2017

Política de Seguridad de la Información

La información es un activo que como otros activos importantes del Organismo, es esencial para las actividades y, en consecuencia, necesita de una protección adecuada.

ENARGAS

ENTE NACIONAL REGULADOR DEL GAS

Versión 1.0

Índice

1. INTRODUCCION

En septiembre de 2003, la Oficina Nacional de Tecnologías de Información (ONTI) convocó a especialistas en seguridad informática de diversos Organismos públicos, con el fin de conocer sus opiniones respecto a una estrategia de seguridad de la información para el Sector Público Nacional. Como corolario de las reuniones mantenidas, se concluyó en la necesidad de que los Organismos Públicos cuenten con Políticas de Seguridad de la Información escritas, derivando en la emisión, por parte de la Jefatura de Gabinete de Ministros, de la Decisión Administrativa 669/2004. La misma estableció la obligatoriedad para los organismos del Sector Público Nacional (comprendidos en los incisos a y c del artículo 8° de la Ley N° 24.156 y sus modificatorias) de:

- Conformar un Comité de Seguridad de la Información.
- Designar un coordinador del Comité de Seguridad de la Información.

1.1. ¿Qué es la Seguridad de la Información?

La información es un activo que, como otros activos importantes del Organismo, es esencial para las actividades y, en consecuencia, necesita una protección adecuada. Como resultado de la creciente interconexión de los sistemas de procesamiento de datos, la información se expone a un gran número y a una variedad de amenazas y vulnerabilidades.

La información puede existir en diversas formas. Se puede imprimir o escribir en papel, almacenar electrónicamente, transmitir por correo o por medios electrónicos, presentar en películas, o expresarse en la conversación. Cualquiera sea su forma o medio por el cual se comparte o almacena, siempre deberá tener una protección adecuada.

La seguridad de la información, para el caso del Organismo, es la protección de la información de los riesgos de uso indebido, garantizando la confidencialidad, la integridad y la disponibilidad de la misma.

La seguridad de la información se logra implementando un conjunto apropiado de controles, incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Los controles necesitan ser establecidos, implementados, monitoreados, revisados y mejorados, donde sea necesario, para asegurar que se cumplan los objetivos específicos del Organismo. Esto debe implementarse en conjunto con los demás procesos de la gestión regulatoria.

1.2. ¿Por qué es necesaria la Seguridad de la Información?

La definición, el logro, el mantenimiento y la mejora de la seguridad de la información pueden ser esenciales para que el Organismo cumpla con las funciones y facultades que le ha asignado el Art. 52 de la Ley Nº 24.076 y para mantener una adecuada imagen institucional.

Las organizaciones, sus sistemas y redes de información enfrentan amenazas de seguridad procedentes de una gran variedad de fuentes, incluyendo fraudes asistidos por computadora, espionaje, sabotaje, vandalismo, incendios o inundaciones. Las causas de daño, tales como códigos maliciosos y ataques de piratería por computadora, y negación del servicio se han vuelto más comunes, más ambiciosos y cada vez más sofisticados.

La seguridad de la información es importante para las gestiones de regulación, control y resolución de controversias del Organismo y para proteger la infraestructura crítica. La interconexión de las redes públicas y privadas y el compartir los recursos de información incrementan la dificultad para lograr el control del acceso. La tendencia a la computación distribuida también ha debilitado la efectividad de un control central y especializado.

Muchos sistemas de información no han sido diseñados para ser seguros. La seguridad que se puede lograr a través de medios técnicos es limitada, y debiera ser apoyada por la gestión y los procedimientos adecuados. La identificación de los controles requiere planificación y atención cuidadosa a los detalles. La gestión de la seguridad de la información requiere, como mínimo, la participación de todos los empleados del Organismo. También se puede requerir asesoría especializada de organizaciones externas.

1.3. Alcance

La presente Política de Seguridad de la Información se dicta en cumplimiento de la normativa vigente, 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 la Máxima Autoridad del Organismo y por todos quienes integran su planta de personal, sea cual fuere su nivel jerárquico y su situación de revista.

1.4. Alineación con estándares internacionales

Todas las definiciones de la presente Política de Seguridad de la Información están alineadas con los estándares internacionalmente aceptados para la práctica de seguridad de la información, particularmente respecto de:

NORMA IRAM/ISO/IEC 27002:2013 Código de Buenas Prácticas para la Seguridad de la Información.

1.5. Alineación con regulaciones argentinas en relación con la materia

Todas las definiciones de la presente Política de Seguridad de la Información están alineadas con los requerimientos particulares de:

Ley N° 25.326 sobre PROTECCIÓN DE LOS DATOS PERSONALES Y REGLAMENTACIÓN DEL ARTÍCULO N° 43 DE LA CONSTITUCIÓN NACIONAL (conocida como Ley de Habeas Data).

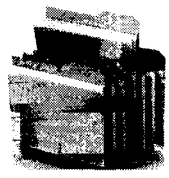
Ley N° 11.723 sobre Propiedad Intelectual (y reglamentaciones relacionadas).

Decreto N° 1172/2003 de Acceso a la Información Pública y la Ley N° 27.275 sobre el Derecho de Acceso a la Información Pública.

2. ESTRUCTURA DE LA POLITICA

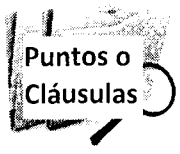
Esta política se divide en dos partes, y guarda la siguiente estructura:

- Cuatro capítulos introductorios, con los términos generales y el establecimiento de la Evaluación y el Tratamiento de los riesgos.
- Catorce puntos o cláusulas que abarcan los diferentes aspectos o dominios de la seguridad de la información. Se presentan de manera sistemática y consistente.



Política de Seguridad de la Información

1. Introducción
2. Estructura de la Política
3. Términos y Definiciones
4. Evaluación y Tratamiento de Riesgos



Puntos o Cláusulas

5. Política de Seguridad
6. Organización
7. Seguridad de los Recursos Humanos
8. Gestión de Activos
9. Control de Accesos
10. Cifrado
11. Seguridad Física y Ambiental
12. Seguridad en las Operaciones
13. Seguridad en las Telecomunicaciones
14. Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información
15. Relaciones con Proveedores
16. Gestión de Incidentes en la Seguridad de la Información
17. Gestión de la Continuidad
18. Cumplimiento

Políticas x Punto
Objetivo = resultado deseado
Controles = para mitigar

Cada punto contiene un número de categorías o grupo de controles de seguridad principales. A continuación, se enumeran los catorce puntos junto con el número de categorías que contiene:

- Política de Seguridad (1 categoría).
- Organización (2 categorías).
- Seguridad de los Recursos Humanos (3 categorías).

- Gestión de Activos (3 categorías).
- Control de Accesos (4 categorías).
- Cifrado (1 categorías).
- Seguridad Física y Ambiental (2 categorías).
- Seguridad en las Operaciones (7 categorías).
- Seguridad en las Telecomunicaciones (2 categorías).
- Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información (3 categorías).
- Relaciones con Proveedores (2 categorías).
- Gestión de Incidentes en la Seguridad de la Información (1 categoría).
- Gestión de la Continuidad (2 categorías).
- Cumplimiento (3 categorías).

Por último, por cada categoría, se establece un objetivo y contiene uno o más controles a realizar.

A modo de síntesis se enuncia a continuación la estructura de cada punto o cláusula:

- Punto o cláusula o dominio
  1. Generalidades
  2. Objetivos
  3. Alcance
  4. Responsabilidades
  5. Política
     - Categorías
- Objetivo
  - Controles

3. TERMINOS Y DEFINICIONES

A los efectos de este documento y de las reglamentaciones que sobre la materia se dictaren, se aplican las siguientes definiciones:

ACTIVO:

Es el conjunto de bienes tangibles o intangibles de información que posee el Organismo. Se clasifican como:

- **Activos de información:** Corresponde a elementos tales como información en sistemas informáticos o en papel, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, documentación archivada o en circulación, resultados de proyectos de investigación, entre otros.

- **Activos de software:** Son elementos tales como: Aplicaciones de software, herramientas de desarrollo y utilitarios adicionales.

- **Activos físicos:** Se consideran activos físicos a los elementos tales como: equipos informáticos, impresoras, máquinas de fax, equipos de comunicaciones, Centrales Telefónicas (PBX), cintas, discos, Unidad no interrumpibles de energía (UPS), teléfonos de línea o celulares, dispositivos de almacenamiento extraíbles, archivos de documentación, entre otros.

ADMINISTRACIÓN DE RIESGOS:

Se entiende por administración de riesgos al proceso de identificación, control y minimización a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

AMENAZA:

Causa potencial de un incidente no deseado que puede ocasionar daño a un sistema u organización.

AUTORIDAD:

Facultad o capacidad de una posición superior para dar órdenes, establecer metas o premisas y que estas sean cumplidas.

CIFRADO:

El cifrado o también llamado "encriptado" es el proceso para volver ilegible información considerada importante. La información, una vez encriptada, solo puede leerse aplicándole una clave.

Para encriptar información se utilizan complejas fórmulas matemáticas y para desencriptar, se debe usar una clave como parámetro para esas fórmulas.

COMITÉ DE SEGURIDAD DE LA INFORMACIÓN:

El Comité de Seguridad de la Información es un cuerpo integrado por un representante de cada una de las Unidades Organizativas que conforman al Organismo. Cada representante debe tener un amplio conocimiento del funcionamiento de la unidad que representa y es el responsable de promover la difusión y apoyo, a la seguridad de la información dentro del Organismo.

CONTRASEÑA FUERTE:

Característica que posee una clave, que la hace más difícil de descifrar tanto por humanos como por computadoras. Para esto debe cumplir ciertas propiedades, como por ejemplo, que sea lo suficientemente larga, que no sea evidente, que combine letras, números y, si es posible, símbolos.

CONTROL:

Medio para gestionar el riesgo, con el fin de minimizar la ocurrencia de eventos peligrosos que comprometan la seguridad de la información. Este incluye políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

DESASTRE:

Es un evento natural o provocado por una vulnerabilidad que afecta a la operatividad de la Organización, dejándolo en situación de emergencia.

EQUIPO O TERMINAL DESATENDIDA:

Se refiere a un equipo sin operador delante del mismo.

EVALUACIÓN DE RIESGOS:

Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria del Organismo.

EVENTO DE SEGURIDAD DE LA INFORMACIÓN:

Un evento de seguridad de la información es la presencia identificada de un estado del sistema, del servicio o de la red que indica un posible incumplimiento de la política de seguridad de la información, una falla de controles, o una situación previamente desconocida que puede afectar la seguridad.

FIRMA DIGITAL:

Una firma digital es un conjunto de datos asociados a un mensaje que permite asegurar la identidad del firmante y la integridad del mensaje. Se basa en el concepto de no repudio. La firma digital no implica que el mensaje esté encriptado, es decir, que este no pueda ser leído por otras personas.

HOSTING:

Es un servicio en el que se proporciona espacio de un equipo a los clientes para poder almacenar páginas web, sitio web, sistema, correo electrónico, archivos, o cualquier contenido accesible vía web.

HOUSING:

Es básicamente una modalidad de vender o alquilar un espacio físico de un centro de datos para que el cliente coloque ahí su propio equipo. La empresa suministra la corriente y la conexión a internet, pero el equipo es administrado completamente por el cliente.

INCIDENTE DE SEGURIDAD:

Un incidente de seguridad es un evento adverso a las condiciones de confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento, o amenaza de romper los mecanismos de seguridad existentes.

MALWARE:

Se refiere a todo software malicioso que se ejecute en una computadora a fin de:

- Robar información de los usuarios.
- Engañar a los usuarios.
- Dañar al equipo residente.
- Consumir Recursos.
- Instalar y actualizar Malware.

Tipos de Malware:

- **Adware:** ADvertisement Software es la publicidad no solicitada; por lo general, se presenta en forma de pop-ups que presentan algún tipo de publicidad. Su finalidad no es infectar nuestra máquina, sin embargo, hay creadores de virus que la utilizan para que en el momento en que hagamos clic nos descargue malware.

- **Backdoors:** Es un software diseñado para permitir el acceso al sistema de manera no convencional, ignorando los procesos de autenticación.

- **Gusanos:** La finalidad de estos es agotar los recursos del sistema residente, es decir, se reproducen en nuestra máquina, en la LAN o hasta donde puedan llegar, y pueden agotar los recursos del sistema residente.

- **Hoax:** Son mensajes en cadena que se distribuyen con la finalidad de obtener correos y engañar a las personas.

- **Keyloggers:** Es un software que recoge todas las pulsaciones del teclado, las guarda y, cada cierto tiempo, manda este reporte al creador.

- **Ransomware:** es un tipo de programa malintencionado que restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción.

- **Rogge:** Simulan ser herramientas de seguridad como antivirus y, en realidad, lo que nos instalan son spyware, keyloggers, troyanos o gusanos.

- **RootKits:** Son aplicaciones que ocultan procesos y limitan o deniegan el acceso a recursos del sistema. Hay Spywares que utilizan los rootkits para ocultarse.

- **Spyware:** Spy Software, o en español Software Espía, recorre nuestro equipo en busca de claves, contraseñas, información valiosa; muchos de estos son capaces de actualizarse como si se tratara de un software normal y pueden enviar la información recabada al creador de dicho spyware.

- **Troyanos:** Estos son programas o herramientas que parecen inofensivos, que nos dan alguna funcionalidad, pero detrás de ellos existe software malicioso.

- **Virus informático:** Es un software que tiene como objetivo alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario.

MEDIO DE SOPORTE:

Material donde se almacenan los datos: papel, fichas perforadas, medios ópticos, discos blandos y duros, y cinta de video, entre otros.

PLAN DE CONTINGENCIA:

Son procedimientos que presentan una estructura estratégica y operativa para ayudar a controlar una situación de emergencia y minimizar las consecuencias negativas.

PROPIETARIOS DE LA INFORMACIÓN:

Son los Responsables de las Unidades Organizativas que tienen a su cargo la clasificación de la información, de acuerdo con su grado de criticidad, como también la responsabilidad de documentar y mantener actualizada la clasificación efectuada, y definir qué usuarios deberán tener permisos de acceso a la información, según su función y competencia. Cada unidad organizativa será responsable de manejar la información que le corresponda según sus misiones y funciones definidas en la estructura del Organismo.

RESPONSABLE DE PROCESOS:

Son los Responsables de los procesos que tienen definidos cada una de las Unidades Organizativas. Estos procesos corresponden a las actividades que realiza cada Unidad Organizativa según sus misiones y funciones definidas en la estructura del Organismo.

RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN:

Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar, en materia de seguridad de la información, a los integrantes del Organismo que lo requieran. Depende del Departamento de Tecnología de la Información.

RIESGO:

Se conoce por riesgo a la combinación de la probabilidad de ocurrencia e impacto de una amenaza.

SEGURIDAD DE LA INFORMACIÓN:

La seguridad de la información se entiende como la preservación de las siguientes características:

- **Confidencialidad**: se garantiza que la información sea accesible solo a aquellas personas autorizadas.

- **Integridad**: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

- **Disponibilidad**: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con ella, toda vez que lo requieran.

Adicionalmente, deberán considerarse los conceptos de:

- **Autenticidad**: busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantar su identidad.

- **Auditabilidad**: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

- **Protección a la duplicación**: consiste en asegurar que una transacción solo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

- **No repudio**: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

- **Legalidad**: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.

- **Confiabilidad de la Información**: significa que la información generada es la adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

A los efectos de una correcta interpretación de la presente Política, se realizan las siguientes definiciones:

- **Información**: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

- **Tecnología de la Información**: Se refiere al hardware y software operados por el Organismo o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

SERVICIO DE PROCESAMIENTO DE INFORMACIÓN:

Cualquier servicio, infraestructura o sistema de procesamiento de información o los sitios físicos que los albergan.

SISTEMAS DE INFORMACIÓN:

Conjunto de componentes relacionados que recolectan (o recuperan), procesan, almacenan y distribuyen información para apoyar la toma de decisiones, cumplimiento de objetivos y el control en la organización.

SLA (Service Level Agreement):

Un Service Level Agreement o Acuerdo de Nivel de Servicio es un acuerdo negociado entre dos partes, en la que una de ellas es el cliente y la otra, un proveedor de servicios, en donde se define un punto de entendimiento común sobre servicios a brindar, niveles de disponibilidad, prioridades, responsabilidades, garantías u otros atributos. Estos acuerdos pueden estar vinculados legalmente o ser un contrato informal (relaciones interdepartamentales).

SPAM:

Es un correo electrónico no deseado que llega a nuestro buzón.

TERCERA PARTE:

Persona u organismo reconocido por ser independiente de las partes involucradas, con relación al asunto en cuestión.

UNIDADES ORGANIZATIVAS:

Se define como unidades organizativas a aquellas estructuras de la organización de este Organismo que dependen del Directorio.

VULNERABILIDAD:

Debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas.

4. EVALUACION Y TRATAMIENTO DE RIESGOS

Generalidades

El Organismo se encuentra expuesto a riesgos en materia de seguridad de la información. No existe la seguridad completa, por lo que es necesario conocer cuál es el mapa de riesgos y tomar acciones tendientes a minimizar los posibles efectos negativos de la materialización de dichos riesgos.

Es por ello que resulta imprescindible gestionar los riesgos a los que se encuentra expuesto del Organismo, como pilar fundamental para la gestión de seguridad.

Objetivo

Conocer los riesgos a los que se expone el Organismo en materia de seguridad de la información.

Generar información de utilidad para la toma de decisiones en materia de controles de seguridad.

Alcance

Esta Política se aplica a toda la información administrada en el Organismo, cualquiera sea el soporte en que se encuentre.

Responsabilidad

El Comité de Seguridad de la Información será responsable de que se gestionen los riesgos de seguridad de la información, brindando su apoyo para el desarrollo de dicho proceso y su mantenimiento en el tiempo.

El Responsable de Seguridad de la Información junto con los Responsables de las Unidades Organizativas serán responsables del desarrollo del proceso de gestión de riesgos de seguridad de la información.

Política

4.1. Evaluación de los riesgos de seguridad

El Organismo evaluará sus riesgos identificándolos, cuantificándolos y priorizándolos en función de los criterios de aceptación de riesgos y de los objetivos de control relevantes para el mismo. Los resultados guiarán y determinarán la apropiada acción de la dirección y las prioridades para gestionar los riesgos de seguridad de la información y para la implementación de controles seleccionados para protegerse contra estos riesgos.

Se debe efectuar la evaluación de riesgos periódicamente, para tratar con los cambios en los requerimientos de seguridad y en las situaciones de riesgo, por ejemplo: cambios producidos en activos, amenazas, vulnerabilidades, impactos, valoración de riesgos. Asimismo, se debe efectuar la evaluación cada vez que ocurran cambios significativos. Es conveniente que estas evaluaciones de riesgos se lleven a cabo de una manera metódica capaz de producir resultados comparables y reproducibles.

El alcance de una evaluación de riesgos puede incluir a todo el Organismo, una parte, un sistema de información particular, componentes específicos de un sistema, o servicios. Resulta recomendable seguir una metodología de evaluación de riesgos para llevar a cabo el proceso.

4.2. Tratamiento de riesgos de seguridad

Antes de considerar el tratamiento de un riesgo, se determinará si los riesgos pueden, o no, ser aceptados. Los riesgos pueden ser aceptados si, por ejemplo: se evaluó que el riesgo es bajo o que el costo del tratamiento no es económicamente viable para la organización. Tales decisiones deben ser tomadas por las autoridades y debidamente documentadas.

Para cada uno de los riesgos identificados durante la evaluación de riesgos, se necesita tomar una decisión para su tratamiento. Las posibles opciones para el tratamiento de riesgos incluyen:

a) Mitigar los riesgos mediante la aplicación de controles apropiados para reducir los riesgos.
b) Aceptar los riesgos de manera objetiva y consciente, siempre y cuando éstos satisfagan claramente la política y los criterios de aceptación de riesgos del Organismo.
c) Evitar los riesgos, eliminando las acciones que dan origen a la ocurrencia de estos.

d) Transferir los riesgos asociados a otras partes interesadas, por ejemplo: compañías de seguro o proveedores.

Para aquellos riesgos donde la decisión ha sido la mitigación, se buscará reducirlos a un nivel aceptable mediante la implementación de controles, teniendo en cuenta lo siguiente:

a) requerimientos y restricciones de legislaciones y regulaciones nacionales e internacionales.
b) objetivos organizacionales.
c) requerimientos y restricciones operativos.
d) costo de implementación y operación en relación directa a los riesgos reducidos, y proporcionales a los requerimientos y restricciones del Organismo.
e) la necesidad de equilibrar las inversiones en la implementación y operación de los controles contra el daño que podría resultar de las fallas de seguridad.

Los controles a implementar pueden ser seleccionados del contenido de las cláusulas o puntos de esta política, o se pueden establecer nuevos controles para satisfacer necesidades específicas del Organismo. Es necesario reconocer que algunos controles pueden no ser aplicables a todo sistema de información o a su ambiente.

Se debe recordar que ningún conjunto de controles puede alcanzar la seguridad absoluta. Los controles implementados deben ser evaluados permanentemente para que puedan ser mejorados en eficiencia y efectividad.

5. POLÍTICA DE SEGURIDAD

Generalidades

Las Políticas de Seguridad de la Información protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos del Organismo.

Es importante que los principios de la Política de Seguridad de la Información sean parte de la cultura organizacional.

Para esto, se debe promover el compromiso de los titulares de las Unidades Organizativas para la difusión, la consolidación y el cumplimiento de la presente Política.

Objetivos

Proteger los activos del Organismo y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Implementar las medidas de seguridad comprendidas en esta Política, identificando los recursos y las partidas presupuestarias correspondientes, sin que ello implique necesariamente la asignación de partidas adicionales.

Mantener la Política de Seguridad de la Información del Organismo actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

Alcance

Esta Política se aplica en todo el ámbito del Organismo, a sus recursos y a la totalidad de los procesos, ya sean internos o externos, vinculados a la entidad a través de contratos o acuerdos con terceros.

Responsabilidad

Los responsables de las Unidades Organizativas, son los encargados de la implementación de esta Política de Seguridad de la Información, así como del cumplimiento de dicha Política por parte de su equipo de trabajo.

La Gerencia de Administración contemplará en caso de ser necesario la asignación de las partidas presupuestarias que se requieran para la implementación de las políticas de seguridad de la información.

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal del Organismo, cualquiera sea su situación de revista, el área a la cual se encuentre afectada y cualquiera sea el nivel de las tareas que desempeñe.

El Comité de Seguridad de la Información del Organismo,

- Procederá a revisar y proponer a la máxima autoridad del Organismo para su aprobación, los oportunos cambios que se apliquen a la Política de Seguridad de la Información y las funciones generales en materia de seguridad de la información;

  A través de las herramientas e informes que provea el Responsable de Seguridad de la Información:

  - tomará conocimiento y supervisará la investigación y el monitoreo de los incidentes relativos a la seguridad;

  - monitoreará cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes;

- Evaluará y elevará a consideración de la máxima autoridad las propuestas relativas a seguridad de la información del Organismo que fueran presentadas por las Unidades Organizativas[1], de acuerdo con sus competencias.

- Acordará las metodologías y los procesos específicos relativos a la seguridad de la información.

- Promoverá la difusión y el apoyo a la seguridad de la información dentro del Organismo y coordinará el proceso de administración de la continuidad de las actividades del Organismo (ver punto "17. Gestión de la Continuidad").

  El Coordinador del Comité de Seguridad de la Información será el responsable de coordinar las acciones del Comité de Seguridad de la Información y de impulsar la implementación y el cumplimiento de la presente Política.

[1] Se refiere a dar curso a las propuestas presentadas por parte de las áreas de acuerdo con sus competencias, elevándolas a la máxima autoridad, a través del Comité de Seguridad, con relación a la seguridad de la información del Organismo. Dichas iniciativas deberán ser aprobadas luego por la máxima autoridad del Organismo.

El Responsable de Seguridad de la Información:

- cumplirá funciones relativas a la seguridad de los sistemas de información del Organismo, lo cual incluye la supervisión de todos los aspectos inherentes a los temas tratados en la presente Política.

Los Propietarios de la Información son responsables de:

- clasificar la información de acuerdo con el grado de sensibilidad y criticidad de la misma,
- documentar y mantener actualizada la clasificación efectuada,
- definir qué usuarios deberán tener permisos de acceso a la información de acuerdo con sus funciones y competencia.

La Gerencia de Recursos Humanos y Relaciones Institucionales deberá:

- notificar a todo el personal que ingresa al Organismo de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, los procedimientos y las prácticas que de ella surjan.
- Asimismo, notificará la presente Política a todo el personal, los cambios que en ella se produzcan e impulsará las tareas de capacitación continua en materia de seguridad.

El Departamento de Tecnología de la Información cumplirá la función de cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología del Organismo. Por otra parte, tendrá la función de efectuar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología apropiada de ciclo de vida de sistemas, y que contemple la inclusión de medidas de seguridad en los sistemas, en todas las fases.

La Gerencia de Asuntos Legales verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación del Organismo con sus empleados y con terceros. Asimismo, asesorará en materia legal al Organismo, en lo que se refiere a la seguridad de la información.

Los usuarios de la información y de los sistemas utilizados para su procesamiento son responsables de conocer, dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente.

La Unidad de Auditoría Interna, es responsable de practicar auditorías periódicas sobre los sistemas y las actividades vinculadas con la tecnología de información, debiendo informar a la Máxima Autoridad del Organismo sobre el cumplimiento de las especificaciones y medidas de seguridad de la información

establecidas por esta Política y por las normas, los procedimientos y las prácticas que de ella surjan (Ver Capítulo 18 Cumplimiento).

5.1. Directrices de Gestión para la Seguridad de la Información

Objetivo

Proporcionar orientación y apoyo al Organismo para la seguridad de la información, en concordancia con sus funciones, las leyes y las regulaciones pertinentes.

Control

5.1.1. Política de seguridad de la información

Esta Política se conforma de una serie de pautas sobre aspectos específicos de la Seguridad de la Información, que incluyen los siguientes tópicos:

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

- **Seguridad en los Recursos Humanos**
  Orientado a reducir los riesgos de error humano, comisión de ilícitos contra el Organismo o uso inadecuado de instalaciones.

- **Gestión de Activos**
  Destinado a mantener una adecuada protección de los activos del Organismo.

- **Control de Accesos**
  Orientado a controlar el acceso lógico a la información.

- **Cifrado**
  Destinado al uso correcto de controles criptográficos.

- **Seguridad Física y Ambiental**
  Destinado a impedir accesos no autorizados, daños e interferencia a las sedes e información del Organismo.

- **Seguridad en las Operaciones**
  Dirigido a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información

- **Seguridad en las Telecomunicaciones**
  Dirigido a garantizar el funcionamiento correcto de los medios de comunicación.

- **Adquisición, Desarrollo y Mantenimiento de los sistemas de Información**
  Orientado a garantizar la incorporación de medidas de seguridad en los sistemas de información desde su adquisición, desarrollo y/o implementación y durante su mantenimiento.

- **Relaciones con Proveedores**
  Orientado a gestionar aspectos de seguridad de la información con los proveedores.

- **Gestión de Incidentes en la Seguridad de la Información**
  Orientado a administrar todos los eventos que atenten contra la confidencialidad, integridad y disponibilidad de la información y los activos tecnológicos

- **Gestión de la Continuidad**
  Orientado a contrarrestar las interrupciones de las actividades y proteger los procesos críticos de los efectos de fallas significativas o desastres.

- **Cumplimiento**
  Destinado 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.

Control

5.1.2. Revisión de las políticas de seguridad de la información

El Comité de Seguridad de la Información revisará cada vez que considere necesario la presente Política, a efectos de mantenerla actualizada. Asimismo, sugerirá toda modificación que sea necesaria en función de posibles cambios que puedan afectar su definición, tales como cambios tecnológicos, variación de los costos de los controles, impacto de los incidentes de seguridad.

6. ORGANIZACIÓN

Generalidades

La presente Política de Seguridad de la Información establece la administración de la seguridad de la información como parte fundamental de los objetivos y las actividades del Organismo.

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

Asimismo, se contemplará la necesidad de disponer de fuentes con conocimiento y experiencia para el asesoramiento, la cooperación y colaboración en materia de seguridad de la información.

Por otro lado, debe tenerse en cuenta que ciertas actividades del Organismo pueden requerir que terceros accedan a información interna, o bien puede ser necesaria la tercerización de ciertas funciones relacionadas con el procesamiento de la información. En estos casos se considerará que la información (digital y no digital) 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.

Objetivos

Administrar la seguridad de la información dentro del Organismo y establecer un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades.

Fomentar la consulta y cooperación con Organismos especializados (Ministerio de Modernización de la Nación, la ONTI, ICIC, etc.) para la obtención de asesoría en materia de seguridad de la información.

Garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información del Organismo.

Alcance

Esta Política se aplica a todos los recursos del Organismo y a todas sus relaciones con terceros que impliquen el acceso a sus datos, recursos y/o a la administración y el control de sus sistemas de información.

Responsabilidad

El Coordinador del Comité de Seguridad de la Información será el responsable de impulsar la implementación de la presente Política.

El Comité de Seguridad de la Información tendrá a cargo el mantenimiento y la presentación de las modificaciones que oportunamente correspondan para la aprobación de la presente Política ante la máxima autoridad del Organismo, el seguimiento de acuerdo con 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, entre otras) y la proposición de asignación de funciones.

El Responsable de Seguridad de la Información asistirá al personal del Organismo 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 del Organismo y verificará la aplicación de las medidas de seguridad necesarias para la protección de la misma.

Los Responsables de las Unidades Organizativas, conjuntamente con el Responsable de Seguridad de la Información, cumplirán la función de autorizar la incorporación de nuevos recursos de procesamiento de información a las áreas de su incumbencia.

La Gerencia de Administración cumplirá la función de incluir, en tiempo oportuno, la obligatoriedad del cumplimiento de esta Política y de todas las normas, procedimientos y prácticas relacionadas, por parte de los eventuales proveedores de servicios, bienes etc., cuya actividad afecte directa o indirectamente a los activos de información; y notificará a los proveedores de bienes o servicios, sobre las modificaciones que se efectúen a la referida Política, dejando a salvo que ello no implica una modificación de las condiciones contractuales correspondientes o las que hagan sus veces.

6.1. Organización interna de la política

Objetivo

Manejar la seguridad de la información dentro del Organismo.

Se debe establecer un marco referencial gerencial o político, para iniciar y controlar la implementación de la seguridad de la información dentro del organismo.

El Directorio debe aprobar la política de seguridad de la información, asignar los roles de seguridad y coordinar y revisar la implementación de la seguridad en todo el organismo.

Control

6.1.1. Responsabilidades y roles en la seguridad de la información

La seguridad de la información es una responsabilidad del Organismo compartida por su Máxima Autoridad y los Responsables de las Unidades Organizativas o Propietarios de la Información. El Comité cuenta con un Coordinador, quien cumple la función de impulsar la implementación de la presente Política.

A través de la resolución 841/2009 se crea el Comité de Seguridad de la Información (ver Anexo I), integrado por representantes de todas las Unidades Organizativas. Entre las funciones del comité

Apoyado en herramientas e informes que provea el Responsable de Seguridad de la Información el Comité de Seguridad de la Información cuenta con las siguientes funciones:

- Revisar y proponer a la máxima autoridad del Organismo, 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 y vulnerabilidades más importantes.
- Tomar conocimiento y supervisar la investigación y el monitoreo de los incidentes relativos a la seguridad.
- Proponer las principales iniciativas para incrementar la seguridad de la información, de acuerdo con las competencias y responsabilidades asignadas a cada Unidad Organizativa.
- Acordar y proponer metodologías y procesos específicos relativos a la seguridad de la información.
- Promover la difusión y el apoyo a la seguridad de la información dentro del Organismo.

- Coordinar el proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de la información frente a interrupciones imprevistas (ver punto "17. Gestión de la Continuidad").

El Coordinador del Comité de Seguridad de la Información coordinará las actividades del Comité de Seguridad de la Información.

El Responsable de Seguridad de la Información tendrá a cargo las funciones relativas a la seguridad de los sistemas de información del Organismo, lo cual incluye la supervisión de todos los aspectos inherentes a seguridad tratados en la presente Política. Entre sus funciones se encuentran:

- Garantizar que la seguridad sea parte del proceso de planificación de los sistemas de información.

- Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.

Control

6.1.2. Segregación de funciones

Se separará en caso de corresponder la gestión o ejecución de ciertas tareas o áreas de responsabilidad, a fin de reducir el riesgo de modificaciones no autorizadas o el mal uso de la información y/o los servicios, por falta de independencia en la ejecución de funciones críticas.

Si este método de control no se pudiera cumplir en algún caso, el Responsable de Seguridad de la Información será el encargado de implementar controles, tales como:

a) Monitoreo de las actividades.
b) Registros de auditoría y control periódico de las actividades.

También se podrá solicitar supervisión por parte de la Unidad de Auditoría Interna.

Asimismo, se documentará la justificación formal por la cual no fue posible efectuar la segregación de funciones.

Se asegurará la independencia de las funciones de auditoría de seguridad, tomando recaudos para que ninguna persona pueda realizar actividades en áreas de responsabilidad única sin ser monitoreada, y la independencia entre el inicio de un evento y su autorización, considerando los siguientes puntos:

a) Separar actividades que requieren connivencia para defraudar

b) Diseñar controles, si existe peligro de connivencia de manera tal que dos o más personas estén involucradas, reduciendo la posibilidad de conspiración.

Control

6.1.3. Contacto con otros organismos

A efectos de intercambiar experiencias y obtener asesoramiento para el mejoramiento de las prácticas y controles de seguridad, se mantendrán contactos con los siguientes Organismos especializados o los que en el futuro los reemplacen en temas relativos a la seguridad informática:

- Subsecretaría de Tecnología y Ciberseguridad del Ministerio de Modernización de la Nación (DA 232/2016), y particularmente con:
  - Oficina Nacional de Tecnologías de Información (ONTI).
  - Infraestructura de Firma Digital.
  - ICIC - Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad.
- Dirección Nacional de Protección de Datos Personales.

Control

6.1.4. Contacto con grupos de interés especial

El Responsable de Seguridad de la información 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. Éste podrá obtener asesoramiento de otros Organismos. Con el objeto de optimizar su gestión, se habilitará al Responsable de Seguridad de la Información el contacto con otros Organismos de la Administración Pública que resulten relevantes.

Debe considerar ser miembro de grupos de interés especial para:

a) Adquirir nuevos conocimientos acerca de las mejores prácticas y estar actualizado.
b) Asegurar que la concientización acerca de la seguridad de la información esté actualizada y completa.
c) Recibir alertas tempranas, avisos y recomendaciones ante ataques y vulnerabilidades.
d) Proporcionar vínculos adecuados durante el tratamiento de los incidentes de seguridad de la información.

Control

6.1.5. Seguridad de la información en la gestión de proyectos

Se deberá contemplar la seguridad de la información en la gestión de proyectos, independientemente del tipo de proyecto a desarrollar por el Organismo.

6.2. Dispositivos móviles y teletrabajo

Objetivo

Garantizar la seguridad de la información cuando se utilizan medios de computación y teletrabajo móviles.

Control

6.2.1. Política de dispositivos móviles

Cuando se utilizan dispositivos informáticos móviles se debe tener especial cuidado en garantizar que no se comprometa la información ni la infraestructura del Organismo.

Se debe tener en cuenta en este sentido, cualquier dispositivo móvil y/o removible, incluyendo: Notebooks, Laptop o PDA (Asistente Personal Digital), Teléfonos Celulares y sus tarjetas de memoria, Dispositivos de Almacenamiento removibles, tales como CDs, DVDs, Disquetes, Tapes, y cualquier dispositivo de almacenamiento de conexión USB, Tarjetas de identificación personal (control de acceso), dispositivos criptográficos, cámaras digitales, etc.

Esta lista no es taxativa, ya que deben incluirse todos los dispositivos que pudieran contener información confidencial del Organismo y, por lo tanto, ser pasibles de sufrir un incidente en el que se comprometa la seguridad del mismo.

Se desarrollarán procedimientos adecuados para estos dispositivos, que abarquen los siguientes conceptos:

a) La protección física necesaria.
b) El acceso seguro a los dispositivos.
c) La utilización segura de los dispositivos en lugares públicos.
d) El acceso a los sistemas de información y servicios del Organismo a través de dichos dispositivos.
e) Las técnicas criptográficas a utilizar para la transmisión de información clasificada.
f) Los mecanismos de resguardo de la información contenida en los dispositivos.

g) La protección contra software malicioso.

La utilización de dispositivos móviles incrementa la probabilidad de ocurrencia de incidentes del tipo de pérdida, robo o hurto. En consecuencia, debe entrenarse especialmente al personal que los utilice. Se desarrollarán normas y procedimientos sobre los cuidados especiales a observar ante la posesión de dispositivos móviles.

Por otra parte, se confeccionarán procedimientos que permitan al poseedor del dispositivo reportar rápidamente cualquier incidente sufrido y mitigar los riesgos a los que eventualmente estuvieran expuestos los sistemas de información del Organismo, los que incluirán:

a) Revocación de las credenciales afectadas
b) Notificación a grupos de Trabajo donde potencialmente se pudieran haber comprometido recursos.

Control

Teletrabajo

El teletrabajo utiliza tecnología de comunicaciones para permitir que el personal trabaje en forma remota desde un lugar externo al Organismo.

El trabajo remoto sólo será autorizado y definido por el Responsable de la Unidad Organizativa a la cual pertenezca el usuario solicitante, o en caso de los Gerentes por la Máxima Autoridad del Organismo, e implementado por el Responsable del Departamento de Tecnología de la Información el cual determinará, conjuntamente con el Responsable de Seguridad de la Información, las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con esta Política, normas y procedimientos existentes.

La solicitud para el trabajo remoto deberá contener las razones que justifiquen esta modalidad.

Para ello, se establecerán procedimientos para el trabajo remoto, que consideren los siguientes aspectos:

a) Los requerimientos de seguridad de comunicaciones, tomando en cuenta la necesidad de acceso remoto a los sistemas internos del Organismo, la sensibilidad de la información a la que se accederá y que pasará a través del vínculo de comunicación y la sensibilidad del sistema interno.
b) La amenaza de acceso no autorizado a información o recursos por parte de otras personas que utilizan el lugar, por ejemplo, familia y amigos.
c) Evitar la instalación / desinstalación de software no autorizado por el Organismo. En los equipos dispuestos por el Departamento de Tecnología de la Información para dicha tarea.

Los recursos y controles comprenden:

a) Proveer el equipamiento adecuado para las actividades de trabajo remoto (Estación de trabajo, Software necesario para acceso remoto, etc.).
b) El horario de trabajo, la clasificación de la información que se puede almacenar en el equipo remoto desde el cual se accede a la red del Organismo y los sistemas internos y servicio a los cuales el trabajador remoto está autorizado a acceder.
c) Definir reglas y orientación respecto del acceso de terceros al equipamiento e información.
d) Proveer el hardware y el soporte y mantenimiento del software.
e) Definir los procedimientos de backup y de continuidad de las operaciones.
f) Efectuar auditoría y monitoreo de la seguridad.
g) Realizar la anulación de las autorizaciones, derechos de acceso y devolución del equipo cuando finalicen las actividades remotas.
h) Asegurar el reintegro del equipamiento en las mismas condiciones en que fue entregado, en el caso en que cese la necesidad de trabajar en forma remota.

El Responsable de Seguridad de la Información será el encargado de implementar procesos de auditoría específicos para los casos de accesos remotos, que serán revisados regularmente. Se llevará un registro de incidentes a fin de corregir eventuales fallas en la seguridad de este tipo de accesos.

7. SEGURIDAD DE LOS RECURSOS HUMANOS

Generalidades

La seguridad de la información se basa en la capacidad para preservar su integridad, confidencialidad y disponibilidad, por parte de los elementos involucrados en su tratamiento: equipamiento, software, bases de datos, documentos físicos, procedimientos, y por parte de los recursos humanos que utilizan dichos componentes.

En este sentido, es fundamental capacitar e informar al personal desde su ingreso y en forma continua, acerca de las medidas de seguridad y confidencialidad que afectan al desarrollo de sus funciones.

Objetivos

Reducir los riesgos de error humano, comisión de ilícitos, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.

Explicitar las responsabilidades en materia de seguridad en la etapa de incorporación de personal, incluirlas en los acuerdos por firmarse y verificar su cumplimiento durante el desempeño del empleado.

Explicitar las responsabilidades en materia de seguridad en la etapa de contratación de servicios, incluirlas en los contratos para firmarse y verificar su cumplimiento durante su desarrollo.

Garantizar que los usuarios estén informados de las posibles amenazas e incumbencias en materia de seguridad de la información, y que se encuentren capacitados para cumplir la Política de Seguridad de la Información del Organismo en el transcurso de sus tareas.

Establecer Compromisos de Confidencialidad con todo el personal y los usuarios externos de las instalaciones de procesamiento de información.

Establecer las herramientas y los mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su recurrencia.

Política de Seguridad de la Información

Alcance

Esta Política se aplica a todo el personal del Organismo, cualquiera sea su situación de revista, y al personal externo que efectúe tareas dentro del ámbito del Organismo.

Responsabilidad

La Gerencia de Asuntos Legales, en conjunto con la Gerencia de Recursos Humanos y Relaciones Institucionales, participará en la confección del Compromiso de Confidencialidad a firmar por los empleados y terceros que desarrollen funciones para el Organismo.

La Gerencia de Recursos Humanos y Relaciones Institucionales notificará a todo el personal de sus obligaciones respecto al cumplimiento de la Política de Seguridad de la Información, gestionará los Compromisos de Confidencialidad con el personal y coordinará las tareas de capacitación de usuarios respecto de la presente Política.

Los Responsables de cada Unidad Organizativa serán los encargados de definir el perfil de acceso a la información del personal a su cargo.

El Responsable de Seguridad de la Información tendrá a su cargo el seguimiento, la documentación y el análisis de los incidentes de seguridad reportados, así como su comunicación al Comité de Seguridad de la Información, a los propietarios de la información y al Programa de Infraestructuras Críticas de Información y Ciberseguridad.

El Responsable de Seguridad de la Información será el encargado de gestionar y administrar los reportes de incidentes y anomalías relativas a la seguridad en la gestión de la información. Asimismo, Informará al Comité de Seguridad de la Información sobre dichos incidentes para que este tome conocimiento, efectué un seguimiento y controle resolución de los incidentes relativos a la seguridad.

Todo el personal del Organismo es responsable de reportar al Departamento de Tecnología de la Información las debilidades e incidentes de seguridad que oportunamente se detecten. Para que luego el Responsable del Departamento junto con el Responsable de Seguridad de la Información registren y toman las acciones correctivas que correspondan.

Política

7.1. Antes del empleo

Objetivo

Promover que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean idóneos para los roles para los cuales son considerados; y reducir el riesgo de robo, fraude y mal uso de los medios.

Las responsabilidades de seguridad deben ser tratadas antes del comienzo formal de las tareas por parte del empleado.

Control

7.1.1. Funciones y Responsabilidades

Es responsabilidad de la Gerencia de Recursos Humanos y Relaciones Institucionales del Organismo y de los Responsables de las Unidades Organizativas la definición de las tareas a cargo de los empleados. Allí se contemplará la inclusión de las responsabilidades en materia de seguridad de la información.

Control

7.1.2. Términos y condiciones de empleo

Como parte de los términos y condiciones iniciales de empleo, los empleados, cualquiera sea su situación de revista, firmarán un Compromiso de Confidencialidad o No Divulgación, en lo que respecta al tratamiento de la información del Organismo. Este Compromiso será confeccionado por la Gerencia de Asuntos Legales y la Gerencia de Recursos Humanos y Relaciones Institucionales, conforme los procedimientos correspondientes. La copia firmada del Compromiso debe ser retenida en forma segura por la Gerencia de Recursos Humanos y Relaciones Institucionales.

Asimismo, mediante el Compromiso de Confidencialidad el empleado declarará conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas en dicho Compromiso a fin de no violar el derecho a la privacidad del empleado.

El responsable de Seguridad de la Información desarrollará un procedimiento para la suscripción del Compromiso de Confidencialidad donde se incluirán aspectos sobre:

- Notificación inicial del Compromiso por parte de la totalidad del personal y en caso de modificaciones
- Revisión del contenido del Compromiso cada vez que se considere necesario.

Los términos y condiciones de empleo establecerán la responsabilidad del empleado en materia de seguridad de la información.

Cuando corresponda, los términos y condiciones de empleo establecerán que estas responsabilidades se extienden más allá de los límites de la sede del Organismo y del horario normal de trabajo.

7.2. Durante el empleo

Objetivo

Asegurar que los usuarios empleados, contratistas y terceras personas estén al tanto de las amenazas de la seguridad de la información, así como notificados de sus responsabilidades y obligaciones, y posean las herramientas suficientes para apoyar la política de seguridad en el curso de su trabajo normal, y reducir el riesgo de error humano.

Esto, en línea con la presente política permitirá definir los controles de seguridad necesarios a lo largo de todo el tiempo de empleo del personal.

Control

7.2.1. Responsabilidades

Los empleados, contratistas y usuarios de terceras partes deberán aplicar la seguridad en concordancia con las políticas y procedimientos establecidos por el Organismo, cumpliendo con lo siguiente:

a) Estar adecuadamente informados de sus roles y responsabilidades de seguridad de la información antes de que se les otorgue el acceso a información sensible o a los sistemas de información.
b) Ser provistos de guías para establecer las expectativas de seguridad de su rol dentro del Organismo.
c) Ser motivados para cumplir con las políticas de seguridad del Organismo.
d) Alcancen un nivel de conciencia sobre la seguridad acorde con sus roles y responsabilidades dentro del Organismo.
e) Cumplir con las condiciones y términos del empleo, los cuales incluyen las políticas de seguridad de la información del Organismo y métodos adecuados de trabajo.
f) Mantenerse con las habilidades y calificaciones adecuadas.

Control

7.2.2. Concientización, formación y capacitación en seguridad de la información

Todos los empleados del Organismo recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos del Organismo. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general, como por ejemplo su estación de trabajo.

El Responsable de la Gerencia de Recursos Humanos y Relaciones Institucionales o quien este designe dentro de su Unidad Organizativa, será el encargado de coordinar las acciones de capacitación que surjan de la presente Política.

Cada doce (12) meses se revisará el material correspondiente a la capacitación, a fin de evaluar la pertinencia de su actualización.

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

Áreas Responsables del material de capacitación
Gerencia de Recursos Humanos y Relaciones Institucionales
Departamento de Tecnología de la Información

El personal que ingrese al Organismo 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, que deban ser tratadas con un orden preferencial.

Control

7.2.3. Procedimiento disciplinario

Se seguirá el procedimiento disciplinario que corresponda según la normativa que resulte de aplicación, para los empleados que violen la Política, Normas y Procedimientos de Seguridad del Organismo.

7.3. Cese del empleo o cambio de puesto de trabajo

Objetivo

Asegurar que los usuarios empleados, contratistas y terceras personas que cesen el vínculo con el Organismo o cambien de empleo, lo realicen de una manera ordenada.

Se deben establecer las responsabilidades para asegurar que la finalización del vínculo entre el Organismo y el usuario empleado, contratista o tercera persona sea manejada y se complete la devolución de todo el equipo y se eliminen todos los derechos de acceso.

Control

7.3.1. Responsabilidad del cese o cambio

Las responsabilidades para realizar la desvinculación o cambio de puesto deben ser claramente definidas y asignadas, incluyendo requerimientos de seguridad y responsabilidades legales a posteriori y, cuando sea apropiado, las responsabilidades contenidas dentro de cualquier acuerdo de confidencialidad, y los términos y condiciones de empleo con continuidad por un período definido luego de la finalización del trabajo del empleado, contratista o usuario de tercera parte.

Puede ser necesario informar a los empleados, contratistas y terceros de los cambios en el personal y los acuerdos de operación, en los casos que resulte necesario dada la función asignada al personal involucrado.

8. GESTIÓN DE ACTIVOS

Generalidades

El Organismo debe tener un acabado conocimiento sobre los activos que posee, como parte importante de la administración de riesgos.

Asimismo, es el propietario de todos los activos generados o adquiridos por él y definidos en el presente documento.

El Responsable de Seguridad de la Información deberá prever la posibilidad de que cualquier activo pueda, con el tiempo, variar en su clasificación.

Objetivo

Garantizar que los activos reciban un apropiado nivel de protección, acorde a la criticidad que resulte con motivo de su clasificación, sobre la base de los niveles de confidencialidad, integridad y disponibilidad que se establecen en el presente capítulo.

Alcance

Comprende a todos los activos administrados por el Organismo y a todo el personal que trabaja para este, cualquiera sea su vinculación laboral.

Responsabilidad

El Responsable de cada Unidad Organizativa determinará o delegará para cada caso, en uno o más funcionarios de su Unidad, la responsabilidad de establecer el grado de criticidad que le corresponde a cada activo de información administrado por su Unidad Organizativa.

Cada funcionario del Organismo velará por que todo activo bajo su responsabilidad sea tratado conforme al nivel de criticidad que le corresponda, según lo establecido en el presente documento.

El Responsable de Seguridad de la Información es el encargado de asegurar que los lineamientos para la utilización de los recursos de la información contemplen los requerimientos de seguridad establecidos según la criticidad de la misma.

Política

8.1. Responsabilidad sobre los activos de información

Objetivo

Todos los activos deben ser inventariados y contar con un propietario nombrado. La implementación de controles específicos puede ser delegada por el propietario conforme sea apropiado, pero el propietario sigue siendo responsable por la protección apropiada de los activos.

Se excluyen del presente apartado los casos específicos con un régimen propio de identificación.

Control

8.1.1. Inventario de activos

El Responsable de cada Unidad Organizativa es el encargado de elaborar el inventario de los Activos bajo su responsabilidad y de mantenerlo actualizado; asimismo, identificará el medio de soporte y ubicación en cada caso.

Cada doce (12) meses, cada Unidad Organizativa deberá actualizar el inventario de los activos bajo su responsabilidad, en caso de modificación.

La Gerencia de Administración a través de su Área de Contabilidad es la responsable de mantener actualizado el inventario de todos los bienes que posee el organismo.

Con respecto a los activos de información, de software y físicos que correspondan a tecnología, el Departamento de Tecnología de la Información será responsable de mantenerlos actualizados siendo estos específicos a su función. Luego los activos físicos y de software antes nombrados serán inventariados junto con la Gerencia de Administración.

Control

8.1.2. Propiedad de los activos

Toda la información y los activos junto a sus medios de procesamiento de información deben ser propiedad de un responsable designado en el organismo.

Se designarán los Propietarios de los activos identificados, quienes deben cumplir sus funciones de propietario, esto es:

a) Informar sobre cualquier cambio que afecte el inventario de activos.
b) Clasificar los activos en función a su valor.
c) Definir los requisitos de seguridad de los activos.
d) Velar por la implementación y el mantenimiento de los controles de seguridad requeridos en los activos.

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 los activos será documentada por los mismos y proporcionada al Responsable de Seguridad de la Información.

Control

8.1.3. Uso aceptable de los activos

Se identificarán, documentarán e implementarán reglas para el uso aceptable de la información y los activos asociados con las instalaciones de procesamiento de la información.

Todos los empleados, contratistas y usuarios de terceras partes deben seguir las reglas para el uso aceptable de la información y los activos asociados con las instalaciones de procesamiento de la misma, incluyendo:

a) Correo electrónico,
b) Sistemas de gestión,
c) Estaciones de trabajo,
d) Dispositivos móviles,
e) Herramientas y equipamiento de publicación de contenidos.

Control

8.1.4. Devolución de activos

Todos los empleados, contratistas y usuarios de terceras partes deben devolver todos los activos del organismo en su poder (software, equipamiento, dispositivos de computación móviles, celulares, tarjetas de ingreso, etc.) tras la terminación de su empleo, contrato, o acuerdo.

En los casos donde el empleado, contratista y usuarios tengan conocimiento que es importante para las operaciones actuales, esa información debe ser documentada y transferida al Organismo.

8.2. Clasificación de la Información

Objetivo

Asegurar que la información reciba un nivel de protección apropiado.

Control

8.2.1. Directrices de clasificación

Los activos de información, a los fines de la implementación de la presente Política y con el alcance en ella previsto, se clasificarán de acuerdo con las tres características en las cuales se basa la seguridad de estos: confidencialidad, integridad y disponibilidad.

A continuación, se establece la metodología de clasificación en función a cada una de las mencionadas características. Sin perjuicio de ello y ante cualquier requisitoria externa al Organismo, su clasificación deberá encuadrar en los parámetros establecidos en la normativa que regula los procedimientos administrativos y el acceso a la información pública.

De la combinación de los tres niveles resultará el nivel de criticidad de cada Activo de Información.

- **Nivel de confidencialidad:**

a) **PÚBLICA:** Que puede ser conocida y utilizada por cualquier persona o sistema de procesamiento de información.
b) **RESERVADA:**
   a. **RESERVADA USO INTERNO**: Que solo puede ser utilizada por todo el personal del Organismo y terceros autorizados.
   b. **RESERVADA CONFIDENCIAL:** Que solo puede ser conocida y utilizada por el personal del Organismo autorizado.
   c. **RESERVADA SECRETA:** Que sólo puede ser conocida y utilizada por un grupo reducido de empleados, generalmente los Responsables de las Unidades Organizativas o el Directorio.

- **Nivel de integridad por modificación no autorizada:**

a) Que se puede restaurar fácilmente y no afecta la operatoria del Organismo.
b) Que se puede restaurar, pero podría ocasionar pérdidas leves para el Organismo, Sector Público Nacional o terceros.
c) Que es difícil restaurar y podría ocasionar pérdidas significativas para el Organismo, Sector Público Nacional o terceros.

d) Que no se puede restaurar, ocasionando pérdidas graves al Organismo, Sector Público Nacional o a terceros.

- **Nivel de disponibilidad**

0) Imposibilidad de acceder a la información sin afectar a la operatoria del Organismo.
1) Imposibilidad de acceder a la información durante siete (7) días corridos: podría ocasionar pérdidas significativas para el Organismo, Sector Público Nacional o terceros.
2) Imposibilidad de acceder a la información durante veinticuatro (24) horas corridas: podría ocasionar pérdidas significativas para el Organismo, Sector Público Nacional o terceros.
3) Imposibilidad de acceder a la información durante cuatro (4) horas corridas: podría ocasionar pérdidas significativas para el Organismo, Sector Público Nacional o terceros.

Al referirse a pérdidas, se contemplarán tanto las mensurables (materiales) como no mensurables (imagen, valor estratégico de la información, obligaciones contractuales o públicas, disposiciones legales, etc.).

El nivel de criticidad será el resultado de:

1. **CRITICIDAD BAJA:** ninguno de los valores asignados supera el 1.
2. **CRITICIDAD MEDIA:** alguno de los valores asignados es 2.
3. **CRITICIDAD ALTA:** alguno de los valores asignados es 3.

Hacer referencia a la clasificación de la información previamente conectada. Solo los Responsables de cada Unidad Organizativa podrán cambiar el nivel de clasificación de cualquiera de las características de los Activos de Información bajo su responsabilidad, cumpliendo con los siguientes requisitos previos:

- Asignarle una fecha de efectividad.
- Comunicárselo al depositario del recurso.
- Realizar los cambios necesarios para que los Usuarios conozcan la nueva clasificación.

Luego de clasificada la información, los autorizados definidos en el apartado Responsabilidad identificarán los recursos asociados (sistemas, equipamiento, servicios, entre otros) y los perfiles funcionales que deberán tener acceso a la misma.

En adelante se mencionará como "activo de información clasificado" (o "datos clasificados") a aquellos que se encuadren en los niveles 1, 2 o 3 de Criticidad.

Control

8.2.2. Etiquetado y manipuleo de la información

Se definirán en caso de corresponder, procedimientos para el rotulado de información, de acuerdo con el esquema de clasificación definido. Estos contemplarán los recursos de información, tanto en formatos físicos como digitales, e incorporarán las siguientes actividades de procesamiento de la información:

- Copia.
- Almacenamiento.
- Transmisión de la información independientemente del recurso empleado.

Control

8.2.3. Manejo de los activos

Para cada uno de los niveles de clasificación, se definen los procedimientos de manejo seguros, incluyendo las actividades de procesamiento, almacenaje, transmisión, de-clasificación y destrucción.

8.3. Gestión de medios

Objetivo

Evitar la divulgación no-autorizada; modificación, eliminación o destrucción de activos; y la interrupción de las actividades. Los medios se debieran controlar y proteger físicamente.

Se deben establecer los procedimientos de operación apropiados para proteger los documentos, medios de cómputo (por ejemplo, cintas y discos), entrada/salida de datos (input/output) y documentación del sistema de una divulgación no-autorizada, modificación, eliminación y destrucción.

Control

8.3.1. Administración de Medios Informáticos Removibles

El Departamento de tecnología de la información, con la asistencia del Responsable de Seguridad de la Información, implementará procedimientos para la administración de medios informáticos removibles, como cintas, discos, pen drives e informes impresos. El cumplimiento de los procedimientos se hará de acuerdo al punto "9.1 Requerimientos para la Gestión de Acceso".

Se deben considerar las siguientes acciones para la implementación de los procedimientos:

a) Eliminar de forma segura los contenidos, si ya no son requeridos, de cualquier medio reutilizable que ha de ser retirado o reutilizado por el Organismo.
b) Requerir autorización para retirar cualquier medio del Organismo y realizar un control de todos los retiros a fin de mantener un registro de auditoría.
c) Almacenar todos los medios en un ambiente seguro y protegido, de acuerdo con las especificaciones de los fabricantes o proveedores y la criticidad de la información almacenada.

Control

8.3.2. Eliminación de Medios de Información

El Departamento de Tecnología de la Información, junto con el Responsable de Seguridad de la Información definirá procedimientos para la eliminación segura de los medios de soporte de información respetando la normativa vigente.

Los procedimientos deben considerar que los siguientes elementos requerirán almacenamiento y eliminación segura:

a) Documentos en papel.
b) Voces u otras grabaciones.
c) Papel carbónico.
d) Informes de salida.
e) Cintas de impresora de un solo uso.
f) Cintas magnéticas.
g) Discos u otros dispositivos removibles.
h) Medios de almacenamiento óptico (todos los formatos incluyendo todos los medios de distribución de software del fabricante o proveedor).
i) Listados de programas.
j) Datos de prueba.
k) Documentación del sistema.
l) Cualquier otro dispositivo que permita almacenar información y que no esté incluido en los puntos anteriores.

La evaluación del mecanismo de eliminación debe contemplar el tipo de dispositivo y la criticidad de la información contenida.

Control

8.3.3. Seguridad de los Medios en Tránsito.

Los procedimientos de transporte de medios informáticos entre diferentes puntos (envíos postales y mensajería) deben contemplar:

a) La utilización de medios de transporte o servicios de mensajería confiables. El Propietario de la Información a transportar determinará qué servicio de mensajería se utilizará conforme la criticidad de la información a transmitir.
b) Suficiente embalaje para envío de medios a través de servicios postales o de mensajería, siguiendo las especificaciones de los fabricantes o proveedores.
c) La adopción de controles especiales, cuando resulte necesario, a fin de proteger la información sensible contra divulgación o modificación no autorizadas. Entre los ejemplos se incluyen:

    1) Uso de recipientes cerrados.
    2) Entrega en mano.
    3) Embalaje a prueba de apertura no autorizada (que revele cualquier intento de acceso).
    4) En casos excepcionales, división de la mercadería a enviar en más de una entrega y envío por diferentes rutas.

9. CONTROL DE ACCESOS

Generalidades

El acceso por medio de un sistema de restricciones 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 la asignación 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.

Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso.

Objetivos

Preservar la información, impidiendo el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.

Implementar la seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.

Controlar la seguridad en la conexión entre la red del Organismo y otras redes públicas o privadas.

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.

Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.

Alcance

La Política definida en este documento se aplica a todas las formas de acceso de aquellos a quienes se les haya otorgado permisos sobre los sistemas de

información, bases de datos o servicios de información del Organismo, cualquiera sea la función que desempeñe.

Asimismo, se aplica al personal técnico que define, instala, administra y mantiene los permisos de acceso y las conexiones de red, y a los que administran su seguridad.

Responsabilidad

El Responsable de Seguridad de la Información estará a cargo de:

- Definir procedimientos para: la gestión de accesos a todos los sistemas, bases de datos y servicios de información multiusuario; el monitoreo del uso de las instalaciones de procesamiento de la información; la solicitud y aprobación de accesos a Internet; el uso de computación móvil, trabajo remoto y reportes de incidentes relacionados; la respuesta a la activación de alarmas silenciosas; la revisión de registros de actividades; y el ajuste de relojes de acuerdo con un estándar preestablecido.
- Definir pautas de utilización de Internet para todos los usuarios.
- Participar en la definición de procedimientos de seguridad para implementar en el ambiente informático, como, por ejemplo, sistemas operativos, servicios de red, enrutadores o gateways y validarlos periódicamente.
- Controlar la asignación de privilegios a usuarios.
- Analizar y sugerir medidas a ser implementadas para efectivizar el control de acceso a Internet de los usuarios.
- Verificar el cumplimiento de las pautas establecidas, relacionadas con control de accesos, registración de usuarios, administración de privilegios, administración de contraseñas, utilización de servicios de red, autenticación de usuarios y nodos, uso controlado de utilitarios del sistema, alarmas silenciosas, desconexión de terminales por tiempo muerto, registro de eventos, protección de puertos, subdivisión de redes, control de conexiones a la red, control de ruteo de red, entre otras.
- Concientizar a los usuarios sobre el uso apropiado de contraseñas y de equipos de trabajo.
- Verificar el cumplimiento de los procedimientos de revisión de registros de auditoría.
- Asistir a los usuarios que corresponda en el análisis de los riesgos a los que se expone la información y los componentes del ambiente informático que le sirven de soporte.

Los Propietarios de la Información estarán encargados de:

- Evaluar los riesgos a los cuales se expone la información con el objeto de:
  - Determinar los controles de accesos, autenticación y utilización para ser implementados en cada caso.

- Definir los eventos / las actividades de usuarios a ser registrados en los sistemas de procesamiento de su incumbencia y la periodicidad de revisión de los mismos.
- Aprobar y solicitar la asignación de privilegios a usuarios.
- Llevar a cabo un proceso formal y periódico de revisión de los derechos de acceso a la información.

Los Propietarios de la Información, junto con la Unidad de Auditoría Interna, definirán un cronograma de depuración de registros en línea, en función de las normas vigentes y de sus propias necesidades.

Los Responsables de las Unidades Organizativas, con la asistencia dl Responsable de Seguridad de la Información, autorizarán el trabajo remoto del personal a su cargo, en los casos en que se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con las normas vigentes. Asimismo, autorizarán el acceso de los usuarios a su cargo, a los servicios y recursos de red y a Internet.

El Departamento de Tecnología de la Información cumplirá las siguientes funciones:

- Implementar procedimientos para la activación y desactivación de derechos de acceso a las redes.
- Analizar e implementar los métodos de autenticación y control de acceso definidos en los sistemas, bases de datos y servicios.
- Evaluar el costo y el impacto de la implementación de "enrutadores" o "gateways" adecuados para subdividir la red y recomendar el esquema apropiado.
- Implementar el control de puertos, de conexión a la red y de ruteo de red.
- Implementar el registro de eventos o actividades de usuarios, de acuerdo con lo definido por los propietarios de la información, así como la depuración de los registros.
- Definir e implementar los registros de eventos y actividades correspondientes a sistemas operativos y otras plataformas de procesamiento.
- Evaluar los riesgos sobre la utilización de las instalaciones de procesamiento de información, con el objeto de definir medios de monitoreo y tecnologías de identificación y autenticación de usuarios (Ej.: biometría, verificación de firma, uso de autenticadores de hardware).
- Definir e implementar la configuración que debe efectuarse para cada servicio de red, de manera de garantizar la seguridad en su operatoria.
- Analizar las medidas a ser implementadas para efectivizar el control de acceso a Internet de los usuarios.
- Otorgar acceso a los servicios y recursos de red, únicamente de acuerdo con el pedido formal correspondiente.
- Efectuar un control de los registros de auditoría generados por los sistemas operativos y de comunicaciones.

La Unidad de Auditoría Interna y/o los especialistas que al efecto se contraten en materia de auditoría de tecnología de la información, tendrán acceso a los registros de eventos, a fin de colaborar en el control y efectuar recomendaciones sobre modificaciones a los aspectos de seguridad.

El Comité de Seguridad de la Información aprobará el análisis de riesgos de la información efectuado. Asimismo, aprobará el período definido para el mantenimiento de los registros de auditoría generados.

Política

9.1. Requerimientos para la Gestión de Acceso

Objetivo

Controlar el acceso a la información. Se debe controlar el acceso a la información, medios de procesamiento de la información y procesos sobre la base de los requerimientos del organismo y de seguridad.

Las reglas de control del acceso deben tomar en cuenta las políticas para la divulgación y autorización de la información.

Control

9.1.1. Política de Gestión de Accesos

En la aplicación de gestión 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 (Ver cláusula 8 Gestión de Activos).
d) Identificar la legislación aplicable y las obligaciones contractuales con respecto a la protección del acceso a datos y servicios.
e) Definir los perfiles de acceso de usuarios estándar, comunes a cada categoría de puestos de trabajo.
f) Administrar los derechos de acceso en un ambiente distribuido y de red, que reconozcan todos los tipos de conexiones y dispositivos disponibles.

Control

9.1.2. Política de uso de los servicios de red

Las conexiones no seguras a los servicios de red pueden afectar a todo el Organismo, 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 su seguridad.

El Departamento de Tecnología de la Información tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red, únicamente de acuerdo con el pedido formal del titular de una Unidad Organizativa que lo solicite para personal de su incumbencia.

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 del Organismo.

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 los servicios de red a los cuales se permite el acceso.

b) Realizar normas y procedimientos de autorización para determinar las personas, las redes y los 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 los servicios de red.

9.2. Administración de Gestión de Usuarios

Objetivo

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

Los procedimientos debieran abarcar todas las etapas en el ciclo de vida del acceso del usuario, desde el registro inicial de usuarios nuevos hasta la baja final de los usuarios que ya no requieren acceso a los sistemas y servicios de información.

Control

9.2.1. Gestión de altas y bajas en el registro de usuarios

El Responsable de Seguridad de la Información en colaboración con los titulares de cada unidad organizativa, definirá un procedimiento de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información multiusuario, el cual deberá:

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 usuario. El uso de identificadores grupales solo debe ser permitido cuando sean convenientes para el trabajo a desarrollar debido a razones operativas.
b) Verificar que el usuario tenga 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 sea coherente con la Política de Seguridad de la Información del Organismo, por ejemplo, que no comprometa la separación de tareas.
d) Notificar a los usuarios un detalle escrito de sus derechos de acceso.
e) Requerir que los usuarios firmen declaraciones en las que señalen 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 60 días;
   - eliminar cuentas inactivas por más de 180 días.

   En el caso de existir excepciones, deberán ser debidamente justificadas y aprobadas. En caso de cancelaciones, inhabilitaciones o eliminaciones de cuentas, no operarán de modo automático. Las excepciones deberán ser solicitadas por el Responsable de la Unidad Organizativa correspondiente.
j) Garantizar que los identificadores de usuario redundantes no se asignen a otros usuarios.
k) Incluir cláusulas de confidencialidad en los contratos de personal y de servicios.

Control

9.2.2. Gestión de los derechos de acceso asignados a usuarios

En los términos de la presente política, se debe identificar y autenticar a cualquier usuario que, de manera local o remota, requiera utilizar los recursos del Departamento de Tecnología de la Información, para lo que se requiere contar con sistemas de seguridad que cumplan con las siguientes características:

- Debe estar activo para acceder a la plataforma, lo que significa que cada usuario tiene que identificarse y autenticarse antes de acceder a un recurso de tecnología por medio de un usuario y una contraseña.
- Una vez se han identificado y autenticado, los usuarios sólo podrán acceder a los recursos sobre los cuales están autorizados.
- Los eventos de ingreso y autenticación de usuarios serán registrados y monitoreados por el Departamento de Tecnología de la Información.

Control

9.2.3. Gestión de los derechos de acceso con privilegios especiales

En los diferentes ambientes de procesamiento, existen cuentas de usuarios con las cuales es posible efectuar actividades críticas, como por ejemplo, instalación de plataformas o sistemas, habilitación de servicios, actualización de software, configuración de componentes informáticos, entre otros. Dichas cuentas no serán de uso habitual (diario), sino que solo serán utilizadas ante la necesidad específica de realizar alguna tarea que lo requiera y se encontrarán protegidas por contraseñas con un mayor nivel de complejidad que el habitual. El Responsable de Seguridad de la Información definirá procedimientos para la administración de dichas contraseñas críticas, que contemplen lo siguiente:

a) Se definirán las causas que justificarán el uso de contraseñas críticas, así como el nivel de autorización requerido.
b) Las contraseñas seleccionadas serán seguras, y su definición será efectuada, como mínimo, por dos personas, de manera que ninguna de ellas conozca la contraseña completa.
c) Las contraseñas y los nombres de las cuentas críticas a las que pertenecen serán resguardadas debidamente.
d) La utilización de las contraseñas críticas será registrada, documentando las causas que determinaron su uso, así como el responsable de las actividades que se efectúen con ellas.
e) Cada contraseña crítica se renovará una vez utilizada, y se definirá un período luego del cual esta será renovada, en caso de que no se la haya utilizado.

f) Se registrarán todas las actividades que se efectúen con las cuentas críticas para luego ser revisadas. Dicho registro será revisado posteriormente por el Responsable de Seguridad de la Información.

Control

9.2.4. Gestión de contraseñas de usuarios

En la asignación de contraseñas 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. Esta declaración estará incluida en el Compromiso de Confidencialidad.
b) Garantizar que los usuarios cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al sistema. Las contraseñas provisorias, que se asignan cuando los usuarios olvidan su contraseña, sólo debe suministrarse una vez identificado el usuario.
c) Generar contraseñas provisorias seguras para otorgar a los usuarios. Se debe evitar la participación de terceros o el uso de mensajes de correo electrónico sin protección (texto claro) en el mecanismo de entrega de la contraseña, y los usuarios deberán dar acuse de recibo cuando la reciban.
d) Almacenar las contraseñas solo en sistemas informáticos protegidos.
e) Utilizar otras tecnologías de autenticación y autorización de usuarios, como por ejemplo, la biométrica (verificación de huellas dactilares), verificación de firma, uso de autenticadores de hardware (como las tarjetas de circuito integrado). El uso de esas herramientas se dispondrá cuando la evaluación de riesgos realizada por el Responsable de Seguridad de la Información, conjuntamente con el Departamento de Tecnología de la Información y el Propietario de la Información, lo determinen necesario (o lo justifiquen).
f) Configurar los sistemas de tal manera que:

- las contraseñas tengan 8 caracteres alfanuméricos, como mínimo, y se consideren fuertes;
- suspendan o bloqueen permanentemente al usuario luego de 3 intentos para acceder al sistema con una contraseña incorrecta (deberá pedir la rehabilitación ante quien corresponda);
- soliciten el cambio de la contraseña cada 90 días;
- impidan que las últimas 6 contraseñas sean reutilizadas;
- establezcan un tiempo de vida mínimo de 7 días para las contraseñas.

Control

9.2.5. Revisión de los derechos de acceso de los 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 no mayores a 6 meses, 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.
b) Revisar las autorizaciones de privilegios especiales, de derechos de acceso a intervalos no mayores a 3 meses.
c) Revisar las asignaciones de privilegios, a fin de garantizar que no se obtengan privilegios no autorizados.

Control

9.2.6. Eliminación o ajuste de los derechos de acceso

El Responsable de Seguridad de la Información junto con el Departamento de Tecnología de la Información revisarán los derechos de acceso de un individuo a los activos asociados con los sistemas y servicios de información tras la desvinculación. Esto determinará si es necesario remover los derechos de acceso.

Producto de un cambio de funciones o un cese del vínculo entre el empleado y el Organismo, deben removerse todos los derechos de acceso que no fueron aprobados para la nueva función, comprendiendo esto accesos lógicos y físicos, llaves, tarjetas de identificación, instalaciones de procesamiento de la información, suscripciones, y remoción de cualquier documentación que lo identifique como un miembro corriente del Organismo.

Si un empleado, contratista o usuario de tercera parte que se está desvinculando tiene conocimiento de contraseñas para cuentas que permanecen activas, éstas deben ser cambiadas tras la finalización o cambio de empleo, contrato o acuerdo.

Se evaluará la reducción o eliminación de los derechos de acceso a los activos de la información y a las instalaciones de procesamiento de la información antes de que el empleo termine o cambie, dependiendo de factores de riesgos, tales como:

a) Si la terminación o cambio es iniciado por el empleado, contratista o usuario de tercera parte, o por la gestión y la razón de la finalización.
b) Las responsabilidades actuales del empleado, contratista o cualquier otro usuario.
c) El valor de los activos accesibles actualmente.

9.3. Responsabilidades del Usuario

Objetivo

El usuario deberá realizar todas las medidas a su alcance para: evitar el acceso de usuarios no-autorizados, evitar poner en peligro la información y evitar el robo de información y los medios de procesamiento de la información.

La cooperación de los usuarios autorizados es esencial para una seguridad efectiva.

Los usuarios deben estar al tanto de sus responsabilidades para mantener controles de acceso efectivos, particularmente con relación al uso de claves secretas y la seguridad del equipo del usuario.

Se debe implementar una política de escritorio y pantalla limpios para reducir el riesgo de acceso no autorizado o daño a los papeles, medios y medios de procesamiento de la información.

Control

9.3.1. Uso de información secreta de autenticación

Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas, que constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.

Los usuarios deben cumplir las siguientes directivas:

a) Mantener las contraseñas en secreto.
b) Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
c) Seleccionar contraseñas de calidad, de acuerdo a las prescripciones informadas por el Responsable del Activo de Información de que se trate, que:
    1. Sean fáciles de recordar.
    2. No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, como, por ejemplo, nombres, números de teléfono, fecha de nacimiento, etc.
    3. No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.
d) Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.
e) Cambiar las contraseñas provisorias en el primer inicio de sesión ("log on").

f) Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.
g) Notificar de acuerdo a lo establecido en la cláusula 16 "Gestión de Incidentes de Seguridad de la Información", cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

Si los usuarios necesitan acceder a múltiples servicios o plataformas y se requiere que mantengan múltiples contraseñas, se notificará a los mismos que pueden utilizar una única contraseña para todos los servicios que brinden un nivel adecuado de protección de las contraseñas almacenadas y en tránsito.

9.4. Control de Acceso a Sistemas y Aplicaciones

Objetivo

Evitar el acceso no autorizado a los servicios de la red.

Se debe controlar el acceso a los servicios de redes internas y externas.

El acceso del usuario a las redes y servicios de las redes no deben comprometer la seguridad de los servicios de la red asegurando:

a) que existan las interfaces apropiadas entre la red del Organismo y las redes de otras organizaciones, y redes públicas;
b) se apliquen los mecanismos de autenticación apropiados para los usuarios y el equipo;
c) el control del acceso del usuario a la información sea obligatorio.

Control

9.4.1. Restricción de acceso a la información

Los usuarios de sistemas de aplicación, con inclusión del personal de soporte, tendrán acceso a la información y a las funciones de los sistemas de aplicación, de conformidad con la presente Política en materia de control de accesos.

Se aplicarán los siguientes controles, para brindar apoyo a los requerimientos de limitación de accesos:

a) Proveer una interfaz para controlar el acceso a las funciones de los sistemas de aplicación. El Propietario de la Información involucrada será responsable de la adjudicación de accesos a las funciones. En el caso de que las actividades involucradas en el otorgamiento de acceso revistan un carácter técnico elevado, serán llevadas a cabo por personal del Departamento de Tecnología

de la Información, conforme a una autorización formal emitida por el Propietario de la Información.

b) Restringir el conocimiento de los usuarios acerca de la información o de las funciones de los sistemas de aplicación a los que no sean autorizados a acceder, con la adecuada edición de la documentación de usuario.
c) Controlar los derechos de acceso de los usuarios, por ejemplo, lectura, escritura, supresión y ejecución.
d) Garantizar que las salidas de los sistemas de aplicación que administran información crítica, contengan solo la información que resulte pertinente para el uso de la salida y que ella se envíe solamente a las terminales y ubicaciones autorizadas.
e) Revisar periódicamente dichas salidas a fin de garantizar la remoción de la información redundante.
f) Restringir el acceso a la información por fuera del sistema encargado de su procesamiento, es decir, la modificación directa del dato almacenado.

Control

9.4.2. Procedimientos de inicio de sesión seguro

El Responsable de Seguridad de la Información, junto con el Departamento de Tecnología de la Información, realizarán una evaluación de riesgos a fin de determinar el método de protección adecuado para el acceso al Sistema Operativo.

Si del análisis realizado surgiera la necesidad de proveer un método de identificación de terminales, se redactará un procedimiento que indique:

a) El método de identificación automática de terminales utilizado.
b) El detalle de transacciones permitidas por cada terminal.

El acceso a los servicios de información solo 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 o aplicaciones, hasta tanto se haya llevado a cabo exitosamente el proceso de conexión.
b) Desplegar un aviso general advirtiendo que solo 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.

d) Validar la información de la conexión solo al completarse la totalidad de los datos de entrada.
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) El registro de conexiones deberá tener:

   - Fecha y hora de la conexión.
   - Detalles de los intentos de conexión no exitosos desde la última conexión exitosa.

En caso de corresponder, el Responsable de Seguridad de la Información, junto con los Propietarios de la Información de que se trate, definirán cuáles se consideran terminales de alto riesgo, por ejemplo, áreas públicas o externas fuera del alcance de la gestión de seguridad del Organismo, o que sirven a sistemas de alto riesgo. Ellas se apagarán después de un período definido de inactividad, tiempo muerto, para evitar el acceso de personas no autorizadas. Esta herramienta de desconexión por tiempo muerto deberá limpiar la pantalla de la terminal y deberá cerrar tanto la sesión de la aplicación como la de red. El lapso por tiempo muerto responderá a los riesgos de seguridad del área y de la información que maneje la terminal.

Para las PC, se implementará la desconexión por tiempo muerto, que limpie la pantalla y evite el acceso no autorizado, pero que no cierra las sesiones de aplicación o de red.

Por otro lado, si un usuario debe abandonar su puesto de trabajo momentáneamente, activará protectores de pantalla con contraseñas, a los efectos de evitar que terceros puedan ver su trabajo o continuar con la sesión de usuario habilitada.

En caso de considerarlo necesario, el Responsable de la Unidad Organizativa de que se trate podrá solicitar al Responsable de Seguridad de la Información la implementación de excepciones de restricción a los horarios de conexión sobre la base de lo dispuesto por el ENARGAS para la jornada laboral.

En estos casos, la limitación del período durante el cual se permiten las conexiones de terminales a los servicios informáticos reduce el espectro de oportunidades para el acceso no autorizado.

Entre los controles que se deben aplicar para el caso previsto en los párrafos precedentes, se enuncian:

a) Utilizar lapsos predeterminados, por ejemplo, para transmisiones de archivos en lote, o sesiones interactivas periódicas de corta duración.
b) Documentar debidamente los agentes que tienen restricciones horarias y las razones de la restricción. También cuando el Propietario de la Información le autorice excepciones para una extensión horaria ocasional.

Control

9.4.3. Sistema de gestión 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:

a) Imponer el uso de contraseñas individuales para determinar responsabilidades.
b) Permitir que los usuarios seleccionen y cambien sus propias contraseñas (luego de cumplido el plazo mínimo de mantenimiento de estas) e incluir un procedimiento de confirmación para contemplar los errores de ingreso.
c) Imponer una selección de contraseñas de calidad, según lo señalado en el punto "Uso de Contraseñas".
d) Imponer cambios en las contraseñas en aquellos casos en que los usuarios mantengan sus propias contraseñas, según lo señalado en el punto 9.2.4 "Gestión de información confidencial de autenticación de usuarios".
e) Obligar a los usuarios a cambiar las contraseñas provisorias en su primer procedimiento de identificación, en los casos en que ellos seleccionen sus contraseñas.
f) Mantener un registro de las últimas contraseñas utilizadas por el usuario y evitar su reutilización.
g) Evitar mostrar las contraseñas en pantalla cuando son ingresadas.
h) Almacenar en forma separada los archivos de contraseñas y los datos de sistemas de aplicación.
i) Almacenar las contraseñas en forma cifrada utilizando un algoritmo de cifrado unidireccional.
j) Modificar todas las contraseñas predeterminadas por el vendedor una vez instalado el software y el hardware (por ejemplo, claves de impresoras, hubs, routers, switches, etc.).
k) 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.

Control

9.4.4. Uso de herramientas de administración de sistemas

La mayoría de las instalaciones informáticas tienen uno o más programas utilitarios que podrían tener la capacidad de pasar por alto los controles de sistemas y aplicaciones. Es esencial que su uso sea limitado y minuciosamente controlado. Se deben considerar los siguientes controles:

a) Utilizar procedimientos de autenticación para utilitarios del sistema.
b) Separar entre utilitarios del sistema y software de aplicaciones.
c) Limitar el uso de utilitarios del sistema a la cantidad mínima viable de usuarios fiables y autorizados.
d) Evitar que personas ajenas al Organismo tomen conocimiento de la existencia y el modo de uso de los utilitarios instalados en las instalaciones informáticas.
e) Establecer autorizaciones para uso ad hoc de utilitarios de sistema.
f) Limitar la disponibilidad de utilitarios de sistema, por ejemplo, durante el transcurso de un cambio autorizado.
g) Registrar todo uso de utilitarios del sistema.
h) Definir y documentar los niveles de autorización para utilitarios del sistema.
i) Remover todo el software basado en utilitarios y software de sistema innecesarios.

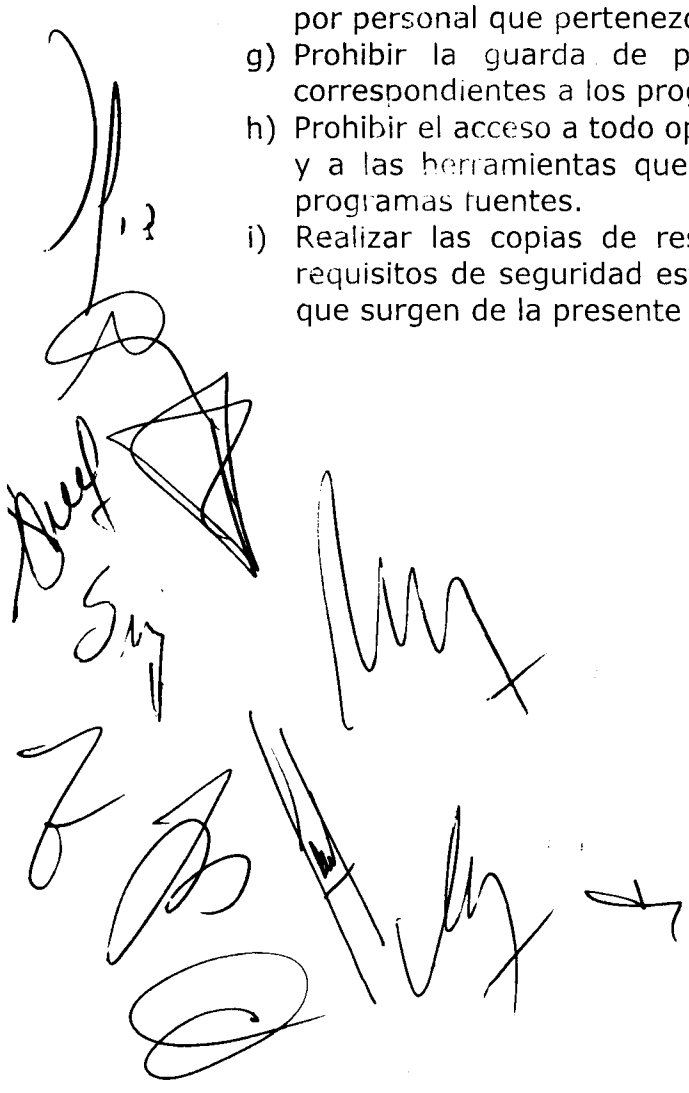
Control

9.4.5. Control de acceso al código fuente de los programas

Para reducir la probabilidad de alteración de programas fuentes, se aplicarán los siguientes controles:

a) El Responsable del Departamento de Tecnología de la Información, propondrá para su aprobación por parte del superior jerárquico que corresponda la función de "administrador de programas fuentes" al personal de su departamento que considere adecuado, quien tendrá en custodia los programas fuentes y debe:
   - Proveer al Área de Aplicaciones del Departamento de Tecnología de la Información los programas fuentes solicitados para su modificación, manteniendo en todo momento la correlación programa fuente / ejecutable.
   - Llevar un registro actualizado de todos los programas fuentes en uso, indicando nombre del programa, programador, Analista Responsable que autorizó, versión, fecha de última modificación y fecha / hora de compilación y estado (en modificación, en producción).
   - Verificar que el Analista Responsable que autoriza la solicitud de un programa fuente sea el designado para la aplicación, rechazando el pedido en caso contrario. Registrar cada solicitud aprobada.
   - Administrar las distintas versiones de una aplicación.
   - Asegurar que un mismo programa fuente no sea modificado simultáneamente por más de un desarrollador.

b) Denegar al "administrador de programas fuentes" permisos de modificación sobre los programas fuentes bajo su custodia.
c) Establecer que todo programa en producción tenga un único programa fuente asociado que garantice su origen.
d) Establecer que el implementador de producción efectuará la generación del programa objeto o ejecutable que estará en producción (compilación), a fin de garantizar tal correspondencia.
e) Desarrollar un procedimiento que garantice que toda vez que se migre a producción el módulo fuente, se cree el código ejecutable correspondiente en forma automática.
f) Evitar que la función de "administrador de programas fuentes" sea ejercida por personal que pertenezca al sector de desarrollo y/o mantenimiento.
g) Prohibir la guarda de programas fuentes históricos (que no sean los correspondientes a los programas operativos) en el ambiente de producción.
h) Prohibir el acceso a todo operador y/o usuario de aplicaciones a los ambientes y a las herramientas que permitan la generación y/o manipulación de los programas fuentes.
i) Realizar las copias de respaldo de los programas fuentes cumpliendo los requisitos de seguridad establecidos por el Organismo en los procedimientos que surgen de la presente política.



10. CIFRADO

Generalidades

La criptografía se usa en forma primaria para proteger la información del riesgo de seguridad que la misma pueda ser interceptada por cualquier persona no autorizada.

Esto reduce la probabilidad de que partes no autorizadas puedan tener acceso a la información.

Se debe tener cuidado con los sistemas de encriptación que no protegen a toda la información para asegurar que aquella información clasificada como confidencial.

Objetivos

Garantizar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, no-repudio, la autenticidad y/o la integridad de la información.

Alcance

Esta Política se aplica a todos los sistemas informáticos, tanto a desarrollos propios o de terceros, y a todos los Sistemas Operativos y/o Software de Base que integren cualquiera de los ambientes administrados por el Organismo en donde residan los desarrollos mencionados.

Responsabilidad

El Responsable de Seguridad de la Información, junto con el Propietario de la Información, definirá en función a la criticidad de la información, los requerimientos de protección necesarios. Luego, el Responsable de Seguridad de la información definirá junto con el Departamento de Tecnología de la Información, los métodos de encriptación a ser utilizados.

Asimismo, el Responsable de Seguridad de la Información cumplirá las siguientes funciones:

- Definir los procedimientos de administración de claves.
- Verificar el cumplimiento de los controles establecidos para el desarrollo y mantenimiento de sistemas.
- Garantizar el cumplimiento de los requerimientos de seguridad para el software.

- Definir procedimientos para: el control de cambios a los sistemas; la verificación de la seguridad de las plataformas y bases de datos que soportan e interactúan con los sistemas; el control de código malicioso; y la definición de las funciones del personal involucrado en el proceso de entrada de datos.

Política

10.1. Controles criptográficos

Objetivo

Se utilizarán sistemas y técnicas criptográficas para la protección de la información en base a un análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad.

Control

10.1.1. 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 del Organismo.
   3. Para el resguardo de información, cuando así surja de la evaluación de riesgos realizada por el Propietario de la Información y el Responsable de Seguridad de la Información.

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 Departamento de Tecnología de la implementará la política de controles criptográficos y asignará la administración de claves.

Control

10.1.2. Administración de claves

Se implementará un sistema de administración de claves criptográficas para respaldar la utilización, por parte del Organismo, de los dos tipos de técnicas criptográficas, a saber:

a) Técnicas de clave secreta (criptografía simétrica), cuando dos o más actores comparten la misma clave y esta se utiliza tanto para cifrar información como para descifrarla.

b) Técnicas de clave pública (criptografía asimétrica), cuando cada usuario tiene un par de claves: una clave pública (que puede ser revelada a cualquier persona) utilizada para cifrar y una clave privada (que debe mantenerse en secreto) utilizada para descifrar. Las claves asimétricas utilizadas para cifrado no deben ser las mismas claves que se utilizan para firmar digitalmente.

Todas las claves serán protegidas contra modificación y destrucción, y las claves secretas y privadas serán protegidas contra copia o divulgación no autorizada.

Se proporcionará una protección adecuada al equipamiento utilizado para generar, almacenar y archivar claves, considerándolo crítico o de alto riesgo.

Control

10.1.3. Firma Digital

La utilización de firmas y certificados digitales, se enmarcará en los parámetros establecidos por la legislación vigente (Ley N° 25.506, el Decreto N° 2628/02, complementarias y modificatorias).

La Gerencia de Asuntos Legales deberá brindar asesoramiento en materia del marco normativo aplicable en aquellos casos en los que resulte necesario establecer acuerdos para respaldar el uso de firmas digitales.

11. 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 para tener en cuenta: la protección física de accesos, la protección ambiental y el transporte, la protección y el mantenimiento de equipos y activos de información.

El establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles tendientes a proteger las instalaciones de procesamiento de información crítica 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 del servicio, así como la perfecta conservación de cualquier medio de información. Deben contemplarse tanto los riesgos en las instalaciones del Organismo como las próximas a este.

Los equipos donde se almacena información pueden requerir mantenimiento periódico, lo que puede generar su traslado y permanencia fuera de las áreas protegidas del Organismo.

Dichos procesos deben ejecutarse cumpliendo procedimientos que aseguren la integridad y confidencialidad de los activos, ya sea físicos, de software o de información.

Asimismo, se tendrá en cuenta la aplicación de procedimientos equivalentes para los activos físicos del Organismo situados fuera de este ("housing") y equipos de terceras partes que contengan activos de software o de información del Organismo ("hosting").

La información almacenada en los sistemas de procesamiento y la documentación contenida en diferentes medios de almacenamiento son susceptibles de ser recuperadas mientras no están siendo utilizadas. Es por eso que el transporte y la disposición final presentan riesgos que deben ser evaluados.

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, independientemente de su ubicación física.

Objetivos

Prevenir e impedir accesos no autorizados, daños e interferencias a las instalaciones o activos físicos, de software y de 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 que alberga la información del Organismo.

Asegurar protección proporcional a los riesgos identificados.

Alcance

Se aplica a todos los activos del Organismo definidos en la Política.

Responsabilidad

El Responsable de Seguridad de la Información junto con el Departamento de Tecnología de la Información y los Propietarios de la Información, según corresponda, definirán las medidas de seguridad a aplicar para cumplir con el objetivo establecido para los activos de Información, según los niveles de criticidad establecidos.

Asimismo, el Responsable de Seguridad de la Información controlará la implementación de las medidas de seguridad establecidas y verificará el cumplimiento de las disposiciones que se definan.

El Departamento de Tecnología de la Información controlará el mantenimiento de los activos físicos que contienen información digitalizada, de acuerdo con las indicaciones de proveedores, tanto dentro como fuera de las instalaciones del Organismo.

Los Responsables de las Unidades Organizativas definirán los niveles de acceso físico del personal del Organismo a las áreas restringidas bajo su responsabilidad.

Los Propietarios de la Información autorizarán formalmente el trabajo fuera de las instalaciones con información de su incumbencia a los empleados del Organismo, cuando lo crean conveniente.

El Responsable de Seguridad de la Información será el encargado de revisar los registros de acceso a las áreas protegidas.

Todo el personal del Organismo es responsable del cumplimiento de la política de pantallas y escritorios limpios, para la protección de la información relativa al trabajo diario en las oficinas.

Política

11.1. Áreas seguras

Objetivo

Evitar el acceso físico no autorizado al Organismo y daños e interferencia con la información del mismo.

Los medios de procesamiento de información crítica o confidencial deben ubicarse en áreas seguras, protegidas por los perímetros de seguridad definidos, con las barreras de seguridad y controles de entrada apropiados. Deben estar físicamente protegidos del acceso no autorizado, daño e interferencia.

Control

11.1.1. Perímetro de seguridad física

En caso de corresponder, se crearán barreras físicas sobre los perímetros de seguridad que limiten el acceso del personal no autorizado a las áreas contenedoras de activos físicos afectados al funcionamiento, almacenamiento o procesamiento de información.

Los responsables de las Unidades Organizativas deberán identificar y clasificar las áreas que se consideren críticas para el correcto funcionamiento, almacenamiento y procesamiento de los activos de información.

Se tomará en cuenta:

a) Definir y documentar claramente los perímetros de seguridad para cada área.
b) Las instalaciones de procesamiento de información deben estar dentro de un área de construcción físicamente sólida, todas las puertas que comunican con el exterior deben estar adecuadamente protegidas contra accesos no autorizados y no deben existir otro tipo de aberturas.
c) Los activos físicos afectados al funcionamiento, almacenamiento o procesamiento de activos de información deberán estar ubicados en áreas clasificadas como seguras ante cualquier contingencia.

d) Verificar la existencia de un área de recepción atendida por personal.-El acceso a dichas áreas y edificios estará restringido exclusivamente al personal autorizado. Los métodos implementados registrarán cada ingreso y egreso en forma precisa.
e) Extender las barreras físicas desde el piso (real) hasta el techo (real), a fin de impedir el ingreso no autorizado y la contaminación ambiental.
f) Identificar claramente todas las puertas de salida de emergencia y los elementos contra incendios y de seguridad.

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

a) Identificación del Edificio y Áreas Seguras.
b) Principales elementos a proteger.
c) Medidas de protección física.

Control

11.1.2. Controles de acceso físico

Todo ingreso y egreso de personas a las áreas protegidas será registrado por un sistema en el cual conste la fecha y hora del evento, e identificación de la persona.

Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por el Responsable de Seguridad de la Información junto con el Departamento de Tecnología de la Información, a fin de permitir el acceso solo al personal autorizado.

Cualquier persona que no esté autorizada para ingresar a un área protegida, deberá ser obligatoriamente acompañada permanentemente por personal autorizado.

Controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas. Se mantendrá un registro protegido para permitir auditar todos los accesos.

Revisar y actualizar cada 6 meses los derechos de acceso a las áreas protegidas, los que serán documentados y firmados, en caso de existir modificaciones a los existentes, por el Responsable de la Unidad Organizativa de la que dependa.

El Responsable de Seguridad de la Información deberá revisar los registros de acceso a las áreas protegidas.

Control

11.1.3. Seguridad de oficinas, despachos, 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 a la seguridad que representan los edificios y zonas aledañas, por ejemplo, filtración de agua desde otras instalaciones.

Se definen los siguientes sitios como áreas protegidas del Organismo, los cuales podrán ser modificados y/o ampliados, especificando los fundamentos, por el Comité de Seguridad, con el refrendo del Directorio.

Áreas Protegidas Mínimas [2]
Centros de Datos
Centrales Telefónicas
Depósitos del Departamento de Tecnología de la Información
Archivo
Biblioteca
Cajas fuertes

Se establecen las siguientes medidas de protección para áreas protegidas:

a) Establecer que las áreas donde se realicen actividades de procesamiento de información serán discretas y ofrecerán un señalamiento mínimo de su propósito.
b) Establecer que las puertas y ventanas permanecerán cerradas cuando no haya vigilancia.
c) Implementar mecanismos de control, para la detección de intrusos, que serán instalados según los estándares profesionales y que deberán ser probados periódicamente.
d) Separar las instalaciones de procesamiento de información administradas por el Organismo, de aquellas administradas por terceros.
e) Restringir el acceso público a las guías telefónicas y listados de teléfonos internos que identifican las ubicaciones de las instalaciones de procesamiento de información sensible.
f) Almacenar los materiales peligrosos o combustibles en áreas seguras, a una distancia prudencial de las áreas protegidas del Organismo.
g) Almacenar los equipos redundantes y la información de resguardo (Back-Ups) en áreas seguras y distantes del lugar de procesamiento, para evitar daños ocasionados ante eventuales contingencias en el sitio principal.

Control

11.1.4. Protección contra amenazas externas y de origen ambiental

Se debe asignar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, revuelta civil y otras formas de desastres naturales o causados por el hombre.

Se debe prestar consideración a cualquier amenaza contra la seguridad presentada por locales vecinos; por ejemplo, un fuego en un edificio vecino, escape de agua en el techo o pisos en sótano o una explosión en la calle.

Se debe considerar los siguientes lineamientos para evitar el daño por fuego, inundación, terremoto, explosión, revuelta civil y otras formas de desastres naturales o causados por el hombre:

a) Los materiales peligrosos o combustibles deben ser almacenados a una distancia segura del área asegurada. Los suministros a granel como papelería no deben almacenarse en el área asegurada;
b) El equipo de reemplazo y los medios de respaldo debieran ubicarse a una distancia segura para evitar el daño de un desastre que afecte el local principal;
c) Se debe proporcionar equipo contra-incendios ubicado adecuadamente.

Control

11.1.5. Trabajo en áreas seguras

Para incrementar la seguridad de las áreas protegidas, se establecerán 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, solo si es necesario para el desarrollo de sus funciones.
b) 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 será otorgado solamente cuando sea necesario y se encuentre autorizado, y monitoreado. Se mantendrá un registro de todos los accesos de personas ajenas y operaciones realizadas.
c) Dentro de las áreas incluidas en el punto 11.1.3., en el cuadro Áreas Protegidas Mínimas, queda prohibido realizar cualquier actividad diferente a la específica relacionada con esta.

Control

11.1.6. Áreas de acceso público, de carga y descarga

Se controlarán los depósitos, los cuales estarán aislados de las instalaciones de procesamiento de información, a fin de impedir accesos no autorizados.

Para ello se establecerán controles físicos que considerarán los siguientes lineamientos:

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) Proteger todas las puertas exteriores del depósito cuando se abre la puerta interna.
c) Inspeccionar el material entrante para descartar peligros potenciales antes de ser trasladado desde el área de depósito hasta el lugar de uso.
d) Registrar el material entrante al ingresar al sitio pertinente.
e) Cuando fuese posible, el material entrante debe estar segregado o separado en sus diferentes partes que lo constituyan.

11.2. Seguridad de los equipos

Objetivo

Evitar pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades del Organismo.

Se debe proteger el equipo de amenazas físicas y ambientales.

11.2.1. Emplazamiento y protección de equipos

El equipamiento será ubicado y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado, teniendo en cuenta los siguientes puntos:

a) Ubicar el equipamiento en un sitio donde se minimice el acceso innecesario y provea un control de acceso adecuado.
b) Ubicar las instalaciones de procesamiento y almacenamiento de información que manejan datos clasificados, en un sitio que permita la supervisión durante su uso.
c) Aislar los elementos que requieren protección especial para reducir el nivel general de protección requerida.
d) Adoptar controles adecuados para minimizar el riesgo de amenazas potenciales.

Se deben establecer lineamientos sobre las actividades de comer, beber y fumar en la proximidad de los medios de procesamiento de la información.

Revisar regularmente las condiciones ambientales para verificar que las mismas no afecten de manera adversa el funcionamiento de las instalaciones de procesamiento de la información.

Se deben aplicar protección contra rayos a todos los edificios y se deben adaptar filtros de protección contra rayos a todas las líneas de ingreso de energía y comunicaciones.

Control

11.2.2. Instalaciones de suministro

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 del Organismo. La determinación de dichas operaciones críticas, será el resultado del análisis de impacto realizado por el Responsable de Seguridad de la Información conjuntamente con los Propietarios de la Información con incumbencia. 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. Debe 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. Dicho análisis será realizado por el Responsable de Seguridad de la Información conjuntamente con los Propietarios de la Información y el responsable del generador de respaldo. Se dispondrá de un adecuado suministro de combustible para garantizar que el generador pueda funcionar por un período prolongado. Cuando el encendido de los generadores no sea automático, se asegurará que el tiempo de funcionamiento de la UPS permita el encendido manual de los mismos. Los generadores serán inspeccionados y probados periódicamente para asegurar que funcionen según lo previsto.

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.

Para evitar una falla en el suministro de energía una de las opciones comprende el tener múltiples fuentes de alimentación eléctrica.

Control

11.2.3. Seguridad del cableado

El cableado de energía eléctrica y de comunicaciones estará protegido contra interceptación o daño, mediante las siguientes acciones:

a) Cumplir con los requisitos técnicos vigentes de la República Argentina.
b) Utilizar conductos embutidos siempre que sea posible.
c) Emplear conductos independientes para separar el cableado eléctrico del cableado de comunicaciones, para evitar interferencias.
d) Acceso controlado a los módulos y cuartos de cableado. Proteger el tendido del cableado troncal (vertical) mediante la utilización de ductos blindados.
e) Inspecciones físicas en busca de dispositivos no autorizados conectados al cableado.
f) Utilizar rotulado de equipos y de cables claramente identificables.

Para los sistemas críticos se contemplará disponer de medios de transmisión duplicados y, de ser posible, por una ruta o un medio diferente.

Para reducir errores, se deberá tener un plano actualizado del cableado y puestos identificados por piso.

Control

11.2.4. Mantenimiento de los equipos

Se realizará el mantenimiento de los equipos informáticos para asegurar su disponibilidad e integridad permanentes. Para ello se debe considerar:

a) El Departamento de Tecnología de la Información mantendrá un listado actualizado del parque informático con el detalle de la frecuencia en que se realizará el mantenimiento preventivo, de acuerdo con los intervalos de servicio y las especificaciones recomendados por el proveedor.

b) Se establecerá que solo el personal calificado y autorizado puede brindar mantenimiento y llevar a cabo reparaciones o modificaciones en los equipos.
c) Se registrarán todas las anomalías, los mantenimientos preventivos y las acciones correctivas que se realicen en los equipos.
d) Se registrará todo movimiento de los equipos informáticos, de la Sede Central del Organismo, Edificio Anexo y Centros Regionales, para su mantenimiento.
e) Se eliminará la información confidencial que contenga cualquier equipo informático que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.

Control

11.2.5. Salida de activos fuera de las instalaciones del Organismo

Los activos no serán retirados de los edificios del Organismo sin una autorización formal.

De acuerdo con el tipo de activo, se puede requerir la autorización de varios responsables.

- Activos de Información: El Responsable de la Unidad Organizativa será el encargado de la autorización.
- Activos de Software: El Responsable de la Unidad Organizativa con el Responsable del Departamento de Tecnología de la Información serán los encargados de la autorización.
- Activos Físicos: El Responsable de la Unidad Organizativa con el Responsable de la Gerencia de Administración serán los encargados de la autorización.

Periódicamente, se llevarán a cabo comprobaciones puntuales para detectar el retiro no autorizado de Activos de Información del Organismo, las que serán llevadas a cabo por la Unidad de Auditoría Interna. El personal será puesto en conocimiento de la posibilidad de realización de dichas comprobaciones.

Control

11.2.6. Seguridad de los equipos fuera de las instalaciones

El uso de equipos destinados al procesamiento de información fuera del Organismo será autorizado por el responsable de la Unidad Organizativa. En el caso de que almacenen información clasificada, deberá ser aprobado, además, por el Propietario de la misma.

La seguridad provista fuera del Organismo debe ser equivalente a la suministrada dentro de su ámbito para un propósito similar, teniendo en cuenta los riesgos de trabajar fuera de él.

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

Control

11.2.7. Reutilización o retiro seguro de equipos

La información puede verse comprometida por una desafectación o una reutilización descuidada del equipo. Los medios de almacenamiento que contienen material crítico, como discos rígidos no removibles, serán físicamente destruidos o sobrescritos de forma segura, en lugar de utilizar las funciones de borrado estándar, según corresponda.

Control

11.2.8. Equipo Informático de usuario desatendido

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 de la Información debe coordinar con la Gerencia de Recursos Humanos y Relaciones Institucionales las tareas de concientización a todos los usuarios charlas de capacitación, acerca de los requerimientos y procedimientos de seguridad, para la protección de equipos desatendidos, así como de sus funciones en relación con la implementación de dicha protección.

Control

11.2.9. Políticas de pantalla y escritorio limpio

Se adopta una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles, y una política de pantallas limpias, en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera de este.

Se aplicarán los siguientes lineamientos:

a) Almacenar con el debido resguardo y cuando corresponda, los documentos en papel y los medios informáticos, en gabinetes u otro tipo de mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.

b) Guardar bajo llave la información crítica del Organismo (preferentemente en una caja fuerte o gabinete a prueba de incendios) cuando no está en uso, especialmente cuando no hay personal en la oficina.
c) Proteger los puntos de recepción y envío de correo postal, y las máquinas de fax no atendidas.
Retirar inmediatamente la información confidencial una vez impresa o fotocopiada.

12. SEGURIDAD EN LAS OPERACIONES

Generalidades

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.

Es conveniente separar los ambientes de desarrollo, prueba y operaciones de los sistemas del Organismo, estableciendo procedimientos que aseguren la calidad de los procesos que se implementen en el ámbito operativo, a fin de minimizar los riesgos de incidentes producidos por la manipulación de información operativa.

Objetivo

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

Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas, procedimientos para la respuesta a incidentes y separación de funciones.

Alcance

Todas las instalaciones de procesamiento de información del Organismo.

Responsabilidad

El Responsable de Seguridad de la Información tendrá a su cargo, entre otros:

- Definir procedimientos para el control de cambios a los procesos operativos documentados, los sistemas e instalaciones de procesamiento de información, y verificar su cumplimiento, de manera que no afecten la seguridad de la información.
- Establecer criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, contemplando la realización de las pruebas necesarias antes de su aprobación definitiva. Verificar que dichos procedimientos de aprobación de software incluyan aspectos de seguridad para todas las aplicaciones.
- Definir procedimientos para el manejo de incidentes de seguridad y para la administración de los medios de almacenamiento.
- Definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso y para garantizar la seguridad de los datos y los servicios conectados en las redes del Organismo.

- Desarrollar procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.
- Verificar el cumplimiento de las normas, procedimientos y controles establecidos.

El Departamento de Tecnología de la Información tendrá a su cargo lo siguiente:

- Controlar la existencia de documentación actualizada relacionada con los procedimientos de operaciones.
- Evaluar el posible impacto operativo de los cambios previstos a sistemas y equipamiento y verificar su correcta implementación, asignando responsabilidades.
- Administrar los medios técnicos necesarios para permitir la segregación de los ambientes de procesamiento.
- Monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad, a fin de evitar potenciales amenazas a la seguridad del sistema o a los servicios del usuario.
- Controlar la realización de las copias de resguardo de información, así como la prueba periódica de su restauración.
- Asegurar el registro de las actividades realizadas por el personal operativo, para su posterior revisión.
- Implementar los controles de seguridad definidos (software malicioso y accesos no autorizados).
- Definir e implementar procedimientos para la administración de medios informáticos de almacenamiento, como cintas, discos, casetes e informes impresos y para la eliminación segura de los mismos.
- Participar en el tratamiento de los incidentes de seguridad, de acuerdo a los procedimientos establecidos.

Cada Propietario de la Información, junto con el Responsable de Seguridad de la Información y el Departamento de Tecnología de la Información, determinarán los requerimientos para resguardar la información por la cual es responsable, incluyendo, en los casos que corresponda, su modo de traslado de acuerdo a su nivel de criticidad.

Política

12.1. Responsabilidades y procedimientos operativos

Objetivo

Asegurar la operación correcta y segura de los medios de procesamiento de la información.

Se deben establecer las responsabilidades y procedimientos para la gestión y operación de todos los medios de procesamiento de la información. Esto incluye el desarrollo de los procedimientos de operación apropiados

Control

12.1.1. Documentación de los Procedimientos Operativos

Se documentarán y mantendrán actualizados los procedimientos operativos necesarios para cumplimentar esta Política. Dichos procedimientos y sus actualizaciones serán revisados anualmente por el Responsable de Seguridad de la Información.

Los procedimientos especificarán las instrucciones para la ejecución detallada de cada tarea, que incluye:

a) Procesamiento y manejo de la información.
b) Requerimientos de programación de procesos, interdependencias con otros sistemas, tiempos de inicio de las primeras tareas y tiempos de terminación de las últimas tareas.
c) Instrucciones para el manejo de errores u otras condiciones excepcionales que puedan surgir durante la ejecución de tareas.
d) Restricciones en el uso de utilitarios del sistema.
e) Personas de soporte para contactar en caso de dificultades operativas o técnicas imprevistas.
f) Reinicio del sistema y procedimientos de recuperación en caso de producirse fallas en el sistema.

Se preparará adicionalmente documentación sobre procedimientos referidos a las siguientes actividades:

a) Instalación y mantenimiento de equipamiento para el procesamiento de información y comunicaciones.
b) Instalación y mantenimiento de las plataformas de procesamiento.
c) Monitoreo del procesamiento y de las comunicaciones.
d) Inicio y finalización de la ejecución de los sistemas.
e) Programación y ejecución de procesos.
f) Gestión de servicios.
g) Resguardo de información.
h) Gestión de incidentes de seguridad en el ambiente de procesamiento y comunicaciones.
i) Reemplazo o cambio de componentes del ambiente de procesamiento y comunicaciones.
j) Uso del correo electrónico.

Control

12.1.2. Gestión de cambios

Se definirán procedimientos para el control de los cambios en el ambiente operativo y de comunicaciones. Todo cambio deberá ser evaluado previamente en aspectos técnicos y de seguridad.

El Responsable de Seguridad de la Información controlará que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de estos ni de la información que soportan. El Departamento de Tecnología de la Información evaluará el posible impacto operativo de los cambios previstos y verificará su correcta implementación.

Se retendrá un registro de auditoría que contenga toda la información relevante de cada cambio implementado.

Los procedimientos de control de cambios contemplarán los siguientes puntos:

a) Evaluación del posible impacto de dichos cambios.
b) Aprobación formal de los cambios propuestos.
c) Planificación del proceso de cambio.
d) Prueba del nuevo escenario.
e) Comunicación de detalles de cambios a todas las personas pertinentes.

Identificación de las responsabilidades por la cancelación de los cambios fallidos y la recuperación respecto de los mismos.

Control

12.1.3. Gestión de capacidades

El Responsable del Departamento de Tecnología de la Información o el personal que este designe, efectuará el monitoreo de las necesidades de capacidad de los sistemas en operación y proyectará las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuados. 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 para que puedan planificar una adecuada acción correctiva.

Control

12.1.4. Separación de entornos de desarrollo, prueba y producción

Los ambientes de desarrollo, prueba y producción, siempre que sea posible, estarán separados preferentemente en forma física, y se definirán y documentarán las reglas para la transferencia de software desde el estado de desarrollo hacia el estado operativo.

Para ello, se tendrán en cuenta los siguientes controles:

a) Ejecutar el software de desarrollo y de producción, en diferentes ambientes, equipos o directorios.
b) Separar las actividades de desarrollo y prueba en entornos diferentes.
c) Impedir el acceso a los compiladores, editores y otros utilitarios del sistema en el ambiente de producción cuando no sean indispensables para su funcionamiento.
d) Utilizar sistemas de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas. Prohibir a los usuarios compartir contraseñas en estos sistemas. Las interfaces de los sistemas identificarán claramente a qué instancia se está realizando la conexión.
e) Definir propietarios de la información para cada uno de los ambientes de procesamiento existentes.
f) El personal de desarrollo no tendrá acceso al ambiente de producción. De ser de extrema necesidad, se establecerá un procedimiento de emergencia para la autorización, la documentación y el registro de dichos accesos.

Para el caso de que no se puedan mantener separados los distintos ambientes en forma física, se deberán implementar los controles indicados en el punto 6.1.2 "Segregación de Funciones".

12.2. Protección contra el malware (código malicioso)

Objetivo

Proteger la integridad del software y la integración.

Se requiere tomar precauciones para evitar y detectar la introducción de códigos maliciosos y códigos móviles no-autorizados.

El software y los medios de procesamiento de la información son vulnerables a la introducción de códigos maliciosos; como ser, entre otros, virus Troyanos, bombas lógicas, etc. El Departamento de Tecnología de la Información capacitará a los usuarios para que estén al tanto de los peligros de los códigos maliciosos.

Control

12.2.1. Control contra el malware (código malicioso)

El Responsable de Seguridad de la Información definirá controles de detección y prevención para la protección contra software malicioso. El Responsable del Departamento de Tecnología de la Información o el personal designado por este, implementará dichos controles.

El Responsable de Seguridad de la Información, junto con el Departamento de Tecnología de la Información, desarrollarán procedimientos adecuados de concientización de usuarios en materia de seguridad y definirán las pautas y los criterios para el control de acceso a los sistemas de información y administración de cambios.

Estos controles deberán considerar las siguientes acciones:

a) Prohibir el uso de software no autorizado por el Organismo.
b) Redactar procedimientos para evitar los riesgos relacionados con la obtención de archivos y software desde redes externas o a través de ellas, o por cualquier otro medio, señalando las medidas de protección por tomar.
c) Instalar y actualizar periódicamente software de detección y reparación de virus, examinando computadoras y medios informáticos, como medida precautoria y rutinaria.
d) Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles (probar dichas actualizaciones en un entorno de prueba previamente, si es que constituyen cambios críticos a los sistemas).
e) Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos del Organismo, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.
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 o unidades extraíbles.
g) Redactar procedimientos para verificar toda la información relativa a software malicioso, garantizando que los boletines de alerta sean exactos e informativos.
h) Concientizar al personal acerca del problema de los falsos virus (hoax) y de cómo proceder frente a ellos.
i) Capacitar a los usuarios para que puedan identificar posibles eventos de riesgo que puedan afectar la información.

12.3. Copia de seguridad

Objetivo

Mantener la integridad y disponibilidad de la información y los medios de procesamiento de información.

Se deben establecer los procedimientos de rutina para implementar la política de respaldo acordada y la estrategia (ver también Cláusula 17.1 Categoría: Continuidad de la seguridad de la información) para tomar copias de respaldo de los datos y practicar su restauración oportuna.

Control

12.3.1. Copias de seguridad de la Información

El Departamento de Tecnología de la Información y el Responsable de Seguridad de la Información determinarán sobre la base de la criticidad de la información de que se trate, un esquema de resguardo.

El Departamento de Tecnología de la Información dispondrá y controlará la realización de dichas copias, así como la prueba periódica de su restauración. Para esto se deberá contar con instalaciones de resguardo que garanticen la disponibilidad de toda la información y del software crítico del Organismo. Los sistemas de resguardo deberán probarse periódicamente, asegurándose de que cumplen con los requerimientos de los planes de continuidad de las actividades del Organismo.

Se definirán procedimientos para el resguardo de la información, que deberán considerar los siguientes puntos:

a) Definir un esquema de rótulo de las copias de resguardo, que permita contar con toda la información necesaria para identificar cada una de ellas y administrarlas debidamente.
b) Establecer un esquema de reemplazo de los medios de almacenamiento de las copias de resguardo, una vez concluida la posibilidad de ser reutilizados, de acuerdo con lo indicado por el proveedor, y asegurar la destrucción de los medios desechados.
c) Almacenar en una ubicación remota copias recientes de información de resguardo, junto con sus registros exactos y completos, y los procedimientos documentados de restauración, a una distancia suficiente como para evitar daños provenientes de un desastre en el sitio principal. Se deberán retener, al menos, tres generaciones o ciclos de información de resguardo, para la información y el software esenciales para el Organismo. Para la definición de información mínima a ser resguardada en el sitio remoto, se deberá tener en

cuenta el nivel de clasificación otorgado a la misma, en términos de disponibilidad, y los requisitos legales a los que se encuentre sujeta.

d) Asignar a la información de resguardo un nivel de protección física y ambiental, según las normas aplicadas en el sitio principal. Extender los mismos controles aplicados a los dispositivos en el sitio principal al sitio de resguardo.
e) Probar periódicamente los medios de resguardo.
f) Verificar y probar periódicamente los procedimientos de restauración, garantizando su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos.

12.4. Registro y Monitoreo

Objetivo

Detectar las actividades de procesamiento de información no autorizadas.

Se deben monitorear los sistemas y se deben reportar los eventos de seguridad de la información. Se deben utilizar bitácoras de operador y se deben registrar las fallas para asegurar que se identifiquen los problemas en los sistemas de información. Se deben cumplir con todos los requerimientos legales relevantes aplicables a sus actividades de monitoreo y registro.

Se debe utilizar el monitoreo del sistema para chequear la efectividad de los controles adoptados y para verificar la conformidad con un modelo de política de acceso.

Control

12.4.1. Registro de eventos

Se producirán y mantendrán registros de auditoría en los cuales se registren las actividades, excepciones, y eventos de seguridad de la información de los usuarios, por un período acordado para permitir la detección e investigación de incidentes.

Se debe evaluar la registración, en los mencionados registros, de la siguiente información:

a) identificación de los usuarios;
b) fechas, tiempos, y detalles de los eventos principales, por ejemplo, inicio y cierre de sesión;
c) identidad del equipo o la ubicación si es posible;
d) registros de intentos de acceso al sistema exitosos y fallidos;
e) registros de intentos de acceso a los datos u otro recurso, exitosos y rechazados;

f) cambios a la configuración del sistema;
g) uso de privilegios;
h) uso de utilitarios y aplicaciones de sistemas;
i) archivos accedidos y el tipo de acceso;
j) direcciones de redes y protocolos;
k) alarmas que son ejecutadas por el sistema de control de accesos;
l) activación y desactivación de los sistemas de protección, tales como sistemas antivirus y sistemas de detección de intrusos.

Control

12.4.2. Protección de los registros de información

Se implementarán controles para la protección de los registros de auditoría contra cambios no autorizados y problemas operacionales, incluyendo:

a) alteraciones de los tipos de mensajes que son grabados;
b) edición o eliminación de archivos de registro;
c) exceso de la capacidad de almacenamiento de los archivos de registro, resultando en la falla para registrar los eventos o sobrescribiendo eventos registrados en el pasado.

Control

12.4.3. Registro de actividad del administrador y operador del sistema

Se registrarán y revisarán periódicamente en particular las actividades de los administradores y operadores de sistema incluyendo:

a) cuenta de administración u operación involucrada;
b) momento en el cual ocurre un evento (éxito o falla);
c) información acerca del evento (por ejemplo, los archivos manipulados) o las fallas (por ejemplo, los errores ocurridos y las acciones correctivas tomadas);
d) procesos involucrados.

Control

12.4.4. Sincronización de Relojes

A fin de garantizar la exactitud de los registros de auditoría, al menos los equipos que realicen estos registros, deben 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.

12.5. Control de Software Operacional

Objetivo

Garantizar la seguridad de los archivos del sistema.

Se debe controlar el acceso a los archivos del sistema y el código fuente del programa, y los proyectos TI. Asimismo, las actividades de soporte se debieran realizar de una manera segura.

Control

12.5.1. Instalación de software en sistemas en producción

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.

- Toda aplicación, desarrollada por el Organismo o por un tercero tendrá un único Responsable designado formalmente por el Responsable del Departamento de Tecnología de la Información.
- Ningún programador o analista de desarrollo y mantenimiento de aplicaciones podrá acceder a los ambientes de producción.
- El Responsable del Departamento de Tecnología de la Información, designará la función de "implementador" al personal de su área que considere adecuado, quien tendrá como funciones principales:
    a. Coordinar la implementación de modificaciones o nuevos programas en el ambiente de Producción.
    b. 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.
    c. 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.
    d. Rechazar la implementación en caso de encontrar defectos y/o si faltara la documentación estándar establecida.

Otros controles a realizar son:

a. Guardar sólo los ejecutables en el ambiente de producción.
b. Llevar un registro de auditoría de las actualizaciones realizadas.
c. Retener las versiones previas del sistema, como medida de contingencia.
d. Definir un procedimiento que establezca los pasos a seguir para implementar las autorizaciones y conformidades pertinentes, las pruebas previas a realizarse, etc.

e. Denegar, cuando correspondiere, permisos de modificación al implementador sobre los programas fuentes bajo su custodia.
f. Evitar, que la función de implementador sea ejercida por personal que pertenezca al sector de desarrollo o mantenimiento.

12.6. Administración de vulnerabilidades técnicas

Objetivo

Se implementará la gestión de las vulnerabilidades técnicas de forma efectiva, sistemática y repetible, con mediciones que confirmen su efectividad. Dichas consideraciones incluirán los sistemas operativos, y cualquier otra aplicación en uso.

Control

12.6.1. Gestión de vulnerabilidades técnicas

Se obtendrá información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, la exposición del Organismo a tales vulnerabilidades evaluadas, y se tomarán las medidas necesarias para tratar los riesgos asociados.

Para ello se contará con un inventario de software donde se detalle información de versiones del mismo, así como datos del proveedor y responsable interno.

El proceso de gestión de las vulnerabilidades técnicas debe comprender:

a) Definición de roles y responsabilidades asociados con la gestión de vulnerabilidades técnicas;
b) Procedimientos de identificación de vulnerabilidades técnicas potenciales;
c) Definición de una línea de tiempo para reaccionar ante las notificaciones de las vulnerabilidades técnicas potencialmente relevantes;
d) Definición de prioridades para la atención de necesidades relacionadas con actualizaciones de seguridad;
e) Identificación de los riesgos asociados y las acciones a llevar a cabo ante vulnerabilidades identificadas;
f) Identificación de los riesgos asociados a la instalación de parches;
g) Aprobación y evaluación de los parches antes de que sean instalados para garantizar que son efectivos y que no resultan en efectos secundarios que no puedan ser tolerados;
h) Consideración de controles alternativos en caso de inexistencia de parches;
i) Generación y mantenimiento de un registro de auditoría para todos los procedimientos emprendidos;
j) Seguimiento y evaluación regular del proceso de gestión de las vulnerabilidades técnicas para garantizar su efectividad y eficiencia.

Control

12.6.2. Restricciones en la instalación de software

Se deben establecer e implementar las reglas que rigen la instalación de software por parte de los usuarios y poner en vigencia una política estricta sobre qué tipo de software pueden instalar los usuarios.

La instalación no controlada de software en dispositivos computacionales puede dar pie a la introducción de vulnerabilidades y a la fuga de información, a la falta de integridad u otros incidentes de seguridad de información o bien a la transgresión de derechos de propiedad intelectual.

12.7. Consideraciones sobre la auditoría de los sistemas de información

Objetivo

Asegurar el cumplimiento de minimizar el impacto de las actividades de auditoría en los sistemas operacionales.

Control

12.7.1. Controles de auditoría de los sistemas de información

Cuando se realicen actividades de auditoría que involucren verificaciones de los sistemas en producción, se tomarán recaudos 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 la Unidad 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.
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.
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.

13. SEGURIDAD EN LAS TELECOMUNICACIONES

Generalidades

Los sistemas de información están comunicados entre sí, tanto dentro del Organismo como con terceros fuera de él. Por lo tanto, es necesario establecer criterios de seguridad en las comunicaciones que se establezcan.

Las comunicaciones establecidas permiten el intercambio de información, que debe estar regulado para garantizar las condiciones de confidencialidad, integridad y disponibilidad de la información que se emite o recibe por los distintos canales.

Objetivo

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

Alcance

Todas las instalaciones de procesamiento y transmisión de información del Organismo.

Responsabilidad

El Responsable de Seguridad de la información tendrá a su cargo, entre otros:

- Definir procedimientos con respecto al uso del correo electrónico.
- Desarrollar procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.
- Verificar el cumplimiento de las normas, procedimientos y controles establecidos.

El Departamento de Tecnología de la Información tendrá a su cargo lo siguiente:

- Controlar la existencia de documentación actualizada relacionada con los procedimientos de comunicaciones.
- Asegurar el registro de las actividades realizadas por el personal operativo, para su posterior revisión.
- Definir e implementar procedimientos para la administración de medios informáticos de almacenamiento, como cintas, discos, casetes e informes impresos y para la eliminación segura de los mismos.

El Responsable de Seguridad de la información junto con el Departamento de Tecnología de la Información y la Gerencia de Asuntos Legales del Organismo evaluarán los contratos y acuerdos con terceros para garantizar la incorporación de consideraciones relativas a la seguridad de la información involucrada en la gestión de los productos o servicios prestados.

Cada Propietario de la Información, junto con el Responsable de Seguridad de la Información y el Departamento de Tecnología de la Información, determinarán los requerimientos para resguardar la información por la cual es responsable.

Política

13.1. Gestión de la seguridad en las redes

Objetivo

Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.

La gestión segura de las redes, la cual puede abarcar los límites organizacionales, requiere de la cuidadosa consideración del flujo de datos, implicancias legales, monitoreo y protección.

También se pueden requerir controles adicionales para proteger la información confidencial que pasa a través de redes públicas.

Control

13.1.1. Controles de red

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

a) Establecer los procedimientos para la administración del equipamiento remoto, incluyendo los equipos en las áreas usuarias.
b) 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. Implementar controles especiales para mantener la disponibilidad de los servicios de red y computadoras conectadas.
c) Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información.

El Responsable del Departamento de Tecnología de la Información o quien este designe dentro de su personal a cargo, implementará dichos controles.

Control

13.1.2. Seguridad de los servicios de red

El Responsable de Seguridad de la Información junto con el Departamento de Tecnología de la Información definirán las pautas para garantizar la seguridad de los servicios de red del Organismo, tanto públicos como privados.

Para ello se tendrán en cuenta las siguientes directivas:

- 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.
- Dicha configuración será revisada periódicamente por el Responsable de Seguridad de la Información.

13.2. Transferencia de información

Objetivo

Mantener la seguridad en el intercambio de información dentro del Organismo y con cualquier otra entidad externa.

Se propenderá a proteger la información y los medios físicos que contiene la información en tránsito.

Control

13.2.1. Políticas y procedimientos para transferencia de información

Se establecerán procedimientos y controles formales para proteger el intercambio de información a través del uso de todos los tipos de instalaciones de comunicación, considerando lo siguiente:

a) Protección de la información intercambiada de la intercepción, copiado, modificación, de que sea mal dirigida, y de su destrucción.
b) detección y protección contra el código malicioso que puede ser transmitido a través del uso de comunicaciones electrónicas.

c) definición del uso aceptable de las instalaciones de comunicación electrónicas.
d) uso seguro de comunicaciones inalámbricas.
e) responsabilidades del empleado, contratista y cualquier otro usuario de no comprometer a la organización, por ejemplo, a través de la difamación, hostigamiento, personificación, reenvío de cadenas de comunicación epistolar, compras no autorizadas y cualquier otro medio (ej.: redes sociales).
f) uso de técnicas criptográficas para proteger la confidencialidad, integridad y la autenticidad de la información.
g) directrices de retención y eliminación para toda la correspondencia en concordancia con las leyes y regulaciones relevantes, locales y nacionales.
h) instrucción del personal sobre las precauciones que deben tomar a la hora de transmitir información del Organismo.

Control

13.2.2. Acuerdos sobre la transferencia de Información

Cuando se realicen acuerdos entre organizaciones para el intercambio de información digital y software, se especificarán el grado de sensibilidad de la información del Organismo 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, exposición o divulgación no autorizada de datos.
e) Uso de un sistema convenido para el rotulado de información clasificada, garantizando que el significado de los rótulos sea inmediatamente comprendido y que la información sea adecuadamente protegida.
f) Términos y condiciones de la licencia bajo la cual se suministra el software.
g) Información sobre la propiedad de la información suministrada y las condiciones de su uso.
h) Normas técnicas para la grabación y lectura de la información y del software.
i) Controles especiales que puedan requerirse para proteger ítems sensibles, (claves criptográficas, etc.).

Control

13.2.3. Seguridad de la mensajería electrónica

La mensajería electrónica como el correo electrónico, el intercambio de datos electrónicos (EDI por sus siglas en inglés), la mensajería instantánea y las redes sociales juegan un muy importante en las comunicaciones organizacionales. La

mensajería electrónica tiene diferentes riesgos que las comunicaciones basadas en papel.

Se considerarán las siguientes medidas de seguridad en los mensajes electrónicos:

- protección de mensajes por el acceso no autorizado, modificaciones o denegación de servicio;
- correcta asignación de la dirección y el transporte del mensaje;
- confiabilidad y disponibilidad general del servicio;
- consideraciones legales, por ejemplo, requerimientos para firmas electrónicas;
- obtención de aprobación previa al uso de los servicios públicos externos tales como mensajería instantánea o el compartir archivos;
- niveles altos de controles de autenticación para los accesos desde las redes públicamente accesibles.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

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 para 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.

Dado que los analistas y programadores tienen el conocimiento de la lógica de los procesos en los sistemas, se deben implementar controles que eviten maniobras dolosas por parte de estas personas u otras que puedan operar sobre los sistemas, las bases de datos y plataformas de software de base (por ejemplo, operadores que puedan manipular los datos y/o atacantes que puedan comprometer/alterar la integridad de las bases de datos) 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, ya que, en general, los aplicativos se asientan sobre este tipo de software.

Objetivos

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 los 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.

Alcance

Esta Política se aplica a todos los sistemas informáticos, desarrollos propios o de terceros y a todos los sistemas operativos y/o software de base que integren

cualquiera de los ambientes administrados por el Organismo en donde residan los desarrollos mencionados.

Responsabilidad

El Responsable de Seguridad de la Información, junto con el Propietario de la Información, el Departamento de Tecnología de la Información, definirán los controles para ser implementados en los sistemas desarrollados internamente o por terceros, en función de una evaluación previa de riesgos. Para la elaboración de estas definiciones los responsables podrán contar con el asesoramiento de la Unidad de Auditoría Interna.

El Responsable de Seguridad de la Información, junto con el Propietario de la Información, determinarán la criticidad de la información en el caso que corresponda. Luego, el Responsable de Seguridad de la Información definirá, junto con el Departamento de Tecnología de la Información, los métodos de encriptación para ser utilizados.

Asimismo, el Responsable de Seguridad de la Información cumplirá las siguientes funciones:

- Definir los procedimientos de administración de claves.
- Verificar el cumplimiento de los controles establecidos para el desarrollo y mantenimiento de sistemas.
- Verificar el cumplimiento de los requerimientos de seguridad para el software que se encuentra en producción.
- Definir procedimientos para: la verificación de la seguridad de las plataformas y bases de datos que soportan e interactúan con los sistemas; el control de código malicioso;

El Responsable del Departamento de Tecnología de la Información designará, al personal de su área que considere adecuado las funciones de "implementador" y "administrador de programas fuentes", cuyas responsabilidades se detallan en el presente capítulo. Asimismo, verificará el cumplimiento de las definiciones establecidas sobre los controles y las medidas de seguridad para ser incorporadas a los sistemas.

El Responsable del Departamento de Tecnología de la Información propondrá quiénes realizarán la administración de las técnicas criptográficas y claves.

La Gerencia de Asuntos Legales incorporará aspectos relacionados con el licenciamiento, la calidad del software y la seguridad de la información en los contratos con terceros por el desarrollo de software. Los Responsables de Seguridad, del Departamento de Tecnología de la Información y la Gerencia de Administración participarán en dicha tarea.

Política

14.1. Requisitos de seguridad de los sistemas de información

Objetivo

Mantener la seguridad en el intercambio de información dentro del Organismo y con cualquier otra entidad externa.

Control

14.1.1. Análisis y especificaciones delos requerimientos de seguridad de la información

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 para incorporar al sistema, así como los controles 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 para los productos a utilizar.
b) Evaluar los requerimientos de seguridad y los controles requeridos, teniendo en cuenta que estos 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.

Control

14.1.2. Seguridad de servicios aplicativos en redes públicas

Se controlarán los mecanismos de distribución y difusión tales como documentos, computadoras, dispositivos de computación móvil, comunicaciones

móviles, correo, correo de voz, comunicaciones de voz en general (analógica o digital), multimedia, servicios o instalaciones postales, equipos de fax, etc.

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

a) Vulnerabilidades de la información en los sistemas de oficina, por ejemplo, la grabación de llamadas telefónicas o teleconferencias, la confidencialidad de las llamadas, el almacenamiento de faxes, la apertura o distribución del correo.
b) Procedimientos y controles apropiados para administrar la distribución de información, por ejemplo, el uso de boletines electrónicos institucionales.
c) Exclusión de categorías de información sensible del Organismo, si el sistema no brinda un adecuado nivel de protección.
d) Limitación del acceso a la información de las actividades que desarrollan determinadas personas, por ejemplo, aquellas que trabajan en proyectos sensibles.
e) La aptitud del sistema para dar soporte a las aplicaciones del Organismo, como la comunicación de órdenes o autorizaciones.
f) Categorías de personal y contratistas o terceros a los que se permite el uso del sistema y las ubicaciones desde las cuales se puede acceder al mismo.
g) Restricción de acceso a determinadas instalaciones a específicas categorías de usuarios.
h) Identificación de la posición o categoría de los usuarios, por ejemplo, empleados del Organismo o contratistas, en directorios accesibles por otros usuarios.
i) Retención y resguardo de la información almacenada en el sistema.
j) Requerimientos y disposiciones relativos a sistemas de soporte de reposición de información previa.

Control

14.1.3. Protección de las transacciones de los servicios de aplicativos

Se tomarán recaudos para la protección de la integridad de la información publicada electrónicamente, a fin de prevenir la modificación no autorizada. Es posible que la información de un sistema de acceso público, por ejemplo, la información en un servidor Web accesible por Internet, deba cumplir con ciertas normas de la jurisdicción en la cual se localiza el sistema o en la cual tiene lugar la transacción electrónica. Se implementará un proceso de autorización formal antes de que la información se ponga a disposición del público, estableciéndose en todos los casos los encargados de dicha aprobación.

Todos los sistemas de acceso público deben prever que:

a) La información que se ingresa al sistema de publicación, o aquella que procesa el mismo, sea procesada en forma completa, exacta y oportuna.

b) La información sensible o confidencial sea protegida durante el proceso de recolección y su almacenamiento.
c) El acceso al sistema de publicación no permita el acceso accidental a las redes a las cuales se conecta el mismo.
d) El responsable de la publicación de información en sistemas de acceso público sea claramente identificado.
e)

14.2. Seguridad en los procesos de desarrollo y soporte

Objetivo

Garantizar que la seguridad informática diseñada e implementada cumpla durante el ciclo de vida de desarrollo de sistemas de información.

Control

14.2.1. Política de desarrollo seguro

El organismo controlara que todo software o sistema de información desarrollado interna o externamente cumplan con los lineamientos de desarrollo seguro, tales como:

- Control de Cambios en los sistemas/software.
- Principios de Construcción Seguros.
- Ambientes de desarrollo seguro.
- Pruebas de seguridad.
- Pruebas de aceptación.
- Protección de datos de prueba.

Control

14.2.2. Procedimientos de Control de Cambios del sistema

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) Efectuar un análisis de riesgos del cambio.
e) Determinar los requisitos de seguridad para el cambio.
f) Analizar el impacto de los cambios sobre los controles de seguridad existentes.
g) Obtener aprobación formal por parte del Departamento de Tecnología de la Información para las tareas detalladas, antes que comiencen de comenzar las mismas.
h) Solicitar la revisión del Responsable de Seguridad de la Información para garantizar que no se violen los requerimientos de seguridad que debe cumplir el software.
i) Efectuar las actividades relativas al cambio en el ambiente de desarrollo.
j) Obtener la aprobación por parte del usuario autorizado y del área de pruebas mediante pruebas en el ambiente correspondiente.
k) Actualizar la documentación para cada cambio implementado, tanto de los manuales de usuario como de la documentación operativa.
l) Mantener un control de versiones para todas las actualizaciones de software.
m) Garantizar que la implementación se llevará a cabo minimizando la discontinuidad de las actividades y sin alterar los procesos involucrados.
n) Informar a las áreas usuarias antes de la implementación de un cambio que pueda afectar su operatoria.
o) Garantizar que sea el implementador quien efectúe el pasaje de los objetos modificados al ambiente operativo.

Control

14.2.3. Revisión Técnica de las aplicaciones tras efectuar cambios en el sistema Operativo

Toda vez que sea necesario realizar un cambio en el Sistema Operativo, los sistemas serán revisados para asegurar que no se produzca un impacto en su funcionamiento o seguridad.

Para ello, se definirá un procedimiento que incluya:

a) Revisar los procedimientos de integridad y control de aplicaciones para garantizar que no hayan sido comprometidas por el cambio.
b) Garantizar que los cambios en el sistema operativo sean informados con anterioridad a la implementación.
c) Asegurar la actualización del Plan de Continuidad de las Actividades del Organismo.

Control

14.2.4. Restricción en los cambios a los paquetes de software

En caso de considerarlo necesario la modificación de paquetes de software suministrados por proveedores, y previa consulta al Departamento de Tecnología de la Información, se debe:

a) Analizar los términos y condiciones de la licencia a fin de determinar si las modificaciones se encuentran autorizadas.
b) Determinar la conveniencia de que la modificación sea efectuada por el Organismo, por el proveedor o por un tercero.
c) Evaluar el impacto que se produciría si el Organismo se hace cargo del mantenimiento.
d) Retener el software original realizando los cambios sobre una copia perfectamente identificada, documentando exhaustivamente por si fuera necesario aplicarlo a nuevas versiones.

Control

14.2.5. Uso de principios de seguridad en ingeniería de sistemas

El Departamento de Tecnología de la Información deberá aplicar los principios para ingeniería de sistemas seguros, se documentará, y aplicará en la implementación de cualquier sistema de información.

Control

14.2.6. Entorno de desarrollo seguro

El Departamento de Tecnología de la Información deberá definir y establecer formalmente la documentación requerida en las diferentes etapas de ciclo de vida de los sistemas.

Control

14.2.7. Desarrollo Externo de Software

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

a) Acuerdos de licencias, propiedad de código y derechos conferidos.
b) Requerimientos contractuales con respecto a la calidad y seguridad 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 establecidos, etc.
d) Verificación del cumplimiento de las condiciones de seguridad.
e) Acuerdos de custodia de los archivos fuentes del software (y cualquier otra información requerida) en caso de quiebra y/o inhabilidad de la tercera parte.

Control

14.2.8. Pruebas de funcionalidad durante el desarrollo de los Sistemas

El Departamento de Tecnología de la Información deberá llevar a cabo durante el desarrollo del sistema las pruebas de la funcionalidad.

Control

14.2.9. Pruebas de aceptación

Se debe cumplir con los formatos y el procedimiento del sistema de calidad para la realización y documentación de las pruebas.

14.3. Datos de prueba

Objetivo

Garantizar la protección de los datos utilizados para la prueba.

Control

14.3.1. Protección de los datos de prueba

Los datos de prueba deben seleccionarse cuidadosamente, en caso de seleccionar datos reales estos deben ser protegidos y controlados.

15. RELACIONES CON PROVEEDORES

Generalidades

Los proveedores del Organismo deben ser notificados en lo que respecta a los aspectos de seguridad que tienen que ver con el establecimiento y todos los requisitos de seguridad de la información del organismo.

Objetivo

Determinar el nivel de seguridad de información y prestación de servicios conforme a los estándares aplicables al proveedor.

Alcance

Los dos grandes puntos del alcance son:

- asegurar la protección de la información del organismo que es accedida por los proveedores, cumpliendo con el nivel de seguridad establecido.
- el mantenimiento del nivel de seguridad de información y prestación de servicios conforme a los estándares aplicables al proveedor.

Responsabilidad

El Responsable de Seguridad de la Información, junto con el Propietario de la Información, deben definir en función a la criticidad de la información, los requerimientos de protección en lo referente al acceso de la información de los proveedores del organismo. Asimismo, las Gerencias de Asuntos Legales y Administración deben garantizar que en los mismos se definan y se acuerden los niveles de seguridad establecidos por el organismo.

Política

15.1. Seguridad de la información en las relaciones con el Proveedor

Objetivo

Garantizar y asegurar la protección de la información del organismo que es accedida por los proveedores, cumpliendo con el nivel de seguridad establecido.

Control

15.1.1. Política de seguridad de la información para las relaciones con el proveedor

Los contratos o acuerdos de tercerización total o parcial para la administración y control de sistemas de información, redes y/o ambientes de equipamiento de Trabajo del Organismo, contemplarán los siguientes aspectos:

a) la identificación y la documentación de los tipos de proveedores, es decir, los servicios de TI, las utilidades de logística, los servicios financieros, los componentes de la infraestructura de TI y a quiénes autorizará al organismo para acceder a su información;
b) un proceso y ciclo de vida estandarizado para administrar las relaciones con los proveedores;
c) la definición de los tipos de acceso a la información que se les permitirá a los distintos tipos de proveedores y el monitoreo y control del acceso;
d) requisitos mínimos de seguridad de la información para cada tipo de información y tipo de acceso para servir de base para los acuerdos individuales con los proveedores en base a las necesidades del organismo y los requisitos y su perfil de riesgo;
e) procesos y procedimientos para monitorear la adherencia a los requisitos de seguridad de información establecidos para cada tipo de proveedor y tipo de acceso, incluida la revisión de terceros y la validación de productos;
f) controles de precisión y nivel de detalles para garantizar la integridad de la información o el procesamiento de información que entrega cualquiera de las partes;
g) tipos de obligaciones aplicables a los proveedores para proteger la información;
h) manejo de incidentes y contingencias asociadas con el acceso a los proveedores, incluidas las responsabilidades del organismo y los proveedores;
i) resiliencia y, en caso de ser necesario, disposiciones de recuperación y contingencia para garantizar la disponibilidad de la información o el procesamiento de información proporcionado por cualquiera de las partes;
j) administración de las transiciones necesarias de información, instalaciones de procesamiento de información y cualquier otra cosa que se deba mover y, garantizando que se mantiene la seguridad de la información a través de todo el período de transición.

Control

15.1.2. Abordar la seguridad dentro de los acuerdos del proveedor

Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que puede acceder, procesar,

almacenar, comunicar o proporcionar componentes de infraestructura de TI para la información del organismo.

A continuación, se definen los términos para incluir, según corresponda en cada caso, en los acuerdos a fin de y poder satisfacer los requisitos de seguridad de la información identificados:

a) descripción de la información que se debe proporcionar o a la que se debe acceder y los métodos para proporcionar o acceder a la información;
b) clasificación de la información de acuerdo al esquema de clasificación del organismo; y si es necesario también realizar el mapeo entre el esquema propio del organismo y el esquema de clasificación del proveedor;
c) requisitos legales y normativos, incluida la protección de datos personales, los derechos de propiedad intelectual y una descripción de sobre cómo se garantizará si se cumplen;
d) obligación de cada parte contractual de implementar un conjunto de controles acordados incluido el control de acceso, la revisión de desempeño, el monitoreo, los informes y la auditoría;
e) reglas de uso aceptable de la información;
f) una lista explícita del personal autorizado para acceder a/o recibir la información o los procedimientos o condiciones del organismo para su autorización y el retiro de la autorización, para el acceso a/o la recepción de la información del organismo al personal del proveedor;
g) políticas de seguridad de la información pertinentes al contrato específico;
h) requisitos y procedimientos de la administración de incidentes (en especial la notificación y la colaboración durante la remediación de incidentes);
i) requisitos de capacitación y concientización para procedimientos específicos y requisitos de seguridad de la información, es decir, para la respuesta ante incidentes y procedimientos de autorización;
j) normativas pertinentes para la subcontratación, incluidos los controles que se deben implementar;
k) socios de acuerdos pertinentes, incluida una persona de contacto para los asuntos de seguridad de la información;
l) derecho a auditar los procesos y los controles del proveedor relacionados al acuerdo;
m) procesos de resolución de defectos y resolución de conflictos;
n) obligación del proveedor a entregar periódicamente un informe independiente sobre la efectividad de los controles y un acuerdo sobre la corrección oportuna de los asuntos pertinentes indicados en el informe;
o) obligaciones del proveedor para cumplir con los requisitos de seguridad del organismo.

Control

15.1.3. Cadena de suministro de tecnologías de la información y comunicaciones

Se deben incluir en los acuerdos con los proveedores, los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones.

Se deben incluir, en caso de corresponder, los siguientes temas en los acuerdos con el proveedor sobre la seguridad de la cadena de suministro:

a) definir los requisitos de seguridad de la información que se aplicarán a la adquisición de tecnologías, productos o servicios de información y comunicación además de los requisitos de seguridad de la información para las relaciones con el proveedor;
b) para los servicios de tecnología de información y comunicación, que requieren que los usuarios propaguen los requisitos de seguridad del organismo en toda la cadena de suministro si los proveedores realizan subcontrataciones para partes del servicio de tecnología de información y comunicación proporcionados al organismo;
c) para los productos de tecnología de información y comunicación que requieren que los proveedores propaguen las prácticas de seguridad correspondientes a través de toda la cadena de suministro si estos productos incluyen componentes comprados a otros proveedores;
d) implementación de un proceso de monitoreo y métodos aceptables para validar que los productos y servicios de tecnología de información y comunicación se adhieren a los requisitos de seguridad establecidos;
e) implementación de un proceso para identificar los componentes de los productos o servicios que son fundamentales para mantener la funcionalidad y que, por lo tanto, requiere una mayor atención y escrutinio cuando se desarrollan fuera del organismo, especialmente si el proveedor del nivel superior externalice los aspectos de los componentes de productos o servicios a otros proveedores;
f) obtención de una garantía de que los componentes críticos y su origen se pueden rastrear en toda la cadena de suministros;
g) obtener la garantía de que los productos de tecnología de información y comunicación entregados funcionan según lo esperado sin ninguna función inesperada o no deseada;
h) definición de las reglas para compartir la información en cuanto a la cadena de suministro y cualquier posible problema y compromiso entre el organismo y los proveedores;
i) implementación de procesos específicos para administrar el ciclo de vida de los componentes de tecnología de información y comunicación junto con la disponibilidad y los riesgos de seguridad asociados. Esto incluye los riesgos de los componentes que ya no están disponibles debido a que los proveedores ya

no están en el negocio o a que ya no proporcionan estos componentes debido a los avances de la tecnología.

15.2. Gestión de la prestación del servicio por proveedores

Objetivo

Garantizar el mantenimiento del nivel acordado de seguridad de información y prestación de servicios

Control

15.2.1. Supervisión y Revisión de los servicios del proveedor

Se llevará a cabo el seguimiento, control y revisión de los servicios de las terceras partes asegurando que se encuentran adheridos a los términos de seguridad de la información y las condiciones definidas en los acuerdos, y que los incidentes de seguridad de la información y los problemas son manejados en forma apropiada.

El Organismo mantendrá control suficiente y visión general de todos los aspectos de seguridad para la información sensible o crítica, o de las instalaciones de procesamiento de información accedidas, procesadas o gestionadas por una tercera parte. Se recomienda que la organización asegure que se mantenga la visibilidad de las actividades de seguridad como gestión de cambios, identificación de vulnerabilidades y reporte/respuesta de incidentes de seguridad de información a través de un proceso de reportes claro y definido, con formato y estructura.

Control

15.2.2. Gestión de cambios a los servicios del proveedor

El proceso de gestión del cambio de un servicio de tercera parte necesita tener cuenta:

- Los cambios realizados por la organización para implementar:
  - mejoras a los servicios corrientes ofrecidos;
  - desarrollo de cualquier aplicaciones y sistemas nuevos;
  - modificaciones o actualizaciones de las políticas y procedimientos del Organismo;
  - nuevos controles para resolver los incidentes de la seguridad de la información y para mejorar la seguridad;
- cambios en los servicios de las terceras partes para implementar:
  - cambios y mejoras de las redes;
  - uso de nuevas tecnologías;

- adopción de nuevos productos o nuevas versiones/publicaciones;
- nuevas herramientas de desarrollo y ambientes;
- cambios de las ubicaciones físicas de las instalaciones de servicio;
- cambio de los proveedores.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

Generalidades

Existen numerosas amenazas que atentan contra la seguridad de la información, representando riesgos latentes que de materializarse pueden ocasionar incidentes de seguridad.

El Organismo cuenta con innumerables activos de información, cada uno de los cuales puede encontrarse expuesto a sufrir incidentes de seguridad. Es por ello que resulta sumamente necesario contar con una capacidad de gestión de dichos incidentes que permita comenzar por su detección, llevar a cabo su tratamiento y colaborar en la prevención de futuros incidentes similares.

Objetivo

Garantizar que los eventos de seguridad de la información y las debilidades asociados a los sistemas de información sean comunicados de forma tal que se apliquen las acciones correctivas en el tiempo oportuno.

Alcance

La Política definida en este documento se aplica a todo incidente que pueda afectar la seguridad de la información del Organismo.

Responsabilidad

El Responsable de Seguridad de la Información tiene a cargo el seguimiento, documentación y análisis de los incidentes de seguridad reportados, así como su comunicación al Comité de Seguridad de la Información, a los Propietarios de la Información y al Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC).

Asimismo, el Responsable de Seguridad de la Información y la Gerencia de Recursos Humanos y Relaciones Institucionales son responsables de comunicar fehacientemente los procedimientos de Gestión de Incidentes al personal del Organismo al inicio de la relación laboral.

La Gerencia de Asuntos Legales, participará en el tratamiento de incidentes de seguridad que requieran de su intervención.

Todo el personal del Organismo es responsable de reportar debilidades e incidentes de seguridad que oportunamente se detecten.

Política

16.1. Gestión de los Incidentes y mejoras de la seguridad de la información

Objetivo

Asegurar que se aplique un enfoque consistente y efectivo a la gestión de los incidentes en la seguridad de la información.

Se deben establecer las responsabilidades y procedimientos para manejar de manera efectiva los eventos y debilidades en la seguridad de la información una vez que han sido reportados. Se debe aplicar un proceso de mejora continua para la respuesta, monitoreo, evaluación y gestión general de los incidentes en la seguridad de la información.

Control

16.1.1. Responsabilidades y procedimientos

Se establecerán procedimientos de manejo de incidentes garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad. Se deben considerar los siguientes ítems:

a) Contemplar y definir todos los tipos probables de incidentes relativos a seguridad, incluyendo como mínimo:
   a. Fallas operativas
   b. Código malicioso
   c. Intrusiones
   d. Fraude informático
   e. Error humano
   f. Catástrofes naturales
b) Comunicar formalmente los incidentes a través de autoridades o canales apropiados tan pronto como sea posible.
c) Contemplar los siguientes puntos en los procedimientos para los planes de contingencia normales (diseñados para recuperar sistemas y servicios tan pronto como sea posible):
   a. Definición de las primeras medidas a implementar.
   b. Análisis e identificación de la causa del incidente.
   c. Planificación e implementación de soluciones para evitar la repetición del mismo, si fuera necesario.
   d. Comunicación formal con las personas afectadas o involucradas con la recuperación del incidente.
   e. Notificación de la acción a la autoridad y/u Organismos pertinentes.
d) Registrar pistas de auditoría y evidencia similar para:
   a. Análisis de problemas internos.

b. Uso como evidencia en relación con una probable violación contractual o infracción normativa, o en marco de un proceso judicial.

e) Implementar controles detallados y formalizados de las acciones de recuperación respecto de las violaciones de la seguridad y de corrección de fallas del sistema, garantizando:
   a. Acceso a los sistemas y datos existentes sólo al personal claramente identificado y autorizado.
   b. Documentación de todas las acciones de emergencia emprendidas en forma detallada.
   c. Comunicación de las acciones de emergencia al titular de la Unidad Organizativa y revisión de su cumplimiento.
   d. Constatación de la integridad de los controles y sistemas del Organismo en un plazo mínimo.

La Gerencia de Asuntos Legales del Organismo intervendrá en las cuestiones de su competencia ante incidentes de seguridad.

Control

16.1.2. Reporte de los eventos de la seguridad de información

Los incidentes relativos a la seguridad serán comunicados tan pronto como sea posible.

Ante la detección de un supuesto incidente o violación de la seguridad, el Responsable de Seguridad de la Información será informado tan pronto como se haya tomado conocimiento. Este indicará los recursos necesarios para la investigación y resolución del incidente, y se encargará de su monitoreo. Asimismo, mantendrá al Comité de Seguridad al tanto de la ocurrencia de incidentes de seguridad.

Sin perjuicio de informar a otros Organismos de competencia, el Responsable de Seguridad de la Información, comunicará al Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC) todo incidente o violación de la seguridad, que involucre recursos informáticos.

Control

16.1.3. Reporte de las debilidades de la seguridad

Los usuarios de servicios de información, al momento de tomar conocimiento directo o indirectamente acerca de una debilidad de seguridad, son responsables comunicar formalmente las mismas al Responsable de Seguridad de la Información.

Se prohíbe expresamente a los usuarios la realización de pruebas para detectar y/o utilizar una supuesta debilidad o falla de seguridad.

Control

16.1.4. Valoración de eventos de seguridad de la información y toma de decisiones

El Departamento de Tecnología de la Información, junto al Responsable de Seguridad de la Información, definirán un proceso que permita documentar, cuantificar y monitorear los tipos, los volúmenes y las anomalías de los incidentes. Esta información se utilizará para identificar aquellos que sean recurrentes y evaluar su impacto.

Control

16.1.5. Respuesta a incidentes de seguridad de la información

Los incidentes de seguridad de información deberán recibir una respuesta de conformidad con los procedimientos documentados.

Control

16.1.6. Aprendizaje de los incidentes de la seguridad de la información

Se definirá un proceso que permita documentar, cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y anomalías. Esta información se utilizará para identificar aquellos que sean recurrentes o de alto impacto. Esto será evaluado a efectos de establecer la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de casos futuros.

Control

16.1.7. Recopilación de evidencias

Ante cualquier evento de seguridad es necesario contar con una adecuada evidencia, para ello los sistemas deberán recolectar los registros correspondientes, que asimismo permitan deslindar cualquier tipo de responsabilidad, según lo establecido en la presente Política.

17. GESTIÓN DE LA CONTINUIDAD

Generalidades

La administración de la continuidad de las actividades es un proceso crítico que debe involucrar a todos los niveles del Organismo.

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, y atenuar las consecuencias de eventuales interrupciones de las actividades del Organismo y asegurar la reanudación oportuna de las operaciones indispensables.

Objetivos

Minimizar los efectos de las posibles interrupciones de las actividades normales del Organismo (sean estás resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.

Analizar las consecuencias de la interrupción de los procesos del Organismo y tomar las medidas correspondientes para la prevención de hechos similares en el futuro.

Maximizar la efectividad de los planes de contingencia del Organismo, incluyendo, 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.
c) **Recuperación:** Consistente en la restauración de los procesos a las condiciones de operación normales.

Asegurar la coordinación entre el personal del Organismo y los terceros que participarán en las estrategias de planificación de contingencias. Asignar funciones para cada actividad definida.

Alcance

Esta Política se aplica a todos los procesos críticos identificados del Organismo.

Responsabilidad

El Responsable de Seguridad de la Información participará activamente en la definición, documentación, prueba y actualización de los planes de contingencia.

El Departamento de Tecnología de la Información y el Responsable de Seguridad de la Información cumplirán las siguientes funciones:

- Identificar las amenazas que puedan ocasionar interrupciones de los procesos y/o las actividades del Organismo.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones.
- Identificar los controles preventivos.
- Desarrollar un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades del Organismo.
- Elaborar los planes de contingencia necesarios para garantizar la continuidad de las actividades del Organismo.

Los Responsables de Procesos revisarán periódicamente los planes bajo su incumbencia, así como identificarán cambios en las disposiciones relativas a las actividades del Organismo, aún no reflejados en los planes de continuidad.

Los Administradores de cada plan verificarán el cumplimiento de los procedimientos implementados para llevar a cabo las acciones contempladas en cada plan de continuidad.

Política

17.1. Gestión de continuidad del Organismo

Objetivo

Mitigar las interrupciones a las actividades del Organismo y proteger los procesos críticos de los efectos de fallas importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.

Control

17.1.1. Proceso de Administración de la continuidad del Organismo

Podrá consultarse al Comité en el marco de sus competencias sobre los proyectos que se elaborarán con respecto al Punto 17.

Las funciones que deberán coordinarse en el proceso de administración para la continuidad de la operatoria de los sistemas de tratamiento de información del Organismo frente a interrupciones imprevistas son las siguientes:

- Identificar y priorizar los procesos críticos de las actividades del Organismo.

- Promover el entendimiento a todos los integrantes del Organismo de la Política de Seguridad de la Información, para que puedan comprendan los riesgos que se enfrentan, 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.
- Elaborar y documentar una estrategia de continuidad de las actividades del Organismo, consecuente con los objetivos y prioridades acordados.
- Proponer planes de continuidad de las actividades del Organismo, de conformidad con la estrategia de continuidad acordada.
- Establecer un cronograma de pruebas periódicas de cada uno de los planes de contingencia, proponiendo una asignación de funciones para su cumplimiento.
- Coordinar actualizaciones periódicas de los planes y procesos implementados.
- Considerar la contratación de seguros que podrían formar parte del proceso de continuidad de las actividades del Organismo.
- Proponer las modificaciones a los planes de contingencia.

Control

17.1.2. Implantación de la continuidad de la seguridad de la información

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, por ejemplo, fallas en el equipamiento, comisión de ilícitos, interrupción del suministro de energía eléctrica, inundación, incendio, desastres naturales, destrucción edilicia, atentados, etc.
- 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.

Esta actividad será llevada a cabo con la participación de los propietarios de los procesos y recursos de información de que se trate y el Responsable de Seguridad de la Información, considerando todos los procesos de las actividades del Organismo y no limitándose a las instalaciones de procesamiento de la información.

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 a la máxima autoridad del Organismo para su aprobación, con el visado del Comité a fin de determinar su concordancia con la presente Política.

Control

17.1.3. Verificación, revisión y evaluación de la continuidad de las Actividades del Organismo

Los propietarios de procesos y recursos de información, con la asistencia del Responsable de Seguridad de la Información y el Departamento de Tecnología de la Información, elaborarán los planes de contingencia necesarios para garantizar la continuidad de las actividades del Organismo.

El proceso de planificación de la continuidad de las actividades considerará los siguientes puntos:

a) Identificar y acordar respecto a todas las funciones y procedimientos de emergencia.
b) Analizar los posibles escenarios de contingencia y definir las acciones correctivas a implementar en cada caso.
c) Implementar procedimientos de emergencia para permitir la recuperación y restablecimiento en los plazos requeridos. Se debe dedicar especial atención a la evaluación de las dependencias de actividades externas y a los contratos vigentes.
d) Documentar los procedimientos y procesos acordados.
e) Instruir adecuadamente al personal, en materia de procedimientos y procesos de emergencia acordados, incluyendo el manejo de crisis.
f) instruir al personal involucrado en los procedimientos de reanudación y recuperación en los siguientes temas:
    a. Objetivo del plan.
    b. Mecanismos de coordinación y comunicación entre equipos (personal involucrado).
    c. Procedimientos de divulgación.
    d. Requisitos de la seguridad.
    e. Procesos específicos para el personal involucrado.
    f. Responsabilidades individuales.
g) Probar y actualizar los planes, guardando evidencia formal de las pruebas y sus resultados.

Asimismo, el proceso de planificación debe concentrarse en los objetivos de las actividades requeridas del organismo, por ejemplo, restablecimiento de los servicios a los usuarios en un plazo aceptable. Deben considerarse los servicios y recursos que permitirán que esto ocurra, incluyendo, dotación de personal, recursos que no procesan información, así como acuerdos para reanudación de emergencia en sitios alternativos de procesamiento de la información.

Control

17.1.4. 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.

Las modificaciones de cada plan de continuidad deben ser propuestas 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 (cómo evaluar la situación, qué personas estarán involucradas, etc.) antes de poner en marcha los mismos.
b) Definir los procedimientos de emergencia que describan las acciones a emprender una vez ocurrido un incidente que ponga en peligro las operaciones del Organismo y/o la vida humana. 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 probado 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 posibles. Se deben mencionar alternativas cuando

corresponda. Es de suma importancia definir a un responsable de declarar el estado de contingencia, lo cual dará inicio al plan.

Control

17.1.5. Ensayo, Mantenimiento y Revaluación 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:

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

- Efectuar pruebas de discusión de diversos escenarios (discutiendo medidas para la recuperación las actividades utilizando ejemplos de interrupciones).
- Realizar simulaciones (especialmente para entrenar al personal en el desempeño de sus roles de gestión posterior a incidentes o crisis).
- Efectuar pruebas de recuperación técnica (garantizando que los sistemas de información puedan ser restablecidos con eficacia).
- 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:

- Efectuar pruebas de recuperación en un sitio alternativo (ejecutando los procesos de las actividades del Organismo en paralelo, con operaciones de recuperación fuera del sitio principal).
- Realizar pruebas de instalaciones y servicios de proveedores (garantizando que los productos y servicios de proveedores externos cumplan con los compromisos contraídos).

Todas las pruebas efectuadas deben ser documentadas, resguardándose la evidencia formal de la ejecución y de los resultados obtenidos.

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.

Cada uno de los Responsables de Procesos es el responsable de las revisiones periódicas de cada uno de los planes de continuidad de su incumbencia, como así también de la identificación de cambios en las disposiciones relativas a las actividades del Organismo aún no reflejadas en dichos planes.

Debe 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 que correspondan serán puestas a consideración de la máxima autoridad del Organismo, para su aprobación, con el visado previo del Comité a fin de determinar su concordancia con la presente Política.

Por otra parte, el resultado de este proceso será dado a conocer a fin de que todo el Personal involucrado tenga conocimiento de los cambios incorporados.

17.2. Categoría: Redundancias

Objetivo

Asegurar la continuidad de la información y que esté integrada a los sistemas de gestión.

Control

17.2.1. Disponibilidad de las instalaciones de procesamiento de la información

Se deben implementar las instalaciones de procesamiento de la información con la debida redundancia a efectos de cumplir con los requisitos definidos.

Para cumplir con lo anterior, deben identificarse los requisitos funcionales para considerar los componentes o arquitecturas redundantes. Hay tener en cuenta durante el diseño, la actividad de la gestión de los riesgos de integridad y confidencialidad de la información que puedan acarrear las redundancias.

18. CUMPLIMIENTO

Generalidades

El presente apartado refiere al cumplimiento de la presente Política, las normas y los procedimientos de seguridad del Organismo, en el marco de sus disposiciones y de la normativa que resulte de aplicación para el caso.

Objetivos

Garantizar que los sistemas, el personal del Organismo y terceros autorizados cumplan con la política, las normas y los procedimientos de seguridad del Organismo.

Revisar la seguridad de los sistemas de información periódicamente, a efectos de garantizar la adecuada aplicación de la política, las normas y los procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información.

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

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 del Organismo.

Alcance

Esta Política se aplica a todo el personal del Organismo, cualquiera sea su situación de revista. Así como también a externos, en los que encuadran proveedores, o cualquier otra persona o empresa que brinde algún tipo de servicio al Organismo.

Asimismo, se aplica a los sistemas de información, normas, procedimientos, documentación y plataformas técnicas del Organismo, y a las auditorías efectuadas sobre estos.

Responsabilidad

El Responsable de Seguridad de la Información cumplirá las siguientes funciones:

- Garantizar, junto con la Gerencia de Asuntos Legales, el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual y a la conservación de registros.

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

Los Responsables de Unidades Organizativas velarán por la correcta implementación y cumplimiento de las normas y los procedimientos de seguridad establecidos en la presente Política, dentro de su área de responsabilidad.

Política

18.1. Cumplimiento de los requisitos legales y contractuales

Objetivo

Evitar las violaciones a cualquier ley; regulación estatutaria; y cualquier requerimiento de seguridad.

Control

18.1.1. Identificación de la Legislación Aplicable

Se definirán y documentarán claramente todos los requisitos normativos 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.

Control

18.1.2. 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 el Organismo.

El Organismo 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 acordadas y lo dispuesto por la normativa vigente.

Control

18.1.3. 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 clasificarán 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.

Las claves criptográficas asociadas con archivos cifrados se mantendrán en forma segura y estarán disponibles para su uso por parte de personas autorizadas cuando resulte necesario.

Se debe considerar la posibilidad de degradación de los medios utilizados para el almacenamiento de los registros. Los procedimientos de almacenamiento y manipulación se implementarán de acuerdo con las recomendaciones del fabricante.

Si se seleccionan medios de almacenamiento electrónicos, se incluirán los procedimientos para garantizar la capacidad de acceso a los datos (tanto legibilidad de formato como medios) durante todo el período de retención, a fin de salvaguardar los mismos contra eventuales pérdidas ocasionadas por futuros cambios tecnológicos.

Los sistemas de almacenamiento de datos serán seleccionados de modo tal que los datos requeridos puedan recuperarse de una manera que resulte aceptable para un tribunal de justicia, por ejemplo, que todos los registros requeridos puedan recuperarse en un plazo y un formato aceptable.

El sistema de almacenamiento y manipulación garantizará una clara identificación de los registros y de su período de retención legal o normativa. Asimismo, se permitirá una adecuada destrucción de los registros una vez transcurrido dicho período, si ya no resultan necesarios para el Organismo.

A fin de cumplir con estas obligaciones, se tomarán las siguientes medidas:

a) Elaborar y divulgar los lineamientos para la retención, almacenamiento, manipulación y eliminación de registros e información.
b) Preparar un cronograma de retención identificando los tipos esenciales de registros y el período durante el cual deben ser retenidos.
c) Mantener un inventario de programas fuentes de información clave.
d) Implementar adecuados controles para proteger la información y los registros esenciales contra pérdida, destrucción y falsificación.

Control

18.1.4. Protección de Datos y Privacidad de la Información Personal

Todos los empleados deben 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.

El Organismo redactará un "Compromiso de Confidencialidad", el cual debe ser suscrito por todos los empleados y contratistas. La copia firmada del compromiso será retenida en forma segura por el Organismo.

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 debe 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.

Control

18.1.5. Prevención del Uso Inadecuado de los Recursos de Procesamiento de Información

Los recursos de procesamiento de información del Organismo se suministran con un propósito determinado. Toda utilización de estos recursos con propósitos no autorizados o ajenos al destino por el cual fueron provistos debe ser considerada como uso indebido.

Todos los empleados deben conocer el alcance preciso del uso adecuado de los recursos informáticos y deben respetarlo.

Control

18.1.6. Regulación de Controles para el Uso de Criptografía

Al utilizar firmas digitales o electrónicas, se debe considerar lo dispuesto por la Ley 25.506 y su decreto reglamentario Decreto 2628/2002, que establecen las condiciones bajo las cuales una firma digital es legalmente válida.

Control

18.2. Revisiones de la seguridad de la información

Objetivo

Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional.

La seguridad de los sistemas de información se debiera revisar regularmente.

Estas revisiones deben realizarse en base a las políticas de seguridad apropiadas y las plataformas técnicas, y los sistemas de información deben ser auditados en cumplimiento con los estándares de implementación de seguridad aplicables y los controles de seguridad documentados.

Control

18.2.1. Revisión independiente de la seguridad de la información

La Unidad de Auditoría Interna por sí, o a través de la contratación de especialistas en la materia, realizará revisiones independientes sobre la implementación de la Política de Seguridad de la Información, a efectos de garantizar que las prácticas del Organismo reflejen adecuadamente sus disposiciones.

Control

18.2.2. Cumplimiento de la Política y normas de seguridad

Cada Responsable de Unidad Organizativa, velará por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos, dentro de su área de responsabilidad.

El Responsable de Seguridad de la Información, realizará revisiones periódicas de todas las áreas del Organismo a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad. Entre las áreas a revisar se incluyen las siguientes:

a) Sistemas de información.
b) Proveedores de sistemas.
c) Propietarios de información.
d) Usuarios.

Los Propietarios de la Información brindarán apoyo a la revisión periódica del cumplimiento de la política, normas, procedimientos y otros requisitos de seguridad aplicables.

Control

18.2.3. Comprobación del cumplimiento

El Responsable de Seguridad de la Información verificará periódicamente que los sistemas de información cumplan con la política, normas y procedimientos de seguridad, las que incluirán la revisión de los sistemas en producción a fin de garantizar que los controles de hardware y software hayan sido correctamente implementados. En caso de ser necesario, estas revisiones contemplarán la asistencia técnica especializada.

En este último caso, el resultado de la evaluación se volcará en un informe técnico para su ulterior interpretación por parte de los especialistas. Para ello, la tarea podrá ser realizada por un profesional experimentado (en forma manual o con el apoyo de herramientas de software), o por un paquete de software automatizado que genere reportes que serán interpretados por un especialista técnico.

La verificación del cumplimiento comprenderá pruebas de penetración y tendrá como objetivo la detección de vulnerabilidades en el sistema y la verificación de la eficacia de los controles con relación a la prevención de accesos no autorizados. Se tomarán los recaudos necesarios en el caso de pruebas de penetración exitosas que comprometan la seguridad del sistema.

Las verificaciones de cumplimiento sólo serán realizadas por personas competentes, formalmente autorizadas y bajo la supervisión.

18.3. Consideraciones de Auditorías de Sistemas

Objetivo

Maximizar la efectividad de y minimizar la interferencia desde/hacia el proceso de auditoría del sistema de información.

Durante las auditorías de los sistemas de información debieran existir controles para salvaguardar los sistemas operacionales y herramientas de auditoría.

Con relación a las auditorías, serán de aplicación las Normas de Control Interno para Tecnologías de Información, aprobadas por la resolución SIGEN N° 48/05.

Control

18.3.1. Controles de Auditoría de Sistemas

Cuando se realicen actividades de auditoría que involucren verificaciones de los sistemas en producción, se tomarán recaudos 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:

e) Acordar con el Área que corresponda los requerimientos de auditoría.
f) Limitar las verificaciones a un acceso de sólo lectura del software y datos de producción.
g) 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
h) Identificar claramente los recursos de tecnologías de información (TI) para llevar acabo las verificaciones, los cuales serán puestos a disposición de los auditores. A tal efecto, la Unidad de Auditoría o en su defecto quien sea propuesto por el Comité de Seguridad de la Información el cual debe ser puesto en conocimiento de las áreas involucradas:

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

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

Control

18.3.2. Protección de los Elementos Utilizados por la Auditoría de Sistemas

Se protegerá el acceso a los elementos utilizados en las auditorías de sistemas, o sea archivos de datos o software, a fin de evitar el mal uso o el compromiso de los mismos.

Dichas herramientas estarán separadas de los sistemas en producción y de desarrollo, y se les otorgará el nivel de protección requerido.

Se tomarán los recaudos necesarios a efectos de cumplimentar las normas de auditoría dispuestas por la Sindicatura General de la Nación.

Control

18.3.3. Control: Sanciones Previstas por Incumplimiento

Se sancionará administrativamente a todo aquel que infrinja lo dispuesto en la presente Política de Seguridad conforme a lo dispuesto por las normas que rigen al personal del Organismo, y eventualmente se realizarán las acciones correspondientes ante el o los Organismos pertinentes.

Sin perjuicio de ello, corresponde mencionar que el agente que no cumpla sus obligaciones puede incurrir también en responsabilidad civil o patrimonial y/o en responsabilidad penal.