códigos ejecutables aprobados y no códigos en desarrollo ni compiladores (a menos que exista excepciones autorizadas por la dirección).
c) El software de las aplicaciones y del sistema operativo sólo se deberían implementar después del ensayo exhaustivo y exitoso; los ensayos deberían incluir pruebas sobre capacidad de uso, seguridad, efectos en otros sistemas y facilidad para el usuario, se debería garantizar que todas las librerías fuente del programa correspondiente estén actualizadas.

d) Se debería usar un sistema de control de configuración para mantener el control del software implementado, así como de la documentación del sistema.
e) Es conveniente instaurar una política de estrategia de restauración al estado anterior antes de implementar los cambios.
f) Se debería conservar un registro para auditoría de todas las actualizaciones de las librerías de los programas operativos.
g) Es conveniente conservar las versiones anteriores del software de aplicación como medida de contingencia.
h) Las versiones antiguas del software se deberían archivar junto con toda la información requerida y los parámetros, procedimientos, detalles de configuración y software de soporte, en la medida en que los datos se retengan en archivo.

Los parches de software se deberían aplicar cuando pueden ayudar a eliminar o reducir las debilidades de la seguridad.

1.3.8.4.2 Protección de los Datos de Prueba del Sistema

Se debería evitar el uso de bases de datos operativos que contiene información sensible con propósitos de prueba. Si se utiliza información sensible para propósitos de prueba, todos los detalles y el contenido sensible se deberían retirar o modificar antes del uso. Se recomienda seguir las siguientes directrices para proteger los datos operativos cuando se emplean con propósitos de prueba:

a) Los procedimientos de control del acceso que se aplican a los sistemas de aplicación operativos también se deberían aplicar a los sistemas de aplicación de pruebas.
b) Debería existir autorización separada cada vez que se copie la información operativa en un sistema de aplicación de prueba.
c) La información operativa se debería borrar del sistema de aplicación de prueba inmediatamente después de terminar la prueba.

d) El copiado y la utilización de la información operativa se debería registrar para brindar un rastro para auditoría.

1.3.8.4.3 Control de Acceso al Código Fuente de los Programas

El acceso al código fuente de programas y a los elementos asociados (como diseños, especificaciones, planes de verificación y planes de validación) se debería controlar para evitar la introducción de funcionalidad no autorizada y evitar los cambios involuntarios. Para el código fuente de programas esto se puede lograr con el almacenamiento central controlado de dicho código, preferiblemente en las librerías fuente de programas. Las siguientes directrices se deberían considerar para controlar el acceso a tales librerías fuente de programas:

a) Cuando sea posible, las librerías fuente de programas no se deberían mantener en los sistemas operativos.
b) El código fuente de programas y las librerías fuente de programas se deberían gestionar de acuerdo con los procedimientos establecidos.
c) El personal de soporte debería tener acceso restringido a las librerías fuente de programas.
d) La actualización de las librerías fuente de programas y de los elementos asociados, así como la emisión de fuentes de programa a los programadores, solamente se debería efectuar después de recibir la autorización apropiada.
e) Los listados de programas se deberían mantener en un entorno seguro.
f) Se debería conservar un registro para auditoría de todos los accesos a las librerías fuente de programas.
g) El mantenimiento y el copiado de las librerías fuente de programas deberían estar sujetos a un procedimiento estricto de control de cambios.

1.3.8.5 Seguridad en los Procesos de Desarrollo y Soporte

Los entornos de soporte y de desarrollo deberían estar estrictamente controlados. Los directores responsables de los sistemas de aplicación también deberían garantizar que todos los cambios propuestos en el sistema se revisan para comprobar que no ponen en peligro la seguridad del sistema ni del entorno operativo.

1.3.8.5.1 Procedimientos de Control de Cambios

Se debería controlar la implementación de cambios utilizando procedimientos formales de control de cambios. Los procedimientos se deberían documentar y hacer cumplir. La introducción de sistemas nuevos y de cambios importantes en los sistemas existentes debería seguir un proceso formal de documentación, especificación, prueba, control de calidad e implementación con gestión. Los procedimientos de control de cambios operativos y de aplicación se deberían integrar. Los procedimientos de control de cambios deberían incluir:

a) El mantenimiento de un registro de los niveles acordados de autorización.
b) La garantía de que los cambios son realizados por los usuarios autorizados.
c) La revisión de los controles y de procedimientos de integridad para asegurar que no se pondrán en peligro debido a los cambios.
d) La identificación de todo el software, la información, las entidades de bases de datos y del hardware que requieran mejora.
e) La obtención de la aprobación formal de las propuestas detalladas antes de iniciar el trabajo.
f) La garantía de que los usuarios autorizados aceptan los cambios antes de las implementaciones.
g) La garantía de que la documentación del sistema está actualizada al finalizar cada cambio y que la documentación antigua se archiva o elimina.
h) El mantenimiento de una versión de control para todas las actualizaciones de software.

i) El mantenimiento de un rastro para auditoría de todos los cambios solicitados.
j) La garantía de que la documentación operativa y los procedimientos de usuario se cambian en función de la necesidad con el objeto de mantener su idoneidad.
k) La garantía de que la implementación de los cambios tiene lugar en el momento oportuno y no perturba los procesos del negocio involucrados.

1.3.8.5.2 Revisión Técnica de las Aplicaciones después de los Cambios en el Sistema Operativo

Cuando se cambian los sistemas operativos, las aplicaciones críticas para el negocio se deberían revisar y someter a prueba para asegurar que no hay un mal impacto en las operaciones ni en la seguridad de la organización. Este proceso debería comprender los siguientes aspectos:

a) Revisión de los procedimientos de integridad y control de la aplicación para asegurarse de que no se han puesto en peligro debido a los cambios en el sistema operativo.
b) Garantía de que el plan y el presupuesto de soporte anual cubrirán las revisiones y pruebas del sistema que resulten de cambios en el sistema operativo.
c) Garantía de la notificación oportuna sobre los cambios en el sistema operativo para permitir la realización de las pruebas y las revisiones apropiadas antes de la implementación.
d) Garantía de que se hacen cambios en los planes de continuidad del negocio.

1.3.8.5.3 Restricciones en los Cambios a los Paquetes de Software

Se debería minimizar y controlar la realización de modificaciones a los paquetes de software, limitarlas a cambios necesarios. Los paquetes de software suministrados por el vendedor se deberían usar sin modificaciones. Cuando sea

necesario modificar un paquete de software, se deberían tener en cuenta los siguientes puntos:

a) El riesgo de que los procesos de integridad y de control incorporados se vean comprometidos.
b) Si es necesario obtener el consentimiento del vendedor.
c) La posibilidad de obtener los cambios requeridos del vendedor como un programa estándar de actualizaciones.
d) El impacto, si la organización se hace responsable del mantenimiento futuro del software como resultado de los cambios.

1.3.8.5.4 Fuga de Información

Se deberían evitar las oportunidades para que se produzca fuga de información, por ello se debería considerar los siguientes aspectos:

a) Exploración de los medios y comunicaciones de salida para determinar la información oculta.
b) Comportamiento de las comunicaciones y del sistema de modulación y enmascaramiento para reducir la probabilidad de que una tercera parte pueda deducir información a partir de tal comportamiento.
c) Utilización de sistemas y software que se consideran con alta integridad (productos evaluados).
d) Monitoreo regular de las actividades del personal y del sistema, cuando está permitido por la legislación o los reglamentos existentes.
e) Monitoreo del uso de los recursos en los sistemas de computador.

1.3.8.5.5 Desarrollo de Software Contratado Externamente

La organización debería supervisar y monitorear el desarrollo de software contratado externamente, se recomienda tener en cuenta lo siguiente:

a) Acuerdos sobre licencias, propiedad de los códigos y derechos de propiedad intelectual.
b) Certificación de la calidad y exactitud del trabajo realizado.
c) Convenios de fideicomiso en caso de falla de la tercera parte.
d) Derechos de acceso para auditar la calidad y exactitud del trabajo realizado.
e) Requisitos contractuales para la calidad y la funcionalidad de la seguridad del código.
f) Realización de pruebas antes de la instalación para detectar códigos troyanos o maliciosos.

1.3.8.6 Gestión de la Vulnerabilidad Técnica

La gestión de la vulnerabilidad técnica se debería implementar de forma eficaz, sistemática y repetible con toma de mediciones para confirmar su eficacia. Estas consideraciones deberían incluir a los sistemas operativos y otras aplicaciones en uso.

1.3.8.6.1 Control de las Vulnerabilidades Técnicas

Se debería obtener información sobre las vulnerabilidades técnicas de los sistemas de información que están en uso, determinar cuan expuesta está la empresa a estas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos. Se recomienda tener en cuenta las siguientes directrices:

a) Se debería definir e instaurar las funciones y responsabilidades asociadas con la gestión de la vulnerabilidad técnica.
b) Es conveniente identificar los recursos de información que se van a utilizar para identificar las vulnerabilidades técnicas.
c) Se debería definir una línea de tiempo para reaccionar ante la notificación de vulnerabilidades técnicas potenciales.

d) Una vez identificada una vulnerabilidad potencial, la organización debería identificar los riesgos asociados y las acciones que se han de tomar.
e) Dependiendo de la urgencia con la que es necesario tratar la vulnerabilidad técnica, la acción a tomar se debería ejecutar de acuerdo con los controles relacionados con la gestión de cambios o siguiendo los procedimientos de respuesta ante incidentes de Seguridad de la Información.
f) Si está disponible un parche, se deberían evaluar los riesgos asociados con su instalación (riesgos impuestos por la vulnerabilidad versus los riesgos de instalar el parche).
g) Es conveniente probar y evaluar los parches antes de su instalación para garantizar que son eficaces y no producen efectos secundarios intolerables.
h) Se debería conservar un registro para auditoría de todos los procedimientos efectuados.
i) El proceso de gestión de la vulnerabilidad técnica se debería monitorear y evaluar a intervalos regulares para garantizar su eficacia y eficiencia.
j) Se deberían tratar primero los sistemas con alto riesgo.

1.3.9 GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN

1.3.9.1 Reporte sobre los Eventos y las Debilidades de la Seguridad de la Información

Es conveniente establecer el reporte formal del evento y los procedimientos de escalada. Se les debería exigir a todos los miembros de una empresa que reporten todos los eventos de Seguridad de la Información y las debilidades tan pronto sea posible al punto de contacto designado.

1.3.9.1.1 Reporte sobre los Eventos de Seguridad de la Información

Todos los empleados, contratistas y usuarios de tercera parte deberían tener conciencia de su responsabilidad para reportar todos los eventos de Seguridad de la Información lo más pronto posible a través de los canales de gestión apropiados y con el procedimiento definido. Los procedimientos de reporte deberían incluir los siguientes aspectos:

a) Procesos adecuados de retroalimentación para garantizar que aquellos que reportan los eventos de Seguridad de la Información reciben notificación de los resultados después que se ha tratado y solucionado el problema.
b) Formatos para el reporte de los eventos de Seguridad de la Información para soportar la acción de reporte y ayudar a que la persona que hace el reporte recuerde todas las acciones necesarias en caso de un evento de Seguridad de la Información.
c) El comportamiento correcto en caso de un evento de Seguridad de la Información (tomar nota sobre los detalles importantes, reportar inmediatamente).
d) Referencia a un proceso disciplinario formal establecido para tratar a los empleados, contratistas o usuarios de tercera parte que cometieron la violación de seguridad.

En entornos de alto riesgo, se pueden suministrar una alarma de coacción[9] a través de la cual una persona bajo coacción pueda indicar tales problemas.

1.3.9.1.2 Reporte sobre las Debilidades en la Seguridad

Se debería exigir a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información que observen y reporten todas las debilidades observadas o sospechadas en los sistemas o servicios tan pronto como sea posible a su director.

[9] Una alarma de coacción es un método para indicar secretamente que tiene lugar una acción “bajo coacción”.

1.3.9.2 Gestión de los Incidentes y las Mejoras en la Seguridad de la Información

Es conveniente establecer las responsabilidades y los procedimientos para manejar los eventos y debilidades de la Seguridad de la Información de manera eficaz una vez se han reportado. Se debería aplicar un proceso de mejora continua a la respuesta de monitorear, evaluar y gestionar en su totalidad estos incidentes de Seguridad de la Información.

1.3.9.2.1 Responsabilidades y Procedimientos

Se deberían establecer las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de Seguridad de la Información. Se recomienda tener en cuenta las siguientes directrices para los procedimientos de gestión de incidentes:

a) Es conveniente instaurar procedimientos para manejar los diferentes tipos de incidentes de Seguridad de la Información.
b) Además de los planes normales de contingencia, los procedimientos también deberían comprender análisis e identificación de la causa, contención, planificación e implementación, comunicación con afectados, reporte de la acción a la autoridad.
c) Se deberían recolectar y asegurar los rastros para auditoría y la evidencia similar para el análisis de los problemas internos, uso de evidencia forense, negociación para la compensación de proveedores y servicios.
d) La acción para la recuperación de las violaciones de la seguridad y la corrección de las fallas del sistema debería estar cuidadosa y formalmente controlada.

Los objetivos de la gestión de los incidentes de Seguridad de la Información se deberían acordar con la dirección y se debería garantizar que los responsables de esta gestión comprenden las prioridades de la organización para el manejo de los incidentes de Seguridad de la Información.

1.3.9.2.2 Aprendizaje Debido a los Incidentes de Seguridad de la Información

Deberían existir mecanismos que permitan cuantificar y monitorear todos los tipos, volúmenes y costos de los incidentes de Seguridad de la Información. La Información obtenida de la evaluación de los incidentes de seguridad, se debería utilizar para identificar los incidentes recurrentes o de alto impacto.

1.3.9.2.3 Recolección de Evidencias

Cuando una acción de seguimiento contra una persona u organización después de un incidente de Seguridad de la Información implica acciones legales, la evidencia se debe recolectar, retener y presentar para cumplir con las reglas para la evidencia establecidas en la jurisdicción pertinente.

En general, las reglas para la evidencia comprenden los siguientes aspectos:

a) Admisibilidad de la evidencia: si la evidencia se puede utilizar o no en la corte;
b) Peso de la evidencia: la calidad y cabalidad de la evidencia

Para lograr la admisibilidad de la evidencia, la organización debería asegurar que sus sistemas de información cumplen cualquier norma o código de práctica publicado para la producción de evidencia admisible.

Todo el trabajo forense se debería llevar a cabo únicamente en copias del material de evidencia. Se debería proteger la integridad de todo el material de evidencia. El proceso de copia del material de evidencia debería estar supervisado por personal de confianza y se debería registrar la información sobre cuándo y cómo se realizó dicho proceso, quién ejecutó las actividades de copiado y qué herramientas o programas se utilizaron.

1.3.10 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

1.3.10.1 Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio

Se debería implementar un proceso de gestión de la continuidad del negocio para minimizar el impacto y la pérdida de activos de información en la organización. En este proceso es conveniente identificar los procesos críticos para el negocio e integrar los requisitos de la gestión de la Seguridad de la Información de la continuidad del negocio con otros requisitos de continuidad relacionados con aspectos tales como operaciones, personal, materiales, transporte e instalaciones.

1.3.10.1.1 Inclusión de la Seguridad de la Información en el Proceso de gestión de la Continuidad del Negocio

Se debería desarrollar y mantener un proceso de gestión para la continuidad del negocio en toda la organización el cual trae los requisitos de Seguridad de la Información necesarios para la continuidad del negocio dentro de la organización. El proceso debería reunir los siguientes elementos para la gestión de la continuidad del negocio:

a) Comprensión de los riesgos que enfrenta la organización en términos de la probabilidad y el impacto en el tiempo, incluyendo la identificación y la determinación de la prioridad de los procesos críticos del negocio.
b) Identificación de todos los activos involucrados en los procesos críticos del negocio.
c) Comprensión del impacto que pueden tener las interrupciones causadas por incidentes de Seguridad de la Información, y establecer los objetivos del negocio para los servicios de procesamiento de información.
d) Consideración para adquirir pólizas de seguros adecuadas que puedan formar parte de todo el proceso de continuidad del negocio.

e) Identificación y consideración de la implementación de controles preventivos y mitigantes adicionales.
f) Identificación de recursos financieros, organizacionales, técnicos y ambientales suficientes para tratar los requisitos identificados de la Seguridad de la Información.
g) Garantizar la seguridad del personal y la protección de los servicios de procesamiento de información y de la propiedad de la organización.
h) Formulación y documentación de los planes de continuidad del negocio que abordan los requisitos de Seguridad de la Información acorde con la estrategia acordada de continuidad del negocio.
i) Prueba y actualización regular de los planes y procesos establecidos.
j) Garantizar que la gestión de la continuidad del negocio está incorporada en los procesos y la estructura de la organización; la responsabilidad por el proceso de gestión de la continuidad del negocio se debería asignar en un nivel apropiado en la organización.

1.3.10.1.2 Continuidad del Negocio y Evaluación de los Riesgos

Se deberían identificar los eventos que pueden ocasionar interrupciones en los procesos del negocio junto con la probabilidad y el impacto de dichas interrupciones, así como sus consecuencias para la Seguridad de la Información.

Los aspectos de Seguridad de la Información en la continuidad del negocio se deberían basar en la identificación de los eventos que pueden causar interrupciones en los procesos del negocio de la organización. Se debería continuar con una evaluación de riesgos para determinar la probabilidad y el impacto de tales interrupciones, en términos de tiempo, escala de daño y periodo de recuperación.

Las evaluaciones de riesgos para la continuidad del negocio se deberían efectuar con la plena participación de los dueños de los recursos y los procesos del negocio. Estas evaluaciones deberían considerar todos los procesos del negocio para identificar, cuantificar y priorizar los riesgos frente a los criterios y los

objetivos pertinentes para la organización, incluyendo los recursos críticos, impactos de las interrupciones, duración permitida de corte y prioridades de recuperación.

Dependiendo de los resultados, se debería desarrollar una estrategia de continuidad del negocio para determinar el enfoque para la continuidad del negocio. Una vez que se ha creado esta estrategia, la dirección debería aprobarla y respaldar el plan para su implementación.

1.3.10.1.3 Desarrollo e Implementación de Planes de Continuidad que Incluyan la Seguridad de la Información

Se deberían desarrollar e implementar planes para mantener o recuperar las operaciones y asegurar la disponibilidad de la información en el grado y la escala de tiempo requerido, después de la interrupción o la falla de los procesos críticos para el negocio. En el proceso de planificación de la continuidad del negocio se deberían considerar los siguientes aspectos:

a) Identificar y acordar todas las responsabilidades y los procedimientos para la continuidad del negocio.
b) Identificar la pérdida aceptable de información y servicios.
c) Implementar los procedimientos que permitan recuperar y restaurar las operaciones del negocio y la disponibilidad de la información en las escalas de tiempo requeridas.
d) Procedimientos operativos que se han de seguir en espera de la terminación de la recuperación y restauración.
e) Documentación de procedimientos y procesos acordados.
f) Formación apropiada del personal en los procedimientos y procesos acordados, incluyendo el manejo de las crisis.
g) Pruebas y actualización de los planes:

1.3.10.1.4 Estructura para la Planificación de la Continuidad del Negocio

Se debería mantener una sola estructura de los planes de continuidad del negocio, para asegurar que todos los planes son consistentes, y considerar los requisitos de la Seguridad de la Información así como identificar las prioridades para pruebas y mantenimiento.

Cada plan de continuidad del negocio debería describir el enfoque para la continuidad, por ejemplo el enfoque para garantizar la disponibilidad y Seguridad de la Información o del sistema de información. Igualmente, cada plan debería especificar el plan de escalada y las condiciones para su activación, así como las personas responsables de ejecutar cada componente del plan. Una estructura para la planificación de la continuidad del negocio debería considerar los siguientes aspectos:

a) Las condiciones para la activación de los planes que describen el proceso a seguir antes de activar cada plan.
b) Los procedimientos de emergencia que describen las acciones por realizar tras un incidente que ponga en peligro las operaciones del negocio.
c) Los procedimientos de respaldo que describen las acciones por realizar para desplazar las actividades esenciales del negocio a lugares temporales alternos y para devolver la operatividad de los procesos del negocio en los plazos requeridos.
d) Los procedimientos operativos temporales por seguir mientras se terminan la recuperación y la restauración.
e) Los procedimientos de reanudación que describen las acciones por realizar para que las operaciones del negocio vuelvan a la normalidad.
f) Una programación de mantenimiento que especifique cómo y cuándo se realizarán pruebas al plan y el proceso para el mantenimiento del plan.
g) Actividades de concientización, educación y formación diseñadas para comprender los procesos de continuidad del negocio y garantizar que los procesos siguen siendo eficaces.

h) Las responsabilidades de las personas, que describan quién es responsable de la ejecución de cada componente del plan. Si se requiere, se deberían nombrar suplentes.
i) Los activos y recursos críticos necesarios para ejecutar los procedimientos de emergencia, respaldo y reanudación.

1.3.10.1.5 Pruebas, Mantenimiento y Reevaluación de los Planes de Continuidad del Negocio

Las pruebas del plan de continuidad del negocio deberían asegurar que todos los miembros del equipo de recuperación son conscientes de los planes y sus responsabilidades para la continuidad del negocio y la Seguridad de la Información.

La programación de las pruebas para los planes de continuidad del negocio debería indicar cómo y cuándo se va a probar cada elemento del plan. Es conveniente utilizar una variedad de técnicas para garantizar que los planes funcionarán en condiciones reales. Estas incluirían:

a) La prueba sobre papel de varios escenarios.
b) Las simulaciones.
c) Las pruebas de recuperación técnica.
d) Las pruebas de recuperación en un lugar alterno.
e) Las pruebas de los recursos y servicios del proveedor.
f) Los ensayos completos.

Cualquier organización puede utilizar estas técnicas. Estas se deberían aplicar de forma pertinente para el plan específico de recuperación.

1.3.11 CUMPLIMIENTO

1.3.11.1 Cumplimiento de los Requisitos Legales

El diseño, el uso, la operación y la gestión de los sistemas de información pueden estar sujetos a requisitos de seguridad estatutarios, reglamentarios y contractuales. Se debería buscar asesoría sobre estos requisitos.

1.3.11.1.1 Identificación de la Legislación Aplicable

Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, así como el enfoque de la organización para cumplir estos requisitos se deberían definir explícitamente, documentar y mantener para desarrollar controles que cubran estas zonas.

1.3.11.1.2 Derechos de Propiedad Intelectual (DPI)

Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material con respecto al cual pueden existir derechos de propiedad intelectual. Se deberían tomar en consideración las siguientes directrices:

a) Publicar una política de cumplimiento de los derechos de propiedad intelectual que defina el uso legal del software y de los productos de información.
b) Adquirir software únicamente a través de fuentes conocidas y de confianza para garantizar que no se violan los derechos de copia.
c) Mantener la concientización sobre las políticas para proteger los derechos de propiedad intelectual y notificar la intención de tomar acciones disciplinarias para el personal que los viole.
d) Mantener registros apropiados de los activos e identificar todos los activos con requisitos para proteger los derechos de propiedad intelectual.

e) Mantener prueba y evidencia sobre la propiedad de licencias, discos maestros, manuales, entre otros.
f) Implementar controles para asegurar que no se exceda el número máximo de usuarios permitidos.
g) Verificar que únicamente se instalan software autorizado y productos con licencia.
h) Suministrar una política para mantener las condiciones de licencia apropiadas.
i) Suministrar una política para la disposición o transferencia de software a otros.
j) Usar herramientas de auditoría adecuadas.
k) Cumplir los términos y condiciones para el software y la información obtenida de redes públicas.
l) No duplicar, convertir en otro formato no extraer grabaciones comerciales diferentes a los permitidos por la ley de derechos de copia.
m) No copiar total ni parcialmente libros, artículos, informes ni otros documentos diferentes a los permitidos por la ley de derechos de copia.

1.3.11.1.3 Protección de los Registros de la Organización

Los registros importantes se deberían proteger contra pérdida, destrucción y falsificación, de acuerdo con los requisitos estatutarios, reglamentarios, contractuales y del negocio. Se deberían clasificar en tipos de registro, cada uno con detalles de los periodos de retención y los tipos de medio de almacenamiento. Los sistemas de almacenamiento de datos se deberían seleccionar de forma tal que los datos requeridos se puedan recuperar en el periodo de tiempo y el formato aceptable, dependiendo de los requisitos que se deben cumplir.

Para cumplir estos objetivos de salvaguarda de registros, la organización debería seguir los siguientes aspectos:

a) Se deberían publicar directrices sobre retención, almacenamiento, manipulación y eliminación de registros e información.

b) Es conveniente publicar una programación de retención que identifique los registros y el periodo de tiempo de su retención.
c) Se recomienda conservar un inventario de las fuentes de información clave.
d) Se deberían implementar los controles apropiados para proteger los registros y la información contra pérdida, destrucción y falsificación.

1.3.11.1.4 Protección de los Datos y Privacidad de la Información Personal

Se debería desarrollar e implementar una política de protección y privacidad de los datos. Esta política se debería comunicar a todas las personas involucradas en el procesamiento de información personal. Con frecuencia esto se logra mejor nombrando a una persona responsable.

1.3.11.1.5 Prevención del Uso Inadecuado de los Servicios de Procesamiento de Información

Se debería disuadir a los usuarios de utilizar los servicios de procesamiento de información para propósitos no autorizados. Todo uso de estos servicios para propósitos no relacionados con el negocio sin autorización de la dirección, o para cualquier propósito no autorizado se debería considerar uso inadecuado de los servicios.

Todos los usuarios deberían conocer el alcance preciso de su acceso permitido y del monitoreo implementado para detectar el uso no autorizado. Esto se puede lograr dando a los usuarios autorización escrita, una copia de la cual debería estar firmada por el usuario y la organización debería conservarla.

1.3.11.1.6 Reglamentación de los Controles Criptográficos

Se deberían utilizar controles criptográficos que cumplan todos los acuerdos, las leyes y los reglamentos pertinentes. Se recomienda tener presentes los siguientes elementos:

a) Restricción de importaciones y/o exportaciones de hardware y software de computadores para la ejecución de funciones criptográficas.
b) Restricción de importaciones y/o exportaciones de hardware y software de computadores diseñados para adicionarles funciones criptográficas.
c) Restricciones al uso de encriptación.
d) métodos obligatorios o discrecionales de acceso por parte de las autoridades del país a la información encriptada mediante hardware o software para brindar confidencialidad al contenido.

1.3.11.2 Cumplimiento de las políticas y las Normas de Seguridad y Cumplimiento Técnico

La seguridad de los sistemas de información se debería revisar a intervalos regulares y llevar a cabo frente a las políticas de seguridad apropiadas, también se deberían auditar las plataformas técnicas y los sistemas de información para determinar el cumplimiento de las normas aplicables sobre implementación de la seguridad y los controles de seguridad documentados.

1.3.11.2.1 Cumplimiento con las Políticas y las Normas de Seguridad

Los directores deberían garantizar que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se llevan a cabo correctamente para lograr el cumplimiento con las políticas y las normas de seguridad.

1.3.11.2.2 Verificación del Cumplimiento Técnico

Los sistemas de información se deberían verificar periódicamente para determinar el cumplimiento con las normas de implementación de la seguridad, la verificación del cumplimiento técnico se puede hacer manualmente por un ingeniero de sistemas con experiencia y/o con la ayuda de herramientas automáticas que generan un informe técnico para la interpretación posterior por parte del especialista técnico.

1.3.11.3 Consideraciones de la Auditoría de los Sistemas de Información

Deberían existir controles para salvaguardar los sistemas operativos y las herramientas de auditoría durante las auditorías de los sistemas de información.

1.3.11.3.1 Controles de Auditoría de los Sistemas de Información

Los requisitos y las actividades de auditoría que implican verificaciones de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar el riesgo de interrupciones de los procesos de negocio. Se debería tener presente las siguientes directrices:

a) Los requisitos de auditoría se deberían acordar con la dirección correspondiente.
b) Se deberían acordar y controlar el alcance de las verificaciones.
c) Las verificaciones se deberían limitar al acceso de solo lectura del software y los datos.
d) El acceso diferente al de solo lectura únicamente se debería permitir para copias aisladas de archivos del sistema que se puedan borrar al terminar la auditoría.
e) Los recursos para llevar a cabo las verificaciones se deberían identificar explícitamente y estar disponibles.
f) Se deberían identificar y acordar los requisitos para el procesamiento especial o adicional.
g) Todo acceso se debería monitorear y registrar para crear un rastro para referencia; el uso de rastros de referencia de tiempo se debería considerar para datos o sistemas críticos.
h) Se recomienda documentar todos los procedimientos, requisitos y responsabilidades.
i) La persona que realiza la auditoría debería ser independiente de las actividades auditadas.

1.3.11.3.2 Protección de las Herramientas de Auditoría de los Sistemas de Información

Se debería proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar su uso inadecuado o ponerlas en peligro.

CAPÍTULO II

ANÁLISIS DE LA NORMA IS0/IEC 27002

CAPÍTULO II: ANÁLISIS DE LA NORMA ISO/IEC 27002

2.1 INTRODUCCIÓN

Como se ha visto en el Capítulo I, la norma ISO/IEC 27002 está constituida por once dominios:

a. Política de seguridad
b. Organización de la Seguridad de la Información
c. Gestión de activos
d. Seguridad de los Recursos Humanos
e. Seguridad física y del entorno
f. Gestión de operaciones y comunicaciones
g. Control de acceso
h. Adquisición, desarrollo y mantenimiento de sistemas de información
i. Gestión de los incidentes de Seguridad de la Información
j. Gestión de la continuidad del negocio
k. Cumplimientos

El presente trabajo es acerca de *políticas de Seguridad Informática*[10], por este motivo se centra el estudio en los tres dominios que involucran este tema:

a. Política de seguridad
b. Organización de la Seguridad de la Información
c. Gestión de activos

Se debe tener mucho cuidado de no mal interpretar el párrafo anterior ya que en ningún momento se dice que los tres dominios sean los más importantes o que los otros no lo sean, solamente se habla acerca del alcance que tiene un modelo se seguridad de información versus un modelo de Seguridad Informática.

[10] Ver ANEXO 1

El alcance del modelo de políticas de Seguridad de la Información es conocido como Gestión de un Sistema de políticas de Seguridad de Información e involucra a los once dominios de la Norma ISO/IEC 27002; mientras que el alcance del modelo de políticas de Seguridad Informática involucra solamente los tres dominios anteriormente mencionados. Por esto, en el análisis de los tres dominios el término “Seguridad de la Información” de la Norma ISO/IEC 27002 será adaptado para este proyecto como “Seguridad Informática”.

Dentro del análisis de los dominios *Organización de la Seguridad de la Información, Gestión de Operaciones y Comunicaciones, Gestión de la Continuidad del Negocio* se encuentran temas como el Plan de Continuidad del Negocio (PCN) que no será analizado o implementado en el presente trabajo debido al alcance del mismo; sin embargo se describe rápidamente las partes de las que está constituido el PCN para facilitar la comprensión cuando se haga mención al mismo.

2.2 PLAN DE CONTINUIDAD DEL NEGOCIO[11]

Las empresas no solamente son vulnerables a grandes desastres, sino también a pequeños cambios que pueden afectar la continuidad del negocio.

Existen factores como: Incremento en la dependencia tecnológica; las presiones de “velocidad del mercado” que han hecho a las empresas sumamente sensibles a catástrofes o eventos menores que generan perturbación en sus operaciones.

En la última década, los riesgos de desastres naturales, las fallas técnicas de carácter accidental, y las actividades maliciosas han incrementado las posibilidades de interrupciones en las empresas. A pesar de este hecho, muy pocas empresas invierten en planificación de actividades para minimizar posibles desastres.

[11] Plan de Continuidad del Negocio, Estándar Internacional BS 25999-2:2007, Alberto Alexander

Existen ciertos enfoques que son similares al Plan de Continuidad del Negocio y a la vez tienen sus diferencias que se enuncian a continuación:

Plan de Recuperación de Desastres (Disaster Recovery Planning DRP).- Se enfoca en la recuperación de los servicios de TI y los recursos de la empresa, dado un evento que ocasionara una interrupción mayor en su funcionamiento.

Plan de Reanudación del Negocio (Business Resumption Planning BRP).- Se centraliza en la reanudación de los procesos de negocios afectados por una falla en las aplicaciones de TI. Se enfoca en la utilización de procedimientos relacionados con el área de trabajo.

Plan de Continuidad de las Operaciones (Continuity of Operations Planning COOP).- Busca la recuperación de las funciones estratégicas de una organización que se desempeñan en sus instalaciones corporativas.

Plan de Contingencia (Contingency Planning CP).- Se enfoca en la recuperación de los servicios y recursos de TI, después de un desastre de dimensiones mayores o de una interrupción menor. Especifica procedimientos y lineamientos para la recuperación, tanto en áreas de la empresa como en las alternas.

Plan Respuesta de Emergencia (Emergency Response Planning ERP).- Su objetivo es salvaguardar a los empleados, el público, el ambiente y los activos de la empresa. Últimamente se busca de inmediato llevar la situación de crisis a un estado de control.

Se puede decir que todos los enfoques tienen un alcance específico, ninguno cubre todas las áreas críticas, y por eso se requiere un enfoque que involucre a todos, este se llama Plan de Continuidad del Negocio (PCN).

Para establecer un PCN se debe seguir un ciclo de vida para el desarrollo y mantenimiento. En el gráfico 2.1 se ilustra el proceso con sus distintas fases y los entregables.

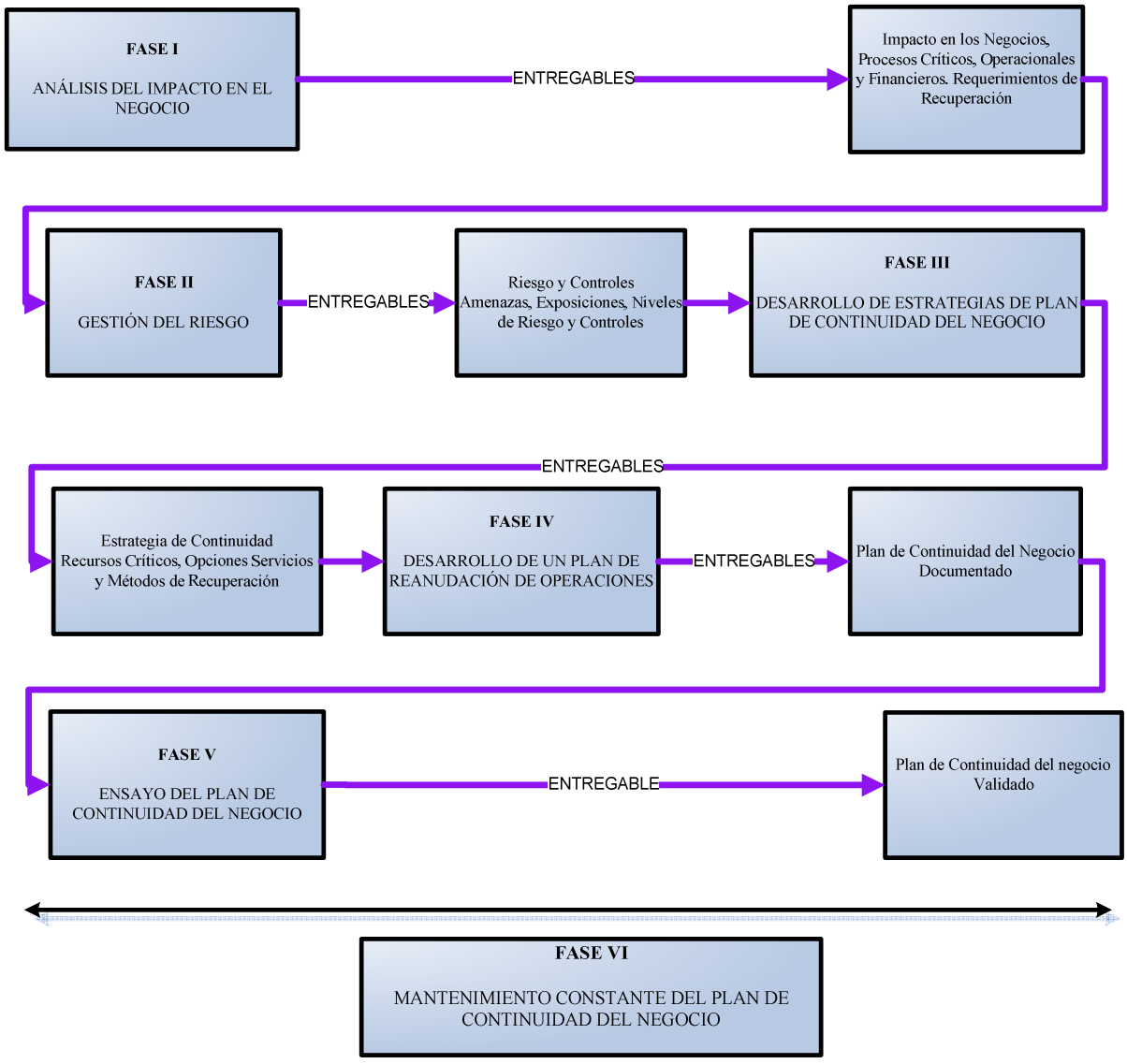


GRÁFICO 2.1 EL PROCESO PCN Y LOS ENTREGABLES

A continuación se realiza una descripción de cada una de las fases.

FASE I ANÁLISIS DEL IMPACTO EN EL NEGOCIO (BUSSINESS IMPACT ANALYSIS BIA)

Esta fase analiza todos los procesos estrechamente relacionados con la misión de la empresa; y la implicación que se tendría en caso de que estos procesos sean interrumpidos.

En esta fase es necesario presentar un informe en el cual se identifican las áreas del negocio que son críticas para el alcance de la misión de la empresa así como el impacto de una interrupción en el desempeño de la empresa.

FASE II GESTIÓN DEL RIESGO

Estas actividades de gestión evalúan las amenazas de un desastre, pormenorizan las vulnerabilidades existentes, los potenciales impactos de un desastre, identifican e implementan los controles necesarios para reducir los riesgos de un desastre, se identifican amenazas para aquellos procesos considerados en el BIA.

En esta fase se debe presentar un informe de riesgos y controles. Este informe identifica las posibles amenazas potenciales de interrupciones del negocio y los riesgos de cada una, además puntualiza las recomendaciones para el control de los riesgos que pueden afectar los procesos esenciales del negocio.

FASE III DESARROLLO DE ESTRATEGIAS DE UN PCN

Se evalúan los requerimientos y se identifican las opciones para la recuperación de procesos críticos y sus recursos si fuesen afectados por un desastre.

Se entrega un informe donde se detalla la identificación de opciones viables para la recuperación de recursos y servicios que pudieron haber sido impactados por una interrupción del negocio. Se aclara que para cada amenaza es necesario elaborar estrategias.

FASE IV DESARROLLO DEL PLAN DE REANUDACIÓN DE OPERACIONES

Esta fase desarrolla un plan para mantener la continuidad del desempeño del negocio, se basa en el Análisis del Impacto en el Negocio (Bussiness Impact Analysis BIA), en la Gestión del riesgo y en el Desarrollo de estrategias de un PCN.

Se debe entregar un informe con procedimientos y lineamientos para la recuperación, restablecimiento de los recursos dañados, y los procesos interrumpidos. Este informe debe contener procedimientos concretos.

FASE V ENSAYO DEL PCN

Se efectúa un ensayo del PCN, para determinar su grado de precisión y actualización.

Se deben entregar los registros para demostrar a terceros la realización de los ensayos, así como las acciones correctivas que la empresa debe efectuar para el Plan de Reanudación de Operaciones.

FASE VI MANTENIMIENTO CONSTANTE DEL PCN

En esta fase se mantiene el PCN en preparación constante para que pueda ejecutarse minimizando las posibilidades de errores.

Se debe entregar los registros y procedimientos que aseguran que el PCN está listo para ejecutarse en caso de presentarse alguna eventualidad.

La vida del PCN comienza en el Análisis del Impacto en el Negocio, seguido de modo secuencial por el denominado Gestión del Riesgo, el desarrollo de la estrategia del PCN, el desarrollo del plan de reanudación de operaciones y el ensayo del PCN.

Los resultados de las fases anteriores conforman la fase para el mantenimiento del PCN.

2.3 ANÁLISIS DOMINIO POLÍTICAS DE SEGURIDAD

Este dominio comprende todas las políticas de Seguridad Informática que pueden aplicarse para salvaguardar información importante en una empresa. Se encuentra conformado por un objetivo de control y dos controles. Como se aprecia en el Gráfico 2.2.

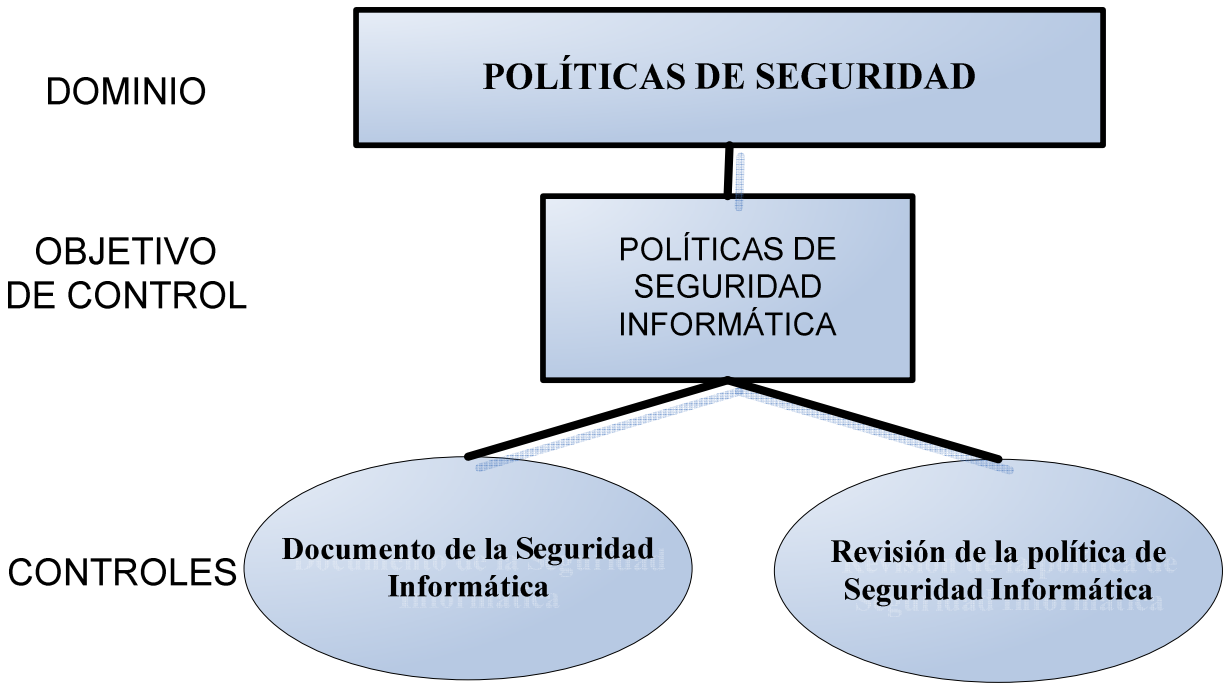


GRÁFICO 2.2 CONSTITUCIÓN DEL DOMINIO "POLÍTICAS DE SEGURIDAD"

2.3.1 OBJETIVO DE CONTROL "ESTABLECER POLÍTICAS DE SEGURIDAD INFORMÁTICA"

El objetivo de control de este dominio ESTABLECER POLÍTICAS DE SEGURIDAD INFORMÁTICA sirve de apoyo y orientación adecuada a la gerencia, de acuerdo a sus requisitos y metas, en especial a las empresas que están iniciando y desean implementar políticas de Seguridad Informática.

Es importante que la dirección se comprometa con todo el proceso de desarrollo e implementación de las políticas, ya que si la dirección no las apoya, entonces será difícil que el resto de la organización lo haga.

2.3.1.1 Primer Control "Documento de la Seguridad Informática"

En el primer control de este dominio es fundamental recalcar que la dirección debe estar en la obligación de aprobar el documento de la política de Seguridad Informática y publicar a sus empleados.

Las pautas que presenta este control para su implementación son de gran utilidad, da un proceso sistemático que es necesario entender y aplicar según sea el caso, es decir, según los objetivos de la organización.

Las guías para implementar este control definen los objetivos de la Seguridad Informática, su alcance e importancia; además, debe contener una estructura para la evaluación y la gestión del riesgo en conjunto con una breve explicación de las normas.

Todas las pautas son importantes, pero se puede decir que la principal es el compromiso que debe establecer la dirección para apoyar las metas, principios y los objetivos del negocio. Si no existiera este apoyo, entonces el proyecto difícilmente saldría adelante.

Las políticas de Seguridad Informática se deben comunicar a todos los empleados de la organización, de tal forma que sea comprensible y para evitar interpretaciones erróneas por parte de los empleados. Los empleados deben aceptar las responsabilidades asignadas así como también respetar los acuerdos de confidencialidad establecidos.

Para mayor comprensión, en el capítulo IV se define cómo desarrollar políticas de Seguridad Informática, cómo evaluarlas y documentarlas en el área de Networking.

2.3.1.2 Segundo Control "Revisión de la Política de Seguridad Informática"

El segundo control involucra obligación por parte de la empresa para revisar la política de Seguridad Informática a períodos regulares o cuando se produzca un cambio significativo.

Cuando se crea el documento de las políticas de Seguridad Informática la organización asigna un coordinador que tenga el respaldo total de la gerencia, corresponde a esta persona mantener y corregir el documento.
Para la revisión de la política de Seguridad Informática se tienen algunos parámetros que son necesarios considerar; sin embargo, los principales y los que se van a considerar para la implementación en Networking son:

Resultados de revisiones independientes.- Que son revisiones realizadas por personas ajenas al área en la cual se está aplicando la política de Seguridad Informática, bien puede ser una persona de otra área o que no pertenezca a la empresa pero que tenga cierta experiencia en esta función. Se puede decir que esta revisión es semejante a una auditoría interna.

Tendencias relacionadas con las amenazas y vulnerabilidades.- Que estaría incluida en el resultado de las revisiones independientes y que corresponde a las amenazas y vulnerabilidades encontradas con la auditoría.

Incidentes reportados.- Que si bien podrían no haber sido registrados en un sistema, se produjeron, se conocen y se deben tener presentes para el documento. Dentro de este punto también se deben incluir los cambios tecnológicos que tengan estrecha relación con la Seguridad Informática.

Con todos estos datos, se evalúa las políticas de Seguridad Informática en el área de Networking para determinar su efectividad y eficiencia.

2.4 ANÁLISIS DOMINIO ORGANIZACIÓN DE LA SEGURIDAD INFORMÁTICA

Con este control se pueden identificar los puntos clave para gestionar la información en la organización.

Este dominio posee dos objetivos de control el primero ADMINISTRAR LA ORGANIZACIÓN INTERNA con ocho controles y el segundo ADMINISTRAR PARTES EXTERNAS con tres controles. En el Gráfico 2.3 se aprecia la constitución de este Dominio.

2.4.1 OBJETIVO DE CONTROL "ADMINISTRAR LA ORGANIZACIÓN INTERNA"

El primer objetivo de control ADMINISTRAR LA ORGANIZACIÓN INTERNA sirve para gestionar la Seguridad Informática dentro de la organización. Se manifiesta nuevamente el compromiso que debería tener la gerencia para aprobar la política de seguridad.

Los coordinadores de cada área deberían se encargados de cumplir su función en conjunto con todas las personas que pertenecen a sus áreas, cuando se desconoce sobre la Seguridad Informática o no se tiene experiencia al respecto, se debería establecer una fuente de asesoría que esté a disposición de la organización para resolver las dudas e inconvenientes que se presentaran.

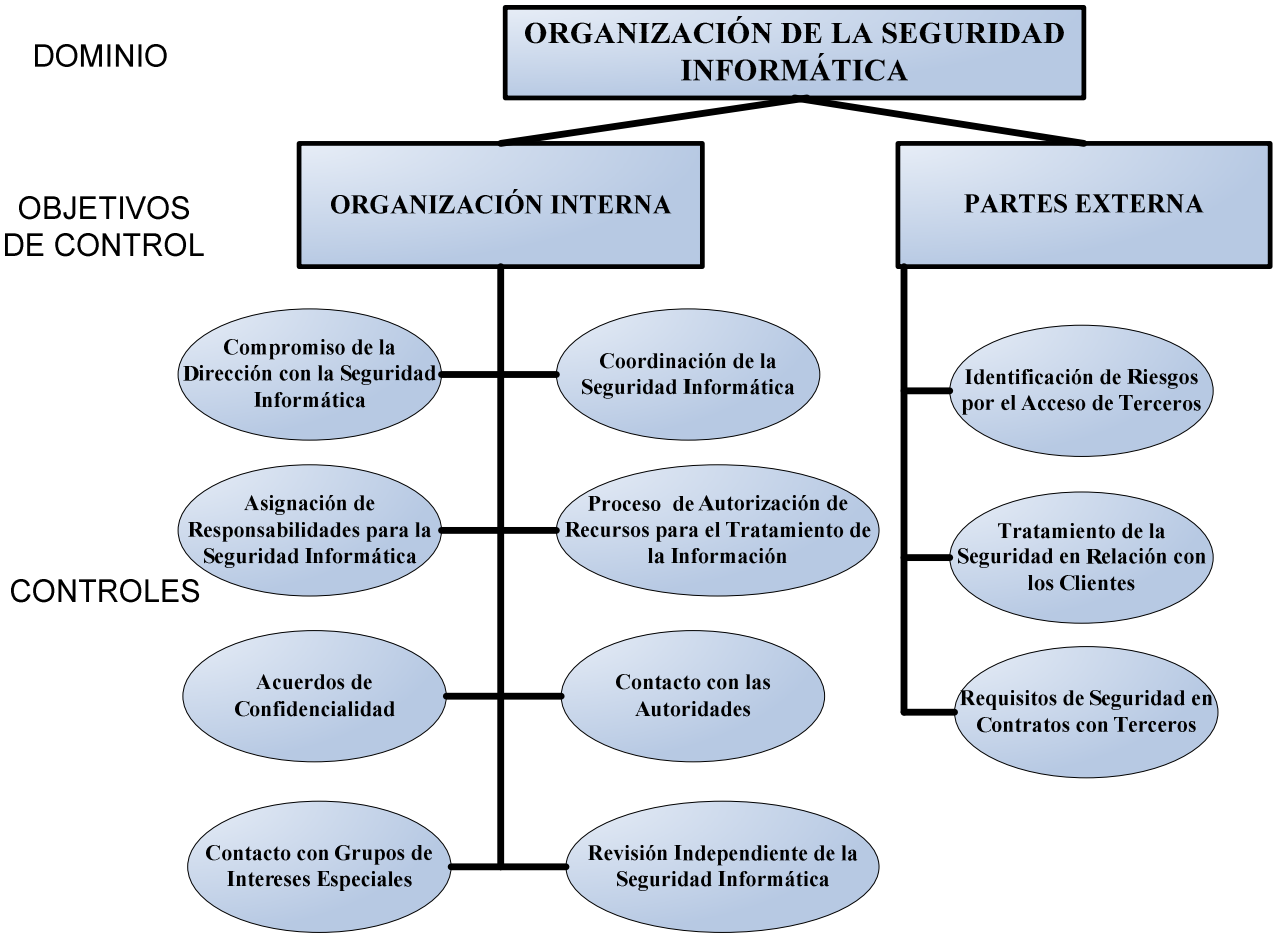


GRÁFICO 2.3 CONSTITUCIÓN DEL DOMINIO "ORGANIZACION DE LA SEGURIDAD INFORMÁTICA"

2.4.1.1 Primer Control "Compromiso de la Dirección con la Seguridad Informática".

El primer control se enfoca en que la dirección debe apoyar la Seguridad Informática dentro de la empresa.

Las pautas para implementar este control son:

a) Asegurar que las metas de la Seguridad Informática están identificadas, satisfacen los requisitos de la organización y están integradas en los procesos pertinentes.
b) Formular, revisar y aprobar la política de Seguridad Informática.

c) Revisar la eficacia de la implementación de la política de Seguridad Informática.
d) Proporcionar un rumbo claro y apoyo visible para las iniciativas de seguridad.
e) Proporcionar los recursos necesarios para la Seguridad Informática.
f) Aprobar la asignación de funciones y responsabilidades específicas para la Seguridad Informática en toda la organización.
g) Iniciar planes y programas para mantener la concientización sobre la Seguridad Informática.
h) Asegurar la coordinación en toda la organización de la implementación de los controles de Seguridad Informática.

Este control será implementado parcialmente en Networking pero no contará con el total apoyo de la gerencia ya que por estos momentos ésta no es una prioridad de la organización.

2.4.1.2 Segundo Control "Coordinación de la Seguridad Informática".

El segundo control es acerca de la coordinación de la Seguridad Informática, menciona que la coordinación debería ser adoptada por los representantes de las diferentes áreas de la organización en conjunto con las personas que pertenecen a cada una de estas áreas (directores, usuarios, administradores, contadores, técnicos).

Este control establece pautas como:

a) Garantizar que las actividades de seguridad se efectúan en cumplimiento de la política de Seguridad Informática.
b) Identificar la forma de manejar los incumplimientos.
c) Aprobar metodologías y procesos para las seguridades de la información, como la evaluación de riesgos y la clasificación de información.

d) Identificar cambios significativos en las amenazas y la exposición de la información y de los servicios de procesamiento de la información a las amenazas.
e) Evaluar la idoneidad y coordinar la implementación de los controles de Seguridad Informática.
f) Promover eficazmente la educación, la formación y la concientización de la Seguridad Informática en toda la organización.
g) Valorar la información recibida del monitoreo y la revisión de los incidentes de Seguridad Informática, y reconocer las acciones apropiadas para responder a los incidentes identificados de la Seguridad Informática.

Este control se aplicará en el departamento de Networking sin ningún problema, a continuación se explica los puntos que se consideran más relevantes:

Identificar la forma de manejar los incumplimientos.- En este punto, se propone crear un reglamento para manejar los incumplimientos de la política de Seguridad Informática, lo cual es adecuado para ayudar al proceso de implementación.

Garantizar que las actividades de seguridad se efectúan en cumplimiento de la política de Seguridad Informática.- Es decir, se debe garantizar que se están cumpliendo las políticas de seguridad implementadas en Networking. La manera de demostrar es con la conducta y actitud de los miembros del departamento y registros que así lo demuestren.

Evaluar la idoneidad y coordinar la implementación de los controles de Seguridad Informática.- Se muestra que la coordinación involucra también la implementación de los controles, mas no solo su determinación y revisión.

En algunas empresas puede ser que sus grupos son demasiado pequeños como para establecer un representante, entonces se puede establecer un solo director o grupo general; desde este punto, se puede decir que se beneficia al proceso de implementación de las políticas de Seguridad porque no es necesario que existan muchas personas para coordinar las tareas.

Como la implementación de este control se lleva a cabo en un área específica de la organización que contiene un grupo de cuatro personas, se nombró a un coordinador para que realice las tareas especificadas en la norma.

2.4.1.3 Tercer Control "Asignación de Responsabilidades para la Seguridad Informática"

El tercer control menciona que se debería definir todas las responsabilidades en cuanto a Seguridad Informática, tiene mucha relación con el documento de la política de seguridad.

Es necesario definir las responsabilidades de forma clara; cuando se asignen a un individuo, y éste delega a otras personas para que se hagan cargo, el individuo que asignó a otras personas sigue siendo responsable por las tareas encomendadas. Para evitar la delegación de responsabilidades a terceras personas, se recomienda asignar responsabilidades de forma equitativa y sin sobrecargar el trabajo del responsable de la seguridad.

En Networking se distribuirá las responsabilidades entre los cuatro integrantes del departamento y designará un coordinador para que revise periódicamente si las políticas se cumplen.

2.4.1.4 Cuarto Control "Proceso de Autorización de Recursos para el Tratamiento de la Información".

El cuarto control da la pauta para definir e implementar un proceso de autorización de la dirección para servicios de procesamiento de información. Es bueno que todos los servicios nuevos tengan aprobación de la dirección, de esta forma se fusiona aun más la gerencia con el desarrollo e implementación de la política de seguridad.

Cuando se tiene que utilizar tecnología de procesamiento de información personal, el procedimiento de autorización también es importante para evitar que

cualquier persona conecte cualquier dispositivo que puede contener alguna vulnerabilidad y afectar a la organización.

Este control se va a implementar en el área de Networking, aunque existen muy pocos procesadores de información integrados a la empresa que han pasado por Networking.

2.4.1.5 Quinto Control "Acuerdos de Confidencialidad"

El quinto control permite identificar los requisitos para la confidencialidad o no-divulgación y crear un documento en donde se los especifique. Todo esto, tomando en consideración la utilización de términos entendibles que se pueden hacer cumplir legalmente, es decir, se ponen las reglas y sanciones claras para quien las incumpla.

Es necesario revisar los requisitos de confidencialidad periódicamente en especial cuando se produzcan cambios significativos. Según la organización, pueden existir diferentes acuerdos de confidencialidad, esto se da porque algunos empleados tienen acceso a zonas más críticas que otros.

Los puntos más relevantes de este control son:

Responsabilidades y acciones de los que suscriben el acuerdo de confidencialidad para evitar la divulgación no autorizada de información.- Este articulo aclara que el acuerdo define los roles de cada parte para proteger la confidencialidad de la información.

Acciones esperadas a tomar en caso de incumplimiento de este acuerdo.- Este punto, sirve de complemento para el acuerdo establecido y permite determinar las sanciones en caso de incumplimiento del mismo.

2.4.1.6 Sexto Control “Contacto con las Autoridades”.

El sexto control menciona que se debería tener contacto con las autoridades mediante procedimientos establecidos que especifiquen cuándo, cómo y a quién deberían dirigirse para reportar algún incidente de Seguridad Informática.

Es fundamental disponer de estos procedimientos ya que en algunos casos, la gente reporta a la persona equivocada o no le dan la importancia que se merece, puede constituir además un respaldo de haber informado el incidente y evitar sanciones.

El registrar y avisar oportunamente el suceso contribuye para que la organización actúe a tiempo y evite perder la *continuidad del negocio*. El tener también en cuenta los contactos con autoridades públicas (policía, bomberos, emergencias, entre otros) cubre una gran zona que muchas empresas no le prestan atención pero que amerita hacerlo.

En Networking se puede establecer este control sin inconvenientes.

2.4.1.7 Séptimo Control “Contacto con Grupos de Intereses Especiales”.

El séptimo control reconoce la importancia de mantener contactos apropiados con grupos de intereses especiales, foros especializados en Seguridad Informática y asociaciones de profesionales.

Se recomienda tener asociaciones para compartir información autorizada, muchas veces ayudan a resolver problemas que se pueden presentar en la organización respecto a las políticas de seguridad, también son de gran utilidad para desarrollar diferentes metodologías de implementación de las políticas de Seguridad Informática.

Este control es muy importante implementarlo en el área de Networking para reportar sucesos de seguridad y actuar de forma inmediata para no detener las actividades de la empresa.

2.4.1.8 Octavo Control "Revisión Independiente de la Seguridad Informática".

El octavo control explica como implementar la revisión independiente de la Seguridad Informática. La revisión independiente es necesaria para asegurar la eficacia, idoneidad y propiedad del enfoque de la organización para la gestión de la Seguridad Informática; la persona encargada de realizar la revisión puede pertenecer a la empresa o puede ser externa a la misma, pero es importante que registre y reporte todos los sucesos encontrados durante la revisión.

Las técnicas de revisión pueden incluir entrevistas de la dirección, verificación de registros, revisión de documentos de la política de Seguridad Informática y cuando se compruebe que el sistema de implementación es inadecuado o no está orientado a los objetivos de la empresa, se debe considerar acciones que sean correctivas. Es muy similar a una auditoría.

Este control permite mejorar el nivel de seguridad robusteciendo las zonas endebles del área de Networking.

2.4.2 OBJETIVO DE CONTROL "ADMINISTRAR PARTES EXTERNAS"

El segundo objetivo de control ADMINISTRAR PARTES EXTERNAS sirve para mantener la Seguridad Informática y de los servicios de procesamiento de información de la organización a los cuales tienen acceso partes externas; no se debe debilitar las zonas de seguridad con la introducción de productos o servicios de partes externas, tampoco se debe descuidar los accesos a la información y los mecanismos de procesamiento de la información para personas externas, en lo posible se debe evitar que personas externas tengan acceso a la información, pero cuando ya es inevitable este hecho, y se debe proporcionar acceso a la

información es necesario realizar una evaluación de los riesgos que implica ese acceso. Una vez establecidos los riesgos entonces se puede acordar y definir los controles necesarios en comunión con las personas externas.

2.4.2.1 Primer Control "Identificación de Riesgos por el Acceso de Terceros"

El primer control menciona que se debería identificar los riesgos para la información y los servicios de procesamiento de la organización, en especial de los procesos del negocio que involucran partes externas, la evaluación de los riesgos ayuda a identificar y calcular cuales son los riesgos que se deben prever antes de otorgar acceso a la información a terceras partes.

Se recomienda también hacer firmar acuerdos de confidencialidad a las partes externas que van a tener acceso a los datos para tener un compromiso por escrito y prevenir la divulgación de información sensible.

Las partes externas podrían poner en riesgo la información de manera involuntaria, o se podrían abrir brechas de inseguridad cuando se aplica deficientemente la gestión de la seguridad; por esto se deben implementar controles que puedan complementarse y ofrecer mayor protección a la información.

Identificar los riesgos y establecer este control en el área de Networking es muy importante para no dar acceso total a los clientes que visitan la empresa.

2.4.2.2 Segundo Control "Tratamiento de la Seguridad en Relación con los Clientes"

El segundo control dice que todos los requisitos de seguridad identificados se deberían abordar antes de dar acceso a los clientes a la información. Se presentan puntos que son importantes considerar:

Política de control de acceso.- Que resume el método de acceso, los identificadores, el proceso de autorización, la declaración que el acceso que no se autorice explícitamente está prohibido.

Convenio para el reporte, la notificación y la investigación de las inexactitudes de la información, incidentes en la Seguridad Informática y violaciones de la seguridad.- Que establece la firma del convenio con el cliente para reportar información incoherente y/o violaciones de la misma.

Puede suceder que los acuerdos con los clientes también impliquen a otras partes, entonces se debería incluir en estos acuerdos, la permisividad para que intervengan, de ser necesario, otras partes.

En el departamento de Networking se aplicará este control para tener respaldos del consentimiento de la dirección del acceso que se debe otorgar a los clientes.

2.4.2.3 Tercer Control "Requisitos de Seguridad en Contratos con Terceros"

El tercer control manifiesta que los acuerdos con terceras partes que implican acceso, procesamiento o gestión de la información, o la adición de productos a los servicios de procesamiento de la información deberían considerar todos los requisitos de seguridad, es decir, no se deberían permitir los malos entendidos o interpretaciones diferentes de los acuerdos establecidos entre la organización y la tercera parte, también se busca la satisfacción de ambas partes. Como parámetros principales de este control se deberían considerar:

Política de control de acceso.- Similar al procedimiento utilizado con los clientes, debe resumir el método de acceso, identificadores, proceso de autorización, la declaración que el acceso que no se autorice explícitamente está prohibido.

Establecer los controles para proteger el activo.- Para conocer los procedimientos que se deben seguir, antes de dar acceso a los activos de información.

Condiciones para la renegociación/terminación del acuerdo.- Estableciendo un plan de contingencia para el caso que termine el acuerdo de lo antes previsto, recalcando en que los acuerdos siempre van a variar entre empresa y la parte externa.

Por lo general, los acuerdos los desarrolla la organización, pero pueden existir casos que la tercera parte tenga esta función. Lo que se debería prever es que la organización garantice que su seguridad no se vería afectada con las condiciones del acuerdo.

En el área de Networking se creará una política que permita cumplir con el trato a terceras personas, sin embargo este control puede no ser aplicado ya que solamente se trata con clientes externos e internos; las terceras personas deben contactar a los otros departamentos ya sea servicio al cliente o a ventas.

2.5 ANÁLISIS DOMINIO GESTIÓN DE ACTIVOS

El reconocimiento y gestión de los activos de información en la organización es importante para determinar los recursos que dispone la empresa y para darles la protección adecuada.

Este dominio posee dos objetivos de control; el primero DETERMINAR LA RESPONSABILIDAD POR LOS ACTIVOS con tres controles, el segundo CLASIFICAR LA INFORMACIÓN con dos controles, esto se aprecia en el Gráfico 2.4.

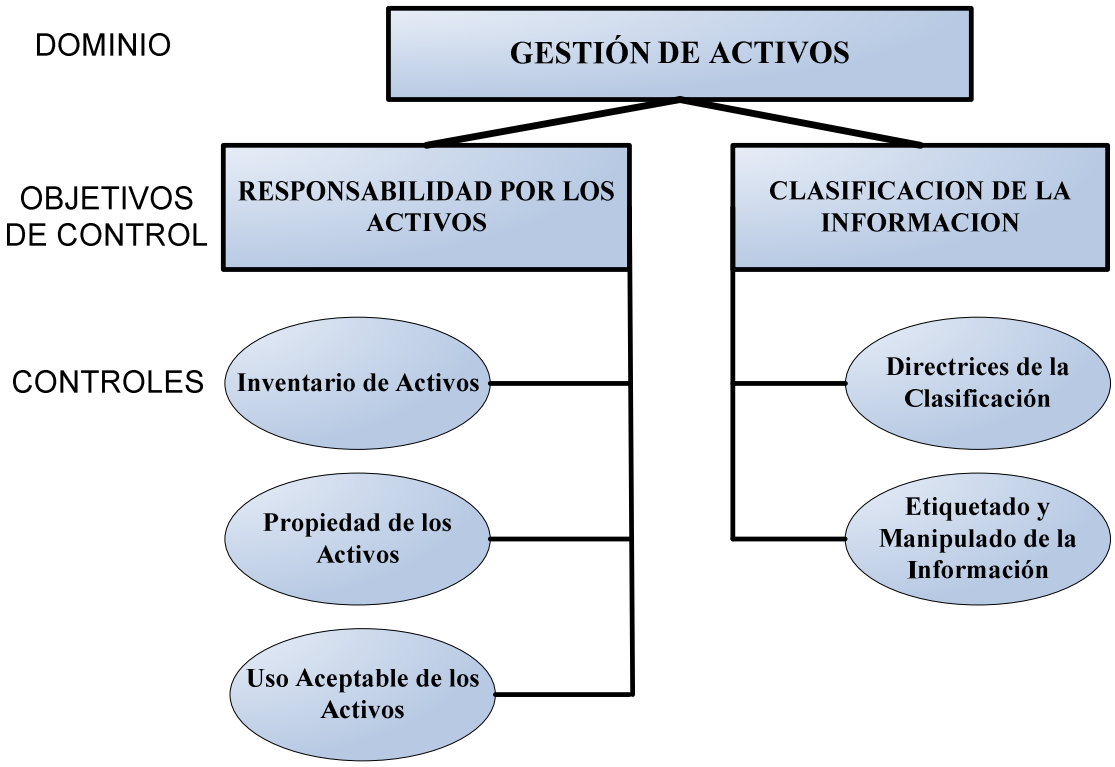


GRÁFICO 2.4 DOMINIO GESTIÓN DE ACTIVOS

2.5.1 OBJETIVO DE CONTROL "DETERMINAR LA RESPONSABILIDAD POR LOS ACTIVOS"

El primer objetivo de control DETERMINAR LA RESPONSABILIDAD POR LOS ACTIVOS sirve para lograr y mantener la protección adecuada de los activos de la organización, menciona que todos los activos se deben revisar y asignarles un dueño, esto es beneficioso porque al distribuir responsabilidades se logra que la gente se comprometa más con la Seguridad Informática.

2.5.1.1 Primer Control "Inventario de Activos"

El primer control recalca el hecho que se deben identificar todos los activos mediante un inventario; como se conoce, activo es todo lo que tenga valor para la empresa.

Por supuesto, existirán diferentes activos y su valor será diferente para cada empresa. Se debería incluir en la identificación de los activos, su clasificación y documentación.

Para identificar los activos más y menos importantes se recomienda listarlos y clasificarlos de acuerdo al criterio de "¿Qué activos me permiten la recuperación de desastres y en cuánto tiempo?".

Existen diversos tipos de activos:

Activos de información.- Bases de datos y archivos de datos, contratos y acuerdos, documentación del sistema, información sobre investigación, manuales de usuario, material de formación, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos de recuperación, registros de auditoría e información archivada.

Activos de Software.- Software de aplicación, software del sistema, herramientas de desarrollo y utilidades.
Activos Físicos.- Equipos de computación, equipos de comunicaciones, medios removibles.

Servicios.- Servicios de computación y comunicaciones, servicios generales como por ejemplo iluminación, calefacción, energía y aire acondicionado.

Personas y sus calificaciones, habilidades y experiencia.
Intangibles tales como reputación e imagen de la organización.
El obtener todos los activos es primordial para la gestión de riesgos.

Este control es muy útil para el departamento de Networking pues en este se dispone de una bodega de equipos exclusiva, algunos manuales y computadores para procesar la información.

2.5.1.2 Segundo Control “Propiedad de los Activos”

El segundo control menciona que toda la información y los activos asociados con los servicios de procesamiento de información deberían tener como propietario a una parte de la organización, no para que se haga lo que sea con el activo de la información, sino que deben cumplir responsabilidades sobre este activo para garantizar el desarrollo, desempeño, el uso y la seguridad del mismo.

La propiedad se puede asignar a un proceso del negocio, a un conjunto definido de actividades, a una aplicación o a un conjunto definido de datos.

Así, si la propiedad se la otorga a un conjunto definido de actividades que se convierte en un servicio, entonces el responsable de cumplir esas actividades también es responsable del activo.

En el área de Networking se designarán dueños de activos conforme a los procesos o actividades definidos.

2.5.1.3 Tercer Control “Uso Aceptable de los Activos”

El tercer control indica que se debería identificar, documentar e implementar las reglas sobre el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de la información, es decir, para garantizar el uso aceptable de la información se deberían establecer directrices y reglas que los empleados tienen la obligación de cumplir.

En el área de Networking el encargado de establecer las directrices y reglas para cada activo es el responsable del activo de información.

2.5.2 OBJETIVO DE CONTROL “CLASIFICAR LA INFORMACIÓN”

El segundo objetivo de control CLASIFICAR LA INFORMACIÓN es asegurar que la información está correctamente clasificada para recibir el nivel adecuado de protección, se conoce que la información tiene diferentes grados de importancia, de igual forma debe ser la protección que se le dé.

2.5.2.1 Primer Control “Directrices de la Clasificación”

El primer control establece directrices para la clasificación de la información en términos de su valor, requisitos legales sensibilidad e importancia para la organización.

Este control permite caer en cuenta que cuando se clasifica la información se deben considerar las necesidades del negocio, también se deberían incluir políticas para reclasificar la información a periodos determinados, por ejemplo puede que información clasificada en una fecha se convierta en pública.

Adicional, el encargado de clasificar la información es el dueño del activo, puede asignar a otra persona, pero él sigue siendo el propietario del activo.

No es aconsejable clasificar la información en demasiadas categorías porque en lugar de facilitar la administración, se puede tornar muy compleja y no práctica.

Las directrices para clasificar la información crean niveles de seguridad diferencian a la información importante de la menos importante, de la privada de la pública o información de terceras personas que se encuentran en la empresa por cualquier motivo.

Este control es muy útil para Networking ya que este departamento tiene acceso a toda clase de información.

2.5.2.2 Segundo Control “Etiquetado y Manipulado de la Información”

El segundo control da la pauta para desarrollar e implementar un conjunto de procedimientos adecuados para el etiquetado y el manejo de la información, esta actividad no es solamente colocar números o signos a la información, tiene que integrarse con un sistema informático, lo ideal sería que para el etiquetado las estrategias deben ser una mezcla de métodos físicos y electrónicos.

El etiquetado de la información tiene relación directa con la clasificación de la información, es decir existen diferentes niveles de etiquetado que reflejan el tipo de información. Para cada nivel se puede definir también procedimientos de manejo, una etiqueta blanca puede ser información no importante y puede ser manipulada por casi toda le gente; una etiqueta roja puede ser muy importante y se debería mantenerla en lugares accesibles solo a personal autorizado.

En este control también se definen procedimientos para interpretar la información de otras organizaciones. La información de otras organizaciones puede estar etiquetada en forma distinta por ello es necesario saber identificar que aquella información es de parte externa.

En el caso especial de la información electrónica, que no puede ser etiquetada físicamente, se puede aplicar métodos de notificación en pantalla.

En Networking se establecerán las pautas para el etiquetado de la información en base al tipo de información identificado en el control anterior.

CAPÍTULO III

ANÁLISIS DE POLÍTICAS PRECEDENTES DE SEGURIDAD Y ESTABLECIMIENTO DEL PLAN PILOTO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

CAPÍTULO III: ANÁLISIS DE POLÍTICAS PRECEDENTES DE SEGURIDAD Y ESTABLECIMIENTO DEL PLAN PILOTO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

3.1 ANÁLISIS DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA PRECEDENTES EN EL ÁREA DE NETWORKING.

3.1.1 GENERALIDADES DEL ANÁLISIS

Para el *análisis de las políticas de Seguridad Informática* no existen definiciones oficiales, se han dado cursos y seminarios refiriéndose a ella, pero no se ha llegado a establecer un concepto.

Como primer concepto, se puede decir que: “el análisis de las políticas de Seguridad Informática comprende la revisión y evaluación independiente y objetiva, por parte de personas independientes y teóricamente competentes del entorno informático de una entidad, abarcando todo o algunas de sus áreas, los estándares y procedimientos en vigor, su idoneidad y el cumplimiento de éstos, de los objetivos fijados, los contratos y las normas legales aplicables, el grado de satisfacción de usuarios y directivos, los controles existentes y el análisis de riesgos”.[12]

Se puede decir entonces que el análisis de las políticas de Seguridad Informática es aquella que tiene como objetivos evaluar los controles de la función informática, determinar la eficiencia de los sistemas, verificar el cumplimiento de las políticas y procedimientos de la empresa en este ámbito y revisar que los recursos materiales y humanos de esta área se utilicen eficientemente.

[12] Miguel Ángel Ramos González, Especialista en Auditoría Informática.

Este análisis surge debido a que la información es uno de los activos más importantes en las empresas, así como el uso de la tecnología y sistemas computarizados para el procesamiento de la información.

Mediante la tabla 3.1 se puede decir que el proceso de Auditoría Informática es el proceso de recolección y evaluación de evidencia para determinar si un sistema:

Salvaguarda Activos	**Daños**
	Destrucción
	Uso no autorizado
	Robo
Mantiene la Integridad de los Datos	**Oportuna**
	Precisa
	Confiable
	Completa
Alcanza Metas Organizacionales	**Contribución de la función Informática**
Consume Recursos Eficientemente	**Utiliza recursos con mesura para procesar la información**

TABLA 3.1 FUNCIONES DEL ANÁLISIS DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

3.1.2 ALCANCE DEL ANÁLISIS DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA

El alcance del análisis de políticas de Seguridad Informática es determinar el entorno y los límites en el cual se desarrolla el mismo. Se debe detallar los temas que fueron examinados, los que fueron omitidos y sus razones.

3.1.3 ANÁLISIS DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA EN NETWORKING DE LA EMPRESA UNIPLEX SYSTEMS S.A. EN QUITO

El departamento de Networking en Quito de la empresa Uniplex Systems S.A., es un pilar fundamental de la organización; cuenta con cuatro empleados que ocupan diferentes rangos.

En el gráfico 3.1 se puede apreciar la estructura de Uniplex y del departamento de Networking.

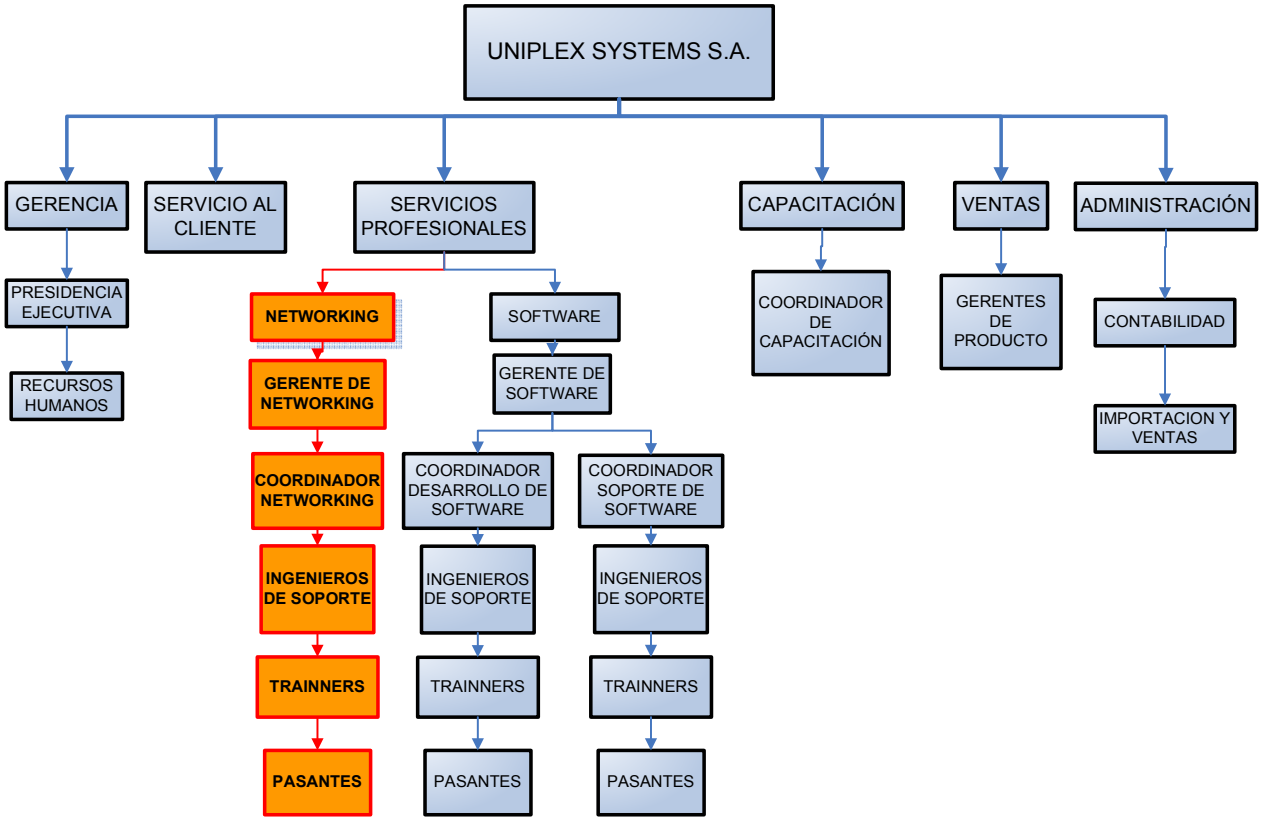


GRÁFICO 3.1 ORGANIGRAMA DE LA EMPRESA

A continuación se describen los datos y la información recogida durante el relevamiento realizado al departamento de Networking, detallando cada uno de los controles que se implementan en la actualidad.

3.1.3.1 Evaluación de la Seguridad Lógica

Alcance del Análisis: El alcance en este punto es determinar cuan efectivos son los controles para el acceso a los elementos procesadores de datos, cuan seguros son los password del área de Networking y cómo está conformada la segregación de funciones del área.

3.1.3.1.1 Permisos

Los permisos se dan mediante el servidor Active Directory; pueden ser como *administrador* o como *usuario* del dominio (cuentas con diferentes niveles de privilegio); cada usuario tiene su propio perfil y puede registrarse en cualquier computadora que se encuentre dentro del dominio.

El permiso que tienen los usuarios de Networking es de *administrador*, ya que los técnicos regularmente requieren instalar software para controlar varios equipos.

Por otro lado; Microsoft Windows tiene en su sistema operativo una cuenta Administrador (cuenta distinta a la otorgada por el Active Directory para registrarse) con diferente password; que permite a los usuarios ingresar al computador pero sin ingresar al dominio de la organización. Esta cuenta puede ser activada cuando el computador realiza el procedimiento de arranque.

3.1.3.1.2 Password

Los miembros de Networking emplean algunos password; para registrarse en el dominio de la empresa; para ingresar como Administrador del sistema operativo Windows en sus computadores, para ingresar al email; incluso existen password para tener contacto con grupos afines en la Web, algunos computadores tienen password del Sistema de Entrada y Salida Básico (Basic Input Output System BIOS); cada uno de estos password es configurado de diferente forma.

Los password para ingresar al dominio de la organización se configuran en el servidor Active Directory; los password para ingresar como Administrador en los ordenadores son configurados localmente, de igual forma el password del BIOS; para los password de las comunidades afines se puede modificar desde el portal de la comunidad (similar a la cuenta de Hotmail, hi5, etc.); el password para ingresar al mail se configura en el servidor de correo (servidor que no está a cargo de Networking).

Es importante acotar que todos los password no tienen restricción de tamaño máximo, solamente de tamaño mínimo de cuatro caracteres.

Los usuarios de Networking pueden modificar los password de ingreso al dominio, password de la cuenta de Administrador, del BIOS, de los grupos de interés en los que se encuentran registrados, pero no pueden modificar el password de la cuenta de correo, para hacerlo deben solicitar al gerente de Software el cambio del password con los motivos por los cuales desea hacerlo,

En caso que algún usuario se olvide el password para registrarse en el dominio, se lo puede modificar en el servidor Active Directory, si se extravía el password de la cuenta de Administrador o del BIOS se corre un grave riesgo y se torna muy difícil recuperarlos, de igual forma si se olvida el password de la comunidad a la cual pertenece; si no recuerda el password de correo, pues el administrador de correo lo puede borrar y poner uno temporal.

Existen otros password que son para administrar equipos que están a cargo del departamento de Networking (switch, firewall, router, access point, módems, entre otros), estos equipos son de infraestructura o se encuentran en la bodega. No se dispone de un documento con los password de los equipos, si se olvida un password se debe reiniciar el equipo a su configuración por defecto.

3.1.3.1.3 Inactividad

Cuando los usuarios permanecen registrados sin actividad durante algún tiempo, algunos computadores siguen en funcionamiento normal; otros entran en suspensión y otros hibernan.

3.1.3.1.4 Segregación de Funciones

En el departamento de Networking se han segregado las funciones de sus miembros para que se hagan cargo de los diferentes productos por marca. Sin embargo, existen funciones similares para algunos usuarios.

Las funciones principales incluyen:

- Monitoreo de la red
- Soporte a clientes internos
- Soporte a clientes externos

3.1.3.2 Evaluación de la Seguridad de las Comunicaciones

Alcance del Análisis.- El alcance en este campo será analizar la seguridad de las comunicaciones, los datos transmitidos, los dispositivos usados durante la transmisión, la documentación necesaria para la realización eficiente y sin interrupciones de esta transmisión, y los sistemas usados para la transmisión de datos de un entorno a otro, comprobando el cumplimiento de las normas de Seguridad Informática.

3.1.3.2.1 Topología de Red

En la topología de red existen equipos de infraestructura que se encuentran distribuidos por toda la empresa y que corresponden monitorear al área de Networking.

En la tabla 3.2 se describen los equipos de la topología, que están a cargo de Networking:

Ítem	Descripción de Equipo	Cantidad
1	Firewall Cisco 515 E	1
2	ALLOT Administrador Ancho de Banda AC402	1
3	Switch Catalyst 2950	2
4	Switch 3COM 3C16475	2
5	Switch Dlink	1
6	Access Point (2 WL 524,2 WL 7760)	4
7	Hub sin marca	3
8	Laptop IBM thinkpad T30	3
9	Desktop Clon	1

TABLA 3.2 EQUIPOS DE NETWORKING

Existe una conexión a través de cable UTP categoría 5e entre todos los elementos de la red.

En el patch panel no se identifican los puntos a los cuales se dirigen las conexiones, para determinar el destino de un cable es necesario seguirlo con la vista, cuando esto no es posible entonces se utiliza un seguidor de señal.

El puerto *External* del Firewall se conecta con el ISP; y del puerto *Internal* se dirige al puerto *External* del Administrador de Ancho de Banda, del puerto Internal de este equipo se dirige a un switch.

Entre los Switch se interconectan solamente con un cable; no existen enlaces redundantes para prever la caída del enlace; en los que son administrables se ha configurado la dirección IP.

Los Hub no son administrables y no se puede determinar el fabricante, son viejos y se han conservado en la empresa por el costo que implicaría comprar switches con igual número de puertos.

Los Access Point trabajan en la banda libre (frecuencia de 2.4 GHz) y tienen configurado un password que solamente lo conocen los miembros de Networking. El método de encripción de los Access Point es WEP (Wired Equivalent Protection), que es un poco antiguo y fácil de descifrar, no se utiliza un método más avanzado porque los computadores de la empresa no lo soportan.

El Internet es una herramienta fundamental para el trabajo, todos los miembros de la empresa tienen acceso a Internet para que efectúen consultas y descargas. Pero no se han establecido normas para el correcto uso de esta herramienta.

Existen restricciones para páginas Web que contienen pornografía, no se posee reglas para el uso de mensajería instantánea (Messenger, Skype, Latinchat, etc.).

3.1.3.2.2 Conexiones Externas

La conexión hacia fuera es mediante un enlace de radiofrecuencia el cual provee 600 Kbps de Capacidad.

Además, existe una salida alterna a Internet con Dial Up que suele utilizarse para realizar pruebas con algunos equipos y para ser utilizada en casos de emergencia.

3.1.3.2.3 Configuración Lógica de Red

En el gráfico 3.2 se presenta un diagrama de la topología de la red de Uniplex Quito S.A., y se explica brevemente su configuración desde la parte externa hacia la parte interna.

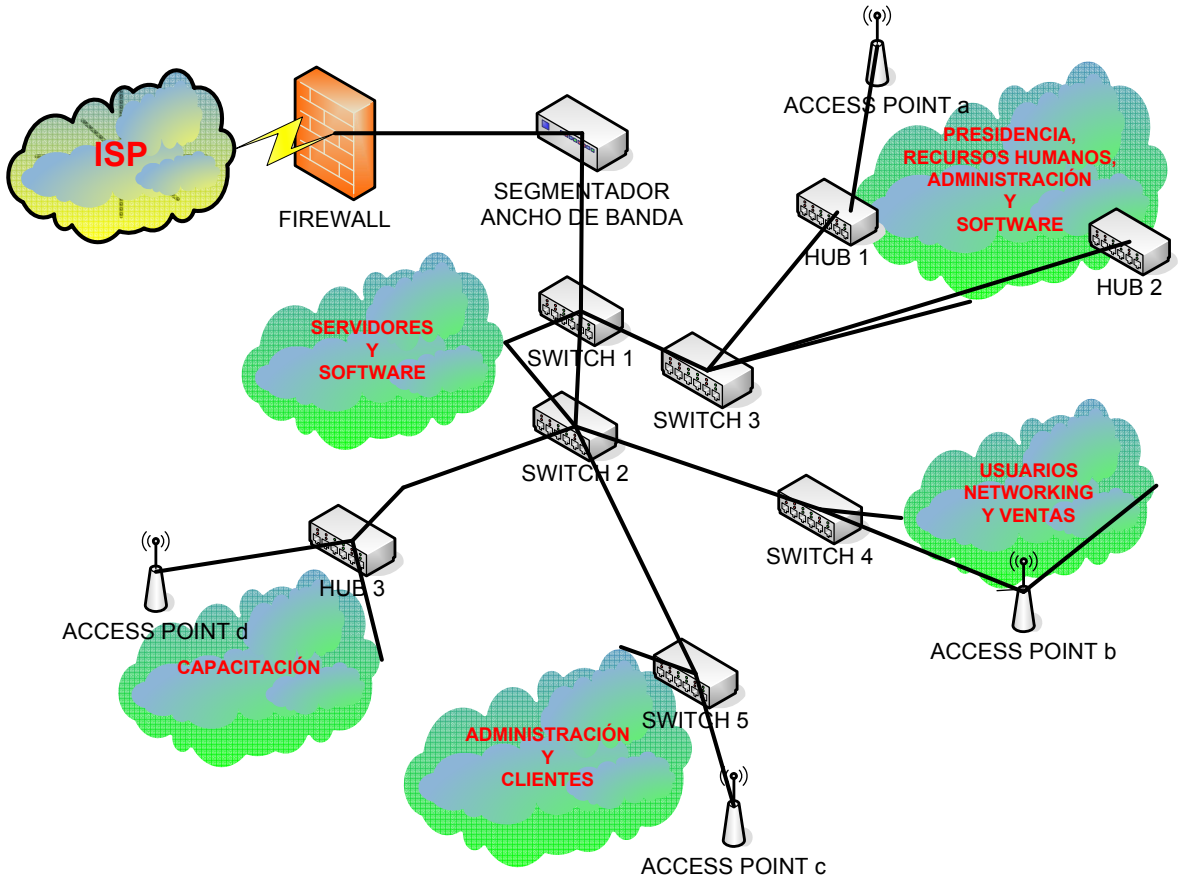


GRÁFICO 3.2 TOPOLOGÍA DE RED

El Firewall recibe el enlace del proveedor de servicio, dispone de tres zonas:

- Internal
- External
- Red Privada Virtual (Virtual Private Network VPN)

Su configuración comprende listas de acceso, filtrado de direcciones, VPN's entre otros, va conectado contra un segmentador de ancho de banda. El acceso a este equipo es mediante una conexión de Telnet, con user y password para cada miembro de Networking. Se puede accesar y configurar este equipo también con un software propietario del fabricante "Seguridad Adaptable para Gestión de Equipo" (Adaptive Security Device Manager ASDM)

El segmentador de ancho de banda limita las conexiones entrantes y salientes a un determinado ancho de banda, incluso puede bloquear algunas aplicaciones, pero no brinda seguridad. Va conectado al switch 1 (switch 3COM) de la red interna. El acceso a este equipo es vía Web y posee un user y password únicos para todos los técnicos de Networking.

El switch 1 (Switch 3COM) no es administrable, se conecta con los demás switch (2,3) en cascada mediante cable UTP, brinda conectividad a todos los servidores y algunos Host de software. Los servidores que dispone la empresa son: Correo, Antivirus, Black Berry, File Maker, DHCP, DNS, Pruebas.

A continuación en la tabla 3.3 se detalla el servidor bajo la responsabilidad de Networking (DHCP, DNS, Antivirus):

Ítem	Descripción de Equipo	Cantidad
1	Servidor IBM X Series 3200 1.86GHz	1
2	Disco Maxtor 160GB, WDC 250GB	1
3	Memoria RAM 1 GB	3
4	Fuente Poder	1

TABLA 3.3 SERVIDOR BAJO RESPONSABILIDAD DE NETWORKING

Servicios contenidos en el equipo:

- Antivirus Symantec (Caducado)
- Active Directory
- Servidor DNS
- Servidor DHCP
- Servidor de Antispam
- Servidor FTP (3CDaemon)
- Máquina Virtual (VMware)
- Servidor Domino Lotus
- Software Impresoras en Red

En el switch 2 (Switch 3COM no administrable), se conectan usuarios de Software, y los switch (4,5); da conectividad a usuarios de Software y al HUB 3 que se encuentra en la sala de Capacitación, éste a su vez da conectividad al Access Point “d”.

El switch 3 (CISCO) es administrable pero solo se ha configurado la dirección IP de administración; sirve para dar conectividad a los usuarios de Presidencia, de Recursos Humanos, de Administración y de Software, también da conectividad a 2 HUB (1,2) utilizados en administración por falta de Puntos de red; en uno de estos HUB se conecta el Access Point “a”, que da conectividad redundante a Presidencia y Recursos Humanos. El acceso a este equipo es mediante una conexión de Telnet, con user y password de técnicos anteriores, no actualizados.

El switch 4 (CISCO) es administrable pero solo se ha configurado la dirección IP de administración, da conectividad a los usuarios de ventas y Networking, así como también al Access Point “b” que es utilizado como enlace redundante. El acceso a este equipo es mediante una conexión de Telnet, con user y password de técnicos anteriores, no actualizados.

El switch 5 (DLINK) es administrable pero no se ha configurado, da conectividad a usuarios de administración y al Access Point “c”, que es utilizado por clientes que visitan la empresa y que requieren conectividad.

En la red interna, todos los equipos (Host, servidores, Access Point, switch, impresoras, etc.) se conectan mediante cable UTP cat 5e, aunque algunas computadoras portátiles tienen la facilidad de conectarse a la red inalámbrica con un adaptador de red.

En la red interna se utiliza Sistema Operativo Windows 2000, 2003, XP, NT, no existen problemas de compatibilidad o de recursos compartidos; los recursos de la red se comparten utilizando la herramienta de Windows para compartir carpetas, en algunos casos, también está configurado un servidor ftp para transferencia de archivos.

En el área de Networking se encuentra una computadora con información de los ingenieros de soporte anteriores que incluyen programas e información de clientes, a estos datos tienen acceso el departamento de ventas y Networking.

Este computador es utilizado además para realizar presentaciones a los clientes, a veces se lo lleva a la localidad del cliente y se queda allí días, semanas o meses. La información se queda en el equipo y no se la extrae porque no se dispone de otro disco para almacenar la información.

En algunos computadores de la empresa se han sacado respaldos de empleados anteriores, es por esto que existe información de clientes que está esparcida y repetida o ya es obsoleta.

No se dispone de archivos de configuración de estos equipos, si un equipo se desconfigura, se debe reconfigurarlo desde cero.

3.1.3.2.4 Mail

Todos los miembros de Networking tienen su cuenta de correo, esta vía de comunicación permite llegar a toda la empresa y para enviar todo tipo de información. Además, el Lotus Notes posee una herramienta para chatear con alguna persona, esta herramienta está totalmente autorizada por la presidencia;

otro tipo de mensajería está prohibida a menos que sea autorizada por gerencia. Al área de Networking no le corresponde la creación o mantenimiento de cuentas de correo, o configuración del chat interno, sin embargo, es su responsabilidad permitir a quien corresponda tener acceso a chat no empresarial (Skype, Messenger, etc.)

Todos los correos entrantes pasan por el servidor de SPAM para evitar que a la empresa ingresen Spyware y correos basura, luego van a sus respectivos destinatarios. Existen usuarios que disponen de Black Berry y se ha configurado para que los correos hagan replicación en el servidor de Correo y en el servidor de Black Berry.

El administrador de la red, quien no tiene un puesto definido sino que pertenece tanto a Networking como Software, es el encargado de realizar las copias de seguridad del correo cada mes en cintas magnéticas; empaquetarlas y enviarlas a la bóveda del banco.

3.1.3.2.5 Antivirus

En la empresa no se han registrado casos severos de pérdida de datos por contaminación con virus, sin embargo han ocasionado que los servicios de la red se tornen lentos.

La empresa disponía de una licencia corporativa de Symantec, pero caducó hace dos meses, se hicieron los análisis respectivos y se optó por cambiar de antivirus, el nuevo convenio sería establecido con McAfee, el análisis fue elaborado por el administrador de la red pero la decisión de compra le corresponde a la gerencia.

Al momento las PCS están con versiones trial de antivirus (McAfee, Kaspersky, Symantec, Nod32, entre otros).

Las actualizaciones de estos antivirus es responsabilidad de cada usuario, deben realizarla directamente desde Internet.

No se hacen escaneos periódicos para detectar virus en los servidores ni en las PCS. No hay ninguna frecuencia para realizar este procedimiento, cada usuario debe realizar su análisis en horario fuera de oficina hasta que se contrate el nuevo antivirus. En algunas máquinas (en las que han tenido problemas frecuentes con virus) ha sido necesario formatear el equipo obteniendo primero un respaldo de la información y escaneándola en busca de virus.

3.1.3.2.6 Firewall

El Firewall que existe en la empresa es un Cisco PIX 515E, configurado de manera que se prohíben todos los servicios y solo se habilitan los necesarios.

EL PIX fue configurado en base a una política que discrimina dos clases de paquetes de red, los entrantes y los salientes.

Por defecto, lo que no se habilite explícitamente está prohibido. Así se les va a denegar el acceso a todos los paquetes de entrada, mientras que a los de salida se les permite la salida.

Algunas de las reglas aplicadas son:

Se realiza Traslación de Direcciones de Red (Network Address Translation NAT) para los paquetes que salen y entran del PIX. Esto es para dar seguridad a las aplicaciones y Host internos de la empresa, de tal manera que los Host que se encuentran afuera apuntan a la dirección pública.

Se han configurado las listas de acceso para evitar ataques del exterior, filtrando a las aplicaciones y no dejando habilitados todos los puertos.

Existen VPN’s configuradas en el PIX para usuarios remotos (cada uno con su username y password) que conectan la zona interna con la zona VPN, entre estas dos zonas no se realiza NAT, simplemente un ruteo para que tengan

conectividad. Los datos que atraviesan las VPN's se encuentran encriptados con algoritmos bastante robustos.

Se tiene configurado un servidor de Protocolo de Tiempo de Red (Network Time Protocol NTP) para que se mantengan siempre actualizadas la fecha y hora con horario mundial.

Para Host que requieren aplicaciones que ocupan *puertos de comunicación*[13] efímeros (puertos que pueden ser cualesquiera para conectarse), se han creado listas exclusivas para estos Host en donde se permite la conectividad en todos los puertos.

El encargado de mantenimiento controla que los servicios permitidos sean los correctos, pero esta tarea la realiza sin ninguna frecuencia y sin planificación; además, solo se revisan las instalaciones cuando hay quejas de los usuarios.

Nunca se hicieron pruebas de auto-hackeo, ni escaneos, ni intentos de intrusión o de escucha. Los miembros de Networking han realizado una prueba para explotar una vulnerabilidad del servidor de correo que demostró que el servidor de correo está protegido de la red externa, pero no de la red interna.

El Firewall puede detectar ataques de *Negación de Servicio*[14] (Deny of Service DoS), pero no se ha configurado esta herramienta; dispone también de configuración de *Calidad de Servicio*[15] (Quality of Service QoS) que tampoco ha sido configurado ya que esta labor la lleva a cabo el segmentador de Ancho de Banda.

El Firewall monitorea los intentos de ingresos, generando logs y mails por cada evento a los miembros de Networking, pero no genera alertas ni warnings ante algún problema de conectividad.

---

[13] Ver Anexo 1
[14] Ver Anexo 1
[15] Ver Anexo 1

No se tienen monitoreados los demás equipos de infraestructura que corresponde al área de Networking.

En la empresa no se dispone de herramientas destinadas exclusivamente para prevenir los ataques de red, en principio debido a que no se han presentado, hasta el momento, problemas en este sentido.

Tampoco existen zonas desmilitarizadas, debido a que no hay datos publicados on-line para usuarios externos desde la red interna.

3.1.3.3 Evaluación de Seguridad en las Aplicaciones.

Alcance del Análisis.- El alcance en esta zona consiste en evaluar la seguridad de las aplicaciones utilizadas en la empresa, la consistencia de sus datos de entrada y la exactitud de sus datos de salida, la integridad de las bases de datos y la existencia y el uso de la documentación necesaria para su funcionamiento, de acuerdo a los estándares propuestos.

3.1.3.3.1 Control de Aplicaciones en PC's

No hay estándares definidos, no hay procedimientos a seguir ni tampoco documentación respecto a la instalación y actualización de la configuración de las PC's.

En el caso de que una PC presente errores en su configuración, se utilizan herramientas de reparación de errores (CD's de instalación de Windows), con el fin de evitar la reinstalación total del sistema y así causar una pérdida innecesaria de tiempo. Sin embargo, en algunas ocasiones la opción más rápida es formatear el equipo, realizando primero un backup de la configuración. No se utiliza la herramienta de Windows para backup (NTBACKUP)[16]

[16] Ver Anexo 1

Cada Usuario de Networking realiza actualizaciones de los programas instalados, como el Internet Explorer, Mozilla, Office, Windows, Java, entre otros; el Java es el más crítico y se actualiza solamente cuando la aplicación a la cual se desea ingresar requiere de una nueva versión.

No existe política de actualización de programas, solamente cuando se presenta un mal funcionamiento o nuevo requerimiento para administrar un nuevo equipo u otro programa.

Solamente el administrador de la red es el encargado de las actualizaciones e instalaciones en las PC's, aunque para los usuarios de Networking no existen restricciones con respecto a la actualización e instalación de programas ya que se deben instalar software especiales para administrar los equipos que ofrece la empresa. (Firewall, Switch, Router, Central IP, Modem, entre otros)

En la empresa existe un software denominado Belarc que permite verificar las actualizaciones que ha realizado un Host en específico, incluso si ha instalado componentes de hardware nuevos. Los usuarios de Networking no poseen claves de acceso a este programa, solo el administrador de la red.

Cuando se hace cambios en las PC's no se guardan copias de las configuraciones anterior y posterior al cambio, tampoco se documentan los cambios que se realizan ni la fecha de las modificaciones.

3.1.3.3.2 Control de Datos en las Aplicaciones de PC's

Los datos de entrada al área de Networking son verificados con el fabricante o con los clientes, este control es efectuado manualmente, por lo cual se asegura su integridad, exactitud y validez.

Con respecto a los datos de salida, no existen restricciones para imprimir los datos de clientes o de productos ya que el departamento de Networking necesita siempre esta información para trabajar.

La empresa cuenta con el software Lotus, que es utilizado para gestionar documentos, realizar planificaciones, actualizar casos de clientes, etc. Pero el departamento de Networking tiene acceso restringido a este programa, con permisos de escritura solo para casos correspondientes a clientes.

3.1.3.4 Evaluación de Seguridad Física

Alcance del Análisis.- Se evaluará el departamento de Networking, los equipos, los dispositivos, los medios de almacenamiento y que las personas que conforman el departamento cumplan con las medidas necesarias en lo relativo a la infraestructura física y al mantenimiento de la seguridad de los recursos de la organización.

3.1.3.4.1 Equipamiento

En el área de Networking existe un servidor con información de clientes, de ingenieros de soporte antecesores y programas freeware. En la tabla 3.4 se detallan los componentes del servidor que fue adquirido en el 2006.

Ítem	Descripción de Equipo	Cantidad
1	Procesador Intel Dual Core	1
2	Fuente Poder	1
3	Mainboard Intel	1
4	Memoria RAM 1 GB	2
5	Discos SATA[17] 180 GB	2

TABLA 3.4 DESKTOP DE NETWORKING

Este servidor se utiliza para dar presentaciones a los clientes y suele llevárselo al sitio del cliente sin sacar toda la información de los técnicos, clientes y programas.

En el área existen 3 Laptop IBM, una PC IBM y algunas computadoras que necesitan ser reparadas, estas computadoras son de clientes internos de la empresa.

[17] Ver ANEXO 1

El administrador de la red es el encargado de elaborar un cuadro de mantenimiento de estas computadoras.

3.1.3.4.2 Control de Acceso a Equipos

Todas las máquinas de Networking disponen de disqueteras y/o lectoras de CD, aunque los disquetes ya no son muy utilizados.

Estos dispositivos están habilitados y no hay ningún control sobre ellos, no se hacen controles automáticos de virus ni se prohíbe el booteo desde estos dispositivos.

Los equipos se encuentran asegurados con un candado de acero y con una clave que solamente la conoce el técnico de su estación de trabajo.

El rack de Networking donde se ubica el switch está a la vista de todos y cerrado con llave, para evitar que el personal de limpieza o cualquier persona desconecten los puertos, o cualquier persona se conecte a un puerto libre.

Existe una bodega que está bajo cargo de Networking, dentro de esta bodega se encuentran equipos de redes muy utilizados por los ingenieros del área. Esta bodega se encuentra bajo llave.

Existen varias llaves que se encuentran en el área de Networking sin clasificar, seguramente se han sacado copias del rack, escritorios y armarios anteriormente pero no se las ha clasificado.

No se realizan controles periódicos sobre los dispositivos de hardware instalados en las PC’s. Una vez que se ha completado la instalación de algún equipo, el administrador de la red no realiza chequeos periódicos, solo revisa los equipos ante fallas en los mismos, o por un problema reportado por el usuario.

3.1.3.4.3 Dispositivos de Soporte

En el departamento de Networking se dispone de los siguientes dispositivos para soporte del cuarto de equipos, que es responsabilidad de software y Networking:

Aire acondicionado: La temperatura se mantiene entre 15ºC y 20ºC. Existen dos instalaciones de aire acondicionado, una localizada en el cuarto de equipos y otra distribuida por toda la empresa, pero el control se encuentra en el departamento de Networking.

Extintor: Existen dos extintores, uno distribuido en el cuarto de equipos y otro localizado afuera del área de Networking. Sin embargo la gente no conoce la forma de utilizar los extintores.

Alarmas contra intrusos: Existe una alarma en la empresa que se activa en los horarios no comerciales, generalmente de noche cuando se cierra la empresa. La alarma se activa con un código que solamente la poseen los coordinadores de cada área, gerencia y presidencia.

Generador de energía: En la empresa cuentan con un generador de energía en el subsuelo, pero a este tiene acceso solamente el personal de administración del edificio.

UPS (Uninterruptible Power Supply): En el cuarto de equipos existen dos UPS pero solamente uno está operativo, éste se utiliza para conectar los servidores. Su tiempo de duración es aproximadamente 15 minutos.

Supresor de sobrevoltaje: Existe un supresor de sobrevoltaje que se conecta a un fax que no se encuentra en el área de Networking.

Puesta a tierra: Existe un sistema de puesta a tierra para el edificio, no se conoce la ubicación exacta; en el departamento de Networking se efectuó la

prueba con un multímetro para comprobar que el sistema de puesta a tierra está correctamente colocado.

La prueba consistió en identificar con un multímetro la fase, neutro y tierra de los toma corrientes del área (gráfico 3.3) y se midió el voltaje entre los tres terminales con los siguientes resultados:

V1 Voltaje Fase - Tierra = 116 V
V2 Voltaje Tierra - Neutro = 0.090 V
V3 Voltaje Fase - Neutro = 116 V

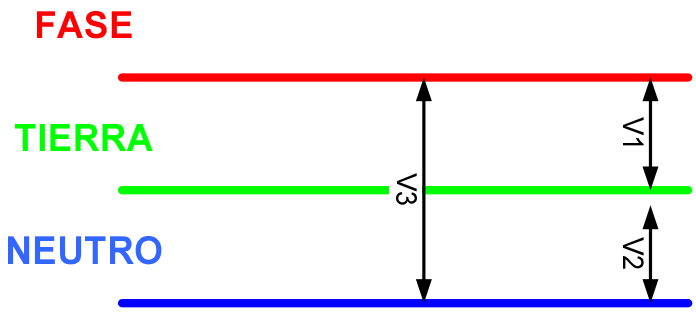


GRÁFICO 3.3 MEDICIONES DE VOLTAJE

Luz de emergencia: En el área en la cual se encuentra el cuarto de equipos existe una luz de emergencia, otra se encuentra localizada en la entrada del área de Networking. En el caso de corte de luz se activa automáticamente.

3.1.3.4.4 Cableado Estructurado

La instalación del cableado en el área de Networking y el cuarto de equipos fue realizada por una tercera empresa, y se implementó un cableado estructurado NO certificado con UTP cat 5e.

Para instalar el cableado de red se tuvieron en cuenta los posibles desastres como inundación, cortes eléctricos, problemas de desagües o campos magnéticos.

Se implementó un techo falso, por donde tendieron el cableado, de fácil accesibilidad ya que se sacan los paneles que lo componen. Desde allí los cables pasan por las columnas del edificio, y se distribuyen a toda la empresa.

En todos los trayectos del cableado se tuvo en cuenta la distancia mínima necesaria entre cables para no provocar interferencias, daños o cortes. Además en la empresa no existen puntos distantes que sobrepasen la distancia máxima permitida según el estándar para el cable.

En el patch panel de Networking existen puntos para continuar con la expansión de la red, incluso existe un patch panel nuevo para instalarlo en caso de requerir más puntos de conectividad.

Los cables en el patch panel de Networking no están debidamente etiquetados y es complicado identificar los puntos de red. Se debe utilizar un seguidor de señal para determinar cuál punto de la pared corresponde al punto en el rack.

En cada escritorio de trabajo de Networking se encuentran:

- Un toma corriente (con instalación a tierra)
- Un jack para teléfono (color blanco)
- Un jack para red (color rojo)

Entre estos jack's y toma corrientes no se producen interferencias debido al trenzado del cable (red y teléfono), y a que la línea eléctrica está aislada de los cables de red y teléfono. Además, la empresa encargada de la instalación de la red midió la interferencia que hay en las bocas de red de las PC's encontrando que eran muy bajas y no representaban riesgos.

Ancho de Banda de la Red.- El cableado (Cat 5e) permite conectarse a 100Mbps (teórico), pero existe broadcast en la red (impresoras y switches) que disminuyen en cierto grado esta tasa de transferencia, sin embargo esto no afecta demasiado el rendimiento de la red.

Para la conectividad con el exterior, el departamento de Networking posee un administrador de ancho de banda que permite asignar a cada usuario o grupo de usuarios un ancho de banda limitado; con el propósito de que no existan saturaciones en la red.

Falla en la Red.- En el departamento de Networking no existe una política de procedimiento a seguir en caso de corte de energía. Solamente se enciende el generador de electricidad y se continúa trabajando.

Si existe otra tipo de falla en la red, el área de Networking no tiene configuradas alarmas para testear la conectividad de los equipos y se espera a que la falla sea reportada.

3.1.3.5 Administración del Cuarto de Equipos

Alcance del Análisis.- El alcance del análisis será evaluar la correcta organización y administración del cuarto de equipos, así como la asignación de tareas y responsabilidades del personal que la conforma, a fin de que ésta brinde condiciones óptimas de operación que posibiliten un ambiente adecuado de control y permitan mejorar la disponibilidad de sus servicios, de acuerdo a las normas existentes que regulan esta actividad.

3.1.3.5.1 Administración del Cuarto de Equipos

No hay responsabilidades puntuales asignadas para el cuarto de equipos de Networking, solamente se conoce que los servidores de correo, Lotus, Black Berry y Help Desk le corresponden a software mientras que los servidores DHCP, DNS y equipos de comunicación le corresponden al área de Networking.

Si existe un problema con los equipos de infraestructura, el administrador de la red debe revisar y apoyarse con técnicos de Networking y software para resolver el problema. Si el problema es mayor entonces el administrador debe solicitar apoyo al fabricante.

Para evitar en cierto grado los problemas de funcionamiento de los equipos, se realiza un mantenimiento preventivo de los equipos de infraestructura y equipos para el trabajo cada seis meses.

Los equipos de infraestructura a cargo de Networking no han sido clasificados formalmente según su prioridad, aunque se puede identificar que los equipos que interconectan a toda la red son los principales, continuando en la escala con las máquinas que utilizan los técnicos para dar soporte.
Cuando un equipo del cuarto de equipos que corresponde al área de Networking es viejo y se debe dar de baja, no existe un procedimiento para hacerlo.

Los cambios que se desean realizar a cualquier equipo de infraestructura primero deben aprobarse por el coordinador y gerencia, y se debe notificar vía email el horario en el cual se va a modificar el equipo.

Los instaladores de las aplicaciones utilizadas en la empresa se encuentran en sus CD’s originales almacenados en carpetas, existen también varios CD’s sin identificar que se encuentran en el área de Networking.

En el cuarto de equipos, todos los servidores tienen licencia original, pero esto está a cargo de software. En el área de Networking los PC’s disponen de licencias originales, sin embargo no existe un registro de licencias utilizadas para las diferentes aplicaciones.

3.1.3.5.2 Capacitación

Cuando ingresa un técnico nuevo al área de Networking, una persona de administración le da una inducción a los procesos y funciones que debe cumplir.

El área de Atención al Cliente es también encargada de dar una inducción acerca del Software utilizado para crear, actualizar y cerrar los casos. Pero la capacitación técnica formal no existe, la inducción es a medida que se visita clientes externos o cuando se dispone de tiempo necesario.

3.1.3.5.3 Backup

Cuando se hace un cambio en la configuración de los equipos de Networking, no se guardan copias de las configuraciones anterior y posterior al cambio, tampoco se documentan los cambios que se realizan ni la fecha de estas modificaciones.

No hay ningún procedimiento formal para la realización ni la recuperación de los backups. Estos se realizan rara vez.

No hay un responsable designado para realizar los backups, aunque generalmente los hace una sola persona, el responsable del área o administrador de la red. Tampoco hay ninguna política en cuanto a asignar un responsable para la restauración de los datos de los backups, esta tarea también la realiza el administrador.

Los backup que se han obtenido se encuentran esparcidos por las computadoras de los técnicos pero sin un registro de fechas.

Referente a los backups de los usuarios de Networking, cada uno debe realizar su backup, ya sea con la utilidad de Windows o quemando en un CD o DVD sus datos.

No se hace ningún backup de los logs generados por las diferentes aplicaciones de los equipos de infraestructura, solo se los almacena en diferentes computadores y se depuran mensualmente.

Los respaldos disponibles no están protegidos con ningún control de acceso ni encriptación. Esta situación puede resultar peligrosa ya que estos archivos contienen información de clientes que sería difícil recuperar.

No hay documentación escrita sobre los datos de los cuales se obtuvo el respaldo, cómo se obtuvo el respaldo, dónde se hace esta copia ni datos históricos referidos a la restauración de los mismos.

3.1.3.5.4 Documentación

El administrador de la red dispone documentación sobre:

Licencias del software y en qué máquinas está instalado, direcciones IP de las máquinas y de los switch.

No hay backups de ninguno de estos datos, se los tiene en digital y se los va modificando manualmente.

Los manuales que se encuentran en el área de Networking, se encuentran clasificados de acuerdo al producto, sin embargo no se encuentran asegurados bajo llave. Algunos se encuentran repetidos o ya son obsoletos.

3.2 GUÍA PARA EL ESTABLECIMIENTO DEL PLAN PILOTO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

3.2.1 INTRODUCCIÓN

La implementación del Plan Piloto de Política de Seguridad Informática PPPSI requiere grandes recursos; por ello la empresa Uniplex Systems está consciente sobre sus razones para implantar el PPPSI.

La razón debe estar documentada y debe contener los costos en contraposición a los beneficios de gestionar la Seguridad Informática.

3.2.2 ALCANCE DEL PPPSI

La definición del alcance es una de las más importantes decisiones en todo el proceso de su establecimiento. El alcance del PPPSI va a depender totalmente de

la empresa, puede contenerla totalmente o simplemente una parte, un simple proceso o un sistema de información.

Una vez determinado el alcance se procede a identificar los distintos activos de información que se convierten en el eje principal del modelo.

3.2.3 ILUSTRACIÓN PARA DEFINIR UN ALCANCE

Como ejemplo, se ha utilizado el Método de las Elipses (que es el más utilizado) y se han determinado brevemente los procesos del departamento de “Networking” de la empresa UNIPLEX Systems S.A.

El método (Gráfico 3.4) consiste en determinar en la elipse más interna los distintos procesos que conforman el proceso de “Networking”, estos son:

- Registro de Llamada
- Verificación tipo de cliente
- Notificación a Ingeniero de Soporte
- Índice de satisfacción de cliente

Se identifican en la elipse intermedia las distintas interacciones que los procesos de la elipse más interna tienen con otros procesos de la organización.

En la elipse más externa, se identifican aquellas organizaciones extrínsecas a la empresa que tienen interacción con los procesos de la elipse concéntrica.
Las flechas indican la interacción entre ambas partes.

El método de las elipses se utiliza como fuente para identificar interfaces, interdependencia con áreas y procesos, así como averiguar los contratos existentes y los grados de acuerdos necesarios. El método también se utiliza para obtener los activos de información, esto se consigue al analizar los procesos identificados y el flujo de información.

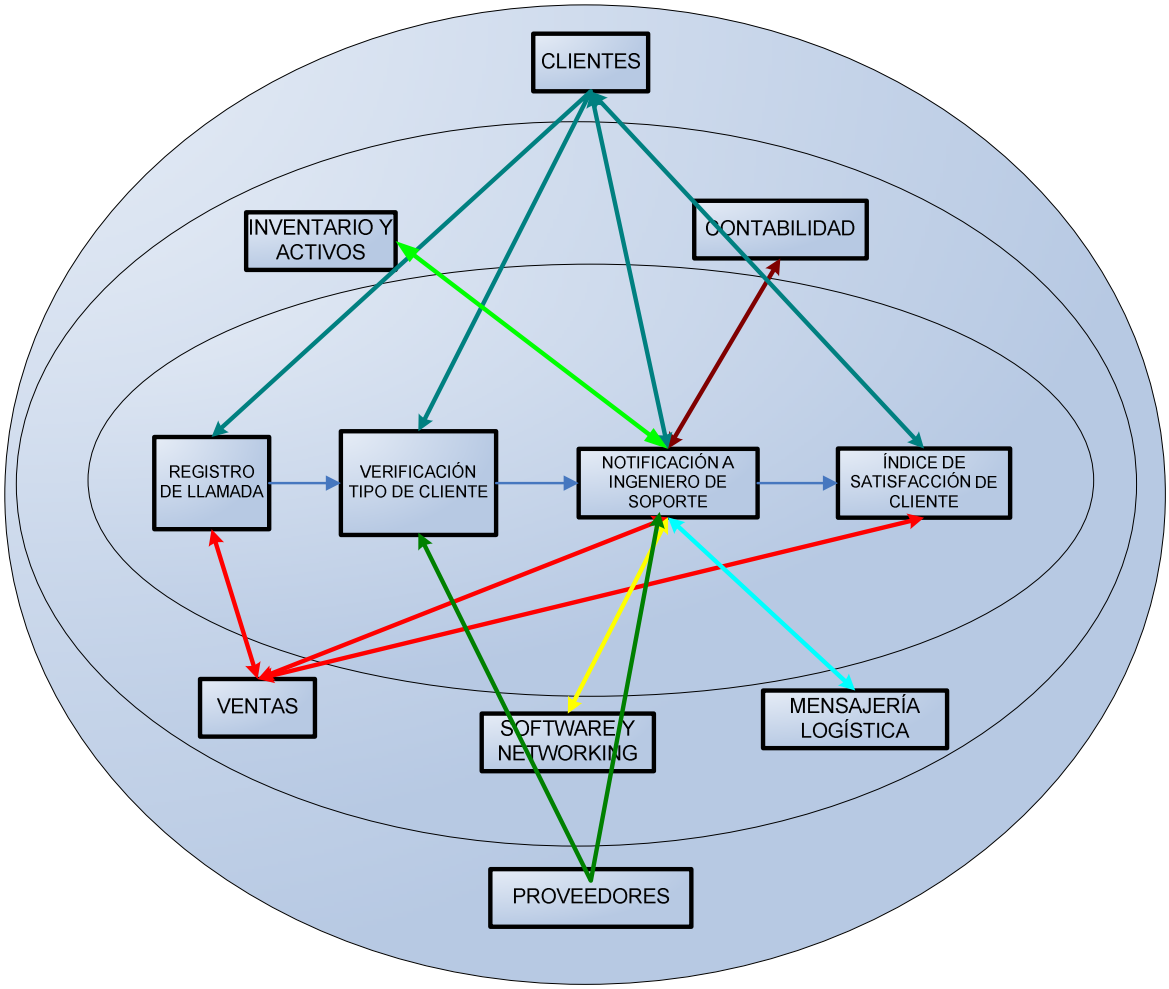


GRÁFICO 3.4 METODOLOGÍA DE LAS ELIPSES EN ATENCIÓN AL CLIENTE

3.2.4 POLÍTICAS DEL PLAN PILOTO DE POLÍTICAS DE SEGURIDAD INFORMATICA (PPPSI)

Una vez establecido el alcance, la empresa define claras políticas de seguridad para apoyar la implementación del PPPSI en la empresa.

La gerencia debe aprobar las políticas, y asegurarse de que todos los empleados las han recibido, entienden su efecto y las ejecutan en sus tareas cotidianas.

3.2.5 ENFOQUE PARA LA GESTIÓN DEL RIESGO

El método de cálculo del riesgo lo puede decidir la organización, pero se debe asegurar que el enfoque sea el adecuado y apropiado para atender los requerimientos organizacionales legales o regulatorios.

El cálculo del riesgo debe ser detallado y complejo como sea necesario, a fin de poder atender todos los requerimientos de la organización y lo requerido por el alcance del PPPSI, pero nada más. El exceso de detalles puede determinar un exceso de trabajo, y un enfoque muy genérico puede conducir a subestimar aspectos de riesgos importantes.

Debe existir un equilibrio entre las tres condiciones básicas para la protección de la información (Confidencialidad, Disponibilidad e Integridad)[18], por ejemplo si la información en un computador está protegida por demasiadas contraseñas difíciles de recordar, y si el responsable por esa información olvida las contraseñas, entonces se pierde la disponibilidad, por otro lado si no tiene ninguna contraseña o ninguna seguridad, entonces se pierde la confidencialidad porque cualquier persona puede acceder a su información.

3.2.6 PROCESO DE CÁLCULO DEL RIESGO

El cálculo de los riesgos de Seguridad Informática para el área de Networking de la empresa Uniplex Systems S.A. incluye el análisis y la evaluación del riesgo.

El análisis del riesgo contempla:

- Identificación de activos de información.
- Identificación de requerimientos legales y comerciales que son relevantes para los activos identificados.

[18] Ver Conceptos en Anexo A

- Tasación de los activos identificados, considerando los requerimientos legales y comerciales, así como los impactos resultantes de una pérdida por confidencialidad, integridad y disponibilidad.
- Identificación de amenazas y vulnerabilidades para cada activo previamente identificado.
- Cálculo de la posibilidad de que las amenazas y vulnerabilidades ocurran.

La evaluación del riesgo contempla:

- Cálculo del riesgo
- Identificación del significado de los riesgos. Esto se hace definiendo criterios y evaluando los riesgos contra una escala predeterminada.

3.2.7 ANÁLISIS DEL RIESGO

3.2.7.1 Identificación de Activos

La identificación de los activos de información en la empresa en el alcance del SGSI (Sistema de Gestión de Seguridad de la Información) es fundamental para su implementación.

Un activo es algo que tiene valor para la organización, sus operaciones y continuidad. Es por esto que los activos necesitan tener protección para asegurar una correcta operación del negocio y una continuidad en las operaciones.

La ISO/IEC 27002 clasifica los activos de información en las siguientes categorías:

- Activos de información (datos, manuales de usuario, etc.).
- Documentos de papel (contratos).
- Activos de software (aplicación, software de sistemas, etc.).
- Activos físicos (computadores, medios magnéticos, etc.).

- Personal (clientes, personal).
- Imagen de la compañía y reputación.
- Servicios (comunicaciones, etc.).

Se puede notar que los activos de información son muy amplios; es fundamental estar conceptualmente claros de qué es un activo de información y conocer sus distintas posibles modalidades, para así poder realizar un correcto análisis y una evaluación del riesgo.

La metodología de las elipses desempeña un papel importante en esta etapa. Con base en este método, la empresa identifica los activos de información.

En la organización, la identificación y tasación de los activos debe realizarlo un grupo de personas que están involucradas en los procesos y subprocesos que abarca el alcance del modelo. Es importante que los dueños (definido en la Descripción de la Norma) de los activos conformen el grupo de identificación y tasación.

3.2.7.2 Identificaciones de Requerimientos Legales y Comerciales Relevantes para los Activos Identificados

Los requerimientos de seguridad para cualquier organización se derivan de tres fuentes:

La primera fuente se deriva de la evaluación de los riesgos que afectan a la organización. Aquí se determinan las amenazas de los activos, luego se ubican las vulnerabilidades, se evalúa su posibilidad de ocurrencia, y se estiman los potenciales impactos.

La segunda fuente es el aspecto legal. Aquí están los requerimientos contractuales que deben cumplirse.

La tercera fuente es el conjunto particular de principios, objetivos y requerimientos para procesar información, que la empresa ha desarrollado para apoyar sus operaciones.

Cuando se identifican los activos de información, se debe analizar si existen requerimientos legales y comerciales relacionados con los activos identificados, de darse este caso, se debe revisar si dichos requerimientos legales involucran otros activos de información.

3.2.7.3 Tasación de Activos

Para realizar la tasación de los activos se establece una escala del 1 al 5; en el cual el 1 significa “muy poco” y 5 “muy alto”. Para poder calificar a cada activo de información, se recomienda efectuar la siguiente pregunta: ¿Cómo una pérdida o falla en un determinado activo afecta la confidencialidad, la integridad y la disponibilidad?

La tabla 3.5 muestra activos de información y su tasación.

ACTIVOS DE INFORMACIÓN	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	TOTAL
Lotus	2	4	5	4
Administrador de base de Datos	5	5	5	5
Técnico	5	2	5	4
Sistema Telefónico	1	1	2	1
Equipo de trabajo	5	5	5	5
Manuales de equipos	1	1	2	1
Información de proveedores	1	1	3	2
CD’s de instalación	1	1	3	2
Archivos de configuración	4	5	1	3
Base de Información	5	5	5	5

TABLA 3.5 TASACIÓN DE ACTIVOS DE INFORMACIÓN

Se debe ejecutar la identificación de los propietarios de cada activo (Tabla 3.6).

ACTIVOS DE INFORMACIÓN	PROPIETARIOS
Lotus	Software
Administrador de base de Datos	Software
Técnico	Servicios profesionales
Sistema Telefónico	Administración
Equipo de trabajo	Servicios profesionales
Manuales de equipos	Servicios profesionales
Información de proveedores	Ventas
CD's de instalación	Networking
Archivos de configuración	Networking
Base de Información	Software

TABLA 3.6 ACTIVOS DE INFORMACIÓN Y PROPIETARIOS

Se recalca que el propietario del activo es responsable por definir apropiadamente la clasificación de seguridad y los derechos de acceso a los activos, y establecer los sistemas de control.

Es recomendable definir también las reglas para el uso aceptable del activo, describiendo acciones permitidas y prohibidas en el uso cotidiano.

3.2.7.4 Identificación de Amenazas y Vulnerabilidades

En las organizaciones, los activos están propensos a las amenazas; "Amenaza es la indicación de un potencial evento no deseado[19]". Para una empresa, las amenazas pueden ser de distintos tipos con base en su origen.

3.2.7.4.1 Clasificación de las Amenazas

Para clasificar las amenazas se aconseja hacerlo por su naturaleza, esto es para facilitar su ubicación.

[19] Alberts y Dorofee, 2003

- Amenazas naturales (inundaciones, tsunamis o maremotos, tornados, huracanes, sismos, tormentas, incendios forestales).
- Amenazas a instalaciones (fuego, explosión, caída de energía, daño de agua, perdida de acceso, fallas mecánicas).
- Amenazas humanas (huelgas, epidemias, materiales peligrosos, problemas de transporte, pérdida de personal clave).
- Amenazas tecnológicas (virus, Hacking, pérdida de datos, fallas de hardware, fallas de software, fallas en la red, fallas en las líneas telefónicas).
- Amenazas operacionales (crisis financieras, pérdida de proveedores, fallas de equipos, aspectos regulatorios, mala publicidad).
- Amenazas sociales (motines, protestas, sabotaje, vandalismo, bombas, violencia laboral, terrorismo).

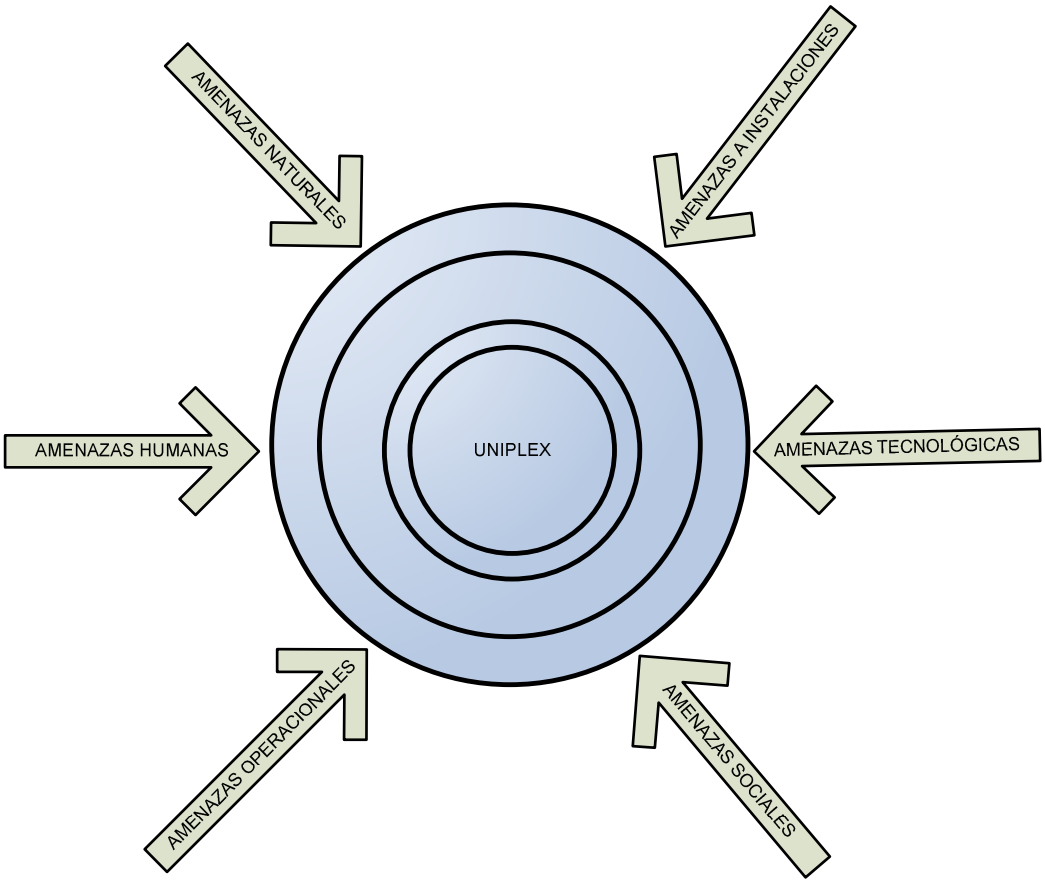


GRÁFICO 3.5 CLASIFICACIÓN DE AMENAZAS

Como se aprecia en el gráfico 3.5; las amenazas pueden originarse de fuentes accidentales o deliberadas, y para que cause daño a los activos de información tendría que afectar una o más vulnerabilidades.

Una vez identificadas las amenazas, se debe evaluar su posibilidad de ocurrencia. La medición de ocurrencia debe hacerla un grupo que tenga conocimiento de la naturaleza de la amenaza y pueda consultar las estadísticas respectivas.

Se recomienda utilizar la escala de Likert para medir la posibilidad de ocurrencia, donde 1 significa “muy bajo” y 5 significa “muy alto”.

En este punto, la empresa debe tomar decisiones importantes en relación con el análisis de las amenazas. La decisión sobre cuáles amenazas se descartan por su baja probabilidad de ocurrencia debe revisarse con detenimiento. Puede ocurrir que la amenaza con menor probabilidad de ocurrencia tenga las consecuencias más severas para la empresa.

3.2.7.4.2 Clasificación de las Vulnerabilidades

Las vulnerabilidades son debilidades de seguridad asociadas con los activos de información de una organización.

“Las vulnerabilidades organizacionales son debilidades en las políticas organizacionales o prácticas que pueden resultar en acciones no autorizadas[20]”

Las vulnerabilidades NO causan daño, simplemente son condiciones que pueden hacer que una amenaza afecte a un activo.

En el gráfico 3.6 se presenta la clasificación de las vulnerabilidades en base a la norma ISO/IEC 27002. La clasificación es de gran ayuda a las empresas, en su proceso de identificación de vulnerabilidades de su sistema de gestión de Seguridad Informática.

[20] Alberts y Dorofee, 2003

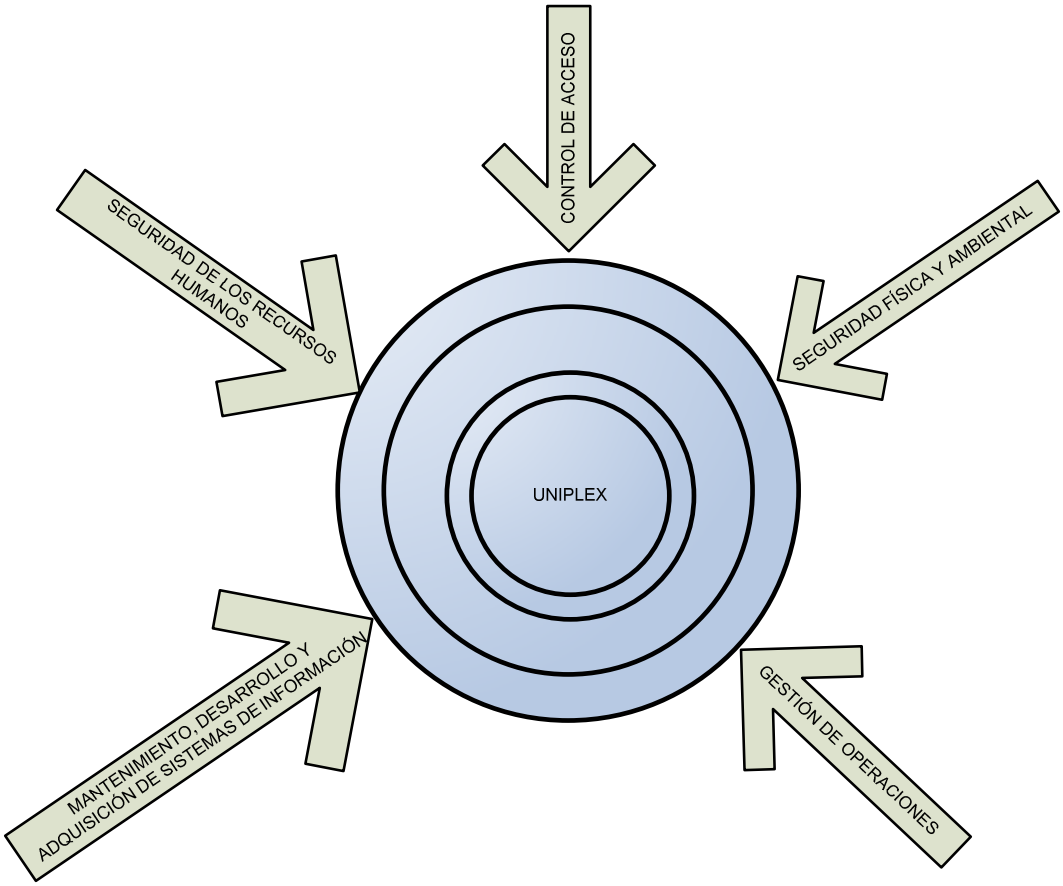


GRÁFICO 3.6 CLASIFICACIÓN DE VULNERABILIDADES

3.2.7.4.3 Descripción de las Categorías de Vulnerabilidades

Las vulnerabilidades pueden clasificarse como:

- Seguridad de los recursos humanos (falta de entrenamiento en seguridad, carencia de toma de conciencia en seguridad, falta de mecanismos de monitoreo, falta de políticas para el uso correcto de las telecomunicaciones, no eliminar los accesos al término del contrato de trabajo, carencia de procedimientos que asegure la entrega de activos al término del contrato de trabajo, empleados desmotivados).

- Control de acceso (segregación inapropiada de redes, falta de política sobre escritorio y pantalla limpia, falta de protección al equipo de

comunicación móvil, política incorrecta para control de acceso, password sin modificarse).

- Seguridad física y ambiental (control de acceso físico inadecuado a oficinas, salones y edificios, ubicación en áreas sujetas a inundaciones, almacenes desprotegidos, carencia de programas para sustituir equipos, mal cuidado de equipos, susceptibilidad de equipos a variaciones de voltaje).

- Gestión de operaciones y comunicación (complicadas interfaces para usuarios, control de cambio inadecuado, gestión de red inadecuada, carencia de mecanismos que aseguren el envío y recepción de mensajes, carencia de tareas segregadas, carencia de control de copiado, falta de protección en redes públicas de conexión).

- Mantenimiento, desarrollo y adquisición de sistemas de información (protección inapropiada de llaves criptográficas, políticas incompletas para el uso de criptografía, carencia de validación de datos procesados, carencia de ensayos de software, documentación pobre de software, mala selección de ensayos de datos).

Una vez identificadas las vulnerabilidades, por cada una de ellas, se debe evaluar la posibilidad de que sean explotadas por la amenaza. Se recomienda utilizar la escala de Likert para medir la posibilidad de ocurrencia, donde 1 significa “muy bajo” y 5 significa “muy alto”.

Para que un activo pueda ser afectado, es necesario que la vulnerabilidad y la amenaza se presenten en ese activo. La pregunta fundamental es: ¿Qué amenaza pudiese explotar cuál de las vulnerabilidades?

Entre las amenazas, existen las vulnerabilidades, los riesgos y los activos de información, una secuencia de relación de causalidad y probabilidad de

ocurrencia. Se presenta un gráfico (gráfico 3.7) con la relación causa-efecto entre activos, riesgo, vulnerabilidad y amenaza.

En algún momento previo al inicio de las actividades del cálculo del riesgo, o antes de identificar las amenazas y vulnerabilidades, deben identificarse los controles ya existentes en el sistema para medir su eficacia. Un control ineficaz es una vulnerabilidad.

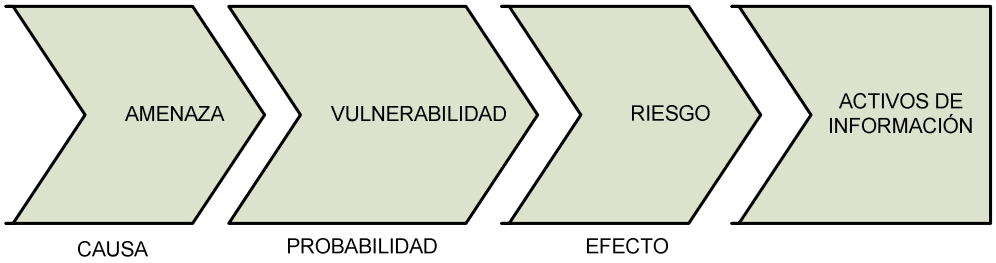


GRÁFICO 3.7 RELACIÓN CAUSA-EFECTO ENTRE ELEMENTOS DEL ANÁLISIS DEL RIESGO

3.2.7.5 Cálculo de las Amenazas y Vulnerabilidades

Una vez identificadas las amenazas y vulnerabilidades es necesario calcular la posibilidad de que puedan juntarse y causar un riesgo. El riesgo se define como: "La probabilidad de que una amenaza pueda explotar una vulnerabilidad en particular[21]"; este cálculo se realiza en base a la escala de Likert.

Es muy conveniente calcular la posibilidad de la presencia de amenazas; para este fin se deben considerar los siguientes aspectos de las amenazas:

Amenazas deliberadas.- La posibilidad de amenazas deliberadas en la motivación, conocimiento, capacidad y recursos disponibles para posibles atacantes y la atracción de los activos para sofisticados atacantes.

Amenazas accidentales.- La posibilidad de amenazas accidentales puede estimarse utilizando la experiencia y la estadística.

[21] Peltier, 2001

Incidentes del pasado.- Los incidentes ocurridos en el pasado ilustran los problemas en el actual sistema de protección.

Nuevos desarrollos y tendencias.- Esto incluye informes, novedades y tendencias obtenidas de diferentes medios, como Internet.

3.2.7.6 Análisis del Riesgo y su Evaluación

El análisis del riesgo ayuda a identificar y calcular los riesgos basados en la identificación de los activos, y en el cálculo de las amenazas y vulnerabilidades.

Los riesgos se calculan de la combinación de los valores de los activos, que expresan el impacto de pérdidas por confidencialidad, integridad y disponibilidad y del cálculo de la posibilidad de que amenazas y vulnerabilidades relacionadas se junten y causen un incidente. (Tabla 3.7)

Los niveles de riesgo calculados sirven para poder priorizar e identificar los más problemáticos.

ACTIVO	AMENAZA	IMPACTO DE LA AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICIÓN DEL RIESGO	PRIORIZACIÓN
Software	Virus	3	5	15	2
Software	Falla de energía	2	2	4	4
Técnico	Accidente	4	2	8	3
Técnico	Venta de información	4	4	16	1

TABLA 3.7 MÉTODO PARA EL CÁLCULO DEL RIESGO

El método que se utiliza en el presente trabajo consiste en relacionar los factores del impacto de la amenaza y la probabilidad de ocurrencia de la amenaza. El primer paso consiste en evaluar el impacto económico de la amenaza; usando una escala predefinida, se recomienda una escala de Likert, donde 1 es bajo y 5 es alto.

El paso siguiente consiste en utilizar la misma escala para medir la posibilidad de ocurrencia de la amenaza. El tercer paso consiste en calcular la medición del riesgo, multiplicando los valores obtenidos del impacto económico de la amenaza y el de la posibilidad de ocurrencia de la amenaza. Finalmente, las amenazas pueden ser priorizadas en orden, con base en su factor de exposición al riesgo.

3.2.8 EVALUACIÓN DEL RIESGO

3.2.8.1 Evaluación del Riesgo

Para realizar la evaluación del riesgo, se debe determinar cuáles son aquellas amenazas cuyos riesgos son los más relevantes.

Para determinar los más relevantes, se utiliza la escala de Likert y los siguientes criterios:

- Impacto económico del riesgo.
- Tiempo de recuperación de la empresa.
- Posibilidad real de ocurrencia del riesgo.
- Posibilidad de interrumpir las actividades de la empresa.

Se ilustra en la Tabla 3.8 la forma en que se debe evaluar el significado del riesgo.

RIESGO		**CRITERIO PARA EVALUAR LA IMPORTANCIA DEL RIESGO**				
Activos	Amenazas	Impacto Económico del Riesgo	Tiempo de Recuperación de la Empresa	Probabilidad de Ocurrencia del Riesgo	Probabilidad de Interrumpir Actividades de la empresa	TOTAL

TABLA 3.8 ESCALA DE RIESGO PARA EVALUAR SIGNIFICADO DEL RIESGO

3.2.8.2 Tratamiento del Riesgo y el Proceso de Toma de Decisión Gerencial

Una vez efectuados el análisis y la evaluación del riesgo, se debe decidir las acciones a tomar con esos activos. Se puede aplacar los riesgos mediante los controles de la norma.

3.2.8.3 Proceso de Toma de Decisiones

Cuando se ha calculado el riesgo, se debe iniciar un proceso de toma de decisiones para determinar qué va a ocurrir con el riesgo, la decisión está principalmente influenciada por los objetivos de la organización pero por lo general siempre está ligada con estos dos factores:

- El posible impacto si el riesgo se pone de manifiesto
- Que tan frecuente puede suceder

3.2.8.4 Estrategias Posibles para el Tratamiento del Riesgo

3.2.8.4.1 Reducción del Riesgo

Si la decisión de reducir el riesgo fue elegida, es importante determinar con exactitud los controles que permiten cumplir con esta decisión. Los controles reducen el riesgo de dos maneras:

- Reduciendo la posibilidad de que la vulnerabilidad sea explotada por la amenaza.
- Reduciendo el posible impacto si el riesgo ocurriese, detectando eventos no deseados, reaccionando y recuperándose de ellos.

No existe un método general para seleccionar objetivos de control y controles. Este proceso involucra numerosas decisiones y consultas, usualmente

discusiones con distintas partes de la organización y con un determinado número de personas clave. En fin, la selección de los controles debe producir un resultado que más se adecúe a la organización en términos de sus requerimientos.

3.2.8.4.2 Objetivamente Aceptar el Riesgo

Algunas veces se presenta el caso en el cual la organización no encuentra controles para mitigar el riesgo, y en la mayoría de estas ocasiones la implantación de los controles tiene un costo mayor que las consecuencias del riesgo. Con este panorama, la decisión de aceptar el riesgo es la más adecuada.

Se debe documentar la aceptación del riesgo y definir el criterio de aceptación. La gerencia debe aprobar y firmar la decisión de aceptación del riesgo.

3.2.8.4.3 Transferencia del Riesgo

Cuando se presenta la situación en la cual es difícil reducir o controlar el riesgo a un nivel aceptable se puede transferir el riesgo a una tercera parte.

Se puede utilizar una aseguradora para la transferencia del riesgo, pero se debe tener mucho cuidado con el riesgo residual. El contrato con las empresas aseguradoras siempre tendrá exclusiones y condiciones que se aplicarán de acuerdo con la clase de ocurrencia.

Se debe analizar la transferencia del riesgo a la aseguradora para determinar cuánto del riesgo actual será transferido; en muchas ocasiones, las empresas aseguradoras no eliminan inmediatamente un evento de accidente.

Si se utiliza la tercerización para que se manejen activos, se debe recordar que la responsabilidad siempre está en la misma organización y no en la prestadora de servicios.

3.2.8.4.4 Evitar el Riesgo

Por evitar el riesgo se entiende cualquier acción orientada a cambiar las actividades, o la manera de desempeñar una actividad comercial en particular.
El riesgo puede evitarse por medio de:

- No desarrollar ciertas actividades comerciales (la no utilización de Internet)
- Mover los activos de un área de riesgo
- Decidir no procesar información crítica.

Se presenta en forma esquemática el proceso de toma de decisiones para elegir una opción de tratamiento del riesgo (Gráfico 3.8).

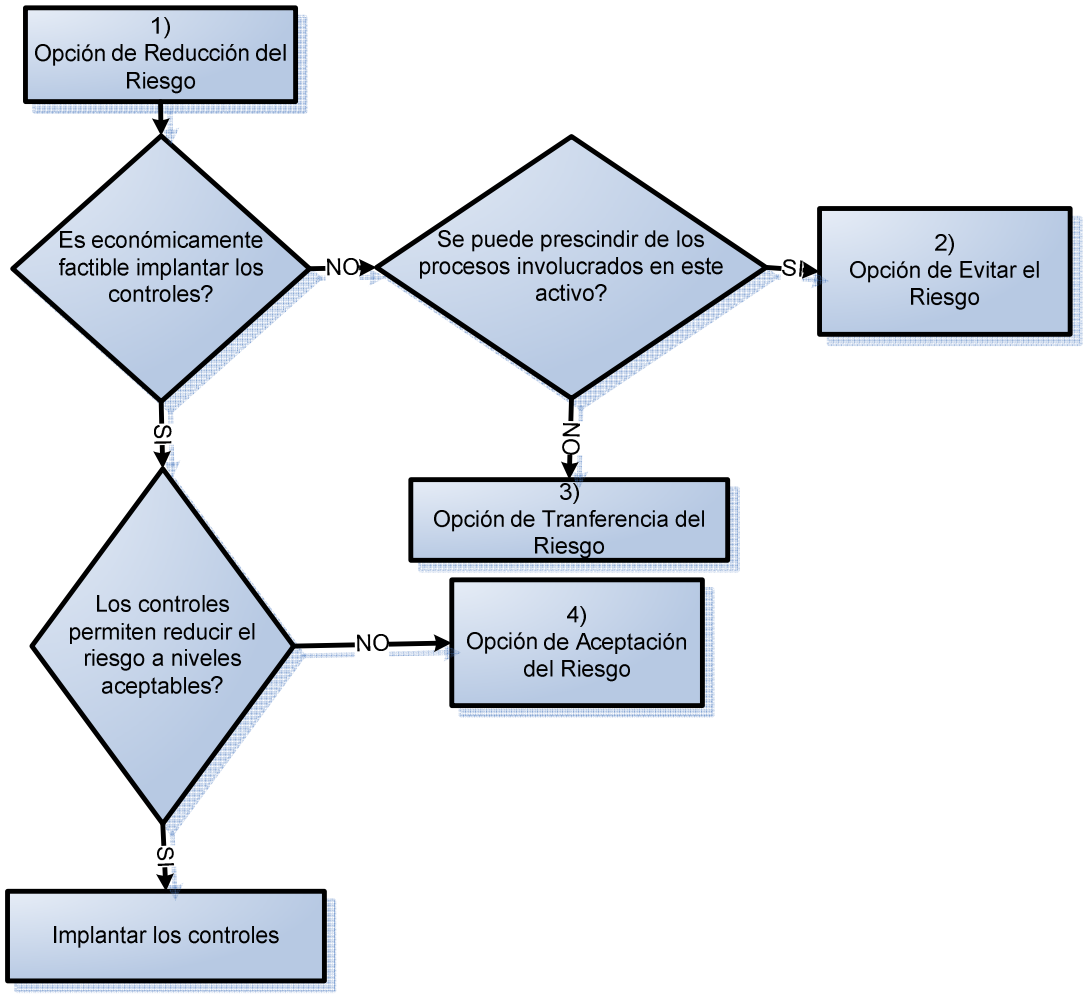


GRÁFICO 3.8 PROCESO DE TOMA DE DECISIONES PARA LA ELECCIÓN DE UNA OPCIÓN DE TRATAMIENTO DEL RIESGO

3.2.9 RIESGO RESIDUAL

El riesgo residual es el riesgo remanente que siempre está presente al implementar las decisiones del tratamiento del riesgo. Puede ser difícil de calcular pero al menos debe realizarse una evaluación para asegurar que logra la protección suficiente.

Si es inaceptable tener riesgo residual, deben tomarse decisiones para resolverlo. Se puede aplicar más controles, establecer arreglos con aseguradoras para lograr reducir el riesgo a niveles aceptables.

En algunas situaciones, el reducir el riesgo a niveles aceptables puede no ser posible o representar un costo exageradamente elevado. En este caso, se aplicaría la estrategia de aceptación del riesgo.

La gerencia debe aprobar los riesgos residuales propuestos, y efectuar evaluaciones a intervalos planeados, y revisar el nivel de riesgo residual y de riesgo aceptable identificado.

3.2.9.1 Seleccionar Objetivos de Control y Controles para el Tratamiento de Riesgos

Una vez identificados los procesos de tratamiento del riesgo y haberlos evaluado, se debe decidir qué objetivos de control y controles se van a implementar.

La selección de objetivos de control y controles debe hacerse tomando en cuenta el criterio establecido para la aceptación del riesgo, así como los requerimientos legales, reguladores y contractuales. Como se puede notar, la ISO/IEC 27002 contiene gran número de controles para poder aplicarlos en la empresa.

3.2.9.2 Preparación de la Declaración de Aplicabilidad

La declaración de aplicabilidad es un documento importante del SGSI, que debe incluir los objetivos de control y controles que serán aplicados y los que serán

excluidos. La declaración de aplicabilidad da la oportunidad a la empresa de que asegure que no ha omitido algún control.

En la Tabla 3.9 se presenta un ejemplo de enunciado de aplicabilidad.

Objetivos de Control	Controles	Aplicabilidad		Justificación
		SI	NO	
5.1 Política de Seguridad de Información	Documento de Políticas de Seguridad Informática	X		Es necesario establecer las políticas de seguridad, y revisarlas periódicamente. Se debe revisar periódicamente estas políticas para asegurar que se mantengan adecuadas
	Revisión de las Políticas de Seguridad Informática	X		
6.1 Organización Interna	Compromiso de la Dirección con la Seguridad de la Información	X		Es necesario tener controles y políticas para el manejo de la Seguridad Informática dentro de la organización.
	Coordinación de la Seguridad Informática	X		
	Asignación de responsabilidades para la Seguridad Informática	X		
	Proceso de autorización para los servicios de procesamiento de información	X		
	Acuerdos sobre confidencialidad	X		
	Contacto con las autoridades	X		
	Contactos con grupos de intereses especiales	X		
	Revisión independiente de la Seguridad Informática	X		
	Documento de políticas de Seguridad Informática	X		

TABLA 3.9 DECLARACIÓN DE APLICABILIDAD PROCESO CAPTACIONES

3.2.9.3 Plan de Tratamiento del Riesgo

Una vez establecido el tratamiento del riesgo, se debe identificar y planear las actividades. Cada actividad de implementación debe ser identificada con claridad y descomponerse en subactividades para poder distribuir a las personas.

Las actividades que se consideran fundamentales para formular el plan de tratamiento del riesgo son:

- Identificar, con la precisión requerida, los factores limitadores del proyecto y establecer la estrategia para debilitarlos.
- Establecer las prioridades del proyecto.
- Identificar con claridad las fechas de entrega, lo mismo que los hitos del proyecto.
- Estimar los requerimientos de recursos y a la vez identificar los recursos.
- Identificar la ruta crítica del proyecto.

3.2.9.4 Mantenimiento y Monitoreo del SGSI

Todo proyecto debe ser revisado con regularidad, de igual forma ocurre con los objetivos de control y controles que se implementan. Como se sabe, a medida que transcurre el tiempo, los servicios o mecanismos se deterioran, por ello, el monitoreo tiene el propósito de detectar el deterioro e iniciar las acciones correctivas de lugar.

Como actividades de monitoreo y mantenimiento del SGSI se tienen:

- Detectar los eventos de seguridad, y evitar así los incidentes de seguridad, al utilizar los indicadores.
- Determinar si las acciones tomadas son efectivas para resolver una violación de seguridad.
- Establecer criterios para medir la efectividad de los controles para verificar que se hayan cumplido los requerimientos de seguridad.
- Revisar las evaluaciones del riesgo a intervalos planeados, y revisar el nivel del riesgo residual y el riesgo aceptable identificados.
- Realizar auditorías SGSI internas a intervalos planeados.
- Realizar inversiones gerenciales del SGSI sobre una base regular para asegurar que el alcance es el adecuado, y se identifiquen las mejoras en el proceso SGSI.

3.2.9.5 Revisión de los Riesgos y Evaluación

Se deben revisar los resultados del análisis y la evaluación del riesgo para visualizar cualquier modificación.

La constante evolución de la empresa y la tecnología hace que surjan nuevos activos de información o sean alterados los ya existentes.

Las revisiones en la organización, medición de la eficacia de los controles y la aparición de nuevas amenazas y vulnerabilidades puede afectar el escenario de los riesgos.

Existen numerosas fuentes que pueden ocasionar la aparición de nuevos riesgos, cuando se detecta el nuevo riesgo se debe recalcular e identificar las alteraciones en las opciones de tratamiento del mismo, así como las modificaciones pertinentes en los objetivos de control y controles determinados y documentados.

3.3 ESTABLECIMIENTO DEL PLAN PILOTO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

Con el análisis de las políticas de Seguridad Informática precedentes en el área de Networking se pudo determinar cuáles políticas están siendo aplicadas y cuáles podrían hacer falta. A continuación se establece el Plan Piloto de Políticas de Seguridad Informática PPPSI.

3.3.1 ALCANCE DEL PLAN PILOTO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA (PPPSI)

El alcance del PPPSI será el área de Networking de la empresa Uniplex Systems S.A. Quito.

3.3.2 ILUSTRACIÓN DEL ALCANCE

Se utiliza el método de las elipses para lo cual se han determinado los procesos del departamento de “Networking” de la empresa UNIPLEX Systems S.A.

En el centro del gráfico 3.9 se aprecian los procesos que conforman el departamento de Networking:

- Asignación a Técnico
- Diagnóstico de Problema
- Planificación de Asistencia e Implementación
- Informe Técnico

Se identifican en la elipse intermedia las distintas interacciones que los procesos de la elipse más interna tienen con el área de: servicio al cliente, mensajería, inventario de activos y ventas.

En la elipse más externa se tiene a los proveedores y clientes. Las flechas en ambos sentidos indican que la interacción entre las partes es bidireccional.

Así pues, el proceso de “Asignación de Técnico” se relaciona con los procesos “Servicio al Cliente” y “Ventas” (flecha roja); el proceso de “Diagnóstico de Problema” se relaciona con “Clientes” (flecha verde); “Planificación de Asistencia e Implementación” se relaciona con “Servicio al Cliente”, “Mensajería”, “Inventario de activos” , “Clientes” y “Proveedores” (flecha Azul) y el proceso “Informe Técnico” se relaciona con “Servicio al Cliente”, “Mensajería” y “Ventas”.

La persona del proceso “Servicio al Cliente” es quien se encarga de entregar el informe técnico y de facturar al cliente las horas de soporte.

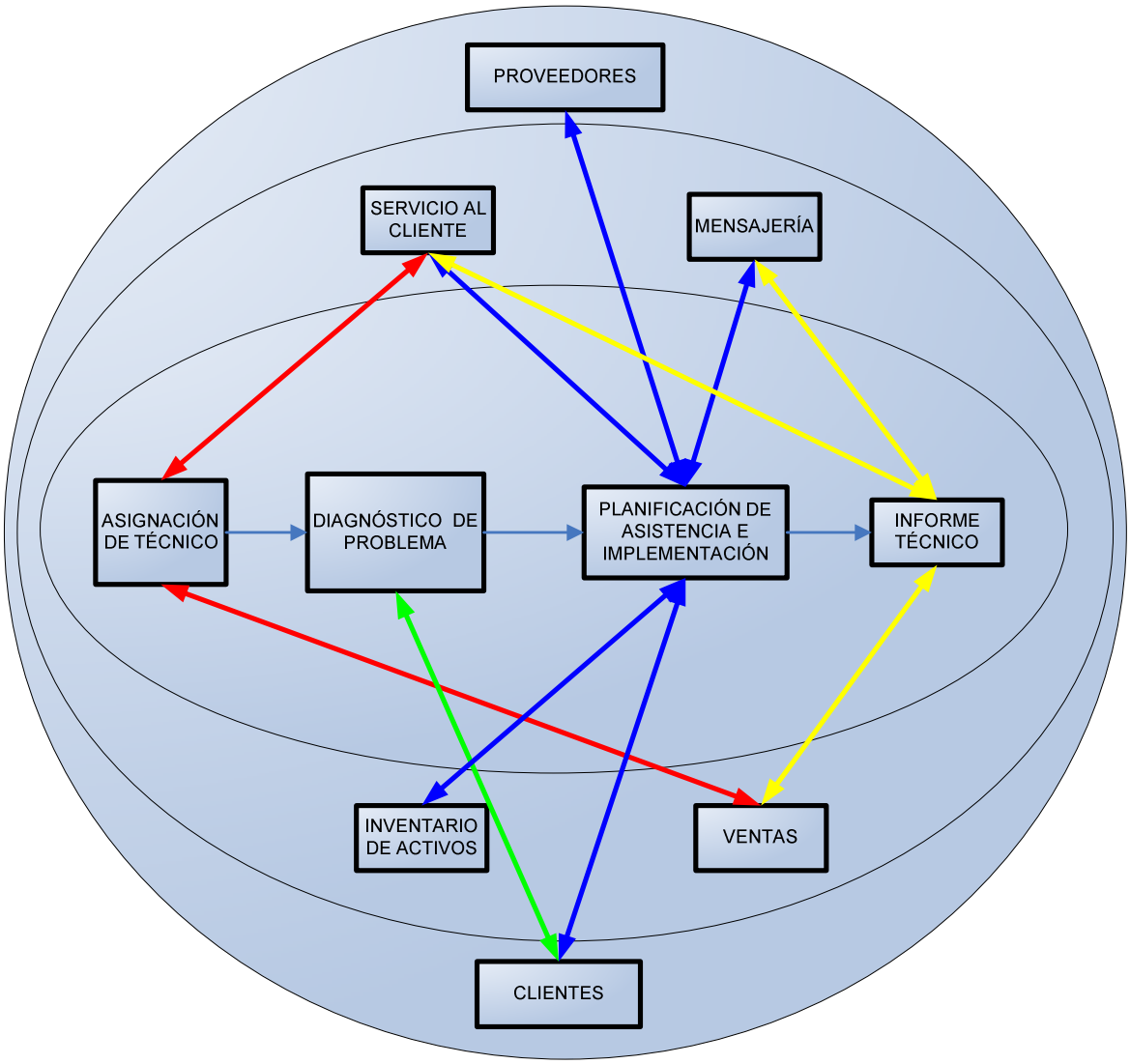


GRÁFICO 3.9 METODOLOGÍA DE LAS ELIPSES EN NETWORKING

3.3.3 POLÍTICAS DEL PLAN PILOTO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA PPPSI

Las políticas definidas para apoyar la implementación del Plan Piloto de Políticas de Seguridad Informática son:

La tecnología de información y los sistemas de información son de vital importancia como activos en el departamento de Networking de la empresa Uniplex Systems S.A.

Sin un sistema de información y sus respectivas tecnologías de información, confiables y seguras, la empresa afectaría su desarrollo de actividades y operaciones tanto activas como pasivas.

La administración del riesgo operacional y tecnológico es directamente proporcional a la gestión vía políticas y controles de sus sistemas de información.

Los colaboradores de Networking asumen una responsabilidad individual respecto a los criterios de confidencialidad, integridad y disponibilidad de los sistemas y tecnologías de información, así como del uso de información privilegiada en la institución. Lo cual refleja un compromiso personal de cada uno de ellos hacia los clientes externos e internos del la empresa. Estos conceptos se utilizarán para establecer los criterios para la evaluación del riesgo.

El área de Networking de la empresa Uniplex Systems debe tener un Plan Piloto de Políticas de Seguridad Informática, con la finalidad de mitigar riesgos operativos y de tecnología de información, fortalecer la cultura de administración de riesgos en función del desarrollo de valores éticos y morales respecto a la Seguridad Informática y fomentar en los colaboradores la responsabilidad del manejo de la Seguridad Informática, desde la perspectiva de la confidencialidad, la integridad y la disponibilidad de la información.

Previo a la implementación del PPPSI es necesario efectuar un análisis de la situación actual de políticas de Seguridad Informática, este análisis se encuentra en el literal 3.1.

3.3.4 ENFOQUE PARA LA GESTIÓN DEL RIESGO

El enfoque estará determinado por documentación en la cual se registrarán los siguientes aspectos:

- Los criterios para la aceptación del riesgo de la organización.
- Identificación de los niveles aceptables del riesgo para la organización.

- Cobertura de todos los aspectos del alcance del PPPSI, de tal manera que incluya todos los controles de los tres dominios de la norma ISO/IEC 27002.
- La relación costo-beneficio y verificar el buen balance entre el gasto en recursos contra el deseado grado de protección, y asegurando que los recursos gastados sean correlacionados con la potencial pérdida y el valor de los activos protegidos.

3.3.5 ASPECTOS A CONTEMPLAR AL EFECTUAR EL ANÁLISIS DEL RIESGO

Se desarrolla el Análisis y Evaluación del riesgo que comprende:

- Identificación de Activos
- Identificación de requerimientos legales y comerciales
- Tasación de activos
- Identificación de amenazas, vulnerabilidades y probabilidad de ocurrencia
- Análisis del riesgo y su evaluación
- Aspectos a contemplar al efectuar la evaluación del riesgo

3.3.5.1 Identificación de Activos

En la tabla 3.10 se presentan los activos identificados en el área de Networking.

ÍTEM	ACTIVOS DE INFORMACIÓN	PROPIETARIOS
1	Correo	Software
2	Help Desk	Software
3	Administrador de Red	Networking y Software
4	Central Telefónica	Administración
5	Técnico	Networking
6	Conexión a Internet	Networking
7	Información de Clientes y Proveedores	Networking y Ventas
8	Equipo de trabajo	Networking
10	Mensajero	Administración

TABLA 3.10 ACTIVOS DE NETWORKING

3.3.5.2 Identificación de Requerimientos Legales y Comerciales Relevantes para los Activos Identificados

Los equipos que se encuentran en Networking suelen alquilarse a clientes para que reemplacen sus equipos en caso de fallas. Al momento no existen contratos vigentes con clientes así que los equipos de Networking no deben cumplir ningún cumplimiento legal.

Referente al requerimiento comercial no existe en Networking equipo para la venta, este equipo se encuentra inventariado en otra bodega y ésta pertenece al departamento de ventas y administración.

3.3.5.3 Tasación de Activos

ÍTEM	ACTIVOS DE INFORMACIÓN	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	TOTAL
1	Correo	4	5	5	5
2	Help Desk	3	3	3	3
3	Administrador de red	5	4	5	5
4	Central Telefónica	2	2	1	2
5	Técnico	5	4	3	4
6	Conexión a Red e Internet	2	3	5	3
7	Información clientes y proveedores	5	4	4	4
8	Equipo de trabajo	5	5	5	5
9	Inventario (equipos disponibles)	1	2	4	2
10	Mensajero	2	3	1	2
11	Cobrador	1	1	1	1
12	Backups	1	2	2	2
13	Manuales	1	1	2	1

TABLA 3.11 TASACIÓN DE ACTIVOS DE INFORMACIÓN

Se realiza la tasación de los activos y se califica su confidencialidad, integridad y disponibilidad siguiendo la escala de Likert[22] aplicando la siguiente pregunta *¿Cómo una pérdida o falla en un determinado activo afecta la confidencialidad, la integridad y la disponibilidad?*

[22] Escala en donde 1 es bajo y 5 es alto.

La tabla 3.11 muestra los activos de información y su tasación.

Se identifican los propietarios de cada activo en la tabla 3.12. En el proyecto se tomarán en cuenta los activos que pertenecen a Networking.

ÍTEM	ACTIVOS DE INFORMACIÓN	PROPIETARIOS
1	Correo	Software
2	Help Desk	Software
3	Administrador de Red	Networking y Software
4	Central Telefónica	Administración
5	Técnico	Networking
6	Conexión a Red e Internet	Networking
7	Información de Clientes y Proveedores	Networking y Ventas
8	Equipo de trabajo	Networking
10	Mensajero	Administración

TABLA 3.12 ACTIVOS DE INFORMACIÓN Y PROPIETARIOS

3.3.5.4 Identificación de Amenazas, Vulnerabilidades y la Probabilidad de que la Amenaza pueda Explotar la Vulnerabilidad

A continuación se desarrolla la identificación de las amenazas y vulnerabilidades para cada uno de los activos de información que pertenece al área de Networking.

- Administrador de Red
- Técnico
- Conexión a Red e Internet
- Información de Clientes y Proveedores
- Equipo de Trabajo

En la tabla 3.13 se presentan las Amenazas y Vulnerabilidades encontradas en el área de Networking y la posibilidad de que la amenaza explote la vulnerabilidad de la empresa Uniplex Systems S.A.

ÍTEM	ACTIVOS DE INFORMACIÓN	AMENAZAS	VULNERABILIDADES	POSIBILIDAD DE QUE VULNERE
1	Administrador de red	Enfermedad o muerte	Accidente	1
			No cuidar la salud	1
		Cambio de empleo	No tener buen sueldo	2
		Fuga de información	No existe sistema de vigilancia	2
			Acceso sin restricciones	3
			No revisar a las personas que entran y salen	1
			No definir deberes y responsabilidades	3
			No tener experiencia	2
		Daño Voluntario	No tener empleado responsable	1
			Empleado estresado o irritado	1
		Robo de Equipos	Armarios sin seguros	3
			Muchas llaves sin identificar	1
2	Técnico	Enfermedad o muerte	Accidente	1
			No cuidar la salud	1
		Cambio de empleo	No tener buen sueldo	2
		Fuga de información	No existe sistema de vigilancia	2
			Acceso sin restricciones	3
			No revisar a las personas que entran y salen	1
			No definir deberes y responsabilidades	3
			No tener experiencia	2
		Daño Voluntario	No tener empleado responsable	1
			Empleado estresado o irritado	1
		Robo de Equipos	Armarios sin seguros	3
			Muchas llaves sin identificar	1
3	Conexión a Red e Internet	Virus	No tener instalado un antivirus	2
			No actualizar el antivirus	4
			No escanear los equipos regularmente	5
			No disponer de licencia de antivirus	1
		Fallas de red	Cableado inadecuado no certificado	5
			No monitorear frecuentemente	4
			No tener enlace de backup	2
			Fallas en UPS	2
		Hackers	Puertos no protegidos en el Firewall	1
			Backdoors Habilitados	1
			No haber configurado seguridades en la red	3
		Desastres naturales	Infraestructura inadecuada	1
		Fallas de Proveedor	No tener otro proveedor	1
			No tener un convenio SLA (Service Level Agreement)	1

TABLA 3.13 AMENAZAS Y VULNERABILIDADES

ÍTEM	ACTIVOS DE INFORMACIÓN	AMENAZAS	VULNERABILIDADES	POSIBILIDAD DE QUE VULNERE
4	**Información de clientes y proveedores**	Virus	No tener instalado un antivirus	2
			No actualizar el antivirus	4
			No escanear los equipos regularmente	5
			No disponer de licencia de antivirus	1
		Daños Físicos	Equipos con información siempre encendidos	2
			Fallas de Hardware	1
		Fuga de información	Todos tienen acceso a la información	2
			Información exclusiva no está encriptada	2
			No tener experiencia	2
5	**Equipo de trabajo**	Robo de Equipos	No tomar precaución en la calle	2
			Equipos sin seguro en la Oficina	3
			No tener identificados los equipos y manuales	2
			Todos tienen acceso a manuales de equipos	3
			Inventario no actualizado	4
		Virus	No tener instalado un antivirus	2
			No actualizar el antivirus	4
			No escanear los equipos regularmente	5
			No disponer de licencia de antivirus	1
		Daños Físicos	Equipos viejos	3
			No dar mantenimiento preventivo	3
			No existen normas de seguridad	2
			No existen suficientes repuestos o respaldos	3
			No existe capacitación en caso de accidente	2
			No tener infraestructura	1

TABLA 3.13 AMENAZAS Y VULNERABILIDADES (CONTINUACIÓN)

3.3.5.5 Análisis de Riesgo y su Evaluación

ÍTEM	ACTIVOS DE INFORMACIÓN	AMENAZAS	IMPACTO DE LA AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICIÓN DEL RIESGO	PRIORIZACION
1	Administrador de red	Enfermedad o Muerte	2	1	2	3
		Cambio de empleo	2	1	2	3
		Fuga de información	3	1	3	2
		Daño Voluntario	2	1	2	3
		Robo de Equipos	4	1	4	1
2	Técnico	Enfermedad o Muerte	2	1	2	3
		Cambio de empleo	2	1	2	3
		Fuga de información	2	3	6	1
		Daño Voluntario	1	1	1	5
		Robo de Equipos	4	1	4	2
3	Conexión a Red e Internet	Virus	2	4	8	2
		Fallas de red	2	5	10	1
		Hackers	3	1	3	5
		Desastres naturales	5	1	5	3
		Fallas de Proveedor	2	2	4	4
4	Información de clientes y proveedores	Virus	2	4	8	1
		Daños Físicos	2	2	4	2
		Fuga de información	3	1	3	3
5	Equipo de Trabajo	Robo de Equipos	3	1	3	3
		Dañados Físicamente	2	2	4	2
		Virus	2	4	8	1

TABLA 3.14 ANÁLISIS DE RIESGO Y SU EVALUACIÓN

En la Tabla 3.14 se tabula el Impacto de la amenaza, probabilidad de ocurrencia, medición del riesgo y priorización para los activos que le corresponden a Networking.

El impacto de la amenaza y la probabilidad de ocurrencia son obtenidos con la escala de Likert, la medición del riesgo es el producto de estos valores y la priorización es el orden de importancia en base a la medición del riesgo (el de mayor valor es el de prioridad uno, el siguiente es de prioridad dos, y así sucesivamente; si existen valores similares entonces tienen la misma prioridad).

3.3.5.6 Aspectos a Contemplar al Efectuar la Evaluación del Riesgo

3.3.5.6.1 Evaluación del Riesgo

Para realizar la evaluación del riesgo, se determinan aquellas amenazas cuyos riesgos son los más relevantes utilizando la escala de Likert y los siguientes criterios:

- Impacto económico del riesgo.
- Tiempo de recuperación de la empresa.
- Probabilidad real de ocurrencia del riesgo.
- Probabilidad de interrumpir las actividades de la empresa.

Se ilustra en la tabla 3.15 la forma en que se debe evaluar el significado del riesgo.

RIESGO		CRITERIO PARA EVALUAR LA IMPORTANCIA DEL RIESGO				
ACTIVOS	**AMENAZAS**	**IMPACTO ECONÓMICO DEL RIESGO**	**TIEMPO DE RECUPERACIÓN DE LA EMPRESA**	**PROBABILIDAD DE OCURRENCIA DEL RIESGO**	**PROBABILIDAD DE INTERRRUMPIR ACTIVIDADES DE LA EMPRESA**	**TOTAL**
Administrador de red	Enfermedad	2	2	1	1	6
	Cambio de empleo	2	2	2	1	7
	Fuga de información	4	3	1	1	9
	Daño Voluntario	2	2	1	2	7
	Robo de Equipos	5	4	2	2	13

TABLA 3.14 ESCALA DE RIESGO Y SU EVALUACIÓN

RIESGO		CRITERIO PARA EVALUAR LA IMPORTANCIA DEL RIESGO				
ACTIVOS	AMENAZAS	IMPACTO ECONÓMICO DEL RIESGO	TIEMPO DE RECUPERACIÓN DE LA EMPRESA	PROBABILIDAD DE OCURRENCIA DEL RIESGO	PROBABILIDAD DE INTERRRUMPIR ACTIVIDADES DE LA EMPRESA	TOTAL
Técnico	Enfermedad	3	2	1	1	7
	Cambio de empleo	2	2	2	1	7
	Fuga de información	4	3	1	1	9
	Daño Voluntario	2	2	1	1	6
	Robo de Equipos	5	4	2	2	13
Conexión a Red e Internet	Virus	2	1	3	2	8
	Fallas de red	3	2	3	4	12
	Hackers	3	3	1	3	10
	Desastres naturales	3	4	1	5	13
	Fallas de Proveedor	2	1	1	4	8
Información clientes y proveedores	Virus	2	1	3	2	8
	Daños Físicos	3	3	1	1	8
	Fuga de información	3	5	2	2	12
Equipo de Trabajo	Robo de Equipos	3	2	3	1	9
	Daños Físicos	4	3	2	2	11
	Virus	2	1	3	1	7

TABLA 3.15 ESCALA DE RIESGO Y SU EVALUACIÓN (CONTINUACIÓN)

3.3.5.6.2 Tratamiento del Riesgo y el Proceso de Toma de Decisión Gerencial

Para el tratamiento del riesgo se tiene la siguiente tabla 3.16 de evaluación:

CRITERIO	TRATAMIENTO DEL RIESGO
de 5 hasta 7	Aceptar
de 8 hasta 12	Reducir
de 13 en adelante	Transferir
No existen niveles para evitar el riesgo	Evitar

TABLA 3.16 TRATAMIENTO DEL RIESGO

Se realiza el análisis de los controles para determinar cuáles son aplicables.

Cuando se ha calculado el riesgo, se debe iniciar un proceso de toma de decisiones para determinar qué va a ocurrir con el riesgo, la decisión está principalmente influenciada por los objetivos de la organización pero por lo general siempre está ligada con estos dos factores:

- El posible impacto si el riesgo se pone de manifiesto.
- Qué tan frecuente puede vulnerar.

3.3.5.6.3 Estrategias Posibles para el Tratamiento del Riesgo

ACTIVOS	AMENAZAS	TOTAL	Tratamiento del Riesgo
Administrador de red	Enfermedad	6	Aceptar
	Cambio de empleo	7	Aceptar
	Fuga de información	9	Reducir
	Daño Voluntario	7	Aceptar
	Robo de Equipos	13	Transferir
Técnico	Enfermedad	7	Aceptar
	Cambio de empleo	7	Aceptar
	Fuga de información	9	Reducir
	Daño Voluntario	6	Aceptar
	Robo de Equipos	13	Transferir
Conexión a Red e Internet	Virus	8	Reducir
	Fallas de red	12	Reducir
	Hackers	10	Reducir
	Desastres naturales	13	Transferir
	Fallas de Proveedor	8	Reducir
Información de clientes y proveedores	Virus	8	Reducir
	Daños Físicos	8	Reducir
	Fuga de información	12	Reducir
Equipo de Trabajo	Robo de Equipos	9	Reducir
	Dañados Físicamente	11	Reducir
	Virus	7	Aceptar

TABLA 3.17 ESTRATEGIAS DE TRATAMIENTO DEL RIESGO

Para el tratamiento del riesgo (tabla 3.17) se procederá de la siguiente manera:

El riesgo de los activos que va a ser Aceptado requiere de un registro en el cual la gerencia demuestre que se acepta el riesgo asociado a estos activos.

Para el riesgo de los activos que va a ser Reducido se aplicará los controles de la norma ISO/IEC 27002.

Para el riesgo de los activos que va a ser Transferido se contrató un seguro que protege económicamente a los activos contra los desastres naturales y robos principalmente.

No existen activos con la opción EVITAR, ya que todos son indispensables y no se puede prescindir de ninguno.

3.3.6 RIESGO RESIDUAL

Se dejará un riesgo remanente debido a que para las amenazas identificadas es evidente que no se pueden eliminar todas las vulnerabilidades.

El riesgo residual es aceptable para las diferentes amenazas identificadas y se dispone de un registro de aceptación de este riesgo remanente (Anexo 2).

3.3.6.1 Seleccionar Objetivos de Control y Controles para el Tratamiento de Riesgos

A continuación se determina los controles que pueden ser implementados
Una vez identificados los procesos de tratamiento del riesgo y haberlos evaluado, se debe decidir qué objetivos de control y controles se van a implementar.

3.3.6.2 Preparación de la declaración de aplicabilidad

La declaración de aplicabilidad es un documento importante del PPPSI, que debe incluir los objetivos de control y controles que serán aplicados y los que serán excluidos. La declaración de aplicabilidad da la oportunidad a la empresa de que asegure que no ha omitido algún control.

En la tabla 3.18 se presenta el enunciado de aplicabilidad.

Objetivos de Control	Controles	Aplicabilidad		Justificación
		SI	NO	
Políticas de Seguridad Informática	Documento de políticas de Seguridad Informática	X		Es necesario establecer las políticas de seguridad, y revisarlas periódicamente. Se debe revisar periódicamente estas políticas para asegurar que se mantengan adecuadas
	Revisión de las políticas de Seguridad Informática	X		
Organización Interna	Compromiso de la Dirección con la Seguridad de la Información	X		Es necesario tener controles y políticas para el manejo de la Seguridad de la Información dentro de la organización.
	Coordinación de la Seguridad Informática	X		
	Asignación de responsabilidades para la Seguridad Informática	X		
	Proceso de autorización para los servicios de procesamiento de información	X		
	Acuerdos sobre confidencialidad	X		
	Contacto con las autoridades	X		
	Contactos con grupos de interés especiales	X		
	Revisión independiente de la Seguridad Informática	X		
Entidades externas	Identificación de riesgos relacionados con partes externas	X		No se necesitan controles para mitigar riesgos con entidades externas. Se debe establecer requerimientos de seguridad porque hay documentos muy confidenciales que son trasladados por terceros.
	Abordaje de seguridad cuando se trata con clientes	X		
	Abordaje de seguridad en los acuerdos con terceras partes	X		
Responsabilidad por los activos	Inventario de Activos	X		Es necesario tener controles para la protección desapropiada de los activos organizacionales.
	Propietario de los activos	X		
	Uso aceptable de los activos	X		
Clasificación de la información	Directrices de clasificación	X		Es necesario tener controles para asegurar que la información reciba un nivel de protección apropiado.
	Etiquetado y manejo de la información	X		

TABLA 3.18 DECLARACIÓN DE APLICABILIDAD

CAPÍTULO IV

IMPLEMENTACIÓN DEL PLAN PILOTO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA "PPPSI"

CAPÍTULO IV: IMPLEMENTACIÓN DEL PLAN PILOTO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA “PPPSI”

4.1 DESARROLLO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

El desarrollo de las políticas de Seguridad Informática realizada en el área de Networking de la empresa Uniplex Systems S.A. se deriva del análisis del tratamiento del riesgo (en donde se califican los activos de información y se determina si se acepta, reduce, transfiere o evita el riesgo) versus el enunciado de aplicabilidad de los controles correspondientes a los tres dominios de la norma:

- Política de Seguridad Informática
- Aspectos Organizativos de la Seguridad Informática
- Gestión de Activos

4.1.1 PROCEDIMIENTO PARA DESARROLLAR LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA

A continuación se explica cómo desarrollar una política de Seguridad Informática.

En la tabla 3.17 que trata de las Estrategias de Tratamiento del Riesgo, se define la acción a tomar con el activo (Aceptar, Reducir, Transferir, Evitar).

Para los activos cuya opción es ACEPTAR, la gerencia debe aprobar el documento para aceptación del riesgo y las razones por las cuales se lo acepta.

Para la mayoría de activos, la opción elegida es REDUCIR y para éstos se aplicarán los controles de la norma ISO/IEC 27002.

Para los activos que van a ser TRANSFERIDOS, se contrató un seguro que protege económicamente a los activos contra los desastres naturales y robos principalmente.

No existen activos con la opción EVITAR, ya que todos son indispensables y no se puede prescindir de ninguno.

Una vez determinado cuál será la acción a tomar con el activo; se verifica en la tabla 3.18 cuales controles van a ser aplicados para esa amenaza.

Para determinar las políticas de Seguridad Informática del PPPSI se verificó cuáles son los activos más importantes y con cuáles controles se ha de mejorar la seguridad.

Por ejemplo; para el activo *Conexión a Red e Internet* cuya amenaza es el *virus* y cuya opción de tratamiento del riesgo es REDUCIR, se pueden aplicar los controles:

Documento de la política de Seguridad de la Información; en donde se crea la política que determina la existencia de un responsable por las actualizaciones, modificaciones, arreglos del antivirus; así como también una política señalando que debe existir un procedimiento para conectar medios de procesamiento de la información que no pertenecen a la empresa.

Asignación de responsabilidades; en donde se determina quién debe actualizar el antivirus, con cuánta frecuencia revisar los casos de virus detectados en la red y tomar acción para eliminar el virus y evitar su propagación.

Proceso de autorización para los servicios de procesamiento de información; para evitar que la red interna se contagie de virus debido a computadores externos.

Propietario de los activos.- Similar al control Asignación de Responsabilidades pero en este control los dueños corresponden a procesos, conjuntos de

actividades, aplicación y dentro de estos se asignan responsabilidades a las personas. Es decir, el propietario del activo Conexión a Red e Internet es el área de Networking; y la responsabilidad de actualizar el antivirus es del administrador de la red.

Uso Aceptable de los activos.- Para disminuir el ingreso de software malicioso a través de la navegación en Internet por parte de los usuarios.

Contacto con las Autoridades.- Para avisar a las autoridades, en caso de ser necesario, infecciones que no han podido ser controladas o cualquier otra novedad.

Abordaje de la seguridad cuando se trata con clientes.- Para informar a los clientes que su computador va a ser examinado por el antivirus, o para verificar que no exista software maligno. Todo esto previo a otorgarle el acceso a la información.

Así pues, las políticas que se deben aplicar son:

Se debe establecer un documento con las políticas de Seguridad Informática para ser aplicadas en el área de Networking de la empresa Uniplex Systems S.A.

La gerencia debe designar una persona encargada de coordinar las actividades del Plan Piloto de Políticas de Seguridad Informática PPPSI
El coordinador debe establecer las tareas y responsabilidades que serán asignadas a sus subordinados, los cuales deberán aceptar el acuerdo de confidencialidad, de derecho de propiedad intelectual u otro documento que la empresa considere necesario.

El coordinador debe establecer el lineamiento para uso aceptable de los recursos de la empresa, este documento debe ser revisado y aprobado por la gerencia y comunicado a todos los miembros del área.

Se debe establecer procesos de autorización para medios de procesamiento de información, los medios pueden ser de la empresa o ajenos. La aceptación del ingreso de este medio de procesamiento de información debe estar registrada debidamente.

Cuando una persona ajena a la empresa desea tener acceso a la información, debe tener la aprobación de la gerencia en un documento que así lo especifique. Se debe especificar el tiempo que el usuario tendrá acceso a la información.

Usuarios externos a la empresa que deseen o necesiten tener acceso a información importante de la empresa, deben firmar un acuerdo de confidencialidad.

Estas políticas conllevan a establecer un documento de tareas y responsabilidades creado por el coordinador en el cual se enuncie que:

El administrador de la red será el responsable de instalar y actualizar el antivirus, revisar infecciones detectadas en la red y tomar acción para eliminar el virus y evitar su propagación inmediata.

El administrador de la red debe revisar cualquier medio de procesamiento de la información previo a ser conectado en la LAN de Uniplex. Debe verificar que exista un antivirus actualizado o instalarlo en caso de ser necesario.

El administrador de la red debe comunicar al dueño del activo ajeno a la empresa que se debe revisar su medio de información previo a la habilitación del acceso. Si no acepta entonces se debe comunicar inmediatamente al coordinador y gerencia para tomar las acciones respectivas.

Para medios de almacenamiento (discos externos, flash memory, entre otros) se debe correr el antivirus, para el caso de computadores (laptops, desktops) se debe verificar que está instalado un antivirus y ejecutarlo.

En caso de una situación de emergencia en la cual no se pueda verificar si hay un antivirus instalado o no se lo pueda ejecutar en el medio de procesamiento de información, se debe comunicar a gerencia mediante email que existe un riesgo de infección al conectar este medio a la LAN.

Éste es el procedimiento para establecer las políticas de Seguridad Informática para el activo CONEXIÓN A RED E INTERNET cuya amenaza es VIRUS, es importante recordar que estas políticas pueden ser modificadas para proteger a más activos y evitar desarrollar excesivo número de políticas que podrían confundir y hacer más compleja su implementación.

4.1.2 CONTROLES APLICABLES PARA EL RESTO DE ACTIVOS

El proceso de desarrollo de políticas para el resto de activos es idéntico; a continuación se detallan los activos y su relación con los controles de la Norma ISO/IEC 27002.

Para el activo ADMINISTRADOR DE RED cuya amenaza es FUGA DE INFORMACIÓN se utilizan los siguientes controles:

- Documento de Políticas de seguridad de informática
- Asignación de Responsabilidades para la Seguridad Informática
- Acuerdos sobre confidencialidad
- Propietario de los activos
- Uso aceptable de los activos
- Etiquetado y manejo de la información.

Para el activo TÉCNICO cuya amenaza es FUGA DE INFORMACIÓN se utilizan los siguientes controles:

- Documento de políticas de Seguridad Informática
- Asignación de Responsabilidades para la Seguridad Informática

- Acuerdos sobre confidencialidad
- Propietario de los activos
- Uso aceptable de los activos
- Etiquetado y manejo de la información.

Para el activo CONEXIÓN A RED E INTERNET cuya amenaza es FALLAS DE RED se utilizan los siguientes controles:

- Documento de políticas de Seguridad Informática
- Asignación de Responsabilidades para la Seguridad Informática
- Proceso de autorización para los servicios de procesamiento de la información
- Contacto con las autoridades
- Inventario de activos
- Propietario de los activos
- Uso aceptable de los activos

Para el activo CONEXIÓN A RED E INTERNET cuya amenaza es HACKERS se utilizan los siguientes controles:

- Documento de Políticas de Seguridad Informática
- Revisión de la política de Seguridad Informática
- Compromiso de la dirección con la Seguridad de la Información.
- Asignación de Responsabilidades para la Seguridad Informática
- Proceso de autorización para los servicios de procesamiento de la información.
- Contacto con grupos de intereses especiales.
- Identificación de los riesgos relacionados con las partes externas.
- Abordaje de la seguridad cuando se trata con los clientes.
- Abordaje de la seguridad en los acuerdos con terceras partes.
- Propietario de los activos.

Para el activo INFORMACIÓN DE CLIENTES Y PROVEEDORES cuya amenaza es VIRUS se utilizan los siguientes controles:

- Documento de la política de Seguridad Informática
- Asignación de Responsabilidades
- Proceso de autorización para los servicios de procesamiento de información
- Propietario de los activos
- Uso Aceptable de los activos
- Contacto con las Autoridades
- Abordaje de la seguridad cuando se trata con clientes

Para el activo INFORMACIÓN DE CLIENTES Y PROVEEDORES cuya amenaza es DAÑOS FÍSICOS se utilizan los siguientes controles:

- Documento de Políticas de Seguridad Informática
- Asignación de Responsabilidades para la Seguridad Informática
- Contacto con las autoridades
- Contacto con grupos de intereses especiales.
- Identificación de los riesgos relacionados con las partes externas.
- Abordaje de la seguridad en los acuerdos con terceras partes.
- Inventario de Activos.
- Propietario de los activos.
- Uso aceptable de los activos.

Para el activo INFORMACIÓN DE CLIENTES Y PROVEEDORES cuya amenaza es FUGA DE INFORMACIÓN se utilizan los siguientes controles:

- Documento de Políticas de Seguridad Informática
- Asignación de Responsabilidades para la Seguridad Informática
- Proceso de autorización para los servicios de procesamiento de información

- Acuerdos sobre confidencialidad
- Contacto con las autoridades
- Identificación de los riesgos relacionados con las partes externas.
- Abordaje de la seguridad cuando se trata con los clientes.
- Abordaje de la seguridad en los acuerdos con terceras partes.
- Inventario de Activos.
- Propietario de los activos.
- Directrices de clasificación
- Etiquetado y manejo de la información.

Para el activo EQUIPO DE TRABAJO cuya amenaza es ROBO DE EQUIPOS se utilizan los siguientes controles:

- Documento de Políticas de Seguridad Informática
- Asignación de Responsabilidades para la Seguridad Informática
- Acuerdos sobre confidencialidad
- Contacto con las autoridades
- Revisión independiente de la Seguridad Informática
- Identificación de los riesgos relacionados con las partes externas.
- Abordaje de la seguridad cuando se trata con los clientes.
- Inventario de activos.
- Propietario de los activos.
- Uso aceptable de los activos.

4.1.3 POLÍTICAS APLICADAS EN NETWORKING

Las políticas que se aplican en el área de Networking de la empresa Uniplex Systems S.A. se estratifican en tres niveles, para la gerencia, para el coordinador y para el técnico y administrador de la red.

Las políticas de Seguridad Informática para el área de Networking se hallan documentadas en el Anexo 2.

En el Anexo 3 se muestra la implementación de las políticas de Seguridad Informática.

4.2 FORMULACIÓN DE GUÍAS PARA DOCUMENTAR Y EVALUAR LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA DEL PPPSI

Para la formulación de guías para documentar y evaluar las políticas se tiene como referencia la siguiente pirámide de documentos (Gráfico 4.1), la pirámide consta de cuatro niveles en donde el nivel uno será el primer instructivo que debe realizarse y el cuarto será el último.

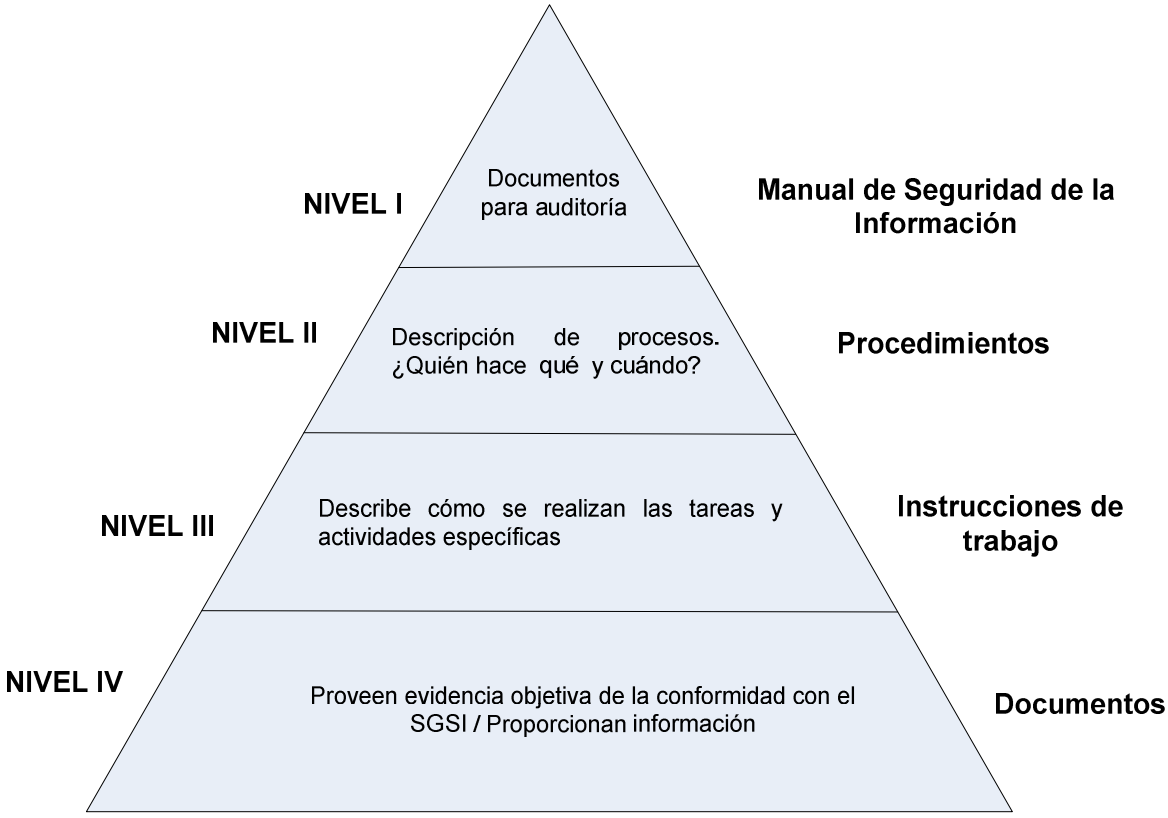


GRÁFICO 4.1 PIRÁMIDE DE DOCUMENTOS

4.2.1 NIVEL I. MANUAL DE SEGURIDAD DE LA INFORMACIÓN

Este manual se utiliza para facilitar las auditorías y resume información muy importante. Los aspectos primordiales de este manual serán:

I. Enunciados de las Políticas del PPPSI

En este punto se extrae las políticas establecidas para apoyar el Plan de Políticas de Seguridad Informática para el área de Networking.
Para mayor detalle del enunciado ver 3.3.3.

II. Alcance del PPPSI

El alcance está determinado por la gerencia, se puede encontrar el alcance más detallado en 3.3.1.

III. Procedimientos y controles de soporte

En el área de Networking de la empresa Uniplex Systems S.A. fue realizado un análisis del estado de las políticas de Seguridad Informática previo a la implementación de este proyecto.

Este análisis se efectuó el 31 de Octubre de 2008 por la **Ing. Carolina Granja**, técnico del área de Software en conjunto con Richard Posso, técnico del área de Networking. Para revisar mayor detalle del análisis se lo puede encontrar en el literal 3.1

Los puntos analizados referentes a Seguridad Informática fueron:

Evaluación de la Seguridad Lógica

Alcance del Análisis.- El alcance en este punto fue determinar cuán efectivos estuvieron los controles para el acceso a los elementos procesadores de datos,

cuán seguros eran los password del área de Networking y cómo estaba conformada la segregación de funciones del área. Se analizaron:

- Permisos
- Passwords
- Inactividad
- Segregación de funciones

Evaluación de la Seguridad de las Comunicaciones

Alcance del Análisis.- El alcance en este campo fue evaluar la seguridad de las comunicaciones, los datos transmitidos, los dispositivos usados durante la transmisión, la documentación necesaria para la realización eficiente y sin interrupciones de esta transmisión, y los sistemas usados para la transmisión de datos de un entorno a otro. Se analizaron:

- Topología de Red
- Conexiones Externas
- Configuración Lógica de red
- Mail
- Antivirus
- Firewall

Evaluación de la Seguridad en las Aplicaciones.

Alcance del Análisis.- El alcance en esta zona consistió en evaluar la seguridad de las aplicaciones utilizadas en la empresa, la consistencia de sus datos de entrada y la exactitud de sus datos de salida, la integridad de las bases de datos y la existencia y el uso de la documentación necesaria para su funcionamiento, de acuerdo a los estándares propuestos. Se analizaron:

- Control de Aplicaciones en PC’s
- Control de datos en las aplicaciones de PC’s

Evaluación de la Seguridad Física

Alcance del Análisis.- Se evaluó que el área de Networking, los equipos, los dispositivos, los medios de almacenamiento y las personas que conforman el departamento, cumplan con las medidas necesarias en lo relativo a la infraestructura física y al mantenimiento de la seguridad de los recursos de la organización. Se analizaron:

- Equipamiento
- Control de Acceso a Equipos
- Dispositivos de Soporte
- Cableado Estructurado

Administración del Cuarto de Equipos

Alcance del Análisis.- El alcance del análisis fue evaluar la correcta organización y administración del cuarto de equipos, así como la asignación de tareas y responsabilidades del personal que la conforma, a fin de que ésta brinde condiciones óptimas de operación que posibiliten un ambiente adecuado de control y permitan mejorar la disponibilidad de sus servicios, de acuerdo a las normas existentes que regulan esta actividad. Se analizaron:

- Administración del Cuarto de Equipos
- Capacitación
- Backup
- Documentación

Este análisis permitió determinar qué políticas se están aplicando en la empresa, cuáles podrían ser mejoradas y cuáles hacen falta.

IV. Descripción de la metodología de evaluación del riesgo

Para realizar la evaluación del riesgo, se aplicó un procedimiento metodológico conformado por los siguientes pasos:

- Identificación de Activos
- Identificación de requerimientos legales y comerciales
- Tasación de activos
- Identificación de amenazas y vulnerabilidades
- Cálculo de amenazas y vulnerabilidades
- Análisis del riesgo y su evaluación
- Aspectos a contemplar al efectuar la evaluación del riesgo

V. Plan de tratamiento del riesgo

Existen infinidad de criterios para el tratamiento del riesgo, el aplicado en la empresa, es el mostrado en la tabla 3.17.

VI. Declaración de Aplicabilidad.

La declaración de aplicabilidad describe todos los controles que van a ser aplicados en el área de Networking. Ver Tabla 3.18.

4.2.2 NIVEL II. PROCEDIMIENTOS

A continuación se describen los documentos definidos para la norma ISO 27001-2005 que pueden ser aplicados en la norma ISO 27002.

- Documentar el alcance del Modelo PPPSI.
- Documentar las políticas de Seguridad Informática y la política del PPPSI.
- Documentar la metodología de evaluación del riesgo

- Documentar los criterios para aceptar los riesgos e identificar los niveles de riesgo aceptables.
- Documentar el inventario de activos y sus propietarios.
- Documentar la tasación de los activos de información.
- Documentar las amenazas y vulnerabilidades de los activos de información.
- Documentar el proceso de evaluación de opciones de tratamiento del riesgo.
- Documentar el proceso de selección de objetivos de control y controles para el tratamiento del riesgo
- Documentar la aprobación de la gerencia para los riesgos residuales propuestos.
- Documentar la autorización de la gerencia para implementar y operar el PPPSI.
- Documentar el enunciado de aplicabilidad.
- Documentar el plan de tratamiento del riesgo.
- Documentar la asignación de roles y responsabilidades.
- Documentar cómo medir la efectividad de los controles o grupos de controles seleccionados, y especificar cómo se van a utilizar estas mediciones para evaluar la efectividad del control, para producir resultados comparables y reproducibles.
- Elaborar el registro de las acciones y eventos que podrían tener un impacto sobre la efectividad o desempeño del PPPSI.
- Procedimiento para el control de documentos.
- Definir en un procedimiento documentando las responsabilidades, los requerimientos para la planeación y realización de las auditorías y para el reporte de resultados y mantenimiento de registros.
- Procedimiento para evaluar la exposición de la organización ante las vulnerabilidades técnicas.
- Evidencia documentada donde se proporciona la capacitación o se realizan otras acciones para satisfacer estas necesidades.

4.2.3 NIVEL III. INSTRUCCIONES DE TRABAJO

Las instrucciones de trabajo explican cómo debe desarrollarse una tarea específica (numeración de documentos, etiquetar información, etc.). Además, están en función de la experiencia que la empresa tiene respecto a la Seguridad Informática, se desarrollarán instructivos necesarios para cumplir con los controles de los tres Dominios.

4.2.4 NIVEL IV. DOCUMENTOS

En este nivel se agrupan tanto los registros como los documentos utilizados en el PPPSI. El punto clave de este nivel es identificar la diferencia entre *registro* y *documento*.

El registro es una evidencia de que lo que se dice se ha cumplido, es un aval que permite afirmar que se está cumpliendo con lo acordado. El documento es un conjunto de información que tiene su propio medio de soporte, por ejemplo puede ser la política de seguridad, un reporte o formulario.

En el ANEXO 2 se detallan los documentos, instrucciones de trabajo y registros que se han de implementar en la empresa, mismos que sirven para evaluar las políticas de seguridad en las auditorías:

- Documento de Acuerdo de Confidencialidad.
- Documento de Políticas de Seguridad de Informática.
- Documento para Asignación de Responsabilidades.
- Documento para Uso Aceptable de los Activos de información.
- Instructivo de Inventario de Activos.
- Instructivo para Etiquetado y Manejo de la Información.
- Instructivo para Revisión de las Políticas de Seguridad Informática.
- Registro de Compromiso de la Dirección con la Seguridad Informática.
- Registro de Contacto con Grupos de Intereses.
- Registro de Contacto con las Autoridades.
- Registro de Revisión Independiente de la Seguridad Informática.

4.3 MANUAL DE USUARIO PARA IMPLEMENTAR LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA

En el anexo 4 se presenta una breve guía para los usuarios de Networking.

4.4 COSTOS

Una vez concluida la implementación del Plan Piloto de Políticas de Seguridad Informática en el área de Networking de la empresa Uniplex Systems S.A. se presenta los costos referenciales.

Los costos se los ha dividido en dos grupos; costos de diseño y costos de implementación:

4.4.1 COSTOS DE DISEÑO

Es aquí donde se consideran los valores de los elementos necesarios previos a la implementación del PPPSI (tabla 4.1).

Costos de Diseño	Valor $
Norma ISO 27002	**33**
Costo Personal (cuatro meses)	**2000**
Cursos de Seguridad de la Información.	**300**
Otros	**200**
SUBTOTAL	**2533**

TABLA 4.1 COSTOS DE DISEÑO

Los valores que se consideraron son:

1.- Norma.- Norma ISO/IEC 27002 adquirida a ICONTEC. Es necesario poseer la norma para analizarla e implementarla.

2.- Personal.- Es el salario del coordinador para diseñar el PPPSI. Se considera el monto total por los cuatro meses invertidos en el proyecto.

3.- Curso.- Se siguió un curso de Seguridad de la Información dictado en Junio de 2008 en el Hotel Quito para tener más experiencia referente a las normas ISO de seguridad.

4.- Otros.- Son imprevistos como utilización de Internet, recopilación de información; etc.

4.4.2 COSTOS DE IMPLEMENTACIÓN

En estos costos se consideran los valores de los elementos necesarios para la implementación del PPPSI (tabla 4.2). Estos valores son los siguientes:

Costos de Implementación	$
*Costo de Software Whats Up	**0**
*Costo de Software Belarc	**0**
Disco Duro externo para respaldos.	**235**
Póliza de Seguro	**500**
Otros	**100**
SUBTOTAL	**835**[23]

TABLA 4.2 COSTOS DE IMPLEMENTACIÓN

1. Costo de Software What's Up.- Uniplex Systems S.A. es partner de este producto, razón por la cual la licencia de la cual dispone es gratis para dar demostraciones a sus clientes.

2. Costo de Software Belarc.- Software que permite realizar un inventario de todos los equipos de la red, permite verificar si alguien ha conectado dispositivos de almacenamiento en sus estaciones de trabajo (discos duros, flash, entre otros). Permite verificar qué software ha sido instalados o removido. Uniplex Systems es partner de este producto y por lo tanto la licencia es gratis para dar presentaciones a clientes.

[23] La empresa Uniplex Systems S.A. al ser partner de algunos proveedores, puede utilizar software sin costo alguno.

3. Disco duro externo para respaldos.- Se adquirió un disco duro externo de 750GB para sacar respaldos de la información principal del cuarto de equipos.

4. Póliza de Seguros.- Se contrató una póliza para proteger los equipos de Infraestructura.

5. Otros.- Investigación en Internet, horas extra; etc.

4.4.3 COSTO TOTAL

Una vez presentados los costos de diseño e implementación del PPPSI se obtiene el costo para el área de Networking de la empresa Uniplex Systems S.A. (tabla 4.3)

Costo	Valor $
Costo Diseño	**2133**
Costo Implementación	**835**
COSTO TOTAL	**2968**

TABLA 4.3 COSTO TOTAL

4.4.4 BENEFICIOS

Los beneficios obtenidos al implementar el Plan de Políticas de Seguridad Informática en el área de Networking pueden clasificarse en cuantificables y no cuantificables; los cuantificables se describen en la Tabla 4.4.

Ítem	Beneficios de Proteger equipo de Networking	Costos
1	Firewall Cisco PIX 515E	1395
2	ALLOT Administrador de Ancho de Banda AC 402	1560
3	Switch Catalyst 2950	591
4	Switch 3COM 3C16475	150
5	Switch Dlink	40
6	Access Point	335
7	Laptop IBM (2)	300
8	Desktop Clon	500
	TOTAL	**4871**

TABLA 4.4 BENEFICIOS[24]

[24] Valores de la póliza establecida con la empresa aseguradora.

Como beneficios no cuantificables se tienen:

- Auditorías de Seguridad Informática más precisas y confiables.
- Concientización global sobre la importancia de la Seguridad Informática.
- Mayor control de la información proporcionada a terceros.
- Mayor seguridad en relación al ambiente informático.
- Mejor reacción a incidentes de Seguridad Informática.
- Mejora la imagen de la empresa y aumenta la confianza de terceros.
- Orden en el área de trabajo bajo un marco normativo que evita la duplicación de tareas, facilita el almacenamiento, intercambio y organización de información en medios informáticos.
- Planeamiento y manejo de la Seguridad Informática más efectivos.
- Reducción de los riesgos involucrados al manejo de información en medios informáticos.

4.4.5 RELACIÓN COSTO BENEFICIO

Costo	Valor $
Beneficio	4871
Costo Implementación	2968
Diferencia	1903

TABLA 4.5 RELACIÓN COSTO BENEFICIO

Como se aprecia en la tabla 4.5 la diferencia entre el beneficio obtenido y el costo de implementar el Plan de Políticas de Seguridad Infórmatica es positiva.

CAPÍTULO V
CONCLUSIONES Y RECOMENDACIONES

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- En el área de Networking de la empresa Uniplex Systems S.A. se definieron los aspectos que involucran el Plan Piloto de Políticas de Seguridad Informática, la adopción de este Plan permitió establecer los aspectos que involucran una correcta Seguridad Informática.

- En el área de Networking de la empresa Uniplex S.A. se han especificado motivos principales por los cuales es necesario implementar políticas de Seguridad Informática, lo que fué objeto de análisis a través del desarrollo sistemático del Plan Piloto de Políticas de Seguridad Informática (PPPSI).

- En el área de Networking de la empresa Uniplex Systems S.A. se determinó el procedimiento que se consideró más conveniente para desarrollar políticas para la Seguridad Informática, corregir algunas y mejorar otras. No se desarrollan excesivas políticas de seguridad porque el plan piloto puede colapsar o ser rechazado por el exceso de normas aplicadas.

- En el área de Networking de la empresa Uniplex Systems S.A. se identificaron las falencias y fortalezas de las políticas de Seguridad Informática precedentes; con base a esto, se desarrollaron e implementaron mejores y nuevas Políticas de Seguridad Informática para el área.

- El propósito principal del Plan Piloto de Políticas de Seguridad Informática instaurado en el área de Networking de la empresa Uniplex Systems S.A. es disminuir el riesgo al cual están sujetos los activos de información en la empresa. El proceso para identificar los activos de información dentro del alcance del plan piloto es fundamental así como también lo es la evaluación de los riesgos de los activos.

- La GUÍA DE USUARIO instaurada en el área de Networking de la empresa Uniplex Systems S.A. es muy clara y específica, no da lugar a malos entendidos por parte de los usuarios del área. Además, se asignó responsabilidades y obligaciones de forma equitativa entre los miembros del área.

5.2 RECOMENDACIONES

- Se recomienda extender el modelo de políticas de Seguridad Informática desde el área de Networking a toda la empresa, por supuesto debe contar con el total apoyo de la gerencia y debe ser un objetivo planteado para la organización.

- Se recomienda desarrollar y establecer un Sistema de Gestión de Seguridad de Información (SGSI) cuyo alcance es más extenso que el Plan Piloto de Políticas de Seguridad Informática (PPPSI) ya que involucra todos los once dominios de la norma, abarca todos los aspectos de seguridad de información que pueden ayudar a reducir aún más el riesgo con la información, con el fin de robustecer y hacer más confiable a la empresa.

- Se recomienda analizar las normas de la familia 27000 para mantener en mejoramiento continuo el Plan Piloto de Políticas de Seguridad Informática. En especial se recomienda revisar la Guía de Auditoría de un Sistema de Seguridad, porque este control debe ser implementado periódicamente.

- Debido a que la información es muy importante, se recomienda que las empresas capaciten personal referente a las normas de Seguridad de la Información, y no verlo como un gasto sino como una inversión ya que los beneficios obtenidos sobrepasan fácilmente a los costos de inversión.

BIBLIOGRAFÍA

- Seminario ISO 27002 Intensivo. Information Security INC. Medios Digitales. 2007

- Guía Para la Elaboración de Políticas de Seguridad. Universidad Nacional de Colombia. 2003.

- Information technology – Code of Practice for information security management. Internacional Standard ISO/IEC 17790. First Edition, 2000.

- Políticas de Seguridad de la Información, Decisión Administrativa. Buenos Aires, Argentina 2004.

- Política Oficial de Seguridad Informática del Centro de Investigación Científica y de Educación Superior de Ensenada. México, México 2001

- Modelo de Política de Seguridad de la Información para Organismos de la Administración Pública. Buenos Aires, Argentina 2001

- Políticas de Seguridad de la Información para una entidad Financiera. CÓRDOVA Edith. Lima, Perú 2002.

- INTERNET: http://www.iso27000.es

- INTERNET: http://www.ipswitch.com

- INTERNET: http://nmap.org

ANEXOS

ANEXO 1

CONCEPTOS GENERALES RESPECTO A LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA

ANEXO 1: CONCEPTOS GENERALES RESPECTO A LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA

A continuación se aclaran ciertos términos utilizados en esta norma.

- **Aceptación del riesgo**.- Decisión de aceptar el riesgo.

- **Activo**.- Cualquier cosa que tenga valor para la organización.

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

- **Análisis de riesgos**.- Uso sistemático de la información para identificar las fuentes y estimar el riesgo.

- **Calidad de Servicio**.- **QoS** (*Quality of Service*) son las tecnologías que garantizan la transmisión de cierta cantidad de datos en un tiempo dado (*throughput*).

- **Confidencialidad**.- Propiedad de la información para asegurar que solo la o las personas autorizadas posean acceso a ella.

- **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. Es sinónimo de contramedida o salvaguarda.

- **Directriz**.- Descripción que aclara lo que se debería hacer y como hacerlo, para alcanzar los objetivos establecidos en las políticas.

- **Disponibilidad**.- Propiedad de la información para estar utilizable cuando se lo requiera.

- **Documento**.- Es un conjunto de información que tiene su propio medio de soporte, por ejemplo puede ser la política de seguridad, un reporte o formulario.

- **Disco SATA**.- Tecnología de disco duro para almacenamiento de información a través de enlace serial, su acrónimo es Serial Advanced Technology Attachment**.**

- **Dominios de la Norma**.- Estructura más general de la norma ISO27002, dentro de esta se encuentran los objetivos de control y los controles.

- **Evaluación de riesgos**.- Todo proceso de análisis y valoración del riesgo.

- **Evento de Seguridad de la información**.- Un evento de Seguridad de la información es la presencia identificada de un estado del sistema, del servicio o de la red que indica un posible incumplimiento de la política de Seguridad de la información, una falla de controles, o una situación previamente desconocida que puede ser pertinente para la seguridad.

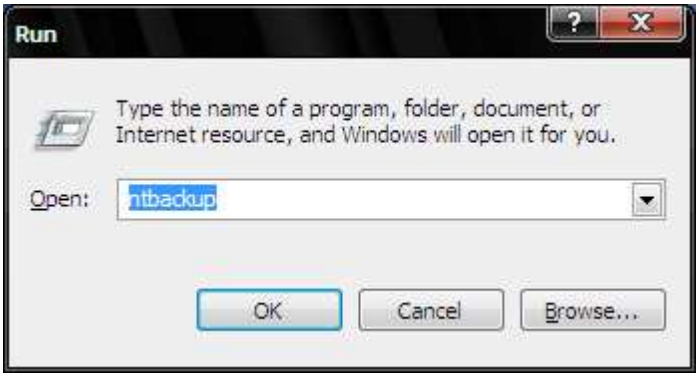
- **Gestión del riesgo**.- Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

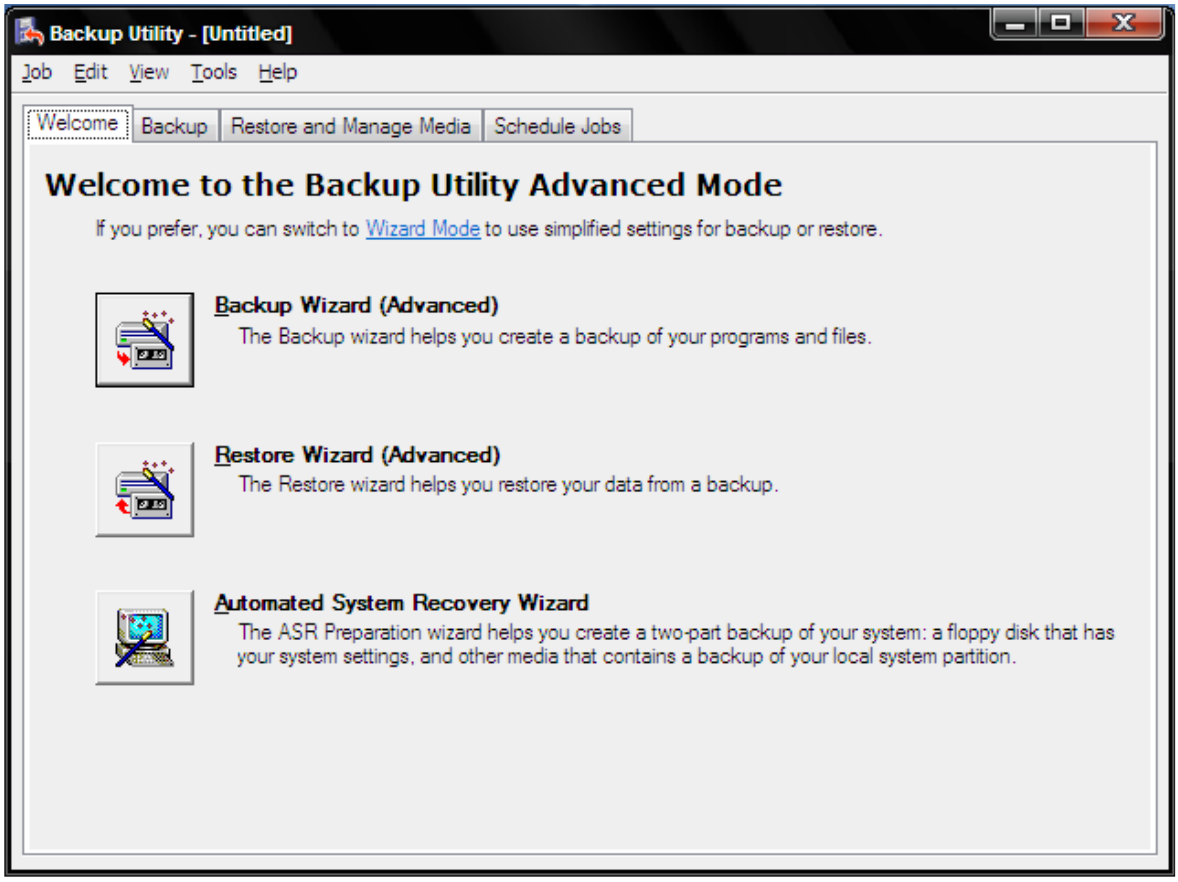
- **Incidente de Seguridad de la información**.- Un incidente de Seguridad de la información está indicado por un solo evento o una serie de eventos inesperados o no deseados de Seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la Seguridad de la información.

- **Integridad**.- Propiedad de la información para asegurar que no ha sido modificada y se encuentra integra.

- **Negación de Servicio.-** Un ataque de "Negación de Servicio" ("Deny of Service" DoS) es aquel en el que el atacante trata de mantener demasiado ocupado algún recurso para que no pueda responder a las peticiones legítimas o para denegar a los usuarios legítimos el acceso a un equipo.

- **Ntbackup.-** Utilidad para obtener respaldos en Windows.

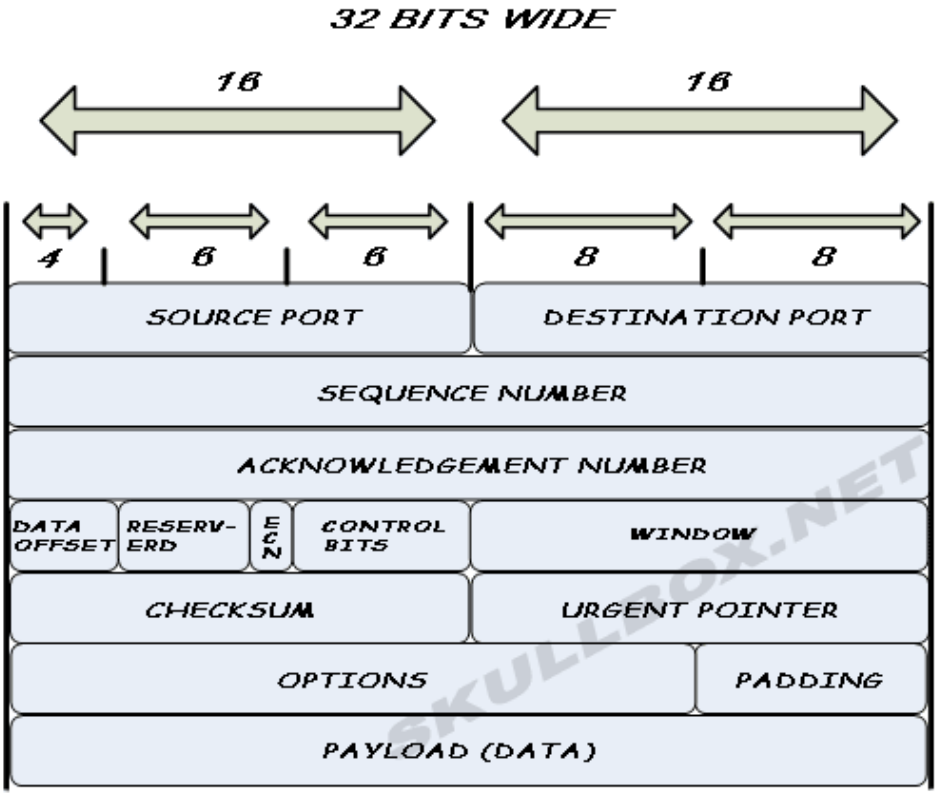




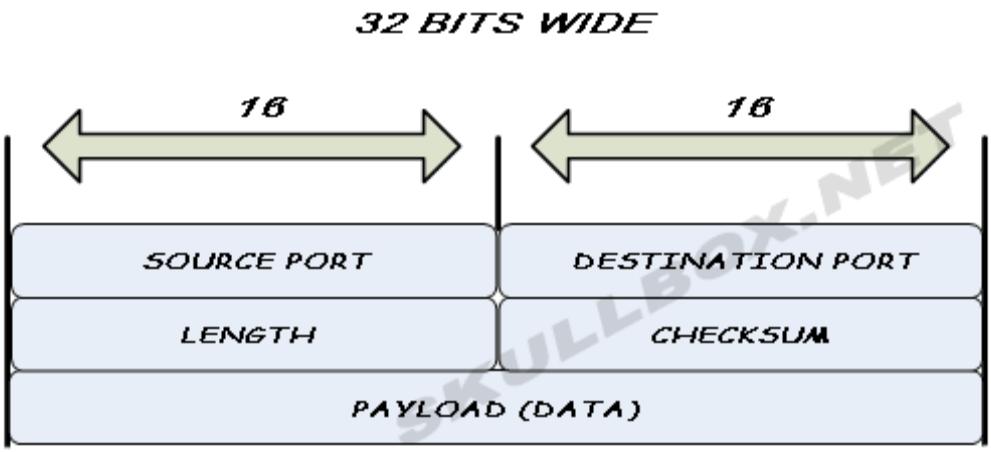
- **Política**.- Toda Intención y directriz expresada formalmente por la dirección.

- **Puertos de Comunicación.-** UDP (User Datagram Protocol) y TCP (Transmission Control Protocol) utilizan puertos para permitir la comunicación entre aplicaciones.

TCP FRAME STRUCTURE



UDP FRAME STRUCTURE



El campo de puerto tiene una longitud de 16 bits, por lo que el rango de valores válidos va de 0 a 65.535. El puerto 0 está reservado, pero es un valor permitido como puerto origen si el proceso emisor no espera recibir mensajes como respuesta.

  - Los puertos 1 a 1023 se llaman puertos "bien conocidos" y en sistemas operativos tipo Unix enlazar con uno de estos puertos requiere acceso como súper usuario.
  - Los puertos 1024 a 49.151 son puertos registrados.
  - Los puertos 49.152 a 65.535 son puertos efímeros y son utilizados como puertos temporales, sobre todo por los clientes al comunicarse con los servidores.

- **Registro**.- Es una evidencia de que lo que se dice se ha cumplido, es un aval que permite presentar que se está cumpliendo con lo acordado.

- **Riesgo**.- Combinación de la probabilidad de un evento y sus consecuencias.

- **Riesgo residual**.- El riesgo remanente después del tratamiento del riesgo.

- **Seguridad de la información**.- Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no-repudio y confiabilidad pueden estar involucradas.

- **Seguridad Informática**.- Preservación de la confidencialidad, integridad y disponibilidad de la información almacenada en medios informáticos tales como CD’s, disquetes, discos duros, cintas, memorias flash, etc.

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

- **Tercera parte**.- Persona u organismo reconocido por ser independientes de las partes involucradas, con relación al asunto en cuestión.

- **Tratamiento del riesgo**.- Proceso de selección e implementación de medidas apara modificar el riesgo.

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

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

ANEXO 2

DOCUMENTOS, INTRUCCIONES DE TRABAJO Y REGISTROS DESARROLLADOS EN EL PLAN PILOTO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

ANEXO 2: DOCUMENTOS, INTRUCCIONES DE TRABAJO Y REGISTROS DESARROLLADOS EN EL PLAN PILOTO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

DOCUMENTOS

Titulo:			
Documento de Acuerdo de Confidencialidad			
Serial:	**Fecha Emisión:**	**Fecha Modificación:**	**Aprobación:**
Elaborado Por:	**Revisado y Aprobado Por:**	**Página:**	

I. INTRODUCCIÓN

A continuación se define el acuerdo de confidencialidad establecido entre Uniplex Systems y los miembros de Networking.

II. ACUERDO DE CONFIDENCIALIDAD

Este acuerdo se celebra en este día (poner fecha) entre UNIPLEX Systems S.A. una compañía constituida bajo las leyes del Ecuador con domicilio en Quito en lo posterior referida como “la Parte Reveladora”, debidamente representada por su Presidente Ejecutivo y representante legal Señor Robert Moss Ferreira y el Señor (Nombre del empleado) por sus propios derechos, con domicilio en (Domicilio Empleado), en lo posterior referido a "la Parte Receptora”.

En consideración a que la Parte receptora en su calidad de (cargo que ocupa) de la Parte Reveladora tendrá acceso a información confidencial no divulgada de Uniplex Systems S.A., la utilización de dicha información confidencial se regula como sigue:

Información Confidencial y Materiales

El termino “Información Confidencial” significa, para efectos de este acuerdo, información de uso restringido que la Parte Reveladora ha designado como confidencial o secreta y que deberá ser tratada como información no divulgada o reservada por la Parte Receptora. Esta “información Confidencial” puede incluir, sin limitarse a éstas, las siguientes:
Información relacionada con productos de software o hardware de propiedad de la Parte Reveladora, lanzados o no al mercado;

Información relativa a la promoción de cualquier producto de la Parte Reveladora;

Información relativa a la promoción de cualquier producto de la Parte Reveladora;

Información relativa a datos contables, financieros, de personal, estrategias comerciales o tecnológicas, diseño de productos u ofertas de servicios;

Las políticas o prácticas comerciales de la parte Reveladora e información recibida de otros, que la Parte Reveladora esté obligada a tratar como confidencial.

No será considerada información Confidencial aquella que:

Es o subsecuentemente llega a ser públicamente disponible, sin violación de la Parte Receptora de obligación alguna para con la Parte Reveladora;

Fue conocida por la Parte Receptora de fuente diferente a la de la Parte Reveladora, y no por el rompimiento de una obligación de confidencialidad debida a la Parte reveladora.

Se denominaran como “Materiales Confidenciales” a todos los materiales que contienen Información Confidencial, incluyendo, entre otros, documentos escritos o impresos, y discos o cintas de computadores , sean estos legibles por maquina o por el usuario. Si la Información Confidencial es relevada de manera verbal, la Parte Reveladora informará sobre el contenido reservado de dicha información.

Restricciones

La Parte Receptora no revelará ninguna Información Confidencial a terceras personas durante el plazo de cinco (5) anos contados a partir de la fecha de su revelación por la Parte Reveladora, excepto en los siguientes casos:

La Parte Receptora puede revelar Información Confidencial en cumplimiento de una orden judicial o gubernamental. Siempre que la Parte Receptora de a la Parte Reveladora notificación razonable previa a tal revelación.

Para mantener la confidencialidad de la información, la Parte Receptora deberá tomar precauciones de seguridades razonables, por lo menos tan estrictas como aquellas que toma para proteger su propia información confidencial.

La Parte Receptora reconoce que la Parte Reveladora tendrá derecho a ser indemnizada por los daños y perjuicios que pudiere producirle la mala utilización o la revelación no autorizada de la información Confidencial, y a iniciar las acciones que le faculta la Ley de Propiedad Intelectual y el Código Penal.

Propiedad de la información

Toda información Confidencial y materiales Confidenciales son y permanecerán de propiedad de la parte reveladora. Al revelar información a la Parte Receptora, la Parte Reveladora no otorga a la Parte Receptora ningún

derecho, ni expreso ni sobreentendido, a los derechos de autor (copyright), patentes, marcas o información relativa a cualquier información confidencial.

Límites de este Acuerdo

Los términos de confidencialidad estipulados bajo este Acuerdo no tienen como intención el limitar los derechos de cualquiera de las partes para desarrollar o adquirir productos independientemente, sino el prohibir el uso de la información Confidencial perteneciente a la Parte Reveladora, una vez que la Parte Receptora deje de colaborar con la Parte Reveladora.

Enmiendas

Este Acuerdo constituye el acuerdo total entre las partes con respecto al objeto del mismo. Este acuerdo no podrá ser modificado excepto por un acuerdo escrito de fecha posterior a la fecha de este Acuerdo y firmado por ambas partes. No será admisible ninguna modificación o adición a este convenio que no sea formalizada de esta manera.

Jurisdicción y Competencia

Este Acuerdo se sujetará, en cuanto a su formación, aplicación e interpretación, a las leyes de la República del Ecuador y ambas partes acuerdan someterse a la jurisdicción de los jueces competentes de la Provincia de Pichincha.

Cualquier notificación relativa a este Acuerdo será presentada a cualquiera de las partes por escrito, con constancia de recepción.

Si cualquier disposición de este Acuerdo fuera juzgada por una corte competente como nula o ilegal, las demás disposiciones continuarán en pleno vigor y efecto.

Todas las obligaciones creadas por este Acuerdo continuarán en vigencia aún después de cualquier cambio o terminación de la relación profesional existente entre las partes.

Firma

Para constancia, firman las partes por duplicado.

Titulo:			
Documento de Políticas de Seguridad Informática			
Serial:	**Fecha Emisión:**	**Fecha Modificación:**	**Aprobación:**
Elaborado Por:	**Revisado y Aprobado Por:**	**Página:**	

I. INTRODUCCIÓN

El presente documento muestra las políticas que serán aplicadas en el área de Networking de la empresa Uniplex Systems S.A.

II. POLÍTICAS

Las políticas que se aplican en el área de Networking de la empresa Uniplex Systems S.A. se estratifican en tres niveles, para la gerencia, para el coordinador y para el técnico y administrador de la red, éstas son:

LA GERENCIA DEBE:

- Aprobar un documento de la Política del PPPSI, con su alcance y objetivo, el documento debe estar aprobado por la gerencia, debidamente registrado e identificado.
- Establecer un documento con las políticas de seguridad informática para ser aplicadas en el área de Networking de la empresa Uniplex Systems S.A.
- Revisar el documento de las políticas de seguridad informática mínimo una vez al año o cuando amerite (cambios tecnológicos, jurídicos, etc.). Se deben crear registros de las revisiones que incluyan datos como fecha de revisión, novedades encontradas, personas involucradas en la revisión, entre otros.
- Aprobar un documento en el cual se demuestre el apoyo para implementar las políticas, este documento debe ser registrado y etiquetado.

- Designar una persona encargada de coordinar las actividades de seguridad informática, (en el documento se hará mención a esta persona solamente como Coordinador).
- Aprobar los procesos de autorización para medios de procesamiento de información desarrollados por el coordinador, los medios pueden ser de la empresa o ajenos.
- Realizar una auditoría interna mínimo cada seis meses o cuando se considerase necesario, para verificar el estado del PPPSI. Esta auditoría debe estar a cargo de una persona ajena al área que tenga relación con la seguridad informática; debe además ser registrada y documentada.
- Analizar y aprobar acuerdos de confidencialidad cuando el intercambio de información con terceras partes así lo amerite. Se deberá guardar el documento o una copia del acuerdo.
- Aprobar la documentación creada por el Coordinador: para asignación de propietarios de activos de información, de responsabilidades y obligaciones de los miembros del área, para uso aceptable de los activos de información, las sanciones correspondientes en caso de incumplimiento.

EL COORDINADOR DEBE:

- Crear un documento de la Política del PPPSI, con su alcance y objetivo, el documento debe estar aprobado por la gerencia, debidamente registrado e identificado.
- Establecer las tareas y responsabilidades que serán asignadas a sus subordinados, quienes deberán aceptar el acuerdo de confidencialidad, de derecho de propiedad intelectual u otro documento que la empresa considere conveniente. Las tareas y responsabilidades deben ser lo mas explicitas posibles para evitar confusión o malos entendidos entre ambas partes.
- Establecer procesos de autorización para medios de procesamiento de información, los medios pueden ser de la empresa o ajenos. La aceptación del ingreso de este medio de procesamiento de información debe estar registrada debidamente.

- Establecer acuerdo de confidencialidad entre la empresa Uniplex Systems S.A. y los miembros de Networking. Todos los miembros del área deben aceptar los acuerdos de confidencialidad establecidos con la empresa.
- Mantener contacto con foros de seguridad o grupos de interés similares para estar pendiente de las novedades referente a vulnerabilidades y amenazas para la seguridad informática. Las noticias mas relevantes debe comunicárseles a todos los miembros del área.
- Apoyar activamente las auditorías internas que realice la gerencia, para verificar el estado del PPPSI.
- Autorizar acceso a los activos de información para terceras partes, todo esto por escrito en documento que resuma el tipo de información (verificar Instructivo de clasificación de activos de información) a ser revelada, el tiempo de acceso y el motivo.
- Realizar un inventario de activos de información cada seis meses o cuando se considere necesario. En el inventario se deben clasificar todos los activos de información que le correspondan al área.
- Crear documentación: para asignación de propietarios de activos de información, de responsabilidades y obligaciones de los miembros del área; para uso aceptable de los activos de información, las sanciones correspondientes en caso de incumplimiento.
- Establecer criterios para clasificar la información en términos de su valor, sensibilidad, importancia para el área y desarrollar un instructivo para etiquetar la información y su adecuada manipulación.
- Notificar a gerencia cualquier novedad encontrada respecto a seguridad informática. La notificación puede ser verbal pero se debe registrar en un mail, de lo contrario se asume que la novedad no fue reportada.

EL ADMINISTRADOR DEBE:

- Cuando es necesario adquirir un nuevo producto para el área de Networking, debe determinar las características del producto (Part Number, Compatibilidad de hardware y Software, Requerimientos de hardware y software, entre otros).

- Cuando equipo ajeno al área debe conectarse a la red interna, debe verificar que exista un antivirus instalado y actualizado, si es necesario se debe instalar un antivirus trial y correrlo. Todo esto con el consentimiento del dueño del equipo.
- Comunicar al dueño del activo ajeno a la empresa que se debe revisar su medio de información previo a la habilitación del acceso. Si no acepta entonces se debe comunicar inmediatamente al coordinador y gerencia para que se niegue el acceso a la información.
- Ser el responsable de instalar y actualizar el antivirus, revisar infecciones detectadas en la red y tomar acción para eliminar el virus y evitar su propagación inmediata.
- Si se presentase un caso en el que fuera necesario otorgar acceso a más de tres personas ajenas a la empresa, o cuando gerencia lo considere necesario, debe realizar un documento detallando los riesgos que se corren y sus posibles soluciones.
- Elaborar, mantener y actualizar un documento con todos los password de los usuarios (Ingreso a dominio; ingreso a BIOS); los password excluidos de esta lista serán los password de cuentas de correo de los usuarios. Todos los password deben ser cambiados mínimo cada seis meses.
- Elaborar un cronograma de mantenimiento para las PC’s del área, este mantenimiento lo realizará con el técnico designado.
- Cuando un elemento procesador de datos esta encendido por el lapso no mayor a diez minutos, debe activar un protector de pantalla u otra configuración que proteja los datos en pantalla de tal manera que sea necesario ingresar un password para ver la información nuevamente.
- Etiquetar e identificar el cableado en el área de Networking; y tener un documento en donde se especifique un diagrama de infraestructura y puntos de red del área.
- Instalar Software que permita monitorear el estado de las interfaces de los equipos de la red y que se generen alarmas en caso de falla de una de éstas. Las alarmas pueden incluir envío de mail, envío de sms entre otras.

- Revisar periódicamente los elementos de conmutación como switch y Access Point para configurar, si es necesario, mayor seguridad en la red o en otros casos aumentar la confiabilidad de la red creando enlaces redundantes. Se debe monitorear periódicamente todos los elementos de red principales, sea automáticamente o físicamente. Se deben configurar servidores de Logs en los equipos que permitan hacerlo y se debe tener un histórico con fecha de logs.
- Obtener backup de los datos de Networking (clientes, productos, programas, entre otros), la validación de datos de los cuales se debe obtener respaldo la debe realizar con el coordinador y con gerencia. El backup puede sacarse en DVD's, Cd's o en otro medio que pertenezca a la empresa. El backup también incluye archivos de configuración de los equipos de infraestructura con fechas indicadas.
- En caso de encontrar llaves, debe verificar si pertenecen al área y clasificarla, en caso de que sea ajena al área debe notificar y entregar al departamento de administración.

EL TÉCNICO DEBE:

- El técnico de soporte designado por el coordinador debe mantener contacto con foros, y otros grupos de interés vinculados con la seguridad de la información, para estar al tanto de los avances tecnológicos, amenazas y vulnerabilidades detectadas. Debe publicar al menos una vez cada 15 días alguna noticia en la cartelera y dar una resumen a los miembros del área.
- Apoyar a las actividades del administrador de la red sin que esto afecte sus obligaciones y responsabilidades o cuando el coordinador así lo disponga.
- Obtener un respaldo de la configuración de los equipos de infraestructura al menos una vez cada mes.
- Revisar las configuraciones de los elementos del FIREWALL y ALLOT periódicamente, esta revisión puede hacerla el administrador de la red en conjunto con el coordinador.

- Revisar el tráfico cursado en la red cada mes o cuando la situación lo amerite para determinar si existen comportamientos anómalos y analizarlos.
- Clasificar la información en términos de su valor, sensibilidad e importancia. Debe utilizar el instructivo para clasificación de la información que se encuentra en la documentación de Networking.
- Revisar las políticas del Active Directory para otorgar o quitar permisos a los diferentes usuarios; crear o eliminar usuarios para el dominio interno de la empresa.

A más de las políticas anteriormente descritas; cada usuario de Networking es responsable de respaldar su información, cuando se saquen respaldos en medios externos, debe proteger su información bajo llave en su estación de trabajo.

Cada usuario de Networking es responsable de mantener su estación de trabajo limpia y ordenada.

La responsabilidad de los activos de Networking es responsabilidad de todos los miembros del área; por lo cual cada usuario debe cumplir las obligaciones y responsabilidades, uso adecuado y aceptable de esta forma no se comprometen los activos del área, caso contrario se aplicaran las respectivas sanciones.

El administrador de la red y técnicos deben estar en conformes con el acuerdo de confidencialidad contraído con la empresa.

Titulo:			
Documento para Asignación de Responsabilidades			
Serial:	**Fecha Emisión:**	**Fecha Modificación:**	**Aprobación:**
Elaborado Por:	**Revisado y Aprobado Por:**	**Página:**	

I. INTRODUCCIÓN

El presente documento detalla las responsabilidades que tendrán miembros de Networking de la empresa Uniplex Systems S.A.

II. ASIGNACIÓN DE RESPONSABILIDADES

Las responsabilidades del área quedan distribuidas de la siguiente manera:

Actividad	**Responsable**
Realizar el inventario de activos	Ingeniero de Soporte
Realizar un listado de Password	Administrador de la red
Coordinar las actividades de seguridad	Coordinador
Etiquetar documentos	Networking
Realizar notas de entrega y pedido	Ingeniero de Soporte
Etiquetar cableado	Administrador de la red
Depuración de equipos de la red	Ingeniero de Soporte
Monitoreo y Mantenimiento de equipos	Administrador de la red
Asignación de responsabilidades y Obligaciones	Coordinador
Respaldo de información	Networking
Comunicar políticas a Networking	Coordinador

Titulo:			
Documento para Uso Aceptable de los Activos de Información			
Serial:	**Fecha Emisión:**	**Fecha Modificación:**	**Aprobación:**
Elaborado Por:	**Revisado y Aprobado Por:**	**Página:**	

I. INTRODUCCIÓN

El presente documento detalla las responsabilidades que tendrán miembros de Networking de la empresa Uniplex Systems S.A.

II. ASIGNACIÓN DE RESPONSABILIDADES

Las responsabilidades del área quedan distribuidas de la siguiente manera:

La empresa UNIPLEX Systems dispone de activos de información para apoyar a todos sus empleados en sus actividades diarias, estos activos deben ser utilizados de manera aceptable. El uso correcto de ello se define en los siguientes párrafos:

LINEAMIENTO PARA USO DEL CORREO INTERNO

1. Todo el personal de UNIPLEX, tiene derecho a una cuenta de correo electrónico en el servidor de correo.

2. Es responsabilidad del usuario hacer buen uso de su cuenta, entendiendo por buen uso:

- El no mandar ni contestar cadenas de correo.
- El uso de su cuenta con fines académicos y/o investigación.
- La depuración de su INBOX del servidor (no dejar correos por largos periodos en su buzón de correo).
- El no hacer uso de la cuenta para fines comerciales.

- El respetar las cuentas de otros usuarios Internos y Externos.
- El uso de un lenguaje apropiado en sus comunicaciones.

3. Se asignará solamente una cuenta por usuario.

4. Las cuentas conmutadas para el personal administrativo serán asignas por el administrador del servidor de correo.

5. Su cuenta de correo es personal e intransferible no permitiéndose que segundas personas hagan uso de ella, (compañeros, amigos, hijos, etc.). A menos que sea de asuntos primordiales relacionados con el trabajo.

6. La cuenta se dará de baja cuando UNIPLEX lo considere conveniente una vez que el personal deje de pertenecer a la empresa.

7. Es responsabilidad del usuario el cambiar su password con regularidad, cumpliendo con las normas que se definen en administración de correo acerca del manejo de passwords seguros. El tiempo de vida de los passwords dependerá será de seis meses.

8. El usuario será responsable de la información que sea enviada con su cuenta, por lo cual se asegurará de no mandar SPAMS de información, ni de mandar anexos que pudieran contener información nociva para otro usuario como virus o pornografía.

9. El usuario es responsable de respaldar sus archivos de correo manteniendo en el INBOX (Buzón de correo) solamente documentos en tránsito, sus demás comunicados deberá mantenerlos en su equipo personal o en su defecto en carpetas dentro de su cuenta en el servidor.

10. Al responder comunicados generales o para un grupo específico de usuarios, el usuario deberá cuidar de no responder a TODOS los usuarios salvo cuando ésta sea la finalidad de la respuesta.

11. UNIPLEX se reserva el derecho de enviar al usuario la información que considere necesaria como un medio de comunicación empresarial.

12. La vigencia y espacio de las cuentas será definida por el administrador del Servidor de correo (con la autorización respectiva) de acuerdo a los recursos disponibles, con base en las necesidades del usuario.

13. UNIPLEX se reservará el uso de monitorear las cuentas que presenten un comportamiento sospechoso para la seguridad de la empresa.

14. El usuario es responsable de respetar la ley de derechos de autor, no abusando de este medio para distribuir de forma ilegal licencias de software o reproducir información sin conocimiento del autor.

15. El incumplimiento por parte del usuario del buen uso de su cuenta puede ocasionar la suspensión y posterior baja del sistema de su cuenta.

16. Se recomienda a los usuarios grabar sus trabajos en discos flexibles una vez que su computadora haya revisado el disco con un antivirus actualizado, para evitar cualquier pérdida de información valiosa para ellos.

LINEAMIENTO DEL USO DE INTERNET

1. Desde el equipo asignado a cada usuario será posible hacer uso de la red Internet, únicamente para fines consultivos, definiéndose como consultivo a todas aquellas búsquedas de información que apoyen al usuario a resolver un problema o inconveniente.

2. El administrador de la red es el encargado de asignar una máquina al usuario, quien será responsable durante el tiempo que permanezca en su poder.

3. UNIPLEX se reserva el derecho de revisión para verificar que el software instalado tenga las licencias respectivas en el caso que amerite.

4. Cualquier uso que cause efectos opuestos a la operación de UNIPLEX o ponga en riesgo el uso o rendimiento de la red, será analizado por esta administración para tomar medidas.

5. En caso de usar la cuenta a través de Internet se debe asegurar de salir totalmente de la misma en cada sesión, cuando se desocupe el equipo.

LINEAMIENTO PARA USO DE EQUIPOS

1. Cuando exista la necesidad de sacar un equipo de Uniplex se debe tener autorización del coordinador y de gerencia y la respectiva nota de entrega.

2. No es permitido que los usuarios utilicen equipo de la empresa para asuntos personales (como alquiler a terceros, pruebas personales, entre otros).

3. Cuando se sale con equipos, es necesario disponer de transporte seguro como puede ser un servicio de taxis a domicilio.

LINEAMIENTO PARA USO DE DOCUMENTOS

1. En la empresa existe documentación de equipos que esta a disposición de los empleados para realizar consultas o configuraciones. Los manuales de los equipos deben ser utilizados solamente dentro de la empresa.

2. Si es necesario llevar un manual fuera de la oficina se debe notificar de este hecho al coordinador mediante un correo electrónico.

3. Si el documento esta en digital, se aplicará el acuerdo de confidencialidad.

INSTRUCCIONES DE TRABAJO

Titulo:			
Instructivo de Inventario de Activos			
Serial:	**Fecha Emisión:**	**Fecha Modificación:**	**Aprobación:**
Elaborado Por:	**Revisado y Aprobado Por:**	**Página:**	

I. INTRODUCCIÓN

El presente instructivo permite realizar un inventario de los activos de información que dispone el área de Networking de la empresa Uniplex Systems S.A.

II. PROCEDIMIENTO PARA REALIZAR EL INVENTARIO

Todos los activos deben ser registrados.

La siguiente tabla muestra las características que se deben tomar de cada activo del área. Se llenarán los datos que apliquen.

Ítem	**Equipo**	**Producto**	**Serial Number**	**Part Number**	**Descripción**

Cuando exista la necesidad de prestar o rentar un activo, entonces deberá llenarse una nota de entrega para tener un registro de movimiento del activo.

A continuación se presenta el formato para solicitar equipos al área.

NOTA DE PEDIDO	
Fecha:	**Nota de Pedido No:**
Solicita:	
Cliente:	
Fecha de préstamo:	**Días aproximados:**
Fecha de devolución:	
Motivo de Préstamo:	
Revisado Por:	**Autorizado Por:**
Observaciones:	

Listado de Equipos			
Ítem	**Equipo**	**Descripción**	**Cant.**
Atentamente		**Recibí Conforme**	

A continuación se presenta el formato para entregar equipos.

NOTA DE ENTREGA

Fecha:	**Nota de entrega No:**
Atención:	**Nota de Pedido No:**
Cliente:	
Fecha de préstamo:	**Días aproximados:**
Fecha de devolución:	

Observaciones:	

Sírvase encontrar adjunto a la presente lo siguiente:			
Ítem	**Equipo**	**Descripción**	**Cant.**

Atentamente		**Recibí Conforme**	

Titulo:			
Instructivo para Etiquetado y Manejo de la Información			
Serial:	**Fecha Emisión:**	**Fecha Modificación:**	**Aprobación:**
Elaborado Por:	**Revisado y Aprobado Por:**	**Página:**	

I. INTRODUCCIÓN

Aquí se describe la metodología a utilizar para la asignación del código o serial, la cual aplicará el área de Networking de la empresa Uniplex Systems para identificar los documentos del Plan Piloto de Políticas de Seguridad Informática.

II. PROCEDIMIENTO PARA ETIQUETAR DOCUMENTOS.

Todos los documentos emitidos en el PPPSI serán identificados con una numeración alfanumérica única para cada documento, este número será conocido como el identificador del documento.

El primer carácter (desde la izquierda) corresponde a la función del documento. A continuación se detallan las diferentes funciones del documento.

I Instrucción de trabajo.- Es un documento en donde se define paso a paso el “como” de una actividad.

F Formulario.- Documento utilizado para anotar los resultados de cualquier actividad, el cual podría convertirse en registro.

M Manual.- Es un documento compuesto por cierta extensión en cuanto a número de paginas, que contiene información del Sistema de Gestión de Seguridad de Información.

P Procedimientos.- Es el documento que define “quién hace qué” y “cuándo”. Este documento describe la forma específica para llevar a cabo una actividad o proceso.

R Registros.- Son documentos que sirven como evidencia para demostrar a terceros que un requisito del Plan Piloto de Políticas de Seguridad Informática está implantado y ha sido cumplido. Es un documento donde se mantienen anotados los resultados de alguna actividad realizada. Los registros son las huellas del PPPSI; con ellos se puede demostrar a otros que los “DEBE” o “Actividades” que exige la norma se han realizado.

L Política (Lineamiento).- Es un documento que sirve de lineamiento o guía, que se debe cumplir en el grupo. Las políticas son normas con las cuales hay que cumplir, una actividad o algún aspecto de Networking.

T Tablas.- Es un documento del PPPSI el cual contiene información relevante de la organización. Su representación gráfica podría ser un cuadro, una matriz, etc.

G Guía.- Es un documento que sirve como orientación o consulta y permite localizar fácilmente, en un solo documento, gran parte de los conceptos relacionados con un aspecto en particular.

Los dos siguientes caracteres son numéricos e identifican a cual área de la empresa pertenece el documento según la siguiente tabla:

01	Networking
02	Capacitación
03	Ventas
04	Presidencia
05	Legal
06	Software

07 Administración
08 Atención al cliente

Los tres siguientes dígitos muestran el orden secuencial del documento.

El siguiente carácter, que es alfanumérico, representa una modificación al documento. Se inicia con la primera letra del alfabeto y así hasta la ultima.

Siempre que se modifique un documento, al final se debe incluir un anexo, donde se enumeren las razones por las cuales se ha modificado dicho documento.
En dicho anexo, se especificará el (los) tipo (s) de cambio (s) aplicado(s) al documento, según:

A Añadido.- Se refiere a cuando se agrega algún párrafo o renglón al documento.

F Fusionado.- Se refiere cuando se unifican dos o más documentos en uno solo.

M Modificado.- Se refiere a cuando el cambio solamente se efectúa en algunas partes del documento.

R Reemplazado.- Se refiere a cuando el documento es totalmente cambiado.

Cuando un documento sea modificado, se deberá registrar la fecha en que se aplicaron los cambios en el cuadro “Fecha modificación” del formato del documento, siempre se mantendrá la “Fecha de emisión” intacta.

Si existe un documento que hace referencia a otro, se debe hacer referencia solamente al número serial del equipo mas no a la parte de la modificación; esto es para evitar realizar cambios en todos los documentos que tengan como referencia al documento modificado.

Titulo:			
Instructivo para Revisión de las Políticas de Seguridad Informática			
Serial:	**Fecha Emisión:**	**Fecha Modificación:**	**Aprobación:**
Elaborado Por:	**Revisado y Aprobado Por:**	**Página:**	

I. INTRODUCCIÓN

El presente instructivo para la revisión de las políticas de seguridad Informática evalúa la efectividad de las políticas de seguridad Informática implementadas en el área de Networking de la empresa Uniplex Systems S.A.

II. REVISIÓN DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA

Se debe revisar cada política implementada en el área de Networking con base a la siguiente tabla.

Política	Efectividad de la Política				Observación
	Excelente	Buena	Mala	Pésima	

Si existe documentación de actividades relativas con las políticas, se debe tomar en cuenta para evaluar la política y debe registrarse una observación al respecto.

REGISTROS

Titulo:			
Registro de Compromiso de la Dirección con la Seguridad Informática			
Serial:	**Fecha Emisión:**	**Fecha Modificación:**	**Aprobación:**
Elaborado Por:	**Revisado y Aprobado Por:**	**Página:**	

I. INTRODUCCIÓN

En el presente documento se registra el compromiso que la gerencia establece con el Plan Piloto de Políticas de Seguridad Informática ha implementarse en el área de Networking de la empresa Uniplex Systems S.A.

II. COMPROMISO DE LA GERENCIA CON EL PPPSI

La Gerencia de la empresa Uniplex Systems S.A. ha leído y se encuentra conciente cuan importante es el establecimiento de políticas de seguridad Informática en el área de Networking.

Es por esto que la Gerencia manifiesta el compromiso y el apoyo activo para con el proyecto de implementación de políticas de seguridad Informática.

La Gerencia puede intervenir en el desarrollo e implementación de las políticas, incluso puede dar por terminado el desarrollo de la implementación en caso de considerarlo necesario.

Titulo:			
Registro de Contacto con Grupos de Intereses			
Serial:	**Fecha Emisión:**	**Fecha Modificación:**	**Aprobación:**
Elaborado Por:	**Revisado y Aprobado Por:**	**Página:**	

I. INTRODUCCIÓN

Este registro permite verificar que la persona encargada del contacto con grupos de interés está cumpliendo sus obligaciones.

II. REGISTRO DE CONTACTOS

Fecha de Contacto:

Tema Tratado:

Fuente de información:

Titulo:			
Registro de Contacto con las Autoridades			
Serial:	**Fecha Emisión:**	**Fecha Modificación:**	**Aprobación:**
Elaborado Por:	**Revisado y Aprobado Por:**	**Página:**	

I. INTRODUCCIÓN

El presente documento es un registro de haber tenido contacto con el coordinador y la gerencia acerca del PPPSI.

II. TEMAS TRATADOS

A continuación se especifican los temas mencionados con las autoridades.

Titulo:			
Registro de Revisión Independiente de la Seguridad Informática			
Serial:	**Fecha Emisión:**	**Fecha Modificación:**	**Aprobación:**
Elaborado Por:	**Revisado y Aprobado Por:**	**Página:**	

I. INTRODUCCIÓN

Este documento es un registro de auditoria interna que debe ser realizado una vez cada seis meses en el área de Networking de la empresa Uniplex Systems.

II. DETALLE DE AUDITORÍA

A continuación se presentan las novedades encontradas en la auditoría interna.

ANEXO 3

IMPLEMENTACIÓN DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA

ANEXO 3: IMPLEMENTACIÓN DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA

A continuación se muestran algunas políticas de seguridad informática que sido implementadas en el Área de Networking de la empresa Uniplex Systems S.A.

Por motivos de confidencialidad se indican solo algunas políticas en imágenes.

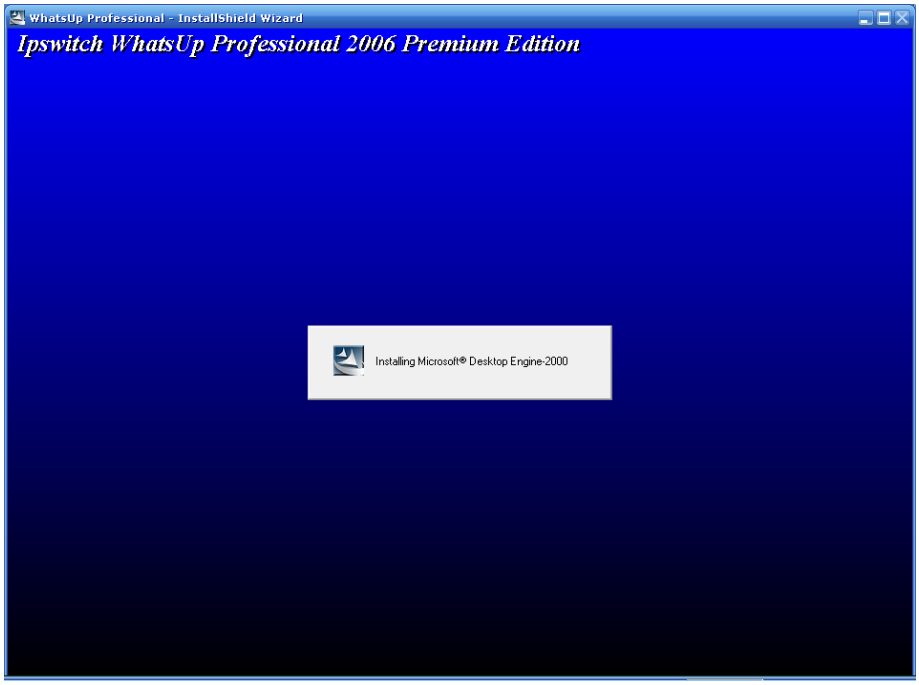
Política: Instalar Software que permita monitorear el estado de las interfaces de los equipos de la red y que se generen alarmas en caso de falla de una de éstas. Las alarmas pueden incluir envío de mail, envío de sms entre otras.

En el área de networking se instaló el programa What's Up, que es una herramienta útil para el monitoreo de la red y permite generar alarmas para notificar algún evento. Se indica el procedimiento de instalación.

Se acepta el contrato de licencia.

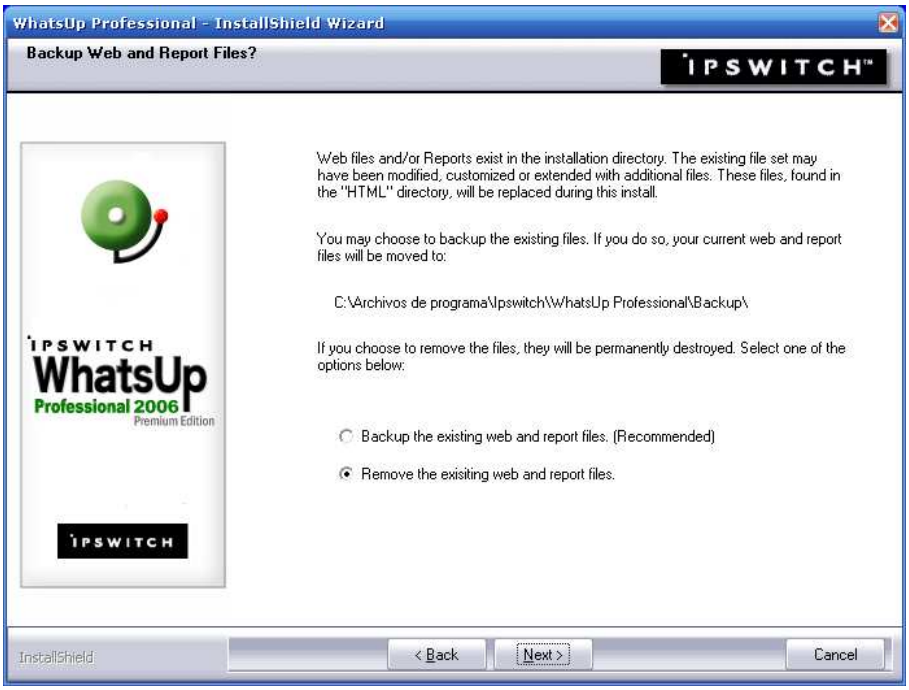
Se elige el path de instalación de la base de datos utilizada por el software.

Procedimiento de Instalación.

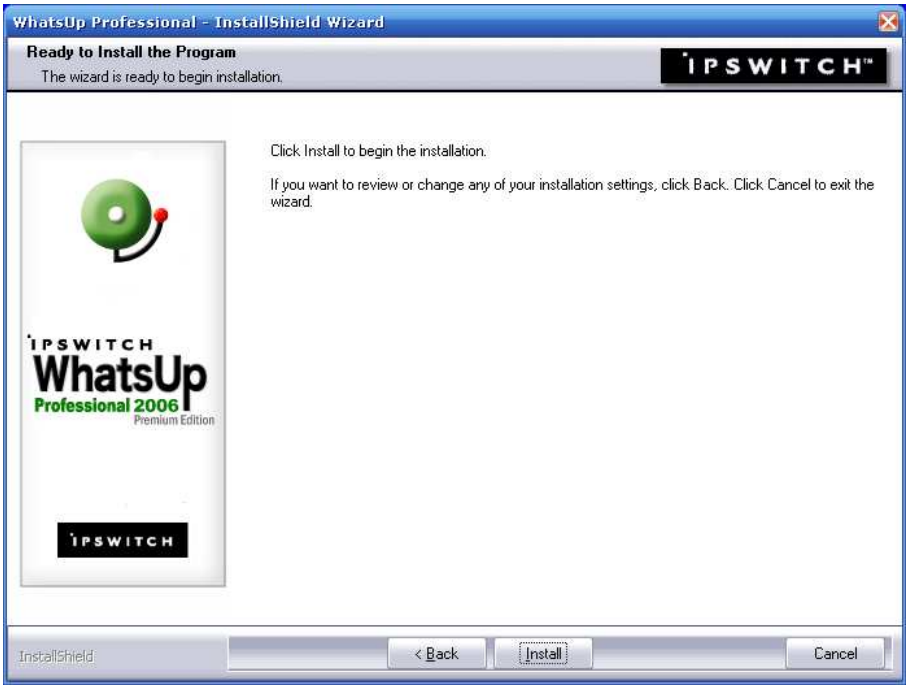


Se elige el path de instalación del programa.

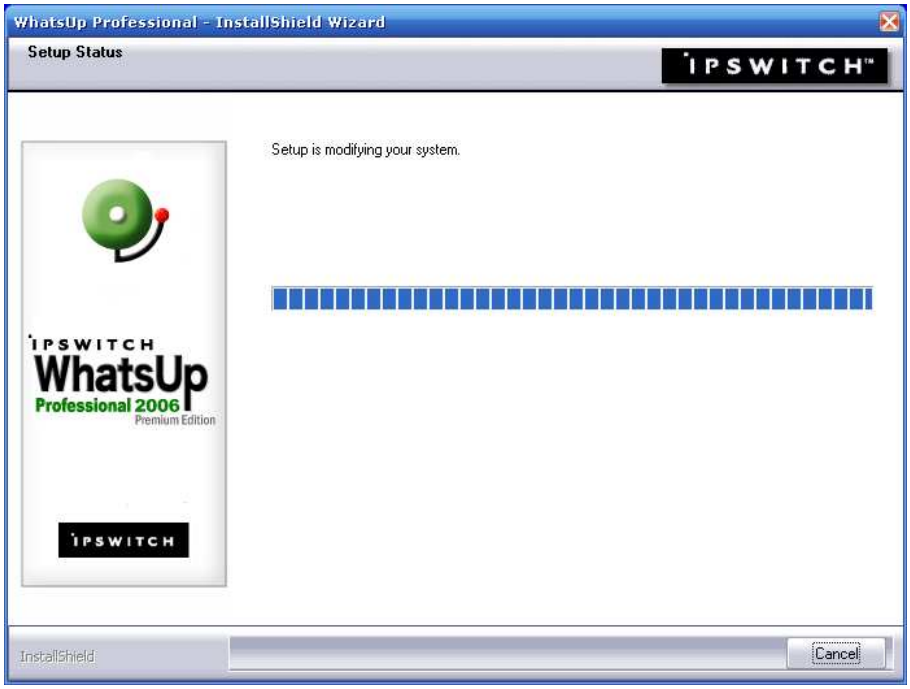
Como el servidor disponía de otra base de datos anteriormente instalada pero que ya no se utiliza se la elimina y se instala la nueva.



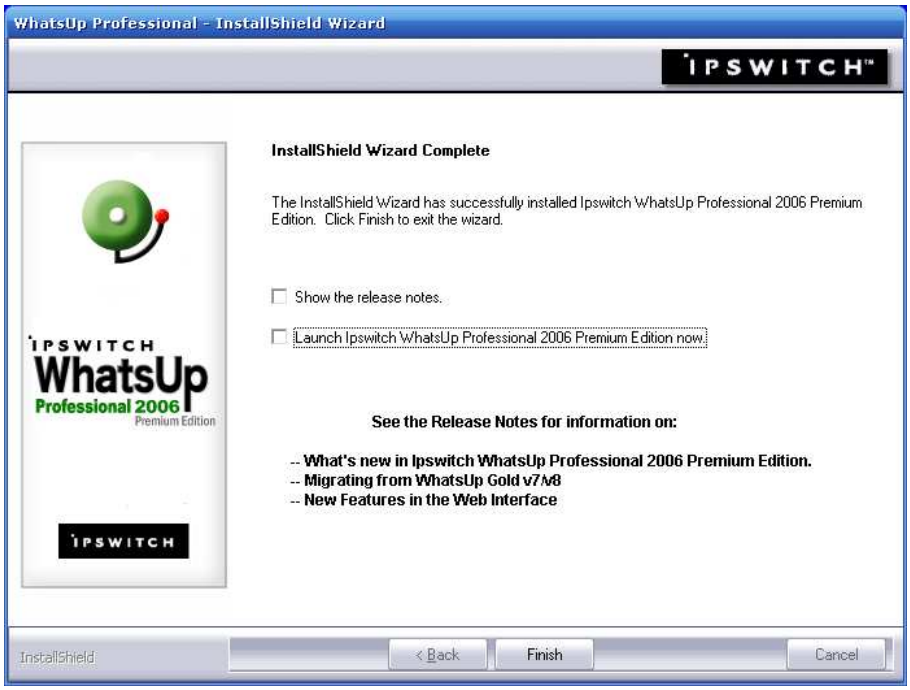
Inicia la ejecución de los instaladores.



Proceso de Instalación completo.

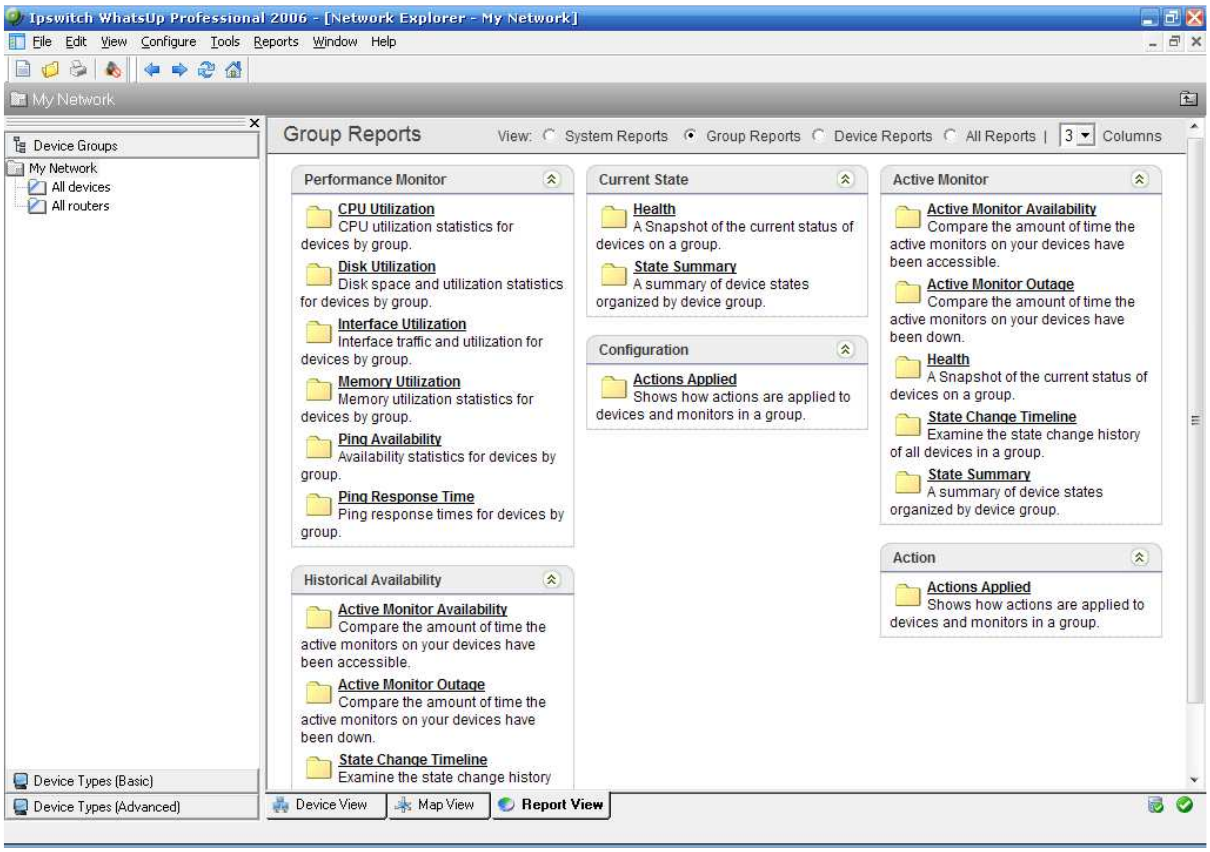


Muestra la opción de ejecutar el programa al instante de terminar la instalación.



Todas estas características pueden ser habilitadas para monitoreo de la red, por supuesto dependen del equipo a ser monitoreado.

Para networking se tiene habilitado el monitoreo en base a la prueba de conectividad básica (PING) para los equipos principales de la red.



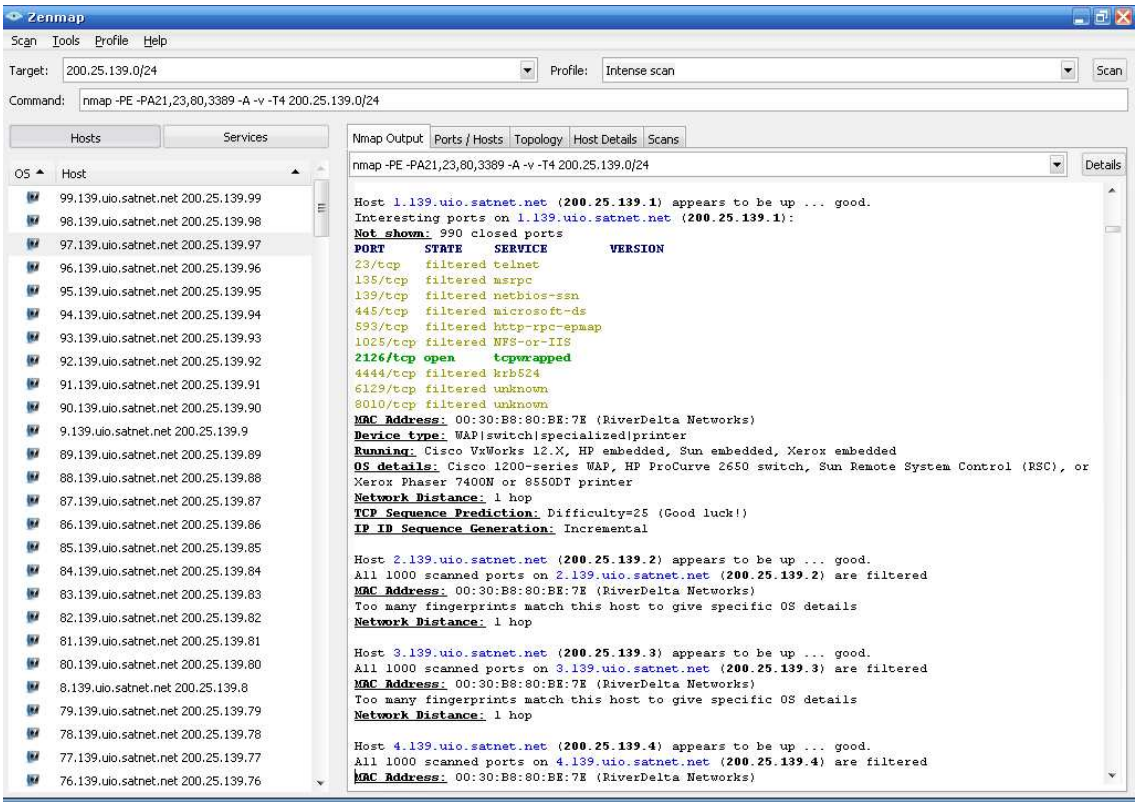
Política: Revisar el tráfico cursado en la red cada mes o cuando la situación lo amerite para determinar si existen comportamientos anómalos y analizarlos.

Para esta política se utiliza dos software que monitorean tráfico ya sea de un host en específico o de una red completa. Permiten guardar un registro de los eventos registrados.

SOFTWARE NMAP

No se indica cómo instalar el programa para proteger a los usuarios.

Como ejemplo; en el siguiente gráfico se apreciar el escaneo realizado a toda la red y los puertos que utiliza un host específico.

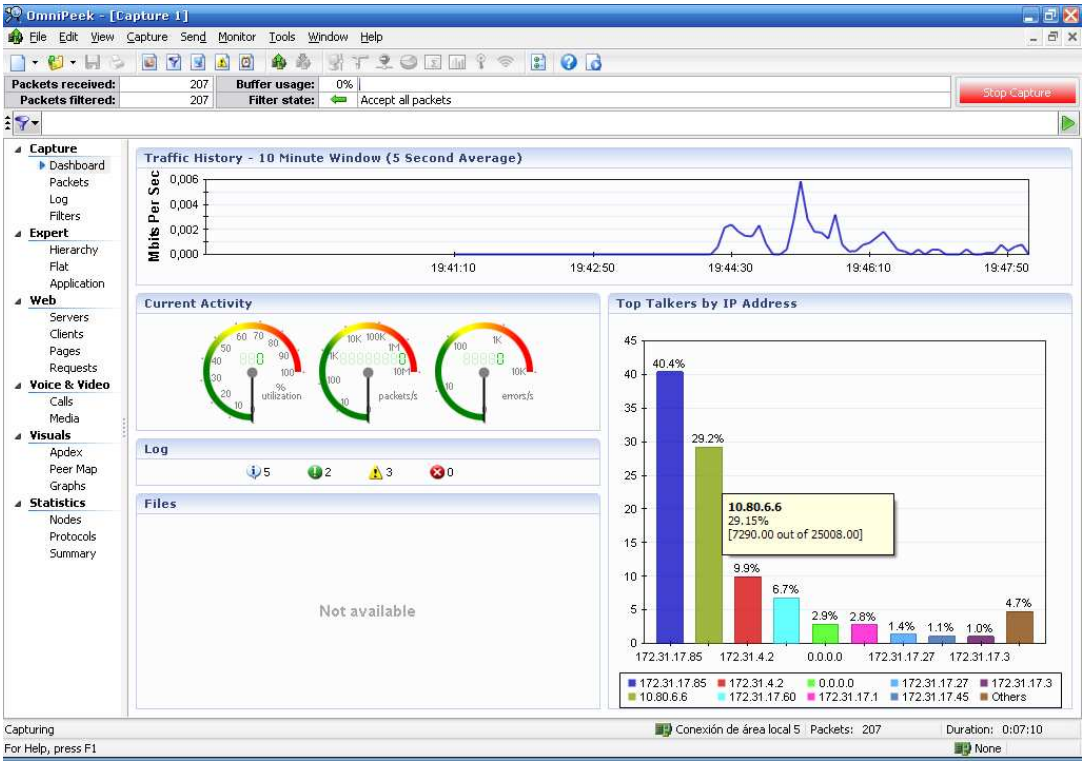


SOFTWARE OMNIPEEK

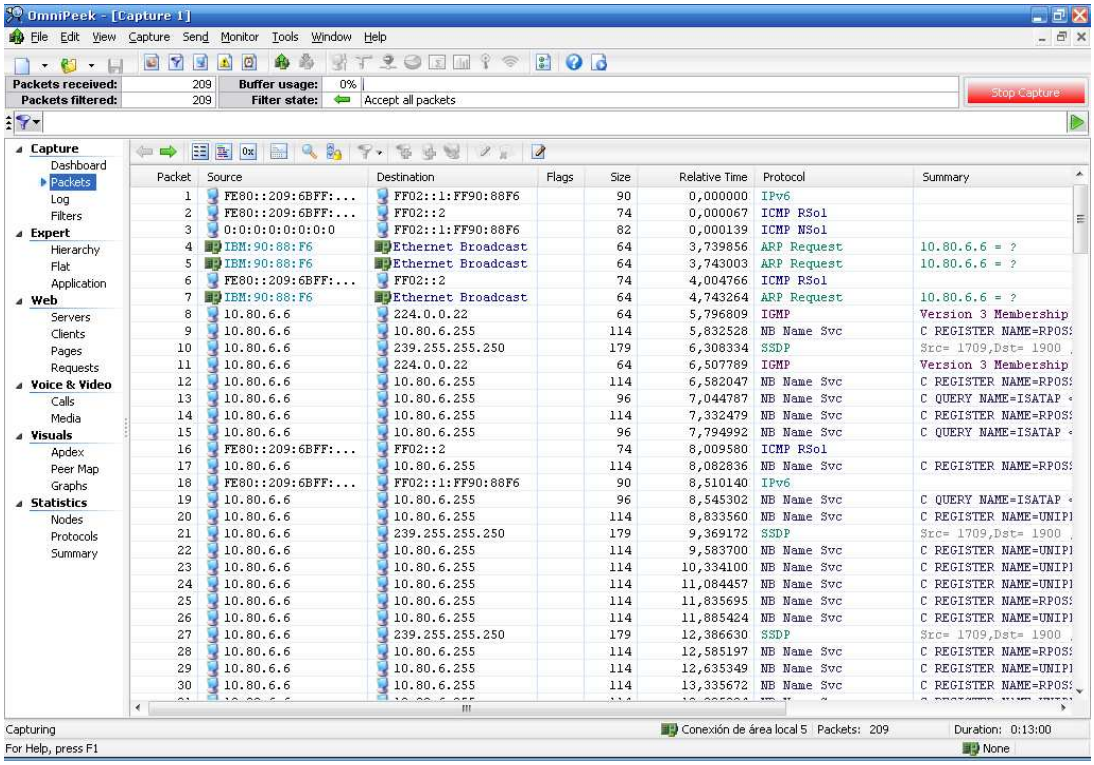
No se indica como instalar el programa para proteger a los usuarios.

Este programa permite obtener tráfico muy detallado de toda la red o de un Host como se puede ver en los siguientes gráficos.

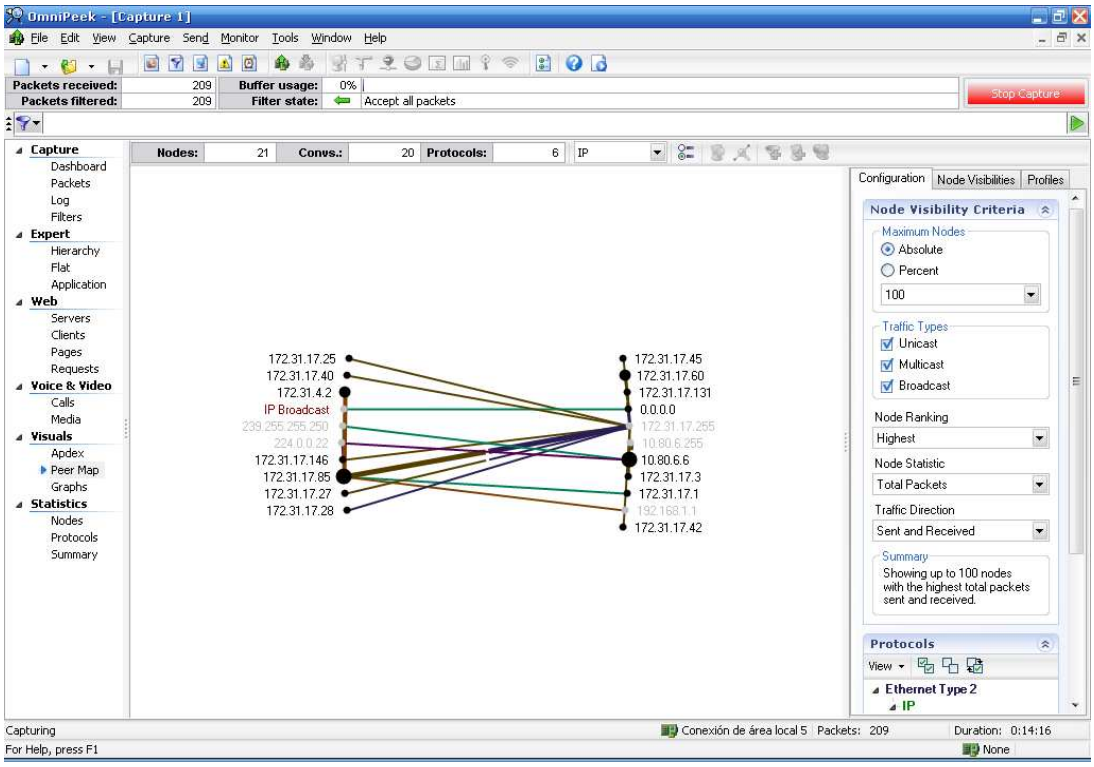
Muestra los que mas trafico están cursando (en este caso al Host)



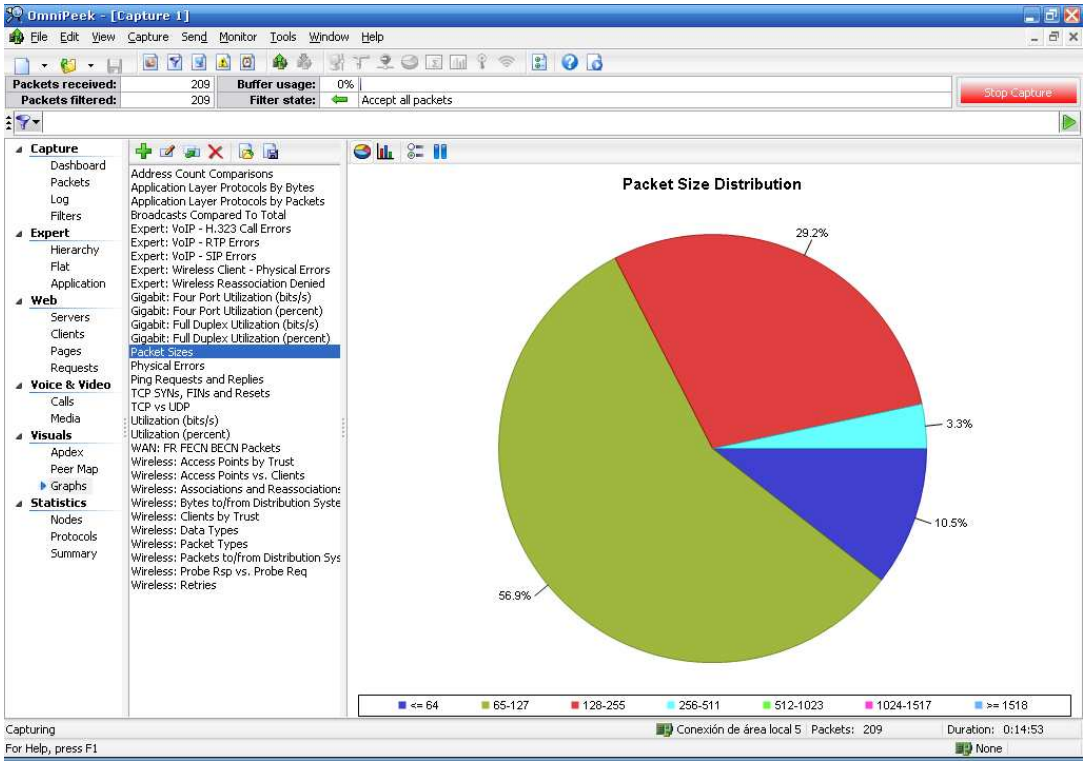
Paquetes entre MAC origen y destino y el protocolo que utiliza.



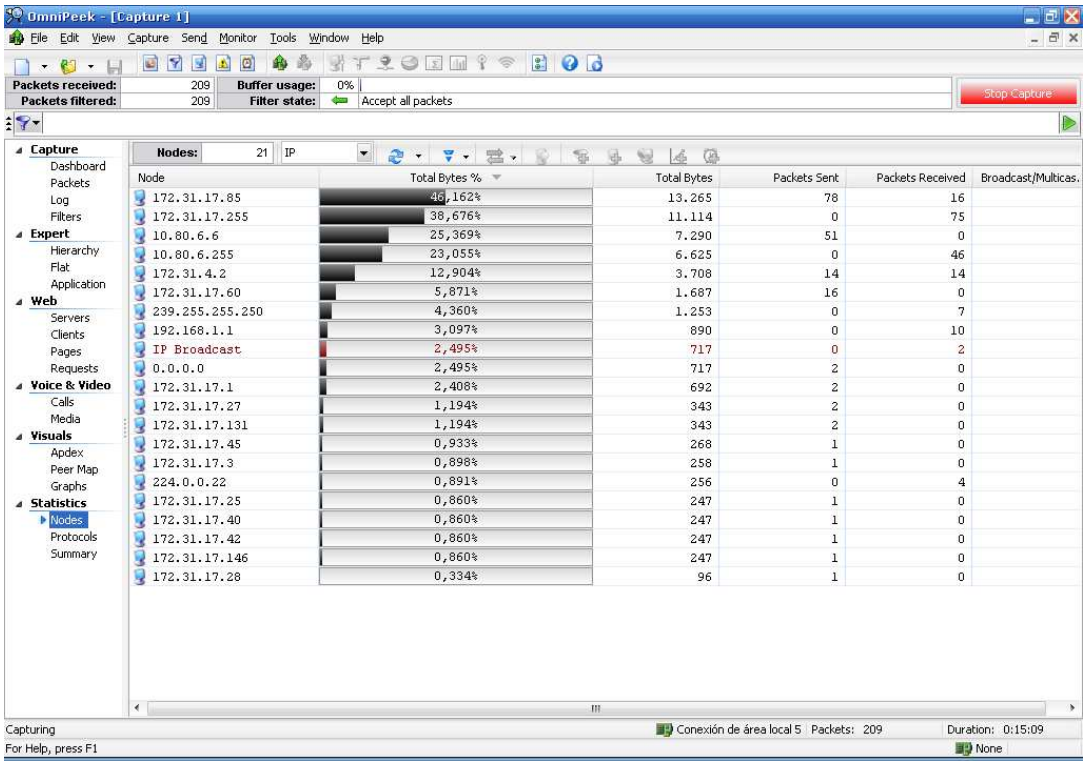
Conversaciones que se establecen entre el Host y todo su ambiente de trabajo.



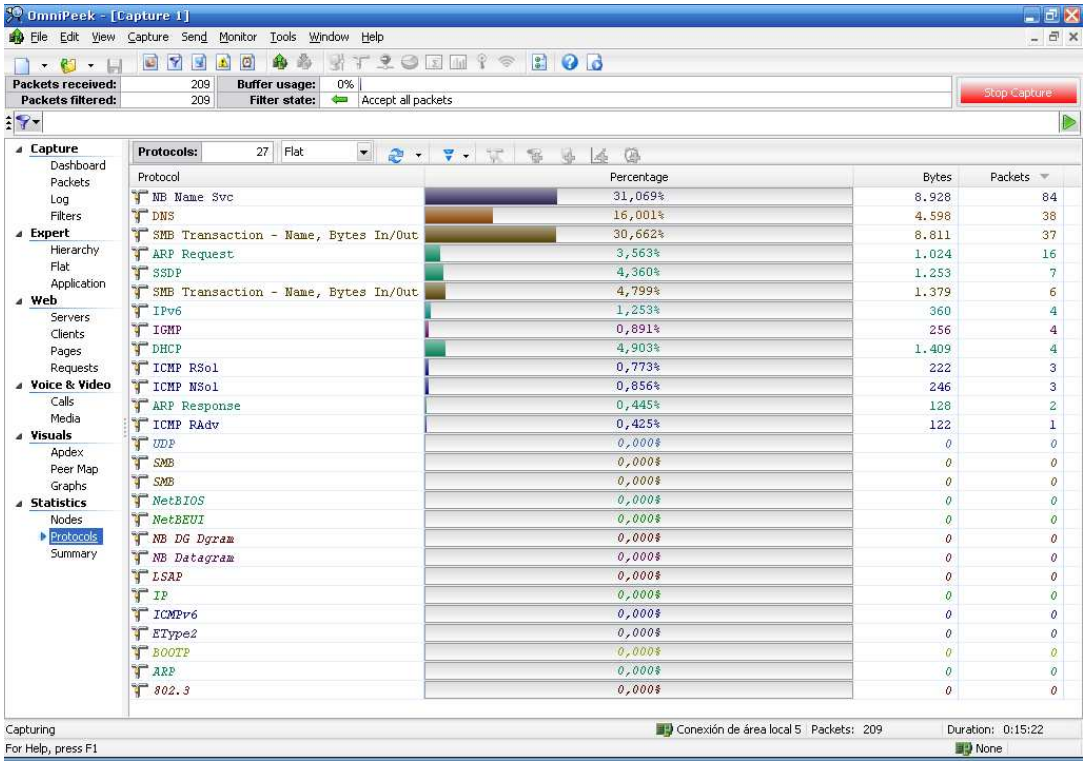
Tamaño de paquetes transmitidos y recibidos.



Estadísticos de los Host que utilizan mayormente el protocolo IP.



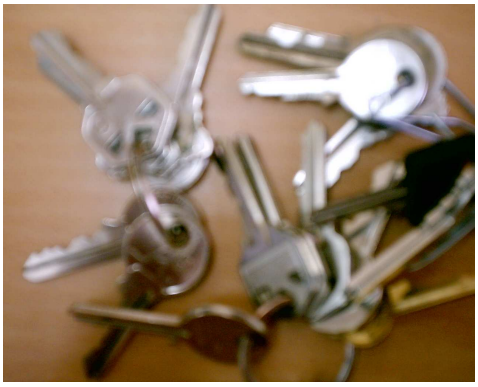
Protocolos que se utilizan en la comunicación.



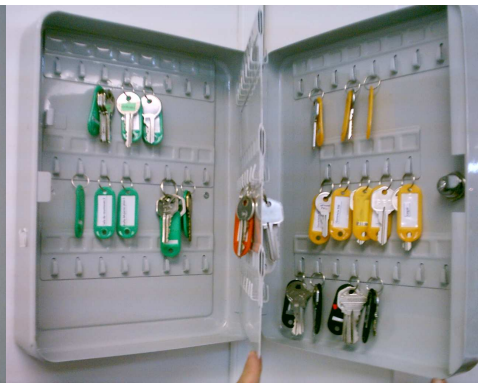
Política: En caso de encontrar llaves, debe verificar si pertenecen al área y clasificarlas, en caso de que sea ajeno al área debe notificar y entregar al departamento de administración.

En el área de networking se encontraron diferentes llaves, se clasificaron o se entregaron al departamento de administración.

ANTES

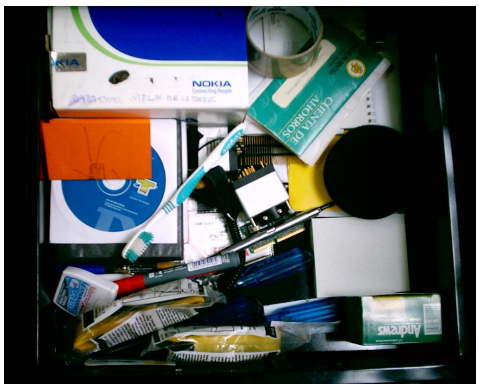


DESPUÉS



Política: Clasificar la información en términos de su valor, sensibilidad e importancia. Debe utilizar el instructivo para clasificación de la información

ANTES



DESPUÉS

ANEXO 4
GUÍA DE USUARIOS

ANEXO 4: GUÍA PARA LOS USUARIOS

PLAN PILOTO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

INTRODUCCIÓN

En la actualidad, la información se encuentra distribuida por todos lados y en todos los medios; por esto es necesario asegurarse que la información que manipula se encuentra correctamente protegida para evitar que personas no autorizadas tengan acceso.

En la mayoría de incidentes reportados la responsabilidad recae en personas que no cometieron el delito, en otros casos a pesar que se conoce al autor de la acción no es posible sancionarlo por falta de evidencias.

El presente manual es un instructivo que permite entender y aplicar correctamente las normas de seguridad para evitar situaciones similares a las mencionadas.

Autorización de Acceso a Información

Existe un acuerdo de confidencialidad que usted ha firmado con la Empresa Uniplex Systems S.A. referente a la información; es por esto que usted tiene acceso libre a cierto tipo de información, esta información la puede encontrar en los gabinetes de su área (manuales, CD’s Brochures, entre otros).

Cuando requiera tener acceso a información o equipo que está en bodega, debe solicitar al coordinador del área y al administrador de la red autorización. En caso de ausencia de cualquiera de los dos, la solicitud debe ser realizada a gerencia.

En la solicitud debe incluir básicamente qué información o equipo necesita, la razón por la cual lo solicita y el tiempo estimado que usted dispondrá la información o equipo.

Se debe tener un registro de haber realizado la solicitud con la respectiva respuesta (afirmativa o negativa) y mostrarla al administrador de la red o al coordinador del área para tener acceso o no a la información.

Cuando tenga acceso a la información o equipo, usted debe verificar el estado del mismo y comunicar inmediatamente al coordinador cualquier novedad caso contrario usted será responsable por los daños encontrados.

Una vez concluido el periodo de préstamo; usted debe entregar la información o equipo al coordinador, quien verificara el estado de la misma y procederá a colocarla en su sitio.

Password

Por normas de la empresa el usuario solo tendrá una contraseña privada para el uso de su correo, las demás contraseñas (acceso al Dominio, acceso al BIOS, acceso como administrador de la estación de trabajo) las tendrá registradas el administrador de la red quién será el responsable de la integridad, confidencialidad y disponibilidad de esta información.

Recuerde que el password del correo debe ser robusto, evitando usar palabras de diccionario, fechas recordatorias, nombres de personas o algo conocido, etc. Se recomienda utilizar símbolos para que su contraseña sea más segura.

Para establecer una contraseña usted puede seguir el siguiente consejo.

Arme una frase que a usted le guste "Yo Soy El Más Maestro De Los Password Y Punto", luego tome las iniciales de cada palabra (YSE+MDLPY.), nótese que la palabra "Más" y "Punto" han sido reemplazadas por los signos "+" y "."; de esta manera se consigue un password fácil de recordar y robusto.

Requerimientos de Password:

- Los password deben contener al menos 6 caracteres.
- Los password deben ser cambiados al menos cada seis meses (Solo los que correspondan cambiarlos a usted).
- En caso de que usted deba abandonar la empresa, debe dejar cambiando su password a uno sencillo y debidamente comunicado a gerencia.

Cuidados con los Password:

- Nunca escriba su password en ninguna parte.
- Nunca use su nombre, el de su compañero, el de sus hijos, algo acerca de usted o sus familiares.
- Nunca use números especiales que sean relacionados con usted, por ejemplo: su número de teléfono, de cédula, de licencias o cualquier cosa que pueda ser descifrada por alguien.
- Nunca utilice un único carácter en su password, esta clave puede ser descifrada muy fácilmente (11111111 o PPPPPPPP).
- Nunca comparta su contraseña con otras personas.
- Nunca use las contraseñas que vienen preestablecidas con un Software, esta contraseña debe ser cambiada.
- Nunca tenga almacenado en su PC “Recordar contraseñas”.

En resumen, trate su contraseña con cuidado, escoja una fuerte y cámbiela regularmente

Antivirus y Antispam

Queda bajo responsabilidad del usuario verificar que su computador se encuentre libre de virus para lo cual debe actualizar su antivirus periódicamente y escanear su computadora.

Si dispone de un medio de almacenamiento de información externo (flash, disco, disquete, etc.), primero debe correr el antivirus previo a tener acceso a la información en el dispositivo.

Si se registra un virus que no puede ser eliminado, entonces debe comunicar inmediatamente al administrador de la red.

Existen archivos SPAM que utilizan hackers y empresas para hacer publicidad, este tipo de archivos llegan como mensajes de correo basura y pueden ser utilizados para:

- Un frente para un fraude.
- Un correo electrónico en cadena.
- Ejecutar códigos ocultos que alterará las configuraciones en su computadora (por ejemplo: dirigirle a usted a un sitio porno).

Si el correo SPAM no tiene ningún valor, ni es relevante para usted o su empresa, solo bórrelo sin abrirlo.

Nunca responda al correo electrónico spam.

No dar su dirección de correo electrónico a cualquiera, excepto a personas que tengan relación con la empresa y en las que usted pueda confiar.

Si un sitio de Internet le pide su dirección de correo electrónico, haga una valoración de riesgos rápida. ¿Es una organización legítima que tiene establecida una reputación? ¿Es alguien que usted nunca ha escuchado antes o no tiene una dirección física de la empresa en el sitio Web? Recuerde que el embustero planea aparentar una empresa legítima.

Si tiene cualquier duda respecto a un mail, por favor comuníquese con el administrador de la red.

Spyware

Estos son pequeños programas que se insertan en el sistema de la computadora para recoger secretamente la información sobre usuarios/empresas sin que ellos lo sepan.

Esto es principalmente para recoger información sobre direcciones de correo electrónico e incluso las contraseñas y detalles de tarjetas de crédito.

Recientemente han surgido advertencias oficiales sobre Spyware que se usan para recoger información sensible comercial, por ejemplo: detalles de contratos.

Si usted sospecha que tiene Spyware instalado en su computador se recomienda que se comunique inmediatamente al administrador de la red.

Parches

Los parches son poco conocidos pero son muy importantes ya que son un soporte para las vulnerabilidades en los sistemas operativos y programas, recuerde que todo tipo de software tiene problemas y defectos que necesitan ser corregidos.

Todos los sistemas operativos necesitan actualizarse de un tiempo a otro. Pero muchas aplicaciones también necesitan ocasionalmente parches.

Si no tiene actualizado su software, tiene el riesgo de que falle, puede que su antivirus no funcione adecuadamente o que una amenaza explote una vulnerabilidad.

Backup

El respaldo es el proceso de tomar una copia de los datos electrónicos, como una copia de archivos contables. Es necesario que usted realice un respaldo continuo

de su información, pues el momento menos pensado fallos en los equipos pueden ocasionar la pérdida de su información. Debe considerar lo siguiente:

Un respaldo formal y eficiente evitará que amenazas naturales o no intencionadas deje de funcionar su negocio. Usted puede copiar datos a:

- Cinta (un método considerado porque puede ser reutilizado).
- Un duplicado disco duro (preferiblemente uno removible)
- Un CD o un DVD

Los datos y frecuencia de respaldos que usted obtenga dependen de la criticidad de los datos. Se recomienda que usted tenga una partición en su disco para los datos importantes y copiados en CD o DVD.

Así pues; si se afecta su computador y no arranca, la partición mantendrá sus datos intactos; o se utilizaran los respaldos en DVD o CD para recuperar la información.

Cuando obtenga respaldo en CD o DVD, no olvide rotular de manera descriptiva sus datos. Uno de los mayores problemas con respaldos ocurre cuando el propietario olvide rotular la información apropiadamente.

Sus CD o DVD deben ser almacenados en su respectivo cancel bajo llave.

Robo de Información e Identidad

Para un negocio es de vital importancia tener la información almacenada apropiadamente, esto incluye papeles o copias electrónicas.

Un individuo puede robar su ID para realizar algún fraude. Mientras usted no es responsable por el fraude perpetrado por otros, el problema después del robo de un ID es recuperar credibilidad con bancos y otras organizaciones financieras.

Algunas cosas que no debe hacer:

- Nunca de información personal en Internet, vía e-mail, en el teléfono o por cartas a menos que usted esté seguro que la comunicación es confiable.
- Recuerde que los bancos nunca preguntan a los usuarios confirmar su password o código de acceso vía email así que no proporcione esta información.
- Cualquier evento extraño debe ser reportado inmediatamente para ser investigado.