

“CASO DE ESTUDIO MAQUIMETALLICA” IT GOVERNANCE

3CM10

GUZMAN FLORES JESSIE PAULINA

Barrios Alvarado Daniel Alejandro
Montaño Europa Sergio
Saldaña Aguilar Gabriela

INDICE

1.- INTRODUCCIÓN.....	4
2.-TÉRMINOS Y CONDICIONES.....	5
3.- POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.....	6
4.- ORGANIZACIÓN DE LA SEGURIDAD.....	8
5.- RELACIONES CON PROVEEDORES.....	13
6.- CLASIFICACIÓN Y CONTROL DE ACTIVOS.....	14
7.- SEGURIDAD EN LA DEFINICIÓN DE PUESTOS DE TRABAJO Y LA ASIGNACIÓN DE RECURSOS.....	21
8.- GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.....	24
9.- SEGURIDAD FÍSICA Y AMBIENTAL.....	25
10.- GESTIÓN DE COMUNICACIONES Y OPERACIONES.....	36
11.- CONTROL DE ACCESOS.....	46
12.- SEGURIDAD EN LAS TELECOMUNICACIONES.....	59
13.- DESARROLLO Y MANTENIMIENTO DE SISTEMAS.....	60
14.- CIFRADO.....	66
15.- ADMINISTRACIÓN DE LA CONTINUIDAD DE LAS ACTIVIDADES....	70
16.- CUMPLIMIENTO.....	79

1 INTRODUCCIÓN

En febrero del presente año, la empresa 'Maquimetalica' convoco a especialistas en seguridad informática de la Escuela Superior de Computo (ESCOM) con el fin de conocer sus opiniones respecto a una estrategia de seguridad informática para la empresa. De estas reuniones surgió la necesidad de que todas las áreas de la empresa cuenten con una Política de Seguridad de la Información, implementada y documentada.

En consecuencia, se conformó un grupo de trabajo con el objeto de formular un modelo de Política de Seguridad de la Información que sirviera de punto de partida para la elaboración de las políticas correspondientes en cada Organismo. Dicho grupo de trabajo decidió basar el modelo en la familia de normas ISO 27000.

El presente modelo podrá sufrir modificaciones futuras, de acuerdo a las novedades que se registren en la materia que trata, las cuales serán debidamente aprobadas y comunicadas.

1.1 Alcance

La presente Política de Seguridad de la Información se dicta en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico del Organismo.

Debe ser conocida y cumplida por toda la planta de personal del Organismo, tanto se trate de directores o jefes de área como técnicos, y sea cual fuere su nivel jerárquico y su situación de revista.

2 TÉRMINOS Y CONDICIONES

A los efectos de este documento se aplicarán las siguientes definiciones:

2.1 Seguridad de la información

La información es el activo más importante de una organización, esta puede existir en varias formas y cada una de ellas debe de ser protegida. La seguridad de la información se define como el conjunto de controles y políticas aplicables dentro de la organización para proteger la información.

2.2 Evaluación de Riesgos

Debido a que la información es algo que nos preocupa demasiado, se debe realizar una evaluación de riesgos tanto de recursos físicos como no físicos para saber de qué manera podemos prevenir algún riesgo y que de esta manera podamos reducir o eliminar algún impacto que puedan ocasionar.

2.3 Administración de Riesgos

Una vez identificados los riesgos y sus posibles consecuencias, se procederá a realizar un plan el cual nos permita administrar estos riesgos e irlos resolviendo de acuerdo a su nivel de amenaza y tiempo de ejecución.

2.4 Comité de la Seguridad de la información

El Comité de Seguridad de la Información, es un cuerpo integrado por representantes de todas las áreas sustantivas del Organismo, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

2.5 Responsable de Seguridad Informática

Es la persona que se encarga de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes del Organismo que así lo requieran.

2.6 Incidente de Seguridad

Un incidente de seguridad es una ocurrencia proveniente del estado del sistema, servicio o red indicando una posible vulnerabilidad o falla en la seguridad de la información.

3 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

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 informáticos minimizando los riesgos de daño y asegurando el eficiente cumplimiento de los objetivos del Organismo. Los principios establecidos deben ser parte de la cultura organizacional, esto se asegura mediante un compromiso de las máximas autoridades del Organismo.

3.1 Objetivo

El Objetivo de este documento es proteger los recursos de información de amenazas internas o externas a la organización, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Asegurar la correcta 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 eficiencia.

Aspectos Generales

La Política se conformará de una serie de pautas sobre dominios específicos de la Seguridad de la Información, que incluyen los siguientes tópicos:

1. Organización de la Seguridad

Orientado a administrar la seguridad de la información dentro del Organismo y establecer un marco gerencial para controlar su implementación.

2.Relaciones con Terceros

Dedicado a la identificación de riesgos del acceso de terceras partes y el manejo de estas.

3.Clasificación y control de activos

Destinado a mantener una identificación de los activos del organismo para su protección.

4.Seguridad ligada a los Recursos Humanos

Orientado a reducir riesgos de error humano, comisión de ilícitos contra el Organismo o uso inadecuado de instalaciones.

5.Gestión de incidentes en la Seguridad de la Información

Dirigido a garantizar la comunicación sobre incidentes sucedidos dentro de las instalaciones en materia de Seguridad.

6.Seguridad física y ambiental

Destinado a impedir el acceso no autorizado, daños e interferencias a las sedes e información del Organismo.

7.Gestión de comunicaciones y operaciones

Orientado a garantizar el correcto funcionamiento y seguro de las instalaciones de procesamiento de la información y medios de comunicación.

8.Control de Accesos

Destinado a controlar el acceso lógico a la información.

9.Seguridad en las Telecomunicaciones

Dirigido a generar procedimientos permisivos y restrictivos acerca de las telecomunicaciones.

10.Desarrollo y mantenimiento de Sistemas

Dedicado a la exitosa incorporación de medidas de seguridad en los sistemas de información desde su desarrollo y/o implementación y durante su mantenimiento.

11.Cifrado

Destinado a la correcta utilización de controles criptográficos.

12.Administración de la continuidad de las actividades del Organismo

Orientado a contrarrestar las interrupciones de las actividades y proteger los

procesos críticos de los efectos de fallas significativas o desastres.

13.Cumplimiento

Dirigido a impedir infracciones y violaciones de las leyes del derecho civil y penal; de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos y de los requisitos de seguridad.

3.2 Sanciones Previstas por Incumplimiento

El incumplimiento de la Política de Seguridad de la Información tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud y características del aspecto no cumplido.

4 ORGANIZACIÓN DE LA SEGURIDAD

Generalidades

La presente Política de Seguridad establece la administración de la seguridad de la información, como parte fundamental de los objetivos y actividades de la empresa.

Por ello, se definirá formalmente un ámbito de gestión para efectuar tareas tales como la aprobación de la Política, la coordinación de su implementación y la asignación de funciones y responsabilidades.

Debe tenerse en cuenta que ciertas actividades la empresa pueden requerir que terceros accedan a información interna. 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 empresa y establecer los pasos a seguir para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades.

Así mismo garantizar la aplicación de medidas de seguridad adecuadas en los

accesos de terceros a la información de la empresa.

Alcance

Esta Política se aplicará a todas las áreas de la Empresa y a todas sus relaciones con terceros que impliquen el acceso a sus datos, recursos y/o a la administración y control de sus sistemas de información.

Responsabilidad

Cada uno de los integrantes del equipo, que en este caso fungirán como integrantes del Comité de Seguridad de la Información serán los responsables de impulsar la implementación de la presente Política. A su vez tendrá a cargo el mantenimiento y la presentación para la aprobación de la presente Política, ante la máxima autoridad de la empresa, 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.

El Responsable de Seguridad Informática asistirá al personal de la empresa en materia de seguridad de la información y coordinará la interacción con Organismos especializados. Asimismo, junto con los propietarios de la información, analizará el riesgo de los accesos de terceros a la información de la empresa y verificará la aplicación de las medidas de seguridad necesarias para la protección de la misma.

4.1 Infraestructura de la Seguridad de la Información

4.1.1 Comité de Seguridad de la Información

La seguridad de la información es una responsabilidad del Organismo compartida por todos los directores Generales, Jefes de Área, Gerentes o equivalentes, por lo cual se crea el Comité de Seguridad de la Información, integrado por todo el personal mencionado anteriormente, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad. El mismo contará con un Coordinador, quien cumplirá la función de impulsar la implementación de la presente Política.

Este Comité tendrá entre sus funciones:

- Revisar y proponer a la máxima autoridad de la empresa 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 de la empresa.
- Coordinar el proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de la información de la empresa frente a interrupciones imprevistas.

4.1.2 Asignación de Responsabilidades en Materia de Seguridad de la Información

El director general asigna las funciones relativas a la Seguridad Informática de la empresa a el responsable de seguridad informática, en adelante el “Responsable de Seguridad Informática”, quien tendrá a cargo las funciones relativas a la seguridad de los sistemas de información de la empresa, lo cual incluye la supervisión de todos los aspectos inherentes a seguridad informática tratados en la presente Política.

El Comité de Seguridad de la Información propondrá a la autoridad que corresponda para su aprobación la definición y asignación de las responsabilidades que surjan del presente Modelo. A continuación, se detallan los procesos de seguridad:

Proceso
Seguridad del Personal
Seguridad Física y Ambiental
Seguridad en las Comunicaciones y las Operaciones
Control de Accesos
Seguridad en el Desarrollo y Mantenimiento de Sistemas
Planificación de la Continuidad Operativa

Cabe aclarar que, si bien los propietarios pueden delegar la administración de sus funciones a personal idóneo a su cargo, conservarán la responsabilidad del cumplimiento de las mismas. La delegación de la administración por parte de los propietarios de la información será documentada por los mismos y proporcionada al

Responsable de Seguridad Informática.

4.1.3 Proceso de Autorización para Instalaciones de Procesamiento de 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 de la empresa.

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.

4.1.4 Asesoramiento Especializado en Materia de Seguridad de la Información

El Responsable de Seguridad Informática será el encargado de coordinar los conocimientos y las experiencias disponibles en el Organismo a fin de brindar ayuda en la toma de decisiones en materia de seguridad. Con el objeto de optimizar su gestión, se habilitará al Responsable de Seguridad Informática el contacto con las Unidades Organizativas de todas las Áreas de la empresa.

5 RELACIONES CON PROVEEDORES

Debido a que nuestros proveedores tienen acceso a la empresa cuando envían sus productos, se debe crear una estrecha relación con las personas que envían a entregar sus productos para evitar algún riesgo de robo.

5.1 Identificación de Riesgos del Acceso de Terceras Partes

Existen diferentes riesgos en el acceso de terceras partes a la empresa, por lo cual lo primero es identificar esos riesgos para poder mitigarlos o eliminarlos; el principal problema es el robo tanto de información como de cualquier otro recurso físico que haya en la empresa.

5.2 Requerimientos de Seguridad en Contratos o Acuerdos de Terceros

Se debe revisar los contratos que existan con terceros y que se apliquen los siguientes controles:

- Cumplimiento de las Políticas de Seguridad de la empresa.
- Protección de los activos de la empresa tanto físicos como información y software.

5.3 Tercerización

5.3.1 Requerimientos de Seguridad en contratos de Tercerización

Los contratos o acuerdos de tercerización total o parcial para la administración de y control de sistemas de información, redes y/o ambientes de PC de la empresa deben cumplir con ciertos puntos en específico, como:

- La forma en que se aplicarán los requisitos legales aplicables.
- Medios para garantizar que todos los involucrados en la tercerización estén al corriente con sus responsabilidades de seguridad

6 CLASIFICACIÓN Y CONTROL DE ACTIVOS

Generalidades

El Organismo debe tener un amplio conocimiento sobre los activos que posee como parte importante de la administración de riesgos. Algunos ejemplos son:

*Recursos Virtuales: Bases de Datos, archivos, documentación de sistemas, manuales técnicos y de usuario, material de capacitación, procedimientos operativos, planes de continuidad, etc.

*Activos Físicos: Equipo informático, de comunicaciones, mobiliario, etc.

*Servicios: Servicios informáticos y de comunicaciones, utilitarios generales.

Los activos deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad con la que cumplen, con el objeto de señalar cómo ha de ser tratada y protegida dicha información.

Este catálogo de activos debe ser constantemente actualizado ya que la información deja de ser sensible o crítica después de un cierto periodo de tiempo. Se debe de considerar la cantidad de categorías a definirse para la clasificación y que estos esquemas no sean lo bastante complejos para su uso diario.

Puesto que la información adopta muchas formas tanto en los sistemas informáticos como fuera de ellos, cada una de estas formas debe ser contemplada para asegurar la confidencialidad, integridad y disponibilidad de la información.

Por último, la información puede pasar a ser obsoleta y por lo tanto de ser necesario debe ser eliminada. La destrucción de la información es un proceso que debe asegurar la confidencialidad de la misma.

Objetivo

Garantizar que los activos de información reciban un apropiado nivel de protección clasificando la información para señalar su sensibilidad y criticidad.

Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

Política

6.1 Inventario de Activos

Se identificarán los activos importantes asociados a cada sistema de información, sus propietarios y su ubicación, para luego elaborar un inventario con dicha información. Este debe ser actualizado ante cualquier modificación de la información registrada y revisada periódicamente en lapsos no mayores a 6 meses. El encargado del inventario y de mantener su integridad es el responsable de cada departamento.

Una vez siendo identificado los activos de la empresa estos deben ser pasados a una hoja de cálculo siguiendo el formato y la clasificación siguientes:

NO.	ID	CATEGORÍA	NOMBRE

Se debe de enumerar cada activo, posteriormente se generará un id perteneciente a su categoría, es decir el id estará compuesto de un número más una letra que denota la categoría a la que pertenece, por ejemplo, si se tuvieran 2 activos pertenecientes a la categoría caja: 1A = Efectivo y 2A = Cheques

ID	CATEGORÍA
A	Caja
B	Cuentas Bancarias
C	Clientes
D	Prestamos, Créditos, Documentos y cuentas por Cobrar
E	Terrenos
F	Edificios
G	Mobiliario y Equipo
H	Maquinaria
I	Equipo de entrega
J	Equipo de Cómputo y Electrónico
K	Gastos de Instalación
L	Papelería y útiles
M	Propaganda y publicidad
N	Primas de Seguros

Ejemplo:

NO.	ID	CATEGORÍA	NOMBRE
1	1A	Caja	Efectivo
2	2A	Caja	Cheques
3	1B	Cuentas Bancarias	Depósitos Bancarios
4	1C	Clientes	Clientes varios

6.2 Clasificación de la Información

Para clasificar un activo de Información se evaluarán las tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad.

Los criterios para clasificar la sensibilidad de la información son:

Confidencialidad:

0 Pública- Información que puede ser conocida y utilizada sin autorización por cualquier persona.

1 De uso interno- Información que puede ser conocida y utilizada por todos los empleados del Organismo y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves.

2 Confidencial- Información que sólo puede ser conocida y utilizada por un grupo de

empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas al Organismo.

3 Secreta- Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección del Organismo, y cuya

divulgación o uso no autorizados podría ocasionar pérdidas graves al mismo.

Integridad:

0 Fácilmente Recuperable- Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operatoria del Organismo.

1 Recuperable- Información cuya modificación no autorizada puede repararse aunque podría ocasionar pérdidas leves para el Organismo, el Sector Público Nacional o terceros.

2 Difícil de Recuperar- Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas para el Organismo, el Sector Público Nacional o terceros.

3 No Recuperable- Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves al Organismo, al Sector Público Nacional o a terceros.

Disponibilidad:

0 Información cuya inaccesibilidad no afecta la operatoria del Organismo.

1 Información cuya inaccesibilidad permanente 2 semanas podría ocasionar pérdidas significativas para el Organismo, el Sector Público Nacional o terceros.

2 Información cuya inaccesibilidad permanente durante 5 días podría ocasionar pérdidas significativas al Organismo, al Sector Público Nacional o a terceros.

3 Información cuya inaccesibilidad permanente durante 30 minutos podría ocasionar pérdidas significativas al Organismo, al Sector Público Nacional o a terceros.

Se tomará el valor asignado a la izquierda de cada clasificación (0,1,2,3) para posteriormente revisar en cuál de las siguientes categorías entra:

-CRITICIDAD BAJA: todos los valores asignados son 0 o 1.

-CRITICIDAD MEDIA: alguno de los valores es un 2.

-CRITICIDAD ALTA: alguno de los valores es un 3.

Los criterios emitidos para la clasificación de la información según su tipo son:

ID	CATEGORÍA
A	Caja
B	Cuentas Bancarias
C	Clientes
D	Prestamos, Créditos, Documentos y cuentas por Cobrar
E	Terrenos
F	Edificios
G	Mobiliario y Equipo
H	Maquinaria
I	Equipo de entrega
J	Equipo de Cómputo y Electrónico
K	Gastos de Instalación
L	Papelería y útiles
M	Propaganda y publicidad
N	Primas de Seguros

Ejemplo: Equipo de redes es el tercer elemento perteneciente al grupo J.

3J	Equipo de Cómputo y Electrónico	Equipo de redes
----	---------------------------------	-----------------

Esto se implementará con una hoja de cálculo donde se podrá ponderar cada una de las rúbricas previamente definidas y usando fórmulas podremos establecer los rangos para identificar si cae dentro de alguna de los posibles niveles de criticidad.

De ser así se colocará una X en la celda correspondiente.

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
0	2	1

CRITICIDAD ALTA	CRITICIDAD MEDIA	CRITICIDAD BAJA
	X	

Este cambio debe ser notificados por el responsable directo, y este a su vez hacérselo saber a los usuarios con acceso a este catálogo para que conozcan la nueva clasificación. En adelante la información con valores 1,2,3 de confidencialidad será conocida como “información clasificada”.

6.3 Rotulado de la Información

Se definirán procedimientos para el rotulado y manejo de información, de acuerdo al esquema de clasificación definido. Los mismos contemplarán los recursos de información tanto en formatos físicos como electrónicos e incorporarán las siguientes actividades de procesamiento de la información:

- Copia
- Almacenamiento
- Transmisión por correo electrónico
- Transmisión oral (telefonía fija y móvil, correo de voz, contestadores automáticos, etc.).

La información será rotulada siguiendo el siguiente formato:

FORMATO:
NOMBRE:
EXTENSIÓN:
TAMAÑO:
UBICACIÓN:

Esta información debe ser almacenada en una Base de datos que funja de catálogo, por otro lado este debe ser actualizado cada que se de alta o de baja un nuevo activo informático.

7 SEGURIDAD EN LA DEFINICIÓN DE PUESTOS DE TRABAJO Y LA ASIGNACIÓN DE RECURSOS

7.1 Seguridad en la Definición de Puestos de Trabajo y la Asignación de Recursos

7.1.1 Control y Política del Personal

Las funciones y responsabilidades en materia de seguridad serán Se llevarán a cabo controles de verificación del personal en el momento en que se solicita el puesto. Estos controles incluirán todos los aspectos que indiquen las normas que, a tal efecto, alcanzan a la empresa.

Se llevarán a cabo controles de verificación del personal en el momento en que se solicita el puesto. Estos controles incluirán todos los aspectos que indiquen las normas que, a tal efecto, alcanzan a la empresa.

7.1.2 Compromiso de Confidencialidad

Como parte de sus términos y condiciones iniciales de empleo, los empleados, firmarán un Compromiso de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información de la empresa. La copia firmada del Compromiso deberá ser retenida en forma segura por el Área de Recursos Humanos u otra competente.

Formato de control de confidencialidad:

CONTRATO DE CONFIDENCIALIDAD

CONTRATO DE CONFIDENCIALIDAD QUE CELEBRAN POR UNA PARTE _____,
REPRESENTADA POR _____ Y POR LA OTRA PARTE D. _____ AL
TENOR DE LAS DECLARACIONES Y CLAUSULAS SIGUIENTES:

DECLARACIONES

Declara la Empresa _____ por conducto de su representante:

- Que es una sociedad mercantil debidamente constituida, como consta en la escritura pública otorgada ante D. _____, Notario de _____;
- D. _____ vecino de _____ con Documento de identidad _____ en representación de la mencionada empresa.

Que es su voluntad obligarse en los términos de este contrato.

Declara el Comprador, por medio de:

- D. _____ vecino de _____ con Documento de identidad _____ en representación propia.
- Que es su voluntad obligarse en los términos de este contrato.

Declaran las partes, pro conducto de sus representantes:

1. Que han decidido transmitirse mutuamente cierta información confidencial, propiedad de cada una de ellas, relacionada con tecnologías, planes de negocios internos, y otros tipos, a la que en lo sucesivo se le denominará "Información Confidencial", relativa a la venta de una de las partes de los servicios de _____;
2. Que cualquiera de ellas, en virtud de la naturaleza de este contrato, podrá constituirse como parte receptora o parte divulgante.
3. Que se reconocen mutuamente la personalidad con la que comparecen a celebrar el presente convenio y manifiestan su libre voluntad para obligarse en los términos de las siguientes:

CLAUSULAS

PRIMERA. Las partes se obligan a no divulgar a terceras partes, la "Información Confidencial", que reciban de la otra, y a darle a dicha información el mismo tratamiento que le darían a la información confidencial de su propiedad.

Para efectos del presente convenio "Información Confidencial" comprende toda la información divulgada por cualesquiera de las partes ya sea en forma oral, visual, escrita, grabada en medios magnéticos o en cualquier otra forma tangible y que se encuentre claramente marcada como tal al ser entregada a la parte receptora.

SEGUNDA. La parte receptora se obliga a mantener de manera confidencial la "Información Confidencial" que reciba de la parte divulgante y a no darla a una tercera parte diferente de sus abogados y asesores que tengan la necesidad de conocer dicha información para los propósitos autorizados en la Cláusula Sexta de este convenio, y quienes deberán estar de acuerdo en mantener de manera confidencial dicha información.

TERCERA. La parte receptora se obliga a no divulgar la "Información Confidencial" a terceros, sin el previo consentimiento por escrito de la parte divulgante.

7.1.3 Términos y Condiciones de Empleo

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 pueden extenderse más allá de los límites de la sede de la empresa y del horario normal de trabajo.

7.2 Capacitación del Usuario

7.2.1 Formación y Capacitación en Materia de Seguridad de la Información

Todos los empleados de la empresa y cuando sea pertinente, los usuarios externos y los terceros que desempeñen funciones en la empresa, recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos que sigue la empresa.

El responsable del Área de Recursos Humanos será el encargado de coordinar las acciones de capacitación que surjan de la presente Política.

Cada mes 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.

Las siguientes áreas serán encargadas de producir el material de capacitación:

Áreas Responsables del Material de Capacitación
Recursos Humanos
Área de Informática
Área de Seguridad Informática

El personal que ingrese a la empresa 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. Por otra parte, se arbitrarán los medios técnicos necesarios para comunicar a todo el personal, eventuales modificaciones o novedades en materia de seguridad.

8 GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

8.1 Comunicación de Incidentes Relativos a la Seguridad

Cuando ocurra algún incidente relacionado con la seguridad de la información se debe avisar inmediatamente a los puestos gerenciales de la empresa y por un canal que solo la gerencia pueda saberlo debido a lo sensible que puede ser la información.

También todo el personal de la empresa debe conocer el manual de procedimientos para que en caso de una emergencia ellos puedan contribuir a la solución.

El formato a ocupar es como sigue:

Nombre	Fecha	Incidente de seguridad o debilidad	Firma
Barrios Alvarado Daniel	12/06/17	Se encontró una vulnerabilidad a la hora de realizar el registro de la pieza...	

8.2 Comunicación de Debilidades en Materia de Seguridad

Los empleados, así como los usuarios del sistema de información debe informar de cualquier debilidad que ellos encuentren ya sea de manera directa o indirecta; deben de reportarse de acuerdo al manual de procedimientos que existe ya que de esta manera será más rápida la atención.

Formato:

Nombre	Fecha	Incidente de seguridad o debilidad	Firma
Barrios Alvarado Daniel	12/06/17	Se encontró una vulnerabilidad a la hora de realizar el registro de la pieza...	

8.3 Comunicación de Anomalías del Software

Se establecen procedimientos para comunicar cualquier anomalía en el software, como, por ejemplo:

- Registrar los síntomas del problema y mensajes que aparecen en pantalla
- Tener medidas de aplicación en caso de que aparezca una anomalía.
- Alertar inmediatamente al encargado de seguridad sobre lo acontecido.

8.4 Procesos Disciplinarios

Existen procesos que se deben seguir una vez que se identifiquen los problemas y se hayan solucionado, ya que también se debe identificar quién o qué fue lo que causó esa vulnerabilidad y poner un castigo a la persona que lo haya ocasionado y ese castigo dependerá de la gravedad del problema.

9 SEGURIDAD FÍSICA Y AMBIENTAL

Generalidades

La seguridad física y ambiental brinda el marco para minimizar los riesgos de daños e interferencias a la información y a las operaciones del Organismo. Asimismo, pretende evitar al máximo el riesgo de accesos físicos no autorizados, mediante el establecimiento de perímetros de seguridad.

Se distinguen tres conceptos a tener en cuenta: la protección física de accesos, la protección ambiental, protección y mantenimiento de equipamiento y documentación.

El establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles tendientes a proteger las instalaciones de procesamiento de información crítica o sensible del Organismo, de accesos físicos no autorizados. El control de los factores ambientales permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio. El equipamiento donde se almacena información es susceptible de mantenimiento periódico, lo cual implica en ocasiones su traslado y permanencia fuera de las áreas protegidas del Organismo.

Dichos procesos deben ser ejecutados bajo estrictas normas de seguridad y de preservación de la información almacenada en los mismos.

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. Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información del Organismo. Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus labores habituales. Proporcionar información al responsable del área sobre los riesgos identificados.

Política

9.1 Perímetro de Seguridad Física

La protección física se llevará a cabo mediante la creación de diversas barreras o medidas de control físicas alrededor de las sedes del Organismo, utilizará perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información, de suministro de energía eléctrica, de aire acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información.

El emplazamiento y la fortaleza de cada barrera estarán definidas por el responsable del Área Informática de acuerdo a la evaluación de riesgos efectuada.

Se implementarán los siguientes lineamientos y controles, según corresponda:

- a)** Definir y documentar claramente el perímetro de seguridad.
- b)** Verificar la existencia de un área de recepción atendida por personal. Si esto no fuera posible, el acceso a dichas áreas y edificios estará restringido exclusivamente al personal autorizado.
- c)** Extender las barreras físicas necesarias desde el piso (real) hasta el techo (real), a fin de impedir el ingreso no autorizado y la contaminación ambiental, por ejemplo, por incendio, humedad e inundación.
- d)** Identificar claramente todas las puertas de incendio de un perímetro de seguridad.

El Responsable de Seguridad Informática llevará un registro actualizado de los sitios protegidos, indicando:

- a)** Identificación del Edificio y Área.
- b)** Principales elementos a proteger.
- c)** Medidas de protección física.

9.2 Controles de Acceso Físico

Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por el Responsable de Seguridad Informática junto con el responsable del Área Informática, a fin de permitir el acceso sólo al personal autorizado. Estos controles de acceso físico tendrán, por lo menos, las siguientes características:

- a)** Supervisar o inspeccionar a los visitantes a áreas protegidas y registrar la fecha y horario de su ingreso y egreso. Sólo se permitirá el acceso mediando propósitos específicos y autorizados dando a conocer al visitante los requerimientos de seguridad del área y los procedimientos de emergencia.

b) Controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas. Se utilizarán los siguientes controles de autenticación para autorizar y validar todos los accesos: personal de guardia con listado de personas habilitadas, por tarjeta magnética o huella digital.

c) Implementar el uso de una identificación visible para todo el personal del área protegida.

d) Revisar y actualizar cada 3 meses los derechos de acceso a las áreas protegidas, los que serán documentados y firmados por el responsable de la Unidad Organizativa de la que dependa.

e) Revisar los registros de acceso a las áreas protegidas cada 2 meses. Esta tarea la realizará quien sea propuesto por el Comité de Seguridad de la Información.

Para efectos de tener un seguimiento con cada uno de los controles mencionados se apoyarán en los siguientes formatos:

a) Control de acceso para visitantes:

Deberán registrarse en una lista que portará el personal que vigila las entradas al lugar, este mismo se encargará de hacerle saber al visitante las reglas que deben ser seguidas y las precauciones que debe tener dependiendo el área al que se dirija.

Lista para controlar el acceso a la instalación:

Nombre	Fecha	Hora de ingreso	Hora de salida	Asunto	Firma
Gabriela Saldaña Aguilar	05/06/17	12:00	14:00	Arreglo de tubería rota	

- b) Para limitar el acceso a las instalaciones de procesamiento de la información es necesario portar un gafete visible con su nombre y un color que identifique su nivel de autoridad u acceso que tiene para manejar la información, estos códigos de colores solo deben ser conocidos por los jefes de cada área. Por otra parte, deben de anotarse en la lista de visitas respectiva de cada departamento:

Código de colores para acceso a visitas:


PERMISOS	COLOR
Se le permite la entrada al área común donde son atendidos los visitantes.	
Se le permite la entrada a la planta.	
Se le permite la entrada a la planta y departamentos específicos.	
Tiene acceso total.	

Lista para controlar el acceso a los departamentos:

Nombre	Fecha	Hora de ingreso	Hora de salida	Asunto	Firma
Gabriela Saldaña Aguilar	05/06/17	12:00	14:00	Arreglo de tubería rota	

- c) La identificación debe contener lo siguiente:
- *Foto tamaño billetera actual, rostro despejado.
 - *Nombre completo.
 - *Edad y Sexo
 - *Color de acceso

DATOS PERSONALES



Esta identificación cuesta alrededor de \$50.

Nombre Área	Descripción Área
Área de Recepción y Distribución	Se dispone de un área específica para descargar y cargar producto, proveniente de suministradores o para ser vendido.
Área de corte con láser	Esta área está ocupada por las máquinas CNC dedicadas a corte láser, entrada restringida.
Área de punzonado	Área restringida para personal autorizado a la utilización de las Punzonadoras.
Área de doblado	Área dedicada al doblado de láminas de distintos materiales, entrada restringida.
Área de soldado	Área existente para personal autorizado a utilizar las soldadoras.
Área de Oficinas	Área dedicada para la Organización y sus distintos departamentos.
Área de Almacenamiento	Área separada de las anteriores dedicada para el almacenamiento.
Área de peligro (uso de nitrógeno líquido, etc..)	Área sumamente restringida para personal autorizado donde se hace uso del material necesario para que las máquinas puedan trabajar correctamente.

9.3 Protección de Oficinas, Recintos e Instalaciones

Para la selección y el diseño de un área protegida se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre. También se tomarán en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad.

Asimismo, se considerarán las amenazas físicas y ambientales de seguridad potencializadas por terceros.

9.4 Desarrollo de Tareas en Áreas Protegidas

Para incrementar la seguridad de las áreas protegidas, se establecen los siguientes controles y lineamientos adicionales. Esto incluye controles para el personal que trabaja en el área protegida, así como para las actividades de terceros que tengan lugar allí:

- 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.
- c) Bloquear físicamente e inspeccionar periódicamente las áreas protegidas desocupadas.
- d) Limitar el acceso al personal del servicio de soporte externo a las áreas protegidas o a las instalaciones de procesamiento de información sensible. Este acceso, como el de cualquier otra persona ajena que requiera acceder al área protegida, será otorgado solamente cuando sea necesario y se encuentre autorizado y monitoreado. Se mantendrá un registro de todos los accesos de personas ajenas.
- e) Pueden requerirse barreras y perímetros adicionales para controlar el acceso físico entre áreas con diferentes requerimientos de seguridad, y que están ubicadas dentro del mismo perímetro de seguridad.
- f) Impedir el ingreso de equipos de computación móvil, fotográficos, de vídeo, audio o cualquier otro tipo de equipamiento que registre información, a menos que hayan sido formalmente autorizadas por el Responsable de dicho área o el Responsable del Área Informática y el Responsable de Seguridad Informática.

g) Prohibir comer, beber y fumar dentro de las instalaciones de procesamiento de la información.

9.5 Aislamiento de las Áreas de Recepción y Distribución

Se controlarán las áreas de Recepción y Distribución, las cuales estarán aisladas de las instalaciones de procesamiento de información, a fin de impedir accesos no autorizados.

Para ello se establecerán los siguientes controles físicos:

- a) Limitar el acceso a las áreas de depósito, desde el exterior de la sede del Organismo, sólo al personal previamente identificado y autorizado.
- b) Diseñar el área de depósito de manera tal que los suministros puedan ser descargados sin que el personal que realiza la entrega acceda a otros sectores del edificio.
- c) Proteger todas las puertas exteriores del depósito cuando se abre la puerta interna.
- d) Inspeccionar el material entrante para descartar peligros potenciales antes de ser trasladado desde el área de depósito hasta el lugar de uso.
- e) Registrar el material entrante al ingresar al sitio pertinente.
- f) Despejar inmediatamente el proceso de recepción o de distribución haya terminado.
- g) No impedir el trabajo de las áreas restantes.

9.6 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) Disponer de múltiples enchufes o líneas de suministro para evitar un único punto de falla en el suministro de energía.
- b) Contar con un suministro de energía interrumpible (UPS) para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas de la empresa. Los planes de contingencia contemplarán las acciones que han de emprenderse ante una falla de la UPS. Los equipos de UPS serán inspeccionados y probados periódicamente para asegurar que funcionan correctamente y que tienen la autonomía requerida.
- c) Montar un generador de respaldo para los casos en que el procesamiento deba continuar ante una falla prolongada en el suministro de energía. Deberá realizarse un análisis de impacto de las posibles consecuencias ante una interrupción prolongada del procesamiento, con el objeto de definir qué componentes será necesario abastecer de energía alternativa.

Asimismo, se procurará que los interruptores de emergencia se ubiquen cerca de las salidas de emergencia de las salas donde se encuentra el equipamiento, a fin de facilitar un corte rápido de la energía en caso de producirse una situación crítica. Se proveerá de iluminación de emergencia en caso de producirse una falla en el suministro principal de energía. Se implementará protección contra descargas eléctricas en todos los edificios y líneas de comunicaciones externas de acuerdo a las normativas vigentes.

9.7 Seguridad del Cableado

El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información estará protegido contra interceptación o daño, mediante las siguientes acciones:

- a) Utilizar piso ducto o cableado embutido en la pared, siempre que sea posible, cuando corresponda a las instalaciones de procesamiento de información.
- b) Proteger el cableado de red contra interceptación no autorizada o daño
- c) Separar los cables de energía de los cables de comunicaciones para evitar interferencias.

- d) Proteger el tendido del cableado troncal (backbone) mediante la utilización de ductos blindados.

9.8 Mantenimiento de Equipos

Se realizará el mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanentes. Para ello se debe considerar:

- a) Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.
- b) Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.
- c) Eliminar la información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.
- d) Someter el equipamiento a tareas de mantenimiento preventivo, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal del responsable del Área Informática.

9.9 Retiro de los Bienes

El uso de equipamiento destinado al procesamiento de información, fuera del ámbito de la empresa, será autorizado por el responsable patrimonial. En el caso de que en el mismo se almacene información clasificada, deberá ser aprobado además por el Propietario de la misma.

Se respetarán permanentemente las instrucciones del fabricante respecto del cuidado del equipamiento. Asimismo, se mantendrá una adecuada cobertura de seguro para proteger el equipamiento.

10 GESTIÓN DE COMUNICACIONES Y OPERACIONES

La proliferación de software malicioso, como virus, troyanos, etc., hace necesario que se adopten medidas de prevención, a efectos de evitar la ocurrencia de tales amenazas.

Debido a que nuestro sistema de información está comunicado entre sí, tanto dentro de la empresa como con terceros fuera de él, es necesario establecer criterios de seguridad en las comunicaciones que se establezcan.

OBJETIVO

Garantizar el correcto y seguro funcionamiento de las instalaciones del procesamiento de la información.

Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas.

10.1 Procedimientos y Responsabilidades Operativas

10.1.1 Documentación de los Procedimientos Operativos

Se documentará y mantendrán actualizados los procedimientos operativos identificados en esta política y se tendrá que pedir autorización para realizar algún cambio.

10.1.2 Control de Cambios en las Operaciones

Para realizar un cambio tanto en software y hardware se debe llevar un control y debe ser evaluado previamente por el encargado de TI. Aparte debe haber una bitácora con los cambios que se han realizado y los motivos de este. Los cambios deben contemplar los siguientes puntos:

- Identificación y registro de cambios significativos
- Evaluación del posible impacto de dichos cambios
- Planificación del proceso del cambio

10.1.3 Procedimientos de Manejo de Incidentes

Se establecen funciones y procedimientos de manejo de incidentes que garantice una respuesta rápida y eficaz, y se debe tomar en cuenta lo siguiente:

1. Contemplar y definir todos los tipos probables de incidentes relativos a la seguridad.
2. Implementar controles detallados sobre la recuperación sobre alguna posible violación de seguridad.

10.1.4 Separación de Funciones e Instalaciones

Se dividirán las funciones y tareas para el monitoreo e instalación de software y hardware a fin de reducir los riesgos de modificaciones o instalaciones no autorizadas. Se implementarán controles como:

- Monitoreo de las actividades.
- Registro de auditoría y control periódico del mismo.
- Que el auditor interno realice una supervisión constante.

10.2 Planificación y Aprobación de Sistemas

10.2.1 Planificación de la Capacidad

El responsable del área Informática, o el personal que éste designe, efectuará el monitoreo de las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas haciendo uso de herramientas que monitoreen el desempeño de los sistemas informáticos. Para ello tomará en cuenta además los nuevos requerimientos de los sistemas, así como las tendencias actuales y proyectadas en el procesamiento de la información del Organismo para el período estipulado de vida útil de cada componente. Asimismo, informará las necesidades detectadas a las autoridades competentes para que puedan identificar y evitar potenciales cuellos de botella, que podrían plantear una amenaza a la seguridad o a la continuidad del procesamiento, y puedan planificar una adecuada acción correctiva.

Se utilizará la versión libre (gratis) que es capaz de monitorizar más de 10,000 nodos y cubre (sin limitaciones) una monitorización de red, de servidores (basados en agentes o de forma remota) y de aplicaciones. Con funcionalidades completas de informes, alertas, integraciones con terceros vía API, etc.

A continuación, se hablará sobre Pandora FMS que es una herramienta de monitoreo de red:

Ventajas:

- Descubre todos los elementos que forman parte de la red de forma sencilla. Ayuda a la optimización de la infraestructura.
- Reduce costes aprovechando al máximo el CPD.
- Detecta cuellos de botella y rediseña la red acorde a las necesidades del sistema.
- Inventaría todos los componentes en un mismo sitio y detecta la aparición de nuevos componentes automáticamente.
- Protege el CPD y detecta ataques de seguridad.
- Detecte qué cantidad de ancho de banda utilizan las aplicaciones y actúe en base a los requerimientos de las mismas.
- Localiza geográficamente todos los componentes.

Por el momento la versión pública para la comunidad nos basta para el monitoreo de la capacidad del Sistema y para obtener estadísticas que nos ayudarán a planear una nueva infraestructura en caso de ser necesario.

Funcionalidad	Community
Monitorización de rendimiento y disponibilidad	✓
Gestión de eventos	✓
Sistema de correlación de eventos	
Recolección de logs	
Gestión centralizada empleando políticas de monitorización	
Actualizaciones de seguridad certificadas	
Geolocalización	✓
Administración por línea de comando	✓
Autenticación LDAP/AD	
Virtualización y cloud computing	
Alta disponibilidad	✓
Escalabilidad horizontal (Metaconsola)	

Monitorización de servicios (BAM)	
Consola visual personalizable	✓
Módulos sintéticos (creación de datos dinámicamente sobre datos existentes)	
Base de datos de histórico para almacenar datos a largo plazo	
Distribución centralizada de plugins	
Capacidad recomendada por servidor	1000 agentes
Monitorización z/OS	
Monitorización SAP R3	

10.2.2 Aprobación del Sistema

El responsable del Área Informática y el Responsable de Seguridad Informática sugerirán criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, solicitando la realización de las pruebas necesarias antes de su aprobación definitiva. Se deben considerar los siguientes puntos:

- a) Verificar el impacto en el desempeño y los requerimientos de capacidad de las computadoras.
- 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 del nuevo sistema no afectará negativamente los sistemas existentes, especialmente en los períodos pico de procesamiento.
- f) Disponer la realización de entrenamiento en la operación y/o uso de nuevos sistemas.

10.3 Protección Contra Software Malicioso

10.3.1 Controles Contra Software Malicioso

- a) El Responsable de Seguridad Informática definirá controles de detección y prevención para la protección contra software malicioso. El responsable del Área Informática, o el personal designado por éste, implementará dichos controles, así como desarrollar procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.
- b) Prohibir el uso de software no autorizado por la empresa.

- c) Redactar procedimientos para evitar los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas, o por cualquier otro medio, señalando las medidas de protección a tomar.
- d) Instalar y actualizar periódicamente software de detección y reparación de virus, examinando computadoras y medios informáticos, como medida precautoria y rutinaria.
- e) Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles
- f) 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.
- g) Redactar procedimientos para verificar toda la información relativa a software malicioso, garantizando que los boletines de alerta sean exactos e informativos.

10.4 Mantenimiento

10.4.1 Resguardo de la Información

El encargado de IT determinará los requerimientos para resguardar el software o dato en función de su valor. Existen procedimientos para el resguardo de la información y estos deben considerar:

1. Tener un control mediante ID sobre todas las copias que se han hecho, así de esta manera será más fácil identificarlas y administrarlas.
2. Checar continuamente los medios de almacenamiento para verificar el espacio disponible y corroborar que aún se encuentran en un estado de vida óptimo.
3. Probar los mecanismos de restauración de la información, para que de esta manera cuando se presente una falla, el método sea el más eficiente y no exista una vulnerabilidad.

Para crear el back up de la información utilizaremos:

Hp DL380 Work Station - Servidor 32gb Ram Y 600 Gb Hd, el cual nos permitirá crear el respaldo de nuestra información de manera periódica y el costo por comprarlo sería de \$12,000.

10.4.2 Registro de Actividades del Personal Operativo

El encargado de IT revisará que se lleve un registro de las operaciones que realiza el personal en los sistemas, por ejemplo:

1. El tiempo de inicio y cierre del sistema.
2. Errores del sistemas y medidas correctivas.
3. Intentos de acceso al sistema por medio de dispositivos externos o software malicioso.
4. Cambio de información crítica.

10.4.3 Registro de Fallas

El encargado de IT revisará que el registro y reporte de fallas siga las normas establecidas anteriormente, al igual que revisará el cumplimiento o arreglo de dichas falla, revisará que los controles o la información no fue comprometida y que la documentación de la falla fue realizada correctamente.

10.5 Administración de la Red

10.5.1 Controles de Red

El Responsable de Seguridad Informática definirá e implementará controles para garantizar la seguridad de los datos y los servicios conectados en las redes de la empresa, contra el acceso no autorizado, considerando la ejecución de las siguientes acciones:

- Establecer los procedimientos para la administración del equipamiento remoto, incluyendo los equipos en las áreas usuarias.

- Establecer controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados.
- Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información.

10.6 Administración y Seguridad de los Medios de Almacenamiento

10.6.1 Procedimientos de Manejo de la Información

Se definirán procedimientos para el manejo y almacenamiento de la información. En los procedimientos se contemplarán las siguientes acciones:

- a) Incluir en la protección a documentos, sistemas informáticos, redes, computación móvil, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general, multimedia, servicios e instalaciones postales, uso de máquinas de fax y cualquier otro ítem potencialmente sensible.
- b) Restringir el acceso solo al personal debidamente autorizado
- c) Mantener un registro formal de los receptores autorizados de datos
- d) Proteger los datos en espera ("colas").
- e) Conservar los medios de almacenamiento en un ambiente que concuerde con las especificaciones de los fabricantes o proveedores.

10.6.2 Seguridad de la Documentación del Sistema

La documentación del sistema puede contener información sensible, por lo que se considerarán los siguientes recaudos para su protección:

- a) Almacenar la documentación del sistema en forma segura.
- b) Restringir el acceso a la documentación del sistema al personal estrictamente necesario. Dicho acceso será autorizado por el Propietario de la Información relativa al sistema.

10.7 Intercambios de Información y Software

10.7.1 Acuerdos de Intercambio de Información y Software Software

Cuando se realicen acuerdos entre empresas para el intercambio de información y software, se especificarán el grado de sensibilidad de la información de la empresa involucrada y las consideraciones de seguridad sobre la misma. Se tendrán en cuenta los siguientes aspectos:

- a) Responsabilidades gerenciales por el control y la notificación de transmisiones, envíos y recepciones.
- b) Procedimientos de notificación de emisión, transmisión, envío y recepción.
- c) Normas técnicas para el empaquetado y la transmisión.
- d) Responsabilidades y obligaciones en caso de pérdida de datos.
- e) Términos y condiciones de la licencia bajo la cual se suministra el software.
- f) Información sobre la propiedad de la información suministrada y las condiciones de su uso.
- g) Normas técnicas para la grabación y lectura de la información y del software.
- h) Controles especiales que puedan requerirse para proteger ítems sensibles.

Todos estos puntos se regularán por medio del antivirus, ya que Karpesky en su versión empresarial nos ayuda a monitorear los correos electrónicos y negar descargas sin una autorización del encargado del área.

Se escogió este antivirus, ya que a la hora estar realizando el análisis de los diferentes proveedores de este servicio, se determinó que era el más adecuado para los requerimientos de la empresa, el costo de la licencia e instalación es de \$4,500.

10.7.2 Seguridad del Correo Electrónico

Se implementarán controles para reducir los riesgos de incidentes de seguridad:

1. La vulnerabilidad de los mensajes al acceso o modificación no autorizadas o la negación del servicio
2. Posible interceptación y el consecuente acceso a los mensajes en los medios de transferencia que intervienen en la distribución de los mismos.
3. Que la contraseña la sepa únicamente la persona propietaria del correo electrónico, ya que si la contraseña es pública puede generar robo de información.
4. La posible recepción de código malicioso en un mensaje de correo electrónico, el cual afecte la seguridad de la computadora o de la red.

10.7.3 Política de Correo Electrónico

1. Protección contra ataques al correo electrónico, por ejemplo, virus, interceptación, etc.
2. Protección de archivos adjuntos de correo electrónico.
3. Uso de técnicas criptográficas para proteger la confidencialidad e integridad de los mensajes electrónicos.
4. Controles adicionales para examinar mensajes electrónicos que no pueden ser autenticados.
5. Definición de los alcances del uso del correo electrónico por parte del personal de la empresa.

10.7.4 Seguridad de los Sistemas Electrónicos de Oficina

Se controlarán los servicios de comunicación y distribución como computadoras, teléfonos móviles, laptops, tablets, correo electrónico, etc.

Al interconectar dichos medios, se considerarán las implicancias en lo que respecta a la seguridad y a las actividades propias de la empresa, incluyendo:

1. Vulnerabilidades de la información en los sistemas de oficina, por ejemplo, la grabación de llamadas telefónicas o teleconferencias, la confidencialidad de las llamadas.
2. Exclusión de categorías de información sensible de la empresa, si el sistema no brinda un adecuado nivel de protección.
3. Limitación del acceso a la información de las actividades que desarrollan determinadas personas, por ejemplo, aquellas que trabaja en proyectos sensibles.
4. Restricción de acceso a determinadas instalaciones a específicas categorías de usuarios.
5. Identificación de la posición o categoría de los usuarios, por ejemplo, empleados de la empresa.

11 CONTROL DE ACCESOS

Generalidades

El acceso por medio de un sistema de validaciones y excepciones a la información es la base de todo sistema de seguridad informática. Para impedir el acceso no autorizado a los sistemas de información se deben implementar procedimientos formales para controlar los de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

Objetivo

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.

Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.

Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.

11.1 Requerimientos para el Control de Acceso

11.1.1 Política de Control de Accesos

En la aplicación de controles de acceso, se contemplarán los siguientes aspectos:

- a) Identificar los requerimientos de seguridad de cada una de las aplicaciones.
- b) Identificar toda la información relacionada con las aplicaciones.
- c) Establecer criterios coherentes entre esta Política de Control de Acceso y la Política de Clasificación de Información de los diferentes sistemas y redes.
- d) Apoyarnos en el análisis de Riesgos para la elección de controles de acceso.
- e) Identificar la legislación aplicable y las obligaciones contractuales con respecto a la protección del acceso a datos y servicios.
- f) Definir los perfiles de acceso de usuarios estándar, comunes a cada categoría de puestos de trabajo.
- g) Administrar los derechos de acceso en un ambiente distribuido y de red, que reconozcan todos los tipos de conexiones disponibles.

11.1.2 Reglas de Control de Acceso

Las reglas de control de acceso especificadas, deberán:

- a) Indicar expresamente si las reglas son obligatorias u optativas
- b) Establecer reglas sobre la premisa “Todo debe estar prohibido a menos que se permita expresamente”.
- c) Controlar los cambios en los rótulos de información que son iniciados automáticamente.
- d) Controlar los cambios en los permisos de usuario que son iniciados automáticamente.

Reglas para el control de acceso a la información:

- * Sólo el jefe de cada departamento está autorizado a reportar los cambios de la información que le pertenece.
- * Los cambios hechos a la información deben inmediatamente actualizados en la copia de seguridad que se tiene de ellos, de esto se encargará el área de respaldo y seguridad de la información.
- * El encargado de modificar los permisos de usuarios es el departamento de IT, se debe hacer una petición de modificación del perfil del usuario.
- * Toda información perteneciente a la organización debe estar rotulada e indexada en el catálogo correspondiente, esto es obligatorio para el departamento encargado del respaldo y seguridad de la información.
- * Se debe crear una bitácora por día de los movimientos realizados sobre un grupo dado de información, se debe guardar el nombre del usuario que tiene acceso, información a la que accede, estado antes de la modificación y después de, fecha y hora de la modificación.

11.2 Administración de Acceso de Usuarios

Con el objetivo de impedir el acceso no autorizado a la información se implementarán procedimientos formales para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información.

11.2.1 Registración de Usuarios

El Responsable de Seguridad Informática definirá un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información multiusuario.

Las reglas son:

- a) Utilizar identificadores de usuario únicos, de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo empleado.
- b) Verificar que el usuario tiene autorización del Propietario de la Información para el uso del sistema, base de datos o servicio de información.
- c) Verificar que el nivel de acceso otorgado es adecuado para el propósito de la función del usuario y es coherente con la Política de Seguridad del Organismo.
- d) Entregar a los usuarios un detalle escrito de sus derechos de acceso.
- e) Requerir que los usuarios firmen declaraciones señalando que comprenden y aceptan las condiciones para el acceso.
- f) Garantizar que los proveedores de servicios no otorguen acceso hasta que se hayan completado los procedimientos de autorización.
- g) Mantener un registro formal de todas las personas registradas para utilizar el servicio.
- h) Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización, se desvincularon del Organismo o sufrieron la pérdida/robo de sus credenciales de acceso.

i) Efectuar revisiones periódicas con el objeto de:

- cancelar identificadores y cuentas de usuario redundantes
- inhabilitar cuentas inactivas por más de 1 mes
- eliminar cuentas inactivas por más de 3 meses

En el caso de existir excepciones, deberán ser debidamente justificadas y aprobadas.

j) Garantizar que los identificadores de usuario redundantes no se asignen a otros usuarios.

k) Incluir cláusulas en los contratos de personal y de servicios que especifiquen sanciones si el personal o los agentes que prestan un servicio intentan accesos no autorizados.

El procedimiento es como sigue:

Al momento de hacer una petición de acceso al sistema primero debe de validar su existencia dentro de la Base de datos, una vez siendo validado se procede a revisar sus credenciales para establecer los filtros necesarios y asegurarse de que sólo pueda entrar a la información a la que tiene permiso según su nivel de acceso otorgado. Una vez dentro se genera el registro en el historial de acceso al sistema. Si el usuario permanece más de 5 min sin actividad se suspenderá su sesión. En caso de no estar autorizado, de igual manera se suspenderá su sesión y se mandará una alerta de acceso denegado.

11.2.2 Administración de Privilegios

Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor más importante que contribuye al más uso de la información dentro del Sistema.

Los sistemas multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal. El proceso es el siguiente:

- a) Identificar los privilegios asociados a cada producto del sistema.
- b) Asignar los privilegios a individuos sobre la base del requerimiento mínimo para su rol funcional.
- c) Mantener un proceso de autorización y un registro de todos los privilegios asignados.
- d) Establecer un período de vigencia para el mantenimiento de los privilegios luego del cual los mismos serán revocados.

11.2.3 Administración de Contraseñas de Usuario

La asignación de contraseñas se controlará a través de un proceso de administración formal, mediante el cual deben respetarse los siguientes pasos:

- a) Requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto y las contraseñas de los grupos de trabajo exclusivamente entre los miembros del grupo.
- b) Garantizar que se den a conocer los cambios en las contraseñas iniciales que les han asignado a los usuarios.
- c) Generar contraseñas provisionales seguras para otorgar a los usuarios.
- d) Almacenar las contraseñas sólo en sistemas informáticos protegidos.
- e) Utilizar otras tecnologías de autenticación y autorización de usuarios, como ser la biométrica

f) Configurar los sistemas de tal manera que:

- las contraseñas tengan al menos 8 caracteres incluyendo: números, letras mayúsculas y minúsculas, y alguno de los siguientes caracteres especiales * :) (? # % & /
- solicitar el cambio de la contraseña cada que se necesite.
- establecer un tiempo de vida mínimo de 1 semana para las contraseñas.

11.2.4 Revisión de Derechos de Acceso de Usuarios

A fin de mantener un control eficaz del acceso a los datos y servicios de información, el Propietario de la Información de que se trate llevará a cabo un proceso formal, a intervalos regulares mensuales, a fin de revisar los derechos de acceso de los usuarios. Se deberán contemplar los siguientes controles:

- a) Revisar los derechos de acceso de los usuarios a intervalos mensuales
- b) Revisar las autorizaciones de privilegios especiales de derechos de acceso a intervalos mensuales
- c) Revisar las asignaciones de privilegios a intervalos mensuales, a fin de garantizar que no se obtengan privilegios no autorizados.

11.3 Responsabilidades del Usuario

11.3.1 Equipos Desatendidos en Áreas de Usuarios

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.

El Responsable de Seguridad Informática debe coordinar con el Área de Recursos Humanos las tareas de concientización a todos los usuarios y contratistas, acerca de los requerimientos y procedimientos de seguridad, para la protección de equipos

desatendidos, así como de sus funciones en relación a la implementación de dicha protección.

Los usuarios cumplirán con las siguientes pautas:

- a) Concluir las sesiones activas al finalizar las tareas, a menos que puedan protegerse mediante un mecanismo de bloqueo adecuado, por ejemplo, un protector de pantalla protegido por contraseña.
- b) Proteger las PC's o terminales contra usos no autorizados mediante un bloqueo de seguridad o control equivalente.

11.4 Control de Acceso a la Red

11.4.1 Política de Utilización de los Servicios de Red

Las conexiones no seguras a los servicios de red pueden afectar a toda la empresa, 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.

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 empresa.

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.
- c) Establecer controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red.

11.4.2 Autenticación de Usuarios para Conexiones Externas

Las conexiones externas son de gran potencial para accesos no autorizados a la información de la empresa.

Por consiguiente, el acceso de usuarios remotos estará sujeto al cumplimiento de procedimientos de autenticación. El Responsable de Seguridad Informática, conjuntamente con el Propietario de la Información de que se trate, realizarán una evaluación de riesgos a fin de determinar el mecanismo de autenticación que corresponda en cada caso. La autenticación de usuarios remotos puede llevarse a cabo utilizando:

- a) Un método de autenticación físico (por ejemplo tokens de hardware), para lo que debe implementarse un procedimiento que incluya:
 - Asignación de la herramienta de autenticación.
 - Registro de los poseedores de autenticadores.
 - Método de revocación de acceso del autenticador, en caso de compromiso de seguridad.
- b) Un protocolo de autenticación (por ejemplo desafío / respuesta), para lo que debe implementarse un procedimiento que incluya:
 - Establecimiento de las reglas con el usuario.
 - Establecimiento de un ciclo de vida de las reglas para su renovación.

Los procedimientos y controles de re-llamada, o dial-back, pueden brindar protección contra conexiones no autorizadas a las instalaciones de procesamiento de información de la empresa.

11.4.3 Protección de los Puertos (Ports) de Diagnóstico Remoto

Algunas computadoras son administradas con una herramienta de diagnóstico remoto. Si no están protegidos, estos puertos de diagnóstico proporcionan un medio de acceso no autorizado. Por lo cual deberán ser protegidas por un mecanismo adecuado el cual niegue cualquier acceso ajeno a la empresa.

11.4.4 Subdivisión de Redes

Para controlar la seguridad en redes extensas, se podrán dividir en dominios lógicos separados. Para esto se definirán y documentarán los perímetros de seguridad que sean convenientes. Estos perímetros se implementarán mediante la instalación de firewalls.

11.4.5 Acceso a Internet

El acceso a Internet será utilizado con propósitos autorizados o con el destino por el cual fue provisto. El responsable de IT definirá procedimientos para solicitar y aprobar accesos a Internet, los accesos serán autorizados formalmente por los gerentes responsables de cada área ya que cada área maneja distintas necesidades.

11.4.6 Control de Conexión a la Red

Se implementarán controles para limitar la capacidad de conexión de los usuarios, dichos controles se podrán implementar en los "gateways" que separen los diferentes dominios de la red. Algunas de las restricciones serían:

- Páginas de juegos o apuestas.
- Páginas de pornografía.
- Transferencias de archivos.

11.4.7 Seguridad de los Servicios de Red

El responsable de IT definirá las pautas para garantizar la seguridad de los servicios de red de la empresa, tanto públicos como privados. Para ello se tendrán en cuenta las siguientes opciones:

- Mantener instalados y habilitados sólo aquellos servicios que sean utilizados.
- Controlar el acceso lógico a los servicios, tanto a su uso como a su administración.
- Configurar cada servicio de manera segura, evitando las vulnerabilidades que pudieran presentar.

- Instalar periódicamente las actualizaciones de seguridad.

11.5 Control de Acceso al Sistema Operativo

11.5.1 Identificación Automática de Terminales

El responsable de IT realizará una evaluación de riesgos a fin de determinar el método de protección adecuado para el acceso al sistema operativo.

11.5.2 Procedimientos de Conexión de Terminales

El acceso a los servicios de información sólo será posible a través de un proceso de conexión seguro. El procedimiento de conexión en un sistema informático será diseñado para minimizar la oportunidad de acceso no autorizado.

Este procedimiento, por lo tanto, debe divulgar la mínima información posible acerca del sistema, a fin de evitar proveer de asistencia innecesaria a un usuario no autorizado.

El procedimiento de identificación deberá:

- a) Mantener en secreto los identificadores de sistemas.
- b) Desplegar un aviso general advirtiendo que sólo los usuarios autorizados pueden acceder a la computadora.
- c) Evitar dar mensajes de ayuda que pudieran asistir a un usuario no autorizado durante el procedimiento de conexión. Apoyarse en el análisis de riesgos.
- d) Validar la información de la conexión sólo al completarse la totalidad de los datos de entrada. Si surge una condición de error, el sistema no debe indicar que parte de los datos es correcta o incorrecta.
- e) Limitar el número de intentos de conexión no exitosos permitidos y:
 - Registrar los intentos no exitosos.
 - Impedir otros intentos de identificación, una vez superado el límite permitido.

- Desconectar conexiones de comunicaciones de datos.
- f) Limitar el tiempo máximo permitido para el procedimiento de conexión. Si este es excedido, el sistema debe finalizar la conexión.
- g) Desplegar la siguiente información, al completarse una conexión exitosa:
- Fecha y hora de la conexión exitosa anterior.

El procedimiento es el siguiente:

Si se requiere acceder a un servicio, se deberá abrir una sesión con un máximo de 3 intentos, la interfaz será austera con los datos suficientes como para realizar la tarea, se deberá de iniciar un temporizador que le de como máximo 30 minutos para conectarse al servicio, una vez terminada la conexión se debe registrar esto en la bitácora y desplegar la fecha y hora de conexión al servicio.

11.5.3 Identificación y Autenticación de los Usuarios

Todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán 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.

En circunstancias excepcionales, cuando existe un claro beneficio para el Organismo, podrá utilizarse un identificador compartido para un grupo de usuarios o una tarea específica.

El id será alfanumérico no mayor a 8 caracteres. Se puede usar el código ASCII por completo.

11.5.4 Sistema de Administración de Contraseñas

Las contraseñas constituyen uno de los principales medios de validación de la autoridad de un usuario para acceder a un servicio informático. Los sistemas de administración de contraseñas deben constituir una herramienta eficaz e interactiva que garantice contraseñas de calidad. El Sistema de administración de contraseñas debe:

- Imponer el uso de contraseñas individuales para determinar responsabilidades.
- Permitir que los usuarios seleccionen y cambien sus propias contraseñas (luego de cumplido el plazo mínimo de mantenimiento de las mismas) e incluir un procedimiento de confirmación para contemplar los errores de ingreso, dichas contraseñas deberán ser reportadas al encargado de IT para que en caso de olvido se pueda recuperar.
- Imponer una selección de contraseñas de calidad según lo señalado en el punto "Uso de Contraseñas".
- Imponer cambios en las contraseñas en aquellos casos en que los usuarios mantengan sus propias contraseñas, según lo señalado en el punto "Uso de Contraseñas".
- Obligar a los usuarios a cambiar las contraseñas provisorias en su primer procedimiento de identificación, en los casos en que ellos seleccionen sus contraseñas.
- Mantener un registro de las últimas contraseñas utilizadas por el usuario, y evitar la reutilización de las mismas.
- Evitar mostrar las contraseñas en pantalla, cuando son ingresadas.
- Almacenar en forma separada los archivos de contraseñas y los datos de sistemas de aplicación.
- Almacenar las contraseñas en forma cifrada utilizando un algoritmo de cifrado unidireccional.
- Modificar todas las contraseñas predeterminadas por el vendedor, una vez instalado el software y el hardware (por ejemplo claves de impresoras, hubs, routers, etc.).
- Garantizar que el medio utilizado para acceder/utilizar el sistema de contraseñas, asegure que no se tenga acceso a información temporal o en

tránsito de forma no protegida.

11.5.5 Limitación del Horario de Conexión

Las restricciones al horario de conexión deben suministrar seguridad adicional a las aplicaciones de alto riesgo. La limitación del periodo durante el cual se permiten las conexiones de terminales a los servicios informáticos reduce el espectro de oportunidades para el acceso no autorizado. Se implementará un control de esta índole para aplicaciones informáticas sensibles, especialmente aquellas terminales instaladas en ubicaciones de alto riesgo.

12 SEGURIDAD EN LAS TELECOMUNICACIONES

12.1 Registro y Revisión de Eventos

12.2 Monitoreo del Uso de los Sistemas

12.3 Sincronización de Relojes

A fin de garantizar la exactitud de los registros de auditoría, al menos los equipos que realicen estos registros, deberán tener una correcta configuración de sus relojes. Para ello, se dispondrá de un procedimiento de ajuste de relojes, el cual indicará también la verificación de los relojes contra una fuente externa del dato y la modalidad de corrección ante cualquier variación significativa.

12.4 Trabajo Remoto

El trabajo remoto utiliza tecnología de comunicaciones para permitir que el personal trabaje en forma remota desde un lugar externo la empresa, el trabajo remoto sólo será autorizado por la alta gerencia, o superior jerárquico correspondiente, a la cual pertenezca el usuario solicitante, conjuntamente con el responsable de IT, cuando se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con la política, normas y procedimientos existentes.

13 DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Generalidades

El desarrollo y mantenimiento de las aplicaciones es un punto crítico de la seguridad. Durante el análisis y diseño de los procesos que soportan estas aplicaciones se deben identificar, documentar y aprobar los requerimientos de seguridad a incorporar durante las etapas de desarrollo e implementación. Adicionalmente, se deberán diseñar controles de validación de datos de entrada, procesamiento interno y salida de datos.

Se deben implementar controles que eviten maniobras riesgosas por parte de estas personas u otras que puedan operar sobre los sistemas, bases de datos y plataformas de software de base y en el caso de que se lleven a cabo, identificar rápidamente al responsable.

Asimismo, 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.

Objetivo

Asegurar la inclusión de controles de seguridad y validación de datos en el desarrollo de los sistemas de información.

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.

13.1 Requerimientos de Seguridad de los Sistemas

13.1.1 Análisis y Especificaciones de los Requerimientos de Seguridad

Esta Política se implementa para incorporar seguridad a los sistemas de información (propios o de terceros) y a las mejoras o actualizaciones que se les incorporen. Los requerimientos para nuevos sistemas o mejoras a los existentes especificarán la necesidad de controles. Estas especificaciones deben considerar los controles automáticos a incorporar al sistema, como así también controles y manuales de apoyo.

Se deben tener en cuenta las siguientes consideraciones:

- a) Definir un procedimiento para que durante las etapas de análisis y diseño del sistema, se incorporen a los requerimientos, los correspondientes controles de seguridad. Este procedimiento debe incluir una etapa de evaluación de riesgos previa al diseño, para definir los requerimientos de seguridad e identificar los controles apropiados. Las áreas involucradas podrán solicitar certificaciones y evaluaciones independientes para los productos a utilizar.
- b) Evaluar los requerimientos de seguridad y los controles requeridos, teniendo en cuenta que éstos deben ser proporcionales en costo y esfuerzo al valor del bien que se quiere proteger y al daño potencial que pudiera ocasionar a las actividades realizadas.
- c) Considerar que los controles introducidos en la etapa de diseño, son significativamente menos costosos de implementar y mantener que aquellos incluidos durante o después de la implementación.

13.2 Seguridad de los Archivos del Sistema

Para evitar la pérdida, modificación o uso inadecuado de los datos pertenecientes a los sistemas de información, se establecerán controles y registros de auditoría, verificando:

- La validación de datos de entrada.
- El procesamiento interno.
- La autenticación de mensajes (interfases entre sistemas).
- La validación de datos de salida.

13.2.1 Control del Software Operativo

- Se definen los siguientes controles a realizar durante la implementación del software en producción, a fin de minimizar el riesgo de alteración de los sistemas:
- Ningún programador o analista de desarrollo y mantenimiento de aplicaciones podrá acceder a los ambientes de producción.
- Toda aplicación tendrá un único responsable designado formalmente por el responsable del Área Informática.
- El responsable del Área Informática, propondrá para su aprobación por parte del superior jerárquico que corresponda, la asignación de la función de “implementador” al personal de su área que considere adecuado, quien tendrá como funciones principales:
- Coordinar la implementación de modificaciones o nuevos programas en el ambiente de Producción.
- Asegurar que los sistemas aplicativos en uso, en el ambiente de Producción, sean los autorizados y aprobados de acuerdo a las normas y procedimientos vigentes.
- Instalar las modificaciones, controlando previamente la recepción de la prueba aprobada por parte del Analista Responsable, del sector encargado del testeo y del usuario final.
- Rechazar la implementación en caso de encontrar defectos y/o si faltara la documentación estándar establecida.

- Otros controles a realizar son:
- Guardar sólo los ejecutables en el ambiente de producción.
- Retener las versiones previas del sistema, como medida de contingencia.
- Definir un procedimiento que establezca los pasos a seguir para implementar las autorizaciones y conformes pertinentes, las pruebas previas a realizarse, etc.
- Evitar, que la función de implementador sea ejercida por personal que pertenezca al sector de desarrollo o mantenimiento.

13.2.2 Control de Cambios a Datos Operativos

Se definirá un procedimiento para que durante la etapa de diseño, se incorporen controles de validación a fin de eliminar o minimizar los riesgos de fallas de procesamiento y/o vicios por procesos de errores.

13.3 Seguridad de los Procesos de Desarrollo y Soporte

Esta Política provee seguridad al software y a la información del sistema de aplicación, por lo tanto se controlarán los entornos y el soporte dado a los mismos.

13.3.1 Procedimiento de Control de Cambios

A fin de minimizar los riesgos de alteración de los sistemas de información, se implementarán controles estrictos durante la implementación de cambios imponiendo el cumplimiento de procedimientos formales. Éstos garantizarán que se cumplan los procedimientos de seguridad y control, respetando la división de funciones.

Para ello se establecerá un procedimiento que incluya las siguientes consideraciones:

- a) Verificar que los cambios sean propuestos por usuarios autorizados y respete los términos y condiciones que surjan de la licencia de uso.
- b) Mantener un registro de los niveles de autorización acordados.
- c) Solicitar la autorización del Propietario de la Información, en caso de tratarse de

cambios a sistemas de procesamiento de la misma.

d) Identificar todos los elementos que requieren modificaciones (software, bases de datos, hardware).

e) Revisar los controles y los procedimientos de integridad para garantizar que no serán comprometidos por los cambios.

f) Obtener aprobación formal por parte del Responsable del Área Informática para las

tareas detalladas, antes que comiencen las tareas.

g) Solicitar la revisión del Responsable de Seguridad Informática para garantizar que no se violen los requerimientos de seguridad que debe cumplir el software.

h) Efectuar las actividades relativas al cambio en el ambiente de desarrollo.

i) Actualizar la documentación para cada cambio implementado, tanto de los manuales de usuario como de la documentación operativa.

j) Mantener un control de versiones para todas las actualizaciones de software.

k) Garantizar que la implementación se llevará a cabo minimizando la discontinuidad de las actividades y sin alterar los procesos involucrados.

l) Informar a las áreas usuarias antes de la implementación de un cambio que pueda afectar su operatoria.

El procedimiento es como sigue:

Si llegase a haber un cambio dentro del Sistema se deberá generar un reporte que contenga los cambios por departamento realizados, para que de esta manera el encargado de IT los procese con su equipo de trabajo y se actualicen. Finalmente se hará saber al resto de los departamentos involucrados los nuevos cambios.

Reporte de modificaciones:

Fecha	Departamento	Acción	Descripción
12/08/17	Ventas	Eliminación	Se ha eliminado del catálogo de clientes, al cliente con id : Q21JH00F

13.3.2 Desarrollo Externo de Software

Para el caso que se considere la tercerización del desarrollo de software, se establecerán normas y procedimientos que contemplen los siguientes puntos:

- a) Acuerdos de licencias, propiedad de código y derechos conferidos.
- b) Requerimientos contractuales con respecto a la calidad del código y la existencia de garantías.
- c) Procedimientos de certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan auditorías, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software establecido, etc.
- d) Verificación del cumplimiento de las condiciones de seguridad contempladas en los requerimientos de Seguridad en Contratos de Tercerización.
- e) Acuerdos de custodia de las fuentes del software (y cualquier otra información requerida) en caso de quiebra de la tercera parte.

14 CIFRADO

14.1 Política de Utilización de Controles Criptográficos

El Organismo establece la presente Política de uso de controles criptográficos, a fin de determinar su correcto uso. Para ello se indica que:

A. Se utilizarán controles criptográficos en los siguientes casos:

1. Para la protección de claves de acceso a sistemas, datos y servicios.
2. Para la transmisión de información clasificada, fuera del ámbito de la empresa.
3. Para el resguardo de información, cuando así surja de la evaluación de riesgos realizada.

B. Se desarrollarán procedimientos respecto de la administración de claves, de la recuperación de información cifrada en caso de pérdida, compromiso o daño de las claves y en cuanto al reemplazo de las claves de cifrado.

C. El Responsable del Área Informática propondrá la siguiente asignación de funciones:

- Implementación de la política de controles criptográficos
- Administración de claves

D. Se utilizarán los siguientes algoritmos de cifrado y tamaños de clave:

- Cifrado simétrico

Algoritmo	Longitud de Clave
AES	128/192/256
3DES	168 bits
IDEA	128 bits
RC4 y RC2	128 bits

- 2. Cifrado Asimétrico

Casos de Utilización	Algoritmo	Longitud de Clave
Para certificados utilizados en servicios relacionados a la firma digital (sellado de tiempo, almacenamiento seguro de documentos electrónicos, etc.)	RSA	2048 bits
	DSA	2048 bits
	ECDSA	210 bits
Para certificados de sitio seguro	RSA	1024 bits
Para certificados de Certificador o de información de estado de certificados	RSA	2048 bits
	DSA	2048 bits
	ECDSA	210 bits
Para certificados de usuario (personas físicas o jurídicas)	RSA	1024 bits
	DSA	1024 bits
Para digesto seguro	ECDSA SHA-1	160 bits 256 bits

14.2 Cifrado

Mediante la evaluación de riesgos que llevará a cabo la alta gerencia y el encargado de IT, se identificará el nivel requerido de protección, tomando en cuenta el tipo y la calidad del algoritmo de cifrado utilizado y la longitud de las claves criptográficas a utilizar. Al implementar la Política del Organismo en materia criptográfica, se considerarán los controles aplicables a la exportación e importación de tecnología criptográfica.

14.3 Firma Digital

Las firmas digitales proporcionan un medio de protección de la autenticidad e integridad de los documentos electrónicos. Pueden aplicarse a cualquier tipo de documento que se procese electrónicamente. Se implementan mediante el uso de una técnica criptográfica sobre la base de dos claves relacionadas de manera única, donde una clave, denominada privada, se utiliza para crear una firma y la otra, denominada pública, para verificarla.

Asimismo, es importante proteger la integridad de la clave pública. Esta protección se provee mediante el uso de un certificado de clave pública.

Se recomienda que las claves criptográficas utilizadas para firmar digitalmente no sean empleadas en procedimientos de cifrado de información. Dichas claves deben ser resguardadas bajo el control exclusivo de su titular.

En algunos casos podría ser necesario establecer acuerdos especiales para respaldar el uso de las firmas digitales. A tal fin se deberá obtener asesoramiento legal con respecto al marco normativo aplicable y la modalidad del acuerdo a implementar.

14.4 Normas Procedimientos y Métodos

Se redactarán las normas y procedimientos necesarios para:

- a) Generar claves para diferentes sistemas criptográficos y diferentes aplicaciones.
- b) Generar y obtener certificados de clave pública de manera segura.
- c) Distribuir claves de forma segura a los usuarios que corresponda, incluyendo información sobre cómo deben activarse cuando se reciban.
- d) Almacenar claves, incluyendo la forma de acceso a las mismas por parte de los usuarios autorizados.
- e) Cambiar o actualizar claves, incluyendo reglas sobre cuándo y cómo deben cambiarse las claves.
- f) Recuperar claves pérdidas o alteradas como parte de la administración de la continuidad de las actividades de la empresa, por ejemplo para la recuperación de la información cifrada.
- g) Archivar claves, por ejemplo, para la información archivada o resguardada.
- h) Destruir claves.

15 ADMINISTRACIÓN DE LA CONTINUIDAD DE LAS ACTIVIDADES DEL ORGANISMO

Generalidades

El desarrollo e implementación de planes de contingencia es una herramienta básica para garantizar que las actividades del Organismo puedan restablecerse dentro de los plazos requeridos.

Dichos planes deben mantenerse actualizados y transformarse en una parte integral del resto de los procesos de administración y gestión, debiendo incluir necesariamente controles destinados a identificar y reducir riesgos, atenuar las consecuencias de eventuales interrupciones de las actividades del organismo y asegurar la reanudación de las operaciones indispensables.

Objetivo

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) Notificación / Activación: Consistente en la detección y determinación del daño y la activación del plan.
- b) Reanudación: Consistente en la restauración temporal de las operaciones y recuperación del daño producido al sistema original.
- c) Recuperación: Consistente en la restauración total de las capacidades de proceso del sistema a las condiciones de operación normales.

Asegurar la coordinación con el personal del Organismo y los contactos externos que participarán en las estrategias de planificación de contingencias.

15.1 Proceso de la Administración de la Continuidad del Organismo

El Comité de Seguridad de la Información, será el responsable de la coordinación del desarrollo de los procesos que garanticen la continuidad de las actividades del Organismo.

Este Comité tendrá a cargo la coordinación del proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de información del Organismo frente a interrupciones imprevistas, lo cual incluye las siguientes funciones:

- a) Identificar y priorizar los procesos críticos de las actividades del Organismo.
- b) Asegurar que todos los integrantes del Organismo comprendan los riesgos que la misma enfrenta, en términos de probabilidad de ocurrencia e impacto de posibles amenazas, así como los efectos que una interrupción puede tener en la actividad del Organismo.
- c) Elaborar y documentar una estrategia de continuidad de las actividades del Organismo consecuente con los objetivos y prioridades acordados.
- d) Proponer planes de continuidad de las actividades del Organismo de conformidad con la estrategia de continuidad acordada.
- e) Establecer un cronograma de pruebas periódicas de cada uno de los planes de contingencia, proponiendo una asignación de funciones para su cumplimiento.
- f) Coordinar actualizaciones periódicas de los planes y procesos implementados.
- g) Considerar la contratación de seguros que podrían formar parte del proceso de continuidad de las actividades del Organismo.
- h) Proponer las modificaciones a los planes de contingencia.

15.2 Continuidad de las Actividades y Análisis de los Impactos

Con el fin de establecer un Plan de Continuidad de las Actividades del Organismo se deben contemplar los siguientes puntos:

- Identificar los eventos (amenazas) que puedan ocasionar interrupciones en los procesos de las actividades.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones, tanto en términos de magnitud de daño como del período de recuperación. Dicha evaluación debe identificar los recursos críticos, los impactos producidos por una interrupción, los tiempos de interrupción aceptables o permitidos, y debe especificar las prioridades de recuperación.
- Identificar los controles preventivos, como por ejemplo sistemas de supresión de fuego, detectores de humo y fuego, contenedores resistentes al calor y a prueba de agua para los medios de backup, los registros no electrónicos vitales, etc.

Según los resultados de la evaluación de esta actividad, se desarrollará un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades del Organismo. Una vez que se ha creado este plan, el mismo debe ser propuesto por el Comité de Seguridad de la Información a la máxima autoridad del Organismo para su aprobación.

15.3 Marco para la Planificación de la Continuidad de las Actividades del Organismo

Se mantendrá un solo marco para los planes de continuidad de las actividades del Organismo, a fin de garantizar que los mismos sean uniformes e identificar prioridades de prueba y mantenimiento.

Cada plan de continuidad especificará claramente las condiciones para su puesta en marcha, así como las personas a cargo de ejecutar cada componente del mismo. Cuando se identifiquen nuevos requerimientos, se modificarán los procedimientos de emergencia establecidos, por ejemplo, los planes de evacuación o los recursos de

emergencia existentes.

El administrador de cada plan de continuidad será el encargado de coordinar las tareas definidas en el mismo. Estas modificaciones deberán ser propuestas por el Comité de Seguridad de la Información para su aprobación.

El marco para la planificación de la continuidad de las actividades del Organismo, tendrá en cuenta los siguientes puntos:

- a) Prever las condiciones de implementación de los planes que describan el proceso a seguir antes de poner en marcha los mismos.
- b) Definir los procedimientos de emergencia que describan las acciones a emprender una vez ocurrido un incidente. Esto debe incluir disposiciones con respecto a la gestión de las relaciones públicas y a vínculos eficaces a establecer con las autoridades públicas pertinentes, por ejemplo, la policía, bomberos y autoridades locales.
- c) Realizar los procedimientos de emergencia que describan las acciones a emprender para el traslado de actividades esenciales del Organismo o de servicios de soporte a ubicaciones transitorias alternativas, y para el restablecimiento de los procesos en los plazos requeridos.
- d) Redactar los procedimientos de recuperación que describan las acciones a emprender para restablecer las operaciones normales del Organismo.
- e) Definir un cronograma de mantenimiento que especifique cómo y cuándo será aprobado el plan, y el proceso para el mantenimiento del mismo.
- f) Efectuar actividades de concientización e instrucción al personal, diseñadas para propiciar la comprensión de los procesos de continuidad las actividades y garantizar que los procesos sigan siendo eficaces.
- g) Documentar las responsabilidades y funciones de las personas, describiendo los responsables de la ejecución de cada uno de los componentes del plan y las vías de contacto posible. Se deben mencionar alternativas cuando corresponda.

Descripción	Responsables / afectados	Plan de Contingencia
Fuga de Información	El responsable sería el encargado de sistemas ya que el acceso al sistema es vulnerable y el afectado sería la empresa	1.-Avisar al encargado directo y a los afectados del suceso. 2.-Revisar las bitácoras de acceso, posibles vulnerabilidades o puertas traseras por donde pudo haber salido la información. 3.-Mandar a llamar a las personas que tenían directo acceso a esta información. 4.-Iniciar proceso de restauración y sanción.
Seguimiento inadecuado a las órdenes de compra y venta.	El encargado del área de ventas ya que se puede perder ventas por el mal funcionamiento	1.-Avisar al encargado del área y a los afectados del mal funcionamiento. 2.-Revisar cuantas órdenes fueron afectadas y aislarlas para su posterior revisión. 3.-Aplicar las sanciones necesarias. 4.-Iniciar proceso de restauración.
Captura incorrecta de la información acerca de equipo y maquinaria.	El área de producción sería el afectado por lo mismo de que llegan tarde las máquinas, piezas u otras cosas se atrasan las órdenes	1.-Avisar al encargado del área y a los afectados del mal funcionamiento. 2.-Entrar a las Bases de Datos y corregir la información.

Cambios en el Sistema no informados.	El responsable es el encargado de sistemas ya que debe de informar de los cambios y explicar si es que existe algún procedimiento diferente	1.-Avisar al encargado del área y a los afectados de la mala comunicación de cambios. 2.-Actualizar sistema y su información.
Backups rutinarios no hechos periódicamente	El responsable es el del área de sistemas y el afectado principal sería el área de producción	1.-Avisar al encargado del área y a los afectados. 2.-Aplicar sanciones de ser necesario. 3.-Realizar el backup de la información.
Presencia de Software Malicioso	El encargado del área de sistemas	1.-Avisar al encargado del área y a los afectados. 2.-Interrumpir el trabajo de los sistemas que podrían ser infectados 3.-Iniciar Proceso de desinfección.
Ciberataques	El de sistemas debe cuidar que el sitio esté arriba siempre y exista un respaldo de la información	1.-Avisar al encargado del área y a los afectados. 2.-Iniciar proceso de protección
Barreras físicas ineficientes	El encargado de seguridad	1.-Avisar al encargado del área y a los afectados. 2.-Hacer análisis de mejoras. 3.-Iniciar proceso de mejoramiento.

Servicio Caído	El área de sistemas le debe dar el mantenimiento adecuado	1.-Avisar al encargado del área y a los afectados. 2.-Suspender labores de las áreas afectadas. 3.-Reiniciar el servicio.
----------------	---	---

Para generar un plan de continuidad del negocio es necesario enlistar las amenazas y riesgos que enfrenta la empresa, en este caso hablando más específicamente de amenazas y riesgos que supone la información, es por eso que se realiza el análisis de riesgos para identificar el impacto que estos tiene y las pérdidas que supondrán. Los pasos a seguir para realizar este análisis son:

-Enlistar los activos de la empresa y calcular su valor tomando en cuenta: El valor de adquisición del activo, el costo de mantenimiento y el valor de la empresa en el mercado.

-Enlistar las amenazas y riesgos a los que se enfrenta cada activo. Se debe de anotar el responsable, el porcentaje de ocurrencia y una descripción de esta.

-Se evalúan los riesgos realizando los siguientes cálculos:

- a) Identificar vulnerabilidades y el factor de exposición (FE) por activo.
- b) Determinar la tasa de ocurrencia anual (TOA) de cada vulnerabilidad por activo.
- c) Determinar la expectativa de pérdida simple (EPS) multiplicando VA por FE (por amenaza por activo).
- d) Determinar la expectativa de pérdida anual (EPA) multiplicando la TOA por la EPS (por amenaza por activo).
- e) Priorizar activos por EPA.

-Se realizan escenarios donde se pretende mostrar el costo que supondría en cuanto a pérdidas para la empresa y el costo que tendría recuperar el equilibrio que se mantenía, también se hacen cálculos de tiempo que tardaría realizar el proceso de recuperación. Se deben de establecer procedimientos de recuperación para cada posible escenario.

-Finalmente en base a esto salen las acciones preventivas como podría ser el monitoreo continuo del funcionamiento del organismo.

13.3 Ensayo, Mantenimiento y Reevaluación de los Planes de Continuidad del Organismo

Debido a que los planes de continuidad de las actividades del Organismo pueden fallar, por suposiciones incorrectas, errores o cambios en el equipamiento, se establecen las siguientes pautas de acción:

- El Comité de Seguridad de la Información establecerá un cronograma de pruebas periódicas de cada uno de los planes de contingencia.
- El cronograma indicará quienes son los responsables de llevar a cabo cada una de las pruebas y de elevar el resultado obtenido al Comité.

Se deberán utilizar diversas técnicas para garantizar que los planes de contingencia funcionarán ante un hecho real, y éstas incluirán por lo menos:

- a) Efectuar pruebas de discusión de diversos escenarios.
- b) Realizar simulaciones.
- c) Efectuar pruebas de recuperación técnica.
- d) Realizar ensayos completos probando que el Organismo, el personal, el equipamiento, las instalaciones y los procesos pueden afrontar las interrupciones.

Para las operaciones críticas del Organismo se tomarán en cuenta, además, los siguientes mecanismos:

- a) Efectuar pruebas de recuperación en un sitio alternativo.
- b) Realizar pruebas de instalaciones y servicios de proveedores.

Los planes de continuidad de las actividades del Organismo serán revisados y actualizados periódicamente, para garantizar su eficacia permanente. Se incluirán procedimientos en el programa de administración de cambios del Organismo para garantizar que se aborden adecuadamente los tópicos de continuidad de las actividades.

La periodicidad de revisión de los planes de contingencia es la siguiente:

Rutinas	PERIODICIDAD
Backups	semanal
Revisión estado de los Servicios	semanal
Revisión equipo de monitoreo	mensual
Reporte de fallas en el Sistema	diario
Revisión de mantenimiento de equipo de cómputo	mensual
Reporte de activos enlistados	diario
Reporte de ataques al sistema	diario
Revisión de roles y desempeños	mensual
Limpieza y Actualización de Software	bimestral
Cambio de contraseñas	trimestral
Revisión Barreras físicas	semestral

Deberá prestarse atención, especialmente, a los cambios de:

- a) Personal.
 - b) Direcciones o números telefónicos.
 - c) Estrategia del Organismo.
 - d) Ubicación, instalaciones y recursos.
 - e) Legislación.
 - f) Contratistas, proveedores y clientes críticos.
 - g) Procesos, o procesos nuevos / eliminados.
 - h) Tecnologías.
 - i) Requisitos operacionales.
 - j) Requisitos de seguridad.
 - k) Hardware, software y otros equipos (tipos, especificaciones, y cantidad).
 - l) Requerimientos de los sitios alternativos.
 - m) Registros de datos vitales.
- Todas las modificaciones efectuadas serán propuestas por el Comité de Seguridad de la Información para su aprobación por el superior jerárquico que corresponda.

16 CUMPLIMIENTO

Generalidades

El diseño, operación, uso y administración de los sistemas de información están regulados por disposiciones legales y contractuales.

Los requisitos normativos y contractuales pertinentes a cada sistema de información deben estar debidamente definidos y documentados.

El Área Legal de la empresa, será responsable de encuadrar jurídicamente la formulación e implementación de la política.

Objetivos

Cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas a la empresa y/o al empleado o que incurran en responsabilidad civil o penal como resultado de su incumplimiento.

Optimizar la eficacia del proceso de auditoría de sistemas y minimizar los problemas que pudiera ocasionar el mismo, o los obstáculos que pudieran afectarlo.

Garantizar la existencia de controles que protejan los sistemas en producción y las herramientas de auditoría en el transcurso de las auditorías de sistemas.

Determinar los plazos para el mantenimiento de información y para la recolección de evidencia de la empresa.

Alcance

Esta Política se aplica a todo el personal de la empresa, cualquiera sea su situación de revista.

Asimismo, se aplica a los sistemas de información, normas, procedimientos, documentación y plataformas técnicas de la empresa y a las auditorías efectuadas sobre los mismos.

Responsabilidad

El Responsable de Seguridad Informática cumplirá las siguientes funciones:

- a) Definir normas y procedimientos para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual y a la conservación de registros.
- b) Realizar revisiones periódicas de todas las áreas de la empresa a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad.

- c) Verificar periódicamente que los sistemas de información cumplan la política, normas y procedimientos de seguridad establecidos.
- d) Garantizar la seguridad y el control de las herramientas utilizadas para las revisiones de auditoría.

Todos los empleados de los mandos medios y superiores conocerán, comprenderán, darán a conocer, cumplirán y harán cumplir la presente Política y la normativa vigente.

16.1 Cumplimiento de Requisitos Legales

16.1.1 Identificación de la Legislación Aplicable

Se definirán y documentarán claramente todos los requisitos normativos y contractuales pertinentes para cada sistema de información. Del mismo modo se definirán y documentarán los controles específicos y las responsabilidades y funciones individuales para cumplir con dichos requisitos.

16.1.2 Derechos de Propiedad Intelectual

Se implementarán procedimientos adecuados para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual.

Los empleados únicamente podrán utilizar material autorizado por la empresa.

La empresa solo podrá autorizar el uso de material producido por el mismo, o material autorizado o suministrado al mismo por su titular, conforme los términos y condiciones acordados y lo dispuesto por la normativa vigente.

La infracción a estos derechos puede tener como resultado acciones legales que podrían derivar en demandas penales.

16.1.2.1 Derecho de Propiedad Intelectual del Software

El software es considerado una obra intelectual que goza de la protección de la Ley 11.723 de Propiedad Intelectual. Esta Ley establece que la explotación de la propiedad intelectual sobre los programas de computación incluirá, entre otras formas, los contratos de licencia para su uso o reproducción. Los productos de software se suministran normalmente bajo acuerdos de licencia que suelen limitar el uso de los productos al equipamiento específico y su copia a la creación de copias de resguardo solamente.

El responsable de IT, con la asistencia del abogado, analizará los términos y condiciones de la licencia, e implementará los siguientes controles:

- Definir normas y procedimientos para el cumplimiento del derecho de propiedad intelectual de software que defina el uso legal de productos de información y de software.
- Divulgar las políticas de adquisición de software y las disposiciones de la Ley de Propiedad Intelectual, y notificar la determinación de tomar acciones disciplinarias contra el personal que las infrinja.
- Mantener un adecuado registro de activos.
- Conservar pruebas y evidencias de propiedad de licencias, discos maestros, manuales, etc.
- Implementar controles para evitar el exceso del número máximo permitido de usuarios.
- Verificar que sólo se instalen productos con licencia y software autorizado.
- Elaborar y divulgar un procedimiento para el mantenimiento de condiciones adecuadas con respecto a las licencias.
- Elaborar y divulgar un procedimiento relativo a la eliminación o transferencia de software a terceros.
- Utilizar herramientas de auditoría adecuadas.
- Cumplir con los términos y condiciones establecidos para obtener software e información en redes públicas.

16.1.3 Protección de los Registros del Organismo

Los registros críticos del Organismo se protegerán contra pérdida, destrucción y falsificación. Algunos registros pueden requerir una retención segura para cumplir requisitos legales o normativos, así como para respaldar actividades esenciales del Organismo.

Los registros se clasifican en diferentes tipos, por ejemplo registros contables, registros de base de datos, registros de auditoría y procedimientos operativos, cada uno de ellos detallando los períodos de retención y el tipo de medios de almacenamiento, por ejemplo papel, microfichas, medios magnéticos u ópticos.

16.1.4 Protección de Datos y 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. La empresa redactará un “Compromiso de Confidencialidad”, el cual deberá ser suscrito por todos los empleados. La copia firmada del compromiso será retenida en forma segura por la empresa.

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. 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.

16.2 Revisiones de la Política de Seguridad y la Compatibilidad Técnica

16.2.1 Cumplimiento de la Política de Seguridad

Cada responsable área, revisará la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos, dentro de su área de responsabilidad. El responsable de IT, realizará revisiones periódicas de todas las áreas de la empresa a efecto de garantizar el cumplimiento de la política, normas y procedimientos de seguridad. Entre las áreas a revisar se incluyen las siguientes:

- Sistemas de información.
- Proveedores de sistemas.
- Propietarios de información.
- Usuarios.

16.3 Consideraciones de Auditorías de Sistemas

16.3.1 Controles de Auditoría de Sistemas

Cuando se realicen actividades de auditoría que involucren verificaciones de los sistemas en producción, se tomarán acciones en la planificación de los requerimientos y tareas, y se acordará con las áreas involucradas a efectos de minimizar el riesgo de interrupciones en las operaciones.

Se contemplarán los siguientes puntos:

- a) Acordar con el Área que corresponda los requerimientos de auditoría.
- b) Controlar el alcance de las verificaciones. Esta función será realizada por el responsable de auditoría.
- c) Limitar las verificaciones a un acceso de sólo lectura del software y datos de producción. Caso contrario, se tomarán los resguardos necesarios a efectos de aislar y contrarrestar los efectos de las modificaciones realizadas, una vez finalizada la auditoría. Por ejemplo:

- Eliminar archivos transitorios.
- Eliminar entidades ficticias y datos incorporados en archivos maestros.
- Revertir transacciones.
- Revocar privilegios otorgados

RECURSOS DE IT A SER UTILIZADOS EN LA AUDITORÍA

Sistema de Información

Base de Datos

Hardware

Software de Auditoría

Conexiones de Red

Personal de Oficina

Personal de Seguridad

Equipo de Monitoreo

d) Identificar claramente los recursos de tecnologías de información (TI) para llevar a cabo las verificaciones, los cuales serán puestos a disposición de los auditores. A tal efecto, quien sea propuesto por el Comité de Seguridad de la Información completará el siguiente cuestionario, el cual deberá ser puesto en conocimiento de las áreas involucradas.

e) Identificar y acordar los requerimientos de procesamiento especial o adicional.

f) Monitorear y registrar todos los accesos, a fin de generar una pista de referencia. Los datos a resguardar deben incluir como mínimo:

- Fecha y hora.
- Puesto de trabajo.
- Usuario.
- Tipo de acceso.
- Identificación de los datos accedidos.
- Estado previo y posterior.
- Programa y/o función utilizada.

g) Documentar todos los procedimientos de auditoría, requerimientos y responsabilidades.

16.4 Sanciones Previstas por Incumplimiento

Se sancionará administrativamente a todo aquel que viole lo dispuesto en la presente Política de Seguridad conforme a lo dispuesto por las normas que rigen al personal de la Administración Pública Nacional, y en caso de corresponder, se realizarán las acciones correspondientes ante el o los Organismos pertinentes.

Las sanciones sólo pueden imponerse mediante un acto administrativo que así lo disponga
cumpliendo las formalidades impuestas por los preceptos constitucionales, la Ley de Procedimiento Administrativo y demás normativas específicas aplicables.

El agente que no da debido cumplimiento a sus obligaciones puede incurrir también en responsabilidad civil o patrimonial cuando ocasiona un daño que debe ser indemnizado y/o en responsabilidad penal cuando su conducta constituye un comportamiento considerado delito por el Código Penal y leyes especiales.

A grandes rasgos, existen seis tipos de sanciones que el empresario puede aplicar, siempre atendiendo a lo que pudiera decir el convenio aplicable en cada caso, por lo que obtenemos el siguiente listado:

1. **Amonestación:** Con la amonestación se pone en conocimiento al trabajador de cuál es la conducta indeseable que hay que corregir, pudiendo avisar de las posibles consecuencias que se producirían en caso de persistir en ella. Se puede hacer tanto de forma verbal como por escrito.
2. **Suspensión de empleo y sueldo:** Esta sanción viene recogida en el artículo 45.1 letra h del ET, cuando está justificada por motivos disciplinarios. No obstante, no podrá aplicarse si el convenio aplicable no lo contempla como una sanción adecuada para la falta concreta que se haya cometido. La suspensión no finaliza el contrato laboral, sino que congela las obligaciones de trabajar y de remunerar dicho trabajo durante un periodo de tiempo determinado.
3. **Descuento proporcional del sueldo:** Solo se podrá aplicar un descuento al salario del trabajador cuando se pueda cuantificar una dejación de funciones, de forma que no pueda entenderse como una multa de haber. Es decir, no se puede dejar de pagar lo trabajado, sino que se debe demostrar que lo que no se ha pagado es porque no se ha trabajado.
4. **Traslado forzoso:** Aunque esta sanción no aparece recogida en la legislación de forma explícita, sí está presente en los convenios colectivos con cierta normalidad, sin que el empleado tenga derecho a indemnización. Se puede entender como traslado el cambio de puesto y funciones, además de un posible cambio de residencia.
5. **Limitación en las promociones:** Muchos convenios contemplan este supuesto en el caso de faltas graves o muy graves. Consiste en prohibir que el trabajador se presente a pruebas selectivas de ascenso profesional dentro de

la organización, durante un tiempo limitado. También se puede aplicar limitando las opciones de ascenso de forma temporal (por ejemplo, no teniendo en cuenta la antigüedad para este fin)

6. Despido disciplinario: Se trata de la sanción más grave y, por tanto, está reservada para las faltas más graves y culpables. Con ella se termina la relación laboral sin que el empleado tenga derecho a indemnización.