ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001, PARA LA INTRANET DE LA CORPORACIÓN METROPOLITANA DE SALUD

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

ALVAREZ ZURITA FLOR MARÍA
GARCÍA GUZMÁN PAMELA ANABEL

DIRECTOR: ING. FERNANDO FLORES

Quito, Octubre 2007

DECLARACIÓN

Nosotras, Flor María Álvarez Zurita y Pamela Anabel García Guzmán, declaramos que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada por ningún grado o calificación profesional; y que hemos consultado las referencias bibliográficas que se incluyen en este documento.

La Escuela Politécnica Nacional, puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley, Reglamento de Propiedad Intelectual y por la normativa institucional vigente.

_____	_____
Flor María Álvarez Zurita	Pamela Anabel García Guzmán

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Flor María Álvarez Zurita y Pamela Anabel García Guzmán, bajo mi supervisión.

_____

Ing. Fernando Flores

DIRECTOR DE PROYECTO

AGRADECIMIENTO

Al Ing. Fernando Flores, por su valiosa guía y acertada dirección para la culminación de este proyecto.

Al Ing. José Carlos Álvarez, por su colaboración durante la recolección de la información para el desarrollo de este Proyecto.

A nuestros amigos y compañeros por la ayuda brindada y su amistad incondicional, sin sus palabras de aliento no hubiese sido posible continuar hasta la finalización del Proyecto.

Flor María Álvarez Zurita
Pamela Anabel García Guzmán

DEDICATORIA

A mis padres, César Álvarez y Zoila Zurita; que desde el cielo guiaron la culminación de mis estudios y me brindaron la luz que necesitaba para continuar.

A mis hermanos José y Fernando que de una u otra forma estuvieron junto a mí para apoyarme incondicionalmente.

A mi compañera de proyecto Pamela, por no desfallecer hasta conseguir la finalización del mismo.

A David que es un gran apoyo para mi desarrollo profesional y personal, que fue una luz en el camino de la culminación del proyecto.

Flor María Álvarez

DEDICATORIA

A mis queridos padres,
por su apoyo incondicional y su amor.

A mis hermanas y a mi hermano,
por estar siempre a mi lado.

A mi compañera Flor,
por no dejarse caer ante las adversidades

A ellos les debo el haber conquistado mis sueños.

Pamela Anabel García Guzmán

PRESENTACIÓN

El presente proyecto tiene como objetivo la Implementación de un Sistema de Gestión de Seguridad de la Información para la Intranet de la Corporación Metropolitana de Salud en base a la Norma ISO 27001 con el fin de lograr una gestión de la red de manera organizada, adecuada y garantizando que los riesgos de seguridad de la red sean minimizados en base a los procedimientos para el tratamiento de los mismos.

Para poder realizar este proyecto tomamos como bases las guías que se indican en la Norma ISO 27001, acorde a la realidad de la Corporación Metropolitana de Salud.

También se realizó un análisis preventivo y correctivo en mejora de la administración y gestión de la Intranet conforme a la Norma ISO 27001 identificando las vulnerabilidades presentes en la organización.

Por último presentamos la referencia de los costos que implican la implementación del Sistema de Gestión de Seguridad de Información en la Corporación, de acuerdo a los riesgos de seguridad encontrados en la organización.

RESUMEN

En el presente proyecto de titulación se pretende dar una adecuada solución de seguridad a la Corporación Metropolitana de Salud, tomando como base estándares internacionales.

El primer capítulo proporciona los lineamientos básicos de la seguridad de la información, una visión general de la gestión de riesgos así como las diferentes alternativas para el tratamiento de los riesgos identificados , la evolución de la norma 27001, y finalmente nos da una descripción de la Norma ISO 27001:2005, en donde señala que la seguridad de información no se trata sólo de aspectos tecnológicos sino su objetivo es organizar la seguridad de información, es por este motivo que propone toda una secuencia de acciones tendientes al “Establecimiento, Implementación, Operación, Monitorización, Revisión, Mantenimiento y Mejora del SGSI (Sistema de Gestión de Seguridad de la Información).

En el segundo capítulo se presenta una breve descripción de los 11 dominios del estándar ISO 17799, en el cual se documenta los procesos y procedimientos que ayudarán a garantizar la seguridad de la información en la CMS.

En el tercer capítulo se muestra el análisis de la situación actual de la CMS, a partir de este resultado se identifican los activos más importantes para la empresa y se realiza una identificación, análisis y evaluación de vulnerabilidades en la CMS, para posteriormente realizar una selección de controles y objetivos de control de la Norma ISO 17799.

En el cuarto capítulo se presenta un plan de tratamiento de riesgos en donde se identifican las acciones apropiadas así como los responsables para minimizar los riesgos identificados para posteriormente realizar la implementación del SGSI en base a los controles seleccionados y finalmente se obtiene como resultado el manual de procedimientos para la implementación

del SGSI. Lo cual se complementa con costos referenciales de la implementación del sistema propuesto. En el capítulo final se dan las conclusiones y recomendaciones en base al desarrollo de este proyecto de titulación.

ÍNDICE

CAPITULO II: DESCRIPCIÓN DE LOS 11 DOMINIOS DEL ESTÁNDARES ISO 27001

INDICE DE FIGURAS

CAPITULO I:

CAPITULO III:

CAPITULO IV:

INDICE DE TABLAS

CAPITULO III:

CAPITULO IV:

I

INTRODUCCIÓN Y NORMAS ISO PARA LA SEGURIDAD DE LA INFORMACIÓN

1.1. CONCEPTOS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

1.1.1. INTRODUCCIÓN

En muchas organizaciones la seguridad de la información es tratada como un problema sólo tecnológico, sin tomar en cuenta que la seguridad de la información es un problema organizativo y de gestión, lo que con lleva a que las organizaciones no sean capaces de afrontar ataques provenientes de todos los ángulos.

No es suficiente contar con tecnología sofisticada, la gestión implica conocer la situación de lo que queremos tratar y tener claro hacia donde queremos ir, es decir, determinar un objetivo y tomar las acciones necesarias para conseguirlo. La definición de un modelo para la gestión de la seguridad de la información implica involucrar a toda la organización y no sólo al área encargada de implantar el modelo, lo cual trae como resultado el éxito del proyecto tanto en su implantación como en su mantenimiento, es así que se debe fomentar el cambio cultural para concienciar acerca de importancia de la seguridad.

El objetivo de seguir una recomendación internacional con respecto a la seguridad de la información es tener un protocolo común para la medida y gestión de los riesgos de información.

1.1.2. DEFINICIÓN DE SEGURIDAD DE LA INFORMACIÓN

La información de la empresa es uno de los activos más importantes que poseen y tiene un valor para la organización y por lo tanto se debería desarrollar mecanismos que aseguren una protección adecuada. Los objetivos de la seguridad de la información son proteger a la organización de amenazas, minimizar los años y maximizar el retorno de las inversiones y las oportunidades del negocio.

En vista de que la información de una organización puede adoptar diversas formas, como: escrita en papel, impresa, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en vídeo o hablada electrónicamente. Debería protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene.

La seguridad de la información consiste en la preservación de su confidencialidad, integridad y disponibilidad:

- **Confidencialidad:** acceso a la información por parte únicamente de quienes están autorizados.

- **Integridad:** mantenimiento de la exactitud y completitud de la información y sus métodos de procesos.

- **Disponibilidad:** acceso a la información y sus activos asociados por parte de los usuarios autorizados cuando lo requieran.

La seguridad de la información se consigue implantando un conjunto apropiado de controles, que pueden ser políticas, procedimientos, estructuras organizativas y funciones de software. El objetivo de estos controles es asegurar que se cumplen con los requisitos de seguridad de la información.

1.2. GESTIÓN DE RIESGOS

1.2.1. INTRODUCCIÓN

La gestión del riesgo es una parte fundamental de la Norma ISO 27001. Los controles en el anexo A del estándar deberían ser seleccionados en base a los resultados de la evaluación del riesgo, se requiere medir y evaluar los riesgos así como revisar y reevaluar los riesgos en una etapa futura para asegurar que se tiene implantando una eficaz seguridad de información.

Ya que los controles son seleccionados en base a los resultados de la gestión de riesgo, es claro que si una empresa no está bien informada sobre los riesgos no podrá alcanzar una efectiva gestión de control.

1.2.2. DEFINICIÓN DE RIESGO

Riesgo es el daño potencial que puede surgir por un proceso presente o evento futuro. Diariamente en ocasiones se lo utiliza como sinónimo de probabilidad, pero en el asesoramiento profesional de riesgo, el riesgo combina la probabilidad de que ocurra un evento negativo con cuanto daño dicho evento causaría.[1]

1.2.3. FUENTES DE RIESGO

Hay distintas fuentes las cuales pueden tener un impacto en la organización. Una fuente es llamada amenaza. Una amenaza tiene el potencial de causar un incidente no deseado, el cual puede provocar daños al sistema, la organización y a los activos. Pueden ser amenazas de la naturaleza, accidentes causados por negligencia o amenazas intencionales causadas por acciones maliciosas. Para que una amenaza cause daño tendría que explorar la vulnerabilidad del sistema, aplicación o servicio.

[1] Tomado de Wikipedia, la enciclopedia libre

Figura 1.1. Fuentes de riesgo

1.2.4. ANÁLISIS DEL RIESGO

Para implantar un Sistema de Gestión de Seguridad de Información según ISO 27000, la organización requiere determinar el alcance del estándar en la empresa, y en base a ese alcance identificar todos los activos de información. Luego es requerido un análisis de riesgo para identificar qué activos están bajo riesgo. El objetivo del análisis del riesgo es apreciar la magnitud del riesgo que afecta a los activos de la información. "Se deben tomar decisiones en relación a que riesgos la organización aceptará y qué controles serán implantados para mitigar el riesgo"[2]. Es deber de la gerencia revisar el SGSI a intervalos planificados para asegurar su adecuación y eficacia, ya que ISO 27001:2005 es un sistema dinámico que obliga a la gerencia estar constantemente revisando y definiendo controles, sus amenazas, vulnerabilidades e iniciar acciones correctivas y preventivas cuando sea necesario.

[2] Tomado del documento "Análisis del Riesgo y el Sistema de Gestión de Seguridad de Información. El enfoque ISO 27001:2005" (Alberts, Dorofeee, 2003).

1.2.5. PROCESO DE EVALUACIÓN DEL RIESGO

La figura 1.2 muestra el proceso de evaluación del riesgo que permite a una organización estar en conformidad con los requerimientos del estándar ISO 27001.

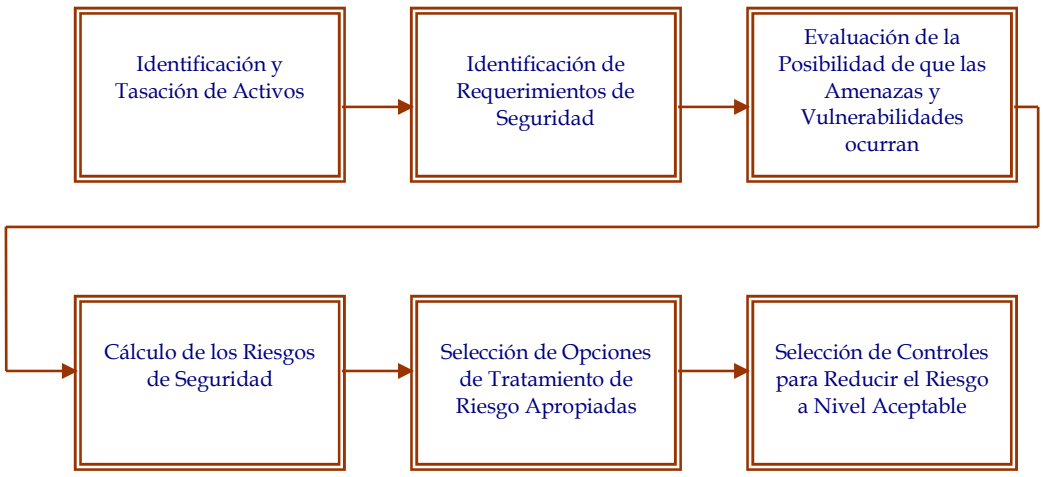

Figura 1.2. Proceso de Evaluación del Riesgos

Identificación y tasación de activos

Cada activo debe estar claramente identificado y valorado apropiadamente, y su propietario y clasificación de seguridad acordada en la organización. El ISO 17799:2005 (Código de Práctica para la Gestión de la Seguridad de Información) clasifica los activos de la siguiente manera:

1) Activos de información: bases de datos y archivos de datos, documentación del sistema, manuales de usuario, materiales de entrenamiento, procedimientos operativos de apoyo, planes de continuidad.

2) Documentos impresos: documentos impresos, contratos, lineamientos, documentos de la compañía, documentos que contienen resultados importantes del negocio.

3) Activos físicos: Equipos de comunicación y computación, medios magnéticos, otros equipos técnicos.

4) Personas: Personal, clientes, suscriptores.

5) Imagen y reputación de la compañía.

6) Servicios: Servicios de computación y comunicación, otros servicios técnicos.

La valoración de activos, basada en las necesidades del negocio de una organización, es un factor elemental en la evaluación de riesgos. Para poder encontrar la protección adecuada para los activos, es necesario evaluar su valor en términos de su importancia para el negocio. “Para poder tasar los valores de los activos y poder relacionarlos apropiadamente, una escala de valor para activos debe ser aplicada”[1].

Identificación de requerimientos de seguridad

Con el objetivo de identificar los requisitos de seguridad de la organización, es aconsejable basarse en las tres fuentes principales, que se describen a continuación:

a) La primera fuente es derivada de la valoración de riesgos de la organización. Con ella se identifica las amenazas a los activos, se evalúa las vulnerabilidades y la probabilidad de su ocurrencia.

b) La segunda fuente es el conjunto de requisitos legales, estatutos, regulaciones y contratos que debería satisfaces la organización, sus socios comerciales, los contratistas y los proveedores de servicios.

c) La tercera fuente está formada por los principios, objetivos y requisitos que forman parte del tratamiento de la información que la organización ha desarrollado para apoyar sus operaciones.

Identificación de amenazas y vulnerabilidades

Las vulnerabilidades son debilidades asociadas con los activos de la empresa. Las debilidades pueden ser explotadas por las amenazas, causando incidentes no deseados, que pudieran terminar causando pérdidas, daño o deterioro a los activos. La vulnerabilidad como tal, no causa daño, es simplemente una condición o conjunto de condiciones que pueden permitir que una amenaza afecte a un activo.

Cálculo de los riesgos de seguridad

El propósito de la evaluación del riesgo es el de identificar y evaluar los riesgos. La evaluación de riesgo es una consideración consecuente:

a) **Consecuencias**.- del impacto económico que probablemente resulte de un fallo de seguridad, teniendo en cuenta las posibles consecuencias de pérdida de confidencialidad, integridad o disponibilidad de la información y otros activos;

b) **Probabilidad**.- la probabilidad realista de que ocurra dicho fallo a la luz de las amenazas y vulnerabilidades existentes, así como de los controles implantados.

Los resultados de esta evaluación ayudarán a dirigir y determinar una adecuada acción gerencial y las prioridades para gestionar los riesgos de seguridad de la información, y la implantación de los controles adecuados para protegerse contra dichos riesgos. El proceso de evaluación de riesgos y selección de controles, pueden requerir que sea realizado varias veces para cubrir partes diferentes de la organización o sistemas de información individuales.

Es importante, efectuar revisiones periódicas de los riesgos de seguridad y de los controles implantados para:

- Tener en cuenta los cambios de los requisitos y las prioridades de negocio de la organización.
- Considerar nuevas amenazas y vulnerabilidades.
- Confirmar que las medidas de control siguen siendo eficaces y apropiadas.

1.2.6. SELECCIÓN DE OPCIONES PARA EL TRATAMIENTO DEL RIESGO

Cuando los riesgos han sido identificados y evaluados, la organización debería identificar y evaluar la acción más apropiada para tratar los riesgos, lo que se conoce como el Plan de Tratamiento de Riesgos (PTR), que es un documento o conjunto de ellos, de vital importancia para el SGSI. El objetivo fundamental es describir de forma bien clara las actualizaciones que se van a realizar para disminuir los riesgos a niveles aceptables, qué recursos van a asignarse para la realización de cada una de estas actualizaciones, las responsabilidades asociadas y las posibles prioridades en la ejecución de las actualizaciones.

Para el tratamiento del riesgo existen cuatro estrategias.

1.2.6.1. Reducción del riesgo

Para los riesgos donde la opción de reducirlos ha sido escogida, se deben implementar los apropiados controles para disminuirlos a los niveles de aceptación previamente identificados por la empresa.

Al identificar los controles a ser implantados es importante considerar los requerimientos de seguridad relacionados con el riesgo, así como las vulnerabilidades y las amenazas previamente identificadas.

Los controles pueden reducir los riesgos valorados en varias maneras:

- Reduciendo la posibilidad de que la vulnerabilidad sea explotada por las amenazas.
- Reduciendo la posibilidad de impacto si el riesgo ocurre detectando eventos no deseados, reaccionando o recuperándose de ellos.

La elección de cualquiera de estas maneras para controlar los riesgos dependerá de una serie de factores, tales como: requerimientos comerciales de la organización, el ambiente, y las circunstancias en que la firma requiere operar.
Un aspecto muy importante que se debe tomar en cuenta si la empresa opta por este método para el tratamiento del riesgo, es el económico.

1.2.6.2. Aceptación del riesgo

Es probable que a la empresa se le presente situaciones donde no se pueden encontrar controles ni tampoco es viable diseñarlos o el costo de implantar el control es mayor que las consecuencias del riesgo. En estas circunstancias una decisión razonable pudiera ser la de inclinarse por la aceptación del riesgo, y vivir con las consecuencias si el riesgo ocurriese.

En el caso en que la empresa no pueda manejar el riesgo debido al costo de la implantación de los controles y las consecuencias son devastadoras para la empresa, se deben visualizar las opciones de “transferencia del riesgo” o la de “evitar el riesgo”.

1.2.6.3. Transferencia del riesgo

La transferencia del riesgo, es una opción para la empresa, cuando es muy difícil, tanto técnica como económicamente para la organización llevar al riesgo a un nivel aceptable. En estas circunstancias podría ser económicamente factible, transferir el riesgo a una aseguradora.

Hay que tomar en cuenta, que con las empresas aseguradoras, siempre existe un elemento de riesgo residual. Siempre existen condiciones con las aseguradoras de exclusiones, las cuales se aplicarán dependiendo del tipo de

ocurrencia, bajo la cual no se provee una indemnización. La transferencia del riesgo por lo tanto, debe ser muy bien analizada para así poder identificar con precisión, cuánto del riesgo actual está siendo transferido.
Otra posibilidad es la de utilizar a terceras partes para el manejo de activos o procesos considerados críticos. En la medida en que la empresa tercializadora esté preparada para asumir dicha responsabilidad.
Lo que debe estar claro, es que al tercerizar servicios, el riesgo residual no se delega, es responsabilidad de la empresa.

1.2.6.4. Evitar el riesgo

La opción de evitar el riesgo, describe cualquier acción donde las actividades del negocio, o las maneras de conducir la gestión comercial del negocio, se modifican, para así poder evitar la ocurrencia del riesgo.

Las maneras habituales para implementar esta opción son:

- Dejar de conducir ciertas actividades.
- Desplazar activos de información de un área riesgosa a otra.
- Decidir no procesar cierto tipo de información si no se consigue la protección adecuada.

La decisión por la opción de “evitar el riesgo” debe ser balanceada contra las necesidades financieras y comerciales de la empresa.

1.2.6.5. Selección de controles para reducir los riesgos a un nivel aceptable

Para reducir el riesgo evaluado dentro del alcance del SGSI considerado, controles de seguridad apropiados y justificados deben ser identificados y seleccionados.

La selección de controles debe ser sustentada por los resultados de la evaluación del riesgo. Las vulnerabilidades con las amenazas asociadas indican donde la protección pudiera ser requerida y qué forma debe tener.

Cuando se seleccionan controles para la implementación, un número de factores deben ser considerados:

- Uso de controles
- Transparencia del usuario
- Ayuda otorgada a los usuarios para desempeñar su función
- Relativa fuerza de controles
- Tipos de funciones desempeñadas

1.2.7. RIESGO RESIDUAL

Una vez que las decisiones del tratamiento del riesgo han sido implementadas, siempre habrá un riesgo residual. Es necesario calcular cuánto las decisiones del tratamiento del riesgo ayudan a reducir el riesgo, y cuánto queda de riesgo residual. El riesgo residual es definido como “aquel riesgo que queda en la empresa después de haber implementado el plan de tratamiento del riesgo”.

El riesgo residual es muchas veces difícil de calcular, pero por lo menos un estimado debe ser determinado.

En el caso de que el riesgo residual no fuera aceptable, una decisión gerencial debe ser tomada para resolver la situación. Una opción es la de identificar diferentes opciones de tratamiento del riesgo, incrementar los controles, o establecer arreglos con aseguradoras, para finalmente poder reducir el riesgo a un nivel aceptable. Es importante estar claros, que una buena práctica es la de no tolerar riesgos inaceptables, pero en algunas circunstancias, podría ser necesario tener que aceptarlos. Los riesgos residuales que son aceptados, deben ser documentados y aprobados por la gerencia. Si la opción de tratamiento del riesgo no está demostrando eficacia en alcanzar los niveles deseados de riesgo, deben tomarse las acciones correctivas de lugar.

1.3. CONTROLES DE UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

ISO 27001 contiene un anexo A, que considera los controles de la norma ISO 17799 para su posible aplicación en SGSI que implante cada organización.

La descripción de cada uno de los controles y dominios se verá en el capítulo II del presente proyecto de titulación.

1.4. ESTRUCTURA DEL SISTEMA DE GESTIÓN

1.4.1. INTRODUCCIÓN

Un Sistema de Gestión es una herramienta de la que dispone la Gerencia para dirigir y controlar un determinado ámbito.

Las empresas tienen la posibilidad de implantar un número variable de estos Sistemas de Gestión para mejorar la organización y beneficios sin imponer una carga a la organización.

1.4.2. OBJETIVO

Los Sistemas de Gestión se aplican en el marco de todas las actividades que se ejecutan en la organización y son válidos solo si cada uno de ellos interactúa con los demás armónicamente.

La estructura de los Sistemas de Gestión debe ser tal que sea factible realizar una coordinación y un control ordenado y permanente sobre la totalidad de las actividades que se realizan. Deben estructurarse y adaptarse al tipo y características de cada organización, tomando en consideración particularmente los elementos que sean apropiados para su estructuración; para lo cual se debe definir:

- Estructura Organizativa.
- Resultados deseables que se pretenden lograr.
- Procesos que se llevan a cabo para cumplir con la finalidad.
- Procedimientos mediante los cuales se ejecuta las actividades y tareas.
- Recursos con los cuales se dispone.

El objetivo de los estándares de Gestión de ISO es llegar a un único Sistema de Gestión que contemple todos los aspectos necesarios para la organización, basándose en el ciclo PDCA y el proceso de mejora continua.

1.4.3. OPERATIVIDAD DE LOS SISTEMAS DE GESTIÓN

Los Sistemas de Gestión adaptados al tipo particular de organización, debe operar de tal manera que se de la confianza apropiada; es decir que:

- Sean bien comprendidos por la totalidad de los protagonistas
- Operan en forma eficaz
- Los resultados satisfacen las expectativas de las partes interesadas
- Se enfatiza las acciones preventivas ante cualquier clase de problemas

1.5.NORMAS ISO 27000

1.5.1. HISTORIA[3]

Durante más de un siglo, el Instituto Británico de Normas Técnicas (BSI) y la Organización Internacional de Normas Técnicas (ISO) han brindado parámetros globales a [3]las normas técnicas de operación, fabricación y desempeño. Solo faltaba que BSI e ISO propusieran una norma técnica para la seguridad de la información.

[3] Tomado de http://www.iso27000.es/sgsi.html

En 1995, el BSI publicó la primera norma técnica de seguridad; la BS 7799, la cual fue redactada con el fin de abarcar los asuntos de seguridad relacionados con el e – commerce. La Norma se consideraba inflexible y no tuvo gran acogida. No se presentó la norma técnica en un momento oportuno y los problemas de seguridad no despertaron mucho interés en ese entonces.

En Mayo de 1999, el BSI intentó de nuevo publicar su segunda versión de la Norma BS 7799, la que fue una revisión más amplia de la primera publicación.
En Diciembre del 2000, La ISO adoptó y publicó la primera parte de su norma BS 7799 bajo el nombre de ISO 17799.

En Septiembre del 2002 se publicó BS 7799 – 2; en esta revisión se adoptó el "Modelo de Proceso" con el fin de alinearla con ISO 9001 e ISO 14001.
El 15 de Octubre del 2005 se aprueba la Norma ISO 27001:2005 y en 2006 existen más de 2030 compañías certificadas a nivel mundial.

1.5.2. DEFINICIÓN DE LAS NORMAS ISO 27000

La serie ISO 27000 es una Familia de Estándares internacionales para Sistemas de Gestión de Seguridad de la Información (SGSI), que propone requerimientos de sistemas de gestión de seguridad de la información, gestión de riesgo, métricas y medidas, guías de implantación, vocabulario y mejora continua.

• ***ISO 27000***

En fase de desarrollo. 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.

• ***ISO 27001***

Es la norma principal de requerimientos 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 serán certificados por auditores externos los SGSI de las organizaciones. Fue publicada el 15 de Octubre de 2005 y sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última. En su Anexo A, lista en forma de resumen los objetivos de control y controles que desarrolla la ISO17799:2005 (futura ISO27002), para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en esta última, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.

• ***ISO 27002 (ISO 17799)***

En fase de desarrollo; probable publicación en 2007. 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. Será la sustituta de la ISO17799:2005, que es la que actualmente está en vigor, y que contiene 39 objetivos de control y 133 controles, agrupados en 11 cláusulas. Como se ha mencionado en su apartado correspondiente, la norma ISO27001 contiene un anexo que resume los controles de ISO17799:2005.

• ***ISO 27003***

En fase de desarrollo; probable publicación en Octubre de 2008. Contendrá una guía de implementación de SGSI e información acerca del uso del modelo PDCA 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***

Especificará las métricas y las técnicas de medida aplicables para determinar la eficiencia y efectividad de la implantación 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.

• ***ISO 27005***

Probable publicación en 2007 ó 2008. Consistirá en una guía para la gestión del riesgo de la seguridad de la información y servirá, por tanto, de apoyo a la ISO27001 y a la implantación de un SGSI. Se basará en la BS7799-3 (publicada en Marzo de 2006) y, probablemente, en ISO 13335.

• ***ISO 27006***

Especificará el proceso de acreditación de entidades de certificación y el registro de SGSI.

1.5.3. BENEFICIOS DE LAS NORMAS ISO 27000

Entre los beneficios que se obtienen por la implementación del conjunto de normas ISO 27000 en una organización, se tiene:

- Establecimiento de una metodología de gestión de la seguridad clara y estructurada.
- Reducción del riesgo de pérdida, robo o corrupción de información.
- Los clientes tienen acceso a la información a través medidas de seguridad.
- Los riesgos y sus controles son continuamente revisados.
- Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
- Las auditorias externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.
- El sistema se integra con otros sistemas de gestión (ISO9001, ISO14001, OHSAS).
- Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.
- Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.
- Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.

- Proporciona confianza y reglas claras a las personas de la organización.
- Reduce costes y mejora los procesos y servicio.
- Aumenta la motivación y satisfacción del personal.
- Seguridad garantizada en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías.

1.5.4. NORMATIVAS DE REFERENCIA

Para la aplicación de la norma ISO 27001:2005, es indispensable tener en cuenta la última versión de:

"ISO/IEC 17799:2005, Information technology — Security techniques — Code of practice for information security management"

1.6.TÉRMINOS Y DEFINICIONES [3]

La siguiente terminología aplica a esta norma:

Activo (Asset).- en relación con la seguridad de información, se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización.

Aceptación de Riesgos.- Decisión de aceptar un riesgo

Análisis de Riesgo.- Uso sistemático de la información para identificar fuentes y estimar el riesgo.

Administración del Riesgo.- Actividades coordinadas para dirigir y controlar las medidas necesarias para la observación del riesgo dentro de la organización.

Confidencialidad (Confidenciality).-Acceso a la información por parte únicamente de quienes estén autorizados.

Disponibilidad (Avalaibility).- Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran.

Declaración de Aplicabilidad.- documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos, además de la justificación tanto de su selección como de la exclusión de controles incluidos en el ANEXO A.

Evaluación de riesgos.- Proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

Incidente de Seguridad.- Evento único o serie de eventos de seguridad de la información inesperada o no deseada que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de información.

Integridad.- Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Riesgo Residual.- el riesgo que permanece tras el tratamiento de riesgos.

Seguridad de la Información.- Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.

Eventos de Seguridad de la Información.- suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de

seguridad de la información o fallo de las savalguardias, o una situación anterior o desconocida que podría ser relevante para la seguridad.

Tratamiento de Riesgo.- Proceso de selección e implementación de medidas para modificar el riesgo.

Valoración de Riesgos.- Proceso Completo de análisis y evaluación de riesgos.

1.7. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

1.7.1. INTRODUCCION

1.7.1.1. Antecedentes

Esta escasa seguridad que hubo en los orígenes del boom de Internet hizo saltar la alarma, de tal forma que la seguridad de la información empezó a tomarse en serio, tanto en el ámbito empresarial, como comercial y por supuesto jurídico-legal.

Pero esta seguridad no afecta sólo al tráfico que circula por la red. Debe entenderse la seguridad como algo integral. Debe abordar problemas desde tráfico en red, hasta seguridad física de servidores y bases de datos de información.

Los gerentes de seguridad de la información han esperado mucho tiempo a que alguien tomara el liderazgo para producir un conjunto de normas de seguridad de la información que estuviera sujeto a auditoria y fuera reconocido globalmente. Se cree que un código de normas de la seguridad apoyaría los esfuerzos de los gerentes de tecnología de la información en el sentido que facilitaría la toma de decisión de compra, incrementaría la cooperación entre

los múltiples departamentos por ser la seguridad el interés común y ayudaría a consolidar la seguridad como prioridad empresarial.

Desde su publicación por parte de la Organización Internacional de Normas en diciembre de 2000, ISO 17799 surge como la norma técnica de seguridad de la información reconocida a nivel mundial. ISO 17799 se define como "un completo conjunto de controles que incluye las prácticas exitosas de seguridad de la información".

1.7.1.2. Norma ISO 27001

El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto sobre el que se construye ISO 27001.

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización. Este proceso es el que constituye un SGSI, que podría considerarse, por analogía con una norma tan conocida como la ISO 9001, como el sistema de calidad para la seguridad de la información.

El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información son conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

1.7.1.3. Alcance de la Norma ISO 27001

ISO/IEC 27001:2005 es una norma que establece los requisitos de los sistemas de gestión de la seguridad de la información. Esta norma esta diseñada para asegurar la selección de los controles de seguridad adecuados y

proporcionados para proteger la información y dar la confianza a partes interesadas incluyendo a los clientes de una empresa.

Es conveniente para varios tipos diferentes de uso empresarial, incluyendo lo siguiente:

- Formulación de exigencias y objetivos para la seguridad
- Asegurar la gestión más rentable de los riesgos
- Asegurar el cumplimiento legal
- Desarrollar un proceso para la puesta en práctica y la gestión de controles para asegurar el conocimiento de los objetivos de seguridad específicos de una empresa.
- Identificación y clarificación de los procesos existentes en la gestión de la seguridad de la información.
- Puede ser usado por la dirección para determinar el estado de las actividades de la gestión de la seguridad de la información.
- Como herramienta de auditores internos y externos para determinar el grado de cumplimiento con la política, directivas y normas adoptadas por una empresa.
- Para proporcionar información relevante sobre la política de la seguridad de la información, directivas, normas y procedimientos dentro del mercado.
- Para proporcionar información relevante sobre seguridad de la información a clientes.

1.7.1.4. Objetivo de la Norma ISO 27001

Entre los objetivos que se pretenden cumplir con la Norma ISO 27001, tenemos:

- Aumentar el valor de un servicio "seguro": Esta filosofía supone implementar un SGSI para potenciar un servicio que ya incorpora

funciones de seguridad, en el que un SGSI va a aportar beneficios directos.

- Potenciar un servicio final: Esta opción supone la implantación de un SGSI ligado a los servicios y/o procesos de negocio. De esta forma, se da un valor añadido a los mismos, bañándolos de una capa de seguridad adicional.

- Reforzar los servicios y procesos internos: Esta filosofía pretende implantar el SGSI para fortalecer determinados servicios y procesos internos, en los que una mejora en la seguridad pueda suponer una ventaja para la organización. En general, se suele traducir en la implementación del SGSI en el área de IT, por ser uno de los principales responsables del tratamiento y conservación de la información de la compañía, o en áreas en las que se maneja información de especial relevancia, como podrían ser las áreas de I+D+i (prototipos, diseños, etc), recursos humanos (datos de caracter personal) o financiero (datos económicos).

- Potenciar la gestión interna: Por último, otra de las filosofías que a veces se utiliza para decidir el alcance es identificar aquellas partes de la organización en las que la implantación del SGSI, como sistema de gestión, sirva para potenciar y estructurar la gestión interna. Es quizás una de las filosofías más discutibles, ya que existen multitud de sistemas de gestión centrados en distintos aspectos y quizás el de la seguridad pueda no ser el más indicado en todos los casos, pero en determinadas situaciones puede ser una opción.

1.7.2. REQUISITOS DE LA DOCUMENTACION DEL SGSI [3]

Un Sistema de Gestión de la Seguridad de la Información basado en ISO 27001 está formado por una serie de documentos que pueden clasificarse en una pirámide de cuatro niveles.

Fig 1.3 Pirámide de cuatro niveles para la clasificación de documentos

La documentación de un SGSI deberá incluir:

1.7.2.1. Documentos de Nivel 1

Forman el manual de seguridad. Son los siguientes:

- Alcance del SGSI: ámbito de la organización que queda sometido al SGSI. Se debe incluir una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas, prestando especial atención en aquellos casos en los que el ámbito de influencia del SGSI considere una parte menor de la organización como delegaciones, divisiones, áreas, procesos o tareas concretas.
- Política y objetivos de seguridad: documento de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información.

- Metodología de evaluación de riesgos: descripción de cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado.
- Informe de evaluación de riesgos: estudio resultante de aplicar la metodología de evaluación anteriormente mencionada.
- Plan de tratamiento del riesgo: documento que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información e implantar los controles necesarios para proteger la misma.
- Declaración de aplicabilidad (SOA -Statement of Applicability-, en sus siglas inglesas): documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.
- Procedimientos relativos al nivel 1: procedimientos que regulan cómo se realizan, gestionan y mantienen los documentos enumerados en el nivel 1.

1.7.2.2. Documentos de Nivel 2

Procedimientos: documentos que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información y describen cómo medir la efectividad de los controles.

1.7.2.3. Documentos de Nivel 3

Instrucciones, checklists y formularios: documentos que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información.

1.7.2.4. Documentos de Nivel 4.

Registros: documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI; están asociados a documentos de los

otros tres niveles como output que demuestra que se ha cumplido lo indicado en los mismos.

1.7.3. CONTROL DE DOCUMENTOS

Todos los documentos requeridos por el SGSI serán protegidos y controlados. Un procedimiento documentado deberá establecer las acciones de administración necesarias para:

- Aprobar documentos y prioridades o clasificación de empleo.
- Revisiones, actualizaciones y reaprobaciones de documentos.
- Asegurar que los cambios y las revisiones de documentos sean identificados.
- Asegurar que las últimas versiones de los documentos aplicables estén disponibles y listas para ser usadas.
- Asegurar que los documentos permanezcan legibles y fácilmente identificables.
- Asegurar que los documentos estén disponibles para quien los necesite y sean transferidos, guardados y finalmente dispuestos acorde a los procedimientos aplicables a su clasificación.
- Asegurar que los documentos de origen externo sean identificados.
- Asegurar el control de la distribución de documentos.
- Prevenir el empleo no deseado de documentos obsoletos y aplicar una clara identificación para poder acceder a ellos y que queden almacenados para cualquier propósito.

1.7.4. RESPONSABILIDADES DE ADMINISTRACIÓN

a) **La administración proveerá evidencias de sus compromisos para el establecimiento, implementación, operación, monitorización, mantenimiento y mejora del ISMS a través de:**

- Establecimiento de la política del SGSI.
- Asegurar el establecimiento de los objetivos y planes del SGSI.

- Establecer roles y responsabilidades para la seguridad de la información.
- Comunicar y concienciar a la organización sobre la importancia y apoyo necesario a los objetivos propuestos por la política de seguridad, sus responsabilidades legales y la necesidad de una continua mejora en este aspecto.
- Proveer suficientes recursos para establecer, operar, implementar, monitorizar, revisar, mantener y mejorar el ISMS.
- Decidir los criterios de aceptación de riesgos y los niveles del mismo.
- Asegurar que las auditorias internas del ISMS, sean conducidas y a su vez conduzcan a la administración para la revisión del ISMS.

b) **Formación, preparación y competencia:**

La organización asegurará que todo el personal a quien sean asignadas responsabilidades definidas en el ISMS sea competente y esté en capacidad de ejecutar las tareas requeridas, para ello deberá proveer las herramientas y capacitación necesaria (Documento: Planificación, guías y programas de formación y preparación).

1.7.5. IMPLEMENTACION DE UN SGSI

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA; tradicional en los sistemas de gestión de la calidad.

A continuación se describen los pasos a seguir para la implementación del SGSI:

1.7.5.1. Plan (Establecer el SGSI)

- Definir el alcance del SGSI en términos del negocio.
- Definir una política de seguridad

- Definir una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos del negocio que especifique los niveles de riesgo aceptables y unos criterios de aceptación de los riesgos.
- Identificar los riesgos
- Analizar y evaluar los riesgos
- Identificar y evaluar las distintas opciones de tratamiento de los riesgos
- Seleccionar los objetivos de control y los controles del Anexo A de la norma ISO 27001 para el tratamiento del riesgo y que cumplan con los requerimientos identificados en el proceso de evaluación y tratamiento del riesgo
- Definir una declaración de aplicabilidad

1.7.5.2. Do (Implementar y Utilizar el SGSI)

- Definir un plan de tratamiento de riesgos
- Implantar el plan de tratamiento de riesgos
- Implementar los controles
- Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles seleccionados.
- Procurar programas de formación y concienciación en relación a la seguridad de la información dirigidos a todo el personal.
- Gestionar las operaciones del SGSI.
- Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información.
- Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.

1.7.5.3. Check (Monitorizar y revisar el SGSI)

La organización deberá:

- Ejecutar procedimientos de monitorización y revisión
- Revisar regularmente la efectividad del SGSI

- Medir la efectividad de los controles para verificar que se cumple con los requisitos de seguridad.
- Revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables
- Realizar periódicamente auditorias internas del SGSI en intervalos planificados.
- Revisar el SGSI por parte de la dirección
- Actualizar los planes de seguridad
- Registrar acciones y eventos

1.7.5.4. Act (Mantener y mejorar el SGSI)

La organización deberá regularmente:

- Implantar en el SGSI las mejoras identificadas.
- Realizar las acciones preventivas y correctivas adecuadas en relación a la cláusula 8 de la norma ISO 27001.
- Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.
- Asegurarse que las mejoras introducidas alcanzan los objetivos previstos.

II

DESCRIPCIÓN DE LOS 11 DOMINIOS DEL ESTÁNDARES ISO 27001

2.1.POLÍTICA DE SEGURIDAD

2.1.1. DOCUMENTO DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La gerencia debe aprobar el documento de política de seguridad de información y es deber de la gerencia publicar este documento a toda la organización. El documento de política deberá contener:

a) una definición de la seguridad de información y sus objetivos globales y el alcance y su importancia como un mecanismo que permite compartir información;
b) el objetivo de la gerencia como soporte de los objetivos y principios de la seguridad de la información;
c) una estructura para el establecimiento de los objetivos de control y controles, incluida la estructura de la valoración del riesgo y el manejo de riesgos;
d) una breve explicación de las políticas, principios, normas y requisitos de conformidad más importantes para la organización;
e) una definición de las responsabilidades generales y específicas en materia de la gestión de seguridad de información, incluida el reporte de las incidencias de seguridad;
f) las referencias a documentación que pueda sustentar la política, ejemplo: políticas y procedimientos mucho más detallados para sistemas de información específicos o las reglas que los usuarios deberían cumplir.

Revisión de la política de seguridad de la información

Se debe realizar la revisión de la política de seguridad de la información a intervalos regulares planificados, los resultados de la revisión deben reflejar los cambios que afecten a la valoración inicial de los riesgos en la organización.

2.2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

2.2.1. ORGANIZACIÓN INTERNA

Se debe establecer una estructura de la seguridad de la información, de tal manera que satisfaga todos los requerimientos, para lo cual es indispensable la participación de los representantes de las diferentes áreas dentro de la organización para cubrir las distintas necesidades.

Comité de gestión de seguridad de la información

La administración deberá realizar las siguientes funciones:

a) Identificar los objetivos de seguridad de información, encontrar los requerimientos de la organización e integrarlos en procesos relevantes;
b) formular, revisar y aprobar las políticas de seguridad de información;
c) revisar la efectividad de la implementación de las políticas de seguridad de la información;
d) proporcionar una clara dirección y apoyo para las iniciativas de seguridad;
e) proporcionar los recursos necesarios para la seguridad de información;
f) aprobar la asignación de roles específicos y responsabilidades para la seguridad de la información;
g) iniciar planes y programas para mantener el conocimiento de la seguridad de información;

h) asegurar que la implementación de controles de la seguridad de información esté coordinada en la organización.

Coordinación de la seguridad de la información

Las actividades que se debería realizar:

a) asegurar que las actividades de seguridad sean ejecutadas en conformidad con la política de seguridad;
b) cómo manejar los incumplimientos;
c) aprobar los métodos y procesos para manejar la seguridad de información;
d) identificar las nuevas amenazas de la información;
e) evaluar la coordinación de la implementación de los controles de la seguridad de información;
f) promover la educación de la seguridad de información;
g) evaluar la información recibida del monitoreo y de la revisión de los incidentes de seguridad, y recomendar acciones apropiadas en respuesta a los incidentes de seguridad identificados.

Asignación de las responsabilidades de la seguridad de información

Deben ser definidas claramente todas las responsabilidades de la seguridad de la información. Se deberá tomar en cuenta lo siguiente:

a) identificar claramente los activos y los procesos de seguridad asociados con cada sistema específico.
b) nombrar al responsable de cada activo o proceso de seguridad, y documentar los detalles de esta responsabilidad.
c) definir y documentar claramente los niveles de autorización.

Procesos de autorización para los recursos de tratamiento de la información

Se debe definir e implementar el proceso de autorización de recursos para el tratamiento de la información. La siguiente guía debería ser considerada:

a) los nuevos recursos deben tener la aprobación de la gerencia. Además se debe tener la aprobación del directivo responsable del mantenimiento del entorno de seguridad de la información.
b) donde sea necesario, se deberá comprobar que el hardware y el software son compatibles con los demás dispositivos del sistema.
c) el uso de recursos de tratamiento de la información personales (laptops, dispositivos portátiles) para la organización, puede introducir nuevas vulnerabilidades y por lo tanto se deben identificar e implementar controles.

Acuerdos de confidencialidad

Se debe identificar y revisar regularmente los requerimientos para la confidencialidad reflejando las necesidades de la organización para la protección de información. Los siguientes elementos deben ser considerados:

a) una definición de la información a ser protegida;
b) duración del acuerdo, incluyendo casos donde la confidencialidad podría necesitar ser mantenida indefinidamente;
c) acciones requeridas cuando un acuerdo se termina;
d) responsabilidades y acciones de signatarios para evitar el descubrimiento de información no autorizada;
e) propiedad de información, secretos del oficio y propiedad intelectual y cómo está relacionada para la protección de la confidencialidad de información;
f) el uso permitido de información confidencial, y derechos del signatario para usar la información;
g) el derecho para analizar y monitorear actividades que involucren información confidencial;
h) proceso para notificar y reportar una divulgación no autorizada o brechas de información confidenciales;
i) términos para que la información sea retornada o destruida a la suspensión del acuerdo;
j) acciones esperadas a ser tomadas en el caso de la brecha de este acuerdo;

Contacto con autoridades

Se debe tener contactos apropiados con autoridades, para informar en casos de incidentes de seguridad y cómo deberían estos incidentes ser reportados

La revisión independiente de seguridad de información

La revisión independiente de seguridad de información se deberá realizar a intervalos regulares planeados o cuando ocurren cambios significativos de los métodos utilizados por la organización. La revisión independiente debe asegurar que el manejo de la seguridad de la información sea continuo, adecuado y eficaz.

Tal revisión debe ser llevada por individuos independientes del área de revisión. Los individuos que llevan a cabo estas revisiones deben tener las habilidades especiales y experiencia. Los resultados de la revisión independiente deben ser registrados y reportados a la gerencia.

Si la revisión identifica que los métodos de la organización e implementación para el manejo de la seguridad de información es inadecuada o no conforme con la dirección de la seguridad de información declarada en el documento de política de seguridad de la información, se deberá considerar acciones correctivas.

2.2.2. PARTES EXTERNAS

El acceso de terceros a los recursos de tratamiento de información no debe comprometer la seguridad de la información.

Identificación de riesgos relacionados a las partes externas

Los riesgos de los recursos de tratamiento de la información y los activos de información de la organización que involucran partes externas deben ser identificados e implementar controles apropiados antes de conceder el acceso. Se debe tomar en cuenta los siguientes problemas:

a) que recursos de tratamiento de la información necesita ser accedida;
b) que tipo de acceso necesita la tercera parte, por ejemplo: acceso físico, acceso lógico.

c) el valor y sensibilidad de la información involucrada, y su criticidad para la operación del negocio;
d) los controles necesarios para proteger la información que no será accesible por terceros;
e) el personal de la parte externa involucrado en el manejo de la información de la organización;
f) cómo el personal autorizado que tiene acceso pueden ser identificados;
g) los diferentes medios y controles empleados por la parte externa cuando almacena, procesa, comunica, comparte e intercambia información;
h) el impacto de que la tercer parte no tenga acceso cuanto esta requiera o que esta reciba información errónea.
i) prácticas y procedimientos para tratar con incidentes de seguridad de información y potenciales daños, y los términos y condiciones para la continuidad del acceso de la parte externa en el caso de un incidente de seguridad de la información;
j) requerimientos legales y regulatorios y otras obligaciones contractuales que la tercera parte deberá tomar en cuenta.

2.3.ADMINISTRACIÓN DEL RECURSO

2.3.1. Responsabilidad para los recursos

Se debe asignar a los recursos de la organización, propietarios quienes serán los responsables de mantener una protección adecuada.

Inventario de activos

Los inventarios de los activos ayudan a garantizar que se obtenga una protección eficaz. La organización debe identificar los activos y su valor e importancia. Sobre esta base la organización puede proporcionar niveles de protección proporcionales a dicho valor e importancia. Debería establecerse y mantenerse el inventario de los activos importantes asociados con cada sistema de información.

Propiedad de los recursos

Todos los recursos de tratamiento de la información y los activos de información de la organización deben ser de propiedad de una parte designada. El dueño del recurso debe ser responsable de:

1. asegurar que recursos de tratamiento de la información y los activos de información sean apropiadamente clasificados;
2. definir y revisar periódicamente las restricciones de acceso y clasificación, tomando en cuenta políticas de control de acceso aplicables.

Uso aceptable de recursos

Se debe identificar, documentar e implementar las reglas para el uso aceptable de los recursos del tratamiento de la información y los activos de información. Se debe incluir:

a) reglas para el correo electrónico y uso de Internet;
b) guía para el uso de dispositivos móviles, especialmente para el uso fuera de la organización;

2.3.2. Clasificación de la información

Dar a cada recurso la protección adecuada de acuerdo a su clasificación, esta clasificación se dará en base a niveles de sensibilidad y criticidad.

Guías de clasificación

La información debe ser clasificada de acuerdo a su valor, requerimientos legales, sensibilidad, y criticidad de la organización. La clasificación que se da a la información es una forma para determinar cómo manejarla y protegerla.

La información suele dejar de tener importancia o criticidad tras cierto tiempo. Estos aspectos deberían considerarse, puesto que una sobre clasificación conllevaría un gasto adicional innecesario. La clasificación puede cambiar de acuerdo conciertas políticas predeterminadas.

Debería considerarse el número de categorías de clasificación y los beneficios obtenidos con su uso. Es conveniente cuidar la interpretación de los catálogos

de clasificación de otras organizaciones que pueden tener distintas definiciones de conceptos iguales o llamados de forma similar.

Etiquetado y tratamiento de la información

Un apropiado conjunto de procedimientos para el etiquetado y tratamiento de la información debe ser desarrollado e implementado de acuerdo al esquema de clasificación adoptado por la organización.

El marcado de información puede tener formato físico o electrónico de acuerdo a su necesidad. La salida precedente de los sistemas que traten información clasificada como sensible o crítica debería llevar una etiqueta de clasificación adecuada.

2.4.SEGURIDAD DE RECURSOS HUMANOS

2.4.1. SEGURIDAD EN LA DEFINICIÓN DEL TRABAJO Y LOS RECURSOS

Asegurar que cada persona dentro de la organización comprenda sus responsabilidades, ya que es un factor que influye en la preservación de la seguridad de la información.

Roles y responsabilidades

Se debe definir y documentar los roles y responsabilidades de empleados, contratistas y otras partes involucradas con la organización. Los roles de seguridad y responsabilidades deben incluir los requisitos para:

a) implementar y actuar de acuerdo con las políticas de seguridad de información;
b) proteger los activos de accesos no autorizados, divulgación, modificación, destrucción e interferencia;
c) ejecutar procesos particulares de seguridad o actividades;
d) garantizar que responsabilidades se asignen a los individuos para acciones tomadas;
e) reportar eventos de seguridad o eventos potenciales u otros riesgos para la organización.

Selección y política de personal

La selección del personal debe llevarse a cabo en base a las leyes, regulaciones, y ser correspondiente con los requerimientos de la organización. Se debería incluir controles como los siguientes:

a) la disponibilidad de referencias satisfactorias sobre actitudes, por ejemplo: una personal y otra de la organización;
b) la comprobación del currículum vital del candidato;
c) la confirmación de las certificaciones académicas y profesionales;
d) una comprobación independiente de identificación;
e) una comprobación más detallada, como chequear el record policial.

Términos y condiciones del empleo

Los términos y las condiciones de empleo deberían establecer la responsabilidad del empleado en materia de seguridad de la información. Los términos y condiciones del empleo deben reflejar la política de seguridad de la organización además para aclarar y declarar:

a) que todos los empleados, contratistas y usuarios de terceras partes quienes tengan acceso a información sensible deberían firmar un acuerdo de confidencialidad o no divulgación antes de concederle el acceso a los recursos de tratamiento de información;
b) responsabilidades y derechos del empleado, contratista y otro usuario;
c) responsabilidades para la clasificación de información y administración de los activos asociados con los sistemas de información y servicios manejados por los empleados, contratistas y usuarios de una tercera parte;
d) responsabilidades de los empleados, contratistas y una tercera parte para el manejo de la información recibida de otras compañías o partes externas;
e) responsabilidades de la organización para el manejo de la información personal;
f) responsabilidades que están extendidas fuera de las premisas de la organización y fuera de las horas de trabajo, ejemplo: en el caso de trabajar en casa;

g) acciones a ser tomadas si los empleados, contratistas y la tercera parte se descuidan de los requerimientos de la seguridad de la organización.

2.4.2. DURANTE EL EMPLEO

Asegurar que los empleados, contratistas y usuarios de una tercera parte estén conscientes de sus responsabilidades, de tal manera que sus roles sean ejecutados adecuadamente. Además debe conocer las políticas establecidas y aplicarlas.

Conocimiento, educación y entrenamiento de seguridad de la información

Deben recibir el conocimiento adecuado de la seguridad de información y las actualizaciones de las políticas de la organización todos los empleados, contratistas y terceras partes. El entrenamiento de los conocimientos de seguridad debe comenzar con un proceso de inducción formal para introducir las políticas de seguridad de la información y expectativas antes del acceso a la información o a los servicios.

El entrenamiento continuo debe darse de acuerdo a los requisitos de seguridad, marco legal controles del negocio, así como la preparación para el uso correcto de los recursos de tratamiento de la información.

Proceso disciplinario

Se debe establecer un proceso disciplinario formal para minimizar los riesgos de la seguridad de la información.

Un proceso disciplinario formal debe asegurar un tratamiento para empleados que pueden comprometer la seguridad. El proceso disciplinario formal debe proveer una respuesta que toma en cuenta factores como la naturaleza o gravedad de la brecha y su impacto en el negocio y otros factores requeridos.

2.4.3. TERMINACIÓN O CAMBIO DE EMPLEO

Manejar de manera ordenada la terminación o cambio de empleo, en donde está incluido el retiro de los derechos de acceso, retorno de equipos y finalizar con las responsabilidades respectivas.

Responsabilidades de la terminación

La comunicación de terminación de responsabilidades debe incluir requerimientos de seguridad prolongado y responsabilidades legales, donde sea apropiado, responsabilidades contenidas dentro de acuerdos de confidencialidad, y los términos y condiciones del empleo continuado para un periodo definido antes del fin del empleo del empleado, contratista o usuario de la tercer parte.

Retorno de los recursos

El proceso de terminación debe ser formalizado para incluir el retorno de todo el software emitido, documentos corporativos y equipo.

En el caso donde empleados, contratistas y usuario de la tercera parte compra el equipo de la organización o usa su propio equipo personal, procedimientos debe ser seguido para asegurar que toda la información relevante es transferida a la organización y borrada del equipo.

En el caso donde un empleado, contratista y usuario de la tercera parte tenga conocimiento que es importante para la continuidad de las operaciones, esa información debe ser documentada y transferida a la organización.

Remover el derecho de acceso

Cambios de un empleo debe ser reflejado en remover todos los derechos de acceso que no fueran aprobados por el nuevo empleado. Se debe considerar factores como:

a) si la terminación o cambio es inicializada por el empleado, contratista o usuario de la tercera parte, o por la administración y la razón de su terminación;
b) las responsabilidades actuales del empleado, contratista u otro usuario;
c) el valor de los activos actualmente accesibles.

2.5.SEGURIDAD FÍSICA Y AMBIENTAL

2.5.1. LAS ÁREAS SEGURAS

Los recursos importantes para el tratamiento de la información deben ser ubicados en áreas seguras de tal manera que se provenga el acceso no autorizado.

El perímetro de seguridad físico

Los perímetros de seguridad debe ser usadas para proteger áreas que contienen recursos de tratamiento de información. Se debe considerar los siguientes puntos:

a) el perímetro de seguridad deben ser definidos claramente;
b) el perímetro de un edificio o un lugar que contenga recursos de tratamiento de información debería tener solidez física;
c) se debería instalar un área de recepción manual u otros medios de control del acceso físico al edificio o lugar. Dicho acceso se debería restringir solo al personal autorizado;
d) las barreras físicas se deberían extender, si es necesario, desde el suelo al techo para evitar entradas no autorizadas o contaminación del entorno;
e) todas las puertas para incendios del perímetro de seguridad deberían tener alarma y cierre automático.
f) sistemas de detección de intrusos apropiados debe ser instalado para cubrir todas las puertas externas y ventanas accesibles; áreas desocupadas deben ser alarmadas en todo momento;
g) recursos de tratamiento de información manejados por la organización debe ser físicamente separada de los manejos de terceras partes.

La entrada física controlada

Se debe asegurar que solo personal autorizado sea permitido el acceso. La siguiente guía debe ser considerada:

a) las visitas a las áreas seguras se deberían supervisar u ordenar y registrarse su fecha y momento de entrada y salida;
b) solo el personal autorizado debe tener acceso a información sensible y a los recursos de su tratamiento. Se deberían usar controles de autenticación;
c) se debería exigir a todo el personal que lleve puesta alguna forma de identificación visible y se pedirá que se identifique a cualquiera que no lleve identificación;
d) personal de servicio que apoya la tercera parte debe ser concedido el acceso restringido a áreas seguras o recursos de tratamiento de información sensible cuando se requiera, este acceso debe ser autorizado y supervisado;
e) se debería revisar y actualizar regularmente los derechos de acceso a las áreas de seguridad, y revocar cuando sea necesario.

Seguridad de oficinas, despachos y recursos

Se debe diseñar y aplicar la seguridad física de oficinas, despachos y recursos. La siguiente guía debe ser considerada:

a) los recursos críticos deben estar en áreas que estén aisladas del acceso público;
b) los edificios deberían ser discretos y dar mínimas indicaciones de su propósito, sin signos obvios, fuera o dentro del edificio, que identifiquen la presencia de actividades de tratamiento de información;
c) el público no debería acceder automáticamente a los ambientes o directorios de información personal de la organización que identifiquen lugares con recursos de tratamiento de información sensible.

Protección contra amenazas externas y ambientales

Se debe diseñar y aplicar la protección física contra fuego, inundaciones, terremotos, explosiones, y otras formas naturales o desastres hechas por el hombre. La siguiente guía debe ser considerada para evitar cualquier daño:

a) Los materiales peligrosos y combustibles se deberían almacenar en algún lugar distante de las áreas seguras.

b) El equipo y los medios de respaldo deberían estar a una distancia de seguridad conveniente para evitar que se dañen por un desastre en el área principal.
c) Apropiados equipos contra incendios deben ser proporcionados y colocados en lugares adecuados.

Trabajando en áreas seguras

Se debe diseñar y aplicar protecciones físicas y guías de trabajo en áreas seguras. La siguiente guía debe ser considerada:

a) el personal debe estar al tanto sólo de las actividades del área que necesita conocer;
b) se debería evitar el trabajo no supervisado en áreas seguras tanto por motivos de salud como para evitar oportunidades de actividades maliciosas;
c) áreas seguras desocupadas deben ser físicamente bloqueadas y periódicamente chequeadas;
d) no se debería permitir la presencia de equipos de fotografía, vídeo, audio u otras formas de registro salvo autorización especial.

2.5.2. Seguridad de los equipos

Garantizar la continuidad del negocio mediante la protección adecuada de los activos de la organización.

Instalación y protección de equipos

El equipo debe ser protegido para reducir el riesgo de amenazas del entorno, así como las oportunidades de acceso no autorizado. Se debería considerar los siguientes pasos:

a) los equipos se deberían situar donde se minimicen los accesos innecesarios a las áreas de trabajo;
b) los equipos de tratamiento y almacenamiento de información que manejen datos sensibles se deberían instalar donde se reduzca el riesgo de que otros vean los procesos durante su uso;
c) los elementos que requieran especial protección se deberían aislar para reducir el nivel general de protección requerido;

d) para minimizar los riesgos de posibles amenazas como las siguientes: incendio, explosivos, humo, agua, polvo, vibraciones, agentes químicos, interferencias en el suministro eléctrico, radiaciones electromagnéticas;
e) la organización debería incluir en su política cuestiones sobre fumar, beber y comer cerca de los equipos de tratamiento de información;
f) se deberían vigilar las condiciones ambientales que puedan afectar negativamente al funcionamiento de los equipos de tratamiento de información;
g) la protección de rayos debería se aplicado en todos los edificios y protección de rayos deben ser encajados en fuentes de entrada y líneas de comunicación;
h) el uso de métodos de protección especial, como el revestimiento del teclado debe ser considerado para el equipamiento en ambientes industriales;
i) el equipo de tratamiento de información sensible debe ser protegido para minimizar el riesgo de fuga de información.

Utilidades de apoyo

Las utilidades de apoyo como electricidad, suministro de agua, alcantarillado, calefactor/ventilador, y aire acondicionado deben ser adecuadas para los sistemas que ellos están soportando. Las utilidades de apoyo deben ser regularmente inspeccionadas y probarlo para asegurar su funcionamiento apropiado y para reducir algún riesgo.

Se recomienda instalar un Sistema de Alimentación Ininterrumpida (U.P.S.) para asegurar el funcionamiento continuo de los equipos que soporten operaciones críticas del negocio.

Se debería instalar interruptores de emergencia cerca de las puertas de emergencia de las salas de equipos para facilitar una desconexión rápida en caso de emergencia. Por si falla la energía se debería disponer de alumbrado de emergencia. Se deberían instalar en todos los edificios, así como en todas las líneas exteriores de comunicaciones, sistemas y filtros de protección de rayos.

El suministro de agua debe ser estable y adecuado para proporcionar aire acondicionado, equipo de humidificación y sistemas de supresión de fuego. Un sistema de alarma para detectar el mal funcionamiento en las utilidades de apoyo deben ser evaluadas e instaladas si se requiere.

Deben conectarse los equipos de las telecomunicaciones al proveedor de servicios por lo menos dos rutas diversas para prevenir que el fracaso en una conexión quite los servicios de la voz.

Seguridad del cableado

Se debería proteger contra intercepciones o daños el cableado de energía y telecomunicaciones que transporten datos o soporten servicios de información. Se debe considerar:

a) las líneas de energía y telecomunicaciones en las zonas de tratamiento de información, se deberían enterrar, cuando sea posible, o adoptarse medidas alternativas de protección;
b) la red cableada se debería proteger contra intercepciones no autorizadas o daños;
c) se deberían separar los cables de energía de los de comunicaciones para evitar interferencias;
d) se debe usar clara identificación de cables y señales de equipos para minimizar los errores de manejo, como parchar accidentalmente los cables de red mala;
e) una documentación de lista de parches debe ser usada para reducir la posibilidad de error;
f) se deberían considerar medidas adicionales para sistemas sensibles o críticos.

Mantenimiento de equipos

El equipo debe ser correctamente mantenido para asegurar su disponibilidad e integridad. Se debería considerar las siguientes indicaciones:

a) los equipos se deberían mantener de acuerdo a las recomendaciones de intervalos y especificaciones de servicio del suministrador;

b) sólo el personal de mantenimiento debidamente autorizado debería realizar la reparación y servicio de los equipos;
c) se deberían registrar documentalmente todas las fallas, reales o sospechados, así como todo el mantenimiento preventivo o correctivo;
d) se deberían adoptar las medidas adecuadas cuando se envíen los equipos fuera de las instalaciones, para su mantenimiento;
e) se deberían cumplir todos los requisitos impuestos por las políticas de seguridad.

Seguridad de los equipos fuera de los locales de la organización

La seguridad debe ser aplicada a los equipos de acuerdo a los diferentes riegos de trabajo de afuera de los locales de la organización. Para la protección de los equipos fuera de la organización se debe considerar:

a) los equipos y medios que contengan datos con información y sean sacados de su entorno habitual no se deberían dejar desatendidos en sitios públicos;
b) se deberían observar siempre las instrucciones del fabricante para proteger los equipos, por ejemplo, contra exposiciones a campos electromagnéticos intensos;
c) los controles para el trabajo en el domicilio se deberían determinar mediante una evaluación de los riesgos y aplicarse los controles convenientes según sea apropiado, por ejemplo, en controles de acceso a los computadores, una política de puesto de trabajo despejado y cierre de las zonas de archivo;
d) se deberían cubrir la inseguridad de los equipos fuera de su lugar de trabajo.

Seguridad en el reuso o eliminación de equipos

Todos los elementos del equipo que contengan dispositivos de almacenamiento de datos deberían comprobarse antes de su reuso o eliminación para asegurar que todo dato sensible y software bajo licencia se ha borrado o sobrescrito.

Los dispositivos que contienen información sensible deben ser físicamente destruidos o la información debe ser destruida, borrada o sobrescrita usando técnicas para asegurar que la información original no sea recuperable.

Remover la propiedad

Equipo, información o software no debe estar fuera de lugar sin la previa autorización. Se debe considerar:

a) equipo, información o software no debe estar fuera de lugar sin la previa autorización;
b) empleados, contratistas y usuarios de la tercer parte que tienen autorización para permitir remover fuera de lugar a los recursos deben ser claramente identificados;
c) deben ponerse límites de tiempo para el levantamiento de equipo y los ingresos, chequeando su cumplimiento;
d) donde sea necesario y apropiado, equipo debe ser registrado cuando es trasladado fuera de la organización y registrar cuando este es retornado.

2.6. GESTIÓN DE COMUNICACIONES Y OPERACIONES

2.6.1. PROCEDIMIENTOS Y RESPONSABILIDADES DE OPERACIÓN

Establecer responsabilidades y procedimientos para la gestión y operación de todos los recursos de tratamiento de información, de tal manera que se consiga reducir el riesgo de un mal uso del sistema deliberado o por negligencia.

Documentación de procedimientos operativos

Se deberían documentar los procedimientos de operación y hacerlo disponible para todos los usuarios que necesitan de ellos. Los procedimientos de operación deberían especificar las instrucciones necesarias para la ejecución detallada de cada tarea, incluyendo:

a) el proceso y utilización correcto de la información;
b) respaldo;

c) los requisitos de planificación, incluyendo las interdependencias con otros sistemas, con los tiempos de comienzo más temprano y final más tardío posibles de cada tarea;
d) las instrucciones para manejar errores u otras condiciones excepcionales que puedan ocurrir durante la tarea de ejecución, incluyendo restricciones en el uso de servicios del sistema;
e) los contactos de apoyo en caso de dificultades inesperadas operacionales o técnicas;
f) las instrucciones especiales de utilización de resultados, como el uso de papel especial o la gestión de resultados confidenciales, incluyendo procedimientos de destrucción segura de resultados producidos como consecuencia de tareas fallidas;
g) arranque del sistema y los procedimientos de recuperación a utilizar en caso de fallo del sistema;
h) la administración de auditoria e información de registro del sistema.

Control de cambios operacionales

Se deberían controlar los cambios en los equipos, software o procedimientos para evitar cualquier fallo de seguridad o del sistema. Considerar los siguientes controles y medidas:

a) la identificación y registro de cambios significativos;
b) planificación y verificación de cambios;
c) la evaluación del posible impacto de los cambios;
d) un procedimiento formal de aprobación de los cambios propuestos;
e) la comunicación de los detalles de cambio a todas las personas que corresponda;
f) procesos y responsabilidades para cancelar y recuperar de cambios no exitosos o eventos imprevistos.

Separación de los recursos de desarrollo, prueba y producción

Se debe separar los recursos para desarrollo, prueba y producción con el objetivo de obtener la segregación de las responsabilidades implicadas. Los siguientes elementos deben ser considerados:

a) se deben definir y documentar reglas para la transferencia el software del entorno de desarrollo al de producción;
b) se debe ejecutar en diferentes sistemas o procesadores el software de desarrollo y el de producción y en dominios o directorios diferentes;
c) los compiladores, editores y otras herramientas de desarrollo o utilidades del sistema no deberían ser accesibles desde los sistemas de producción, cuando no se necesiten;
d) el ambiente del sistema de pruebas debe emular la operación del sistema los más cercano posible;
e) usar diferentes procedimientos de conexión en los sistemas de producción y prueba para reducir el riesgo de confusión. Se debería impulsar a que los usuarios para que empleen contraseñas diferentes para estos dos sistemas y los menús deberían exhibir los mensajes de identificación apropiados;
f) datos sensibles no deben ser copiado en los sistemas de pruebas.

2.6.2. GESTIÓN DE SERVICIOS EXTERNOS

Establecer un nivel apropiado de seguridad de la información y entregar el servicio de acuerdo con el contratista.

Entrega del servicio

La entrega del servicio de la parte externa debe incluir los acuerdos de seguridad, definiciones de servicio, y aspectos de administración del servicio. En el caso de arreglos de outsourcing, la organización debe planear las transiciones necesarias (de información, recursos de tratamiento de la información, y alguna otra cosa que necesite ser movida), y debe asegurar que la seguridad es mantenida en el periodo de transición.

Monitoreando y revisando los servicios de las partes externas

La monitorización deben asegurar que los términos de seguridad de la información y condiciones de los acuerdos estén siendo cumplidos, esta monitorización debe ser realizada regularmente. Es recomendable seguir los siguientes pasos:

a) monitorear los niveles de desempeño del servicio para verificar el cumplimiento de los acuerdos;
b) revisar el informe de los servicios producidos por la partes externa y acordar regularmente las reuniones de progreso como requerido por los acuerdo;
c) proporcionar información acerca de los incidentes de la seguridad de la información y revisar esta información por la parte externa y la organización;
d) revisar auditoria de partes externas y registrar los eventos de seguridad, problemas de operación, fallas, enfatizando las fallas y rupturas relacionadas a la entrega de servicio;
e) resolver y manejar cualquier problema identificado.

2.6.3. PLANIFICACIÓN Y ACEPTACIÓN DEL SISTEMA

Garantizar el funcionamiento del sistema, además el sistema debe ser escalable de modo que permita crecimientos futuros y asegurar la continuidad del negocio.

Planificación de la capacidad

Deberían comprobarse las demandas actuales y las proyecciones de los requisitos futuros de capacidad para asegurar la disponibilidad de capacidad de procesamiento y almacenamiento adecuados. Estas proyecciones deberían tener en cuenta los requisitos de las nuevas actividades y sistemas, así como la tendencia actual y proyectada de tratamiento de la información en la organización.

Los administradores deberían usar esta información para identificar y evitar los posibles cuellos de botella que puedan representar una amenaza a la seguridad del sistema o a los servicios al usuario, y para planificar la acción correctora apropiada.

Aceptación del sistema

Se deberían establecer criterios de aceptación para nuevos sistemas de información y versiones nuevas o mejoradas y se deberían desarrollar con ellos

las pruebas adecuadas antes de su aceptación. Los administradores se deberían asegurar que los requisitos y criterios de aceptación de los nuevos sistemas estén claramente definidos, acordados, documentados y probados. Se deberían considerar los siguientes controles:

a) los requisitos de rendimiento y capacidad de los computadores;
b) los procedimientos de recuperación de errores y reinicio, así como los planes de contingencia;
c) la preparación y prueba de procedimientos operativos de rutina según las normas definidas;
d) un conjunto acordado de controles y medidas de seguridad instalados;
e) manual de procedimiento eficaz;
f) Plan de continuidad del negocio;
g) la evidencia de que la instalación del nuevo sistema no producirá repercusiones negativas sobre los existentes, particularmente en los tiempos con pico de proceso como a fin de mes;
h) la evidencia de que se ha tenido en cuenta el efecto que tendrá el nuevo sistema en la seguridad global de la organización;
i) la formación en la producción o utilización de los sistemas nuevos.
j) Facilidad de uso, evitar errores humanos.

2.6.4. PROTECCIÓN CONTRA SOFTWARE MALICIOSO

Evitar crear agujeros de seguridad mediante la prevención y detección de software malicioso.

Controles contra software malicioso

Se debe implementar controles para detención, prevención y recuperación. Los controles siguientes deberían ser considerados:

a) establecer una política formal que prohíba el uso de software no autorizado;
b) establecer una política formal para la protección contra los riesgos asociados con los archivos y software proveniente de redes externas, indicando que medidas preventivas se tomará;

c) realizar revisiones regulares del software y de los datos contenidos en los sistemas que soportan procesos críticos de la organización;
d) instalar y actualizar frecuentemente software de detección de código malicioso y de reparación de virus;
e) definir procedimientos y responsabilidades de administración para la protección de antivirus;
f) preparar planes de continuidad del negocio apropiados para recuperarse de los ataques de virus, incluyendo todos los datos y software necesarios de respaldo;
g) implementar procedimientos para regularmente reunir información, como suscripción a listas de correo y/o verificación de sitios web dando información acerca de nuevos códigos maliciosos;
h) implementar procedimientos para verificar la información relativa al software malicioso y asegurarse que los boletines de alerta son precisos e informativos.

2.6.5. GESTIÓN INTERNA DE RESPALDO

Garantizar la continuidad del negocio, mediante la preservación de los servicios del tratamiento de la información y comunicaciones.

Recuperación de la información

Se deberían hacer y probar regularmente copias de seguridad de toda la información esencial del negocio y del software de acuerdo con la política de respaldo. Se debe considerar los siguientes controles:

a) un nivel mínimo de información de respaldo debe ser definida;
b) registros exactos y completos de las copias de seguridad y a procedimientos documentados de recuperación deben ser producidos;
c) la magnitud y frecuencia de respaldos deben reflejarse en los requerimientos de negocio de la organización, los requerimientos de seguridad involucrados, y la criticidad de la información para la continuidad de operación del negocio;

d) los respaldos deben ser almacenados a una distancia suficiente para evitar todo daño por un desastre en el local principal.

e) se debería dar a la información de respaldo un nivel adecuado de protección física y del entorno, un nivel consistente con las normas aplicadas en el local principal. Se deberían extender los controles y medidas aplicados a los medios en el local principal para cubrir el local de respaldo;

f) los medios de respaldo se deberían probar regularmente, donde sea factible, para asegurar que son fiables cuando sea preciso su uso en caso de emergencia,

g) se deberían comprobar y probar regularmente los procedimientos de recuperación para asegurar que son eficaces y que pueden cumplirse en el tiempo establecido por los procedimientos operativos de recuperación;

h) en situaciones donde la confidencialidad es importante, los respaldos deben ser protegidos por medio de la encripción.

2.6.6. GESTIÓN DE LA SEGURIDAD DE REDES

Proteger la información de las redes y tener una infraestructura estable de redes de comunicaciones.

Controles de red

Las redes deben ser adecuadamente administradas y controladas para mantener la seguridad de los sistemas y aplicaciones, incluyendo información en circulación. Se debe considerar los siguientes controles y medidas:

a) la responsabilidad operativa de las redes debería estar separada de la operación de los computadores si es necesario,
b) establecer responsabilidades y procedimientos para la gestión de los equipos remotos, incluyendo los de las áreas de los usuarios,
c) establecer controles y medidas especiales para salvaguardar la confidencialidad y la integridad de los datos que pasen a través de redes públicas, así como para proteger los sistemas conectados. También se deberían requerir controles y medidas especiales para mantener la

disponibilidad de los servicios de las redes y de los computadores conectados;

d) aplicar monitoreo y registro adecuado, para almacenar las acciones de seguridad relevantes;
e) coordinar estrechamente las actividades de gestión tanto para optimizar el servicio al negocio como para asegurar que los controles y medidas se aplican coherentemente en toda la infraestructura de tratamiento de la información.

Seguridad de los servicios de la red

Las características de seguridad, niveles de servicio, y administración de requerimientos de todos los servicios de la red deben ser identificados e incluidos en cualquier acuerdo de servicios de la red. La organización debe asegurar que los proveedores de servicio implementen estas características. El proveedor de servicio debe manejar los servicios convenidos de una manera segura.

2.6.7. UTILIZACIÓN DE LOS MEDIOS DE INFORMACIÓN

Usar apropiadamente los medios de información de tal manera que se minimicen los daños a los activos.

Gestión de medios removibles

Debería haber procedimientos para la gestión de los medios informáticos removibles como cintas, discos o resultados impresos. Se debe considerar los siguientes controles:

a) se deberían borrar cuando no se necesiten más, los contenidos de todo medio reutilizable del que se desprenda la organización;
b) todo medio desechado por la organización debería requerir autorización y se debería guardar un registro de dicha eliminación,
c) todos los medios se deberían almacenar a salvo en un entorno seguro, de acuerdo con las especificaciones de los fabricantes;
d) la información almacenada en medios que necesita estar disponible más tiempo que el tiempo de vida del medio (de acuerdo a las especificaciones del fabricante) debe también ser almacenada en otro

lugar para evitar pérdida de información debido a la deterioración de los medios de comunicación;

e) se debe considerar la registración de los medios removibles para limitar la oportunidad para la pérdida de datos;
f) los medios removibles deben solamente ser habilitados si hay una razón del negocio para hacerlo.

Eliminación de medios

Se deberían eliminar los medios de forma segura y sin peligro cuando no se necesiten más. Es apropiado considerar:

a) los medios que contengan información sensible se almacenarán y eliminarán de forma segura;
b) los procedimientos deben identificar los elementos que requieren una eliminación segura;
c) puede ser más fácil eliminar con seguridad todos los medios que intentar separar los que contienen información sensible;
d) muchas organizaciones ofrecen servicios de recolección y eliminación de papel, equipos y medios. Debería cuidarse la selección de los proveedores adecuados según su experiencia y que satisfaga los controles que adopten;
e) se debería registrar la eliminación de elementos sensibles donde sea posible para mantener una pista de auditoria.

Procedimientos de manipulación de la información

Se deberían establecer procedimientos de manipulación y almacenamiento de la información de forma coherente con su clasificación para protegerla de su mal uso o divulgación no autorizada. Los siguientes elementos deben ser considerados:

a) etiquetado en la administración de todos los medios;
b) restricciones de acceso para identificar al personal no autorizado;
c) mantenimiento de un registro formal de recipientes autorizados de datos;
d) aseguramiento de que los datos de entrada, su proceso y la validación de la salida están completos;

e) protección de los datos que están en cola para su salida en un nivel coherente con su criticidad;
f) almacenamiento de los medios en un entorno acorde con las especificaciones del fabricante;
g) minimizar la distribución de datos;
h) identificación clara de todas las copias de datos para su atención por el receptor autorizado;
i) revisión de las listas de distribución y de receptores autorizados a intervalos regulares.

Seguridad de la documentación de sistemas

Se debe proteger la documentación de sistemas de accesos no autorizados. Considerar los siguientes controles:

a) la documentación de sistemas se debería almacenar con seguridad;
b) la lista de acceso a la documentación de sistemas se debería limitar al máximo, y ser autorizada por el propietario de la aplicación;
c) la documentación de sistemas mantenida en una red pública, o suministrada vía una red pública, se debería proteger adecuadamente.

2.6.8. INTERCAMBIO DE INFORMACIÓN

Garantizar la seguridad de la información, mantener la integridad para lo cual se debe seguir procedimientos que controlan los intercambios de información.

Políticas y procedimientos del intercambio de información

Los procedimientos y controles a ser seguidos cuando se usa medios de comunicación electrónicos para el intercambio de información deben considerar los siguientes elementos:

a) procedimientos diseñados para proteger el intercambio de información de intercepciones, copia, modificación, pérdida de ruta, y destrucción;
b) procedimientos para la detección y protección de software malicioso que puede ser transmitido a través del uso de comunicaciones electrónicas;
c) procedimientos para la protección de la comunicación de información electrónica sensible;

d) políticas o guías para el uso aceptable de los medios de comunicación electrónicos;
e) procedimientos para el uso de comunicaciones inalámbricas, tomando en cuenta los riesgos particulares involucrados;
f) las responsabilidades de empleados, contratistas, y otros usuarios no be comprometer a la organización, por ejemplo a través de la difamación, remitiendo de cartas de la cadena, la compra desautorizado, etc.;
g) uso de técnicas criptográficas, ejemplo: para la protección de confidencialidad, integridad y autenticación de la información;
h) retención y eliminación de las guías para toda la correspondencia del negocio, incluyendo mensajes, de acuerdo con la legislación local y nacional pertinente y regulaciones;
i) no dejar información sensible o crítica en medios impresos, ejemplo: copias, estos pueden ser accedidos por personal no autorizado;
j) controles y restricciones asociados con el envío de medios de comunicación, ejemplo: envío automático de correo electrónico a direcciones de correo externas;
k) recordar al personal que deben tomar las precauciones apropiadas, ejemplo: no revelar información sensible para evitar ser escuchado o interceptado por casualidad al realizar una llamada telefónica;
l) no dejar mensajes que contienen información en máquinas contestadoras estos pueden ser escuchados por personal no autorizado;
m) recordar al personal acerca de los problemas de usar máquinas facsímile;
n) recordar al personal no registrar datos demográficos, como la dirección de e-mail u otra información personal, en cualquier software para evitar la colección de uso no autorizado;
o) recordar al personal que las máquinas facsímiles modernas o fotocopiadoras tienen caché de páginas y almacenamiento de páginas en el caso de páginas o falta de transmisión, el cual podrá imprimir una vez que la falta es aclarada.

Acuerdos de intercambio

Los acuerdos deben ser establecidos para intercambiar la información y software entre la organización y partes externas. Los acuerdos de intercambio debe considerar las siguientes condiciones de seguridad:

a) responsabilidades de administración para controlar y notificar la transmisión , despacho y recibo;
b) procedimientos para notificar el remitente de transmisión, despacho y recibo;
c) procedimientos para asegurar la identificación y no repudiación;
d) normas técnicas mínimas para empaquetar y transmitir;
e) los acuerdos de la plica;
f) las normas de identificación de mensajero;
g) responsabilidades y obligaciones en el evento de incidentes de seguridad de la información, como pérdida de datos;
h) uso de sistema de rotulación convenido para la información sensible o crítica, asegurando que el significado de los rótulos es inmediatamente comprendido y que la información es apropiadamente protegida;
i) la propiedad y responsabilidades para la protección de datos, derechos de autor, licencias de software y consideraciones similares;
j) estándares técnicos para registrar y leer información y software;
k) controles especiales que pueden ser requeridos para proteger elementos sensibles, como claves criptográficas.

Seguridad de medios en tránsito

La información puede ser vulnerable a accesos no autorizados, a mal uso o a corrupción durante su transporte físico. Se deberían aplicar los siguientes controles y medidas:

a) deberían usarse transportes o mensajeros fiables;
b) debería convenirse entre las gerencias una lista de mensajeros autorizados;
c) procedimientos para comprobar la identificación de los mensajeros;
d) la envoltura debería ser suficiente para proteger el contenido contra cualquier daño físico que pueda ocurrir durante el tránsito;

e) deberían adoptarse controles especiales para proteger la información sensible de la divulgación o modificación no autorizadas;

Mensajería electrónica

Se debe proteger apropiadamente la información involucrada en mensajes electrónicos. Las consideraciones de seguridad para mensajería electrónica debe incluir lo siguiente:

a) protección de mensajes de acceso no autorizado, modificación o deniego de servicio;
b) asegurar el correcto direccionamiento y transporte del mensaje;
c) confiabilidad y disponibilidad del servicio;
d) consideraciones legales, por ejemplo los requisitos para las firmas electrónicas;
e) obtener la aprobación antes de usar los servicios públicos externos;
f) niveles más fuertes de autenticación para controlar el acceso de redes públicas.

Sistemas de información comerciales

Políticas y procedimientos deben ser desarrollados e implementados para proteger la información asociada con la interconexión de sistemas de información comerciales. Se debe incluir:

a) las vulnerabilidades conocidas en los sistemas administrativos y de contabilidad donde la información es compartida entre diferentes partes de la organización;
b) vulnerabilidades de información en sistemas de comunicación comerciales, ejemplo: confidencialidad de llamadas, abriendo el correo, distribución de correo.
c) políticas y controles apropiados para manejar la compartición de información;
d) establecer categorías de información del negocios sensibles y documentos clasificados si el sistema no proporciona un nivel de protección adecuado;

e) restringir el acceso a información del diario que relaciona a los individuos seleccionados, por ejemplo personal que trabaja en los proyectos sensibles;
f) establecer categorías del personal, contratistas o compañeros comerciales permitiendo usar el sistema y las localizaciones de la que puede accederse;
g) identificar el estado de los usuarios, ejemplo: empleados de la organización o contratistas en directorios para el beneficio de otros usuarios.

2.6.9. SERVICIOS DE COMERCIO ELECTRÓNICO

Garantizar el uso adecuado del comercio electrónico y evitar la pérdida de seguridad.

Comercio electrónico

Información involucrada en el comercio electrónico que pasa sobre una red pública debe ser protegida de actividades fraudulentas, divulgación no autorizada y modificación. Consideraciones de seguridad en comercio electrónico debe incluir lo siguiente:

a) el nivel de confidencialidad de cada parte debe exigir confidencialidad, ejemplo: a través de autenticación;
b) asegurar que el compañero comercial esté totalmente informado de sus autorizaciones;
c) determinar y encontrar requerimientos para la confidencialidad, integridad, prueba de expedición y recibo de documentos claves, y la no – repudiación de contratistas;
d) nivel de confianza requerido en la integridad de listas de precios anunciadas;
e) la confidencialidad de cualquier dato o información sensible;
f) la confidencialidad e integridad de cualquier transacción, información de pago, detalles de dirección de entrega, y confirmación de recepción;
g) comprobación apropiado para verificar información del pago proporcionada por un cliente;

h) seleccionar un apropiado formulario de pago para guardar contra fraude;
i) el nivel de protección requerido para mantener la confidencialidad e integridad de información;
j) anulación de pérdida o duplicación de información de la transacción;
k) la obligación asociada con cualquier transacción fraudulenta;
l) requerimientos seguros.

Transacciones en línea

Información involucrada en transacciones en línea deben ser protegidas para prevenir transmisiones incompletas, pérdida de enrutamiento, alteración de mensajes no autorizados, divulgación no autorizada, duplicación de mensajes no autorizados. Las consideraciones de seguridad para transacciones en línea deben incluir lo siguiente:

a) el uso de firmas electrónicas por cada una de las partes involucradas en la transacción;
b) todos los aspectos de la transacción, ejemplo: asegurando que:
    1. Las credenciales del usuario de todas las partes son válidas y verificadas;
    2. Las transacciones permanecen confidencial; y
    3. Privacidad asociada con todas las partes involucradas es retenido;
c) el camino de comunicaciones entre todas las partes involucradas es encriptado;
d) protocolos usados para la comunicación entre todas las partes involucradas es asegurado;
e) asegurar que el almacenamiento de los detalles de la transacción son localizadas fuera de cualquier ambiente público, ejemplo: en una plataforma existente de la Intranet organizacional, y no retuvo y expuso en un medio de almacenamiento directamente accesible del Internet;
f) donde una autoridad es usada para propósitos de seguridad, por ejemplo: para los propósitos de emitir y mantener firmas digitales y/o los certificados digitales.

Publicidad de información disponible.

Se debería cuidar la protección de la integridad de la información publicada para evitar la modificación no autorizada que pueda dañar la reputación de la organización que la publica. El software, datos y otra información que requiera un alto nivel de integridad y que estén disponibles públicamente deberían protegerse por mecanismos adecuados, por ejemplo, firmas digitales. Se debe tratar de:

a) se obtenga una protección de datos de acuerdo con la legislación;
b) la entrada de información y su tratamiento por el sistema de publicación se procesarán completa y exactamente en forma oportuna;
c) la información sensible se protegerá durante su eliminación y almacenamiento;
d) el acceso al sistema de publicación no permitirá el acceso no autorizado a las redes a las que está conectado.

2.6.10. MONITORIZACIÓN

Asegurar que los sistemas se usan adecuadamente y cumplen los requerimientos establecidos, en caso de incidentes de seguridad estos deben ser registrados.

Registros de Auditoria

Se debe registrar las actividades de los usuarios en los registros de auditoria, así como los eventos de seguridad para que sea de ayuda en investigaciones futuras. Los registros de auditoria deben incluir:

a) ID de usuario;
b) fecha, hora, y detalles de eventos claves, ejemplo: conexión y desconexión;
c) si es posible identidad del monitor o localización;
d) en los sistemas de acceso registrar el intento de exitoso y fracaso;
e) en los sistemas de acceso registrar el intento de exitoso y fracaso de los datos;
f) cambios a la configuración de los sistemas;
g) uso de privilegios;

h) uso de utilidades del sistema y aplicaciones;
i) acceso a los archivos y tipo de acceso;
j) direcciones de red y protocolos;
k) alarmas establecidas por el sistema de control de acceso;
l) activación y desactivación de sistemas de protección, como sistemas de anti-virus y sistemas de protección de intrusos.

Monitorizando el uso del sistema

Establecer procedimientos para la supervisión del uso de los recursos de tratamiento de la información. El nivel de monitorización requerido para recursos individuales debe ser determinado por la valoración de riesgos. Las áreas que deben ser consideradas incluye:

a) acceso autorizado;
b) todas las operaciones privilegiadas;
a) intentos de acceso desautorizado;
b) alertas del sistema o fallas;
c) cambios o intentos de cambias en el ambiente del sistema de seguridad y sus controles.

Con que frecuencia se revisan los resultados de las actividades de monitorización depende de los riesgos involucrados. Se debe considerar los siguientes puntos:

a) criticidad de los procesos de aplicación;
b) valor, sensibilidad y criticidad de la información involucrada;
c) la experiencia pasada de infiltración del sistema y mal uso, y la frecuencia de vulnerabilidades que han sido explotadas;
d) magnitud de los sistemas de interconexión (particularmente en redes públicas);
e) registrando servicios siendo desactivados.

Protección de información del registro

Debe protegerse los registros contra el acceso desautorizado. Se debe tomar en cuenta:

a) alteraciones a los tipos de mensajes que son grabados;
b) archivos de registro siendo editados o anulados;
c) capacidad de almacenamiento de los medios de archivo de registro extendiéndose, resultado cualquier falla de eventos de grabación o sobre escrito los pasados eventos de registro;

Registro de administrador y operador

Se deben registrar las actividades del sistema de administrador y sistema de operador.

Los registros deben incluir:

a) el tiempo en que un evento ha ocurrido (éxito o falla);
b) información acerca del evento (ejemplo: manipulación de archivos) o falla (ejemplo: error ha ocurrido y acciones correctivas);
c) que cuenta y que administrador u operador fue involucrado;
d) que procesos fueron involucrados.

Sincronización del reloj

Los relojes de información de los sistemas de información dentro de una organización o dominio de seguridad debe ser sincronizado con una fuente de tiempo exacta.

Donde una computadora o sistemas de comunicaciones tienen la capacidad para operar un reloj en tiempo real, el reloj debe ser establecido de acuerdo a un estándar convenido, ejemplo: Coordinación Universal de Tiempo (UTC) y debe haber un procedimiento que verifica y corrige cualquier variación significante.

2.7. CONTROL DE ACCESOS

2.7.1. REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESOS

Se debería controlar el acceso a la información y los procesos del negocio sobre la base de los requisitos de seguridad y negocio. Se deberían tener en cuenta para ello las políticas de distribución de la información y de autorizaciones.

Política de control de accesos

En la política de control de accesos se debería tener bien definido y documentado los requisitos del negocio para el control de acceso, definiéndose de forma clara las reglas y derechos de cada usuario. Debería contemplar:

a) requisitos de seguridad de cada aplicación de negocio individualmente;
b) identificación de toda la información relativa a las aplicaciones;
c) políticas para la distribución de la información y las autorizaciones;
d) coherencia entre las políticas de control de accesos y las políticas de clasificación de la información en los distintos sistemas y redes;
e) legislación aplicable y las obligaciones contractuales respecto a la protección del acceso a los datos o servicios;
f) perfiles de acceso de usuarios estandarizados según las categorías comunes de trabajos;
g) administración de los derechos de acceso en un entorno distribuido en red que reconozca todos los tipos disponibles de conexión;
h) segregación de roles en el control de acceso;
i) requerimientos para autorización formal de pedidos de acceso;
j) requerimientos para revisiones periódicas de control de acceso;
k) remover derechos de accesos.

2.7.2. GESTIÓN DE ACCESO DE USUARIOS

Se debería establecer procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios.

Estos procedimientos deberían cubrir todas las etapas de acceso de los usuarios, desde el registro inicial de los nuevos hasta la baja del registro de los usuarios que ya no requieran dicho acceso a los sistemas y servicios.

Registro de usuarios

Se considera un procedimiento de registro de ingreso y salida de usuarios para garantizar y revocar el acceso a los sistemas y servicios de información. El registro debería incluir:

a) la utilización de un identificador único para cada usuario,
b) la comprobación de la autorización del usuario por el propietario del servicio para utilizar el sistema o el servicio de información.
c) verificación de la adecuación del nivel de acceso asignado al propósito del negocio y su consistencia con la política de seguridad de la organización
d) la entrega a los usuarios de una relación escrita de sus derechos de acceso;
e) la petición a los usuarios para que reconozcan con su firma la comprensión de las condiciones de acceso;
f) la garantía de que no se provea acceso al servicio hasta que se hayan completado los procedimientos de autorización;
g) el mantenimiento de un registro formalizado de todos los autorizados para usar el servicio;
h) la eliminación inmediata de las autorizaciones de acceso a los usuarios que dejan la organización o cambien de trabajo en ella;
i) la revisión periódica y eliminación de identificadores y cuentas de usuario redundantes;
j) la garantía de no reasignación a otros usuarios de los identificadores de usuario redundantes.

Gestión de privilegios

Al hablar de privilegios se refiere a la prestación o recurso de un sistema de información multiusuario que permita evitar controles del sistema o de la aplicación. El uso inadecuado de privilegios en el sistema, muchas veces se

revela como el factor principal que contribuye al fallo de los sistemas que han sido atacados con éxito.

Se deberían considerar los pasos siguientes para controlar la asignación de privilegios:

a) identificar los privilegios asociados a cada elemento del sistema;
b) asignar privilegios a los individuos según los principios de “necesidad de su uso” “caso por caso”;
c) mantener un proceso de autorización y un registro de todos los privilegios asignados. No se otorgarán privilegios hasta que el proceso de autorización haya concluido;
d) promover el desarrollo y uso de rutinas del sistema para evitar la asignación de privilegios a los usuarios;
e) promover el desarrollo y uso de programas que eviten la necesidad de correr con privilegios;
f) asignar los privilegios a un identificador de usuario distinto al asignado para un uso normal.

Gestión de contraseñas de usuario

Las contraseñas son medios, para validar la identidad de un usuario con el fin de acceder a un sistema o servicio de información. Se debería controlar la asignación de contraseñas por medio de un proceso de gestión formal que debería:

a) requerir que los usuarios firmen un compromiso para mantener en secreto sus contraseñas;
b) proporcionar inicialmente una contraseña temporal segura que forzosamente deben cambiar inmediatamente después;
c) establecer procedimientos para verificar la identidad de un usuario antes de proveer una contraseña ya sea temporal, nueva o reemplazo;
d) establecer un conducto seguro para hacer llegar las contraseñas temporales a los usuarios;
e) las contraseñas temporales deberían ser individuales;
f) el usuario debería confirmar la recepción de la contraseña;

g) las contraseñas no deberían ser almacenadas en la computadora sin estar protegidas;
h) las contraseñas por defecto de los vendedores de software o sistemas deberían cambiarse en la siguiente instalación.

Revisión de los derechos de acceso de los usuarios

Para mantener un control efectivo del acceso a los datos y servicios de información, se debería establecer un proceso de revisión periódica de los derechos de acceso de los usuarios. Este debería:

a) revisar los derechos de acceso de los usuarios a intervalos de tiempo regulares y después de cualquier cambio;
b) revisar y cambiar los derechos de los accesos a los usuarios, cuando un empleado sea reasignado a otro puesto de trabajo dentro de la misma empresa;
c) revisar más frecuentemente las autorizaciones de derechos de acceso con privilegios especiales;
d) comprobar las asignaciones de privilegios a intervalos de tiempo regulares para asegurar que no se han obtenido privilegios no autorizados.

2.7.3. RESPONSABILIDADES DE LOS USUARIOS

Los usuarios deberían ser conscientes de sus responsabilidades en el mantenimiento de la eficacia de las medidas de control de acceso, en particular respecto al uso de contraseñas y a la seguridad del material puesto a su disposición.

Uso de contraseñas

Las contraseñas ofrecen un medio de validar la identidad de cada usuario, pudiendo así establecer los derechos de acceso a los recursos o servicios de tratamiento de la información. Todos los usuarios deberían ser informados acerca de:

a) mantener la confidencialidad de las contraseñas;

b) evitar la escritura de las contraseñas en papel;
c) cambiar las contraseñas si se tiene algún indicio de su vulnerabilidad;
d) seleccionar contraseñas de buena calidad, con una longitud mínima de 6 caracteres;
e) cambiar las contraseñas a intervalos de tiempo regulares o en proporción al número de accesos;
f) cambiar las contraseñas temporales la primera vez que se ingrese al sistema;
g) no incluir contraseñas en ningún procedimiento automático de conexión, que, las deje almacenadas permanentemente;
h) no compartir contraseñas de usuario individuales.
i) no utilizar las mismas contraseñas para el negocio y fuera del negocio.

Equipo informático de usuario desatendido

El equipo informático instalado en zonas de usuario debería tener la protección adecuada. Se les debería recomendar a los usuarios y proveedores de servicio:

a) cancelar todas las sesiones activas antes de marcharse, salvo si se dispone de una herramienta de bloqueo general;
b) desconectar (log-off) los servidores o los computadores centrales cuando se ha terminado la sesión (y no sólo apagar el terminal o el computador personal);
c) proteger el terminal o el puesto de trabajo cuando no estén en uso con un bloqueador de teclado.

Políticas de limpieza de pantalla y escritorio

Deberían adoptarse políticas de limpieza de escritorio para evitar papeles y unidades extraíbles que contengan información que requiera protección. Debería considerarse en la limpieza:

a) información crítica o sensitiva del negocio;
b) deberían dejarse con protector de pantalla Terminales y computadores que soliciten ingreso de contraseñas;
c) deberían ser protegidos los puntos de ingreso y salida de correos, fax;
d) prevenir el uso de tecnología de fotocopiado no autorizado;

e) remover desde las impresoras información crítica o sensitiva del negocio.

2.7.4. CONTROL DE ACCESO A LA RED

Hay que asegurarse que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios, por medio de:

a) interfaces adecuadas entre la red de la organización y las redes públicas o las privadas de otras organizaciones;
b) mecanismos adecuados de autenticación para los usuarios y los equipos;
c) control de los accesos de los usuarios a los servicios de información.

Política de uso de los servicios de la red

Los usuarios sólo deberían tener acceso directo a los servicios para los que estén autorizados de una forma específica. Se debería formular la política de uso de las redes y los servicios de la red, que es conveniente que cubra:

a) las redes y los servicios de la red a los que se puede acceder;
b) los procedimientos de autorización para determinar quién puede acceder a qué redes y a qué servicios de la red;
c) los controles y procedimientos de gestión para proteger el acceso a las conexiones de las redes y a los servicios de la red.
d) el significado de usar el acceso a las redes y servicios de redes.

Autenticación de usuarios para conexiones externas

Las conexiones externas son una fuente potencial de accesos no autorizados a la información, por ejemplo, las realizadas con sistemas de acceso por línea telefónica y módem. Es importante determinar qué nivel de protección es requerido a partir de una evaluación de riesgos, lo que se necesita para seleccionar adecuadamente el método de autenticación.

La autenticación de los usuarios remotos puede lograrse, por ejemplo, usando una técnica criptográfica, mecanismos de hardware o protocolos adecuados. También pueden usarse líneas privadas dedicadas o un mecanismo de

verificación de la dirección del usuario en la red para asegurarse del origen de las conexiones.

Autenticación de nodos de la red

Los dispositivos de conexión remota automática significan una amenaza de accesos no autorizados a las aplicaciones, se deberían autenticar las conexiones a sistemas informáticos remotos.

La autenticación de nodos puede ser una alternativa a la autenticación de grupos de usuarios remotos, cuando éstos estén conectados a un sistema compartido seguro.

Protección a puertos de diagnóstico remoto

Debería controlarse de una manera segura el acceso a los puertos de diagnóstico. En muchos computadores y sistemas de comunicación se instala un servicio de conexión dialup para que los ingenieros de mantenimiento puedan realizar diagnósticos remotos, los que pueden permitir accesos no autorizados si no están protegidos.

Segregación en las redes

Un método para controlar la seguridad de grandes redes es dividirlas en dominios lógicos separados, cada uno protegido por un perímetro definido de seguridad. Entre las dos redes a interconectar puede implantarse como perímetro un gateway seguro que controle los accesos y los flujos de información entre los dominios. Se debería configurar este gateway para que filtre el tráfico entre ellos y bloquee los accesos no autorizados de acuerdo con la política de control de accesos de la organización.

Control de conexión a las redes

Los requisitos de la política de control de accesos para redes compartidas, necesitan incorporar controles que restrinjan las capacidades de conexión de los usuarios. Las restricciones que se impongan se deberían basar en los requisitos de las aplicaciones del negocio y se deberían mantener y actualizar de acuerdo a ellos. Estas restricciones podrían ser, por ejemplo:

a) correo electrónico;
b) transferencia de archivos;
c) acceso interactivo;
d) acceso desde la red limitado a días de la semana u horas concretas.

Control de enrutamiento en la red

Las redes compartidas, especialmente las que cruzan las fronteras de la organización, pueden requerir controles de enrutamiento que garanticen que las conexiones entre computadores y los flujos de información no incumplan la política de control de acceso a las aplicaciones.

La conversión de direcciones de la red también es un mecanismo muy útil para aislar redes y evitar rutas de propagación desde la red de una organización a la red de otra.

2.7.5. CONTROL DE ACCESO AL SISTEMA OPERATIVO

Las prestaciones de seguridad a nivel de sistema operativo se deberían utilizar para restringir el acceso a los recursos del computador, los que deberían ser capaces de:

a) identificar y verificar la identidad de cada usuario autorizado, y si procede, el terminal o la ubicación física del mismo;
b) registrar los accesos satisfactorios y fallidos al sistema;
c) registrar el uso de privilegios especiales al sistema;
d) generar una alarma cuando se quebrante las políticas de seguridad;
e) suministrar mecanismos, adecuados de autenticación;
f) cuando proceda, restringir los tiempos de conexión de usuarios.

Procedimientos de conexión de terminales

Se debería diseñar un procedimiento para conectarse al sistema informático que minimice la posibilidad de accesos no autorizados. Un buen procedimiento de conexión debería:

a) no mostrar identificación del sistema o aplicación hasta que termine el proceso de conexión;

b) mostrar un mensaje que advierta la restricción de acceso al sistema sólo a usuarios autorizados;
c) no ofrecer mensajes de ayuda durante el proceso de conexión que puedan guiar a usuarios no autorizados;
d) validar la información de conexión sólo tras rellenar todos sus datos de entrada.
e) limitar el número de intentos fallidos de conexión;
f) limitar los tiempos máximo y mínimo permitidos para efectuar el proceso de conexión; y concluir si se exceden;
g) mostrar la fecha y hora de la anterior conexión realizada con éxito y la información de los intentos fallidos desde la última conexión;
h) no mostrar la contraseña ingresada al inicio de la conexión;
i) no transmitir contraseñas en texto plano sobre la red.

Identificación y autenticación del usuario

Todos los usuarios deberían disponer de un identificador único para su uso personal y exclusivo, a fin de que pueda posteriormente seguirse la pista de las actividades de cada responsable particular. Los identificadores no deberían dar indicación alguna del nivel de privilegio del usuario, por ejemplo, supervisor, director, etc.

Sistema de gestión de contraseñas

Los sistemas de gestión de contraseñas deberían proporcionar un medio eficaz e interactivo para asegurar la calidad de las mismas. Un buen sistema de gestión de contraseñas debería:

a) imponer el uso de contraseñas individuales con el fin de establecer responsabilidades;
b) permitir que los usuarios escojan sus contraseñas, las cambien e incluyan un procedimiento de confirmación para evitar errores al introducirlas;
c) imponer la selección de contraseñas de calidad;
d) imponer el cambio de contraseñas;

e) imponer el cambio de contraseñas iniciales en la primera conexión si son los usuarios quienes las escogen;
f) mantener un registro de las anteriores contraseñas utilizadas, por ejemplo, durante el último año, e impedir su reutilización;
g) no mostrar las contraseñas en la pantalla cuando se están introduciendo;
h) almacenar las contraseñas y los datos del sistema de aplicaciones en sitios distintos;
i) almacenar las contraseñas en forma cifrada mediante un algoritmo de cifrado unidireccional.

Utilización de las facilidades del sistema

Es fundamental que se restrinja el uso de sistemas o aplicaciones y se mantenga fuertemente controlado el acceso a las mismas. Los controles siguientes deberían ser considerados:

a) usar procedimientos de autenticación para las facilidades del sistema;
b) separar las facilidades del sistema de las aplicaciones de software;
c) limitar el uso de las facilidades del sistema al mínimo número de usuarios autorizados y fiables;
d) autorizar el uso de las facilidades con un propósito concreto (ad hoc);
e) limitar la disponibilidad de las facilidades del sistema;
f) registrar todo uso de las facilidades del sistema;
g) definir y documentar los niveles de autorización para las facilidades del sistema;
h) desactivar todas las facilidades basadas en software y el software de sistemas que no sean necesarios.
i) no dar disponibilidad de las facilidades del sistema a usuarios que tienen acceso a aplicaciones en sistemas donde utilizan separación de tareas.

Desconexión automática de terminales

Se deberían desactivar tras un periodo definido de inactividad los terminales situados en áreas públicas o no cubiertas por la gestión de seguridad de la

organización, o que sirvan a sistemas de alto riesgo, para evitar el acceso de personas no autorizadas.

Limitación del tiempo de conexión

Estas medidas de control se deberían emplear para aplicaciones sensibles, en especial para terminales instalados en áreas públicas o no cubiertas por la gestión de seguridad de la organización. Restricciones como por ejemplo:

a) el uso de ranuras de tiempo predeterminado;
b) restricción de tiempos de conexión al horario normal de oficina, si no existen requisitos para operar fuera de este horario.
c) considerar re – autenticación a intervalos determinados

2.7.6. CONTROL DE ACCESO A LAS APLICACIONES

Se deberían restringir el acceso lógico al software y a la información sólo a los usuarios autorizados. Las aplicaciones deberían:

a) controlar el acceso de los usuarios a la información y las funciones del sistema de aplicación, de acuerdo con la política de control de accesos;
b) protegerse de accesos no autorizados desde otras facilidades o software de sistemas operativos que sean capaces de eludir los controles del sistema o de las aplicaciones;
c) no comprometer la seguridad de otros sistemas con los que se compartan recursos de información;

Restricción de acceso a la información

Se debería dar acceso a la información y a las funciones del sistema de aplicaciones sólo a los usuarios de éste, incluido el personal de apoyo. Deberían considerarse las siguientes medidas:

b) establecer menús para controlar los accesos a las funciones del sistema;
a) controlar los derechos de acceso de los usuarios;
c) controlar los derechos de acceso de los usuarios a otras aplicaciones;
d) asegurarse que las salidas de los sistemas de aplicación que procesan información sensible, sólo contienen la información correspondiente para el uso de la salida y se envían, únicamente, a los terminales y sitios autorizados.

Aislamiento de sistemas sensibles

Algunos sistemas de aplicaciones pueden necesitar un tratamiento especial, que corran en un procesador dedicado, que sólo compartan recursos con otros sistemas de aplicaciones garantizados o que no tengan limitaciones. Las consideraciones siguientes son aplicables:

a) el propietario de la aplicación debería indicar explícitamente y documentar la 'sensibilidad' de ésta;
b) cuando una aplicación sensible se ejecute en un entorno compartido, se deberían identificar y acordar con su propietario los sistemas de aplicación con los que compartan recursos.

2.7.7. INFORMÁTICA MÓVIL Y TELETRABAJO

Se deberían considerar los riesgos de trabajar en un entorno desprotegido cuando se usa informática móvil y aplicar la protección adecuada. En el caso del teletrabajo la organización debería implantar protección en el lugar del teletrabajo y asegurar que existen los acuerdos adecuados para este tipo de trabajo.

Informática móvil

Se debería adoptar especial cuidado para asegurar que la información no se comprometa cuando se usan dispositivos de informática móvil como portátiles, agendas, calculadoras y teléfonos móviles. Se debería formalizar una política que tenga en cuenta los riesgos de trabajar con dispositivos de informática móvil, especialmente en entornos desprotegidos.

Esta política también debería incluir reglas y consejos para conectar los dispositivos de informática móvil a las redes así como una guía para el uso de estos dispositivos en lugares públicos.

Se debería tener cuidado cuando se usen dispositivos de informática móvil en lugares públicos, salas de reuniones y otras áreas desprotegidas fuera de locales de la organización.

Cuando estos dispositivos se usen en lugares públicos, es importante tener cuidado para evitar el riesgo de que se enteren personas no autorizadas. Se

debería disponer de equipos para realizar respaldos rápidos y fáciles de la información, a los que se debería dar la protección adecuada, por ejemplo, contra robo o pérdida.

Teletrabajo

El teletrabajo usa tecnologías de comunicación para que el personal pueda trabajar de manera remota desde un lugar fijo situado fuera de su organización. Se debería proteger debidamente el lugar de teletrabajo contra, por ejemplo, el robo del equipo o información, la distribución no autorizada de información, el acceso remoto no autorizado a los sistemas internos de la organización o el mal uso de los dispositivos.

Se debería considerar lo siguiente:

a) la seguridad física real del lugar de teletrabajo, teniendo en cuenta la del edificio y la de su entorno local;
b) el entorno de teletrabajo propuesto;
c) los requisitos de seguridad de las comunicaciones, teniendo en cuenta la necesidad de acceso remoto a los sistemas internos de la organización;
d) la amenaza de acceso no autorizado a información y recursos por otras personas;
e) el uso de las redes en el hogar, y de los requisitos o restricciones en la configuración de los servicios de red inalámbrica;
f) políticas y procedimientos para prevenir problemas debido a derechos de desarrollo de propiedad intelectual en equipos privados;
g) acceso a equipos privados;
h) requerimientos de protección utilizando firewall y antivirus.

2.8. ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

2.8.1. REQUISITOS DE SEGURIDAD DE LOS SISTEMAS

Todos los requisitos de seguridad, incluyendo las disposiciones para contingencias, la infraestructura, las aplicaciones de negocio y las aplicaciones desarrolladas por usuario; deberían ser identificados y justificados en la fase de

requisitos de un proyecto, consensuados y documentados como parte del proceso de negocio global para un sistema de información.

Análisis y especificación de los requisitos de seguridad

Los requisitos y controles de seguridad deberían reflejar el valor de los activos de información implicados y el posible daño a la organización que resultaría de fallos o ausencia de seguridad. La estimación del riesgo y su gestión son el marco de análisis de los requisitos de seguridad y de la identificación de los controles y medidas para conseguirla.

2.8.2. SEGURIDAD DE LAS APLICACIONES DEL SISTEMA

Se deberían diseñar dentro de las aplicaciones las medidas de control y las pistas de auditoria o los registros de actividad. Éstos deberían incluir la validación de los datos de entrada, el tratamiento interno y los datos de salida.

Se pueden requerir medidas y controles adicionales en los sistemas que procesen o tengan impacto sobre activos sensibles, valiosos o críticos para la organización.

Control del proceso interno

Se deberían incorporar a los sistemas comprobaciones de validación para detectar corrupción de datos. Áreas de riesgo específicas a considerar serían:

a) la ubicación y uso en los programas de funciones ‘añadir’ y ‘borrar’ para cambiar los datos;
b) los procedimientos para evitar programas que corran en orden equivocado o después del fallo de un proceso anterior;
c) el uso de programas correctos de recuperación después de fallas para asegurar el proceso correcto de los datos.
d) protección contra ataques de desbordamiento de buffer.

Autenticación de mensajes

La autenticación de mensajes es una técnica utilizada para detectar cambios no autorizados o una corrupción del contenido de un mensaje transmitido electrónicamente.

Se debería establecer en aplicaciones que requieran protección de la integridad del contenido de los mensajes, por ejemplo, transferencia electrónica de fondos, especificaciones, contratos, propuestas u otros intercambios electrónicos de datos importantes.

2.8.3. CONTROLES CRIPTOGRÁFICOS

Se deberían usar sistemas y técnicas criptográficas para proteger la información sometida a riesgo, cuando otras medidas y controles no proporcionen la protección adecuada.

Política de uso de los controles criptográficos

La organización debería desarrollar una política de uso de las medidas criptográficas para proteger la información.

El desarrollo de una política debería considerar lo siguiente:

a) un enfoque de gestión del uso de las medidas criptográficas a través de la organización;
b) un enfoque de gestión de claves, incluyendo métodos para tratar la recuperación de la información cifrada en caso de pérdida, divulgación o daño;
c) los papeles y responsabilidades de cada cual;
d) la implantación de la política;
e) la gestión de las claves;
f) la forma de determinar el nivel de protección criptográfico adecuado;
g) las normas a adoptar para su implantación eficaz a través de la organización.

Gestión de claves

La gestión de las claves criptográficas es crucial para el uso eficaz de las técnicas criptográficas. Se debería instalar un sistema de gestión para dar soporte al uso por la organización de los dos tipos de técnicas criptográficas, que son:

a) las técnicas de clave secreta, donde dos o más partes comparten la misma clave, que se usa tanto para cifrar como para descifrar la información;
b) las técnicas de clave pública, donde cada usuario tiene un par de claves, una pública (que puede conocer cualquiera) y otra privada (que ha de mantenerse en secreto);
c) el sistema de gestión de claves se debería basar en un conjunto acordado de normas, procedimientos y métodos seguros para:
    a. generar claves para distintos sistemas criptográficos y distintas aplicaciones;
    b. generar y obtener certificados de clave pública;
d) distribuirlas a los usuarios previstos, incluyendo la forma de activarlas y recibirlas;
e) almacenar claves, incluyendo la forma de obtención de acceso a las claves;
f) cambiar o actualizar claves, incluyendo reglas para saber cuándo y cómo;
g) tratar las claves comprometidas (afectadas);
h) revocar claves, incluyendo la forma de desactivarlas o retirarlas;
i) recuperar claves que se han perdido o corrompido como parte de la gestión de continuidad del negocio;
j) archivar claves;
k) destruir claves;
l) hacer seguimiento y auditorías de las actividades relacionadas con la gestión de las claves.

Para reducir la probabilidad de comprometer las claves, se deberían definir fechas de activación y desactivación para que sólo puedan utilizarse durante un periodo limitado. Este debería depender de las circunstancias del uso de las medidas de control criptográficas y del riesgo percibido.

2.8.4. SEGURIDAD DE LOS ARCHIVOS DEL SISTEMA

El mantenimiento de la integridad del sistema debería ser responsabilidad del grupo de desarrollo o de la función del usuario a quien pertenezcan las aplicaciones del sistema o el software.

Control del software en producción

Se debería controlar la implantación de software en los sistemas operativos. Para minimizar el riesgo de corrupción deberían considerarse los siguientes controles:

a) la actualización de las librerías de programas operativos sólo se debería realizar por el responsable correspondiente autorización de la gerencia.
b) los sistemas operativos deberían tener sólo código ejecutable, si es posible.
c) no se debería implantar código ejecutable en un sistema operativo mientras no se tenga evidencia del éxito de las pruebas;
d) se debería mantener un control de todo el software implementado así como la documentación del sistema;
e) se debería tener una estrategia de retroceso antes de implementar un cambio;
f) se debería mantener un registro de auditoria de todas las actualizaciones a las librerías de programas en producción.
g) se deberían retener las versiones anteriores de software como medida de precaución para contingencias.

El software adquirido que se use en sistemas operativos se debería mantener en el nivel de soporte del proveedor. Se deberían aplicar parches al software cuando ayuden a eliminar o reducir las vulnerabilidades.

Protección de los datos de prueba del sistema

Las pruebas de sistema y de aceptación, generalmente requieren un volumen de datos lo mas próximo posible al volumen real. Se deberían aplicar los controles y medidas siguientes:

a) los procedimientos de control de acceso que se consideran para las aplicaciones del sistema operacional se deberían utilizar;

a) autorizar por separado cada vez que se copie información operativa a un sistema de aplicación en prueba;

b) borrar la información operativa de la aplicación del sistema en prueba en cuanto ésta se complete;

c) registrar la copia y uso de la información operativa a efectos de seguimiento para auditoria.

Control de acceso a la librería de programas fuente

Para reducir la probabilidad de corrupción de los programas del sistema, se debería mantener un estricto control en el acceso a las librerías de programas fuente como los siguientes:

a) si es posible, las librerías no deberían residir en los sistemas operativos.

b) se debería nombrar un encargado de la librería para cada aplicación.

c) el personal de apoyo informático no debería tener libre acceso, sin restricción;

d) la actualización de librerías de programas y la entrega de programas a los programadores se debería realizar sólo por el responsable;

e) los listados de programas se deberían mantener en un entorno seguro.

f) se debería mantener un registro de auditoría de todos los accesos a las librerías

g) el mantenimiento y copia de las librerías de programas fuente debería estar sujeta a procedimientos estrictos de control de cambios.

2.8.5. SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE

Se deberían controlar estrictamente los entornos del proyecto y de soporte. Los directivos responsables de los sistemas de aplicaciones también lo deberían ser de la seguridad del entorno del proyecto o su soporte. Se deberían asegurar de la revisión de todo cambio propuesto al sistema para comprobar que no debilite su seguridad o la del sistema operativo.

Procedimientos de control de cambios

Se deberían exigir procedimientos formales de control de cambios que garanticen que la seguridad y los procedimientos de control no están debilitados. Este proceso debería incluir:

a) el mantenimiento de un registro de los niveles de autorización acordados;
b) la garantía de que los cambios se realizan por usuarios autorizados;
c) la revisión de los controles y los procedimientos de integridad;
d) la identificación de todo el software, información, entidades de bases de datos y hardware que requiera mejora;
e) la obtención de la aprobación formal para propuestas detalladas;
f) la garantía de la aceptación por el usuario autorizado de los cambios;
g) la garantía de la forma de implantación que minimice la interrupción del negocio;
h) la garantía de actualización de la documentación del sistema al completar cualquier cambio y del archivo o destrucción de la documentación antigua;
i) el mantenimiento de un control de versiones de toda actualización del software;
j) el mantenimiento de un seguimiento de auditoría de todas las peticiones de cambio;
k) la garantía del cambio de la documentación operativa y de los procedimientos de usuario en función de la necesidad;
l) la garantía de la adecuación del tiempo de implantación de los cambios para no dificultar los procesos de negocio implicados.

Revisión técnica de los cambios en el sistema operativo

Se deberían revisar y probar las aplicaciones del sistema cuando se efectúen cambios, para asegurar que no impactan adversamente en el funcionamiento o en la seguridad. Este proceso debería cubrir:

a) la revisión de los procedimientos de control de la aplicación y de la integridad;

b) la garantía de que el plan de soporte anual y el presupuesto cubren las revisiones y las pruebas del sistema;
c) la garantía de que la modificación de los cambios del sistema operativo se realiza a tiempo;
d) la garantía de que se realizan los cambios apropiados en los planes de continuidad del negocio.

Restricciones en los cambios a los paquetes de software

Se deberían usar los paquetes de software suministrados por los proveedores sin modificación en la medida que sea posible y practicable. Cuando haya necesidad de modificarlos, se deberían considerar los aspectos siguientes:

a) el riesgo de debilitamiento de las medidas de control incorporadas y sus procesos de integridad;
b) la obtención del consentimiento del vendedor;
c) la posibilidad de obtener los cambios requeridos como actualizaciones normales del programa del vendedor;
d) el impacto causado si la organización adquiere la responsabilidad del mantenimiento futuro del software como resultado de los cambios.

Canales encubiertos y código Troyano

Canales por donde puede salir la información, deben ser controlados.

Se debe considerar los siguientes aspectos para limitar el riesgo de la salida de la información, por ejemplo con el uso y la explotación de canales secretos:

a) exploración de medios y de comunicaciones de salida para información oculta,
b) usar sistemas y software que se consideran ser de alta integridad, por ejemplo con productos evaluados;
c) supervisión regular de las actividades del personal y del sistema;
d) supervisión de los recursos utilizados en sistemas informáticos.

Desarrollo externo del software

Deberían ser considerados los siguientes aspectos cuando se externalice el desarrollo de software:

a) acuerdos bajo licencia, propiedad del código y derechos de propiedad intelectual;
b) certificación de la calidad y exactitud del trabajo realizado;
c) acuerdos para hacerse cargo en el caso de fallo de terceros;
d) derechos de acceso para auditar la calidad y exactitud del trabajo realizado;
e) requisitos contractuales sobre la calidad del código;
f) pruebas antes de la implantación para detectar el código Troyano.

2.8.6. GESTIÓN DE VULNERABILIDAD TÉCNICA

Se pretende reducir riesgos, resultado de la explotación de vulnerabilidades técnicas publicadas. La misma que debe ser puesta en ejecución de una manera eficaz, sistemática, y repetible con las medidas tomadas para confirmar su eficacia.

Control de vulnerabilidades técnicas

Se requiere de información oportuna sobre vulnerabilidades técnicas de los sistemas de información que son utilizados en la organización, y la evaluación de la exposición de la organización a tales vulnerabilidades.

Se debería seguir los siguientes pasos para establecer un proceso eficaz de la gestión de las vulnerabilidades técnicas:

a) definir y establecer los roles y las responsabilidades asociados a la gestión de vulnerabilidades técnicas;
b) identificar los recursos de información que serán utilizados para identificar vulnerabilidades técnicas relevantes;
c) definir tiempo máximo para reaccionar a las notificaciones de vulnerabilidades técnicas potencialmente relevantes;
d) cuando se haya identificado una vulnerabilidad técnica potencial, la organización debe identificar los riesgos asociados y las acciones que se tomarán;
e) dependiendo de la prioridad de la vulnerabilidad técnica, la acción tomada se debe realizar según los procedimientos para manejar incidente de la seguridad de la información;

f) determinar los riesgos asociados a instalar un parche;
g) probar y evaluar los parches antes de que sean instalados para asegurarse son eficaces y no dan lugar a los efectos secundarios que no pueden ser tolerados;
h) mantener un registro de auditoria para todos los procedimientos emprendido;
i) el proceso de gestión de la vulnerabilidad técnica se debe supervisar y evaluar regularmente para asegurar su eficacia y eficacia;
j) los sistemas en el alto riesgo se deben tratar primero.

2.9. GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION

2.9.1. DIVULGACIÓN DE EVENTOS Y DE DEBILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN

Para asegurar los eventos y las debilidades de la seguridad de la información asociados a los sistemas de información, los procedimientos formales de la divulgación y de escalada del acontecimiento deben estar en lugar. Todos los empleados, contratistas y usuarios de los terceros deben ser enterados de los procedimientos para divulgar diversos tipos de eventos y de debilidad que pudieron tener un impacto en la seguridad de activos de organización.

Divulgación de eventos de la seguridad de la información

Procedimientos de divulgación formal del acontecimiento de la seguridad de la información se deben establecer, junto con una respuesta del incidente y un procedimiento de escalada, precisando la acción que se adquirirá recibo de un informe de un acontecimiento de la seguridad de la información. Los mismos que deben incluir:

a) el comportamiento correcto que se emprenderá en caso de que se de un evento de la seguridad de la información;
b) Un proceso disciplinario formal establecido para los empleados, contratistas o usuarios de los terceros que ocasionen riesgos de la seguridad.

Divulgación de debilidades de la seguridad

Todos los empleados, contratistas y usuarios de los terceros de los sistemas y de los servicios de información deben observar y divulgar cualquier debilidad observada o sospechada de la seguridad en sistemas o servicios. El mecanismo de divulgación debe estar tan fácil, accesible, y disponible como sea posible.

2.9.2. ADMINISTRACIÓN DE INCIDENTES Y MEJORAS DE LA SEGURIDAD DE LA INFORMACIÓN

Se deben definir las responsabilidades y procedimientos para manejar acontecimientos y debilidades de la seguridad de la información con eficacia una vez que se hayan divulgado. Un proceso de la mejora continua se debe aplicar a la respuesta, supervisión, evaluación, y administración total de los incidentes de seguridad de la información.

Responsabilidades y procedimientos

Las responsabilidades y los procedimientos de la gerencia se deben establecer para asegurar una respuesta rápida, eficaz, y ordenada a los incidentes de la seguridad de la información. Deben ser considerados algunos aspectos:

a) los procedimientos se deben establecer para manejar diversos tipos de incidente de la seguridad de la información;
b) planes de contingencia normales;
c) los rastros de intervención y evidencia similar se deben recoger y asegurar, como apropiado;
d) la acción correcta para recuperarse de brechas de seguridad y de fallos del sistema debe estar cuidadosamente y formalmente controlados.

Aprendizaje desde incidentes de seguridad de la información

Debe haber mecanismos que permitan la cuantificación y supervisión de incidentes de seguridad de la información. La información obtenida de la evaluación de los incidentes de la seguridad de la información se debe utilizar para identificar impactos de incidentes que se repiten.

Colección de evidencia

Se deben desarrollar procedimientos internos para recoger y presentar evidencia para los propósitos de la acción disciplinaria manejados dentro de una organización. En general, las reglas deberían ser:

a) admisibilidad de la evidencia;
b) peso de evidencia: la calidad y lo completo de la evidencia.

Para alcanzar la admisibilidad de la evidencia, la organización debe asegurarse de que sus sistemas de información se conforman con cualquier estándar o código de la práctica publicado para la producción de la evidencia admisible. El peso de evidencia proporcionado debe conformarse con cualquier requisito aplicable.

2.10. GESTIÓN DE CONTINUIDAD DEL NEGOCIO

2.10.1. ASPECTOS DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO

La gestión de la continuidad del negocio debería incluir controles para la identificación y reducción de riesgos, limitar las consecuencias de incidencias dañinas y asegurar la reanudación, a tiempo, de las operaciones esenciales. Así como reducir la interrupción causada por desastres y fallas de seguridad.

Proceso de gestión de la continuidad del negocio

Debería incluir los siguientes elementos clave:

a) comprender los riesgos que la organización corre desde el punto de vista de su vulnerabilidad e impacto;
b) identificar los activos envueltos en el proceso crítico del negocio;
c) comprender el impacto que tendrían las interrupciones en el negocio;
d) considerar la adquisición de los seguros adecuados que formarán parte del proceso de continuidad del negocio;
e) implementar controles adicionales de prevención y mitigación;
f) formular y documentar planes de continuidad del negocio en línea con la estrategia acordada;
g) probar y actualizar regularmente los planes y procesos instalados;

h) asegurar que la gestión de la continuidad del negocio se incorpora en los procesos y estructura de la organización.

Continuidad del negocio y análisis de impactos

El estudio para la continuidad del negocio debería empezar por la identificación de los eventos que pueden causar interrupciones en los procesos de negocio. Se debería continuar con una evaluación del riesgo para determinar el impacto de dichas interrupciones.

Desarrollo e implantación de planes de contingencia

Este control fue definido para asegurar la disponibilidad de la información en niveles aceptables y de acuerdo al nivel critico en el negocio. Se debería considerar:

a) identificar procedimientos de emergencia;
b) identificar una pérdida aceptable de información y servicios;
c) Implantar procedimientos de emergencia para la recuperación en los plazos requeridos;
d) Documentar los procedimientos y procesos acordados;
e) Formación apropiada del personal en los procedimientos y procesos de emergencia acordados;
f) Prueba y actualización de los planes.

Marco de planificación para la continuidad del negocio

Se debería mantener un esquema único de planes de continuidad del negocio para asegurar que dichos planes son consistentes y para identificar las prioridades de prueba y mantenimiento. El mismo que debería considerar:

a) las condiciones para activar los planes que describen el proceso a seguir antes de dicha activación;
b) procedimientos de emergencia que describen las acciones a realizar tras una contingencia que amenace las operaciones del negocio y/o vidas humanas;

c) procedimientos de respaldo con las acciones a realizar para desplazar de forma temporal a lugares alternativos las actividades esenciales del negocio;
d) procedimientos de reanudación que describen las acciones a realizar para que las operaciones del negocio vuelvan a la normalidad;
e) un calendario de mantenimiento que especifique cómo y cuándo se harán pruebas del plan, así como el proceso para su mantenimiento;
f) actividades de concientización y formación diseñadas para comprender los procesos de continuidad del negocio;
g) responsabilidades de las personas, describiendo a cada responsable de la ejecución de cada etapa del plan.

Prueba, Mantenimiento y reevaluación de los planes

Los planes de continuidad del negocio se deberían probar y mantener con ayuda de revisiones y actualizaciones regulares para asegurar la continuidad de su eficacia.

Deberían utilizarse diversas técnicas para proporcionar la seguridad de que los planes funcionarán en la vida real. Éstas deberían incluir:

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

Cualquier organización puede usar estas técnicas, y deberían, en cualquier caso, reflejar la naturaleza del plan de recuperación específico.

2.11. CUMPLIMIENTO

2.11.1. CUMPLIMIENTO CON LOS REQUISITOS LEGALES

Con este control se busca evitar los incumplimientos de cualquier ley civil o penal, requisito reglamentario, regulación u obligación contractual, y de todo requisito de seguridad. El diseño, operación, uso y gestión de los sistemas de

información puede estar sujeto a requisitos estatutarios, regulatorios y contractuales de seguridad.

Identificación de la legislación aplicable

Se deberían definir y documentar de forma explícita todos los requisitos legales, regulatorios y contractuales que sean importantes para cada sistema de información.

Derechos de propiedad intelectual

Se deberían implantar los procedimientos apropiados para asegurar el cumplimiento de las restricciones legales sobre el uso del material protegido como derechos de autor y los productos de software propietario. Se debería considerar:

a) publicar una política de conformidad de los derechos de propiedad intelectual;
b) publicar normas para los procedimientos de adquisición de productos de software;
c) mantener la concientización sobre los derechos de propiedad intelectual, publicando la intención de adoptar medidas disciplinarias para el personal que los viole;
d) mantener los registros apropiados de activos;
e) mantener los documentos que acrediten la propiedad de licencias, material original, manuales, etc.;
f) implantar controles para asegurar que no se exceda el número máximo de usuarios permitidos;
g) comprobar que sólo se instale software autorizado y productos bajo licencia;
h) establecer una política de mantenimiento de las condiciones adecuadas de la licencia;
i) establecer una política de eliminación de software o de su transferencia a terceros;
j) usar herramientas adecuadas de auditoría;

k) cumplir los términos y condiciones de uso del software y de la información obtenida de redes públicas;
l) Evitar duplicación, convirtiendo a otro formato;
m) Evitar la copia parcial o total de libros, artículos o reportes de otros documentos.

Salvaguarda de los registros de la organización

Se deberían proteger los registros importantes de la organización frente a su pérdida, destrucción y falsificación. Es necesario guardar de forma segura ciertos registros, tanto para cumplir ciertos requisitos legales o regulatorios, como para soportar actividades esenciales del negocio.

Para dar cumplimiento a éstas obligaciones la organización debería dar los pasos siguientes:

a) publicar guías sobre la retención, almacenamiento, tratamiento y eliminación de los registros y la información;
b) establecer un calendario de retenciones que identifique los períodos para cada tipo esencial de registros;
c) mantener un inventario de las fuentes de información clave;
d) implantar los controles y medidas apropiadas para la protección de los registros y la información esencial contra su pérdida, destrucción o falsificación.

Protección de los datos y de la privacidad de la información personal

El cumplimiento de la legislación de protección de datos personales requiere una estructura y controles de gestión apropiados. Por mayor facilidad se puede designar un encargado de dicha protección que oriente a los directivos, usuarios y proveedores de servicios sobre sus responsabilidades individuales y sobre los procedimientos específicos a seguir.

Evitar el mal uso de los recursos de tratamiento de la información

Todo uso de los recursos informáticos para fines no autorizados o fuera del negocio se debería considerar como impropio. Si dicha actividad se identifica mediante supervisión y control u otros medios, se debería poner en

conocimiento del gerente responsable de adoptar la acción disciplinaria apropiada.

El uso de un computador con fines no autorizados puede llegar a ser un delito penal. Por tanto, es esencial que todos los usuarios sean conscientes del alcance preciso del acceso que se les permite.

Regulación de los controles criptográficos

El uso de controles criptográficos debería regularse en acuerdos, leyes, reglamentos de cada país. Este control puede incluir:

a) la importación y/o exportación de hardware y software para realizar funciones criptográficas;
b) restricción del uso de encripción;
c) métodos obligatorios o discrecionales de los países para acceder a la información que esté cifrada por hardware o software.

2.11.2. REVISIONES DE LA POLÍTICA DE SEGURIDAD Y DE LA CONFORMIDAD TÉCNICA

Se requiere asegurar la conformidad de los sistemas con las políticas y normas de seguridad. Se deberían hacer revisiones regulares de la seguridad de los sistemas de información.

Conformidad con la política de seguridad

Los gerentes deberían asegurarse que se cumplan correctamente todos los procedimientos de seguridad dentro de su área de responsabilidad. Se deberían realizar revisiones regulares que aseguren el cumplimiento de las políticas y normas de seguridad, si se encuentra incumplimiento, se debería:

a) determinar las causas;
b) evaluar la necesidad de acciones para que no se incumpla nuevamente;
c) determinar e implementar acciones correctivas;
d) revisión de las acciones implementadas.

Comprobación de la conformidad técnica

Se debería comprobar regularmente la conformidad con las normas de implantación de la seguridad en los sistemas de información. La comprobación de la conformidad técnica implica el examen de los sistemas operativos para asegurar que se han implementado correctamente las medidas y controles de hardware y software.

2.11.3. CONSIDERACIONES SOBRE LA AUDITORIA DE SISTEMAS

Con este control se busca maximizar la efectividad y minimizar las interferencias en el proceso de auditoria del sistema; estableciendo la necesidad de controles para salvaguardar los sistemas operativos y las herramientas de auditoria durante las auditorias del sistema.

Controles de auditoria de sistemas

Se deberían planificar cuidadosamente y acordarse los requisitos y actividades de auditoria que impliquen comprobaciones en los sistemas operativos, para minimizar el riesgo de interrupción de los procesos de negocio. Podría incluir:

a) acordarse los requisitos de auditoria con la gerencia apropiada;
b) controlar el alcance de las verificaciones;
c) las verificaciones se deberían limitar a accesos solo de lectura al software y a los datos;
d) otro acceso distinto a solo lectura, únicamente se debería permitir para copias aisladas de archivos del sistema;
e) los recursos de tecnología de la información para realizar verificaciones deberían ser explícitamente identificados y puestos a disposición;
f) los requisitos para procesos especiales o adicionales deberían ser identificados y acordados;
g) todos los accesos deberían ser registrados y supervisados;
h) todos los procedimientos, requisitos y responsabilidades deberían estar documentados.

Protección de las herramientas de auditoria de sistemas

Se necesitarían proteger las herramientas de auditorias de sistemas por ejemplo, software o archivos de datos, para evitar cualquier posible mal uso o daño; para evitar una posible pérdida o información comprometida.

III

DISEÑO PARA LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA INTRANET DE LA CORPORACIÓN METROPOLITANA DE SALUD

3.1. ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA INTRANET CORPORATIVA

En este capítulo se describirá la infraestructura actual de la red de la CMS hasta finales de Agosto del 2007, los datos obtenidos son resultado de la información recogida en colaboración del administrador de la red de la Corporación, inventario realizado y revisión de las instalaciones físicas de la red.

Esta información nos permitirá realizar el análisis de la situación actual de la red en cuanto a seguridad para determinar el punto de partida para la implementación del Sistema de Gestión de Seguridad.

3.1.1. ANTECEDENTES

La Corporación Metropolitana de Salud es una persona jurídica de derecho privado con finalidad social, sin fines de lucro, con sujeción al Título 30 del Libro I del Código Civil Ecuatoriano, a las demás leyes pertinentes de la República del Ecuador y a su Estatuto, aprobado mediante Acuerdo Ministerial Número 902 del 19 de Julio del 2004, emitido por el Ministerio de Salud Pública.

Fue creada con el objetivo principal de desarrollar los mecanismos y las acciones que permitan la implantación de un Sistema de Aseguramiento en Salud voluntario, preferentemente para los ciudadanos y ciudadanas del Distrito Metropolitano de Quito, bajo los principios de universalidad y

solidaridad; como una herramienta para aumentar la cobertura, la calidad y la calidez en la atención de salud, contando con infraestructura, tecnología de calidad y los soportes necesarios para su funcionamiento.

La Misión de la Corporación es prestar servicios de aseguramiento, para garantizar con calidad y humanismo el acceso a servicios de salud de los sectores más vulnerables de la población.

3.1.2. INFRAESTRUCTURA DE LA RED DE LA CORPORACIÓN

3.1.2.1. Ubicación física de la Corporación Metropolitana de Salud (CMS)

La Corporación Metropolitana de Salud opera en el Edificio de la Dirección Metropolitana de Salud, ubicado en las calles Jorge Washington y Av. Amazonas, con vigilancia las 24 horas del día.

El edificio posee seis pisos, distribuidos en dos áreas, las que se encuentran separadas por las escaleras de acceso junto a los ascensores. La CMS, tiene oficinas en la Planta Baja y en el cuarto piso del edificio. En la planta baja funciona el área de Afiliación y Caja y en el piso superior se encuentra el área Administrativa Financiera y la Dirección General. Con respecto a la disposición física de los servidores de la Corporación, estos se encuentran ubicados en el cuarto piso del edificio, en el Área Administrativa Financiera que cuenta con una alarma de seguridad para su acceso.

Los pisos ocupados por la Corporación son de concreto, cuentan con cableado estructurado categoría 5e, lo que facilita la administración física de la red. Cuentan con una red propia de energía eléctrica para los equipos, debidamente separada del cableado de datos.

3.1.2.2. Estructura de la red LAN de la CMS

La red LAN de la CMS cuenta con 4 servidores, 34 estaciones de trabajo de las cuales 26 son clones y 8 son portátiles que se encuentran en el cuarto piso,

distribuidas por departamentos como se muestra en la figura 3.1, las demás estaciones se encuentran en planta baja.

En el cuarto de servidores se tiene:

- 1 Switch 2024 Baseline 3Com de 24 puertos, de los cuales actualmente se encuentran 14 puertos utilizados.
- 1 Switch 2016 Baselina 3Com de 16 puertos, de los cuales se encuentran 11 puertos en uso.

En la planta baja se tiene:

- 1 Switch D-Link DES – 1016 D de 16 puertos, de los cuales 9 se encuentran utilizados

La velocidad de transmisión por la red es de 100 Megabits por segundo.

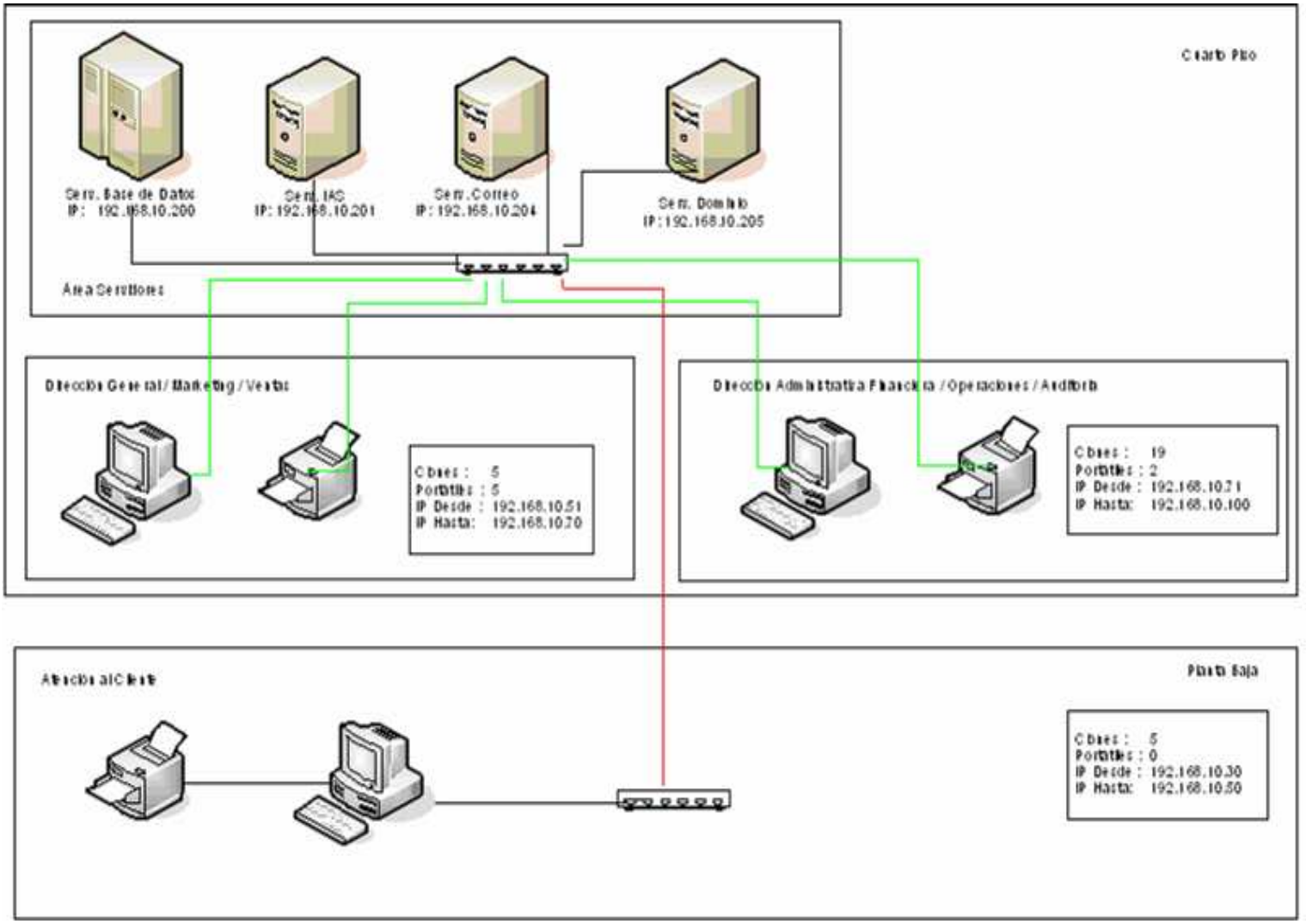

Fig. 3.1. Diagrama de la red LAN de la CMS

3.1.2.2.1. Datos de los servidores

A continuación se detallan los cuatro servidores con los que cuenta la CMS:

Internet Access Server(IAS): El software que se utiliza para levantar el aplicativo que utilizan los usuarios tanto internos como externos está desarrollado en Oracle Aplication Server 10g, además tiene instalado como antivirus el Symantec Client Enterprise Edition 10.1, las características principales del servidor son las siguientes:

Aplicación	Internet Aplication Server	
Procesador	Intel Pentium 4	2.80 Ghz
Disco Duro	80Gb	
Memoria	512 Mb RAM	
Dirección IP	WAN: 201.217.111.170	LAN: 192.168.10.201
Sistema Operativo	Windows Server 2003 Enterprise Edition	

Tabla 3.1. Características del servidor IAS

Base de Datos: Utiliza como base de datos el software Oracle Data Base 10g release 2, levantado sobre el sistema operativo Linux Centos 4.2, con las siguientes características del hardware:

Aplicación	Base de Datos	
Procesador	2 Intel Xeon	2.80 Ghz
Disco Duro	130 Gb	
Memoria	2.00 Gb RAM	
Dirección IP	192.168.10.200	
Sistema Operativo	Linux Centos 4.2	

Tabla 3.2 Características del servidor de Base de Datos

Internet y Correo Electrónico: Utiliza los beneficios del sistema operativo Linux, el aplicativo Squid para levantar el servidor de correo electrónico, con las siguientes características físicas:

Aplicación	Internet, Correo Electrónico	
Procesador	Intel P4	2.80 Ghz
Disco Duro	80Gb	
Memoria	512 Mb	
Dirección IP	WAN: 200.107.42.52	LAN: 192.168.10.204
Sistema Operativo	Linux Versión 2.6	

Tabla 3.3. Características de servidor de correo electrónico e internet

Dominio: Para el servicio de Dominio se utiliza el Active Directory, del sistema operativo Windows 2003 Server.

Aplicación	Servidor de Dominio	
Procesador	Intel P4	2.80 Ghz
Disco Duro	80Gb	
Memoria	512 Mb	
Dirección IP	192.168.10.205	
Sistema Operativo	Windows Server 2003 Enterprise Edition	

Tabla 3.4. Características del servidor de dominio

En cuanto a instalaciones de parches, no se tiene un procedimiento aprobado para la actualización y mantenimiento de software.

3.1.2.2.2. *Datos de las estaciones de trabajo*

Las 34 estaciones de trabajo tienen instalado el antivirus Symantec Client, así como Microsoft Office XP Profesional, utilizan como navegador Web a Microsoft Internet Explorer 5.0, tienen instalado además Acrobat Reader. A continuación se detallan las características de los equipos:

CPU	21 equipos desktops Clon	
Procesador	Intel Pentium IV	2.80 Ghz
Disco Duro	10 equipos con 40 GB	11 equipos con 80 GB
Memoria	10 equipos con 256 MB	11 equipos con 512 MB
Sistema Operativo	Windows XP Professional con Service Pack 2	

Tabla 3.5. Característica de los equipos de cómputo desktops Clon

CPU	3 portátiles EliteGroup	
Procesador	Mobile	1.6 Ghz
Disco Duro	40 GB	
Memoria	496 MB	
Sistema Operativo	Windows XP Professional con Service Pack 2	

Tabla 3.6. Características de las computadoras portátiles EliteGroup

CPU	5 equipos desktops Imax	
Procesador	Intel	2.80 Ghz
Disco Duro	80 GB	
Memoria	192 MB	
Sistema Operativo	Windows XP Professional con Service Pack 2	

Tabla 3.7. Características de los equipos de cómputo desktops Imax

CPU	4 portátiles HP Compaq	
Procesador	Intel	2.80 Ghz
Disco Duro	40 GB	
Memoria	256 MB	
Sistema Operativo	Windows XP Professional con Service Pack 2	

Tabla 3.8. Características de las computadoras portátiles HP Compaq

CPU	1 portátil Acer	
Procesador	Intel	1.86 Ghz
Disco Duro	100 GB	
Memoria	512 MB	
Sistema Operativo	Windows XP Professional con Service Pack 2	

Tabla 3.9. Características de la computadora portátil Acer

Además en la red LAN se encuentran conectadas 10 impresoras de las cuales 4 son HP LaserJet 1320N, 5 impresoras Epson LX – 300 y 1 impresora Fargo. Actualmente en la red interna no se encuentra implementado ningún sistema de gestión que permita una administración de la red. Es decir no cuenta con

ninguna herramienta de Software, Hardware que permita el monitoreo de la red y el análisis de vulnerabilidades.

3.1.2.3. Estructura de la red WAN de la CMS

La Corporación cuenta con dos enlaces a Internet, 1 Enlace SDSL (sincrónico) de 1.024/1024 Kbps contratado a la compañía SURATEL y que es utilizado para acceso de los prestadores de salud a la aplicación de Planillaje.

1 Enlace ADSL (asincrónico) de 256/128 Kbps contratado a la compañía Andinadatos y que es utilizado para acceso a la Internet.

Cuenta con 2 módems que son propiedad de los proveedores del servicio de Internet. Los que se encuentran conectados al Switch 3 Com para proveer tanto del servicio de Internet a la red interna como el acceso de los prestadores hacia los servidores.

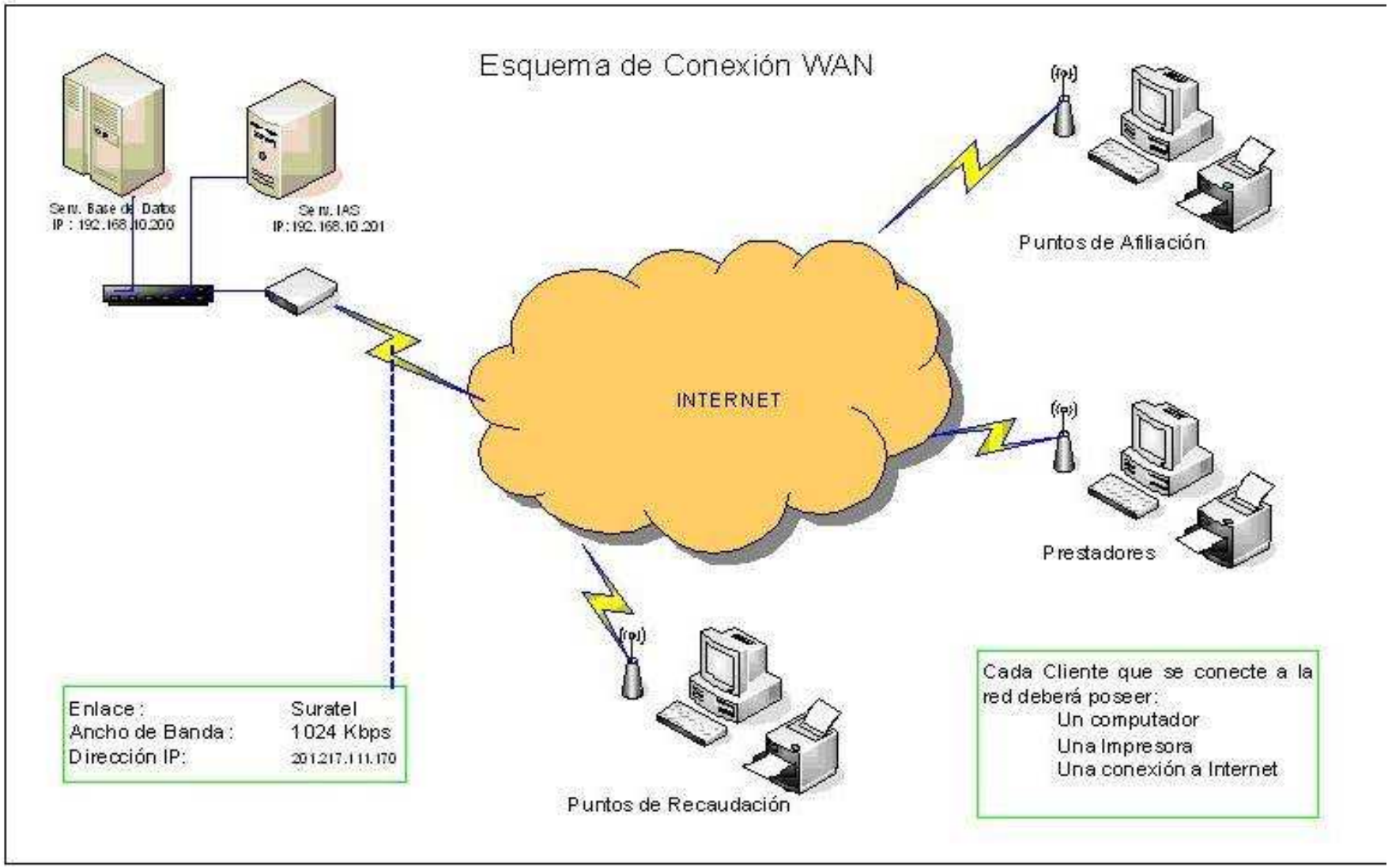

Fig. 3.2. Diagrama de la red WAN de la CMS

3.1.2.3.1. Enlaces de comunicación

La Corporación Metropolitana de Salud cuenta para su funcionamiento con dos enlaces de Internet, a continuación se da una descripción de cada uno de los enlaces:

Proveedor	ANDINADATOS
Teléfono	2924217 – 2941955 – 1800100100
Contacto	Diego Domínguez
Ancho de Banda	ADSL 256-128 Kbps Corporativo
Contrato	No. 850181
Direcciones IP Reales	200.107.42.52
Descripción Enlace	Dedicado exclusivamente a correo interno e Internet

Tabla 3.10. Características del enlace con Andinadatos

Proveedor	Suratel - TV Cable
Teléfono	2992400 – 6002444
Contacto	Ejecutivo Técnico Última Milla: Byron Ponce ext 2520. Ejecutivo Técnico Internet: Xavier Rojas. Ejecutivo SAC (Atención al Cliente Corporativo): Roberto Guerrero ext. 2225.
Ancho de Banda	1024/1024 kbps Metro Ethernet
Contrato	No. 65799
Direcciones IP Reales	201.217.111.170
Descripción Enlace	Dedicado exclusivamente al uso del sistema para los prestadores de salud

Tabla 3.11. Características del enlace con Suratel

3.1.3. SEGURIDAD DE LA INFORMACIÓN IMPLEMENTADA ACTUALMENTE EN LA CORPORACIÓN

Para proporcionar una visión de la situación actual de la seguridad en la Corporación, se realizó un análisis para determinar el grado de seguridad y saber cómo la empresa ha venido salvaguardando las ventajas competitivas.

3.1.3.1. Seguridad de las Comunicaciones

Correo Electrónico

La CMS cuenta con un sistema único de correo tanto para mail interno como externo, este se encuentra alojado en el servidor interno que se utiliza para la navegación de Internet, se encuentra bajo Linux y es administrado a través de SendMail, el mismo que fue configurado en su momento por un proveedor de la compañía y q actualmente es administrado por el Encargado de TIC.

La CMS tiene adquirido en NIC un dominio (cms.com.ec), el mismo que es el dominio de todas las cuentas de correo que se crean.

El correo se lee a través de un cliente de correo como Microsoft Outlook u Outlook Express el cual debe estar instalado en cada una de las maquinas clientes.

La configuración del servidor permite que todos los correos se almacenen en cada una de las maquinas clientes, y que no queden residente en el servidor.

El Outlook Express se instala con su configuración por defecto y puede ser modificado por el usuario, el que puede modificar las siguientes características:

- Vista previa,
- Confirmación de lectura,
- Block sender,
- Controles ActiveX y Scripts.

Si un empleado necesita una dirección de mail, porque su puesto de trabajo lo amerita, el Gerente del área al que pertenece le avisa al encargado de TIC, y éste le crea la cuenta de correo respectiva.

Los empleados no usan el mail solamente para funciones laborales, sino también con fines personales. Es posible ver los mail que se envían y se reciben a través del administrador, pero actualmente no se realizan controles, de manera que pueden usarlo para cualquier fin.

Antivirus

La CMS adquirió a inicios del 2007 33 licencias corporativas del antivirus Symantec Client, con lo cual se tienen protegidas al Servidor de Dominio (licencia para servidor) y a el numero de maquinas indicadas (licencias Cliente), las otras computadoras (laptops) se mantienen con el AVG.

No han existido muchos inconvenientes con virus, a excepción de algunos dispositivos extraíbles.

Desde Internet se actualizan las listas de virus del Symantec, el mismo que se actualiza en el Servidor. Los usuarios son los responsables de actualizar sus propios antivirus y para esto tienen en su escritorio un icono apuntando a la última actualización bajada de Internet. No se hacen chequeos ocasionales para ver si se han actualizado los antivirus.

No se hacen escaneos periódicos buscando virus en los servidores ni en las PC´s. No hay ninguna frecuencia para realizar este procedimiento, ni se denominó a ningún responsable. En algunas máquinas (en las que han tenido problemas frecuentes con virus), cuando el equipo se inicia, entonces comienza un escaneo del antivirus antes del inicio de Windows.

Ataques de red

En la empresa no disponen 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. No hay herramientas para detección de intrusos.

No hay controles con respecto a la ocurrencia de Denial of Service. No existen herramientas que lo detecten, ni hay líneas de base con datos sobre la actividad normal del sistema para así poder generar avisos y limitar el tráfico de red de acuerdo a los valores medidos.

Contraseñas

El archivo de los passwords del sistema no se almacena en el directorio por default del Linux, en el /etc/passwd, aquí solo se almacena un archivo con los

nombres y demás datos de usuarios. Este archivo está en texto plano y puede ser accesible ya que no está encriptado. El archivo que contiene las passwords se encuentra en otro directorio, al cual solo el root tiene permisos para accederlo, éste es un archivo shadow, donde están encriptadas. Se usa encriptación one way (en un solo sentido), de manera que no es posible desencriptar. En el momento del logeo, se encripta la contraseña ingresada por el usuario y se compara ésta contraseña encriptada con el dato almacenado que también está cifrado, si ambos son diferentes el logeo será fallido. Para modificar las passwords, Linux accede a los datos simulando ser root, por lo que es posible la transacción.

3.1.3.2. Seguridad de las Aplicaciones

Seguridad de Base de Datos

En la empresa se utiliza Oracle Data Base 10g release 2 para el almacenamiento y la administración de los datos, los cuales están almacenados en su repositorio respectivo de Base de Datos, el cual maneja las seguridades propias de la OracleDataBase.

Solo existe una aplicación informática de uso de la CMS, este aplicativo esta formado por algunos módulos como Contabilidad, Tesorería, Afiliación, Salud.

El nivel de acceso a la aplicación, se lo realiza a través del propio aplicativo, en el modulo de administración, donde se registran y se dan los accesos respectivos a cada uno de los usuarios del sistema informático.

La única persona que puede tener acceso a los archivos de la base de datos es el administrador del sistema y todo aquel que opere el servidor de aplicaciones (es decir las personas que tengan acceso físico al equipo y con clave).

Los aplicativos que administran la base de datos disponen de recursos suficientes para su funcionamiento, ya que aproximadamente solo el 30% de los recursos del servidor están en uso, el resto está ocioso.

Cada una de las transacciones efectuadas en las distintas tablas de la base de datos, se almacenan en el registro de Auditoria propio de Oracle, con lo que se

puede determinar entre otras cosas que usuario, desde que maquina y en que fecha realizó alguna transacción.

Control de Aplicaciones en PC's

Actualmente ningún usuario puede instalar aplicaciones en sus equipos, en caso de querer instalar una nueva aplicación se debe dar a conocer la necesidad de la misma y luego solicitar al Encargado de TIC la instalación respectiva.

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. Solo hay una instalación básica de alguna versión del Windows, Internet Explorer, Antivirus (Symantec, AVG) y en aquellas maquinas que requieren acceso al sistema se les instala las el ORacleForms Runtime y el Oracle Reports Runtime para que se pueda ejecutar la aplicación desarrollada.

Tampoco se realizan actualizaciones de los programas instalados, como el Internet Explorer y el Microsoft Office. No se buscan Service Packs ni nuevas versiones. No se tiene políticas de actualización de programas.

Solamente el Encargado de TIC es el responsable de las instalaciones en las PC's, para los usuarios existen restricciones con respecto a la instalación de programas. Pueden bajar de la web cualquier aplicación pero no instalarla en su PC.

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

3.1.3.3. Seguridad Física

Control de acceso físico al centro de cómputo

En el momento de la instalación del centro de cómputos no se efectuó un análisis de costo-beneficio para determinar que controles de acceso físico sería necesario implementar.

La sala de equipos se encuentra ubicado en un antiguo baño que permanece cerrada con una única llave, de la que es custodio el administrador del sistema, pero la puerta tiene una cerradura muy vieja, por lo que es susceptible de abrir con otros objetos. La sala no dispone de un sistema de detección y extinción de incendios. Esta sala al ser un antiguo baño tiene únicamente un tapón que le protege de la canalización de agua más cercana.

La empresa cuenta con guardias de seguridad; en horarios laborales se ubican en el exterior e interior de la misma, y cuando se cierra la empresa cuentan con un guardia en la entrada del edificio, las áreas correspondientes a Atención al Cliente y al área Administrativa Financiera manejan un sistema de alarma, el mismo que debe ser activado cada noche previo a la salida de las áreas respectivas. No hay tarjetas magnéticas de entrada ni llaves cifradas en ningún sector del edificio.

El personal que tiene el acceso permitido al centro de cómputos es el de Tecnologías de Información y Comunicaciones.

En horas de oficina hay un control de entrada que identifica a los empleados y registra su hora de entrada y de salida. Los controles de acceso son propios de la unidad, no del edificio, que es de uso compartido con otras actividades. No hay ningún control sobre qué hay en el piso de arriba o en el piso de abajo.

Control de acceso a los equipos

Dispositivos como disqueteras y lectoras de CD están habilitadas y no hay ningún control sobre ellos, no se hacen controles automáticos de virus ni se prohíbe el booteo desde estos dispositivos. Nunca hubo robo de datos usando medios externos.

No se realizan controles periódicos sobre los dispositivos de hardware instalados en las PC´s, de manera que alguien podría sacar o poner alguno. Una vez que se ha completado la instalación de algún equipo, el administrador del sistema no realiza chequeos rutinarios o periódicos, solo revisa los equipos ante fallas en los mismos, o por un problema reportado por el usuario.

Los servidores del centro de cómputos no se apagan en horarios no laborales, debido a que se debe acceder a ellos desde los prestadores de salud en un horario 365x7x24, permanecen prendidos las 24 horas del día.

Estructura del Edificio

Cuando se construyó el edificio de la empresa, no se tuvo en cuenta el diseño del centro de cómputos y sus condiciones de seguridad. Por este motivo actualmente está ubicado en un antiguo baño. Está ubicado en un piso elevado, ya que en los pisos inferiores se encuentra otras instituciones.

Las paredes externas del centro de cómputos son del mismo tamaño de las paredes de todo el piso, existe una ventana pequeña que da hacia fuera del edificio, tiene una puerta pequeña de madera con un área de 10x40 cms de vidrio para poder ver hacia el interior. No existen puertas en la mayoría de oficinas.

Dispositivos de Soporte

En la empresa disponen de los siguientes dispositivos para soporte del equipamiento informático:

- Aire acondicionado y calefacción para el centro de cómputo: la temperatura se mantiene entre 19ºC y 20ºC. solo para esta área, con el fin de mantener esta temperatura todos los días.

- UPS: (Uninterruptible Power Supply) en el centro de cómputos hay un APS en serie que pueden mantener los servidores y funcionando por aproximadamente 4 horas.

- Cada computadora tiene su propio UPS que las protege durante 5 minutos aproximadamente para poder resguardar los datos y apagar el computador durante una falla de energía.

- Descarga a tierra: Existe una conexión a tierra que funcionan como descarga para el edificio.

Cableado Estructurado

La instalación del cableado fue tercerizada, y se implementó un cableado estructurado. Para diagramar los canales de red se tuvieron en cuenta los posibles desastres como inundación, cortes eléctricos, problemas de desagües o campos magnéticos.

El cableado se lo realiza a través de canaletas que se ubican en el contorno de cada una de las paredes por donde tienen que pasar los cables, estas canaletas, se utilizan además perfiles de aluminio en algunas áreas. Estos paneles no son prácticos a la hora de hacer modificaciones en el cableado, debido a la cantidad de cables que pasan por ellos y al poco espacio con el que cuentan, pero resultaron económicos y son seguros en cuanto no es fácil desarmarlos.

En todo el trayecto del cableado se tuvo en cuenta la distancia mínima necesaria entre cables para no provocar interferencias, daños o cortes. Además no hay distancias grandes recorridas con cables UTP.

3.1.3.4. Administración del centro de procesamiento de datos

Responsabilidad del equipo de sistemas

No hay responsabilidades puntuales asignadas a cada empleado, tampoco hay un encargado de la seguridad. Existe un responsable general del área de Tecnologías de Información y Comunicaciones, que es el Encargado de TIC. Él es el que planifica y delega las tareas a un único empleado del área de sistemas adicional, generalmente una vez por semana haciéndolo responsable de sus propios tiempos.

El administrador es el encargado de reportar a los jefes de área sobre las actividades en el AREA DE TIC. Estos reportes generalmente se realizan a modo de auto evaluación ya que no son un pedido de ningún directivo.

Mantenimiento

- Solicitud de mantenimiento: cada vez que los usuarios necesitan asesoramiento o servicios del área de tecnologías, se comunican

telefónicamente con el encargado explicando su situación. Cada requerimiento no se registra en un documento.

- Mantenimiento preventivo: Se tenía contratado un servicio de mantenimiento de hardware con una empresa externa, pero actualmente ese trabajo es realizado por el personal de TIC.

- Clasificación de datos y hardware: los equipos de la empresa no han sido clasificados formalmente según su prioridad, aunque se puede identificar que las máquinas que están en el sector de atención al público tienen mayor prioridad que el resto. En la escala siguen las de financiero, dirección, y por último el resto de las PC´s, en cuanto al orden de solución de problemas.

- Rótulos: Actualmente existe un inventario detallado de las características de los equipos de computación con su respectivo rotulo de inventario, al igual que las licencias.

Instaladores

Los instaladores de las aplicaciones utilizadas en la empresa se encuentran en sus CD´s originales almacenados en un armario del centro de cómputos, y no disponen de instaladores en disquetes.

Licencias

Están actualmente licenciados 34 equipos con Windows XP y 33 equipos con Microsoft Office 2003. Se adquirieron las licencias de la Base de Datos Oracle, y de las herramientas de desarrollo.

Backup

- Backups de datos en los servidores:

  Cuando se hace un cambio en la configuración del servidor, no se guardan copias de las configuraciones anterior y posterior al cambio, ni

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. Además no se realizan chequeos para comprobar que el funcionamiento sea el correcto.

- Backups de datos en las PC's:

Los usuarios deben realizar sus propios backups de los datos almacenados en sus máquinas, ya que estos datos son propiedad de los empleados.

Si hacen un backup deberían hacerlo en sus propias máquinas o en disquetes.

Documentación

En el centro de cómputo existe documentación sobre:

- Licencias del software, y en qué máquinas está instalado.
- Números IP de las máquinas y de los switches.
- Gráficos de la ubicación física de los equipos de las distintas áreas.

No hay backups de ninguno de estos datos, ya que son documentos impresos que se van modificando manualmente.

Existe un plan de contingencia elaborado por la empresa desarrolladora del software, pero no se ha realizado la implementación del mismo.

3.2.ESTABLECIMIENTO DE REQUERIMIENTOS DEL SGSI

Para el establecimiento de los requerimientos del SGSI es necesario determinar la estructura organizacional de la organización, para de esta forma identificar los procesos críticos de la misma, así como las diferentes entidades que influyen de alguna manera, luego de entender los procesos de la organización se puede definir el alcance del SGSI dependiendo de la realidad de la Corporación.

3.2.1. ESTRUCTURA ORGANIZACIONAL POR PROCESOS DE LA CORPORACIÓN METROPOLITANA DE SALUD

Para tener una visión clara del alcance del establecimiento de SGSI es indispensable comprender la estructura organizacional de la empresa, para más adelante identificar los activos más importantes en base a los objetivos del negocio y su criticidad, tal como recomienda la norma ISO 27001:2005.

A continuación de detalla la estructura organizacional por procesos de la Corporación Metropolitana de Salud y las funciones respectivas de cada proceso y subproceso, así como las organizaciones externas a la CMS:

Subproceso "Gestión de Recursos Humanos"

- Informe de reclutamiento y selección
- Informes consolidados de evaluación de desempeño
- Acciones de personal registradas y contratos
- Consolidación del plan de capacitación
- Informe de ejecución del plan de capacitación
- Nómina de pago
- Reportes estadísticos
- Informes de sumarios administrativos y vistos buenos

Subproceso "Gestión de Servicios Institucionales"

- Plan de transporte
- Informes de ejecución del plan de transporte
- Plan de adquisiciones
- Informes de ejecución del plan de adquisiciones
- Planes de mantenimiento
- Informe de ejecución de los planes de mantenimiento
- Inventario de bienes muebles e inmuebles
- Informes para el pago de servicios básicos

- Informe de servicios informáticos
- Informe de proveeduría
- Plan de mejoramiento de calidad
- Informe del Plan de mejoramiento

Subproceso de "Gestión Informática"

- Plan informático
- Informe de ejecución del Plan Informático
- Informe de desarrollo de Software
- Plan de mantenimiento de Software y Hardware
- Plan de mejoramiento de procesos automatizados
- Informes de administración de redes de conectividad
- Informe de ejecución del plan de mejoramiento
- Plan informático de contingencia
- Informe de ejecución del plan de contingencia

PROCESO DE GESTIÓN FINANCIERA

Subproceso de "Gestión presupuestaria y Contabilidad"

- Proforma presupuestaria
- Informe de ejecución de la pro forma
- Informes y reportes de estados financieros
- Informes de control previo y concurrente
- Informes de saldos financieros
- Reformas presupuestarias
- Liquidación presupuestaria
- Consolidación financiera
- Registro de transacciones económicas con afectación presupuestaria
- Cédulas presupuestarias codificadas
- Plan de mejoramiento de la calidad

- Informe de ejecución del plan de mejoramiento

Subproceso "Administración de Caja"

- Informes de pagos a terceros
- Informes de cobros a terceros
- Informes de pagos de nómina
- Informes de custodia de garantías y valores
- Informes de control previo
- Programación mensual conjunta de administración de caja
- Plan de mejoramiento de la calidad
- Informe de ejecución del plan de mejoramiento

Proceso "Aseguramiento de la Calidad"

- Plan estratégico y operativo
- Informes de ejecución del plan estratégico y operativo
- Informes de gestión de procesos gobernantes
- Informes de gestión de procesos habitantes de apoyo
- Informes de gestión de habilidades de asesoría
- Informes de gestión de procesos de valor agregado
- Reportes del Sistema Común de Información para los usuarios
- Informe de convenios y compromisos de gestión
- Plan de mejoramiento de la Calidad
- Plan e informe de mejoramiento continuo de la calidad de gestión

Proceso "Asesoría Jurídica"

- Demandas y Juicios
- Informe de criterios jurídicos
- Contratos y convenios
- Informes Legales Periódicos

- Plan e Informe de mejoramiento de la calidad

Proceso "Promoción de la Salud"

- Atención al cliente
- Aceptación de clientes
- Recepción de quejas, reclamos, sugerencias, consultas
- Resolución de quejas para lo cual se coordina con el área indicada
- Operación de las políticas de promoción de la salud
- Operación de la información, comunicación y educación
- Operación de la participación comunitaria

Proceso "Afiliación de Clientes"

- Ingreso de nuevos clientes en el sistema
- Definición de planes y coberturas acorde a las necesidades del cliente
- Emisión de facturas para pago de afiliación
- Entrega de tarjetas de afiliación
- Recepción de pago mensual (Servicio de cobranza)

Proceso "Operaciones y Servicios Generales"

- Actualización de estados de afiliación
- Bloqueo y desbloqueo de afiliados
- Inscripción de nuevos prestadores del servicio médico
- Mantenimiento del sistema en prestadores

Proceso "Operación, Control y Mejoramiento en gestión de servicios de salud"

- Prestadores verificación cobertura de la afiliación
- Prestación de servicio médico
- Emisión factura al afiliado
- Registro de atención en el sistema

- Recepción de factura del prestador
- Auditoria para comprobar valores
- Autorización para la emisión de pago respectivo
- Entrega efectivo
- Informes de ejecución del plan de aseguramiento de salud

ORGANIZACIONES EXTERNAS A LA CMS

Clientes

Los clientes pueden ser considerados de dos maneras:

1. Individual, incluyendo a la familia.
2. Corporativo, empresa que desea afiliar a sus empleados.

Prestadores de Servicios

Se refiere a las instituciones o empresas que dan servicios médicos, por ejemplo: hospitales, clínicas, etc.

Proveedores de Internet

Empresas que prestan el servicio de Internet, para nuestro caso, son: Suratel y TV Cable.

3.2.2. DEFINICIÓN DEL ALCANCE DEL SGSI DE LA CMS

Una vez que ya se tienen identificados los procesos que forman parte de la empresa, se determinará el alcance del SGSI en base a un método que brinde una identificación clara de las dependencias, relaciones entre las divisiones, áreas, procesos de la organización. Para nuestro caso seleccionamos un método sencillo pero preciso como es el método de las eclipses, en el cual se deben definir identificar los procesos principales de la organización, así como las organizaciones internas y externas a los mismos, y la relación de estas con los procesos. En base a esto identificamos los procesos principales a los siguientes:

- Promoción de Salud

- Afiliación de clientes
- Operaciones y Servicios Generales
- Operación, Control y Mejoramiento en gestión de servicios de la salud

El segundo paso de este método es identificar la eclipse intermedia las distintas interacciones que los subprocesos de la eclipse concéntrica tienen con otros procesos de la empresa. El objetivo es identificar a los dueños de esos procesos y los activos de información involucrados en el eclipse concéntrico, para determinar cuales son los recursos indispensables para que la empresa pueda cumplir con sus objetivos de negocio.

En la eclipse externa se identifican aquellas organizaciones extrínsecas a la empresa que tienen cierto tipo de interacción con los subprocesos identificados. Las flechas indican la interacción. Aquí también se deben identificar los distintos tipos de activos de información, con el objetivo de averiguar el tipo de acuerdos que se debe establecer con las terceras partes. Esta información se obtiene del siguiente diagrama:

ESTRUCTURA ORGANIZACIONAL POR PROCESOS

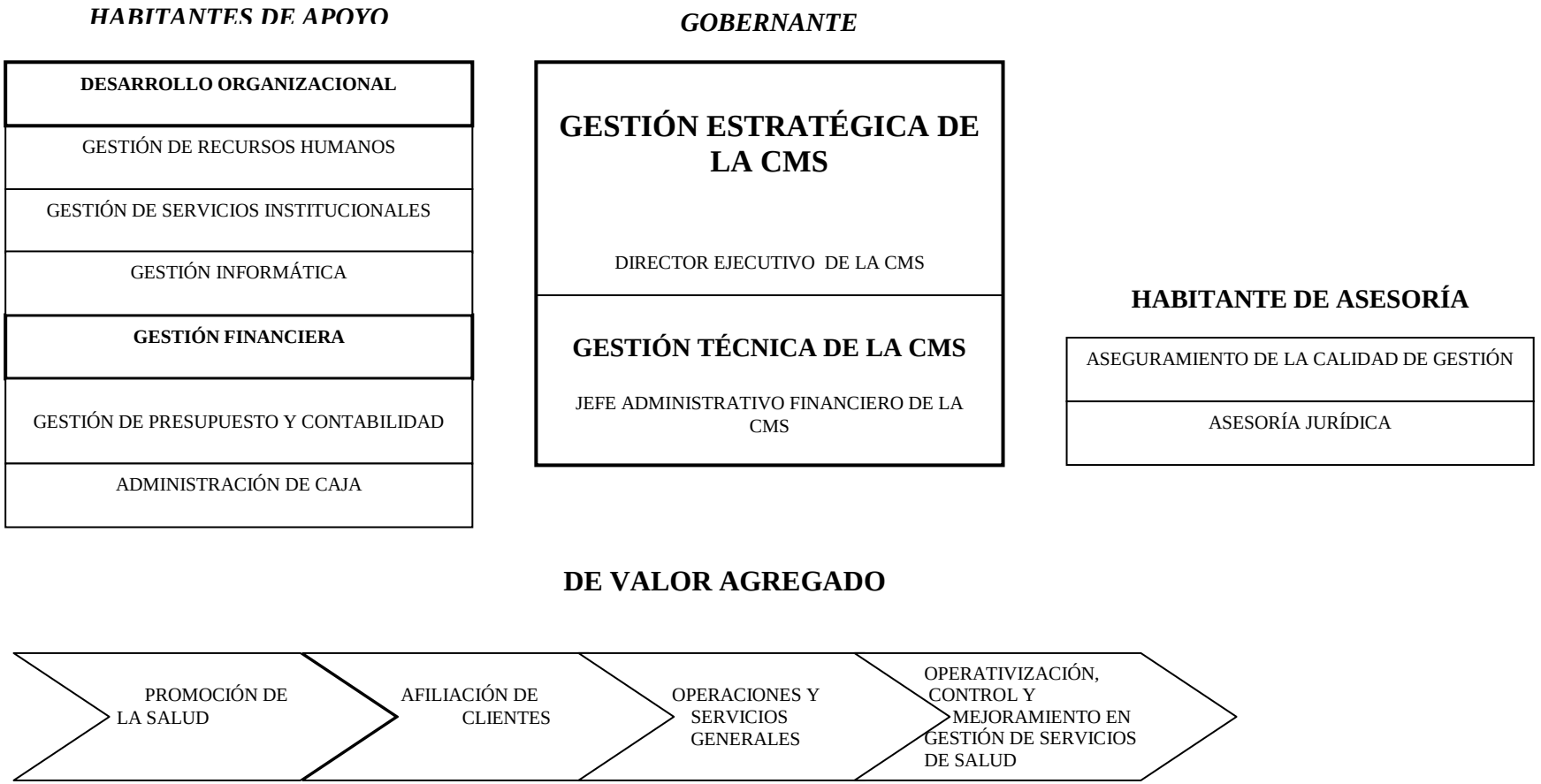

Figura 3.3 Estructura Organizacional por Procesos de la CMS.

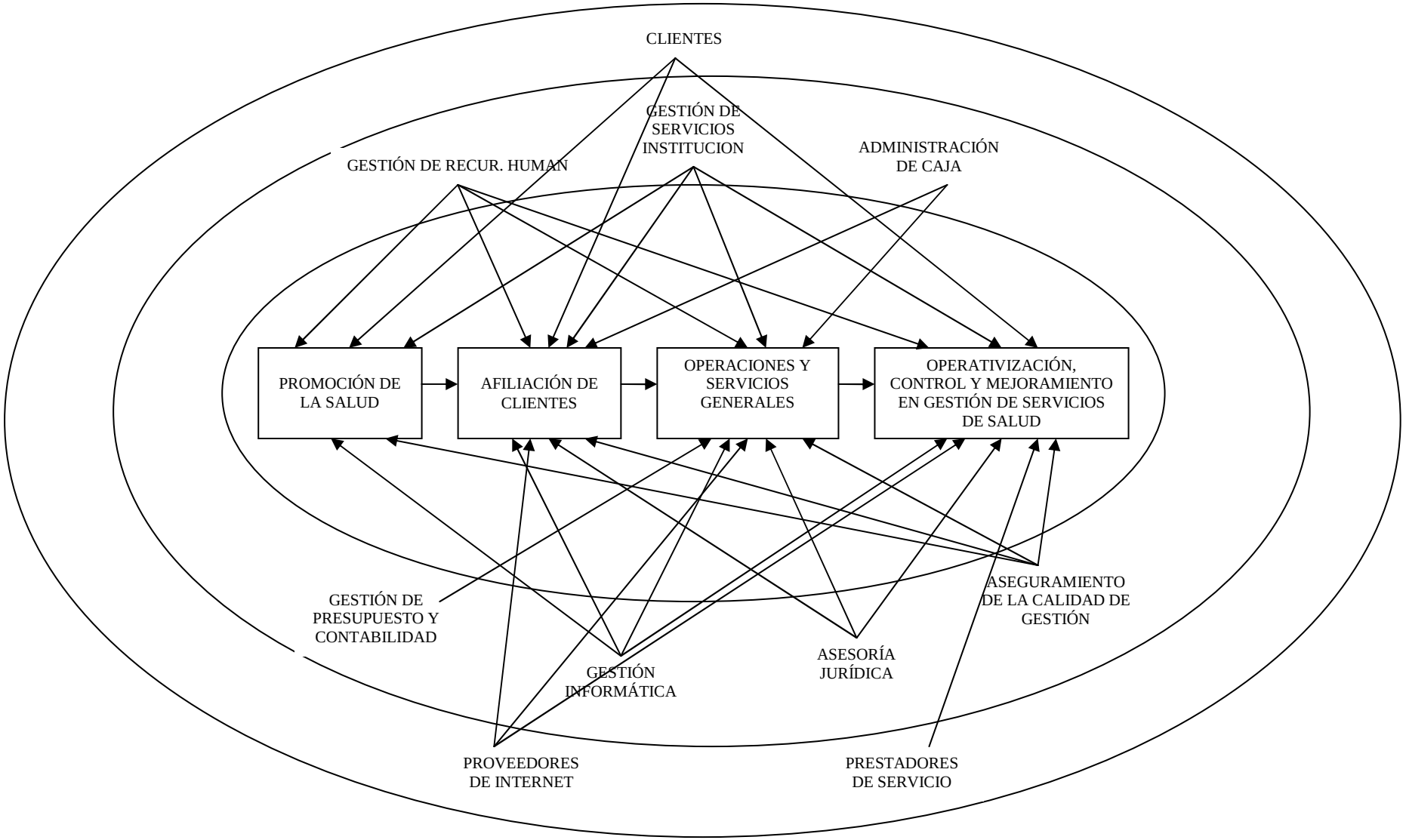

Figura 3.4 Método de Eclipses para los procesos de la CMS

3.3. IDENTIFICACIÓN, ANÁLISIS Y EVALUACIÓN DE VULNERABILIDADES EN LA INTRANET CORPORATIVA

Previa la identificación, análisis y evaluación de vulnerabilidades es necesario realizar una revisión de varias metodologías de riesgos para seleccionar la más adecuada acorde la realidad de la empresa y de esta manera analizar las vulnerabilidades actualmente presentes en la Corporación. A continuación se detallan algunas metodologías:

3.3.1. METODOLOGÍA DE RIESGOS

Hay varios métodos para realizar el análisis de riesgos, cada método tiene sus propias características, así como sus ventajas y desventajas. Es necesario comprender los diferentes métodos y sus ventajas y desventajas para seleccionar un método de análisis de riesgos que se ajuste a las características de la empresa.

- ISO 13335-1:2004
- ISO73
- AS 4360 (Australia)
- NIST SO 800-30 (USA)
- MAGERIT 2.0 (España)
- EBIOS (Francia)
- OCTAVE (Cert)
- GMITS

A continuación realizamos una breve descripción de algunos de estos métodos:

MAGERIT

MAGERIT es la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas promovida por el Consejo Superior de Informática. MAGERIT define los procedimientos para guiar a la

Administración paso a paso en el establecimiento de la protección necesaria y como respuesta a su dependencia creciente respecto de las técnicas electrónicas, informáticas y telemáticas. Los objetivos:

• Analizar los riesgos que soporta un determinado sistema de información y el entorno asociable con él, entendiendo por riesgo la posibilidad de que suceda un daño o perjuicio. El análisis de riesgos permite identificar las amenazas que acechan a los distintos componentes pertenecientes o relacionados con el sistema de información (conocidos como "activos"), para determinar la vulnerabilidad del sistema ante esas amenazas y para estimar el impacto o grado de perjuicio que una seguridad insuficiente puede tener para la organización. Se obtiene así una medida del riesgo que corre el sistema analizado.

• Recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos investigados, mediante la gestión de riesgos.

EBIOS (Francia)

Es una herramienta de gestión de los riesgos, el método EBIOS permite apreciar y tratar los riesgos relativos a la seguridad de los sistemas de información (SSI).
Posibilita también la comunicación dentro del organismo y también con los asociados para contribuir al proceso de la gestión de los riesgos SSI.
También se considera una herramienta de negociación y de arbitraje brindando las justificaciones necesarias para la toma de decisiones (descripciones precisas, retos estratégicos, riesgos detallados con su impacto en el organismo, objetivos y requerimientos de seguridad explícitos).
Una herramienta de concienciación
EBIOS permite concienciar a las partes involucradas en un proyecto (dirección general, financiera, jurídica o recursos humanos, diseñador del proyecto,

director del proyecto, usuarios), implicar a los actores del sistema de información y uniformizar el vocabulario.

OCTAVE (Cert)

Un equipo pequeño de personas del área operacional y el departamento de tecnologías de la información deberán trabajar juntos para dirigir las necesidades de seguridad de la organización. El equipo utiliza el conocimiento de muchos empleados para definir el estado actual de seguridad, identificación de riesgos para los activos críticos, y el conjunto de estrategias de seguridad.

OCTAVE es diferente de las valoraciones tecnológicas. Enfocada en el riesgo organizacional y estratégico, riesgos operacionales balanceados, prácticas de seguridad y tecnología.

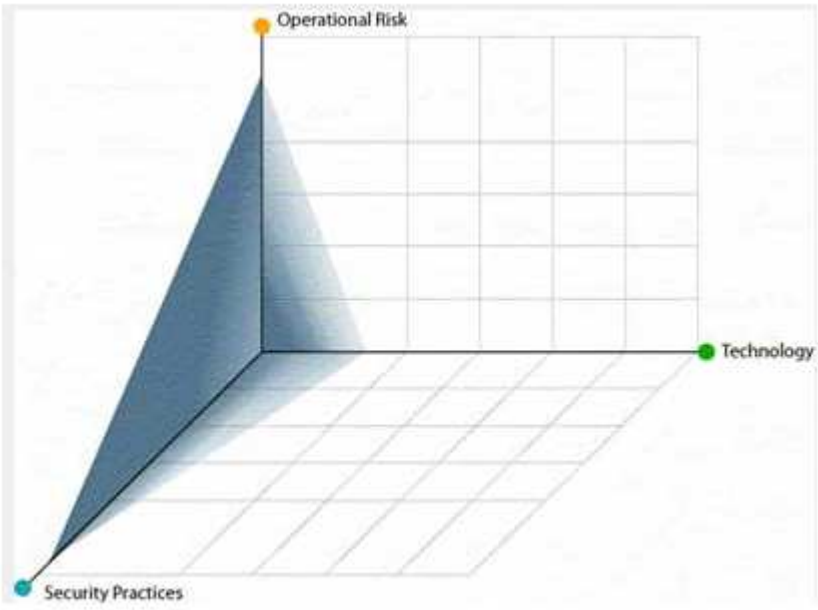

Figura 3.5 Método de Octave

Como se ilustra en la figura 3.5, OCTAVE es manejada por riesgos operacionales y prácticas de seguridad. La tecnología es examinada solo en relación con prácticas de seguridad.

El criterio de OCTAVE define un estándar para el manejo de riesgos, valoración y evaluación de seguridad de información. Actualmente hay dos métodos reconocidos:

- Método OCTAVE- para grandes organizaciones
- OCTAVE-S- para medianas organizaciones

GUIAS PARA LA ADMINISTRACIÓN DE SEGURIDAD DE IT

De acuerdo a las Guías para la administración de seguridad IT (GMITS), se consideran los siguientes métodos para la valoración de riesgos:

1) Acercamiento Básico
2) Análisis de riesgo detallado
3) Acercamiento combinado
4) Acercamiento informal

Acercamiento Básico

La seguridad es manejada sin una valoración de riesgos, se refiere al criterio de seguridad de información general y estándares y guías usadas en una específica empresa.

Características

En vista de que este método es fácil, este puede reducir el tiempo y costo requerido para la valoración de riesgos. Sin embargo, las guías no pueden satisfacer a todas las empresas.

La seguridad es tratada de la misma manera a través de la organización. Este método emplea controles que pueden ser llevados a cabo, permitiendo a la organización reforzar su manejo de seguridad para evitar que se pase por alto los riesgos.

En este procedimiento, los dos siguientes procedimientos son llevados a cabo:

Análisis de riesgo detallado

Los riesgos son evaluados en términos de posibles efectos, amenazas y vulnerabilidades causan la pérdida de confidencialidad, integridad o disponibilidad de los activos de información.

Características

Debido a que en hace en lo posible un correcto análisis de riesgos, este método puede ser usado para seleccionar apropiados controles basados en el riesgo. Sin embargo, la valoración de riesgos toma tiempo y es costoso.

Acercamiento combinado

Generalmente, este método combina el acercamiento básico y el análisis de riesgo detallado.

Características

Este método compensa las ventajas y desventajas de los otros dos métodos. Sin embargo, si los activos importantes no son propiamente identificados, este método pierde sus ventajas.

Acercamiento informal

Este método involucra un análisis de riesgos basados en la experiencia o en la decisión de la persona responsable.

Características

La desventaja de este método radica en el análisis de riesgos sin aprender nuevas técnicas. Sin embargo, es posible que se cometan errores, o se pasarán por alto procedimientos, en vista de que no hay ninguna estructura.

3.3.2. ELECCCIÓN DEL MÉTODO DE ANÁLISIS DE RIESGOS

Para el análisis de riesgos se optó por las: “Guías para la administración de seguridad de IT” con un análisis detallado, ya que este método nos ayuda a

cumplir con nuestro objetivo que es seleccionar controles adecuados basados en los riesgos encontrados, es decir este método se ajusta a los requerimientos de la norma ISO 27001.

3.3.3. ESCALA DE VALORACIÓN DE RIESGOS

A continuación se explicará las escalas utilizadas para la valoración del riesgo, el umbral de tolerancia del riesgo y el criterio para este umbral. Para la valoración de riesgos se identificará y evaluará a los activos basados en las necesidades de la organización. Una organización debería determinar un criterio para la determinación de los tres elementos (confidencialidad, integridad, disponibilidad).

Activos de información (Confidencialidad)	Clase	Descripción
1	Pública	Puede ser revelado y proporcionado a terceras partes. Si el contenido fuera revelado, hubiera pequeños efectos en las operaciones de la CMS.
2	Uso interno	Puede solo ser revelada y proporcionado en la CMS (no disponible a terceras partes). Si el contenido fuera revelado, no hubiera mucho efecto en las operaciones de la CMS
3	Secreto	Puede ser solo revelado y proporcionado a partes específicas y departamentos. Si el contenido fuera revelado, hubiera un gran efecto en las operaciones de la CMS
4	Alta confidencialidad	Puede ser solo revelado y proporcionado a partes específicas. Si el contenido fuera revelado, hubiera un efecto irrecuperable en las operaciones de la CMS.

Tabla 3.12 Estándares para confidencialidad

Activos de información (Integridad)	Clase	Descripción
1	No necesaria	Usado solo para consulta. No tiene posibles problemas
2	Necesaria	Si el contenido fuera falsificado, hubiera problemas, pero estos no afectarían mucho las operaciones de la CMS
3	importante	Si la integridad se perdiera, hubiera un efecto fatal en las operaciones de la CMS

Tabla 3.13. Estándares para integridad

Activos de información (Disponibilidad)	Clase	Descripción
1	Bajo	Si la información no llegara a estar disponible, no hubiera efectos en las operaciones de la CMS
2	Mediano	Si la información no llegara a estar disponible, hubiera algún efecto en las operaciones de la CMS. Sin embargo, métodos alternativos pudieran ser usados para las operaciones, o los procesos podrían ser demorados hasta que la información esté disponible
3	Alto	Si la información no estuviera disponible cuando sea necesitada en algún momento, hubiera un fatal efecto en las operaciones de la CMS.

Tabla 3.14. Estándares para disponibilidad

La frecuencia de ocurrencia de las amenazas debe ser evaluada. A partir de la lista de amenazas, las amenazas deben ser revisadas basadas en la experiencia de operaciones y datos estadísticos que han sido ya coleccionados.

Las amenazas son típicamente divididas en tres categorías: “Baja”,”Media”,”Alta”.

Amenazas		
Probabilidad de ocurrencia	**Categoría**	**Descripción**
1	Bajo	Hay una baja probabilidad. La frecuencia de ocurrencia es una vez al año o menos.
2	Medio	Hay una moderada probabilidad. La frecuencia de ocurrencia es una vez cada medio año o menos.
3	Alto	Hay una alta probabilidad. La frecuencia de ocurrencia es una vez al mes o más.

Tabla 3.15. Criterios para determinar las categorías de las amenazas

Vulnerabilidades		
Probabilidad de ocurrencia	**Categoría**	**Descripción**
1	Bajo	Se tiene controles de seguridad muy débiles o no se tiene ningún control de seguridad, de tal manera que esta vulnerabilidad es susceptible de ser explotada fácilmente
2	Medio	Hay un moderado control de seguridad
3	Alto	Si en el activo se tiene los controles de seguridad adecuados, de tal manera que sea muy difícil explotar esta vulnerabilidad

Tabla 3.16. Criterios para determinar las categorías de las vulnerabilidades

3.3.4. IDENTIFICACIÓN DE ACTIVOS

Para la identificación de los activos se utilizaron los datos proporcionados por el administrador de la red, y para facilitar el análisis y gestión de riesgos se han dividido los activos en cinco categorías de información, a continuación se detalla cada una de las cinco categorías:

3.3.4.1. Activos de información

Documentación y Registros	
Descripción	Soporte estático no electrónico que contiene datos.
Activos	Actas Documentación de procesos (POA: Plan Operativo Anual) Contratos con los clientes Contratos con los proveedores de servicio médico Facturas Memos Oficios Reglamento del SRI Papel Tarjetas de Afiliación

Activos Auxiliares	
Descripción	Otros dispositivos que ayudan al funcionamiento de la organización
Activos	Suministros de oficina

Activos Intangibles	
Descripción	Activos que representan el buen nombre de la empresa y la imagen que los clientes tienen de ella.
Activos	Imagen y Reputación de la empresa

3.3.4.2. Software

Sistemas Operativos	
Descripción	Esta denominación comprende todos los programas de una computadora que constituyen la base operativa sobre la cual se ejecutarán todos los otros programas (servicios o aplicaciones). Incluye un núcleo y funciones o servicios básicos. Dependiendo de su arquitectura, un sistema operativo puede ser monolítico o puede estar formado por un micronúcleo y un conjunto de módulos del sistema. El sistema operativo abarca principalmente todos los servicios de gestión del hardware (CPU, memoria, discos, periféricos e interfaces redes), los servicios de gestión de tareas o procesos y los servicios de gestión de usuarios y de sus derechos. Windows Server 2003 Enterprise Edition Linux CentOs 4.2 Linux version 2.6 Windows XP Profesional SP 2

Paquete de programas o software estándar	
Descripción	El software estándar o paquete de programas es un producto comercializado como tal (y no como desarrollo único o específico) con soporte, versión y mantenimiento. Presta un servicio « genérico » a los usuarios y a las aplicaciones pero no es personalizado o específico como la aplicación profesional.
Activos	Antivirus Symantec Cliente. Software de contabilidad Software de atención al cliente, Microsoft Visio Nero Suite Microsoft Visual Estudio Microsoft Project Adobe Illustrator

Software de Aplicación de Oficina	
Descripción	Datos y servicios informáticos compartidos y privados, que utilizan los protocolos y tecnologías de comunicación (por ejemplo, tecnología de Internet).
Activos	Aplicación Oracle para acceso a la información de usuarios

3.3.4.3. Activos Físicos

Hardware Portátil	
Descripción	Hardware informático diseñado para poder ser transportado manualmente con el fin de utilizarlo en lugares diferentes.
Activos	Portátil
PC's de Oficina	
Descripción	Hardware informático que pertenece al organismo o que es utilizado en los locales del organismo.
Activos	Estaciones de trabajo.

Equipos de Oficina	
Descripción	Hardware para la recepción, la transmisión o la emisión de datos.
Activos	Impresoras, Copiadoras, Teléfonos, Fax

Servidores	
Descripción	Hardware informático que pertenece al organismo y maneja información importante de la empresa y clientes.
Activos	Servidor de Base de datos Servidor de Correo electrónico Servidor de Dominio Servidor IAS (Internet Access Server)

Soporte electrónico	
Descripción	Soporte informático conectado a una computadora o a una red informática para el almacenamiento de datos. Susceptible de almacenar un gran volumen de datos sin modificar su pequeño tamaño. Se utiliza a partir de equipo informático estándar.
Activos	Disquete, CD-ROM, disco duro extraíble, memoria extraíble

Medios de comunicación	
Descripción	Los medios o soportes de comunicación y telecomunicación pueden caracterizarse principalmente por las características físicas y técnicas del soporte (punto a punto, difusión) y por los protocolos de comunicación (enlace o red – capas 2 y 3 del modelo OSI de 7 capas).

Activos	Cableado Estructurado, tecnología Ethernet, cables, Switch, MODEM.

Establecimiento	
Descripción	El tipo establecimiento está formado por el conjunto de lugares que contienen todo o parte del sistema y los medios físicos necesarios para su funcionamiento.
Activos	Edificio, oficinas, zona de acceso reservado, zona protegida

3.3.4.4. Servicios

Comunicación	
Descripción	Servicios y equipo de telecomunicaciones brindados por un prestador.
Activos	Línea telefónica, central telefónica, redes telefónicas internas.

Energía	
Descripción	Servicios y medios (fuentes de energía y cableado) necesarios para la alimentación eléctrica del hardware y los periféricos.
Activos	Entrada de la red eléctrica.

Correo Electrónico	
Descripción	Dispositivo que permite, a los usuarios habilitados, el ingreso, la consulta diferida y la transmisión de documentos informáticos o de mensajes electrónicos, a partir de computadoras conectadas en red.
Activos	Correo electrónico interno, correo electrónico vía web.

Portal Externo	
Descripción	Un portal externo es un punto de acceso que encontrará o utilizará un usuario cuando busque información o un servicio del organismo. Los portales brindan un gran abanico de recursos y de servicios.
Activos	Portal de información (Página Web de la empresa)

3.3.4.5. Personas

Empleados	
Descripción	Es el personal que manipula elementos delicados en el marco de su actividad y que tiene una responsabilidad particular en ese tema. Puede disponer de privilegios particulares de acceso al sistema de información para cumplir con sus tareas cotidianas.
Activos	Dirección de Recursos Humanos, Dirección Financiera, Administrador del Sistema, Dirección General

3.3.5. IDENTIFICACIÓN DE REQUERIMIENTOS

Se identificará los requerimientos de los activos de la CMS en base a los objetivos del negocio, aspectos legales para de esta manera identificar las

obligaciones del SGSI. Los requerimientos están determinados con respecto a: Confidencialidad (C), Disponibilidad (D) e Integridad (I)

ACTIVOS DE INFORMACIÓN

Los requerimientos de seguridad de la información deberían están enfocados en base a la Confidencialidad, Disponibilidad e Integridad.

- La información no debería ser vista por personal no autorizado (C)
- La información puede ser modificada únicamente por personal autorizado (I)
- La información debería estar disponible en cualquier momento (D)

SOFTWARE

Si el Software es comercial la confidencialidad no aplica, para software propietario de la organización existe el requerimiento de confidencialidad.

- Las aplicaciones no deberían ser utilizadas por personal no autorizado. (C)
- El software puede ser modificado únicamente por personal autorizado (I)
- El software, en especial aplicaciones deberían estar disponibles al menos durante la jornada laboral (D)

ACTIVOS FÍSICOS

Para los activos físicos se debe enfocar los requerimientos de hardware, no en la información que procesen, que transmitan o almacenen.

- Los cambios en el Hardware deben ser realizados únicamente por personal autorizado (I)
- El Hardware debe ser accesible por el personal autorizado al menos durante la jornada laboral (D)

SERVICIOS

Los servicios agrupan información, software y activos físicos, se deben especificar los requerimientos en base a los aspectos más importantes.

- Los servicios deberían ser consistentes y completos (I)
- Los servicios deberían estar disponibles cuando ser requiera (D)

Típicamente la confidencialidad no aplica a servicios, sin embargo depende de la naturaleza del servicio.

PERSONAS

Para las personas los requerimientos únicamente se enfocan en la disponibilidad de las personas. Por ejemplo:

- El administrador del sistema debe proveer el funcionamiento correcto de los servicios de la red y sistemas (Disponibilidad del personal)

3.3.6. VALORACIÓN DE LOS ACTIVOS

El objetivo es identificar la valoración de todos los activos dentro del alcance del SGSI, indicando que impacto puede sufrir el negocio con la pérdida de Confidencialidad, Integridad, Disponibilidad.

Para obtener esta valoración, se realizaron conversaciones con el personal encargado de cada proceso; que conocen la importancia de cada activo dentro de la empresa, para así determinar los niveles de Confidencialidad, Integridad y Disponibilidad requeridos para cada proceso, que permitan cumplir con las operaciones del negocio.

Tabla 3.17. Valoración de Activos

ACTIVOS	ELEMENTOS DE INFORMACIÓN	VALOR	RAZÓN
Hardware Portátil	Confidencialidad	3	La información almacenada debe ser vista únicamente por el personal autorizado.
	Integridad	3	Es necesaria la integridad de la información almacenada, en especial cuando es la de clientes
	Disponibilidad	2	Para que los empleados puedan trabajar adecuadamente necesitan acceder a la información, sin embargo pueden recurrir a documentos o servidores donde contengan información
PCs de oficina	Confidencialidad	3	La información almacenada debe ser vista únicamente por el personal autorizado.
	Integridad	3	Es necesaria la integridad de la información almacenada, en especial cuando es la de clientes
	Disponibilidad	2	Para que los empleados puedan trabajar adecuadamente necesitan acceder a la información, sin embargo pueden recurrir a documentos o servidores donde contengan información

Servidores	Confidencialidad	4	Solo personal específico debe acceder a la información de los servidores debido a que manejan información clientes, proveedores, empleados de la compañía. Para que no la puedan modificar.
	Integridad	3	Es necesario asegurar que la información de los servidores no sea alterada ni modificada sin autorización, para que no se perjudique el negocio
	Disponibilidad	3	Es indispensable que los servidores estén accesibles al menos el 100% en las horas laborables, para no afectar a los clientes, proveedores, inclusive empleados.
Equipos de Oficina	Confidencialidad	2	Información de negocio que se imprima o se fotocopie necesita confidencialidad.
	Integridad	2	Se necesita los equipos de oficina(impresora), pero si eventualmente falla se puede seguir trabajando
	Disponibilidad	2	Si bien son necesarios los equipos, se puede trabajar aunque no estén disponibles
Soporte electrónico	Confidencialidad	2	Cuando se tenga información de negocio almacenada en estos equipos es necesario su protección
	Integridad	1	Es un medio temporal para almacenar información
	Disponibilidad	1	No es requerido, cuando la información es redundante
Documentación y Registros	Confidencialidad	3	Debido a que la documentación maneja información de clientes, proveedores y empleados es necesaria que pueda ser vista por personal autorizado para que no sea modificada.
	Integridad	3	Es necesario que la documentación no sea alterada, ni se produzca pérdidas de la misma debido a que son el único respaldo físico de contratos, procedimientos, etc.
	Disponibilidad	2	Se debe acceder a la información en cualquier momento que sea requerido
Empleados	Confidencialidad	2	Cierta información debe ser manejada al interior de la empresa por lo cual no debe ser divulgada
	Integridad	1	No hay aspectos de integridad relacionados con los empleados
	Disponibilidad	2	Los empleados deben estar disponibles para resolver posibles problemas que se presenten
Establecimiento	Confidencialidad	1	Es un edificio público
	Integridad	3	Se debe proteger la integridad física del edificio Matriz donde se encuentran los servidores
	Disponibilidad	1	Si no pueden acceder al edificio, se puede acceder remotamente a la aplicación del sistema
	Confidencialidad	2	Se debe proteger que las líneas no sean interceptadas para que no se escuchen conversaciones de negocio.

Servicio de Comunicaciones	Integridad	2	Se necesita que los servicios de comunicaciones funcionen adecuadamente
	Disponibilidad	3	Se requiere que estén disponibles, debido a que son necesarias para la comunicación con los proveedores, clientes, reclamos, etc.
Servicio de energía eléctrica .	Confidencialidad	1	La entrada de la red eléctrica no requiere confidencialidad
	Integridad	2	La entrada de la red eléctrica no debe sufrir de manipulaciones
	Disponibilidad	3	Para que las operaciones de la empresa sean desarrolladas es importante que esté en funcionamiento la mayor parte del tiempo la entrada de la red eléctrica
Servicio de correo electrónico	Confidencialidad	4	Debe tener confidencialidad porque probablemente esté viajando información de la CMS que debe manejar solo ciertos departamentos y especialmente si la información viaja por una red pública
	Integridad	2	Los datos no deben ser modificados, pero en el caso que se pierda la integridad al utilizar el servicio de correo electrónico, los datos originales podrán ser recuperados
	Disponibilidad	2	El correo electrónico debe estar disponible en horas de trabajo, pero en el caso de que no esté disponible, existen otros métodos que ayudan a solucionar este problema , como servicio de fax, hiperterminal, teléfono, etc.
Aplicación Oracle para acceso a la información del servicio	Confidencialidad	4	Alta confidencialidad porque maneja información personal de los usuarios
	Integridad	3	La aplicación debe mantener la integridad para evitar modificaciones en la información de los clientes.
	Disponibilidad	2	Es importante tener siempre disponible la información de los usuarios, pero si no estuviera disponible en este momento y se la obtuviera después, no afecta críticamente las operaciones de la CMS
Portal de información (Página Web de la empresa)	Confidencialidad	1	El sitio Web debe ser accesible por cualquier persona, en cualquier momento
	Integridad	3	La información presentada en el sitio Web debe ser correcta
	Disponibilidad	3	El sitio Web debe estar disponible a los clientes
Suministros de oficina	Confidencialidad	1	Es el equipamiento de oficina estándar, no se requiere confidencialidad
	Integridad	2	El equipo de oficina debe trabajar confiablemente, es usado para procesar los registro s de los clientes. Cualquier error puede ser reconocido cuando se observa la salida.
	Disponibilidad	1	Los suministro s de oficina durante las horas normal de trabajo, no causa mayor problema si alguna pieza falla, ya que hay impresoras, teléfonos, etc

Imagen de la empresa Reputación	Confidencialidad	1	La confidencialidad no es aplicada en la imagen y reputación de la empresa
	Integridad	1	La integridad no es aplicada en la imagen y reputación de la empresa
	Disponibilidad	1	La disponibilidad no es aplicada en la imagen y reputación de la empresa
Paquetes o software estándar	Confidencialidad	1	Este es un software estándar el cual no es confidencial para todos
	Integridad	2	El software debe funcionar correctamente
	Disponibilidad	2	El software debe estar disponible durante horas de trabajo, pero si hay un problema con un PC, otro PC puede ser usado
Sistemas operativos	Confidencialidad	4	Los datos de los clientes, que es información personal es procesada en el servidor, razón por la cual estos datos deber ser adecuadamente protegidos
	Integridad	3	Los datos de los clientes, que es información personal es procesada en el servidor, estos datos deben ser correctos
	Disponibilidad	3	La continua disponibilidad del servidor es necesaria para un exitoso desempeño de la organización
Medios y Soporte	Confidencialidad	1	El cableado estructurado no requiere confidencialidad
	Integridad	3	El cableado estructurado debe funcionar bien, ya que es parte de la red de la empresa
	Disponibilidad	3	Siempre debe estar disponible ya que probablemente cause la interrupción de actividades propias de la Organización

3.3.7. IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES

El objetivo es identificar las amenazas que pueden a las que se exponen los activos dentro del alcance del SGSI y las vulnerabilidades que pueden ser explotadas por las amenazas. A continuación detallamos las amenazas principales clasificadas acorde al origen de la misma.

1.- Desastres Naturales.- Sucesos que pueden ocurrir sin intervención humana	
Amenaza: Fuego Daños por agua Desastres Naturales	**Activos:** Activos Físicos Servicios de Comunicación, Energía Documentación y Registros
Afecta: Disponibilidad del Servicio, Integridad, Trazabilidad del servicio, Trazabilidad de los datos	

2.- De origen industrial.- Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.	
Amenaza: Corte de suministro eléctrico Degradación en el HW Condiciones inadecuadas de temperatura y /o humedad	**Activo:** Activos Físicos Servicios de Comunicación, Energía Documentación y Registros
Afecta: Disponibilidad, Confidencialidad, Integridad, Trazabilidad del servicio, Trazabilidad de los datos, Funcionamiento y Procesamiento correcto de datos.	

3.- Errores y Fallos no intencionados.- Fallos no intencionales causados por las personas.	
Amenaza: Errores de los usuarios Errores de Administración Errores de Configuración Escapes de Información Alteración de información Degradación de información Introducción de Información incorrecta Divulgación de información Errores de actualización Indisponibilidad del personal Incumplimiento con la legislación Corrupción de archivos de registros Brechas de seguridad no detectadas Virus de Computación, Fuerza Bruta y ataques de diccionario	Activo: Activos Físicos Servicios de Comunicación, Energía Documentación y Registros. Software
Afecta: Disponibilidad del Servicio, Confidencialidad, Integridad, Autenticidad de los usuarios del servicio, Autenticidad del origen de datos, Cumplimiento con regulaciones de seguridad, Trazabilidad del servicio, Trazabilidad de los datos	

4.- Ataques intencionados.- Fallos deliberados causados por las personas.	
Amenaza: Instalación no autorizada o cambios de SW Manipulación de la configuración Brechas de seguridad no detectadas Suplantación de la identidad del usuario. Uso no previsto	**Activo:** Activos Físicos Servicios de Comunicación, Energía Documentación y Registros. Software

Abuso de privilegios de acceso Acceso no autorizado Análisis de Tráfico Negación de Servicio Robo Ataque Destructivo Ingeniería Social Inautorizada copia de SW o información Virus de Computación, Fuerza Bruta y ataques de diccionario	
Afecta: Disponibilidad del Servicio, Confidencialidad, Integridad, Autenticidad de los usuarios del servicio, Autenticidad del origen de datos, Cumplimiento con regulaciones de seguridad, Trazabilidad del servicio, Trazabilidad de los datos, Plan de Contingencia	

En la siguiente tabla se detallan las vulnerabilidades que se presentan en cada uno de los activos, y las amenazas que pueden explotar dichas vulnerabilidades.

Tabla 3.18 Amenazas y Vulnerabilidades

ACTIVOS	AMENAZAS	VULNERABILIDADES
Hardware Portátil	Fuego	Falta de protección contra fuego
	Daños por agua	Falta de protección física adecuada
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres
	Acceso no autorizado a la portátil	Falta de Protección por desatención de equipos
	Corte de suministro eléctrico o Falla en el aire acondicionado	Funcionamiento no confiable del UPS o funcionamiento no adecuado del aire acondicionado
	Instalación no autorizada o cambios de Software	Falta de control de acceso
	Incumplimiento con la legislación	Falta de conocimiento de protección de derechos de SW por parte de los empleados
	Uso no previsto	Falta de políticas
	Incumplimiento con controles de seguridad	Falta de conocimiento de seguridad por parte del personal
	Degradación del HW	Falta de mantenimiento adecuado
	Inautorizada copia de SW o información propietaria	Falta de políticas
	Ataque destructivo	Falta de protección física
	Robo	Falta de protección física adecuada
	Fuego	Falta de protección contra fuego
	Daños por agua	Falta de protección física adecuada
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados

PCs de oficina		por desastres
	Acceso no autorizado a las PCs de oficina	Falta de Protección por desatención de equipos
	Corte de suministro eléctrico o Falla en el aire acondicionado	Funcionamiento no confiable del UPS o funcionamiento no adecuado del aire acondicionado
	Instalación no autorizada o cambios de Software	Falta de control de acceso
	Incumplimiento con la legislación	Falta de conocimiento de protección de derechos de SW por parte de los empleados
	Uso no previsto	Falta de políticas
	Incumplimiento con controles de seguridad	Falta de conocimiento de seguridad por parte del personal
	Degradación del HW	Falta de mantenimiento adecuado
	Inautorizada copia de SW o información propietaria	Falta de políticas
	Ataque destructivo	Falta de protección física
	Robo	Falta de protección física adecuada
Servidores	Fuego	Falta de protección contra fuego
	Daños por agua	Falta de protección física adecuada
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres
	Corrupción de archivos de registros	Falta de Protección de los archivos de registro
	Negación de Servicio	Incapacidad de distinguir una petición real de una falsa
	Corte de suministro eléctrico o Falla en el aire acondicionado	Funcionamiento no confiable del UPS o funcionamiento no adecuado del aire acondicionado
	Acceso no autorizado a través de la red	Código malicioso desconocido
	Degradación o Falla del HW	Falta de mantenimiento adecuado
	Manipulación de la configuración	Falta de control de acceso
	Incumplimiento con controles de seguridad	Falta de conocimiento de seguridad por parte del personal
	Incapacidad de restauración	Falta de planes de continuidad del negocio
	Análisis de tráfico	Falta de establecimiento de una conexión segura (VPN)
	Brechas de seguridad no detectadas	Falta de monitoreo de los servidores
	Ataque destructivo	Falta de protección física
Equipos de Oficina	Fuego	Falta de protección contra fuego
	Daños por agua	Falta de protección física adecuada
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres
	Degradación o Falla de HW	Falta de Mantenimiento
	Ataque destructivo	Falta de protección física
	Uso no previsto	Falta de políticas Falta de control de acceso
Soporte electrónico	Fuego	Falta de protección contra fuego
	Daños por agua	Falta de protección física adecuada
	Desastres naturales	Condiciones locales donde los

		recursos son fácilmente afectados por desastres
	Condiciones inadecuadas de temperatura y/o humedad	Susceptibidad al calor y humedad
	Ataque destructivo	Falta de protección física
	Robo	Falta de atención del personal
Documentación y Registros.	Fuego	Falta de protección contra fuego
	Daños por agua	Falta de protección física adecuada
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres
	Pérdida de información	Errores de los empleados Almacenamiento no protegido
	Divulgación de información de clientes	Almacenamiento no protegido
	Incumplimiento de leyes en cuanto a la información de clientes o empleados	Falta de conocimiento de los empleados
	Incorrecta o incompleta documentación del sistema	Falta de documentación actualizada del sistema
	Contratos incompletos	Falta de control para el establecimiento de contratos
	Ataque destructivo	Falta de protección física
	Incapacidad de restauración	Falta de planes de continuidad del negocio
	Modificación no autorizada de información	Insuficiente entrenamiento de empleados
Empleados	Errores de los empleados y acciones equivocadas	Falta de conocimiento y oportuno entrenamiento
	Insuficiente personal	Falta de acuerdos definidos para reemplazo de empleados
	Divulgación de información confidencial	Falta de acuerdos de confidencialidad
Establecimientos	Fuego	Falta de protección contra fuego
	Daños por agua	Falta de protección física adecuada
	Acceso no autorizado	Falta de políticas Falta de protección física
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres
Servicio de Comunicaciones	Fuego	Falta de protección contra fuego
	Daños por agua	Falta de protección física adecuada
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres
	Degradación del servicio y equipos	Falta de mantenimiento adecuado
	Errores de configuración	Falta de conocimiento del administrador
	Manipulación de la configuración	Falta de control de acceso
	Uso no previsto	Falta de políticas
	Ataque destructivo	Falta de protección física
	Fallas de servicios de telefonía	Falta de acuerdos bien definidos con terceras partes
	Fuego	Falta de protección contra fuego

Servicio de energía eléctrica	Daños por agua	Falta de protección física adecuada
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres
	Ataque destructivo	Falta de protección física
Servicio de correo electrónico	Errores de los usuarios	Falta de conocimiento del uso del servicio
	Suplantación de la identidad del usuario	Falta de control de acceso
	Análisis de tráfico	Falta de establecimiento de una conexión segura (VPN)
	Uso no previsto	Falta de políticas
	Fallas de servicios de soporte (telefonía, servicios de Internet)	Falta de acuerdos bien definidos con terceras partes
Aplicación Oracle para acceso a la información de usuarios	Errores de los usuarios	Falta de conocimiento del uso de la aplicación
	Errores de configuración	Falta de capacitación del administrador del sistema
	Escapes de información	Falta de control de acceso
	Errores de actualización del programa	Falta de procedimientos aprobados
	Manipulación de la configuración	Falta de control de acceso
	Suplantación de identidad del usuario	Falta de control de Acceso
	Abuso de privilegios de acceso	Falta de políticas de seguridad
	Negación de servicio	Incapacidad para distinguir una petición real de una petición falsificada
Portal de información (Página Web de la empresa)	Modificación no autorizada del sitio Web	Falta de procedimientos para cambios
	Negación de servicio	Falta de recursos necesarios
	Sitio Web no disponible	Fallas en los acuerdos de niveles de servicio
	Publicación de información incorrecta de la CMS	Falta de procedimiento aprobados
Suministros de Oficina	Fuego	Falta de protección contra fuego
	Daños por agua	Falta de protección física adecuada
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres
	Robo	Falta de atención Falta de protección física
Imagen de la empresa Reputación	Divulgación de datos de los clientes	Insuficiente seguridad de información de los clientes
Paquetes o software estándar	Negación de Servicio	Capacidad insuficiente de los recursos
	Virus de Computación, Fuerza Bruta y ataques de diccionario	Falta de Protección(AV) actualizada
	Spoofing, Escape de información	Falta de control de acceso
	Falta de capacidad de restauración	Falta de copias backup continuas

	Uso no previsto	Falta de políticas de seguridad
Sistemas operativos	Negación de Servicio	Capacidad insuficiente de los recursos
	Errores de Configuración del servicio	Falta de capacitación del administrador Incompleto o incorrecto documentación del sistema
	Virus de Computación, Fuerza Bruta y ataques de diccionario	Falta de Protección (AV) actualizada
	Falta de capacidad de restauración	Falta de copias de backup continuas
	Pérdida de Servicio	Actualizaciones incorrectas Instalación de SW no autorizado
	Controles de Seguridad no cumplidos	Falta de Políticas de Seguridad
	Alteración no autorizado de la configuración	Falta de control de acceso
Medios y Soporte	Acceso no autorizado a la información	Falta de protección física
	Robo	Falta de protección física
	Daños de cables	Falta de protección física
	Análisis de tráfico	Falta de establecimiento de una conexión segura (VPN)
	Brechas de seguridad no detectadas	Falta de monitoreo de la red

3.3.8. EXPOSICIÓN DEL RIESGO

Se analizará la probabilidad de que cada amenaza y el nivel de vulnerabilidad, teniendo como resultado el nivel de exposición de riesgo de cada activo de la CMS.

Valoración:

A= probabilidad de ocurrencia de la amenaza, en base a los registros de los últimos 2 años.

V= Nivel de vulnerabilidad.

ACTIVOS	AMENAZAS	VALOR	DESCRIPCIÓN
Hardware Portátil	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector donde se encuentra la CMS
	V1: Falta de protección contra fuego	Media	Actualmente en la CMS no se tienen ninguna protección contra fuego, como extintores
	A2: Daños por agua	Baja	No se ha registrado este tipo de incidente
	V2: Falta de protección física adecuada	Baja	Las instalaciones donde se encuentran los usuarios, con los equipos portátiles no presentan penetrabilidad de agua.
	A3: Desastres naturales	Baja	No se ha registrado este tipo de incidente
	V3: Condiciones locales donde los recursos son fácilmente afectados por desastres	Media	No existen protecciones requeridas para enfrentar daños causados ante desastres naturales
	A4: Acceso no autorizado a la portátil	Media	Existen diferentes motivos para acceso al equipo sin autorización, ya sea código malicioso,
	V4: Falta de Protección por desatención de equipos	Alta	Se puede acceder fácilmente a la máquina, si no se la deja con la respectiva seguridad
	A5: Corte de suministro eléctrico o Falla en el aire acondicionado	Media	Los cortes de suministros eléctricos se presentan todos los años en el país
	V5: Funcionamiento no confiable del UPS o funcionamiento no adecuado del aire acondicionado	Media	Los portátiles no se conectan a un UPS general, únicamente cuentan con la batería
	A6: Instalación no autorizada o cambios de Software	Baja	Este problema no ha ocurrido en el último año
	V6: Falta de control de acceso	Media	Los usuarios no tienen permisos para instalar programas, pero existe la opción de que violen las seguridades de la información del administrador
	A7: Incumplimiento con la legislación	Baja	No se presentan registros
	V7: Falta de conocimiento de protección de derechos de SW por parte de los empleados	Alta	En la empresa no se tiene conocimiento de las leyes de protección de derechos de autor
	A8: Uso no previsto	Media	Es considerable el porcentaje de personas que utiliza los recursos para otras actividades diferentes del negocio
	V8: Falta de las políticas	Alta	No se encuentran definidas políticas de seguridad
	A9: Incumplimiento con	Alta	El porcentaje de fallas en la

	controles de seguridad		seguridad es alto
	V9: Falta de conocimiento de seguridad por parte del personal	Alta	No se encuentran definidas políticas de seguridad para conocimiento de los usuarios
	A10: Degradación del HW	Medio	Los equipos ya han presentado varias fallas de HW
	V10: Falta de mantenimiento adecuado	Medio	No se realiza un mantenimiento continuo de los equipos
	A11: Copia no autorizada de SW o información propietaria	Medio	Se han encontrado Cd piratas de SW con licencia.
	V11: Falta de políticas	Alta	No se encuentran definidas políticas de seguridad para conocimiento de los usuarios
	A12: Ataque destructivo	Baja	No se presentan registros de este problema
	V12: Falta de protección física	Alta	Los usuarios se llevan las portátiles, y las utilizan en medios no seguros
	A13: Robo	Media	Se tiene registrado un caso de robo de equipos
	V 13: Falta de protección física	Alta	No se tiene una adecuada protección física dentro de la CMS
PCs de oficina	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector donde se encuentra la CMS
	V1: Falta de protección contra fuego	Media	Actualmente en la CMS no se tienen ninguna protección contra fuego, como extintores
	A2: Daños por agua	Baja	No se ha registrado este tipo de incidente
	V2: Falta de protección física adecuada	Baja	Las instalaciones donde se encuentran los usuarios, con los equipos no presentan penetrabilidad de agua.
	A3: Desastres naturales	Baja	No se ha registrado este tipo de incidente
	V3: Condiciones locales donde los recursos son fácilmente afectados por desastres	Media	No existen protecciones requeridas para enfrentar daños causados ante desastres naturales
	A4: Acceso no autorizado a las PCs de oficina	Media	Existen diferentes motivos para acceso al equipo sin autorización, ya sea por curiosidad, malicia
	V4: Falta de Protección por desatención de equipos	Alta	Se puede acceder fácilmente a la máquina, si no se la deja con la respectiva seguridad
	A5: Corte de suministro eléctrico o Falla en el aire acondicionado	Media	Los cortes de suministros eléctricos se presentan todos los años en el país
	V5: Funcionamiento no confiable del UPS o funcionamiento no adecuado del aire	Media	Los portátiles no se conectan a un UPS general, únicamente cuentan con la batería

	acondicionado		
	A6: Instalación no autorizada o cambios de Software	Baja	Este problema no ha ocurrido en el último año
	V6: Falta de control de acceso	Baja	Los usuarios no tienen permisos para instalar programas, pero hay la posibilidad que con herramientas no autorizadas monitoreen la red y las contraseñas que viajan por la misma
	A7: Incumplimiento con la legislación	Baja	No se presentan registros
	V7: Falta de conocimiento de protección de derechos de SW por parte de los empleados	Alta	En la empresa no se tiene conocimiento de las leyes de protección de derechos de autor
	A8: Uso no previsto	Media	Es considerable el porcentaje de personas que utiliza los recursos para otras actividades diferentes del negocio
	V8: Falta de las políticas	Alta	No se encuentran definidas políticas de seguridad
	A9: Incumplimiento con controles de seguridad	Alta	El porcentaje de fallas en la seguridad es alto
	V9: Falta de conocimiento de seguridad por parte del personal	Alta	No se encuentran definidas políticas de seguridad para conocimiento de los usuarios
	A10: Degradación del HW	Medio	Los equipos ya han presentado varias fallas de HW
	V10: Falta de mantenimiento adecuado	Medio	No se realiza un mantenimiento continuo de los equipos
	A11: Inautorizada copia de SW o información propietaria	Medio	Se han encontrado Cd piratas de SW con licencia.
	V11: Falta de políticas	Alta	No se encuentran definidas políticas de seguridad para conocimiento de los usuarios
	A12: Ataque destructivo	Baja	En la CMS no se ha presentado este problema
	V12:Falta de protección física	Alta	La seguridad del edificio es muy escasa
	A13: Robo	Media	Se tiene registrado un caso de robo de equipos
	V 13: Falta de protección física	Alta	No se tiene una adecuada protección física dentro de la CMS
	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector donde se encuentra la CMS
	V1: Falta de protección contra fuego	Media	Actualmente en la CMS no se tienen ninguna protección contra fuego, como extintores

Servidores	A2: Daños por agua	Baja	No se ha registrado este tipo de incidente
	V2: Falta de protección física adecuada	Media	Las instalaciones donde se encuentran los servidores eran un antiguo baño, del cual no se han retirado las instalaciones de agua.
	A3: Desastres naturales	Baja	No se ha registrado este tipo de incidente
	V3: Condiciones locales donde los recursos son fácilmente afectados por desastres	Media	No existen protecciones requeridas para enfrentar daños causados ante desastres naturales
	A4:Corrupción de archivos de registros	Baja	No se han presentado problemas de este nivel
	V4: Falta de Protección de los archivos de registro	Media	La única persona que tiene acceso a los servidores es el administrador, pero puede ser interceptada la información que viaja en la red
	A5: Negación de Servicio	Media	Este ataque no se ha presentado todavía, pero puede ocurrir
	V5: Incapacidad de distinguir una petición real de una falsa	Alta	No existe una protección efectiva ante este ataque
	A6: Corte de suministro eléctrico o Falla en el aire acondicionado	Media	Los cortes de energía eléctrica son frecuentes en el país
	V6: Funcionamiento no confiable del UPS o funcionamiento no adecuado del aire acondicionado	Media	Los servidores se encuentran conectados al UPS que tiene una duración de 3 horas, luego del cual se apagarían.
	A7: Acceso no autorizado a través de la red	Medio	Existe siempre la posibilidad que alguien no autorizado logré ingresar a través de la red
	V7: Código malicioso desconocido	Medio	Esto puede pasar, pues siempre sale nuevo código dañino que no es reconocido por los antivirus.
	A8: Degradación o Falla del HW	Medio	Son equipos que no han sido actualizados de HW hace mucho tiempo
	V8: Falta de mantenimiento adecuado	Medio	No se realiza un mantenimiento preventivo y correctivo adecuado
	A9: Manipulación de la configuración	Baja	No se tiene registros de este tipo de problemas
	V9: Falta de control de acceso	Alta	El ingreso al cuarto de servidores no está muy protegido, únicamente cuenta con una puerta de una llave de fácil apertura
	A10: Incumplimiento con controles de seguridad	Media	Se han presentado registros de intentos de ingreso a los servidores sin autorización

	V10: Falta de conocimiento de seguridad por parte del personal	Alta	Los empleados de la empresa tienen muy poco conocimiento de las políticas de seguridad
	A11: Incapacidad de restauración	Alta	No se encuentra definido un plan de contingencia
	V11: Falta de planes de continuidad del negocio	Alta	No se realizan respaldos, ni se encuentran definidos procedimientos para enfrentar fallas
	A12: Análisis de tráfico	Media	Se han encontrado sniffers en la red
	V12: Falta de establecimiento de una conexión segura	Media	Se utilizan protocolos de encripción SSL en http
	A13: Brechas de seguridad no detectadas	Baja	No se han registrado eventos de este problema
	V13: Falta de monitoreo de los servidores	Alta	No se realiza continuo monitoreo de los servidores
	A14: Ataque destructivo	Baja	En la CMS no se ha presentado este problema
	V14: Falta de protección física	Alta	La seguridad del edificio es muy escasa
Equipos de Oficina	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector donde se encuentra la CMS
	V1: Falta de protección contra fuego	Media	Actualmente en la CMS no se tienen ninguna protección contra fuego, como extintores
	A2: Daños por agua	Baja	No se ha registrado este tipo de incidente
	V2: Falta de protección física adecuada	Baja	Las instalaciones donde se encuentran los usuarios, con los equipos no presentan penetrabilidad de agua.
	A3: Desastres naturales	Baja	No se ha registrado este tipo de incidente
	V3: Condiciones locales donde los recursos son fácilmente afectados por desastres	Media	No existen protecciones requeridas para enfrentar daños causados ante desastres naturales
	A4: Degradación o Falla de HW	Media	Se han presentado problemas en algunas impresoras y teléfonos
	V4: Falta de Mantenimiento	Alta	No se realiza un mantenimiento de los equipos, los mismos que utilizados por todos los usuarios.
	A5: Ataque destructivo	Baja	En la CMS no se ha presentado este problema
	V5: Falta de protección física	Alta	La seguridad del edificio es muy escasa
	A6: Uso no previsto	Alta	Se han encontrado a varios usuarios con uso no adecuado del teléfono y las impresoras
	V6.1: Falta de Políticas	Alto	No se encuentran definidos

			procedimientos para un uso adecuado de los equipos
	V6.2: Falta de Control de Acceso	Alta	No se tiene control para el uso de los equipos
Soporte electrónico	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector donde se encuentra la CMS
	V1: Falta de protección contra fuego	Media	Actualmente en la CMS no se tienen ninguna protección contra fuego, como extintores
	A2: Daños por agua	Baja	No se ha registrado este tipo de incidente
	V2: Falta de protección física adecuada	Baja	El soporte electrónico se guarda adecuadamente en estanterías adecuadas
	A3: Desastres naturales	Baja	No se ha registrado este tipo de incidente
	V3: Condiciones locales donde los recursos son fácilmente afectados por desastres	Media	No existen protecciones requeridas para enfrentar daños causados ante desastres naturales
	A4: Condiciones inadecuadas de temperatura y/o humedad	Baja	Esto no se ha registrado debido al funcionamiento adecuado del aire acondicionado
	V4: Susceptibidad al calor y humedad	Alta	Los CD, disquetes son susceptibles a la humedad
	A5:Ataque destructivo	Baja	En la CMS no se ha presentado este problema
	V5: Falta de protección física	Alta	La seguridad de estos elementos es muy escasa
	A6:Escape de información	Alta	Se han presentado pérdidas en la oficina
	V6: Manipulación inadecuada de información	Alta	No se tiene un procedimiento aprobado de manipulación de la información
	A6: Robo	Alta	Se han presentado pérdidas en la oficina
	V6:Falta de atención del personal	Alta	El personal deja descuidadas sus cosas
Documentación y Registros.	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector donde se encuentra la CMS
	V1: Falta de protección contra fuego	Media	Actualmente en la CMS no se tienen ninguna protección contra fuego, como extintores
	A2: Daños por agua	Baja	No se ha registrado este tipo de incidente
	V2: Falta de protección física adecuada	Baja	Los documentos se encuentran en gavetas protegidas contra ingreso de agua.
	A3: Desastres naturales	Baja	No se ha registrado este tipo de incidente
	V3: Condiciones locales donde los recursos son fácilmente afectados por desastres	Media	No existen protecciones requeridas para enfrentar daños causados ante desastres naturales

	A4: Pérdida de información	Media	Se han presentado problemas debido a fallas de los empleados
	V4.1: Errores de los empleados	Alta	No se realizan respaldos de la información, esto combinado con los errores de los usuarios
	V4.2 : Almacenamiento no protegido	Media	Los documentos se encuentran en gavetas bajo llave. Pero susceptible a daños por fuerza bruta
	A5: Divulgación de información de clientes	Media	No se encuentran definidos políticas de confidencialidad
	V5: Almacenamiento no protegido	Media	Los documentos se encuentran en gavetas bajo llave. Pero susceptible a daños por fuerza bruta
	A6: Incumplimiento de leyes en cuanto a la información de clientes o empleados	Baja	No se han presentado problemas de este tipo con clientes
	V6: Falta de conocimiento de los empleados	Media	Los empleados nuevos no son capacitados apropiadamente, lo que ocasiona desconocimiento de los reglamentos
	A7: Incorrecta o incompleta documentación del sistema	Baja	La compañía tiene documentado los procesos del Sistema
	V7: Falta de documentación actualizada del sistema	Media	No se encuentran documentación actualizada de los cambios realizados en el sistema.
	A8: Contratos incompletos	Media	Se han presentado problemas con el contrato con los proveedores de internet
	V8: Falta de control para el establecimiento de contratos	Baja	Los contratos los revisan todos los niveles de la empresa, desde el solicitante hasta el director ejecutivo
	A9: Ataque destructivo	Baja	En la CMS no se ha presentado este problema
	V9: Falta de protección física	Alta	La seguridad de estos elementos es muy escasa
	A10: Incapacidad de restauración	Alta	No se encuentra definido un plan de contingencia
	V10: Falta de planes de continuidad del negocio	Alta	No se realizan respaldos, ni se encuentran definidos procedimientos para enfrentar fallas
	A11: Modificación no autorizada de la información	Media	Se han registrado problemas debidos a cambios en la información no previstos
	V11: Insuficiente entrenamiento de empleados	Baja	Los empleados conocen sus responsabilidades, y autorizaciones permitidas a la información

Empleados	A1: Errores de los empleados y acciones equivocadas	Alta	Nuevos empleados encuentran frecuentemente fallas debido a errores de empleados anteriores
	V1: Falta de conocimiento y oportuno entrenamiento	Media	Los empleados nuevos no son capacitados apropiadamente, lo que ocasiona desconocimiento de los reglamentos
	A2: Insuficiente personal	Media	Se presenta sobre todo en fechas de vacaciones de empleados, o cuando se enferman
	V2: Falta de acuerdos definidos para reemplazo de empleados	Media	No se encuentra definido un procedimiento claro para el reemplazo temporal
	A3: Divulgación de información confidencial	Media	Se puede presentar con empleados que han salido en malos términos de la empresa
	V3: Falta de acuerdos de confidencialidad	Baja	Se encuentra definido en el contrato los acuerdos de confidencialidad a los que se compromete el empleado
Establecimientos	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector donde se encuentra la CMS
	V1: Falta de protección contra fuego	Media	Actualmente en la CMS no se tienen ninguna protección contra fuego, como extintores
	A2: Daños por agua	Baja	No se ha registrado este tipo de incidente
	V2: Falta de protección física adecuada	Baja	Las instalaciones no presentan daños mayores debido a lluvias
	A3: Acceso no autorizado	Media	Se han registrado varios problemas debido a ingreso de personas no autorizadas
	V3.1: Falta de protección física	Alta	La CMS cuenta con un único guardia que controla todo el edificio
	V3.2: Falta de políticas	Alta	No se encuentran definidas políticas para restringir el acceso a determinados lugares de la empresa
	A4: Desastres naturales	Baja	No se ha registrado este tipo de incidente
	V4: Condiciones locales donde los recursos son fácilmente afectados por desastres	Media	No existen protecciones requeridas para enfrentar daños causados ante desastres naturales
Servicio de Comunicac	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector donde se encuentra la CMS
	V1: Falta de protección contra fuego	Media	Actualmente en la CMS no se tienen ninguna protección contra fuego, como extintores
	A2: Daños por agua	Baja	No se ha registrado este tipo

			de incidente
	V2: Falta de protección física adecuada	Baja	Las instalaciones donde se encuentran la PBX, no presentan penetrabilidad de agua.
	A3: Desastres naturales	Baja	No se ha registrado este tipo de incidente
	V3: Condiciones locales donde los recursos son fácilmente afectados por desastres	Media	No existen protecciones requeridas para enfrentar daños causados ante desastres naturales
	A4: Degradación del servicio y equipos	Media	Se han presentado problemas debido a congestión de las líneas, y pérdidas del servicio de telefonía
	V4: Falta de mantenimiento adecuado	Alta	No se realiza un mantenimiento adecuado de la central telefónica.
	A5: Errores de configuración	Baja	No se tienen registros de problemas debido a errores de configuración de la central
	V5: Falta de conocimiento del administrador	Media	El administrador tiene conocimiento muy básico de la central
	A6: Manipulación de la configuración	Baja	No se han registrado problemas debido a cambios en la configuración
	V6: Falta de control de acceso	Media	No se tiene control para el uso de los servicios
	A7: Uso no previsto	Media	En el año se han presentado varios incidentes donde se han encontrado a los empleados utilizando los equipos para fines personales, más que para fines de negocio
	V7: Falta de políticas	Media	No se encuentran políticas de seguridad definidas y de conocimiento de los usuarios
	A8: Daños de cables, ataques destructivos	Baja	En la CMS no se ha presentado este problema
	V8: Falta de protección adecuada	Alta	Los cables de líneas telefónicas se encuentran en lugares públicos.
	A9: Fallas de servicios de telefonía	Alta	Se encuentra registrado varias fallas al año de las líneas telefónicas
	V9: Falta de acuerdos bien definidos con terceras partes	Alta	No se negocian contratos que cubran los cambios continuos del negocio de terceras partes.
Servicio de energía eléctrica	A 1: Fuego	Baja	La oportunidad que de se produzca fuego no es muy alta
	V1: Falta de protección contra fuego	Alta	Actualmente en la CMS no se tienen ninguna protección contra fuego, como extintores
	A2: Daños por agua	Media	Al año se presentan algunos

			registros de daños causados por lluvias.
	V2: Falta de protección física adecuada	Media	La entrada de la red eléctrica no se encuentra en un lugar seguro
	A3: Desastres naturales	Baja	En los últimos años no se ha presentado ningún desastre natural y es poco probable que ocurra
	V3: Falta de protección frente a desastres naturales	Media	No existen protecciones requeridas para enfrentar daños causados ante desastres naturales
	A 4: Ataque destructivo	Baja	Este tipo de ataque es muy poco probable que ocurra
	V 4: Falta de protección física	Baja	La entrada de la red eléctrica se encuentra en un lugar seguro
Servicio de correo electrónico	A1: Errores de los usuarios	Baja	Sólo se ha registrado una sola vez al año este incidente
	V1: Falta de conocimiento del uso del servicio	Media	Los usuario deben recibir entrenamiento en cómo usar los servicios
	A2: Suplantación de la identidad del usuario	Baja	No se ha registrado ningún incidente todavía
	V2: Falta de control de acceso	Alta	Actualmente no se tienen una política aprobada, está en proceso de desarrollo todavía
	A3: Análisis de tráfico	Baja	No se ha registrado ningún incidente
	V3: Falta de establecimiento de una conexión segura (VPN)	Alta	Ya que la información viaja en texto plano por la red pública sin encripción, se tiene un alto nivel de vulnerabilidad
	A4: Uso no previsto	Alta	En varias ocasiones se ha utilizado este servicio con fines personales
	V4: Falta de políticas	Alta	Actualmente no se tienen una política aprobada, está en proceso de desarrollo todavía
	A5: Fallas de servicios de soporte (telefonía, servicios de Internet)	Media	En el año se registró este incidente dos veces
	V5: Falta de acuerdos bien definidos con terceras partes	Alta	No se tienen bien definidos los acuerdos de servicios con los proveedores de Internet
Aplicación Oracle para acceso a la información de usuarios	A1: Errores de los usuarios	Media	Se han presentado varios registros de problemas debido a fallas de los usuarios de la aplicación
	V1: Falta de conocimiento del uso de la aplicación	Baja	Al ingresar un nuevo usuario del servicio se le capacita para el correcto uso del sistema
	A2: Errores de configuración	Baja	Todavía no se ha registrado errores de configuración
	V2: Falta de capacitación del	Baja	El administrador es una persona preparada con

	administrador del sistema		experiencia
	A3: Escapes de información	Baja	Todavía no se ha registrado errores en el mantenimiento o actualización del programa, pero puede suceder
	V3: Falta de control de acceso	Media	Se controla el acceso a este aplicativo mediante claves, las cuales pueden ser fácilmente vulnerables debido a que no se cuenta con una política definida de generación de claves.
	A4: Errores de actualización del programa	Baja	No se ha registrado este incidente
	V4: Falta de procedimientos aprobados	Alta	No se cuenta con procedimiento de actualización de este SW
	A5: Manipulación de la configuración	Baja	Todavía no se ha registrado ninguna manipulación en la configuración
	V5: Falta de control de acceso	Media	Es posible que los usuarios utilicen passwords no apropiados ya que no se cuentan con política.
	A6: Suplantación de la identidad del usuario	Baja	No se ha registrado ningún incidente
	V6: Falta de Control de acceso	Alta	En vista de que no se lleva actualizaciones del aplicativo, es más fácil explotar esta vulnerabilidad
	A7: Abuso de privilegios de acceso	Baja	No se ha registrado ningún incidente
	V7: Falta de políticas de seguridad	Alta	Actualmente no se tienen una política aprobada, está en proceso de desarrollo todavía
	A8: Negación de servicio	Media	Esta forma de ataque no ha tenido lugar todavía, pero podría pasar en cualquier momento
	V8: Incapacidad para distinguir una petición real de una petición falsificada	Alta	Hay ciertas formas de ataque de deniego de servicio, donde no existe ninguna protección contra estos tipos de ataque
Portal de información (Página Web de la empresa)	A1: Modificación no autorizada del sitio Web	Baja	La probabilidad global de modificación desautorizado es baja; el sitio de Web es bien protegido contra eso.
	V1: Falta de procedimientos para cambios	Alta	Actualmente no se cuenta con procedimientos para cambios del Sitio Web
	A2: Negación de servicio	Baja	No se ha registrado ningún incidente
	V2: Falta de recursos necesarios	Media	Los usuario deben recibir entrenamiento en cómo usar los servicios

	A3: Sitio Web no disponible	Media	Dos veces en el año se registro este evento
	V3: Fallas en los acuerdos de niveles de servicio	Media	No se tienen bien definidos los nivel es de servicio en los contratos
	A4: Publicación de información incorrecta de la CMS	Baja	Hasta el momento no se ha tenido ningún tipo de problema con esta amenaza
	V 4: Falta de procedimiento aprobados	Baja	Antes de la publicación de información, se tienen una aprobación de la gerencia
Suministros de oficina	A1: Fuego	Baja	La oportunidad que de se produzca fuego no es muy alta
	V1: Falta de protección contra fuego	Alta	Actualmente en la CMS no se tienen ninguna protección contra fuego, como extintores
	A2: Daños por agua	Baja	No se ha registrado este tipo de incidente
	V2: Falta de protección física adecuada	Baja	No se tiene cercanía con instalaciones de agua
	A3: Desastres naturales	Baja	No se ha registrado este tipo de incidente
	V3: Condiciones locales donde los recursos son fácilmente afectados por desastres naturales	Media	No existen protecciones requeridas para enfrentar daños causados ante desastres naturales
	A4: Robo	Alta	Se ha presentado en algunas ocasiones este incidente
	V4.1: Falta de atención	Baja	El personal está en las instalaciones en horas de trabajo, y además cuenta con un guardia las 24 horas
	V4.2: Falta de protección física	Baja	Los suministros de oficina están debidamente asegurados
Imagen de la empresa Reputación	A1: Divulgación de datos de los clientes	Baja	No se ha registrado este tipo de incidente
	V1: Insuficiente seguridad de información de los clientes	Alta	Es vulnerable a eventos donde puede conducir a la mala imagen en público
Paquetes o software estándar	A1: Negación de Servicio	Baja	No se ha registrado este tipo de incidente
	V1: Capacidad insuficiente de los recursos	Baja	Se cuenta con los recursos suficientes
	A2: Virus de Computación, Fuerza Bruta y ataques de diccionario	Alta	Se ha registrado varias veces virus
	V2: Falta de Protección(AV) actualizada	Alta	No se lleva ningún tipo de actualización para el software
	A3: Spoofing, Escape de información	Baja	No se ha registrado este tipo de incidente
	V3: Falta de control de acceso	Baja	En el Sw estándar no se necesita ningún tipo de

			control de acceso
	A4: Falta de capacidad de restauración	Baja	No se ha registrado este tipo de incidente
	V4: Falta de copias de backup continuas	Alta	No se tiene copias de respalda para restauración
	A5: Uso no previsto	Alta	El personal en algunas ocasiones hacen uso de estas herramientas con fines personales
	V5: Falta de políticas de seguridad	Alta	Actualmente no se tienen una política aprobada, está en proceso de desarrollo todavía
Sistemas operativos	A 1: Negación de Servicio	Baja	Esta forma de ataque no ha tomado lugar todavía, pero podría pasar en cualquier momento
	V 1: Capacidad insuficiente de los recursos	Media	La recursos de los SOs, es suficiente para la cantidad de información que maneja la CMS.
	A2: Errores de Configuración del servicio	Baja	No se han presentado registros de este problema
	V2.1: Falta de capacitación del administrador	Media	El administrador no cuenta con gran conocimiento de los Sistemas operativos de los servidores.
	V2.2: Incompleto o incorrecto documentación del sistema	Media	Se tiene la documentación del sistema, pero sin seguir ningún procedimiento aprobado
	A 3: Virus de Computación, Fuerza Bruta y ataques de diccionario	Media	El servidor ha sido afectado una vez por un Virus de computación
	V 3: Falta de Protección (AV) actualizada	Alta	No se sigue procedimientos aprobados para la actualización y mantenimiento del software
	A 4: Falta de capacidad de restauración	Media	Todavía no ha pasado este incidente pero puede pasar en cualquier tiempo si no se tiene copias de backups
	V 4: Falta de copias de backup continuas	Alta	Esta vulnerabilidad puede ser fácilmente afectada porque no se tiene copias de backups
	A 5: Pérdida de Servicio	Baja	No se ha registrado ningún incidente
	V 5.1: Actualizaciones incorrectas	Alta	No se cuenta con un procedimiento para las actualizaciones
	V 5.2: Instalación de SW no autorizado	Alta	Esta vulnerabilidad puede ser fácilmente debido a que no se sigue ninguna política de seguridad
	A 6: Controles de Seguridad no cumplidos	Alta	En la CMS no se ha definido controles de seguridad, razón por la cual ciertos controles

			no han sido cumplidos
	V 6: Falta de Políticas de Seguridad	Alta	Actualmente no se tienen una política aprobada, está en proceso de desarrollo todavía
	A7: Alteración no autorizado de la configuración	Baja	No se ha registrado ningún incidente
	V 7: Falta de control de acceso	Alta	El control de acceso puede ser fácilmente vulnerado debido a la débil seguridad física de los equipos de cómputo
Medios y Soporte	A1: Acceso no autorizado a la información	Media	Se han encontrado máquinas personales conectadas a la red
	V1: Falta de protección física	Media	No se tiene una adecuada protección física dentro de la CMS
	A 2: Robo	Baja	No se ha registrado ningún incidente
	V 2: Falta de protección física	Alta	No se tiene una adecuada protección física dentro de la CMS
	A3: Daños de cables	Baja	No se ha registrado este tipo de incidente
	V3: Falta de protección adecuada	Baja	El sistema de cableado esta debidamente instalado y protegido
	A4: Análisis de tráfico	Baja	No se ha registrado este tipo de incidente
	V4: Falta de establecimiento de una conexión segura (VPN)	Alta	La información viaja en texto plano en la red interna
	A5: Brechas de seguridad no detectadas	Baja	No se ha registrado este tipo de incidente
	V5: Falta de monitoreo de la red	Alta	No cuenta con ningún tipo de monitoreo de la red

Tabla 3.19. Exposición del Riesgo

3.4. PLAN DE TRATAMIENTO DE RIESGOS PARA IDENTIFICAR ACCIONES, RESPONSABILIDADES Y PRIORIDADES EN LA GESTIÓN DE LOS RIESGOS DE LA SEGURIDAD DE LA INTRANET.

A continuación describimos las principales responsabilidades de los miembros implicados en la seguridad de la información para la gestión de los riesgos basados en los dominios:

- El **Área de Sistemas** es responsable de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de

seguridad a lo largo de toda la organización, todo esto en coordinación con la Dirección Ejecutiva y Jefatura Administrativa Financiera y con el área de Auditoria Interna. También es responsable de evaluar, adquirir e implantar productos de seguridad informática, y realizar las demás actividades necesarias para garantizar un ambiente informático seguro. Además debe ocuparse de proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad, y en particular en los casos de infección de virus, penetración de hackers, fraudes y otros percances.

- El **Encargado de Sistemas** es responsable de dirigir las investigaciones sobre incidentes y problemas relacionados con la seguridad, así como recomendar las medidas pertinentes.

- El **Proveedor del Sistema Informático** es responsable de establecer los controles de acceso apropiados para cada usuario de Base de Datos, revisar las bitácoras de acceso y de llevar a cabo las tareas de seguridad relativas a los sistemas que administra, El Proveedor del Sistemas también es responsable de informar al Encargado de Sistemas sobre toda actividad sospechosa o evento insólito.

- El **Comité de Seguridad de la Información** del Organismo, procederá a revisar y proponer a la máxima autoridad del Organismo para su aprobación la Política de Seguridad de la Información y las funciones generales en materia de seguridad de la información; monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes; tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad; aprobar las principales iniciativas para incrementar la seguridad de la información , de acuerdo a las competencias y responsabilidades asignadas a cada área1, así como acordar y aprobar metodologías y procesos específicos relativos a seguridad de la información; garantizar que la seguridad sea parte del proceso de planificación de la información; evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios; promover la difusión y apoyo a la

seguridad de la información dentro del Organismo y coordinar el proceso de administración de la continuidad de las actividades del Organismo.

- Los usuarios son responsables de cumplir con todas las políticas de la Corporación relativas a la seguridad informática y en particular:

    - Conocer y aplicar las políticas y procedimientos apropiados en relación al manejo de la información y de los sistemas informáticos.
    - No divulgar información confidencial de la Corporación a personas no autorizadas.
    - No permitir y no facilitar el uso de los sistemas informáticos de la Corporación a personas no autorizadas.
    - No utilizar los recursos informáticos (hardware, software o datos) y de telecomunicaciones (teléfono, fax) para otras actividades que no estén directamente relacionadas con el trabajo en la Corporación.
    - Proteger meticulosamente su contraseña y evitar que sea vista por otros en forma inadvertida.
    - Seleccionar una contraseña robusta que no tenga relación obvia con el usuario, sus familiares, el grupo de trabajo, y otras asociaciones parecidas.
    - Reportar inmediatamente a su jefe inmediato o a un funcionario de Sistemas cualquier evento que pueda comprometer la seguridad de la Corporación y sus recursos informáticos, como por ejemplo contagio de virus, intrusos, modificación o pérdida de datos y otras actividades poco usuales.

El **Comité de Seguridad de la Información** tendrá a cargo el mantenimiento y la presentación para la aprobación de la Política, ante la máxima autoridad de la Corporación, el seguimiento de acuerdo a las incumbencias propias de cada área de las actividades relativas a la seguridad de la información (análisis de riesgos, monitoreo de incidentes, supervisión de la investigación,

implementación de controles, administración de la continuidad, impulsión de procesos de concientización, etc.) y la proposición de asignación de funciones.

Los **Responsables de las Unidades Organizativas** cumplirán la función de autorizar la incorporación de nuevos recursos de procesamiento de información a las áreas de su incumbencia.

El **Responsable del Área Legal** participará notificará a los proveedores sobre las modificaciones que se efectúen a la Política de Seguridad, además de participar en la confección del Compromiso de Confidencialidad a firmar por los empleados y terceros que desarrollen funciones en el organismo, en el asesoramiento sobre las sanciones a ser aplicadas por incumplimiento y en el tratamiento de incidentes de seguridad que requieran de su intervención.

El **Responsable del Área de Recursos Humanos** incluirá las funciones relativas a la seguridad de la información en las descripciones de puestos de los empleados, informará a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información, gestionará los Compromisos de Confidencialidad con el personal y coordinará las tareas de capacitación de usuarios.
El Responsable de Seguridad Informática tendrá a su cargo, entre otros:

- Definir procedimientos para el control de cambios a los procesos operativos documentados.
- Definir y documentar una norma clara con respecto al uso del correo electrónico (políticas del correo electrónico).
- Definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso y para garantizar la seguridad de los datos y los servicios conectados en las redes del Organismo.
- Desarrollar procedimientos adecuados de concientización de usuarios en materia de seguridad.
- Verificar el cumplimiento de las normas, procedimientos y controles establecidos.

- Monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad, a fin de evitar potenciales amenazas a la seguridad del sistema o a los servicios del usuario.
- Implementar los controles de seguridad definidos (software malicioso y accesos no autorizados).
- Definir e implementar procedimientos para la administración de medios informáticos de almacenamiento, como cintas, discos, casetes e informes impresos y para la eliminación segura de los mismos.

Una vez que hemos definido los responsables para el manejo de las vulnerabilidades, tenemos que identificar las acciones que vamos a tomar sobre cada riesgo, por lo cual realizamos una valoración de los mismos en base a la información obtenida en el capítulo anterior. Además de obtener la valoración vamos a tomar la decisión de aceptar o tratar el riesgo.

VALORACIÓN DE RIESGOS DEL SGSI

La valoración de riesgos es ejecutada una vez que ya se ha creado un inventario de activos de información y determinando las categorías de importancia de los activos de información y el criterio para la evaluación de amenazas y vulnerabilidades.

El valor de un riesgo puede ser calculado usando la siguiente fórmula y los valores para el "valor de los activos de información", "escala de las amenazas" y "nivel de vulnerabilidad".

C: Valor del riesgo por la confidencialidad

I: Valor del riesgo por la integridad

D: Valor del riesgo por la disponibilidad

Valor del riesgo = "Valor del activo" x "Amenazas" x "Vulnerabilidades"

(Ejemplo)

Elementos de activos de información — Valor de los activos

- C: confidencialidad — 4
- I: integridad — 2
- D: disponibilidad — 1

Amenaza 3

Vulnerabilidad 3

El valor del riesgo para este caso es calculado de la siguiente forma:

Valor del riesgo por la confidencialidad: 4 x 3 x 3 = 36

Valor del riesgo por la integridad: 2 x 3 x 3 = 18

Valor del riesgo por la disponibilidad: 1 x 3 x 3 = 9

Figura 4.1. Ejemplo de cálculo para la valoración del riesgo

En base a la información obtenida en el capítulo anterior se puede realizar este cálculo y determinar el valor de riesgo de cada activo.

Una vez que tenemos la valoración de los riesgos debemos tomar la decisión de aceptar el riesgo o reducirlo, debemos determinar un valor mínimo como límite para aceptar el riesgo, sobre ese valor deben tomarse medidas sobre los riesgos. En nuestro caso seleccionamos como nivel límite de riesgo es el 4, es decir valores menores a 4 se tomará la decisión de aceptar el riesgo.

Luego de analizar el cuadro anterior determinamos que con este nivel los riesgos que aceptamos son aquellos que tienen una mínima probabilidad de ocurrencia con un poco impacto en caso de que lleguen a presentarse. A continuación presentamos una tabla con los niveles de riesgos:

	AMENAZA								
	1			**2**			**3**		
	VULNERABILIDAD								
ACTIVOS DE INFORMACIÓN	**1**	**2**	**3**	**1**	**2**	**3**	**1**	**2**	**3**
1	1	2	3	2	4	6	3	6	9
2	2	4	6	4	8	12	6	12	18
3	3	6	9	6	12	18	9	18	27
4	4	8	12	8	16	24	12	24	36

Tabla 3.20. Niveles de Riesgos

Aquellos riesgos con niveles menores a 4 como se muestra en la tabla anterior, son aquellos que se van a aceptar. Como se puede observar son aquellos con una valoración mínima para no afectar la funcionalidad de la organización.
A continuación presentamos las opciones para el tratamiento de los riesgos:

3.5. ESTUDIO DE FACTIBILIDAD DE APLICACIÓN DE LOS CONTROLES DE LA NORMA (ANEXO A) PARA LA INTRANET.

En base a las vulnerabilidades identificadas en la CMS se detallarán los controles que ayudarán a cubrir estas vulnerabilidades, los demás controles no se consideraron debido a que no dan una mayor solución a los riesgos.

3.5.1. FACTIBILIDAD DE LOS CONTROLES DEL DOMINIO POLÍTICA DE SEGURIDAD

Política de Seguridad de la Información.

Documento de Política de Seguridad de la Información

Mediante las políticas de seguridad se busca que los empleados tengan conocimiento de la seguridad de información, de tal manera que se reduzca los errores de los empleados y también limitará los problemas que podría ocurrir y sus impactos. El entrenamiento y otros controles asegurarán que los empleados comprendan el problema del mal uso y también se les informará que cualquier uso no autorizado será demandado y todas las evidencias necesarias serán recopiladas. Las personas que trabajan en la CMS deben seguir políticas de acuerdo a las leyes relevantes, las cuales prohíben la copia de SW o información propietaria.
El documento de políticas de seguridad, específica la dirección de seguridad que va a seguir la empresa, se reducirá este problema si en la CMS se emite políticas de seguridad y se da conocer a todo el personal.

3.5.2. FACTIBILIDAD DE LOS CONTROLES DEL DOMINIO ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD

Organización interna.

Asignación de responsabilidades sobre seguridad de la información

Asegurar un entrenamiento adecuado de los empleados, mejorando la cultura de la seguridad de información en la CMS, lo cual reducirá los errores de los empleados y también limitará los problemas que podría ocurrir y sus impactos.

Proceso de autorización de recursos para el tratamiento de la información

Con estos controles se trata de reducir el riesgo de acceso a los recursos de la información de forma no autorizada, para lo cual se asigna responsabilidades para la seguridad de la información a través de la CMS, para evitar el mal uso de los activos.

3.5.3. FACTIBILIDAD DE LOS CONTROLES DEL DOMINIO GESTIÓN DE ACTIVOS DE LA RED DE INFORMACIÓN

Responsabilidad sobre los activos.

Inventario de activos

Se trata de controlar que los activos no sean robados mediante la asignación de propietarios, y con el inventario se busca tener identificados todos los activos de la CMS.

Propiedad de los recursos

Se trata de controlar que los activos no sean robados mediante la asignación de propietarios, y con el inventario se busca tener identificados todos los activos de la CMS.

Uso aceptable del uso de los recursos

Para minimizar este riesgo se utilizan guías de utilización de los activos fuera de las premisas de la CMS.

3.5.4. FACTIBILIDAD DE LOS CONTROLES DEL DOMINIO SEGURIDAD DE LOS RECURSOS HUMANOS

Seguridad en la definición del trabajo y los recursos.

Roles y responsabilidades

Introduciendo estos controles y haciendo que los empleados estén conscientes de su propia responsabilidad, lo cual ayudará a reducir el riesgo de probabilidad de este problema. Si algo sale mal, el impacto seguirá siendo alto, este riesgo no puede reducirse más allá.

Se busca reducir este riesgo, si se escoge de manera oportuna a los empleados, para lo cual se tendrá una política de selección del personal donde se detallará sus roles y responsabilidades, de esta manera evitar que los empleados realicen tareas que estén fuera de sus responsabilidades.

Selección y política del personal

Se busca reducir este riesgo, si se escoge de manera oportuna a los empleados, para lo cual se tendrá una política de selección del personal.

Términos y condiciones de la relación laboral

Se reducirá el riesgo del mal uso de los activos si los empleados comprenden sus responsabilidades, y sus roles con respecto a la seguridad de información.

Durante el empleo.

Responsabilidades de administración

Si se asegura que los empleados tengan un apropiado conocimiento de las amenazas de la seguridad, se reducirá este riesgo y sus posibles impactos. También con la ayuda del conocimiento de los roles y responsabilidades de cada empleado, se reducirá el mal uso de los activos

Conocimiento, educación y entrenamiento de la seguridad de información

Si se asegura que los empleados tengan un apropiado conocimiento de las amenazas de la seguridad, se reducirá este riesgo y sus posibles impactos.

Asegurar un entrenamiento adecuado de los empleados, mejorando la cultura de la seguridad de información en la CMS, lo cual reducirá los errores de los empleados y también limitará los problemas que podría ocurrir y sus impactos.

Proceso disciplinario

Si se asegura que los empleados tengan un apropiado conocimiento de las amenazas de la seguridad, se reducirá este riesgo y sus posibles impactos.
Los empleados de la CMS deben tener conocimiento de los riesgo que se toma al ejecutar código malicioso desconocido y que consecuencias puede traer esta acción, este debe ser un proceso disciplinario continuo.

3.5.5. FACTIBILIDAD DE LOS CONTROLES DEL DOMINIO SEGURIDAD FÍSICA Y DEL ENTORNO

Áreas seguras

Perímetro de seguridad física

Con la aplicación de este control, se dará una protección adecuada para evitar un ataque destructivo. Con la provisión de una protección física adecuada a los activos de la CMS:
Con la aplicación de estos controles se brinda a los empleados los recursos necesarios para llevar un correcto manejo de la documentación o registro, como por ejemplo. Escritorios con llaves, para proteger la información más sensible.

Controles físicos de entradas

Mediante este control se evita el acceso no autorizado a los activos de la empresa, mediante una protección física adecuada.

Seguridad de oficinas, despachos y recursos

Con este control se da una protección física adecuada a los activos de la CMS, además de brindar a los empleados los recursos necesarios para llevar un

correcto manejo de la documentación o registro, como por ejemplo. Escritorios con llaves, para proteger la información más sensible.

Seguridad de los equipos.

Utilidades de apoyo

Se evita la interrupción de los servicios que ofrecen los activos con la aplicación de estos controles

Mantenimiento de equipos

Se minimiza este riesgo con un apropiado mantenimiento de los equipos de la CMS.

Seguridad de equipos fuera de los locales de la organización

Con estos controles se asegura que los equipos sean protegidos de amenazas físicas y del ambiente, y por ende se evita el acceso no autorizado a estos activos.

3.5.6. FACTIBILIDAD DE LOS CONTROLES DEL DOMINIO GESTIÓN DE COMUNICACIONES Y OPERACIONES

Procedimientos y responsabilidades de operación

Documentación de procedimientos operativos

Se debe tener documentados los procedimientos de actualización para evitar una errónea actualización y por consiguiente pérdida del servicio

La utilización de este control reducirá este riesgo, ya que se documentará solos los procedimientos de operación permitidos y necesarios para la ejecución del Sistema Operativo.

Control de cambios operacionales

Se debe tener documentados los procedimientos de actualización para evitar una errónea actualización y por consiguiente pérdida del servicio

Gestión de servicios externos.

Entrega del servicio

Con este control se busca reducir las fallas en los acuerdos de niveles de servicio con partes externas, para lo cual la CMS debe mantener un nivel apropiado de seguridad y chequea la implementación de los acuerdos.

Monitorización y revisión de los servicios de las terceras partes

Se reducirá el riesgo de fallos de servicios entregados por terceras partes si se tiene bien definidos los acuerdos y se toma en cuenta aspectos relacionados con la seguridad.

Planificación y aceptación del sistema.

Planificación de la capacidad

Con una adecuada planificación del sistema se evitará la degradación del servicio.

Aceptación del sistema

Con una adecuada planificación del sistema se evitará la degradación del servicio.

Protección contra software malicioso.

Controles contra software malicioso

Los controles seleccionados reducirán la probabilidad de que este problema ocurra, pero un nuevo código malicioso siempre puede causar un problema, por lo tanto el riesgo no puede reducirse más allá.

Estos controles reducirá la probabilidad de que este problema ocurra mediante la implementación de procedimientos apropiados para la protección contra SW malicioso.

Gestión interna de respaldo.

Recuperación de la información

Este control reducirá este riesgo al máximo mediante una política de respaldo y una restauración oportuna.

Gestión de la seguridad de red.

Controles de red

Con la aplicación de estos controles se reducirá el riesgo de la negación del servicio mediante una adecuada gestión de la red.

Es establecimiento de estos controles busca mantener la confidencialidad de los datos y así evitar el acceso no autorizado a la red, información y servicio.

Seguridad de los servicios de red

Es establecimiento de estos controles busca mantener la confidencialidad de los datos y así evitar el acceso no autorizado a la red, información y servicio.

Utilización de los medios de información.

Gestión de medios removibles

Con el establecimiento de estos controles se busca tener un procedimiento de manipulación de información para protegerla del mal uso o divulgación no autorizada

Procedimientos de manipulación de la información

Con el establecimiento de estos controles se busca tener un procedimiento de manipulación de información para protegerla del mal uso o divulgación no autorizada

Intercambio de información.

Mensajería electrónica

Se trata de minimizar la transmisión de SW malicioso a través del uso de comunicaciones electrónicas. Con estos controles se trata de asegurar un intercambio de información segura.

Sistemas de información comerciales

Se trata de minimizar la transmisión de SW malicioso a través del uso de comunicaciones electrónicas.

Monitorización.

Registro de auditoria

Una monitorización apropiada detectaría a tiempo brechas de seguridad y así reducirá los impactos que puede causar estas brechas de seguridad, con este objetivo se ha implementado en la CMS herramientas de administración de redes para realizar una adecuada monitorización y detectar a tiempo huecos de seguridad.

Monitorización del uso del sistema

Monitorización apropiada detectaría a tiempo brechas de seguridad y así reducirá los impactos que puede causar estas brechas de seguridad.

Registros del administrador y operador

Una monitorización apropiada detectaría a tiempo brechas de seguridad y así reducirá los impactos que puede causar estas brechas de seguridad

Registro de fallas

Monitorización apropiada detectaría a tiempo brechas de seguridad y así reducirá los impactos que puede causar estas brechas de seguridad.

3.5.7. FACTIBILIDAD DE LOS CONTROLES DEL DOMINIO CONTROL DE ACCESO

Requerimiento de negocios para control de acceso

Política de control de acceso

Es necesario implementar en las políticas de seguridad el control de acceso necesario que se deben tener para permitir el ingreso a las oficinas así como el procedimiento para eliminar los permisos de personas que han salido de la empresa, si bien el riesgo no va a desaparecer el objetivo es disminuirlo.

Se requieren políticas de control de acceso donde se justifiquen las responsabilidades y obligaciones de las personas que tienen acceso a modificar información de la empresa, y los controles necesarios para proteger información crítica; si bien el riesgo no va a desaparecer el objetivo es disminuirlo.

Gestión de acceso de usuarios

Registro de usuarios

Se requiere un procedimiento de registro de ingreso y salida de usuarios para garantizar el acceso a los sistemas y servicios de información.

Gestión de privilegios

Se requiere un procedimiento de revisión continua de privilegios para garantizar y revocar el acceso a los sistemas y servicios de información. Y de esta manera disminuir cambios no autorizados en información crítica

Revisión de derechos de acceso de los usuarios

Es necesario mantener un control del acceso a los datos y servicios de información, por lo cual se requiere realizar una revisión periódica de los derechos de acceso de los usuarios.

Responsabilidades de los usuarios

Uso de contraseñas

Es necesario que los usuarios estén informados del uso de la contraseña, así como las responsabilidades, y la forma de mantenerla en reserva para evitar acceso a información confidencial por parte de personas ajenas.

Equipo informático de usuarios desatendido

Es necesario que los usuarios tengan conocimiento de la protección que requieren sus equipos, para evitar acceso de terceras personas o pérdida de información de los mismos.

Políticas de limpieza de pantalla y escritorio

Es necesario establecer políticas de limpieza de escritorio para evitar papeles y unidades extraíbles que contengan información que requiera protección

Control de acceso a la red

Política de uso de los servicios de la red

Es necesario asegurar que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios

Autenticación de usuarios para conexiones externas

Es necesario asegurar que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios, por lo cual se requiere mantener un control sobre los sistemas críticos que almacenan información importante de la CMS.

Autenticación de nodos de la red

Es necesario asegurar que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios, una alternativa para evitar conexiones falsas es la autenticación de los nodos permitidos para la red.

Protección a puertos de diagnóstico remoto

Es necesario mantener un control sobre puertos que pueden ser una puerta de ingreso no autorizado a la información de la CMS, por lo cual se deben definir los puertos necesarios y bloquear los demás

Control de conexión a las redes

Los requisitos de la política de control de accesos para redes compartidas, necesitan incorporar controles que restrinjan las capacidades de conexión de los usuarios. Para evitar congestión en los servicios, debido a peticiones falsas.

Por lo cual es indispensable mantener un monitoreo sobre la red para detectar brechas de seguridad y disminuirlas.

Control de enrutamientos en la redes

La conversión de direcciones de la red también es un mecanismo muy útil para aislar redes y evitar rutas de propagación de problemas de seguridad en las redes.

Control de acceso al sistema operativo

Identificación y autenticación del usuario

Se requiere que todos los usuarios deberían disponer de un identificador único para su uso personal y exclusivo, a fin de que pueda posteriormente seguirse la pista de las actividades de cada responsable particular

Control de acceso a las aplicaciones

Restricción de acceso a la información

Se debería dar acceso a la información y a las funciones del sistema de aplicaciones sólo a los usuarios de éste, incluido el personal de apoyo. De esta manera se tendría un mejor control de las personas que tienen acceso para una auditoria.

3.5.8. FACTIBILIDAD DE LOS CONTROLES DEL DOMINIO ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Controles criptográficos

Política de uso de los controles criptográficos

La organización debería desarrollar una política de uso de las medidas criptográficas para proteger la información.

Seguridad en los procesos de desarrollo y soporte

Procedimientos de control de cambios

Se deberían exigir procedimientos formales de control de cambios que garanticen que la seguridad y los procedimientos de control no se alteran y no ocasionan problemas de funcionamiento en la aplicación.

Revisión técnica de los cambios en el sistema operativo

Se deberían revisar y probar las aplicaciones del sistema cuando se efectúen cambios, para asegurar que no impactan adversamente en el funcionamiento o en la seguridad.

Restricciones en los cambios a los paquetes de software

Es necesario usar los paquetes de software suministrados por los proveedores sin modificación en la medida que sea posible y practicable para evitar cambios que afecten el funcionamiento correcto de los servicios.

Canales encubiertos y código troyano

Es necesario usar los paquetes de software suministrados por los proveedores sin modificación en la medida que sea posible y practicable para evitar cambios que afecten el funcionamiento correcto de los servicios. Y puertas que puedan ser aprovechadas por jackers o intrusos.

Gestión de vulnerabilidad técnica

Control de vulnerabilidades técnicas

Se requiere de información oportuna sobre vulnerabilidades técnicas de los sistemas de información que son utilizados en la organización, y la evaluación de la exposición de la organización a tales vulnerabilidades. A fin de evitar brechas de seguridad que pueden ser fácilmente explotadas. Permitiendo el acceso a la red de intrusos.

3.5.9. FACTIBILIDAD DE LOS CONTROLES DEL DOMINIO GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION

Divulgación de eventos y de debilidades de la seguridad de la información

Divulgación de eventos de la seguridad de la información

Es necesario implementar procedimientos de divulgación formal del acontecimiento de la seguridad de la información, junto con una respuesta del incidente y un procedimiento de escalada, para que los empleados puedan implementar las medidas correctivas necesarias.

Administración de incidentes y mejoras de la seguridad de la información

Responsabilidades y procedimientos

Es necesario implementar responsabilidades y los procedimientos se deben establecer para asegurar una respuesta rápida, eficaz, y ordenada a los incidentes de la seguridad de la información.

3.5.10. FACTIBILIDAD DE LOS CONTROLES DEL DOMINIO GESTION DE CONTINUIDAD DEL NEGOCIO

Aspectos de la gestión de continuidad del negocio

Proceso de gestión de la continuidad del negocio

Es indispensable considerar en la gestión de la continuidad del negocio controles para la identificación y reducción de riesgos, limitar las consecuencias

de incidencias dañinas y asegurar la reanudación, a tiempo, de las operaciones esenciales. Debido a fallas en algún equipo o sistema.

Desarrollo e implantación de planes de contingencia

Este control es indispensable para asegurar la disponibilidad de la información en niveles aceptables y de acuerdo al nivel critico en el negocio cuando se presente alguna falla que pueda afectar los servicios.

3.5.11. FACTIBILIDAD DE LOS CONTROLES DEL DOMINIO CUMPLIMIENTO

Cumplimiento con los requisitos legales

Derechos de propiedad intelectual

Se deben implantar procedimientos apropiados para asegurar el cumplimiento de las restricciones legales sobre el uso del material protegido como derechos de autor y los productos de software propietario

Salvaguarda de los registros de la organización

Se requiere proteger los registros importantes de la organización frente a su pérdida, destrucción y falsificación. Es necesario guardar de forma segura ciertos registros, tanto para cumplir ciertos requisitos legales o regulatorios, como para soportar actividades esenciales del negocio.

Protección de los datos y de la privacidad de la información personal

Es necesario basarse en las leyes que protegen datos personales, para evitar problemas legales en los que puede verse involucrada la organización.

Evitar el mal uso de los recursos de tratamiento de la información

Es necesario que los usuarios estén concientes que el uso de un computador con fines no autorizados puede llegar a ser un delito penal.

Revisiones de la política de seguridad y de la conformidad técnica

Conformidad con la política de seguridad

Es necesario que los gerentes, jefes de departamentos se aseguren que se estén cumpliendo correctamente todos los procedimientos de seguridad dentro de su área de responsabilidad, para evitar problemas legales.

3.6. SELECCIÓN DE LOS CONTROLES DE ACUERDO A LA FACTIBILIDAD DE APLICACIÓN.

Una vez indicadas las razones por las cuales se debería escoger los controles, se procederá a la selección de los controles específicos para cubrir cada uno de las amenazas y vulnerabilidades identificadas.

3.6.1. Planteamiento del Problema

Es importante comprender varios factores que conllevaron a aplicar los diferentes controles que sugiere la Norma ISO 27001, actualmente la CMS presenta varios puntos de fallas de seguridad tanto en la red como en la infraestructura. A continuación se indica varios problemas de seguridad presentes en la red de datos de la CMS:

- En la CMS no se cuenta con algún tipo de protección contra ataques provenientes del Internet, por esta razón es importante contar con un sistema de seguridad para que minimice esta amenaza.
- Actualmente no se cuenta con una política de seguridad establecida para definir los lineamientos de seguridad, esto conjuntamente con la falta de un sistema de seguridad hace a la red muy vulnerable a tener huecos de seguridad, especialmente por el hecho de que los empleados navegan libremente por el Internet sin ningún tipo de cuidado y descargan programas provenientes de sitios no confiables. Además no se tiene restricciones en el uso de los recursos de la Corporación con fines personales como por ejemplo: chatear, revisar su correo electrónico personal.

- Para el acceso físico al cuarto de servidores no se cuenta con alguna restricción formal, lo cual puede ocasionar problemas debido a accesos no autorizados.
- No se cuenta con alguna herramienta de administración de red para monitorear continuamente la red de tal forma que se pueda detectar un ataque a tiempo, por ejemplo por algún comportamiento anormal de alguna máquina, o evitar alguna pérdida de servicio mediante la generación de avisos.

3.6.2. Controles seleccionados de la Norma ISO 27001

Los controles seleccionados son los que se adjunta en la siguiente lista:

HARDWARE PORTÁTIL:

Amenazas	***Vulnerabilidades***
Acceso no autorizado a la portátil	Falta de Protección por desatención de equipos
9.2. Áreas seguras 9.2.5. Seguridad de equipos fuera de los locales de la organización 11.1. Requerimiento de negocios para control de acceso 11.1.1. Política de control de acceso 11.3. Responsabilidades de los usuarios 11.3.1. Uso de contraseñas 11.3.2. Equipo informático de usuarios desatendido 15.2. Revisiones de la política de seguridad y de la conformidad técnica 15.2.1. Conformidad con la política de seguridad	
Corte de suministro eléctrico o Falla en el aire acondicionado	Funcionamiento no confiable del UPS o funcionamiento no adecuado del aire acondicionado
9.2. Seguridad de los equipos 9.2.2. Utilidades de apoyo 14.1. Aspectos de la gestión de continuidad del negocio 14.1.3. Desarrollo e implantación de planes de contingencia 14.1.5. Prueba, Mantenimiento y reevaluación de los planes	
Incumplimiento con la legislación	Falta de conocimiento de protección de derechos de SW por parte de los empleados
8.2. Durante el empleo 8.2.2. Conocimiento, educación y entrenamiento de la seguridad de información 15.2. Revisiones de la política de seguridad y de la conformidad técnica 15.2.1. Conformidad con la política de seguridad	
Uso no previsto	Falta de las políticas
5.1. Política de seguridad de la información 5.1.1. Documento de política de seguridad de la información 6.1. Organización interna 6.1.4. Proceso de autorización de recursos para el tratamiento de la información 8.1. Seguridad en la definición del trabajo y los recursos	

8.1.1. Roles y responsabilidades 8.1.3. Términos y condiciones de la relación laboral 8.2. Durante el empleo 8.2.1. Responsabilidades de administración 8.2.2. Conocimiento, educación y entrenamiento de la seguridad de información 8.2.3. Proceso disciplinario 11.3. Responsabilidades de los usuarios 11.3.1. Uso de contraseñas 11.3.2. Equipo informático de usuarios desatendido 15.1. Control de acceso al sistema operativo 15.1.5. Procedimientos de conexión de terminales	
Incumplimiento con controles de seguridad	Falta de conocimiento de seguridad por parte del personal
8.2. Durante el empleo 8.2.2. Conocimiento, educación y entrenamiento de la seguridad de información 8.2.3. Proceso disciplinario 13.1. Divulgación de eventos y de debilidades de la seguridad de la información 13.1.1. Divulgación de eventos de la seguridad de la información 13.2. Administración de incidentes y mejoras de la seguridad de la información 13.2.1. Responsabilidades y procedimientos	
Degradación del HW	Falta de mantenimiento adecuado
9.2. Seguridad de los equipos 9.2.4. Mantenimiento de equipos	
Inautorizada copia de SW o información propietaria	Falta de políticas
5.1. Política de seguridad de la información 5.1.1. Documento de política de seguridad de la información 15.1. Cumplimiento con los requisitos legales 15.1.2. Derechos de propiedad intelectual 15.1.4. Protección de los datos y de la privacidad de la información personal	
Ataque destructivo	Falta de protección física
9.1. Áreas seguras 9.1.1. Perímetro de seguridad física 9.1.2. Controles físicos de entradas 9.1.3. Seguridad de oficinas, despachos y recursos 9.1.4. Protección contra amenazas externas y ambientales	
Robo	Falta de protección física
7.1. Responsabilidad sobre los activos 7.1.1. Inventario de activos 7.1.2. Propiedad de los recursos 7.1.3. Uso aceptable del uso de los recursos 9.1. Áreas seguras 9.1.1. Perímetro de seguridad física 9.1.2. Controles físicos de entradas 9.1.3. Seguridad de oficinas, despachos y recursos 11.3. Responsabilidades de los usuarios 11.3.2. Equipo informático de usuarios desatendido	

PCs DE OFICINA

Amenazas	***Vulnerabilidades***
Acceso no autorizado al equipo	Falta de Protección por desatención de equipos
9.2. Áreas seguras 9.2.5. Seguridad de equipos fuera de los locales de la organización 11.1. Requerimiento de negocios para control de acceso 11.1.1. Política de control de acceso	

11.3. Responsabilidades de los usuarios 11.3.1. Uso de contraseñas 11.3.2. Equipo informático de usuarios desatendido 15.2. Revisiones de la política de seguridad y de la conformidad técnica 15.2.1. Conformidad con la política de seguridad	
Corte de suministro eléctrico o Falla en el aire acondicionado	Funcionamiento no confiable del UPS o funcionamiento no adecuado del aire acondicionado
9.2. Seguridad de los equipos 9.2.2. Utilidades de apoyo 14.1. Aspectos de la gestión de continuidad del negocio 14.1.3. Desarrollo e implantación de planes de contingencia 14.1.5. Prueba, Mantenimiento y reevaluación de los planes	
Incumplimiento con la legislación	Falta de conocimiento de protección de derechos de SW por parte de los empleados
8.2. Durante el empleo 8.2.2. Conocimiento, educación y entrenamiento de la seguridad de información 15.2. Revisiones de la política de seguridad y de la conformidad técnica 15.2.1. Conformidad con la política de seguridad	
Uso no previsto	Falta de las políticas
5.1. Política de seguridad de la información 5.1.1. Documento de política de seguridad de la información 6.1. Organización interna 6.1.4. Proceso de autorización de recursos para el tratamiento de la información 8.1. Seguridad en la definición del trabajo y los recursos 8.1.1. Roles y responsabilidades 8.1.3. Términos y condiciones de la relación laboral 8.2. Durante el empleo 8.2.1. Responsabilidades de administración 8.2.2. Conocimiento, educación y entrenamiento de la seguridad de información 8.2.3. Proceso disciplinario 11.3. Responsabilidades de los usuarios 11.3.1. Uso de contraseñas 11.3.2. Equipo informático de usuarios desatendido 15.1. Control de acceso al sistema operativo 15.1.5. Procedimientos de conexión de terminales	
Incumplimiento con controles de seguridad	Falta de conocimiento de seguridad por parte del personal
8.2. Durante el empleo 8.2.2. Conocimiento, educación y entrenamiento de la seguridad de información 8.2.3. Proceso disciplinario 13.1. Divulgación de eventos y de debilidades de la seguridad de la información 13.1.1. Divulgación de eventos de la seguridad de la información 13.2. Administración de incidentes y mejoras de la seguridad de la información 13.2.1. Responsabilidades y procedimientos	
Degradación del HW	Falta de mantenimiento adecuado
9.2. Seguridad de los equipos 9.2.4. Mantenimiento de equipos	
Inautorizada copia de SW o información propietaria	Falta de políticas
5.1. Política de seguridad de la información 5.1.1. Documento de política de seguridad de la información 15.1. Cumplimiento con los requisitos legales 15.1.2. Derechos de propiedad intelectual 15.1.4. Protección de los datos y de la privacidad de la información personal	
Ataque destructivo	Falta de protección física
9.1. Áreas seguras 9.1.1. Perímetro de seguridad física	

9.1.2. Controles físicos de entradas 9.1.3. Seguridad de oficinas, despachos y recursos 9.1.4. Protección contra amenazas externas y ambientales	
Robo	Falta de protección física
7.1. Responsabilidad sobre los activos 7.1.1. Inventario de activos 7.1.2. Propiedad de los recursos 7.1.3. Uso aceptable del uso de los recursos 9.1. Áreas seguras 9.1.1. Perímetro de seguridad física 9.1.2. Controles físicos de entradas 9.1.3. Seguridad de oficinas, despachos y recursos 11.3. Responsabilidades de los usuarios 11.3.2. Equipo informático de usuarios desatendido	

SERVIDORES

Amenazas	***Vulnerabilidades***
Negación de Servicio	Incapacidad de distinguir una petición real de una falsa
10.6. Gestión de la seguridad de red, 10.6.1. Controles de red 10.6.2. Seguridad de los servicios de red 11.4. Control de acceso a la red 11.4.1. Política de uso de los servicios de la red 11.4.2. Autenticación de usuarios para conexiones externas 11.4.3. Autenticación de nodos de la red 11.4.4. Protección a puertos de diagnóstico remoto 11.4.6. Control de conexión a las redes 12.6. Gestión de Vulnerabilidad Técnica 12.6.1. Control de Vulnerabilidades Técnicas	
Corte de suministro eléctrico o Falla en el aire acondicionado	Funcionamiento no confiable del UPS o funcionamiento no adecuado del aire acondicionado
9.2. Seguridad de los equipos 9.2.2. Utilidades de apoyo 14.1. Aspectos de la gestión de continuidad del negocio 14.1.3. Desarrollo e implantación de planes de contingencia 14.1.5. Prueba, Mantenimiento y reevaluación de los planes	
Acceso no autorizado a través de la red	Código malicioso desconocido
10.6. Gestión de la seguridad de red 10.6.1. Controles de red 10.6.2. Seguridad de los servicios de red 11.4. Control de acceso a la red 11.4.1. Política de uso de los servicios de la red 11.4.2. Autenticación de usuarios para conexiones externas 11.4.3. Autenticación de nodos de la red 11.4.4. Protección a puertos de diagnóstico remoto 11.4.6. Control de conexión a las redes 12.6. Gestión de Vulnerabilidad Técnica 12.6.1. Control de Vulnerabilidades Técnicas	
Degradación o Falla del HW	Falta de mantenimiento adecuado
9.2. Seguridad de los equipos 9.2.4. Mantenimiento de equipos	
Manipulación de la configuración	Falta de control de acceso
9.1.1. Perímetro de seguridad física	

9.1.3. Seguridad de oficinas, despachos y recursos 11.2. Gestión de acceso de usuarios 11.2.2. Gestión de privilegios 11.2.4. Revisión de derechos de acceso de los usuarios 11.5. Control de acceso al sistema operativo 11.5.2. Identificación y autenticación del usuario	
Incumplimiento con controles de seguridad	Falta de conocimiento de seguridad por parte del personal
8.2. Durante el empleo 8.2.2. Conocimiento, educación y entrenamiento de la seguridad de información 8.2.3. Proceso disciplinario 13.1. Divulgación de eventos y de debilidades de la seguridad de la información 13.1.1. Divulgación de eventos de la seguridad de la información 13.2. Administración de incidentes y mejoras de la seguridad de la información 13.2.1. Responsabilidades y procedimientos	
Incapacidad de restauración	Falta de planes de continuidad del negocio
10.5 Gestión interna de respaldo. 10.5.1 Recuperación de la información 14.1. Aspectos de la gestión de continuidad del negocio 14.1.1. Proceso de gestión de la continuidad del negocio 14.1.3. Desarrollo e implantación de planes de contingencia	
Análisis de tráfico	Falta de establecimiento de una conexión segura (VPN)
10.6 Gestión de la seguridad de red. 10.6.1 Controles de red 10.6.2 Seguridad de los servicios de red 11.4. Control de acceso a la red 11.4.2. Autenticación de usuarios para conexiones externas 11.4.4. Protección a puertos de diagnóstico remoto 11.5. Control de acceso al sistema operativo 11.5.2. Identificación y autenticación del usuario 12.6. Gestión de Vulnerabilidad Técnica 12.6.1. Control de Vulnerabilidades Técnicas	
Brechas de seguridad no detectadas	Falta de monitoreo de los servidores
10.10 Monitorización. Objetivo: Detectar actividades no autorizadas. 10.10.2 Monitorización del uso del sistema 10.10.4 Registros del administrador y operador 10.10.5 Registro de fallas 11.4. Control de acceso a la red 11.4.2. Autenticación de usuarios para conexiones externas 11.4.4. Protección a puertos de diagnóstico remoto	
Ataque destructivo	Falta de protección física
9.1. Áreas seguras 9.1.1. Perímetro de seguridad física 9.1.2. Controles físicos de entradas 9.1.3. Seguridad de oficinas, despachos y recursos 9.1.4. Protección contra amenazas externas y ambientales	

EQUIPOS DE OFICINA

Amenazas	***Vulnerabilidades***
Degradación o Falla de HW	Falta de Mantenimiento
9.2. Seguridad de los equipos 9.2.4. Mantenimiento de equipos	
Uso no previsto	Falta de Políticas Falta de Control de Acceso

5.1. Política de seguridad de la información 5.1.1. Documento de política de seguridad de la información 6.1. Organización interna 6.1.4. Proceso de autorización de recursos para el tratamiento de la información 8.1. Seguridad en la definición del trabajo y los recursos 8.1.1. Roles y responsabilidades 8.1.3. Términos y condiciones de la relación laboral 8.2. Durante el empleo 8.2.1. Responsabilidades de administración 8.2.2. Conocimiento, educación y entrenamiento de la seguridad de información 8.2.3. Proceso disciplinario 11.3. Responsabilidades de los usuarios 11.3.1. Uso de contraseñas 11.3.2. Equipo informático de usuarios desatendido 15.1. Control de acceso al sistema operativo 15.1.5. Procedimientos de conexión de terminales

SOPORTE ELECTRÓNICO

Amenazas	***Vulnerabilidades***
Robo	Falta de atención del personal
7.1. Responsabilidad sobre los activos 7.1.1. Inventario de activos 7.1.2. Propiedad de los recursos 7.1.3. Uso aceptable del uso de los recursos 9.1. Áreas seguras 9.1.1. Perímetro de seguridad física 9.1.2. Controles físicos de entradas 9.1.3. Seguridad de oficinas, despachos y recursos 11.3. Responsabilidades de los usuarios 11.3.2. Equipo informático de usuarios desatendido	
Escape de información	Manipulación inadecuada de información
10.7. Utilización de los medios de información 10.7.1. Gestión de medios removibles 10.7.3. Procedimientos de manipulación de la información 11.3. Responsabilidades de los usuarios 11.3.3. Políticas de limpieza de pantalla y escritorio	

DOCUMENTACIÓN Y REGISTROS

Amenazas	***Vulnerabilidades***
Pérdida de información	Errores de los empleados
5.1 Política de seguridad de la información. 5.1.1 Documento de política de seguridad de la información 6.1. Organización interna 6.1.3. Asignación de responsabilidades sobre seguridad de la información 8.1 Seguridad en la definición del trabajo y los recursos. 8.1.1 Roles y responsabilidades 8.2 Durante el empleo. 8.2.2 Conocimiento, educación y entrenamiento de la seguridad de información 13.2. Administración de incidentes y mejoras de la seguridad de la información 13.2.1. Responsabilidades y procedimientos	
Pérdida de información	Errores de los empleados
5.1 Política de seguridad de la información. 5.1.1 Documento de política de seguridad de la información	

6.1 Organización interna. 6.1.3 Asignación de responsabilidades sobre seguridad de la información 8.1 Seguridad en la definición del trabajo y los recursos. 8.1.1 Roles y responsabilidades 8.2 Durante el empleo. 8.2.2. Conocimiento, educación y entrenamiento de la seguridad de información 13.2. Administración de incidentes y mejoras de la seguridad de la información 13.2.1. Responsabilidades y procedimientos	
Pérdida de información	Almacenamiento no protegido
9.1 Áreas seguras. 9.1.1 Perímetro de seguridad física 9.1.3 Seguridad de oficinas, despachos y recursos 11.1. Requerimiento de negocios para control de acceso 11.1.1. Política de control de acceso 13.2. Administración de incidentes y mejoras de la seguridad de la información 13.2.1. Responsabilidades y procedimientos	
Divulgación de información de clientes	Almacenamiento no protegido
9.1 Áreas seguras. 9.1.1 Perímetro de seguridad física 9.1.3 Seguridad de oficinas, despachos y recursos 11.1. Requerimiento de negocios para control de acceso 11.1.1. Política de control de acceso 13.2. Administración de incidentes y mejoras de la seguridad de la información 13.2.1. Responsabilidades y procedimientos 15.1. Cumplimiento con los requisitos legales 15.1.3. Salvaguarda de los registros de la organización 15.1.4. Protección de los datos y de la privacidad de la información personal	
Ataque destructivo	Falta de protección física
9.1. Áreas seguras 9.1.1. Perímetro de seguridad física 9.1.2. Controles físicos de entradas 9.1.3. Seguridad de oficinas, despachos y recursos 9.1.4. Protección contra amenazas externas y ambientales	
Incapacidad de restauración	Falta de planes de continuidad del negocio
10.5. Gestión interna de respaldo.. 10.5.1. Recuperación de la información 14.1. Aspectos de la gestión de continuidad del negocio 14.1.3. Desarrollo e implantación de planes de contingencia	

EMPLEADOS

Amenazas	***Vulnerabilidades***
Errores de los empleados y acciones equivocadas	Falta de conocimiento y oportuno entrenamiento
8.1. Seguridad en la definición del trabajo y los recursos. 8.1.1. Roles y responsabilidades 8.1.2. Selección y política del personal 8.2. Durante el empleo.. 8.2.1. Responsabilidades de administración 8.2.2. Conocimiento, educación y entrenamiento de la seguridad de información 8.2.3. Proceso disciplinario 13.2. Administración de incidentes y mejoras de la seguridad de la información 13.2.1. Responsabilidades y procedimientos	

ESTABLECIMIENTO

Amenazas	*Vulnerabilidades*
Acceso no autorizado	Falta de políticas
5.1. Política de seguridad de la información. 5.1.1. Documento de política de seguridad de la información	
Acceso no autorizado	Falta de protección física
9.1 Áreas seguras. 9.1.2 Controles físicos de entradas 11.1. Requerimiento de negocios para control de acceso 11.1.1. Política de control de acceso 13.1. Divulgación de eventos y de debilidades de la seguridad de la información 13.1.2. Divulgación de debilidades de la seguridad	

SERVICIO DE COMUNICACIONES

Amenazas	*Vulnerabilidades*
Degradación del servicio y equipos	Falta de mantenimiento adecuado
9.2. Seguridad de los equipos 9.2.4. Mantenimiento de equipos	
Uso no previsto	Falta de políticas
5.1. Política de seguridad de la información 5.1.1. Documento de política de seguridad de la información 6.1. Organización interna 6.1.4. Proceso de autorización de recursos para el tratamiento de la información 8.1. Seguridad en la definición del trabajo y los recursos 8.1.1. Roles y responsabilidades 8.1.3. Términos y condiciones de la relación laboral 8.2. Durante el empleo 8.2.1. Responsabilidades de administración 8.2.2. Conocimiento, educación y entrenamiento de la seguridad de información 8.2.3. Proceso disciplinario 11.3. Responsabilidades de los usuarios 11.3.1. Uso de contraseñas 11.3.2. Equipo informático de usuarios desatendido 15.1. Control de acceso al sistema operativo 15.1.5. Procedimientos de conexión de terminales	
Ataque destructivo	Falta de protección física
9.1. Áreas seguras 9.1.1. Perímetro de seguridad física 9.1.2. Controles físicos de entradas 9.1.3. Seguridad de oficinas, despachos y recursos 9.1.4. Protección contra amenazas externas y ambientales	
Fallas de servicios telefonía	Falta de acuerdos bien definidos con terceras partes
10.2 Gestión de servicios externos 10.2.1 Entrega del servicio 10.2.2 Monitorización y revisión de los servicios de las terceras partes	

SERVICIO DE CORREO ELECTRÓNICO

Amenazas	*Vulnerabilidades*
Suplantación de la identidad del usuario	Falta de control de acceso

10.6 Gestión de la seguridad de red 10.6.1 Controles de red 10.6.2 Seguridad de los servicios de red 11.2. Gestión de acceso de usuarios 11.2.1. Registro de Usuarios 11.2.4. Revisión de derechos de acceso de los usuarios	
Análisis de tráfico	Falta de establecimiento de una conexión segura (VPN)
10.6 Gestión de la seguridad de red. 10.6.1 Controles de red 10.6.2 Seguridad de los servicios de red 12.3. Controles criptográficos 12.3.1.Política de uso de los controles criptográficos	
Uso no previsto	Falta de políticas
5.1. Política de seguridad de la información 5.1.1. Documento de política de seguridad de la información 6.1. Organización interna 6.1.4. Proceso de autorización de recursos para el tratamiento de la información 8.1. Seguridad en la definición del trabajo y los recursos 8.1.1. Roles y responsabilidades 8.1.3. Términos y condiciones de la relación laboral 8.2. Durante el empleo 8.2.1. Responsabilidades de administración 8.2.2. Conocimiento, educación y entrenamiento de la seguridad de información 8.2.3. Proceso disciplinario 11.3. Responsabilidades de los usuarios 11.3.1. Uso de contraseñas 11.3.2. Equipo informático de usuarios desatendido 15.1. Control de acceso al sistema operativo 15.1.5. Procedimientos de conexión de terminales	
Fallas de servicios de soporte (telefonía, servicios de Internet)	Falta de acuerdos bien definidos con terceras partes
10.2 Gestión de servicios externos 10.2.1 Entrega del servicio 10.2.2 Monitorización y revisión de los servicios de las terceras partes	

PORTAL DE INFORMACIÓN DE LA CMS

Amenazas	***Vulnerabilidades***
Modificación no autorizada del sitio Web	Falta de procedimientos para cambios
8.1 Seguridad en la definición del trabajo y los recursos. 8.1.1 Roles y responsabilidades 10.1 Procedimientos y responsabilidades de operación. 10.1.1 Documentación de procedimientos operativos 10.1.2 Control de cambios operacionales 11.1. Requerimiento de negocios para control de acceso 11.1.1. Política de control de acceso 11.2. Gestión de acceso de usuarios 11.2.2. Gestión de privilegios 11.4. Control de acceso a la red 11.4.4. Protección a puertos de diagnóstico remoto 12.5. Seguridad en los procesos de desarrollo y soporte 12.5.1. Procedimientos de control de cambios	
Sitio Web no disponible	Fallas en los acuerdos de niveles de servicio
10.2 Gestión de servicios externos. 10.2.1 Entrega del servicio	

10.2.2 Monitorización y revisión de los servicios de las terceras partes

SOFTWARE ESTÁNDAR

Amenazas	***Vulnerabilidades***
Uso no previsto	Falta de políticas de seguridad
5.1. Política de seguridad de la información 5.1.1. Documento de política de seguridad de la información 6.1. Organización interna 6.1.4. Proceso de autorización de recursos para el tratamiento de la información 8.1. Seguridad en la definición del trabajo y los recursos 8.1.1. Roles y responsabilidades 8.1.3. Términos y condiciones de la relación laboral 8.2. Durante el empleo 8.2.1. Responsabilidades de administración 8.2.2. Conocimiento, educación y entrenamiento de la seguridad de información 8.2.3. Proceso disciplinario 11.3. Responsabilidades de los usuarios 11.3.1. Uso de contraseñas 11.3.2. Equipo informático de usuarios desatendido 15.1. Control de acceso al sistema operativo 15.1.5. Procedimientos de conexión de terminales	
Virus de Computación, Fuerza Bruta y ataques de diccionario	Falta de Protección (AV) actualizada
10.4 Protección contra software malicioso. 10.4.1 Controles contra software malicioso 12.5. Seguridad en los procesos de desarrollo y soporte 12.6. Gestión de Vulnerabilidad Técnica 12.6.1. Control de Vulnerabilidades Técnicas 12.5.4. Canales encubiertos y código troyano	
Falta de capacidad de restauración	Falta de copias de backup continuas
10.5 Gestión interna de respaldo.. 10.5.1 Recuperación de la información 14.1. Aspectos de la gestión de continuidad del negocio 14.1.3. Desarrollo e implantación de planes de contingencia	
Pérdida de Servicio	Actualizaciones incorrectas
10.1 Procedimientos y responsabilidades de operación. 10.1.1 Documentación de procedimientos operativos 10.1.2 Control de cambios operacionales 12.5. Seguridad en los procesos de desarrollo y soporte 12.5.1. Procedimientos de control de cambios 12.5.2. Revisión técnica de los cambios en el Sistema Operativo	
Pérdida de Servicio	Instalación de SW no autorizado
10.1 Procedimientos y responsabilidades de operación. 10.1.1 Documentación de procedimientos operativos 10.4 Protección contra software malicioso. 10.4.1 Controles contra software malicioso 12.5. Seguridad en los procesos de desarrollo y soporte 12.5.3. Restricciones en los cambios a los paquetes de SW	
Controles de Seguridad no cumplidos	Falta de Políticas de Seguridad
5.1 Política de seguridad de la información. 5.1.1 Documento de política de seguridad de la información 13.1. Divulgación de eventos y de debilidades de la seguridad de la información 13.1.1. Divulgación de eventos de la seguridad de la información 13.2. Administración de incidentes y mejoras de la seguridad de la información 13.2.1. Responsabilidades y procedimientos 15.2. Revisiones de la política de seguridad y de la conformidad técnica	

15.2.1. Conformidad con la política de seguridad	
Alteración no autorizado de la configuración	Falta de control de acceso
11.1. Requerimiento de negocios para control de acceso 11.1.1. Política de control de acceso 11.2. Gestión de acceso de usuarios 11.2.2. Gestión de privilegios 12.5. Seguridad en los procesos de desarrollo y soporte 12.5.3. Restricciones en los cambios a los paquetes de SW	

MEDIOS Y SOPORTE

Amenazas	***Vulnerabilidades***
Acceso no autorizado a la información	Falta de control de acceso
9.2 Seguridad de los equipos. 9.2.3 Seguridad del cableado 10.6 Gestión de la seguridad de red. 10.6.1 Controles de red 10.6.2 Seguridad de los servicios de red 11.4. Control de acceso a la red 11.4.2. Autenticación de usuarios para conexiones externas 11.4.3. Autenticación de nodos de la red 11.4.4. Protección a puertos de diagnóstico remoto 11.4.6. Control de conexión a las redes 13.2. Administración de incidentes y mejoras de la seguridad de la información 13.2.1. Responsabilidades y procedimientos 15.2. Revisiones de la política de seguridad y de la conformidad técnica 15.2.1. Conformidad con la política de seguridad	
Robo	Falta de protección física
7.1 Responsabilidad sobre los activos. 7.1.1 Inventario de activos 7.1.2 Propiedad de los recursos 7.1.3 Uso aceptable del uso de los recursos 9.2 Seguridad de los equipos. 9.2.3 Seguridad del cableado 13.1. Divulgación de eventos y de debilidades de la seguridad de la información 13.1.1. Divulgación de eventos de la seguridad de la información 13.2. Administración de incidentes y mejoras de la seguridad de la información 13.2.1. Responsabilidades y procedimientos	
Análisis de tráfico	Falta de establecimiento de una conexión segura (VPN)
10.6 Gestión de la seguridad de red. 10.6.1 Controles de red 10.6.2 Seguridad de los servicios de red 12.3. Controles criptográficos 12.3.1. Política de uso de los controles criptográficos	
Brechas de seguridad no detectadas	Falta de monitoreo de la red
10.10 Monitorización. 10.10.2 Monitorización del uso del sistema 10.10.4 Registros del administrador y operador 10.10.5 Registro de fallas	

Una vez seleccionado los controles, podemos realizar la redacción del manual de procedimiento para la implementación del SGSI en base a los controles ya seleccionados.

IV
IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA INTRANET DE LA CORPORACIÓN METROPOLITANA DE SALUD

4.1. MANUAL DE PROCEDIMIENTOS PARA LA IMPLEMENTACIÓN DEL SGSI

A continuación se describe el manual de procedimientos para implementar el SGSI en la Corporación, de los controles seleccionados anteriormente los que no se mencionan en el manual se encuentran detallados en la implementación de los mismos.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Generalidades

La información es un recurso que, como el resto de los activos, tiene valor para el Organismo y por consiguiente debe ser debidamente protegida.
Las Políticas de Seguridad de la Información protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos del Organismo. Es importante que los principios de la Política de Seguridad sean parte de la cultura organizacional.
Para esto, se debe asegurar un compromiso manifiesto de las máximas Autoridades del Organismo y de los titulares de Unidades Organizativas para la difusión, consolidación y cumplimiento de la presente Política.

Objetivo

Proteger los recursos de información del Organismo y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o

accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.
Asegurar la implementación de las medidas de seguridad comprendidas en esta Política. Mantener la Política de Seguridad del Organismo actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

Establecer las directrices, los procedimientos y los requisitos para asegurar la protección oportuna y correcta de los equipos computacionales de la Corporación Metropolitana de Salud y el uso adecuado de los mismos.

Alcance

Esta Política se aplica en todo el ámbito del Organismo, a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.
La finalidad de las políticas de seguridad que se describen en el capítulo 4, es proporcionar instrucciones específicas sobre cómo mantener más seguros tanto los computadores de la Corporación, (conectados o no en red), como la información guardada en ellos. La violación de dichas políticas puede acarrear medidas disciplinarias. Para el desarrollo de las políticas, es necesario considerar las diferentes fuentes de información, que permiten el desempeño diario de las funciones de la corporación. Entre los puntos principales que se deben analizar son: Políticas de seguridad para computadores, comunicaciones
En el cual se debe establecer las directrices, los procedimientos y los requisitos para asegurar la protección oportuna y correcta de los equipos computacionales y sistemas de comunicaciones de la Corporación Metropolitana de Salud y el uso adecuado de los mismos.

El propósito de este manual es establecer las directrices, los procedimientos y los requisitos para asegurar la protección apropiada de la Corporación Metropolitana de Salud al estar conectada a redes de computadoras.

En el desarrollo de estas políticas se debe definir los términos, condiciones y limitantes del servicio de Correo Electrónico Interno y limitantes del servicio de Internet corporativo de la Corporación Metropolitana de Salud.

ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD

Generalidades

Es necesario tener bien definido un marco de gestión para efectuar diferentes tareas tales como la aprobación de la Política, la coordinación de su implementación y la asignación de funciones y responsabilidades, para tener una eficiente administración de la seguridad de información.

Debe tenerse en cuenta que ciertas actividades de la Corporación pueden requerir que terceros accedan a información interna, o bien puede ser necesaria la tercerización de ciertas funciones relacionadas con el procesamiento de la información. En estos casos se considerará que la información puede ponerse en riesgo si el acceso de dichos terceros se produce en el marco de una inadecuada administración de la seguridad, por lo que se establecerán las medidas adecuadas para la protección de la información.

Objetivo

- Administrar la seguridad de la información dentro de la Corporación y establecer un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades.
- Garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información del Organismo.

En este control es necesario definir un Comité de Seguridad que entre sus funciones deberá:

- Revisar y proponer a la máxima autoridad de la Corporación para su aprobación, la Política y las funciones generales en materia de seguridad de la información.

- Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
- Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.
- Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área.
- Acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información.
- Garantizar que la seguridad sea parte del proceso de planificación de la información.
- Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
- Promover la difusión y apoyo a la seguridad de la información dentro del Organismo.
- Coordinar el proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de la información del Organismo frente a interrupciones imprevistas.

Una vez integrado el Comité, es necesario se definan las funciones de los miembros del mismo para poder para que este pueda desempeñar sus actividades y mejorar la seguridad en la Corporación. En la implementación están especificados los miembros del Comité.

El Comité de Seguridad de la Información debe proponer a la Gerencia para su aprobación la definición y asignación de las responsabilidades que surjan de sus funciones.

Es necesario definir el proceso para la autorización de nuevos recursos para el procesamiento de información así como los requerimientos de Seguridad en contratos con Terceros, los principales puntos que se deben considerar lo siguiente:

a) Cumplimiento de la Política de seguridad de la información de la Corporación.
b) Protección de los activos de la Corporación, incluyendo:

- Procedimientos para proteger los bienes de la Corporación, abarcando los activos físicos, la información y el software.
- Procedimientos para determinar si ha ocurrido algún evento que comprometa los bienes, por ejemplo, debido a pérdida o modificación de datos.
- Controles para garantizar la recuperación o destrucción de la información y los activos al finalizar el contrato o acuerdo, o en un momento convenido durante la vigencia del mismo.
- Restricciones a la copia y divulgación de información.

c) Descripción de los servicios disponibles.
d) Nivel de servicio esperado y niveles de servicio aceptables.
e) Permiso para la transferencia de personal cuando sea necesario.
f) Obligaciones de las partes del acuerdo y responsabilidades legales.
g) Definiciones relacionadas con la protección de datos.
h) Acuerdos de control de accesos que contemplen:
    - Métodos de acceso permitidos, y el control y uso de identificadores únicos como identificadores de usuario y contraseñas de usuarios.
    - Proceso de autorización de accesos y privilegios de usuarios.
    - Requerimiento para mantener actualizada una lista de individuos autorizados a utilizar los servicios que han de implementarse y sus derechos y privilegios con respecto a dicho uso.
i) Definición de criterios de desempeño comprobables, de monitoreo y de presentación de informes.
j) Adquisición de derecho a auditar responsabilidades contractuales o surgidas del acuerdo.
k) Establecimiento de un proceso para la resolución de problemas y en caso de corresponder disposiciones con relación a situaciones de contingencia.
l) Responsabilidades relativas a la instalación y al mantenimiento de hardware y software.

m) Estructura de dependencia y del proceso de elaboración y presentación de informes que contemple un acuerdo con respecto a los formatos de los mismos.
n) Proceso claro y detallado de administración de cambios.
o) Controles de protección física requeridos y los mecanismos que aseguren la implementación de los mismos.
p) Métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad.
q) Controles que garanticen la protección contra software malicioso.
r) Elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativos a la seguridad.

GESTIÓN DE LOS ACTIVOS DE RED

Generalidades

La Corporación debe tener conocimiento sobre los activos que posee como parte importante de la administración de riesgos.

Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información.

Objetivo

Garantizar que los activos de información reciban un apropiado nivel de protección. Clasificar la información para señalar su sensibilidad y criticidad. Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

Responsabilidad sobre los activos

Los propietarios de la información son los encargados de clasificarla de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada.

El Responsable de Seguridad Informática es el encargado de asegurar que los lineamientos para la utilización de los recursos de la tecnología de información

contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan.

Cada Propietario de la Información supervisará que el proceso de clasificación y rótulo de información de su área de competencia sea cumplimentado de acuerdo a lo establecido en la Política.

Se identificarán los activos importantes asociados a cada sistema de información, sus respectivos propietarios, para luego elaborar un inventario con dicha información.

El mismo será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad de 4 meses. El encargado de elaborar el inventario y mantenerlo actualizado es cada Responsable de Unidad Organizativa.

En la implementación del manual, se especifica el inventario realizado así como los responsables de cada activo. Una vez realizado el inventario, se debe clasificar el activo, en base a tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad; los cuales se revisaron al inicio de este capítulo. Para clasificar la información se consideró una de las siguientes categorías:

• **CRITICIDAD BAJA**: ninguno de los valores asignados superan el 2.
• **CRITICIDAD MEDIA**: alguno de los valores asignados es 2
• **CRITICIDAD ALTA**: alguno de los valores asignados es 3

Sólo el propietario de la Información puede asignar o cambiar su nivel de clasificación, cumpliendo con los siguientes requisitos previos:
• Asignarle una fecha de efectividad.
• Comunicárselo al depositario del recurso.
• Realizar los cambios necesarios para que los usuarios conozcan la nueva clasificación

SEGURIDAD DE LOS RECURSOS HUMANOS

Generalidades

La seguridad de la información se basa en la capacidad para conservar la integridad, confidencialidad y disponibilidad de los activos.

Para lograr lo anterior es fundamental educar e informar al personal desde su ingreso y en forma continua, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad. Así mismo, es necesario definir las sanciones que se aplicarán en caso de incumplimiento.

Objetivo

Reducir los riesgos de error humano, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.

Indicar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado.

Garantizar que los usuarios estén al corriente de las amenazas en materia de seguridad de la información, y se encuentren capacitados para respaldar la Política de Seguridad de la Corporación en el transcurso de sus tareas normales.

Establecer Compromisos de Confidencialidad con todo el personal y usuarios externos de las instalaciones de procesamiento de información.

Establecer las herramientas y mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia.

Seguridad en la definición del trabajo y los recursos

Las funciones y responsabilidades en materia de seguridad serán incorporadas en la descripción de las responsabilidades de los puestos de trabajo.

Éstas incluirán las responsabilidades generales relacionadas con la implementación y el mantenimiento de la Política de Seguridad, y las

responsabilidades específicas vinculadas a la protección de cada uno de los activos, o la ejecución de procesos o actividades de seguridad determinadas.
En la implementación se especifica el procedimiento para la proceso de selección del personal.

Términos y condiciones de la relación laboral

Los términos y condiciones de empleo establecerán la responsabilidad del empleado en materia de seguridad de la información.
Cuando corresponda, los términos y condiciones de empleo establecerán que estas responsabilidades se extienden más allá de los límites de la sede del Organismo y del horario normal de trabajo.
Los derechos y obligaciones del empleado relativos a la seguridad de la información, por ejemplo en relación con las leyes de Propiedad Intelectual o la legislación de protección de datos, se encontrarán aclarados e incluidos en los términos y condiciones de contrato.

Conocimiento, educación y entrenamiento de la seguridad de información

Todos los empleados de la Corporación y, cuando sea necesario, los usuarios externos y los terceros que desempeñen funciones en la Corporación, deberán recibir una adecuada capacitación y actualización periódica en materia de la política de seguridad, normas y procedimientos para la seguridad. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general, como por ejemplo su estación de trabajo.
El Responsable del Área de Recursos Humanos será el encargado de coordinar las acciones de capacitación que surjan de la Política.
Cada 6 meses se revisará el material correspondiente a la capacitación, a fin de evaluar la pertinencia de su actualización, de acuerdo al estado del arte de ese momento.
El personal que ingrese a la Corporación recibirá el material, indicándosele el comportamiento esperado en lo que respecta a la seguridad de la información,

antes de serle otorgados los privilegios de acceso a los sistemas que correspondan.
Además se otorgará una guía de usuario para que tengan un mejor conocimiento con respecto a las amenazas informáticas y sus posibles consecuencias dentro de la Corporación de tal manera que se llegue a concienciar y crear una cultura de seguridad de la información.

SEGURIDAD FÍSICA Y DEL ENTORNO

Generalidades

La seguridad física y ambiental minimiza los riesgos de daños e interferencias a la información y a las operaciones de la Corporación. Además, trata de evitar al máximo el riesgo de accesos físicos no autorizados, mediante el establecimiento de perímetros de seguridad.
El control de los factores ambientales permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio.
Gran cantidad de información manejada en las oficinas se encuentra almacenada en papel, por lo que es necesario establecer pautas de seguridad para la conservación de dicha documentación.

Objetivo

Prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones e información del Organismo.
Proteger el equipamiento de procesamiento de información crítica del Organismo ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados. Asimismo, contemplar la protección del mismo en su traslado y permanencia fuera de las áreas protegidas.
Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información del Organismo.

Previo a la implementación de un control de seguridad física y del entorno, es necesario que se realice un levantamiento de información de la situación actual de la Corporación en cuanto a su seguridad física para determinar las vulnerabilidades y posibles soluciones.

En puntos previos de este capítulo ya se realizó la recolección de la información necesaria para implementar los controles. En el capítulo 4 se define la implementación de los controles de seguridad física y del entorno.

GESTIÓN DE COMUNICACIONES Y OPERACIONES

Generalidades

Debido a los peligros existentes como software malicioso, virus, troyanos, etc. es importante que se adopten controles para prevenir cualquier tipo de amenazas.

Se debe separar los ambientes de pruebas y de operaciones, establecer procedimientos que garanticen la calidad de los procesos operativos para evitar incidentes producidos por la mala manipulación de información.

Las comunicaciones establecidas permiten el intercambio de información, se deberá establecer controles para garantizar las condiciones de confidencialidad, integridad y disponibilidad de la información que se emite o recibe por los distintos canales.

Objetivo

Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones. Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas.

El administrador de la red debe revisar con el encargado legal de la CMS, todos los contratos y acuerdos con terceros, pues es necesario garantizar la incorporación de consideraciones relativas a la seguridad de la información involucrada en la gestión de los productos o servicios prestados.

En el capítulo siguiente se definen las consideraciones que se deben tener para implementar este control, así como los anexos donde se especifican la implementación que hemos realizado.

Generalidades

Es necesario establecer controles que impidan el acceso no autorizado a los sistemas de información por parte de personal diferente a los que tienen permisos, para lo cual es necesario se implementen procedimientos para controlar la asignación de privilegios de acceso a los diferentes sistemas y aplicativos de la CMS. En estos procedimientos se especifican sugerencias para mejorar el control actual de los accesos de los usuarios a diferentes niveles.

Es importante para la seguridad de la información controlar el acceso a los recursos, y protegerlos contra el acceso no autorizado, modificación o robo.

Para el caso de la CMS se definirán políticas para el control de acceso así como los procedimientos que deben seguirse para poder implementarlos en los sistemas operativos y aplicativos. En los procedimientos considerados se debe tener en cuenta que los mismos consideren identificación, autenticación y autorización de los usuarios.

Objetivo

Entre los principales puntos que se desean cubrir con este control se tienen:

- Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.
- Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.
- Controlar de mejor forma la seguridad en conexiones entre la CMS y los proveedores externos.
- Mantener un registro de eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.

Alcance

En el procedimiento para implementar este control, se define una política de control de acceso que se aplica a todos los usuarios internos y externos que tienen diferentes permisos para acceder a los sistemas de información, red de la CMS, bases de datos.
Asimismo se aplica al personal técnico que define, instala, administra y mantiene los permisos de acceso y las conexiones de red, y a los que administran su seguridad.

POLITICA DE CONTROL DE ACCESO

- Negar el acceso a sistemas de cuentas anónimas o usuarios no identificados
- Limitar o monitorear el uso de cuentas con privilegios especiales
- Suspender o retardar el acceso a sistemas, aplicaciones después de un número de intentos fallidos.
- Remover cuentas obsoletas de usuarios que han dejado la compañía
- Suspender cuentas inactivas después de 30 o 60 días.
- Reforzar un criterio estricto de acceso
- Deshabilitar las configuraciones por defecto, servicios y puertos no requeridos.
- Reemplazar las configuraciones de contraseñas por defecto en las cuentas
- Limitar y monitorear reglas de acceso globales
- Forzar rotación de la contraseña
- Forzar requerimientos de contraseñas
- Sistemas de auditorias y eventos de usuarios y acciones, así como revisión de reportes periódicos.

Si bien el método biométrico es una forma segura de autentificación e identificación, para el caso de la CMS no aplica pues los sistemas a los cuales acceden y son de mayor riesgo es el aplicativo, al cual ingresan los proveedores que se encuentran fuera de la empresa y no resulta cómodo para los usuarios este tipo de metodología además de resultar más costoso.

Contraseñas

El usuario puede generar su contraseña, pero el sistema operativo fuerza al usuario a que el mismo cumpla con ciertos requerimientos, como por ejemplo que contenga un cierto número de caracteres, que incluya caracteres especiales, que no se relaciones con el nombre del usuario de la máquina. Además de mantener un registro de las últimas claves ingresadas, la fecha en la que debe cambiarse.

Si una contraseña trata de ser vulnerada también puede configurarse el registro de intentos fallidos de acceso al sistema con lo cual se puede bloquear el acceso al mismo para de esta manera disminuir el riesgo debido a la vulneración de las contraseñas.

Uso de contraseñas

Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.

Los usuarios deben cumplir las siguientes directivas:

a) Mantener las contraseñas en secreto.
b) Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
c) Seleccionar contraseñas de calidad, de acuerdo a las políticas de seguridad establecidas, en las que básicamente tratan los siguientes puntos:
    1. Sean fáciles de recordar.
    2. No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo nombres, números de teléfono, fecha de nacimiento, etc.
    3. No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.
d) Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.

e) Cambiar las contraseñas provisorias en el primer inicio de sesión (“log on”).
f) Notificar cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

Los usuarios deberán garantizar que los equipos desatendidos sean protegidos adecuadamente. Los equipos instalados en áreas de usuarios, por ejemplo estaciones de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos.

Identificación y Autenticación de los usuarios

Todos los usuarios de la CMS deben tener un identificador único (ID de usuario) solamente para su uso personal exclusivo, de manera que las actividades puedan rastrearse con posterioridad hasta llegar al individuo responsable. Los identificadores de usuario no darán ningún indicio del nivel de privilegio otorgado.

En los casos que se requiere compartir un ID de usuario, tanto el administrador de la red como el responsable de cada área debe autorizar dicha compartición, así como definir el tiempo en el cual se requiere que se comparta el ID, luego del cual se debe eliminar el identificador y los privilegios del mismo.

Restricción del acceso a la información

Los usuarios de sistemas de aplicación, con inclusión del personal de soporte, tendrán acceso a la información y a las funciones de los sistemas de aplicación acorde al procedimiento de asignación de privilegios.

Se aplicarán los siguientes controles, para brindar apoyo a los requerimientos de limitación de accesos:

a) Proveer una interfaz para controlar el acceso a las funciones de los sistemas de aplicación, para lo cual el administrador de la red debe manejar los privilegios de acuerdo al perfil del usuario y con los requerimientos realizados formalmente por el responsable de cada área.

b) Restringir el conocimiento de los usuarios acerca de la información o de las funciones de los sistemas de aplicación a las cuales no sean autorizados a acceder, con la adecuada edición de la documentación de usuario.
c) Controlar los derechos de acceso de los usuarios, por ejemplo, lectura, escritura, supresión y ejecución.
d) Garantizar que las salidas de los sistemas de aplicación que administran información sensible, contengan sólo la información que resulte pertinente para el uso de la salida, y que la misma se envíe solamente a las terminales y ubicaciones autorizadas.
e) Revisar periódicamente dichas salidas a fin de garantizar la remoción de la información redundante.
f) Restringir el acceso a la información por fuera del sistema encargado de su procesamiento, es decir, la modificación directa del dato almacenado.

Protección de los puertos de diagnóstico remoto

Muchas computadoras y sistemas de comunicación son instalados y administrados con una herramienta de diagnóstico remoto. Si no están protegidos, estos puertos de diagnóstico proporcionan un medio de acceso no autorizado. Por consiguiente, serán protegidos por un mecanismo de seguridad apropiado, por lo cual lo primero que debemos determinar es el diagnóstico de que puertos se encuentran abiertos en la red.

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Generalidades

En este control se deben revisar las aplicaciones como puntos críticos de vulnerabilidades, es necesaria una adecuada administración de la infraestructura de base, Sistemas Operativos y Software de Base, en las distintas plataformas, para asegurar una correcta implementación de la seguridad, ya que en general los aplicativos se asientan sobre este tipo de software.

Objetivo

Con este control se pretende cubrir varios puntos de seguridad, entre los principales objetivos se tienen:

- Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.
- Definir los métodos de protección de la información crítica o sensible.

Alcance

Los controles que se detallan a continuación se aplican a los sistemas informáticos, y a los sistemas operativos que integran los ambientes por el organismo de donde residen los mismos.

Para implementar un mayor control a la información confidencial o importante de los diferentes departamentos de la CMS.

Se debe entender como información confidencial a toda información que se refiere a planes de negocio, tecnología no anunciada, información financiera no pública; e información personal como son tarjetas de crédito, contraseñas.

La CMS debe tener aprobado un procedimiento de cambios aprobado por la gerencia, y los cambios deben ser documentados y comunicados a los empleados involucrados. En la implementación se especifica el proceso para llevar a cabo un cambio.

Revisión técnica de los cambios en el sistema operativo

Toda vez que sea necesario realizar un cambio en el Sistema Operativo, los sistemas serán revisados para asegurar que no se produzca un impacto en su funcionamiento o seguridad.

Para ello, el administrador de la red debe tener un procedimiento en el cual se incluye:

a) Revisar los procedimientos de integridad y control de aplicaciones para garantizar que no hayan sido comprometidas por el cambio.

b) Garantizar que los cambios en el sistema operativo sean informados con anterioridad a la implementación. Para lo cual el administrador debe planificar el día en el cual se llevará a cabo el cambio e informarlo a los usuarios y coordinar con los responsables de cada área en caso de que ellos deban realizar algún trabajo por el cual no pueden suspender sus actividades. Estos cambios deben programarse para fines de semana donde no haya impacto en los usuarios.

c) Asegurar la actualización del Plan de Continuidad de las Actividades del Organismo.

Restricción del cambio de paquetes de Software

En caso de considerarlo necesario la modificación de paquetes de software suministrados por proveedores, y previa autorización del Responsable del Área Informática, se deberá:

a) Analizar los términos y condiciones de la licencia a fin de determinar si las modificaciones se encuentran autorizadas.

b) Determinar la conveniencia de que la modificación sea efectuada por la CMS, por el proveedor o por un tercero.

c) Evaluar el impacto que se produce si la CMS se hace cargo del mantenimiento.

d) Retener el software original realizando los cambios sobre una copia perfectamente identificada, documentando exhaustivamente por si fuera necesario aplicarlo a nuevas versiones.

Este es un punto que debe ser analizado con todos los responsables de las áreas y el administrador de la red, deben realmente aprobar los cambios que implica varios procedimientos como son en el ámbito legal, financiero, recursos, etc.

Canales encubiertos y código

Un canal oculto puede exponer información utilizando algunos medios indirectos y desconocidos. El código malicioso está diseñado para afectar a un sistema en forma no autorizada y no requerida por el usuario.

Para lo cual es necesario que la corporación cuente con un software adecuado instalado en cada máquina de los empleados para evitar problemas debido a canales encubiertos y código troyano.

Además de las medidas implementadas con el antivirus, es necesario que previo la instalación de algún software en la CMS se deba considerar:

a) Adquirir programas a proveedores acreditados o productos ya evaluados.
b) Examinar los códigos fuentes (cuando sea posible) antes de utilizar los programas.
c) Controlar el acceso y las modificaciones al código instalado.
d) Utilizar herramientas para la protección contra la infección del software con código malicioso, en este caso la CMS utilizó el antivirus Symantec.

GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION

Divulgación de eventos y de debilidades de la seguridad de la información

Es importante que la CMS tenga un procedimiento a seguir cuando se presente un incidente de seguridad en la red, pues es necesario que pueda aprender de los errores y evitar que un ataque ocurra. Por lo cual es importante que luego de cada incidente siga un procedimiento, técnicas, configuraciones necesarias para reforzar lo modificado y mejorar la seguridad.

Es necesario que se tenga un mejor control del uso apropiado de los recursos de la red, en otros términos, todos los recursos de la informática deben usarse de una manera ética y responsable. El uso de recursos de tecnología de información puede categorizarse ampliamente como aceptable, tolerable, o prohibió:

- El uso aceptable de recursos de tecnología de información es el uso legal consistente con los requerimientos de la organización, en base a las políticas de la misma que permitan solventar los problemas de la Corporación.
- El uso tolerable es el uso legal para otros propósitos que no chocan con en la política del uso aceptable de la organización.

- El uso prohibido es el uso ilegal y todo el otro uso que son aceptables " ni tolerables.

Administración de incidentes y mejoras de la seguridad de la información

Después que el incidente ha sido resuelto, es necesario realizar una documentación del mismo para poder determinar las experiencias aprendidas del mismo. Como resultado de un análisis posterior al reporte de incidentes, el personal de seguridad puede necesitar emitir alarmas o advertencias a todos los empleados de la CMS sobre las acciones tomar para reducir vulnerabilidades que se explotaron durante el incidente.

Entre estas alertas es importante que se especifique de forma clara:

- Asegurar que sólo personal autorizado tiene el acceso a los archivos electrónicos.
- Minimizar el riesgo de modificación desautorizado de archivos electrónicos guardando los datos sensibles en los medios de comunicación trasladables.
- Asegurar que personal apropiado se entrena para proteger los archivos electrónicos sensibles o clasificados
- Proveer del respaldo y recuperación de archivos para proteger contra la pérdida de información
- Asegurar que la seguridad de los archivos electrónicos esté incluido en los planes de seguridad de información globales de su organización.

GESTION DE CONTINUIDAD DEL NEGOCIO

Generalidades

Un punto importante para toda organización, es administrar de forma ordenada las actividades necesarias para la continuidad del negocio, en este procedimiento se deben involucrar a todos los empleados de la CMS.

El plan de continuidad debe mantenerse actualizado y ser una parte integrada en los diversos procesos de los diferentes departamentos de la CMS.

Objetivo

Este control es importante para cubrir los puntos críticos de la CMS en caso de algún desastre, a continuación se detallan los principales objetivos:

- Analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro.
- Maximizar la efectividad de las operaciones de contingencia del Organismo con el establecimiento de planes que incluyan al menos las siguientes etapas:
    a) Detección y determinación del daño y la activación del plan.
    b) Restauración temporal de las operaciones y recuperación del daño producido al sistema original.
    c) Restauración de las capacidades de proceso del sistema a las condiciones de operación normales.
- Asignar funciones para cada actividad definida.

Alcance

Estos controles se aplican a los críticos de la CMS.

Aspectos de la gestión de continuidad del negocio

Al desarrollar el plan de la continuidad del negocio para la CMS, se debe considerar los parámetros sobre los cuales se va a desarrollar el mismo para poder los desastres. Para este caso cuando se realizó en análisis de riesgos y vulnerabilidades se consideraron diferentes tipos de desastres como son:

Desastres naturales:

- Inundaciones
- Terremotos
- Fuego
- Derrumbamientos, avalanchas, y otros movimientos de la tierra

Desastres artificiales, es decir aquellos relacionados con la computación:

- Sabotaje de los sistemas informáticos, y de la información
  Ataques terroristas
- Huelgas
- Protestas
- Ataque de Negación de Servicio en los servidores de la red
- Virus, gusanos, y otros ataques informáticos

Y finalmente se debe considerar un tercer grupo:

- Faltas de la infraestructura (interrupciones para uso general, interrupciones de la energía, etc.)
- Fallas de comunicaciones (hardware interno y externo, así como software y redes)
- Interrupciones del transporte (encierros o limitaciones del aeropuerto, encierros del camino, etc.)

Una vez identificados los tipos de desastres la empresa debe seguir y desarrollar un plan para asegurar la viabilidad a largo plazo de la CMS, es necesario que la gerencia se involucre en la elaboración del plan, pero es el Comité de Seguridad de la Información que determina que tipos de planes son aplicables pues se requiere de financiamiento de los mismos.

Las pruebas son útiles si reflejan también condiciones reales y si los resultados de la prueba se utilizan para mejorar el plan.
Es importante comenzar con un plan simple para probar y después aumentar el alcance de la prueba gradualmente. Para cada caso es importante:

- Identifique el alcance y las metas para la prueba.
- Documente el plan de prueba y los resultados.
- Repase los resultados con los participantes y prepare las lecciones aprendidas de la prueba.
- Ponga al día el plan basado en los resultados de la prueba.

Proceso de gestión de la continuidad del negocio

Para sobrevivir, la organización debe asegurar el funcionamiento de aplicaciones críticas en un tiempo razonable, frente a un desastre. Las organizaciones necesitan entrenar a sus empleados para ejecutar los planes de contingencia, para lo cual se requiere:

- Que los empleados sean consientes de la necesidad del plan
- Informar a todos los empleados de la existencia del plan y proporcionar los procedimientos para seguir en caso de una emergencia
- Entrenar al personal con las responsabilidades identificadas para cada uno de ellos, para realizar la recuperación del desastre y procedimientos de continuidad de negocio
- Dar la oportunidad para que se pueda llevar a cabo el plan de contingencia, para poder realizar un simulacro de la forma en la que se ejecuta el mismo.

Desarrollo e implantación de planes de contingencia

Al desarrollar el plan se debe tener bien definido y especificado las responsabilidades ha asignarse a cada persona responsable de un proceso determinado, para el caso de la CMS se debe considerar los siguientes responsables:

- Personal encargado de la administración de la recuperación.- El cual debe actuar el momento en el cual se presente el desastre, y cuyo trabajo consiste en ejecutar el plan de recuperación de desastre y restaurar los procesos críticos en el menor tiempo, para este caso es el Comité de Seguridad.

- Personal operacional. Son aquellos que están encargados de la operación del negocio hasta que las cosas vuelvan a la normalidad, estas personas tienen responsabilidades cotidianas y desarrollan las mismas funciones bajo circunstancias normales.

- Personal de las comunicaciones. Personal que diseña los medios de comunicar la información a los empleados, a los clientes, y al público en general. Son los encargados de considerar qué información puede darse y por quién. Esto es crítico en los primeros días de una interrupción pues habrá una mayor demanda para la información, y ocurre en un momento en que los canales normales son interrumpidos por daños en los mismos.

Una vez que se encuentra definido el personal necesario para los diferentes procesos del plan, es necesario que se realicen pruebas del mismo. Pues un plan que no ha sido probado puede presentar fallas en el momento de su ejecución. Las pruebas no deben ser costosas ni interrumpir la operación diaria del negocio. Entre las pruebas que se pueden considerar son:

- Prueba de papel. Esto puede ser tan simple como discutir el plan en una reunión del personal considerando sucesos actuales. Es importante documentar la discusión y utilizar cualquier lección aprendida como parte del proceso para mejorar el plan.

- Camino Estructurado. Aquí es donde el personal define diversos panoramas para supervisar el plan en equipo.

- Prueba de componentes. En esta prueba, cada parte del plan total se puede probar independientemente. Los resultados entonces se miran para considerar cómo el plan total pudo haber trabajado si todos los componentes fueron probados simultáneamente.

- Simulación. No incluye realmente la mudanza a una localización alterna sino puede incluir la simulación de interrupciones para uso general como manera de ver que tan completo es un plan.

- Ejercicio de la recuperación del desastre. En esta prueba, se activa el plan y los sistemas informáticos se cambian a sus sistemas de reserva,

que pueden incluir el funcionamiento en los sitios alternativos. Esto a veces se llama una prueba "paralela" pues los sistemas de producción seguirán siendo funcionales mientras que los sistemas de la recuperación se ponen en producción para probar su funcionalidad.

CUMPLIMIENTO

Generalidades

Los controles implementados en puntos anteriores deben ser complementados con regulaciones de disposiciones legales y contractuales que están actualmente rigiendo en el país. Pero es necesario definir internamente de forma clara los requisitos normativos y contractuales pertinentes a cada sistema de información de la CMS.

Objetivos

Entre los principales puntos a cubrir se tienen:

- Cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas al Organismo y/o al empleado o que incurran en responsabilidad civil o penal como resultado de su incumplimiento.
- Garantizar que los sistemas cumplan con la política, normas y procedimientos de seguridad del Organismo.

Alcance

Este control se aplica a todo el personal de la CMS.

Derechos de propiedad intelectual

Es necesario para toda organización conocer las leyes para no tener problemas futuros debido a incumplimiento de las mismas.
La infracción a estos derechos podrían dar como resultado acciones legales que derivarían en demandas penales.
Se deberán tener presentes las siguientes normas:

• Ley de Propiedad Intelectual Nº 83, Registro Oficial 320 de 19 de Mayo de 1998: Protege los derechos de autor de las obras científicas, literarias y artísticas, incluyendo los programas de computación fuente y objeto; las compilaciones de datos o de otros materiales.

Salvaguarda de los registros de la organización

Los registros críticos de la CMS se deben proteger contra pérdida, destrucción y posibles falsificaciones.

Para un mejor control los registros van a clasificarse dependiendo del área y el uso de cada departamento; además de detallar la forma de almacenamiento, el responsable de cada registro y el período de retención, es decir el tiempo que debe transcurrir antes de que sean destruidos.

Es necesario tener presentes las siguientes normas:

• Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos Nº 2002 - 67: De esta ley se deben considerar diferentes artículos como son:

"Art. 5.- Confidencialidad y reserva.- Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta Ley y demás normas que rigen la materia."

"Art. 9.- Protección de datos.- Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros…. El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo."

Protección de los datos y de la privacidad de la información personal

Todos los empleados deberán conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan conocimiento con motivo del ejercicio de sus funciones.

Para mejorar este punto, en la CMS se debe redactar Compromiso de Confidencialidad, el cual deberá ser suscrito por todos los empleados.
Mediante este instrumento el empleado se comprometerá a utilizar la información solamente para el uso específico al que se ha destinado y a no comunicar, diseminar o de alguna otra forma hacer pública la información a ninguna persona, firma, compañía o tercera persona, salvo autorización previa y escrita del Responsable del Activo de que se trate.
Es necesario tener presentes las siguientes normas:
• Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos Nº 2002 - 67: De esta ley se deben considerar diferentes artículos como son:

“Art. 57.- Infracciones informáticas.- Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley.

Reformas al Código Penal

Art. 58.- A continuación del Art. 202, inclúyanse los siguientes artículos innumerados:

"Art. ....- El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica.

La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, serán sancionada con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Si la divulgación o la utilización fraudulenta se realizan por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Art. ....- Obtención y utilización no autorizada de información.- La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica.".

Evitar el mal uso de los recursos de tratamiento de la información

Los recursos de procesamiento de información del Organismo se suministran con un propósito determinado. Toda utilización de estos recursos con propósitos no autorizados o ajenos al destino por el cual fueron provistos debe ser considerada como uso indebido.
Todos los empleados deben conocer el alcance preciso del uso adecuado de los recursos informáticos y deben respetarlo.

Revisiones de la política de seguridad y de la conformidad técnica

Conformidad con la política de seguridad

Cada Responsable de Unidad Organizativa, velará por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos, dentro de su área de responsabilidad.

4.2. IMPLEMENTACIÓN DEL PLAN DE TRATAMIENTO DE RIESGOS

El objetivo de este punto es tomar la acción más apropiada de tratamiento para cada uno de los riesgos identificados, en base al cuadro anterior y al capítulo anterior donde se encontraba la valoración de los riesgos:

Tabla 4.1 Tratamiento de Riesgos

ACTIVOS	AMENAZAS	VULNERABILIDADES	PTR
Hardware Portátil	Fuego	Falta de protección contra fuego	Reducción
	Daños por agua	Falta de protección física adecuada	Aceptación
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptación
	Acceso no autorizado a la portátil	Falta de Protección por desatención de equipos	Reducción
	Corte de suministro eléctrico o Falla en el aire acondicionado	Funcionamiento no confiable del UPS o funcionamiento no adecuado del aire acondicionado	Reducción
	Instalación no autorizada o cambios de Software	Falta de control de acceso	Reducción
	Incumplimiento con la legislación	Falta de conocimiento de protección de derechos de SW por parte de los empleados	Reducción
	Uso no previsto	Falta de las políticas	Reducción
	Incumplimiento con controles de seguridad	Falta de conocimiento de seguridad por parte del personal	Reducción
	Degradación del HW	Falta de mantenimiento adecuado	Reducción
	Inautorizada copia de SW o información propietaria	Falta de políticas	Reducción
	Ataque destructivo	Falta de protección física	Reducción
	Robo	Falta de protección física	Reducción
PCs de oficina	Fuego	Falta de protección contra fuego	Reducción
	Daños por agua	Falta de protección física adecuada	Aceptación
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptación
	Acceso no autorizado al equipo	Falta de Protección por desatención de equipos	Reducción
	Corte de suministro eléctrico o Falla en el aire acondicionado	Funcionamiento no confiable del UPS o funcionamiento no adecuado del aire acondicionado	Reducción
	Instalación no autorizada o cambios de Software	Falta de control de acceso	Reducción

	Incumplimiento con la legislación	Falta de conocimiento de protección de derechos de SW por parte de los empleados	Reducción
	Uso no previsto	Falta de las políticas	Reducción
	Incumplimiento con controles de seguridad	Falta de conocimiento de seguridad por parte del personal	Reducción
	Degradación del HW	Falta de mantenimiento adecuado	Reducción
	Inautorizada copia de SW o información propietaria	Falta de políticas	Reducción
	Ataque destructivo	Falta de protección física	Reducción
	Robo	Falta de protección física	Reducción
Servidores	Fuego	Falta de protección contra fuego	Reducción
	Daños por agua	Falta de protección física adecuada	Aceptación
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptación
	Corrupción de archivos de registros	Falta de Protección de los archivos de registro	Reducción
	Negación de Servicio	Incapacidad de distinguir una petición real de una falsa	Reducción
	Corte de suministro eléctrico o Falla en el aire acondicionado	Funcionamiento no confiable del UPS o funcionamiento no adecuado del aire acondicionado	Reducción
	Acceso no autorizado a través de la red	Código malicioso desconocido	Reducción
	Degradación o Falla del HW	Falta de mantenimiento adecuado	Reducción
	Manipulación de la configuración	Falta de control de acceso	Reducción
	Incumplimiento con controles de seguridad	Falta de conocimiento de seguridad por parte del personal	Reducción
	Incapacidad de restauración	Falta de planes de continuidad del negocio	Reducción
	Análisis de tráfico	Falta de establecimiento de una conexión segura (VPN)	Reducción
	Brechas de seguridad no detectadas	Falta de monitoreo de los servidores	Reducción
	Ataque destructivo	Falta de protección física	Reducción
Equipos de Oficina	Fuego	Falta de protección contra fuego	Reducción
	Daños por agua	Falta de protección física adecuada	Aceptación
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptación
	Degradación o Falla de HW	Falta de Mantenimiento	Reducción
	Ataque destructivo	Falta de protección física	Reducción
	Uso no previsto	Falta de Políticas Falta de Control de Acceso	Reducción
Soporte	Fuego	Falta de protección contra	Reducción

electrónico		fuego	
	Daños por agua	Falta de protección física adecuada	Aceptación
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptación
	Condiciones inadecuadas de temperatura y/o humedad	Susceptibidad al calor y humedad	Aceptación
	Ataque destructivo	Falta de protección física	Reducción
	Robo	Falta de atención del personal	Reducción
	Escape de información	Manipulación inadecuada de información	Reducción
Documentación y Registros.	Fuego	Falta de protección contra fuego	Reducción
	Daños por agua	Falta de protección física adecuada	Aceptación
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptación
	Pérdida de información	Errores de los empleados	Reducción
	Pérdida de información	Almacenamiento no protegido	Reducción
	Divulgación de información de clientes	Almacenamiento no protegido	Reducción
	Incumplimiento de leyes en cuanto a la información de clientes o empleados	Falta de conocimiento de los empleados	Reducción
	Incorrecta o incompleta documentación del sistema	Falta de documentación actualizada del sistema	Reducción
	Contratos incompletos	Falta de control para el establecimiento de contratos	Reducción
	Ataque destructivo	Falta de protección física	Reducción
	Incapacidad de restauración	Falta de planes de continuidad del negocio	Reducción
	Modificación no autorizada de información	Insuficiente entrenamiento de empleados	Reducción
Empleados	Errores de los empleados y acciones equivocadas	Falta de conocimiento y oportuno entrenamiento	Reducción
	Insuficiente personal	Falta de acuerdos definidos para reemplazo de empleados	Reducción
	Divulgación de información confidencial	Falta de acuerdos de confidencialidad	Reducción
Establecimientos	Fuego	Falta de protección contra fuego	Reducción
	Daños por agua	Falta de protección física adecuada	Aceptación
	Acceso no autorizado	Falta de políticas	Reducción
	Acceso no autorizado	Falta de protección física	Reducción
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptación
Servicio de Comunicaciones	Fuego	Falta de protección contra fuego	Reducción
	Daños por agua	Falta de protección física adecuada	Aceptación

	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptación
	Degradación del servicio y equipos	Falta de mantenimiento adecuado	Reducción
	Errores de configuración	Falta de conocimiento del administrador	Reducción
	Manipulación de la configuración	Falta de control de acceso	Reducción
	Uso no previsto	Falta de políticas	Reducción
	Ataque destructivo	Falta de protección física	Reducción
	Fallas de servicios telefonía	Falta de acuerdos bien definidos con terceras partes	Reducción
Servicio de energía eléctrica	Fuego	Falta de protección contra fuego	Reducción
	Daños por agua	Falta de protección física adecuada	Reducción
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptación
	Ataque destructivo	Falta de protección física	Aceptación
Servicio de correo electrónico	Errores de los usuarios	Falta de conocimiento del uso del servicio	Reducción
	Suplantación de la identidad del usuario	Falta de control de acceso	Reducción
	Análisis de tráfico	Falta de establecimiento de una conexión segura (VPN)	Reducción
	Uso no previsto	Falta de políticas	Reducción
	Fallas de servicios de soporte (telefonía, servicios de Internet)	Falta de acuerdos bien definidos con terceras partes	Reducción
Aplicación Oracle	Errores de usuarios	Falta de conocimiento para el uso de la aplicación	Reducción
	Errores de configuración	Falta de capacitación del administrador del sistema	Reducción
	Escapes de información	Falta de control de acceso	Reducción
	Errores de actualización del programa	Falta de procedimientos aprobados	Reducción
	Manipulación de la configuración	Falta de control de acceso	Aceptación
	Suplantación de identidad del usuario	Falta de control de acceso	Reducción
	Abuso de privilegios de acceso	Falta de políticas de seguridad	Reducción
	Negación de servicio	Incapacidad para distinguir una petición real de una petición falsificada	Reducción
Portal de información (Página Web de la empresa)	Modificación no autorizada del sitio Web	Falta de procedimientos para cambios	Reducción
	Negación de servicio	Falta de recursos necesarios	Reducción
	Sitio Web no disponible	Fallas en los acuerdos de niveles de servicio	Reducción
	Publicación de información incorrecta de la CMS	Falta de procedimiento aprobados	Reducción
Suministros de	Fuego	Falta de protección contra fuego	Reducción

Oficina	Daños por agua	Falta de protección física adecuada	Aceptación
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptación
	Robo	Falta de atención	Reducción
	Robo	Falta de protección física	Reducción
Imagen de la empresa Reputación	Divulgación de datos de los clientes	Insuficiente seguridad de información de los clientes	Reducción
Paquetes o software estándar	Negación de Servicio	Capacidad insuficiente de los recursos	Reducción
	Virus de Computación, Fuerza Bruta y ataques de diccionario	Falta de Protección(AV) actualizada	Reducción
	Spoofing, Escape de información	Falta de control de acceso	Reducción
	Falta de capacidad de restauración	Falta de copias de backup continuas	Reducción
	Uso no previsto	Falta de políticas de seguridad	Reducción
Sistemas operatives	Negación de Servicio	Capacidad insuficiente de los recursos	Reducción
	Errores de Configuración	Falta de capacitación del administrador	Reducción
	Errores de Configuración	Incompleto o incorrecto documentación del sistema	Reducción
	Virus de Computación, Fuerza Bruta y ataques de diccionario	Falta de Protección (AV) actualizada	Reducción
	Falta de capacidad de restauración	Falta de copias de backup continuas	Reducción
	Pérdida de Servicio	Actualizaciones incorrectas	Reducción
	Pérdida de Servicio	Instalación de SW no autorizado	Reducción
	Controles de Seguridad no cumplidos	Falta de Políticas de Seguridad	Reducción
	Alteración no autorizado de la configuración	Falta de control de acceso	Reducción
Medios y soporte	Acceso no autorizado a la información	Falta de control de acceso	Reducción
	Robo	Falta de protección física	Reducción
	Daños de cables	Falta de protección física	Aceptación
	Análisis de tráfico	Falta de establecimiento de una conexión segura (VPN)	Reducción
	Brechas de seguridad no detectadas	Falta de monitoreo de la red	Reducción

En el siguiente punto describimos el resultado de nuestro plan para poder implementar el Sistema de Gestión de Seguridad de Información en base a la Norma ISO 27001 en la CMS.

4.3. IMPLEMENTACIÓN DE LOS CONTROLES SELECCIONADOS ACORDE AL MANUAL DE PROCEDIMIENTOS

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Documento de política de seguridad de la información

1.- Seguridad lógica

Identificación

Para dar de alta un usuario al sistema debe existir un procedimiento formal, por escrito, que regule y exija el ingreso de los siguientes datos:

- Identificación del usuario, deberá ser única e irrepetible,
- Password, debe ser personal e ingresado por el usuario,
- Nombre y apellido completo,
- Grupo de usuarios al que pertenece,
- Fecha de expiración del password,
- Fecha de anulación de la cuenta,
- Contador de intentos fallidos,
- Autorización de imprimir,
- Autorización de ingreso al área de usuarios.

Deben asignarse los permisos mínimos y necesarios para que cada usuario desempeñe su tarea.

Deberá restringirse el acceso al sistema o la utilización de recursos en un rango horario definido, teniendo en cuenta que:

- Las cuentas de los usuarios no deben poder acceder al sistema en horarios no laborales, de acuerdo al grupo al que pertenezcan,
- Durante las vacaciones o licencias las cuentas de usuarios deben desactivarse,

La contraseña asociada al acceso de un identificador de usuario a un computador significa la primera verificación de su identidad, permitiendo posteriormente el acceso al computador y a la información que allí reside. Para su protección y de los recursos de la CMS debe mantener su contraseña de verificación de identidad en secreto, no compartirla con persona alguna.
Nota: La contraseña de disco duro es usada para proteger su equipo contra accesos no autorizados, mas no es una contraseña de verificación.

El administrador del sistema deberá realizar un chequeo mensual de los usuarios del sistema, comprobando que existen solo los usuarios que son necesarios y que sus permisos sean los correctos.

El área de recursos humanos deberá comunicar al administrador los cambios de personal que se produzcan. Luego de esta notificación el Administrador de Sistemas debe revocar rápidamente la cuenta o los privilegios de un usuario cuando reciba una orden de un superior.
Cuando un empleado es despedido o renuncia a la CMS, debe desactivarse su cuenta antes de que deje el cargo.

El sistema deberá finalizar toda sesión interactiva cuando la terminal desde donde se esté ejecutando no verifique uso durante un período de cinco minutos, deberá deslogear al usuario y limpiar la pantalla.
Las PC´s deben tener instalado un protector de pantalla con contraseña.
Se debe bloquear el perfil de todo usuario que no haya accedido al sistema durante un período razonable de tiempo.

Se deberá impedir la existencia de perfiles de usuarios genéricos, en todos los sistemas operativos y en el sistema informático de la Empresa. Es decir se prohíbe el uso de cuentas anónimas o de invitado (guest) y los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad. Esto también implica que los administradores de sistemas Unix no deben entrar inicialmente como root, sino primero empleando su propio ID y luego mediante set user id para obtener el acceso como root.

Se deberá minimizar la generación y el uso de perfiles de usuario con máximos privilegios. Estos privilegios, tal como la posibilidad de modificar o borrar los archivos de otros usuarios, sólo deben otorgarse a aquellos directamente responsable de la administración o de la seguridad de los sistemas.

Cuando un usuario recibe una nueva cuenta, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad, y acepta sus responsabilidades con relación al uso de esa cuenta.
La solicitud de una nueva cuenta o el cambio de privilegios debe ser hecha por escrito y debe ser debidamente aprobada.

No debe concederse una cuenta a personas que no sean empleados de la CMS a menos que estén debidamente autorizados, en cuyo caso la cuenta debe expirar automáticamente al cabo de un lapso de 30 días.

Contraseñas
Las reglas de contraseña listadas a continuación están de acuerdo a los requerimientos y estándares internacionales.

La contraseña de verificación de identidad no debe ser trivial o predecible, y debe:

- Ser de al menos 8 caracteres de longitud
- Contener una combinación de caracteres alfabéticos y no alfabéticos (números, signos de puntuación o caracteres especiales) o una combinación de al menos dos tipos de caracteres no alfabéticos.
- No contener su user ID como parte la contraseña.

Sistemas y aplicaciones de la CMS que contengan información clasificada CMS Confidencial requieren que Ud. cambie la contraseña al menos cada tres meses (90 días). Para los casos en los cuales los sistemas o aplicaciones no cuenten con controles técnicos que obliguen al cambio de contraseña, es su responsabilidad cumplir con este requerimiento. Cuando cambie la contraseña

debe seleccionar uno(a) nuevo(a). El password ingresado sea diferente a los últimas cinco utilizados.
Bloquear el perfil de todo usuario que haya intentado acceder al sistema en forma fallida por más de cinco veces consecutivas.
El usuario debe poder modificar su password cuantas veces considere necesario, sin seguir ningún procedimiento formal de aviso.

La contraseña inicial emitida a un nuevo usuario sólo debe ser válida para la primera sesión. En ese momento, el usuario debe escoger otra contraseña.

Las contraseñas predefinidas que traen los equipos nuevos tales como routers, switchs, etc., deben cambiarse inmediatamente al ponerse en servicio el equipo.

El usuario no debe guardar su contraseña en una forma legible en archivos en disco, y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente.

2 - Seguridad de comunicaciones

Topología de red
Deberá existir documentación detallada sobre los diagramas topológicos de la red.

Deberán existir medios alternativos de transmisión en caso de que alguna contingencia afecte al medio primario de comunicación.
Con respecto a la utilización del correo electrónico deben almacenarse datos sobre:

- Correo entrante y saliente,
- Hora de envío,
- Contenido del mail,
- Asunto del mail,

- Archivos adjuntos,
- Reporte de virus de cada parte del mail,
- Direcciones de máquina destino y fuente,
- Tamaño del mensaje.

Con respecto a la utilización de la red informática deben almacenarse datos sobre:

- Ancho de banda utilizado y cuellos de botella en el tráfico de red,
- Tráfico generado por las aplicaciones,
- Recursos de los servidores que utilizan las aplicaciones,
- El estado de cada aplicación, (en cola, ejecutándose, esperando una respuesta),
- Intentos de intrusión,
- Uso de los protocolos,
- Solicitudes de impresión de datos de la empresa.

Todos los cambios en la central telefónica (PABX) y en los servidores y equipos de red de la CMS, incluyendo la instalación de el nuevo software, el cambio de direcciones IP, la reconfiguración de switchs, deben ser documentados y debidamente aprobados, excepto si se trata de una situación de emergencia. Todo esto es para evitar problemas por cambios apresurados y que puedan causar interrupción de las comunicaciones, caída de la red, denegación de servicio o acceso inadvertido a información confidencial.

Propiedad de la información

Con el fin de mejorar la productividad, la CMS promueve el uso responsable de las comunicaciones en forma electrónica, en particular el teléfono, el correo de voz, el correo electrónico, y el fax. Los sistemas de comunicación y los mensajes generados y procesados por tales sistemas, incluyendo las copias de respaldo, se deben considerar como propiedad de la CMS y no propiedad de los usuarios de los servicios de comunicación.

Uso de los sistemas de comunicación

Los sistemas de comunicación de la CMS generalmente sólo deben usarse para actividades de trabajo. El uso personal en forma ocasional es permisible siempre y cuando consuma una cantidad mínima de tiempo y recursos, y además no interfiera con la productividad del empleado ni con las actividades de la CMS.

Conexiones externas

La conectividad a Internet será otorgada para propósitos relacionados con el negocio y mediante una autorización de la Gerencia.
Debe asegurarse que la totalidad del tráfico entrante y saliente de la red interna, sea filtrado y controlado por un firewall prohibiendo el pasaje de todo el tráfico que no se encuentre expresamente autorizado.

Todas las conexiones a Internet de la empresa deben traspasar un servidor Proxy una vez que han traspasado el firewall.

Deben documentarse los servicios provistos a través de Internet y definirse las responsabilidades en cuanto a su administración. No se publicarán en Internet datos referidos a las cuentas de correo de los empleados, deberán exhibir cuentas especiales asignadas a cada área de la empresa.

Cada vez que se establezca una vía de comunicación con terceros (personal de mantenimiento externo, fábricas, proveedor de servicios de Internet, etc.), los mecanismos de transmisión y las responsabilidades de las partes deberán fijarse por escrito.

El uso de Internet debe ser monitoreado periódicamente. Si existe alguna razón para creer que la seguridad está siendo violada, la CMS puede revisar el contenido de las comunicaciones de Internet.

El acceso casual a los mensajes de correo electrónico por los administradores y similares, se considera una violación a la política de seguridad de la información. Sin embargo, la Gerencia tiene el derecho de examinar cualquier información, sin previo consentimiento o notificación del empleado, en caso que se considere que se está utilizando inadecuadamente el equipamiento de la compañía.

Información personal sensitiva

Es importante señalar que hay una categoría de Información Personal (PI) / Datos personales (PD) llamada Información Personal Sensitiva (SPI) que puede requerir cuidados adicionales atendiendo a las leyes propias de los países. SPI es un elemento de información que podría ser usada indebidamente perjudicando a la persona financiera, laboral o socialmente.

Información Personal Sensitiva incluye:

- número de identificación personal (ej. Numero del Seguro Social)
- número de licencia de conducir
- número de cuenta bancaria
- número de tarjeta de crédito o débito en combinación con cualquier código de seguridad
- password o código de acceso que podría permitir acceso a cuentas financieras personales
- información relacionada a la condición natural de la persona tal como su raza u origen étnico, opinión política, membrecía de organizaciones mundiales, creencias filosóficas o religiosas, información relativa al estado de salud física o mental, enfermedad, minusvalía, defectos patológicos o tratamientos médicos, actividad u orientación sexual, records criminalísticas, incluyendo convicciones, decisiones penales y alguna otra información colectada en procesos de administración de justicia relacionada con ofensas o relacionado con comisiones debido a supuestas ofensas, información biométrica o genética, necesidades de bienestar social o beneficios o asistencia recibidos por bienestar social, ya sea que toda o parte de la información descrita arriba directa o indirectamente.

Para toda Información Personal Sensitiva de los empleados de la CMS, de nuestros clientes y otra de carácter individual clasificada Confidencial se debería cumplir mínimo con lo siguiente:

- No almacene Información Personal Sensitiva sin una razón válida de negocio para hacerlo.
- Si tiene una necesidad válida de negocio para almacenar Información Personal Sensitiva en su estación de trabajo u otro medio magnético, esta información debe estar criptografiada.

Si su estación de trabajo o medio magnético conteniendo Información Personal Sensitiva es perdido, robado o se sospecha ha comprometido su seguridad, Ud. debe inmediatamente reportar el incidente y especificar que tipo de Información Personal Sensitiva ha sido expuesta

No envíe información Confidencial CMS a sitios Internet que ofrecen servicios de traducción.

Cuando imprima información Confidencial CMS, Ud. debe protegerla contra robo o acceso no autorizado. (El termino printers incluye: impresoras, ploters y otros dispositivos usados para crear impresiones de salida). La información Confidencial CMS sólo puede ser impresa en un área controlada con acceso permitido sólo a personal con razón de negocio válido, o una instalación atendida donde la información impresa sea entregada sólo a su propietario o también en una impresora con la facilidad de captura que Ud. controle o atienda personalmente.

Ud. puede usar una impresora ubicada en un espacio interno CMS, pero debe recoger su información Confidencial CMS dentro de los 30 minutos siguientes.

Configuración lógica de red

Cuando conecte su equipo a una red interna CMS, se debe considerar varios puntos:

1. No se presente (ej. Enmascarado) o identifique como si Ud. fuera otro usuario en la red. No ejecute programas de monitoreo de trafico (Ej. "sniffer" o similares) sin la debida autorización explícita de la gerencia y la aprobación del administrador de la red.

2. No ejecute pruebas de seguridad o programas contra cualquier sistema o servidor Intranet u otros que Ud. controle directamente sin la debida y explicita autorización gerencial. No agregue cualquier dispositivo que amplíe la infraestructura de la red CMS (ej. dispositivos tales como Switches, Bridges, Routers, Hubs, modems, wireless access points, etc.) por cualquier motivo sin la debida autorización del administrador de la red.

3. Deberá asegurarse que la dirección IP de la empresa sea un número variable y confidencial.

Correo

Deberá existir un procedimiento formal para dar de alta y de baja las cuentas de correo electrónico en el sistema informático.

Todas las cuentas de correo que pertenezcan a la empresa deben estar gestionadas por una misma aplicación. Esta debe asociar una cuenta de correo a una PC en particular de la red interna.

El correo electrónico no debe ser utilizado para enviar cadenas de mensajes, no debe relacionarse con actividades ilegales y no éticas o para mensajes no relacionados con los propósitos de la empresa.

Los datos que se consideraron “confidenciales” o “críticos” deben encriptarse.

Debe existir un procedimiento de priorización de mensajes, de manera que los correos electrónicos de prioridad alta sean resguardados.

Deberá asignarse una capacidad de almacenamiento fija par cada una de las cuentas de correo electrónico de los empleados.

Antivirus

En todos los equipos de la empresa se debe instalar y correr el antivirus actualizado, el mismo que debería cumplir con lo siguiente:

- Detectar y controlar cualquier acción intentada por un software viral en tiempo real.
- Periódicamente ejecutar el "scanning" para revisar y detectar software viral almacenado en la estación de trabajo.
- Hacer una revisión al menos diaria para actualizar la definición del software antivirus.
- Debe ser un producto totalmente legal (con licencia o Software libre).

No deben usarse diskettes u otros medios de almacenamiento en cualquier computadora de la CMS a menos que se haya previamente verificado que están libres de virus u otros agentes dañinos.

Deberá existir un procedimiento formal a seguir en caso que se detecte un virus en algún equipo del sistema.

Firewall

Deberá instalarse y correr un firewall personal en su estación de trabajo,

El firewall debe cumplir con los siguientes criterios básicos:

- Las redes detectadas deben ser tratadas como desconocidas y no confiables.
- Alertar a los usuarios ante nuevos programas solicitando acceso a la red
- Impedir el acceso a sistemas no autorizados.
- Que el firewall del cliente tenga la versión mas reciente disponible.
- Debe ser un producto totalmente legal (con licencia)

El firewall de la empresa debe presentar una postura de negación preestablecida, configurado de manera que se prohíban todos los protocolos y servicios, habilitando los necesarios.

El encargado de mantenimiento debe controlar periódicamente la configuración del firewall y los servicios de red, documentando los resultados de dichas pruebas.

Ataques de red

Toda la información que se considere confidencial deberá encriptarse durante la transmisión, o viajar en formato no legible.

Deberá utilizarse una herramienta que monitoree la red, con el fin de evitar el ataque de denegación de servicio (DoS).

Para disminuir el riesgo de sniffing, la red de la empresa deberá segmentarse física y/o lógicamente.

Con el fin de disminuir la posibilidad de spoofing el firewall deberá denegar el acceso a cualquier tráfico de red externo que posea una dirección fuente que debería estar en el interior de la red interna.

Los archivos de passwords y datos de usuarios no deberán almacenarse en el directorio por default destinado a tal fin. Además deberán estar encriptados utilizando encriptación en un solo sentido (“one way”), con estrictos controles de acceso lógico, de manera de disminuir la posibilidad de ataques.

3 - Seguridad de las aplicaciones

Software

No debe utilizarse software bajado de Internet y en general software que provenga de una fuente no confiable, a menos que se haya sido comprobado en forma rigurosa y que esté aprobado su uso por el Departamento de Informática.

Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución gratuita, a menos que haya sido previamente aprobado por el Departamento de Informática.

Deben mantenerse registros de todas las transacciones realizadas en la base de datos, de manera que éstas puedan revertirse en caso de surgir un problema. Los registros de la base de datos no se borrarán físicamente, sino que deberán marcarse como eliminados.

Deberá existir un responsable en cada área de la empresa, que responda por la información que se maneja en dicho sector. Deberá definir la clasificación de los datos y los controles de acceso que son necesarios, junto con el administrador del sistema.

Control de aplicaciones en PC's

Se deberá generar un procedimiento donde se especifique qué aplicaciones deben instalarse de acuerdo al perfil de cada usuario y con qué frecuencia se harán las actualizaciones de dichas aplicaciones.

Antes de hacer un cambio en la configuración de los servidores se deberá hacer un backup de la configuración existente. Una vez que el cambio ha resultado satisfactorio deberá almacenarse la configuración modificada.
Se deberán documentar no solo el procedimiento de instalación y reparación de equipos, sino además cada uno de los mantenimientos que se les realicen.
Deberán generarse historiales y así calcular datos estadísticos de los cambios realizados y los errores reportados.

En el momento en que un nuevo usuario ingrese a la empresa, se lo deberá notificar y deberá aceptar que tiene prohibida la instalación de cualquier producto de software en los equipos.

Control de datos en las aplicaciones

Deberán protegerse con controles de acceso las carpetas que almacenen los archivos de las aplicaciones, y solo el administrador de sistemas tendrá acceso a ellas.

Ciclo de vida

Antes de realizar alguna modificación en el sistema, deberá realizarse un análisis del impacto de este cambio.

Se deberá implementar una gestión de configuración, y deberán documentarse los cambios desarrollados en las aplicaciones.

Deberá existir un documento formal de solicitud de cambios, donde quede reflejado el motivo y la solicitud del cambio, allí se agregarán los requerimientos de seguridad necesarios, definidos por el responsable de la información y el administrador de sistemas. La documentación de los cambios debe incluir:

- Sistema que afecta,
- Fecha de la modificación,
- Desarrollador que realizó el cambio,
- Empleado que solicitó el cambio,
- Descripción global de la modificación.

Los contratos con terceros deberán contener una cláusula que indique “Derecho de auditar el desempeño del contratado”.

Se deberá informar por escrito la importancia de la seguridad de la información a todo el personal contratado, terceros y consultores. El administrador del centro de cómputos, junto con los directivos, serán quienes:

- Especifiquen los requerimientos de seguridad,
- Determinen los pasos a seguir en caso que no se respete lo establecido en el contrato,
- Establezcan cláusulas sobre confidencialidad de la información,
- Exijan al tercero en cuestión que informe posibles brechas de seguridad existentes.

Con respecto a la contratación de terceros para el desarrollo de aplicaciones, éste deberá entregar a la empresa:

- Aplicación ejecutable,
- Código fuente de la aplicación,
- Documentación del desarrollo,
- Manuales de uso.

4 - Seguridad física

Los computadores de la CMS sólo deben usarse en un ambiente seguro. Se considera que un ambiente es seguro cuando se han implantado las medidas de control apropiadas para proteger el software, el hardware y los datos. Esas medidas deben estar acorde a la importancia de los datos y la naturaleza de riesgos previsibles.

Debe respetarse y no modificar la configuración de hardware y software establecida por el Departamento de Informática

No se permite fumar, comer o beber mientras se está usando un PC.

Deben protegerse los equipos de riesgos del medioambiente (por ejemplo, polvo, incendio y agua).

Cualquier falla en los computadores o en la red debe reportarse inmediatamente ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.

No pueden moverse los equipos o reubicarlos sin permiso. Para llevar un equipo fuera de la Compañía se requiere una autorización escrita.

La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente.

Control de acceso físico al centro de cómputos

Se deberá asegurar que todos los individuos que entren a áreas restringidas se identifiquen y sean autenticados y autorizados para entrar.

Cualquier persona ajena a la empresa que necesite ingresar al centro de cómputos deberá anunciarse en la puerta de entrada, personal de sistemas designado deberá escoltarlo desde la puerta hacia el interior del edificio, acompañándolo durante el transcurso de su tarea, hasta que éste concluya.

El área del centro de cómputos donde se encuentran los servidores, el switch central y demás equipamiento crítico solo debe tener permitido el acceso a los administradores.

Deberán existir guardias de seguridad en permanente monitorización, durante el horario laboral. Se deberán ubicar en el exterior y el interior de la empresa.

Los servidores de red y los equipos de comunicación (PABX, routers, etc.) deben estar ubicados en locales apropiados, protegidos contra daños y robo. Debe restringirse severamente el acceso a estos locales y a los cuartos de cableado a personas no autorizadas mediante el uso de cerraduras y otros sistemas de acceso.

Control de acceso a equipos

Los siguientes controles de seguridad deben ser activados en todas las estaciones de trabajo (workstation) personales con el fin de ayudar a protegerlas contra el robo de la información sensible que dicho equipo pueda contener:

1. Activar la contraseña de disco duro (hard disk password) en los parámetros del BIOS.
2. Configurar la contraseña para proteger el teclado y la pantalla (keyboard/screen lock) que se active automáticamente luego de un período de inactividad. El intervalo de inactividad no debe ser mayor a 15 minutos.
3. Si Ud. conecta su estación de trabajo a una red fuera de la CMS, en la que la administración de niveles de acceso no es controlada (ej. Ud. esta en un

cliente y requiere hacer logon a un dominio de Windows administrado por el cliente), entonces toda la información clasificada Confidencial debe ser criptografiada.

Cualquier dispositivo externo que no se encuentre en uso, deberá permanecer guardado bajo llave dentro del centro de cómputos.

El administrador deberá realizar chequeos periódicos para comprobar:

- La correcta instalación de los dispositivos de los equipos,
- Su buen funcionamiento,
- Sus números de series corresponden con los datos registrados por el administrador al momento de la instalación

Si su portátil no puede ser asegurada físicamente de otra forma (ej: guardarla en un cajón o gaveta del escritorio bajo llave, dentro de una oficina, o llevarla consigo), entonces debe asegurarla con un cable de seguridad o anclaje físico.

Mantenga el equipo en su poder todo el tiempo que sea posible, cuando esté fuera de las premisas de la empresa.

En los viajes aéreos, no despache su portátil con el equipaje, y esté alerta de la posibilidad de robo cuando vaya a través de los puntos de control de los aeropuertos.

No debe dejar su portátil dentro de un vehículo desatendido por un período largo de tiempo.

- Si debe dejar su portátil en un vehículo desocupado, asegúrela al cuerpo del vehículo dentro del baúl.
- Si debe dejar su portátil en un hotel, guárdela en una caja fuerte de haber una disponible.
- Si no hay caja fuerte y posee el cable de seguridad, utilice ese mecanismo.

Dispositivos de soporte

Deberán existir los siguientes dispositivos de soporte en la empresa:

- Aire acondicionado y Calefacción: en el centro de cómputos la temperatura debe mantenerse entre 19º C y 20º C.
- Matafuegos: deberán ser dispositivos químicos y manuales que cumplan las especificaciones para extinguir incendios en equipos eléctricos de computación,
  ~ deberán estar instalados en lugares estratégicos de la empresa,
  ~ el centro de cómputos deberá contar con uno propio ubicado en la habitación de los servidores.
- Alarmas contra intrusos: deberán contar con una alarma que se active en horarios no comerciales. Ésta deberá poder activarse manualmente en horarios laborales ante una emergencia.
- UPS: (Uninterruptible power supply) deberá existir al menos un UPS en el centro de cómputos que atienda a los servidores, con tiempo suficiente para que se apaguen de forma segura.
- Luz de emergencia: deberá existir una luz de emergencia que se active automáticamente ante una contingencia.

Todos estos dispositivos deberán ser evaluados periódicamente por personal de mantenimiento.

Deberán existir procedimientos detallados a seguir por el personal en caso de emergencias, indicando responsables, quiénes deben estar adecuadamente capacitados.

Cableado estructurado

Se deberá documentar en planos los canales de tendidos de cables y las bocas de red existentes.

Deberá medirse periódicamente nivel de ancho de banda de red ocupado. Si este nivel excede un mínimo permitido, deberán tomarse las acciones correctivas necesarias.

Ante un corte del suministro de energía eléctrica deberán apagarse los equipos del centro de cómputos de forma segura, como medida de prevención.

5.- Administración del centro de cómputo

El equipo de sistemas debe hacer hincapié en la concienciación de todos los usuarios, generando una cultura de la seguridad, haciéndolos partícipes de las medidas de seguridad, tanto los usuarios actuales como los que se incorporen en el futuro. El proceso de concienciación debe ser renovado y transmitido a los usuarios en forma anual.
Los usuarios solicitarán asesoramiento o servicios al centro de cómputos a través de mails, de manera que se genere un registro de los trabajos efectuados por los empleados del centro de cómputos y de las solicitudes de los empleados.

Deberá existir un procedimiento para realizar la publicidad de políticas, planes o normas de la empresa y sus modificaciones.
Los administradores deberán informar en tiempo de suspensiones en el servicio necesarias por mantenimiento, especificando fecha, hora y duración de la suspensión.

Deberá generarse un inventario detallado donde se describan los sistemas de información y de los equipos de cómputos utilizados en la organización. Deberá asignarse un responsable de mantenerlo actualizado y de realizar controles periódicos.

Capacitación

Se debe obtener un compromiso firmado por parte del personal respecto al cumplimiento de las medidas de seguridad definidas en la política de seguridad informática, destacando específicamente el mantenimiento de la confidencialidad de las claves de acceso, la no-divulgación de información de la organización, el cuidado de los recursos, la utilización de software sin licencia y el reporte de situaciones anormales. Debe confirmarse este compromiso anualmente o cada vez que se produzcan cambios en las funciones asignadas al personal.

Asegurar que los empleados reciban capacitación continua para desarrollar y mantener sus conocimientos competencia, habilidades y concienciación en materia de seguridad informática dentro del nivel requerido a fin de lograr un desempeño eficaz.

Respaldos

Se deberá asegurar la existencia de un procedimiento aprobado para la generación de copias de resguardo sobre toda la información necesaria para las operaciones de la organización, donde se especifique la periodicidad y el lugar físico donde se deben mantener las copias generadas.

Los archivos de backup deben tener un control de acceso lógico de acuerdo a la sensibilidad de sus datos, además de contar con protección física.

Deben generarse copias de respaldo de las configuraciones de los servidores, documentando las modificaciones realizadas para identificar las distintas versiones. Se deberá establecer un procedimiento de emergencia para dejar sin efecto los cambios efectuados y poder recuperar las versiones autorizadas anteriores.

Se deberá generar una copia de respaldo de toda la documentación del centro de cómputos, incluyendo el hardware, el software, la cual deberá ser de acceso restringido y estar físicamente en un lugar distinto a los centros de procesamiento.

Documentación

Deberá generarse un soporte de documentación, con información correcta, consistente y actualizada, sobre políticas, normas, estándares, procedimientos y manuales. Deberá asignarse un responsable a cargo de la gestión de la documentación en el centro de cómputos.

Deberá existir un registro de los eventos, errores y problemas del hardware y el software utilizados en las operaciones de procesamiento de datos.

Deberán existir una documentación y un registro de las actividades del centro de cómputos (procesos normales, eventuales y excepcionales) que se

desarrollan diariamente, que incluya como mínimo el detalle de los procesos realizados.

Revisión del sistema

La empresa debe asegurar que los sistemas provean las herramientas necesarias para garantizar un correcto control y auditabilidad de forma de asegurar la integridad, exactitud y disponibilidad de la información. Para ello deben existir:

- Herramientas que registren todos los eventos relacionados con la seguridad de la información procesada por los centros de cómputos de la empresa.
- Herramientas que analiza los registros generando reportes, estadísticas, gráficos con relación a los datos recogidos, con distintas frecuencias (diarios, semanales, mensuales y anuales). Deberá tener la capacidad de generar alarmas teniendo en cuenta la severidad de los eventos acontecidos.
- Procedimientos de revisión de los eventos registrados, a cargo de un empleado designado por el administrador, de forma de detectar anomalías y tomar las acciones correctivas necesarias.

Se deberán registrar, mediante logs de auditoria, aquellos eventos relacionados con la seguridad de la información. Dichos registros deberán contener como mínimo:

- Fecha y hora del evento,
- Fuente (el componente que disparó el evento),
- ID del evento (número único que identifica el evento),
- Equipo (máquina donde se generó el evento),
- Usuario involucrado,
- Descripción (acción efectuada y datos asociados con el evento).

Se deberán analizar periódicamente los siguientes eventos específicos como mínimo:

- Controles de acceso y permisos de los usuarios,
- Uso de recursos informáticos,
- Intentos de ingreso al sistema fallidos.

ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD

ORGANIZACIÓN INTERNA

Para administrar la seguridad de información se crea el Comité de Seguridad de la Información, integrado por el representante de cada área. A continuación se indica la conformación del mismo:

Área/Dirección	Representante
Área de sistemas	Administrador de la red
Área de ventas	Jefe de negocios
Dirección administrativa	Jefe Administrativo Financiero
Auditoria interna	Auditor interno
Legal	Asesor jurídico

Tabla 4.2 Conformación del Comité de Seguridad de la Información

ASIGNACIÓN DE RESPONSABILIDADES SOBRE SEGURIDAD DE LA INFORMACIÓN

El Director Ejecutivo es el encargado de asignar las funciones relativas a la Seguridad Informática del Organismo al Administrador de la red, en adelante el "Responsable de Seguridad Informática", quien tendrá a cargo las funciones relativas a la seguridad de los sistemas de información del Organismo, lo cual incluye la supervisión de todos los aspectos inherentes a seguridad informática tratados en la Política.

A continuación se detallan los procesos de seguridad, indicándose en cada caso el/los responsable/s del cumplimiento de los aspectos de esta Política aplicables a cada caso:

Proceso	Responsable
Seguridad del Personal	Encargado de recursos humanos y jefe departamental
Seguridad en las comunicaciones y operaciones	Administrador de la red
Control de acceso	Administrador de la red

Tabla 4.3 Procesos de Seguridad

Proceso de autorización de recursos para el tratamiento de la información

Los nuevos recursos de procesamiento de información serán autorizados por los Responsables de las Unidades Organizativas involucradas, considerando su propósito y uso, conjuntamente con el Responsable de Seguridad Informática, a fin de garantizar que se cumplan todas las Políticas y requerimientos de seguridad pertinentes.

Cuando corresponda, se verificará el hardware y software para garantizar su compatibilidad con los componentes de otros sistemas del Organismo.

El uso de recursos personales de procesamiento de información en el lugar de trabajo puede ocasionar nuevas vulnerabilidades. En consecuencia, su uso será evaluado en cada caso por el Responsable de Seguridad Informática y deberá ser autorizado por el Responsable del Área Informática y por el responsable del área al que se destinen los recursos.

GESTIÒN DE LOS ACTIVOS DE RED

INVENTARIO DE ACTIVOS

A continuación se hace un inventario de los recursos informáticos dentro de la CMS:

Tabla 4.4 Inventario de Activos

DEPARTAMENTO RESPONSABLE	ACTIVO	DESCRIPCIÓN	DETALLES DE LA RESPONSABILIDAD
Administrador de la red	4 Equipos de cómputo	CPU, monitor, teclado, mouse, parlantes, UPS, unidad de CD	El administrador es responsable del mantenimiento y actualización de los servidores.
Administrador de la red	Software	Sistemas Operativos (Windows 2003, CentOS)	
Administrador de la red	Software	Ofimática	
Administrador de la red	Software	Antivirus	
Ventas	2 Equipos de cómputo	CPU, monitor, teclado, mouse, parlantes, UPS, unidad de CD	Son responsables de la protección física de los equipos, reportar fallas en el Software o Hardware.
Ventas	Software	Sistemas Operativos (Windows XP Profesional SP 2)	
Ventas	Software	Ofimática	
Ventas	Software	Antivirus	
Asistente Ejecutivo	1 Equipo de cómputo	CPU, monitor, teclado, mouse, parlantes, UPS, unidad de CD	Son responsables de la protección física de los equipos, reportar fallas en el Software o Hardware.
Asistente Ejecutivo	Software	Sistemas Operativos (Windows XP Profesional SP 2)	
Asistente Ejecutivo	Software	Ofimática	

Asistente Ejecutivo	Software	Antivirus	
Asesoría legal	1 Equipo de cómputo	CPU, monitor, teclado, mouse, parlantes, UPS, unidad de CD	Son responsables de la protección física de los equipos, reportar fallas en el Software o Hardware.
Asesoría legal	Software	Sistemas Operativos (Windows XP Profesional SP 2)	
Asesoría legal	Software	Ofimática	
Asesoría legal	Software	Antivirus	
Negocios	3 Equipo de cómputo	CPU, monitor, teclado, mouse, parlantes, UPS, unidad de CD	Son responsables de la protección física de los equipos, reportar fallas en el Software o Hardware.
Negocios	Software	Sistemas Operativos (Windows XP Profesional SP 2)	
Negocios	Software	Ofimática	
Negocios	Software	Antivirus	
Financiero	1 Equipo de cómputo	CPU, monitor, teclado, mouse, parlantes, UPS, unidad de CD	Son responsables de la protección física de los equipos, reportar fallas en el Software o Hardware.
Financiero	Software	Sistemas Operativos (Windows XP Profesional SP 2)	
Financiero	Software	Ofimática	
Financiero	Software	Antivirus	
Administrador AUS	2 Equipo de cómputo	CPU, monitor, teclado, mouse, parlantes, UPS, unidad de CD	Son responsables de la protección física de los equipos, reportar fallas en el Software o Hardware.
Administrador AUS	Software	Sistemas Operativos (Windows XP Profesional SP 2)	
Administrador AUS	Software	Ofimática	
Administrador AUS	Software	Antivirus	
Recepción	1 Equipo de cómputo	CPU, monitor, teclado, mouse, parlantes, UPS, unidad de CD	Son responsables de la protección física de los equipos, reportar fallas en el Software o Hardware.
Recepción	Software	Sistemas Operativos (Windows XP Profesional SP 2)	
Recepción	Software	Ofimática	
Recepción	Software	Antivirus	
Recepción	1 Equipo de cómputo	Impresora	
Auditoria	3 Equipo de cómputo	CPU, monitor, teclado, mouse, parlantes, UPS, unidad de CD	Son responsables de la protección física de los equipos, reportar fallas en el Software o Hardware.
Auditoria	Software	Sistemas Operativos (Windows XP Profesional SP 2)	
Auditoria	Software	Ofimática	
Auditoria	Software	Antivirus	
Operaciones	8 Equipo de cómputo	CPU, monitor, teclado, mouse, parlantes, UPS, unidad de CD	Son responsables de la protección física de los equipos, reportar fallas en el Software o Hardware.
Operaciones	Software	Sistemas Operativos (Windows XP Profesional SP 2)	

Operaciones	Software	Ofimática	
Operaciones	Software	Antivirus	
Administrativo	2 Equipo de cómputo	CPU, monitor, teclado, mouse, parlantes, UPS, unidad de CD	Son responsables de la protección física de los equipos, reportar fallas en el Software o Hardware.
Administrativo	Software	Sistemas Operativos (Windows XP Profesional SP 2)	
Administrativo	Software	Ofimática	
Administrativo	Software	Antivirus	
Financiero	3 Equipo de cómputo	CPU, monitor, teclado, mouse, parlantes, UPS, unidad de CD	Son responsables de la protección física de los equipos, reportar fallas en el Software o Hardware.
Financiero	Software	Sistemas Operativos (Windows XP Profesional SP 2)	
Financiero	Software	Ofimática	
Financiero	Software	Antivirus	
Financiero	1 Equipo de cómputo	Impresora	
Afiliación	3 Equipo de cómputo	CPU, monitor, teclado, mouse, parlantes, UPS, unidad de CD	Son responsables de la protección física de los equipos, reportar fallas en el Software o Hardware.
Afiliación	Software	Sistemas Operativos (Windows XP Profesional SP 2)	
Afiliación	Software	Ofimática	
Afiliación	Software	Antivirus	
Afiliación	2 Equipo de cómputo	Impresoras	
Cobranzas	1 Equipo de cómputo	CPU, monitor, teclado, mouse, parlantes, UPS, unidad de CD	Son responsables de la protección física de los equipos, reportar fallas en el Software o Hardware.
Cobranzas	Software	Sistemas Operativos (Windows XP Profesional SP 2)	
Cobranzas	Software	Ofimática	
Cobranzas	Software	Antivirus	
Cobranzas	2 Equipo de cómputo	Impresoras	
Administrativo-Financiero	1 Equipo de cómputo	CPU, monitor, teclado, mouse, parlantes, UPS, unidad de CD	
Administrativo-Financiero	Software	Sistemas Operativos (Windows XP Profesional SP 2)	
Administrativo-Financiero	Software	Ofimática	
Administrativo-Financiero	Software	Antivirus	
	Equipo de cómputo	Portátil	La persona que requiera la laptop fuera de la Corporación, debe ser responsable de la protección física y retorne el equipo en

			iguales condiciones en las que fue retirado

SEGURIDAD DE LOS RECURSOS HUMANOS

Las responsabilidades de cada empleado se definen en el momento de su contratación, a continuación se especifica la selección de personal propuesta para la CMS. La implementación de este método está en consideración del departamento de Recursos Humanos de la CMS, para que el departamento en conjunto con la directiva de la Organización apruebe el mismo.

Capacitación del Usuario

En cuanto a la capacitación para el usuario, en el **ANEXO A** se establece una guía para el usuario que los empleados deben tener presente para no incurrir en fallas de seguridad.

Mecanismos para promover la comunicación

En el caso que se necesite informar a todo el personal de alguna debilidad con respecto a la seguridad dependiendo de la complejidad de la situación se optará como primera instancia el correo electrónico interno y si el caso lo amerita se convocará a una reunión en la cual intervendrá el Comité de Seguridad junto con el personal de la Corporación necesario.

SEGURIDAD FÍSICA Y DEL ENTORNO

La seguridad física actualmente está implementada en un modelo de defensa por capas, los controles físicos deben trabajar juntos en la arquitectura, es decir, si una capa falla, otras capas protegerá el recursos físico. Las capas están implementadas dentro del perímetro. Por ejemplo: se tendrá una valla, luego las paredes, luego el guardia, luego la tarjeta de acceso, luego el candado en el caso de una laptop. Esta serie de capas protegerán los recursos más sensibles.

La seguridad necesita proteger todos los recursos de la organización, incluyendo personas y hardware. La seguridad debe fortalecer la productividad ya que provee un ambiente seguro. Esto permite a los empleados enfocarse en sus tareas, en lo posible no permitir que la seguridad física se transforme en un hueco de seguridad.
Las vulnerabilidades con respecto a la seguridad física tienen relación con destrucción física, intrusos, problemas del ambiente y los empleados que han perdido sus privilegios causen daños inesperados de datos o sistemas.

INSTALACIONES

Los materiales de construcción y la composición de la estructura han sido evaluados por las características de protección. La construcción de la Corporación asegura que el edificio no colapse.
Como se indico anteriormente la puerta del cuarto de servidores se puede abrir fácilmente con cualquier tarjeta, razón por la cual se cambiará la puerta, para que cumpla con las siguientes características de seguridad:

- Material resistente, como: madera, aluminio
- Resistente a ingreso forzado
- Cerradura resistente

Además en la puerta del cuarto de servidores se colocará un rótulo de zona de acceso restringido para evitar acceso no autorizado.
Es necesario procedimientos de seguridad para ayudar a proteger la Corporación de actividades devastadoras. Muchas veces estos procedimientos de protección usan componentes de seguridad que son parte del ambiente y por consiguiente no necesitan gastos extras. Los procedimientos que se han considera incluyen copias de respaldo de los datos críticos (**ANEXO B**), componentes de seguridad que ya son parte de los sistemas operativos, y la solicitud de mayor colaboración por parte del guardia actual de la CMS para que permanezca en una sola área atento a cualquier fallo de seguridad.

La seguridad física debería ser complementada con la seguridad contra fuego. Hay estándares nacionales y locales para prevenir, detectar y suprimir el fuego.

En la Corporación se utilizará detectores de fuego activados por el humo, ya que son dispositivos que dan señales de alerta tempranamente. Este detector produce un rayo de luz a través de un área protegida y si el rayo es obstruido, la alarma asume que es humo y sueña. En la figura 1 se ilustra como el dispositivo trabaja.

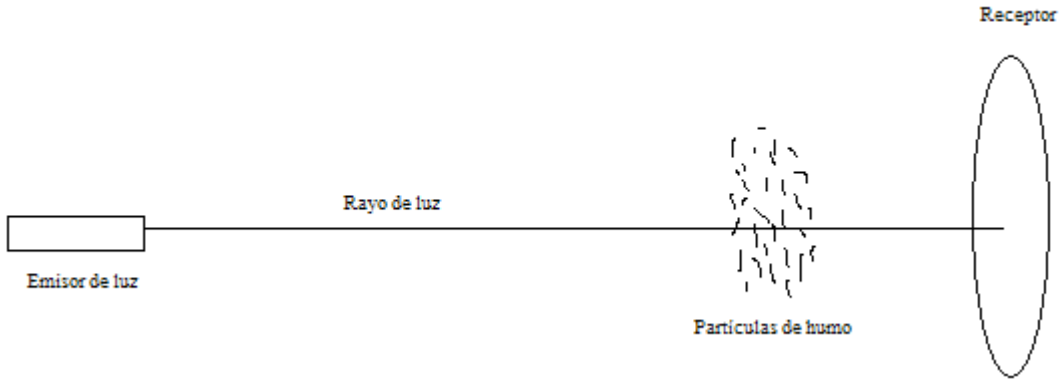

Figura 4.2 Funcionamiento de detector de humo

Se colocarán detectores de fuego en el cuarto de servidores, otra cerca al área de la Asistente ejecutiva y otros censores cerca de la Recepción, de tal manera que se trate de cubrir todas las instalaciones de la Corporación.

Es importante conocer que tipo de fuego y que se debería hacer apara suprimir el fuego. En la tabla siguiente se indica los tipos de fuego.

Clase	Tipos de fuego	Elementos del fuego	Métodos de supresión
A	Combustible común	Productos de madera, papel	Agua
B	Líquido	Petróleo y productos derivados	Gas (Halon) o CO2
C	Eléctrico	Equipos eléctricos	Gas (Halon) o CO2
D	Metales combustibles	Magnesio, sodio, potasio	Polvo seco

Tabla 4.5 Tipos de Fuego

En la Corporación se utilizará extintores portables para suprimir el fuego clase C, y dependiendo de la gravedad de la situación se procederá a llamar a la estación de bomberos más cerca para eliminar el fuego con el agua.

PERÍMETRO DE SEGURIDAD

La primera línea de defensa trata el control del perímetro para prevenir acceso no autorizado a la Corporación. Actualmente en la Corporación esta defensa trabaja de la siguiente manera: Cuando la Corporación es cerrada todas las puertas son aseguradas con un mecanismo de monitoreo en posiciones estratégicas para alertar de actividades sospechosas. Cuando la Corporación está en operación, la seguridad es más complicada porque se debe distinguir el acceso de personas autorizadas de las personas no autorizadas. En la figura se ha identificado el único acceso a la Corporación, esta debe ser apropiadamente protegida, actualmente esta puerta no esta asegurada en horas laborables, es decir es fácilmente accedida, debido a que otras organizaciones trabajan en el edificio donde se encuentra la CMS, no pudimos realizar el cambio de la puerta por otra de mayor seguridad, el costo de nuestra propuesta se adjunta en el análisis económico, la misma que consideraba cambiar la actual puerta por una puerta con cerradura electrónica la cual se podrá abrir con tarjetas electrónicas que serán otorgadas a miembros de la Corporación y para visitantes existirá un timbre y la recepcionista procederá a abrirla desde su lugar de trabajo.

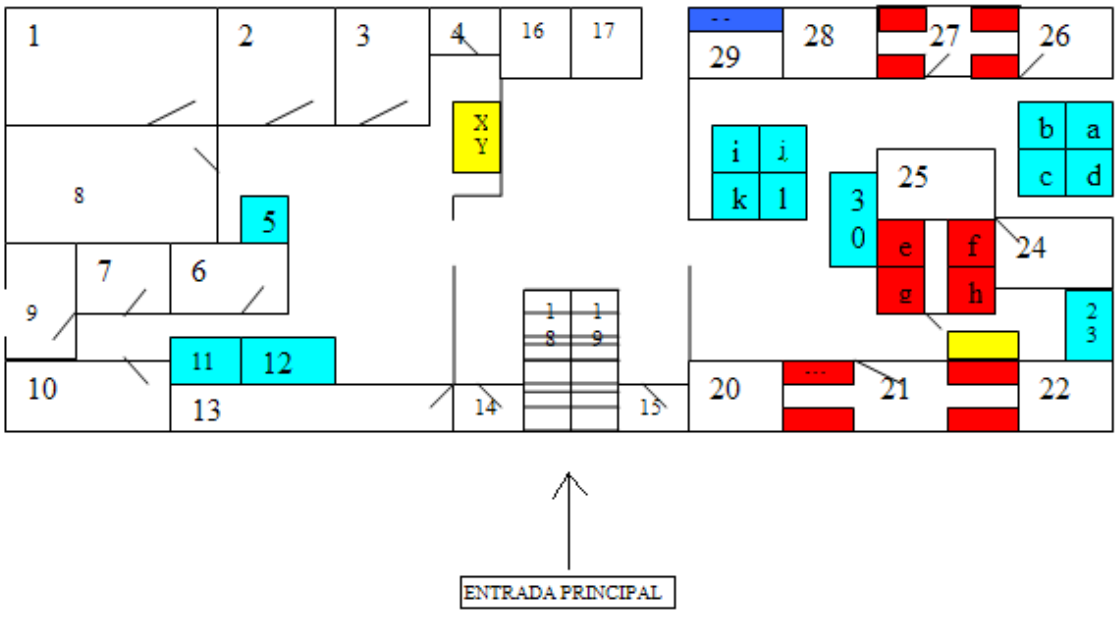

Figura 4.3 Esquema físico de las instalaciones de la CMS

Las cerraduras y llaves son los mecanismos de control de acceso más barato pero de gran importancia para prevenir cualquier acceso no autorizado.

CONTROLES FÍSICOS DE ENTRADAS

Los controles de acceso físico tendrán las siguientes características:

a) Supervisar a los visitantes de la Corporación y registrar la fecha y horario de su ingreso y egreso, esta tarea será realizada por el guardia de seguridad. Sólo se permitirá el acceso mediando propósitos específicos y autorizados.

b) Implementar el uso de una identificación unívoca visible para todo el personal del área protegida e instruirlo acerca de cuestionar la presencia de desconocidos no escoltados por personal autorizado y a cualquier persona que no exhiba una identificación visible.

SEGURIDAD DE OFICINAS, DESPACHOS Y RECURSOS

Se definen los siguientes sitios como áreas protegidas de la Corporación, para lo cual se consideró el tipo de información manejada por cada área.

ÁREAS PROTEGIDAS
Cuarto de servidores
Jefatura Administrativa Financiera
Dirección Ejecutiva
Asesoria Jurídica
Auditoría Interna
Jefatura de Operaciones

Tabla 4.6 Áreas Protegidas

Se establecen las siguientes medidas de protección para áreas protegidas:

a. Ubicar las instalaciones críticas en lugares a los cuales no pueda acceder personal no autorizado.
b. Ubicar las funciones y el equipamiento de soporte, por ejemplo: impresoras, fotocopiadoras, máquinas de fax, adecuadamente dentro del área no protegida para evitar solicitudes de acceso, el cual podría comprometer la información.

c. Establecer que las puertas y ventanas permanecerán cerradas cuando no haya vigilancia.
d. Restringir el acceso público a las guías telefónicas y listados de teléfonos internos que identifican las ubicaciones de las instalaciones de procesamiento de información sensible.
e. Almacenar la información de resguardo (back up) en un sitio seguro y distante del lugar de procesamiento, para evitar daños ocasionados ante eventuales contingencias en el sitio principal: en la caja de seguridad que tiene la Corporación con el Banco.

Desarrollo de Tareas en Áreas Protegidas

Para complementar la seguridad en la las áreas protegidas, se establecen los siguientes controles:

a) Dar a conocer al personal la existencia del área protegida, o de las actividades que allí se llevan a cabo, sólo si es necesario para el desarrollo de sus funciones.
b) Evitar la ejecución de trabajos por parte de terceros sin supervisión, como por ejemplo: trabajos de limpieza.
c) Bloquear físicamente las áreas protegidas desocupadas.
d) Prohibir comer, beber y fumar dentro de las instalaciones de procesamiento de la información.

Suministros de Energía

El equipamiento estará protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía estará de acuerdo con las especificaciones del fabricante o proveedor de cada equipo. Para asegurar la continuidad del suministro de energía, se contemplarán las siguientes medidas de control:

a) Actualmente se cuenta con un suministro de energía ininterrumpible (APS) para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas de la Corporación.

b) Una vez que esté el APS activo, la central eléctrica con la que cuenta el edificio debe ingresar a funcionar hasta que se haya solucionado el problema, es necesario mantener un contacto de forma inmediata con la empresa eléctrica para que se solucione el problema lo más pronto posible.

MANTENIMIENTO DE EQUIPOS

Se realizará el mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanentes. Para ello se debe considerar:

a) Someter el equipamiento a tareas de mantenimiento preventivo, el responsable del área informática mantendrá listado actualizado del equipamiento con el detalle de la frecuencia en que se realizará el mantenimiento preventivo.

b) Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.

c) Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.

A continuación se indica el período aconsejable para realizar los mantenimientos en los equipos de la red.

Equipo	Frecuencia de mantenimiento	Personal autorizado
Servidores	4 meses	Administrador de la red
Estaciones de trabajo	6 meses	Administrador de la red
impresoras	6 meses	Administrador de la red
Central telefónica	12 meses	Administrador de la red

Tabla 4.7 Períodos de Mantenimiento Preventivos

SEGURIDAD DE EQUIPOS FUERA DE LOS LOCALES DE LA ORGANIZACIÓN

La seguridad provista debe ser equivalente a la suministrada dentro del ámbito de la Corporación para un propósito similar, teniendo en cuenta los riesgos de trabajar fuera de la misma.

Se respetarán permanentemente las instrucciones del fabricante respecto del cuidado del equipamiento. En la Corporación se protegerá con candados a las computadoras portátiles para evitar que sean robadas cuando se movilicen fuera de las premisas de la Corporación.

GESTIÓN DE COMUNICACIONES Y OPERACIONES

DOCUMENTACIÓN DE PROCEDIMIENTOS OPERATIVOS

Se documentarán y mantendrán actualizados los procedimientos operativos y sus cambios serán autorizados por el administrador de la red.
En los anexos se encuentran detallados los procedimientos operativos para la implementación de los controles propuestos como son los necesarios para la administración de la red, controles criptográficos, seguridad en los servidores, respaldos, etc. En los cuales se detallan: instrucciones para la ejecución de cada tarea, procesamiento y manejo de información, requerimientos del sistema.

CONTROL DE CAMBIOS OPERACIONALES

El responsable del área informática será el encargado de implementar los cambios operacionales y de comunicaciones; previo a una justificación que explique las razones y cómo mejorará en la productividad de la Corporación.
Este procedimiento de control de cambios contemplarán los siguientes puntos:

a) Identificación y registro de cambios significativos.
b) Evaluación del posible impacto de dichos cambios.
c) Aprobación formal de los cambios propuestos.
d) Planificación del proceso de cambio.
e) Prueba del nuevo escenario.
f) Comunicación de detalles de cambios a todas las personas pertinentes.

g) Identificación de las responsabilidades por la cancelación de los cambios fallidos y la recuperación respecto de los mismos.

PLANIFICACIÓN Y ACEPTACIÓN DEL SISTEMA.

PLANIFICACIÓN DE LA CAPACIDAD

El Responsable del Área Informática, efectuará el monitoreo de las necesidades de capacidad de los sistemas en operación tomando en cuenta los nuevos requerimientos de los sistemas y proyectar las futuras demandas, para garantizar un procesamiento y almacenamiento adecuados. Para lo cual, debe recopilar información previa de los requerimientos de software y hardware para la implementación del sistema o proceso que se piensa desarrollar.

ACEPTACIÓN DEL SISTEMA

Para la aprobación del sistema se debe considerar los siguientes puntos:

a) Verificar si la capacidad de las computadoras están acorde con los requerimientos actuales y futuras proyecciones.
b) Garantizar la recuperación ante errores.
c) Preparar y poner a prueba los procedimientos operativos de rutina según normas definidas.
d) Garantizar la implementación de un conjunto acordado de controles de seguridad.
e) Asegurar que la instalación un nuevo sistema no afecte negativamente los sistemas existentes, especialmente en los períodos pico de procesamiento.

PROTECCIÓN CONTRA SOFTWARE MALICIOSO.

CONTROLES CONTRA SOFTWARE MALICIOSO

Estos controles deberán considerar las siguientes acciones:

a) Prohibir el uso de software no autorizado por la Corporación.
b) Instalar y actualizar periódicamente software de detección y reparación de virus, examinado computadoras y medios informáticos, para esto se implementará el software de anti-virus Symantec (**ANEXO C**).
c) Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles.
d) Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos de la Corporación, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas (políticas de control de acceso).
e) Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.
f) Redactar procedimientos para verificar toda la información relativa a software malicioso, garantizando que los boletines de alerta sean exactos e informativos.
g) Concientizar al personal acerca del problema de los virus y sus posibles consecuencias (**ANEXO A**).

GESTIÓN INTERNA DE RESPALDO.

RECUPERACIÓN DE LA INFORMACIÓN

El Responsable de la Seguridad de Información dispondrá y controlará la realización de dichas copias. Los sistemas de resguardo deberán probarse periódicamente, asegurándose que cumplen con los requerimientos de los planes de continuidad de las actividades de la Corporación. Para los procedimientos del resguardo de información, se considerarán los siguientes puntos:

a) Almacenar en una ubicación remota copias recientes de información de resguardo junto con registros exactos y completos de las mismas y los procedimientos documentados de restauración, a una distancia

suficiente como para evitar daños provenientes de un desastre en el sitio principal.

b) Asignar a la información de resguardo un nivel de protección física y ambiental según las normas aplicadas en el sitio principal. Extender los mismos controles aplicados a los dispositivos en el sitio principal al sitio de resguardo.
c) Verificar y probar periódicamente los procedimientos de restauración garantizando su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos.

Para el resguardo de la información ver **ANEXO B**, donde se considera el respaldo de los servidores para el Plan de Contingencia.

GESTIÓN DE LA SEGURIDAD DE RED.

CONTROLES DE RED

El Responsable de Seguridad Informática definirá controles para garantizar la seguridad de los datos, contra el acceso no autorizado, considerando la ejecución de las siguientes acciones:

a) Para establecer controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos (**ANEXO D**)
b) Implementación de controles especiales para mantener la disponibilidad de los servicios de red y computadoras conectadas (**ANEXO E**)
c) Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información.

UTILIZACIÓN DE LOS MEDIOS DE INFORMACIÓN

GESTIÓN DE MEDIOS REMOVIBLES

Se deberán considerar las siguientes acciones para la administración de los medios informáticos removibles:

a) Eliminar de forma segura los contenidos, si ya no son requeridos, de cualquier medio reutilizable que ha de ser retirado o reutilizado por la Corporación.
b) Almacenar todos los medios en un ambiente seguro y protegido, de acuerdo con las especificaciones de los fabricantes o proveedores.

INTERCAMBIO DE INFORMACIÓN.

MENSAJERÍA ELECTRÓNICA

Se debe documentar normas claras con respecto al uso de correo electrónico:

- Todo empleado de la Corporación puede solicitar y disponer de una cuenta de correo electrónica activa.
- El Área de Sistemas hará la configuración de la cuenta de correo en la computadora asignada al funcionario solicitante.

- La activación de las cuentas de correo Corporativo es centralizada, encargándose de esta el responsable de Sistemas previa autorización del Jefe Administrativo. La activación sigue las políticas dadas por el presente documento.
- Para activar el correo electrónico, se deberá enviar dicha solicitud por escrito y debe ser debidamente aprobada.
- Cuando un usuario recibe una nueva cuenta, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad, y acepta sus responsabilidades con relación al uso de esa cuenta.
- No debe concederse cuentas de correo electrónico a personas que no sean empleados de la Corporación a menos que estén debidamente autorizados, en cuyo caso la activación durará el tiempo que duré la permanencia de la(s) personas en la Institución, para lo cual se requerirá la notificación respectiva del área administrativa.

- Cuando un empleado es despedido o renuncia a la Corporación, debe desactivarse la cuenta de correo correspondiente, para lo cual se requerirá la notificación respectiva por parte del área administrativa.

Entender al correo electrónico como una herramienta más de trabajo provista al empleado a fin de ser utilizada conforme el uso al cual está destinada, faculta al empleador a implementar sistemas de controles destinados a velar por la protección y el buen uso de sus recursos.
Esta facultad, sin embargo, deberá ejercerse salvaguardando la dignidad del trabajador y su derecho a la intimidad. Por tal motivo, el Organismos debe informar claramente a sus empleados: a) cuál es el uso que el organismo espera que los empleados hagan del correo electrónico provisto por el organismo; y b) bajo qué condiciones los mensajes pueden ser objeto de control y monitoreo.
Uso del Correo Electrónico Corporativo

- Es responsabilidad del usuario del correo electrónico hacer buen uso de su cuenta entendiéndose por buen uso:

    - El uso de su cuenta para actividades institucionales administrativas de la Corporación Metropolitana de Salud.
    - Leer diariamente su correo y borrar aquellos mensajes obsoletos para liberar espacio en su buzón de correo
    - El uso de un lenguaje apropiado en sus comunicaciones
    - No permitir que segundas personas hagan uso de su cuenta de correo

- Cada usuario es responsable de respaldar sus correos en su equipo personal.
- La cuenta de correo tiene un límite de 15 MB de capacidad para cada correo enviado o recibido, en caso de que por situación estrictamente laboral requiera ampliarse el limite permitido, el usuario deberá presentar

la solicitud respectiva la misma que será aprobada por el Jefe Administrativo Financiero.

Restricciones

El usuario que tenga acceso a una cuenta de correo electrónico de la Corporación Metropolitana de Salud se compromete a NO usar este servicio para:

- Fines comerciales, políticos, particulares o cualquier otro que no sea el laboral o de investigación para la Institución.

- Enviar SPAMS de información (correo basura) o enviar anexos (archivos adjuntos) que pudiera contener información nociva para otro usuario como virus o pornografía.

- Enviar o recibir contenido ilegal, peligroso, amenazador, abusivo, tortuoso, difamatorio, vulgar, obsceno, calumnioso, que atente contra el derecho a la intimidad, racial, étnico o de cualquier otra forma ofensiva.

- Enviar o recibir cualquier anuncio no solicitado o no autorizado, materiales promociónales, correo de solicitación ("junkmail", "spam"), cartas en cadena ("chain letters), esquemas de pirámides ("pyramid schemes") o cualquier otra forma de solicitud.

- Diseminar virus, caballos de troya, gusanos y otros tipos de programas dañinos para sistemas de proceso de la información de la CMS.

- Congestionar enlaces de comunicaciones o sistemas informáticos mediante la transferencia o ejecución de archivos o programas que no son de uso de la Institución.

- Falsificar encabezados o cualquier otra forma de manipulación de identificadores para desviar el origen de algún contenido transmitido por medio del Servicio.

- Enviar o recibir por correo electrónico algún contenido que no tiene derecho a transmitir por ley o por relación contractual o fiduciaria (tal como información interna, de propiedad y confidencial adquirida o entregada como parte de las relaciones de empleo o bajo Reglamentos de confidencialidad).

- Acechar o de cualquier otra forma hostigar a usuarios de correo electrónico.

La implementación de seguridad en el Servidor de Correo Electrónico se observa en el **ANEXO F**

El proceso de implementación de las políticas de acceso e implementación de seguridad mediante contraseñas se especifica se encuentran adjuntas en el **ANEXO G.**

CONTRASEÑAS

Para reforzar la seguridad en las contraseñas se ha establecidos varios métodos de administración de los mismos en el servidor de dominio reforzando su seguridad y fortaleza para lo cual se ha establecido varios procesos.
En el **ANEXO F** se especifica la forma de reforzar los controles para las contraseñas.
Para la revisión de los privilegios de los usuarios se debe realizar el siguiente procedimiento:

1.- Cada trimestre del año, el administrador de la red enviará una nota por correo electrónico al encargado de cada área de los usuarios bajo su responsabilidad para que el gerente valide los permisos que tiene cada usuario para acceso a la red y al aplicativo.

2.- El gerente debe validar dicha información, y enviar la contestación de la nota al administrador de red, debe elegir entre las siguientes opciones:

- Mantener
- Eliminar
- Cambio de Jefe de Área
- Cambio de privilegios

3.- Dependiendo de las opciones, el administrador de la red debe ejecutar el procedimiento siguiente:

- En caso de mantener, no se debe realizar ningún cambio sobre el perfil del usuario
- Cuando el jefe de área seleccione la opción eliminar, el administrador de la red debe eliminar el perfil del usuario, en caso de algún reclamo el correo es el respaldo de dicha medida.
- En caso de que se solicite Cambio de Jefe de Área, el administrador debe enviar la información de dichos usuarios a los responsables correspondientes, para que validen los privilegios de los mismos.
- En caso de que se especifique cambio de privilegios, el administrador debe cambiar los privilegios de dicho perfil acorde a las especificaciones del responsable del usuario.

Es necesario que en la CMS se adopten medidas necesarias para proteger los equipos y la información que se encuentren en ellos cuando el usuario no se encuentre en su puesto de trabajo para lo cual se requiere:

1.- El usuario debe dejar su sesión bloqueado para que no puedan acceder a su información
2.- Cuando el usuario maneje documentación confidencial, debe guardarla bajo llave en su puesto de trabajo,

3.- En caso de usuarios de equipos portátiles, se debe dejar el computador asegurado al puesto de trabajo, en todo momento.
4.- Todo tipo de contraseñas, claves de acceso deben estar debidamente protegidos. En caso de tener algún documento electrónico donde se almacene información personal de claves, contraseñas. El mismo debe tener protección adicional como es el caso de una contraseña de seguridad.
Para poder realizar un control adecuado de los puestos de trabajos de los usuarios y de la seguridad de la información que manejan, se debe realizar semestralmente el siguiente procedimiento por parte del administrador de la red:

1.- En conjunto con el responsable de cada área, realizar la inspección de los puestos de trabajo, una vez finalizada la jornada laboral.

2.- Revisar que no se encuentre documentación de información confidencial, como plan de negocio, información personal, información financiera sin la debida protección

3.- Revisar que unidades externas no contenga información confidencial sin la protección necesaria.

4.- Revisar que las máquinas de los usuarios se encuentren correctamente apagadas, o sesiones bloqueadas en caso de que el empleado no se encuentre en la misma.

5.- Reportar al gerente o responsable del área por nota, el incumplimiento o expuesto de seguridad que haya encontrado. Identificando el expuesto de seguridad y el usuario responsable del mismo.

POLÍTICA DE UTILIZACIÓN DE LOS SERVICIOS DE RED

Las conexiones no seguras a los servicios de red pueden afectar la seguridad de toda la CMS, por lo tanto, se controlará el acceso a los servicios de red

tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos.

El administrador de la red es el responsable de otorgar los permisos tanto a servicios como recursos de la red, únicamente de acuerdo al pedido formal del responsable de cada unidad.

Este control es particularmente importante para las conexiones de red a aplicaciones que procesen información clasificada o aplicaciones críticas, o a usuarios que utilicen el acceso desde sitios de alto riesgo, por ejemplo áreas públicas o externas que están fuera de la administración y del control de seguridad de la Corporación.

Para ello, se desarrollarán procedimientos para la activación y desactivación de derechos de acceso a las redes, los cuales comprenderán:

a) Identificar las redes y servicios de red a los cuales se permite el acceso.

b) Realizar normas y procedimientos de autorización para determinar las personas y las redes y servicios de red a los cuales se les otorgará el acceso.

Para este control se implementó la asignación el procedimiento de asignación de privilegios.

AUTENTICACIÓN DE USUARIOS PARA CONEXIONES EXTERNAS

Las conexiones externas son de gran potencial para accesos no autorizados a la información del Organismo. Por consiguiente, el acceso de usuarios remotos estará sujeto al cumplimiento de procedimientos de autenticación. Existen diferentes métodos de autenticación, algunos de los cuales brindan un mayor nivel de protección que otros. Para poder implementar una mejora en la seguridad del ingreso desde el internet a nuestra red, en específico al aplicativo que se encuentra en el servidor IAS, se implementó el protocolo de encripción SSL en el servidor, para que esta se combine con la seguridad propia del software y evitar accesos no autorizados (**ANEXO H**)

PROTECCIÓN DE LOS PUERTOS (PORTS) DE DIAGNÓSTICO REMOTO

Para poder determinar cuales realmente requieren estar abiertos y cuales deben estar cerrados, en este caso vamos a trabajar con una herramienta que nos permita determinar cuales puertos se encuentran abiertos. Para nuestro caso proponemos pasos tanto para los servidores en LINUX así como los equipos en Windows, con la ayuda de una herramienta que realice este chequeo además de la administración de la red, ver **ANEXO I**. Además se establece el procedimiento para deshabilitar servicios y puertos innecesarios en los servidores.

CONFIGURACION DE ACCESO POR DEFECTO

Para asegurar que no exista alguna equivocación por parte del administrador del sistema, por defecto se configuran a los usuarios como usuario estándar, es decir sin privilegios de instalación de programas, modificación de archivos de red, desinstalación de programas y sin acceso a los sistemas y aplicaciones.
Al igual debe suceder con los módems y switch se configuran listas de control de acceso que por defecto bloqueen todo y solo permitan el paso de lo que se configura.

MONITOREO DE CONTROL DE ACCESO

Para tener un control más adecuado de la red, identificación de vulnerabilidades en la misma, que puedan conllevar a problemas de control de acceso en el **ANEXO J** se muestra la configuración que realizamos para la implementación de un firewall que nos permitirá utilizar las ventajas del sistema operativo Linux de un servidor para un mayor control de acceso. Así como también se indica en el **ANEXO K** la implementación del aplicativo MRTG que nos permitirá llevar un control del tráfico de la red para determinar un posible problema debido a un incremento considerable en el tráfico de la red.

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Se pueden establecer políticas para el manejo de información crítica que incluya controles criptográficos sobre la misma, a continuación se indica el procedimiento que se debe seguir:

1. En todas las máquinas se debe tener instalado el aplicativo de encripción PGP (**ANEXO D**), pues es un software muy útil sobre todo en redes de mediano tamaño.

2. Al momento que se desee enviar o transportar información confidencial, se debe utilizar el aplicativo PGP para encriptar dicha información.

3. La clave que se utilice para la encripción de la información se debe enviar únicamente a las personas que van a intercambiar la información encriptada. De ser necesario transmitir la información a otras personas es necesario que la persona que envíe el documento utilice diferentes claves de encripción para los diferentes destinos para que no haya la posibilidad de intercepción y recepción de información por parte de personas no autorizadas.

4. El intercambio de claves se debe realizar mediante un correo electrónico previo al envío de la información confidencial.

El procedimiento que se debe seguir para un control de cambios es el siguiente:

1.- SOLICITUD DE CAMBIO: El requerimiento de solicitud de cambios debe presentarse al responsable de la unidad, y presentarle las actividades que se van a realizar en el cambio.

2.- APROBACION DEL CAMBIO.- los requerimientos individuales de cambio deberían justificar la razón y claramente identificar los beneficios y las posibles fallas del cambio. La directiva debe analizar el requerimiento de cambio y posiblemente solicitar mayor información antes de que el cambio sea aprobado.

3.- DOCUMENTACION DEL CAMBIO.- Cuando el cambio es aprobado, debe empezar una documentación donde se vaya identificando todos los pasos que se siguieron hasta finalizar el cambio.

4.- PRUEBAS y PRESENTACION.- El cambio debe ser completamente probado para cubrir algún resultado inesperado.

5.- IMPLEMENTACION.- Cuando un cambio es completamente probado y aprobado, se programa el desarrollo para la implementación, el cual debe constar del procedimiento de monitoreo del mismo.

6.- DOCUMENTACION DE CONTROL DE CAMBIOS.- Los cambios que deben ser documentados son:

- Instalación de nuevas computadoras
- Instalación de nuevas aplicaciones
- Implementación de configuraciones diferentes
- Instalación de parches y actualizaciones
- Nuevas tecnologías integradas
- Políticas, procedimientos actualizados.
- Nuevos dispositivos conectados a la red.

RESTRICCIÓN DEL CAMBIO DE PAQUETES DE SOFTWARE

Para evitar que los usuarios puedan modificar, sin autorización previa cualquier tipo de software, las cuentas de los empleados en el dominio no tienen permisos para realizar ninguna de estas actividades, así como tampoco pueden

instalar ningún tipo de software ni remover sin previa solicitud al administrador de red y sin autorización del responsable de cada área.

CANALES ENCUBIERTOS Y CÓDIGO TROYANO

El antivirus que van a implementar en la CMS cuenta con características necesarias para detectar código troyano y canales encubiertos, por lo cual es necesario la implementación de las especificaciones realizadas para mantener el antivirus actualizado y realizar un chequeo constante de la máquina. En el **ANEXO C** se especifica la forma de configurar el antivirus en cada máquina para mantener protegidos a los usuarios.

GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION

DIVULGACIÓN DE EVENTOS Y DE DEBILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN

Cuando un incidente ha sido reportado, se pueden tomar diferentes acciones como son:

- Validar que efectivamente el incidente se ha producido
- Examinar archivos y registros para detalles del ataque
- Determinar si puede garantizarse una acción legal
- Reevaluar o modificar la seguridad de red de las computadoras en general.

Las pautas siguientes ayudan a las organizaciones a entender y responden a los varios niveles de uso de la computadora impropio.

Molestia.- Estas ofensas generalmente muestran una falta de consideración de otros usuarios de la computadora, pero no amenaza retiro o integridad de la computadora o viola cualquier principio ético. En otros términos, el individuo mostró el juicio pobre simplemente. La organización debe responder emitiendo

al usuario un verbal, copia electrónica, o hardcopy que advierte que su o sus acciones no eran aceptables.

Ética cuestionable.- Estas ofensas involucran a menudo violaciones dónde las ética de acciones son cuestionables o cuando el retiro de una persona o integridad de la computadora fueron violadas. La organización podría responder suspendiendo la cuenta del usuario o acceso de la computadora hasta una sesión formal con un Información Tecnología personal miembro se ha asistido. Una copia de la Internet acceso política de la organización debe darse al usuario con el área específica o la ofensa resaltó.

Criminal.- es cuando un usuario compromete una ofensa que requiere la investigación por local, declaración, o la entrada en vigor de la ley estatal. Cualquier usuario que compromete una ofensa delictiva debe comisar todos los derechos a los privilegios de la computadora de la organización. Cualquiera y toda la información pedidas por local, declare, o la entrada en vigor de la ley federal debe proporcionarse. Si el usuario se encuentra culpable de la ofensa bajo la investigación, debe darse por terminado el contrato con el mismo.

A continuación se detallan los pasos para iniciar el proceso de reportes de incidentes de seguridad encontrados en la CMS:

Objetivo:	Responder apropiada y rápidamente ante un incidente o "issue" de seguridad.
Roles:	Identificar al responsable del área donde se ha generado un incidente de seguridad y trabajar de forma conjunta con el administrador de la red.
Inputs:	Reporte de incidente o "issue"
Outputs:	Comunicación del incidente Respuesta ante el incidente Investigación del incidente Planes de acción correctivos Reporte de mediciones Mejora de los procesos
Consideraciones:	La fuente y calificación de severidad del incidente determina las acciones a seguir.

Tabla 4.8 Proceso de Reportes de Incidentes

Análisis del Incidente.- Los incidentes de seguridad son reportados por diferentes personas en la organización. Por lo cual es necesario que todos los incidentes reportados involucren al administrador de la red y el responsable de cada área. Para que de forma conjunta se puedan definir el procedimiento a seguir para los diferentes problemas.

Reporte del incidente.- Evaluado el incidente con el Administrador local del servicio, se realiza un registro del incidente para que se pueda hacer un seguimiento hasta la solución del mismo. Los pasos necesarios para reportar el incidente son los siguientes:

1.- Determinar si el incidente representa un serio problema como son: acceso no autorizado a información confidencial, alteración de la integridad de un servidor, negación de servicio, alteración de un servicio Web, penetración al sistema, destrucción de datos, fraude, crimen, etc.
2.- Contactar al administrador de la red para reportar el problema
3. - Describir el problema
4.- El administrador del sistema debe inmediatamente registrar el incidente en un archive para identificar información relacionada a cada evento.
5.- EL administrador conjuntamente con el responsable de cada área deben realizar el procedimiento necesario para mitigar dicho incidente en caso de existir. Estos procedimientos dependen del tipo de incidente, pues por ejemplo en caso de una vulnerabilidad en un sistema operativo debido a un virus en la red se debe eliminar el virus. Informar los procesos que deben seguir los usuarios para que el daño no se propague en la red.

ADMINISTRACIÓN DE INCIDENTES Y MEJORAS DE LA SEGURIDAD DE LA INFORMACIÓN

En este procedimiento se debe considerar:

- Como inició el incidente

- Que fallas o vulnerabilidades fueron explotadas
- Como ganaron el acceso
- Como se dieron cuenta del problema
- Como se resolvió temporalmente el incidente
- Si los procedimientos de la resolución de incidentes existentes eran adecuados o requieren la actualización

GESTION DE CONTINUIDAD DEL NEGOCIO

ASPECTOS DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO

Al desarrollar el plan de la continuidad del negocio para la CMS, se debe considerar los parámetros sobre los cuales se va a desarrollar el mismo para poder los desastres.

PROCESO DE GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Los responsables de cada área, deben determinar las aplicaciones críticas de las mismas y desarrollar procedimientos regulares para mantener respaldos continuos de los procesos críticos de cada área. El plan de contingencia de cada proceso debe considerar como mínimo:

- La administración de los recursos críticos, en caso de ser necesaria la implementación del plan de contingencia.
- Identificar los riesgos. Cada riesgo debe identificarse con qué pasos sería necesario detenerlo, pues es más barato evitar la crisis que repararla; por lo cual todos los planes deben tener un enfoque de prevención.
- Documentar el impacto de una pérdida extendida a los funcionamientos y funciones de negocio.
- Debe ser un plan entendible, fácil usar, y fácil para mantener por todos los miembros de la organización.

DESARROLLO E IMPLANTACIÓN DE PLANES DE CONTINGENCIA

El plan de contingencias desarrollado para aplicar en la CMS se adjunta en el **ANEXO B**

CUMPLIMIENTO

CUMPLIMIENTO CON LOS REQUISITOS LEGALES

DERECHOS DE PROPIEDAD INTELECTUAL

Entre los controles que recomienda la Norma ISO 27001 se considera que los empleados únicamente utilicen material autorizado por la organización.
La CMS solo debe autorizar el uso de material producido por el mismo, o material autorizado o suministrado al mismo por su titular, conforme los términos y condiciones acordadas y lo dispuesto por la normativa vigente.

SALVAGUARDA DE LOS REGISTROS DE LA ORGANIZACIÓN

Los registros críticos de la CMS se deben proteger contra pérdida, destrucción y posibles falsificaciones, los formularios que se pueden utilizar para mantener un control de los registros es:

Tipo de Registro	Sistema de Información	Período de Retención	Medio de Almacenamiento	Responsable

A fin de cumplir con estas obligaciones, se tomarán las siguientes medidas:

a) Elaborar y divulgar los lineamientos para la retención, almacenamiento, manipulación y eliminación de registros e información.
b) Preparar un cronograma de retención identificando los tipos esenciales de registros y el período durante el cual deben ser retenidos.
c) Mantener un inventario de programas fuentes de información clave.
d) Implementar adecuados controles para proteger la información y los registros esenciales contra pérdida, destrucción y falsificación.

PROTECCIÓN DE LOS DATOS Y DE LA PRIVACIDAD DE LA INFORMACIÓN PERSONAL

Para este control se redactó un Conducta que deberían cumplir los empleados, la copia firmada del compromiso será retenida en forma segura por la CMS (**ANEXO L**). A través del Compromiso de Confidencialidad se deberá advertir al empleado que determinadas actividades pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad del empleado

REVISIONES DE LA POLÍTICA DE SEGURIDAD Y DE LA CONFORMIDAD TÉCNICA

CONFORMIDAD CON LA POLÍTICA DE SEGURIDAD

El Responsable de Seguridad Informática, realizará revisiones periódicas de todas las áreas del Organismo a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad, este período como mínimo debe ser cada 6 meses. Entre las áreas a revisar se incluyen las siguientes:

a) Sistemas de información.

b) Proveedores de sistemas.

c) Propietarios de información.

d) Usuarios.

4.4. COSTOS REFERENCIALES PARA LA IMPLEMENTACIÓN DEL SISTEMA

Una vez que hemos concluido la implementación del Sistema de Gestión de Seguridad de Información en la CMS, presentamos los costos referenciales tomando en cuenta que se trata de una empresa pública sin fines de lucro, se consideró todos los costos involucrados para mejorar la seguridad en la Organización en base al previo análisis, no todas las soluciones propuestas han sido implementadas, debido al costo que estas representan, pero se ha dado un análisis para estas soluciones en caso de que la corporación las requiera en un futuro cercano.

Para el análisis económico consideramos 2 grupos principales de costos:

COSTO EN EL DISEÑO.- Este es el costo al inicio del análisis de la situación actual de la Organización, documentación para el diseño, recursos invertidos antes de la implementación del sistema.

COSTO EN LA IMPLEMENTACIÓN.- Es el costo incurrido y propuesto como resultado del estudio de las amenazas y vulnerabilidades, y los controles propuestos para minimizar los mismos.
A continuación describimos los valores para cada uno de los costos anteriores:

4.4.1. COSTO EN EL DISEÑO

Aquí se consideran los valores de los elementos necesarios previos a la implementación del SGSI. Los valores que se consideraron son:

1.- Personal.- Es el costo de las personas que trabajamos en el proyecto, considerando el tiempo invertido, la investigación involucrada, así como los recursos personales necesarios para poder realizar el diseño del SGSI y recopilar la información necesaria.

2.- Varios.- Para el SGSI es necesario tener conocimiento de la norma completa para seguir con las recomendaciones que se indican para la implementación, por lo cual fue necesario adquirir las normas para proseguir con el diseño.
En la etapa de diseño no fue necesario ningún tipo de Hardware o Software, pues lo que realizamos fue la obtención de la información necesaria de la situación actual de la CMS y su respectivo análisis.

A continuación la tabla donde se consideran los costos antes mencionados

RECURSO	DESCRIPCION	CANTIDAD	COSTO TOTAL ($)
Personal	Viáticos y Comisiones por dos meses	2	1000
Varios	Documentación de Norma ISO	1	102

	27001:2005		
	Documentación de Norma ISO 17999:2005	1	62
TOTAL			1164

Tabla 4.9 Costos de Diseño

4.4.2. COSTO EN LA IMPLEMENTACIÓN

En estos costos se consideran los valores de los elementos necesarios para la implementación del SGSI. Estos valores son los siguientes:

1.- Personal.- Es el costo de las personas que trabajamos en el proyecto, considerando el tiempo invertido, capacidad intelectual, así como los recursos personales necesarios para poder realizar la implementación del SGSI

2.- Hardware.- El hardware necesario es principalmente para cubrir el control de la seguridad física de la corporación, así como un equipo para mejorar la seguridad en la red de la CMS

3.- Software.- La mayoría de Software que utilizamos en nuestra implementación es libre, o software con licencia que ya se encuentra en la CMS. Esto lo realizamos para minimizar al máximo los gastos y aprovechar de mejor forma los recursos disponibles. Las soluciones con Software con costo no se han podido implementar porque no se pudo invertir en los mismos, pero los ponemos en consideración para referencia de la Organización.
A continuación la tabla donde se consideran los costos antes mencionados

RECURSO	DESCRIPCION	CANTIDAD	COSTO TOTAL ($)
Personal	Viáticos y Comisiones por tres meses	2	1500
Hardware	Extintores Clase C	3	1110
	Candados para portátiles	8	200
	Disco Duro para respaldos de Servidores	1	250
	Sistema de Badgets para seguridad física, tanto Hardware como Software	1	11620
	Firewall	1	2071

Software	PGP	1	239
TOTAL			16990

Tabla 4.10 Costos en la Implementación

4.4.3. COSTO TOTAL

Una vez realizado el análisis de los costos de diseño e implementación del SGSI podemos obtener el costo total para la CMS:

RECURSOS	**COSTO TOTAL ($)**
Costo en Diseño	1164
Costo en la Implementación	16990
TOTAL	**18154**

Tabla 4.11 Costos Referenciales

V
CONCLUSIONES Y RECOMENDACIONES

5.1.CONCLUSIONES

- El Sistema de Gestión de Seguridad de Información se define para cada Organización en base a los riesgos a que esté expuesta y los aspectos intrínsecos de su funcionamiento, y debe alinearse con la actividad de la organización; para realizar de forma estructurada, sistemática y metódica la gestión de la seguridad de Tecnologías de Información.

- Es necesario definir los responsables de cada recurso de la organización y de su protección, siendo conveniente delimitar claramente el área de responsabilidad de cada persona para que no existan huecos ni problemas de definiciones claras de responsabilidades.

- Las medidas para evitar accesos no autorizados y daños en los sistemas suelen ser barreras físicas y de control de cualquier tipo, pero también la ausencia de información sobre lo que contiene un área segura y la falta de signos externos que puedan hacer adivinar su contenido.

- Una adecuada monitorización del uso de los recursos de la red permiten determinar posibles cuellos de botella que derivarían en fallos del sistema y de seguridad, dando tiempo a planificar las ampliaciones o actualizaciones del sistema con la suficiente antelación.

- No es necesario extender el SGSI a toda la organización, pues lo primordial es centrarse en los procesos principales de la organización donde se concentra la mayor parte de las actividades relacionadas con la gestión de información, que suele coincidir con las áreas de sistemas de información donde la seguridad de la información que se gestiona es

crítico para el desarrollo de las actividades de negocio.

- Para poder manejar y responder de forma clara a incidencias de seguridad, es necesario tener especificado un proceso de notificación de incidencias de forma que este sea claro y conocido por todos los empleados de la organización para de esta forma minimizar la probabilidad de recurrencia en el problema.

- La seguridad para los medios de almacenamiento de información deben ser consideradas en las políticas de seguridad, estableciendo los procedimientos para protección contra robo, daño o acceso no autorizado y procedimientos para su destrucción o borrado total cuando no vayan a ser utilizados de nuevo.

- Se deben definir y documentar las reglas y derechos de acceso a los recursos del sistema de información para cada usuario o grupo de usuarios en una declaración de política de accesos. Esta política debe ser coherente con la clasificación de los activos y recorrer exhaustivamente el inventario de recursos.

- Es de gran importancia limitar la asignación de privilegios que permitan evitar los controles de acceso estándar ya que son la principal vulnerabilidad, por lo que deberán estar perfectamente identificados, asignarse sobre la base de la necesidad de uso y evento por evento y a un identificador de usuario distinto al de uso habitual. Los privilegios tienen que revisarse de forma periódica para evitar la existencia de privilegios que ya no son necesarios.

- Para determinar el alcance del SGSI se utilizó el método de las eclipses en la cual está implícita los procesos de la empresa y de esa manera permite tener una perspectiva más clara de los procesos indispensables que ayuden a cumplir con los objetivos de negocio y por ende la

identificación de los activos de información que forman parte de estos procesos.

- La planificación es una parte crucial para una adecuada implementación del SGSI, en donde se analiza el negocio para determinar los activos más importantes, posteriormente se realiza un análisis de los riesgos que las amenazas y vulnerabilidades pueden generar, los cuales serán gestionados con controles apropiadamente implementados y criterios establecidos.

- Una de las bases fundamentales es el apoyo de la alta gerencia, ya que se requiere un cambio de cultura y concientización hace necesario el impulso constante de la Dirección.

- Para la implantación de un estándar para la seguridad de la información es necesario contar con una política de seguridad adecuada. La política poner de manifiesto el compromiso de la dirección en relación a la protección de la información y establecer el marco general de seguridad para el negocio y su objetivo de negocio.

- Es primordial la elección del método de análisis de riesgos, este debe ser elegido de acuerdo a las características del negocio, para nuestro caso se escogió GMIS ya que se ajusta las características de la norma ISO 27001.

- Una de las ventajas de la norma ISO 27001 es que puede ser implementada tanto en empresas pequeñas como en grandes organizaciones.

- Se debe tomar en cuenta que el objetivo de la evaluación del riesgo es identificar y valorar los riesgos a los cuales los sistemas de información y sus activos están expuestos, para identificar y seleccionar los controles adecuados que minimicen los riesgos identificados.

- Para el establecimiento de la seguridad de la información se consideran tres pilares fundamentales: tecnología, procesos y las personas: Las empresas comúnmente invierten grandes sumas de dinero en tecnología y definición de procesos, y se han descuidado del personal de la empresa convirtiéndose así en el eslabón más débil de la cadena de seguridad, por esta razón es fundamental concienciar y fomentar la cultura de la seguridad de la información.

- La seguridad de la información no se debe considerar como un aspecto solo tecnológico sino de tipo organizacional y de gestión, es decir organizar la seguridad de la información e implementar la seguridad en base a los requerimientos de la empresa.

5.2.RECOMENDACIONES

- Identificar de forma clara cuales son los activos y asignarles un grado de protección según su criticidad, indicando como debe ser tratado y protegido; para de esta forma mantener una adecuada protección de los activos.

- Realizar análisis periódicos de los riesgos y monitorear continuamente la situación, pues la seguridad que se requiere proporcionar con un SGSI es permanente para lo cual es necesario de un proceso continuo, más no de acciones puntuales

- Documentar los procedimientos operativos, cualquiera que sea su tipo, detallándose para cada tarea sus requerimientos de programación, interdependencias con otros sistemas, tareas de mantenimiento previstas y procedimientos de recuperación ante incidentes.

- Es aconsejable que se aumente el personal que administra el departamento de IT, pues al implementar el SGSI se incrementan las responsabilidades y al recaer en una sola persona se vuelve complicada la ejecución de las diferentes tareas.

- Se deben definir el comité de recuperación ante contingencias, para que se pueda definir de forma clara las funciones y responsabilidades de cada miembro ante desastres.

- Es recomendable que el desarrollo de cualquier sistema de gestión de seguridad de información respete las normas y leyes vigentes del país, como son por ejemplo el respeto a los derechos de propiedad intelectual.

- Se recomienda la implementación de la norma 27001 porque a más de proteger la empresa, permite mejorar la imagen al exterior.

- La seguridad de la información debe ser considerada como un proceso de mejoramiento continuo y no un estado estático, en donde los nuevos requerimientos de seguridad se ajusten a los cambios de la empresa.