POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION

Instituto de Neurocirugía Dr. Alfonso Asenjo

Junio 2013

CONTROL DE VERSIONES

VERSION	**1.0**	FECHA DE PUBLICACION	**Junio 2013**
AUTOR	Encargado de la Seguridad de la Información		Instituto de Neurocirugía
REVISOR	Comité de Seguridad		Instituto de Neurocirugía
CLASIFICACION	Uso Interno		

A. Declaración Institucional

La presente Política de Seguridad de la Información se dicta en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos, las nuevas tecnologías de la información y de las comunicaciones (TIC), al ser incorporadas progresivamente a los procesos institucionales y al quehacer personal de los funcionarios al ejercer sus labores en el Instituto de Neurocirugía.

Debe ser conocida y cumplida por toda la planta de personal institucional, considerando una serie de beneficios, ventajas y oportunidades de diversa índole, pero conlleva también ciertos riesgos, que pueden eventualmente afectar a los activos de información institucional.

Por otra parte, la dependencia creciente de la institución con respecto a los recursos de infraestructura de TIC aumenta considerablemente los impactos que la materialización de una o más amenazas puedan provocar en sus activos de información.

En el entendido de que los riesgos que se logren identificar estarán siempre presentes, ya que no se pueden eliminar, la institución se compromete a gestionar la seguridad de la información como un proceso contínuo en el tiempo, a través de un programa de implantación de lo que se denominará un "Sistema de Gestión de Seguridad de la Información (SGSI)", basado en la norma internacional ISO/IEC 27001:2005, tendiente a homogeneizar los criterios de seguridad, con el objetivo de preservar los activos de información institucional, basada en metodologías técnicas y estándares en estas materias, con el firme propósito de lograr introducir un ciclo de mejoramiento continuo y sostenible en el tiempo, que permita lograr niveles adecuados de integridad, confidencialidad y disponibilidad, de todos sus activos de información relevantes para la institución, como un principio clave en la gestión de sus procesos.

- **Integridad:** Los componentes del sistema serán accesibles solo por aquellos usuarios autorizados.

- **Confidencialidad:** Los componentes del sistema sólo pueden ser creados y modificados por los usuarios autorizados.

- **Disponibilidad:** Los usuarios deben tener disponibles y accesibles en forma oportuna todos los componentes del sistema cuando sea requerido por usuarios debidamente autorizados.

B. Términos y Definiciones

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

- **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 suplantación de identidades.

- **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 Instituto de Neurocirugía.

- **Acciones contra los datos:** una persona no autorizada podría realizar las siguientes acciones en la información; clasificar y desclasificar, filtrar, alterar, borrar, usurpar, hojear información clasificada, deducir datos confidenciales.

- **Confiabilidad de la información:** es decir, que la información generada sea 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 la 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 computadores, audiovisual u otro.

    - **Sistema de Información:** Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

    - **Tecnología de la Información:** Se refiere al hardware y software operados por el Instituto o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Instituto, sin tener en

cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

- **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 procedimiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria del Instituto de Neurocirugía.

- **Repositorio:** estructura electrónica donde se almacenan documentos electrónicos.

- **Riesgos:** amenazas de impactar y vulnerar la seguridad del activo de información y su posibilidad de ocurrencia.

- **Sistema informático:** conjunto de uno o más computadores, software asociado, periféricos, terminales, usuarios, procesos físicos, medios de transferencia de información y otros, que forman un todo autónomo capaz de realizar procesamiento y/o transferencia de información.

- **Usuario**: entidad o individuo que utiliza un sistema informático.

- **Administración de Riesgos:** se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación 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.

- **Comité de Seguridad de la Información:** El comité de seguridad de la información, es un cuerpo integrado por la Dirección, Subdirectores y Encargada de la Seguridad de la Información de las áreas sustantivas del Instituto de Neurocirugía, destinado a garantizar el apoyo manifiesto de las autoridades a las incitativas de seguridad.

- **Responsable de Seguridad Informática:** 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 Instituto de Neurocirugía que así lo requieran.

- **Incidente de Seguridad:** Un incidente de seguridad es un evento adverso en un sistema de computadores, o red de computadores, que compromete la 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.

- **Funcionarios del Instituto:** tienen la responsabilidad de cumplir con lo establecido en las Políticas de Seguridad de la Información que se han institucionalizadas, aplicarlas en relación a su quehacer habitual y alertar de manera oportuna y adecuada por los canales de comunicación formalmente establecidos, cualquier situación que pueda poner el riesgo la seguridad de la información.

- **Propietario de la Información:** Es el responsable de la información y de los procesos que la manipulan, entre estos manuales, mecánicos o electrónicos. Debe participar activamente en la definición del valor de la información para el Instituto, de manera que se puedan definir los controles apropiados para protegerla.

C. Normas que componen la Política

Son parte de esta política los siguientes dominios establecidos en la NCh-ISO 27001, los cuales abarcan activos de información que interesa proteger:

1. Políticas de Seguridad de la Información
2. Organización de Seguridad de la Información
3. Clasificación de Control de Activos
4. Seguridad de Recursos Humanos
5. Seguridad Física y Ambiental
6. Gestión de las Comunicaciones y Operaciones
7. Gestión de Control de Acceso
8. Adquisición, Desarrollo y Mantenimiento de Seguridad de los Sistemas
9. Gestión de Continuidad del Negocio
10. Cumplimientos Normativos.

1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La información es un recurso que, como el resto de los activos, tiene valor para el Instituto y por consiguiente debe ser debidamente protegida. Por tanto es de vital importancia tomar en cuenta que todo elemento relevante en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de la información es de valor para la Institución.

Para esto, debe existir y se debe asegurar un compromiso de las máximas autoridades del Instituto y de los Jefes o Encargados de las Unidades/Servicios para la difusión, consolidación y cumplimiento de la presente Política.

Objetivos de la gestión de Seguridad de la Información en el Instituto

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

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

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

Realizar un catastro para identificar todos los activos de información relevantes que están presentes directa o indirectamente en cada proceso del Instituto, de tal manera que sea posible abarcar todos los procesos críticos institucionales y aquellos procesos de soporte.

Los activos de información comprenden a la información propiamente tal, en sus múltiples formatos, tales como papel, electrónico o cualquier otro medio; y los equipos/sistemas/infraestructura que soportan la información y las personas que la utilizan y que tienen el conocimiento de los procesos institucionales.

Realizar las actividades necesarias de análisis de riesgo según normativas, técnicas y estándares disponibles y aplicables para diseñar e implantar medidas y controles que permitan mitigar los riegos que sean identificados, sin perder de vista el enfoque de la gestión por procesos institucionales.

Capacitar a todos los empleados acerca de su responsabilidad en el logro de los objetivos de gestión fijados por la institución en materia de seguridad de la información, y de la incorporación progresiva de buenas prácticas laborales relacionadas con ello.

Definir una estructura y un marco de políticas, estándares y procedimientos en materia de seguridad de la información, a ser desarrollada dentro del Instituto.

Mantener la continuidad de sus procesos críticos, dependientes o no de los Sistemas de Información. Hoy más que nunca los procesos que existen en el Instituto están basados en una plataforma tecnológica que permite tener altos niveles de disponibilidad y prestaciones de alto valor y calidad.

Alcance

Esta Política se aplica en todos quienes trabajen en el Instituto de Neurocirugia, cualquiera sea su calidad contractual, incluyendo personal perteneciente a empresas externas, sean Públicas y/o Privadas.

La política cubre toda la información impresa o escrita en papel, almacenada electrónicamente, trasmitida por correo o usando medios electrónicos, mostrada en videos o registros de audio de una conversación.

La presente política adopta su base de contenidos, a partir de las buenas prácticas definidas en el estándar Nch-ISO 27001 y de los requisitos legales, normativos y contractuales relativos a la Seguridad de la Información, que sean aplicables a la organización, como el Decreto Supremo 83 de fecha 03 de junio de 2004 del Ministerio Secretaría General de la Presidencia, que aprueba Norma Técnica para los órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos.

Responsabilidades

Director, Subdirectores, Jefes de Servicios y/o Unidades, sea cual fuere su nivel jerárquico son responsables de la implementación de esta Política de Seguridad de la Información dentro de sus áreas de responsabilidad, así como del cumplimiento de dicha Política por parte de su equipo de trabajo.

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

Las máximas autoridades del Instituto aprueban esta Política y son responsables de la autorización de sus modificaciones.

El **Comité de Seguridad de la Información** del Instituto, procederá a revisar y proponer a la máxima autoridad del Instituto, para su aprobación, la Política de Seguridad de la Información y las funciones generales en materia de seguridad de la información; también procederá a monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las Política de Seguridad de la Información, basándose para todo efecto en lo dictado en la norma estándar ISO/IEC 27001:2005 en el marco de gobernabilidad de la seguridad.

El **Encargado de Seguridad de la Información** velará por la existencia de un conjunto organizado de políticas de seguridad que pongan de manifiesto el enfoque de la institución con respecto a la gestión de la seguridad de la información y formalice su compromiso con la protección de la información.

Los **Propietarios de la Información** son responsables de clasificarla de acuerdo con el grado de sensibilidad y criticidad de la misma, de documentar y mantener actualizada la clasificación efectuada, y de definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia.

El **Responsable de Recursos Humanos** o quien desempeñe esas funciones, cumplirá la función de notificar a todo el personal que ingrese de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan. Además será responsable de incorporar el tema de aplicación y observación de seguridad de la información en su plan de capacitación institucional y velar por la correcta inducción de los funcionarios nuevos en materias de seguridad de la información. Asimismo, notificará la política a todo el personal, de los cambios que en ella se produzcan, la implementación de la suscripción de los Compromisos de Confidencialidad (entre otros) y las tareas de capacitación continúan en materia de seguridad.

Los **usuarios de la información y de los sistemas** deberán conocer las Políticas de Seguridad de la Información que se han institucionalizado y deberán aplicar aquellas que están relacionadas a su quehacer habitual.

Estructura y contenido de las Políticas de Seguridad de la información

1.1. Aprobación de Políticas

- El Comité de Seguridad de la Información del Instituto de Neurocirugía aprueba las presentes políticas elaboradas por el Encargado de Seguridad.

1.2. Comunicación de las Políticas

- El Comité de Seguridad deberá promover la comunicación, difusión y publicación de las políticas al interior del Instituto, utilizando para ello los medios de comunicación existentes.

- Recursos Humanos, deberá incorporar en el proceso de inducción del personal que ingresa, la documentación de las políticas de Seguridad de Información. Posteriormente validará la aceptación y conformidad por parte de cada empleado.

1.3. Revisión y actualización de las Políticas

- Esta política, a partir de su creación, debe ser mantenida y actualizada para representar las situación y lo que espera del Instituto.

- Se deben revisar las políticas de seguridad a lo menos cada 2 años, o cada vez se produzca un cambio significativo en el cual se cree un riesgo al Instituto. Entre los cambios que hacen necesaria la revisión de las políticas, se destacan:
  - Cambios en las leyes y/o reglamentos que afecten al Instituto.
  - Incorporación o modificaciones importantes de procesos críticos del Instituto.
  - Cambios significativos en el soporte tecnológico.
  - Modificaciones en la estructura organizacional.
  - Cambios significativos en las amenazas a que se expone la información.
  - Las revisiones que se efectúen a las políticas de seguridad deben considerar tanto la actualidad de las políticas como su eficacia, eficiencia y cumplimiento.
  - Independiente del proceso de revisión permanente, cada 2 años se deberá ejecutar un proceso formal de revisión y actualización de la totalidad de las políticas, procediendo a modificar e incorporar los posibles cambios. Este proceso conlleva la aprobación anteriormente presentada.

1.4. Cumplimiento de las Políticas

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.

1.5. Consecuencias de las violaciones a la Política de Seguridad

El incumplimiento de la Política de Seguridad de la Información tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud y característica del aspecto no cumplido, las cuales se encuentran tipificadas en el Reglamento Interno.

2. ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN

El Instituto reconoce la importancia de proteger la Información, evitando la divulgación, destrucción, modificación y utilización no autorizada. Para lo cual establece la presente Política de Seguridad de la información organizacional, como parte fundamental de los objetivos y actividades del Instituto.

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

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

Por otro lado debe tenerse en cuenta que ciertas actividades del Instituto pueden requerir que terceros accedan a información interna, o bien puede ser necesaria la externalización de ciertas funciones relacionadas con el procesamiento de la información. En estos casos se considerará que la información puede ponerse en riesgo si el acceso de dichos terceros se produce en el marco de una inadecuada administración de la seguridad, por lo que se establecerán las medidas adecuadas para la protección de la información.

Objetivo

Establecer, administrar y garantizar una estructura de gestión con objeto de iniciar y controlar la implantación de la seguridad de la información dentro del Instituto, así como para la distribución de funciones y responsabilidades.

La Dirección debe aprobar la política de seguridad, asignar roles de seguridad, coordinar y revisar la implantación de la Seguridad en todo el Instituto.

Mantener actualizado las tendencias de la evolución de las normas y métodos, así como proporcionar mecanismos adecuados para el tratamiento de las incidencias de seguridad.

Mantener la seguridad de que los recursos de tratamiento de la información y de los activos de información del instituto sean accesibles por terceros.

Vigencia

Esta Norma de Seguridad de la Información entrará en vigencia a partir del **01 de Agosto de 2013.**

Responsabilidades

El Comité de Seguridad de la Información tendrá a cargo el mantenimiento y la presentación para la aprobación de la presente Política, ante la máxima autoridad del Instituto, el seguimiento y las actividades relativas a la seguridad de la información (análisis de riesgos, monitoreo de incidentes, supervisión de la investigación, implementación de controles, administración de la continuidad, impulsión de procesos de concientización, etc.) y la proposición de asignación de funciones.

El Responsable de Seguridad Informática asistirá al personal del Instituto en materia de seguridad de la información y coordinará la interacción con Institutos especializados.

Asimismo, junto con los propietarios de la información, analizará el riesgo de los accesos de terceros a la información del Instituto y verificará la aplicación de las medidas de seguridad necesarias para la protección de la misma.

El Responsable del Área Administrativa cumplirá la función de incluir en los contratos con proveedores de servicios de tecnología y cualquier otro proveedor de bienes o servicios cuya actividad afecte directa o indirectamente a los activos de información, la obligatoriedad del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas relacionadas.

Política

2.1. Infraestructura de la Seguridad de la Información

2.1.1. Comité de Seguridad de la Información

La seguridad de la información es una responsabilidad del Instituto compartida por todos los funcionarios que el Director del Instituto defina para conformar el Comité de Seguridad de la Información.

Se crea el Comité de Seguridad de la Información, integrado por los Subdirectores o funcionarios que la máxima Autoridad del Instituto defina para efectos de determinar las pertinentes iniciativas de seguridad. El mismo contará con un Coordinador, quien cumplirá la función de impulsar la implementación de la presente Política.

Área / Dirección Representante

Este Comité tendrá entre sus funciones:

- Revisar y proponer a la máxima autoridad del Instituto para su aprobación, la Política y las funciones generales en materia de seguridad de la información.
- Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
- Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.
- Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área.
- Acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información.
- Garantizar que la seguridad sea parte del proceso de planificación de la información.
- Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
- Promover la difusión y apoyo a la seguridad de la información dentro del Instituto.
- Coordinar el proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de la información del Instituto frente a interrupciones imprevistas.

2.1.2. Proceso de Autorización para Instalaciones de Procesamiento de Información

Los nuevos recursos de procesamiento de información serán autorizados por los Responsables de las Unidades involucradas, considerando su propósito y uso, conjuntamente con el Responsable de Seguridad Informática, a fin de garantizar que se cumplan todas las Políticas y requerimientos de seguridad pertinentes.

Cuando corresponda, se verificará el hardware y software para garantizar su compatibilidad con los componentes de otros sistemas del Instituto.

2.1.3. Asesoramiento Especializado en Materia de Seguridad de la Información

El Responsable de Seguridad Informática será el encargado de coordinar los conocimientos y las experiencias disponibles en el Instituto a fin de brindar ayuda en la toma de decisiones en materia de seguridad.

Con el objeto de optimizar su gestión, se habilitará al Responsable de Seguridad Informática el contacto con las Unidades y/o Servicios de todas las Áreas del Instituto.

2.1.4. Revisión Independiente de la Seguridad de la Información

El Área de Auditoría Interna realizará revisiones independientes sobre la vigencia e implementación de la Política de Seguridad de la Información, a efectos de garantizar que las prácticas del Instituto reflejan adecuadamente sus disposiciones.

2.2. Seguridad Frente al Acceso por Parte de Terceros

2.2.1. Identificación de Riesgos del Acceso de Terceras Partes

Cuando exista la necesidad de otorgar acceso a terceras partes a información del Instituto, el Responsable de Seguridad Informática y el Propietario de la Información de que se trate, llevarán a cabo y documentarán una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta, entre otros aspectos:

- El tipo de acceso requerido (físico/lógico y a que recurso).
- Los motivos para los cuales se solicita el acceso.
- El valor de la información.
- Los controles empleados por la tercera parte.
- La incidencia de este acceso en la seguridad de la información del Instituto.

En todos los contratos cuyo objeto sea la prestación de servicios a título personal bajo cualquier modalidad jurídica que deban desarrollarse dentro del Instituto, se establecerán los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, restringiendo al mínimo necesario, los permisos a otorgar.

Se cita a modo de ejemplo:

a) Personal de mantenimiento y soporte de hardware y software.
b) Aseo, casino, guardia de seguridad y otros servicios de soporte tercerizados.
c) Pasantías y otras designaciones de corto plazo.
d) Consultores.

En ningún caso se otorgará acceso a terceros a la información, a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta tanto se hayan implementado los controles apropiados y se haya firmado un contrato o acuerdo que defina las condiciones para la conexión o el acceso.

2.2.2. Requerimientos de Seguridad en Contratos o Acuerdos con Terceros

Se revisarán los contratos o acuerdos existentes o que se efectúen con terceros, teniendo en cuenta la necesidad de aplicar los siguientes controles:

a) Cumplimiento de la Política de seguridad de la información del Instituto.
b) Protección de los activos del Instituto, incluyendo:
   - Procedimientos para proteger los bienes del Instituto, abarcando los activos físicos, la información y el software.
   - Procedimientos para determinar si ha ocurrido algún evento que comprometa los bienes, por ejemplo, debido a pérdida o modificación de datos.
   - Controles para garantizar la recuperación o destrucciónn de la información y los activos al finalizar el contrato o acuerdo, o en un momento convenido durante la vigencia del mismo.
   - Restricciones a la copia y divulgación de información.
c) Descripción de los servicios disponibles.
d) Nivel de servicio esperado y niveles de servicio aceptables.
e) Permiso para la transferencia de personal cuando sea necesario.
f) Obligaciones de las partes emanadas del acuerdo y responsabilidades legales.
g) Existencia de Derechos de Propiedad Intelectual.
h) Definiciones relacionadas con la protección de datos.
i) Acuerdos de control de accesos que contemplen:
   - Métodos de acceso permitidos, y el control y uso de identificadores únicos como identificadores de usuario y contraseñas de usuarios.
   - Proceso de autorización de accesos y privilegios de usuarios.
   - Requerimiento para mantener actualizada una lista de individuos autorizados a utilizar los servicios que han de implementarse y sus derechos y privilegios con respecto a dicho uso.
j) Definición de criterios de desempeño comprobables, de monitoreo y de presentación de informes.
k) Adquisición de derecho a auditar responsabilidades contractuales o

surgidas del acuerdo.

l) Establecimiento de un proceso para la resolución de problemas y en caso de corresponder disposiciones con relación a situaciones de contingencia.

m) Responsabilidades relativas a la instalación y al mantenimiento de hardware y software.

n) Estructura de dependencia y del proceso de elaboración y presentación de informes que contemple un acuerdo con respecto a los formatos de los mismos.

o) Proceso claro y detallado de administración de cambios.

p) Controles de protección física requeridos y los mecanismos que aseguren la implementación de los mismos.

q) Métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad.

r) Controles que garanticen la protección contra software malicioso.

s) Elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativos a la seguridad.

t) Relación entre proveedores y Subcontratistas.

2.3. Tercerización

2.3.1. Requerimientos de Seguridad en Contratos de Tercerización

Los contratos o acuerdos de tercerización total o parcial para la administración y control de sistemas de información, redes y/o ambientes de PC del Instituto, contemplarán además de los puntos especificados en "Requerimientos de Seguridad en Contratos o Acuerdos con Terceros", los siguientes aspectos:

a) Forma en que se cumplirán los requisitos legales aplicables.

b) Medios para garantizar que todas las partes involucradas en la tercerización, incluyendo los subcontratistas, están al corriente de sus responsabilidades en materia de seguridad.

c) Forma en que se mantendrá y comprobará la integridad y confidencialidad de los activos del Instituto.

d) Controles físicos y lógicos que se utilizarán para restringir y delimitar el acceso a la información sensible del Instituto.

e) Forma en que se mantendrá la disponibilidad de los servicios ante la ocurrencia de desastres.

f) Niveles de seguridad física que se asignarán al equipamiento tercerizado.

g) Derecho a la auditoria por parte del Instituto sobre los aspectos tercerizados en forma directa o a través de la contratación de servicios ad-hoc.

3. CLASIFICACIÓN Y CONTROL DE ACTIVOS

Generalidades

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

- **Recursos de información**: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, información archivada, etc.

- **Recursos de software:** software de aplicaciones, sistemas operativos, herramientas de desarrollo, utilitarios, etc.

- **Activos físicos:** equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, PABXs, máquinas de fax, contestadores automáticos), medios magnéticos (cintas, discos), otros equipos técnicos (relacionados con el suministro eléctrico, unidades de aire acondicionado), mobiliario, lugares de emplazamiento, etc.

- **Servicios:** servicios informáticos y de comunicaciones, utilitarios generales (calefacción, iluminación, energía eléctrica, etc.).

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

Frecuentemente, la información deja de ser sensible o crítica después de un cierto periodo de tiempo, por ejemplo, cuando la información se ha hecho pública. Estos aspectos deben tenerse en cuenta, puesto que la clasificación por exceso puede traducirse en gastos adicionales innecesarios para el Instituto.

Las pautas de clasificación deben prever y contemplar el hecho de que la clasificación de un ítem de información determinado no necesariamente debe mantenerse invariable por siempre, y que esta puede cambiar de acuerdo con una Política predeterminada. Se debe considerar la cantidad de categorías a definir para la clasificación dado que los esquemas demasiado complejos pueden tornarse engorrosos y antieconómicos o resultar poco prácticos.

La información adopta muchas formas, tanto en los sistemas informáticos como fuera de ellos.

Puede ser almacenada (en dichos sistemas o en medios portátiles), transmitida (a través de redes o entre sistemas) e impresa o escrita en papel. Cada una de estas formas debe contemplar todas las medidas necesarias para asegurar la confidencialidad, integridad y disponibilidad de la información.

Por último, la información puede pasar a ser obsoleta y por lo tanto, ser necesario eliminarla.

La destrucción de la información es un proceso que debe asegurar la confidencialidad de la misma hasta el momento de su eliminación.

Objetivo

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

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

Alcance

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

Vigencia

Esta Norma de Clasificación y Control de Activos entrará en vigencia a partir del **01 de Agosto de 2013.**

Responsabilidades

Los propietarios de la información son los encargados de clasificarla de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada, y de definir las funciones que deberán tener permisos de acceso a la información.

Debe existir un Encargado de Inventario, quien será responsable:

- Ejecutar las acciones administrativas relativas al uso de los bienes muebles.
- Operar el Sistema Informático de Control del Activo Fijo.
- Identificar todos los Activos de carácter Bien Mueble del Servicio.

- Elaborar y mantener un inventario de todos los Activos de carácter Bien Mueble del Instituto.
- Revisar y monitorear los incidentes relativos a la seguridad de dichos activos.
- Deberá desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado y manejo de la información en concordancia con esquema de clasificación establecido por el Instituto.

Política

3.1. Inventario de activos

Se identificarán los activos importantes asociados a cada sistema de información, sus respectivos propietarios y su ubicación, para luego elaborar un inventario con dicha información.

El mismo será actualizado ante cualquier modificación de la información registrada y revisada una vez al año (mediante Inventario General de Activo Fijo).

3.2. Clasificación de la información

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

A continuación se establece el criterio de clasificación de la información en función a cada una de las mencionadas características:

- Información que puede ser conocida y utilizada per todos los funcionarios del Instituto y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizado podría ocasionar riesgos o pérdidas leves para el Instituto, el Sector Público Nacional o terceros. RESERVADA — USO INTERNO.
- Información que solo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizado podría ocasionar pérdidas significativas al Instituto, al Sector Público Nacional o a terceros. RESERVADA – CONFIDENCIAL.
- Información que solo puede ser conocida y utilizada por un grupo muy reducido de funcionarios(as), generalmente de la alta Dirección del Instituto, y cuya divulgación o uso no autorizado podría ocasionar pérdidas graves al mismo, al Sector Público Nacional o a terceros. RESERVADA SECRETA.

- Integridad:
  - Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operatoria del Instituto.
  - Información cuya modificación no autorizada puede repararse aunque podría ocasionar pérdidas leves para el Instituto, el Sector Público Nacional o terceros.
  - Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas para el Instituto, el Sector Público Nacional o terceros.
  - Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves al Instituto, al Sector Público Nacional o a terceros.

3.3. Rotulado de la Información

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

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

4. SEGURIDAD DE 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, procedimientos, así como de los recursos humanos que utilizan dichos componentes.

En este sentido, es fundamental educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación de revista, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad. De la misma forma, es necesario definir las sanciones que se aplicarán en caso de incumplimiento.

La implementación de la Política de Seguridad de la Información tiene como meta minimizar la probabilidad de ocurrencia de incidentes. Es por ello que resulta necesario implementar un mecanismo que permita reportar las debilidades y los incidentes tan pronto como sea posible, a fin de subsanarlos y evitar eventuales replicaciones. Por lo tanto, es importante analizar las causas del incidente producido y aprender del mismo, a fin de corregir las prácticas existentes, que no pudieron prevenirlo, y evitarlo en el futuro.

Objetivo

Establecer mecanismos para el control adecuado de candidatos potenciales a cargos del Instituto, para reducir el riesgo de error humano, el mal uso de recursos, robo y fraude.

Reducir los daños ocasionados por incidentes de seguridad y mal funcionamiento.

Asegurar que los funcionarios estén conscientes de las amenazas de la seguridad de la información y que se comprometan con la Política General de Seguridad de la Información, en lo que a su trabajo normal se refiere.

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 reclutamiento de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado.

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

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

Alcance

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

Vigencia

Esta Norma de Seguridad de Recursos Humanos entrará en vigencia a partir del **01 de Agosto de 2013.**

Responsabilidades

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

El Comité de Seguridad de la Información será responsable de implementar los medios y canales necesarios para que el Responsable de Seguridad Informática maneje los reportes de incidentes y anomalías de los sistemas. Asimismo, dicho Comité, tomará conocimiento, efectuará el seguimiento de la investigación, controlará la evolución e impulsará la resolución de los incidentes relativos a la seguridad.

El Responsable del Área Legal participara en la confección del Compromiso de Confidencialidad a firmar por los empleados y terceros que desarrollen funciones en el Instituto, en el asesoramiento sobre las sanciones a ser aplicadas por incumplimiento de la presente Política y en el tratamiento de incidentes de seguridad que requieran de su intervención.

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

Política

4.1. Seguridad en la Definición de Puestos de Trabajo y la Asignación de Recursos

4.1.1. Incorporación de la Seguridad en los Puestos de Trabajo

Las funciones y responsabilidades en materia de seguridad serán incorporadas en la descripción de las responsabilidades de los puestos de trabajo.

Éstas incluirán las responsabilidades generales relacionadas con la implementación y el mantenimiento de la Política de Seguridad, y las responsabilidades especificas vinculadas a la protección de cada uno de los activos, o la ejecución de procesos o actividades de seguridad determinadas.

4.1.2. Control y Política del Personal

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

4.1.3. Compromiso de Confidencialidad

Como parte de sus 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 Instituto. La copia firmada del Compromiso deberá ser retenida en forma segura por el Área de Recursos Humanos u otra competente.

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

Se desarrollará un procedimiento para la suscripción del Compromiso de Confidencialidad donde se incluirán aspectos sobre:

a) Suscripción inicial del Compromiso por parte de la totalidad del personal.
b) Revisión del contenido del Compromiso (una vez cada dos años).
c) Método de resuscripción en caso de modificación del texto del Compromiso.

4.1.4. Términos y Condiciones de Empleo

Los términos y condiciones de empleo establecerán la responsabilidad del funcionario(a) 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 Instituto y del horario normal de trabajo.

Los derechos y obligaciones del empleado relativos a la seguridad de la información, por ejemplo en relación con las leyes de Propiedad Intelectual o la legislación de protección de datos, se encontraran aclarados e incluidos en los términos y condiciones de empleo.

4.2. Capacitación del Usuario

4.2.1. Formación y Capacitación en Materia de Seguridad de la Información

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

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

Las siguientes áreas serán encargadas de producir el material de capacitación

El personal que ingrese al Instituto recibirá el material, indicándosele el comportamiento esperado en lo que respecto 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.

4.3. Respuesta a Incidentes y Anomalías en Materia de Seguridad

4.3.1. Comunicación de Incidentes Relativos a la Seguridad

Los incidentes relativos a la seguridad serán comunicados a través de canales gerenciales apropiados tan pronto como sea posible.

Se establecerá un procedimiento formal de comunicación y de respuesta a incidentes, indicando la acción que ha de emprenderse al recibir un informe sobre incidentes.

Dicho procedimiento deberá contemplar que ante la detección de un supuesto incidente o violación de la seguridad, el Responsable de Seguridad Informática sea 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.

4.3.2. Comunicación de Debilidades en Materia de Seguridad

Los usuarios de servicios de información, al momento de tomar conocimiento directa o indirectamente acerca de una debilidad de seguridad, son responsables de registrar y comunicar las mismas al Responsable de Seguridad Informática. Se prohíbe a los usuarios la realización de pruebas para detectar y/o utilizar una supuesta debilidad o falla de seguridad.

4.3.3. Comunicación de Anomalías del Software

Se establecerán procedimientos para la comunicación de anomalías de software, los cuales deberán contemplar:

Registrar los síntomas del problema y los mensajes que aparecen en pantalla.

Establecer las medidas de aplicación inmediata ante la presencia de una anomalía.

Alertar inmediatamente al Responsable de Seguridad Informática o del Activo de que se trate.

Se prohíbe a los usuarios guitar el software que supuestamente tiene una anomalía, a menos que estén autorizados formalmente para hacerlo. La recuperación será realizada.

4.3.4. Procesos Disciplinarios

Se seguirá el proceso disciplinario formal contemplado en las normas estatutarias, y convencionales que rigen al personal de la Administración Pública Nacional, para los empleados que violen la Política, Normas y Procedimientos de Seguridad del Instituto.

5. SEGURIDAD FÍSICA Y AMBIENTAL

Generalidades

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

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

El establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles tendientes a proteger las instalaciones de procesamiento de información crítica o sensible del Instituto, de accesos físicos no autorizados.

El control de los factores ambientales permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio. Deben contemplarse tanto los riesgos en las instalaciones del Instituto como en instalaciones próximas a la sede del mismo que puedan interferir con las actividades.

El equipamiento donde se almacena información es susceptible de mantenimiento periódico, lo cual implica en ocasiones su traslado y permanencia fuera de las áreas protegidas del Instituto. Dichos procesos deben ser ejecutados bajo estrictas normas de seguridad y de preservación de la información almacenada en los mismos. Así también se tendrá en cuenta la aplicación de dichas normas en equipamiento perteneciente al Instituto pero situado físicamente fuera del mismo ("housing") así como en equipamiento ajeno que albergue sistemas y/o preste servicios de procesamiento de información al Instituto ("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 utilizados. Es por ello 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.

Objetivo

Prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones e información del Instituto.

Proteger el equipamiento de procesamiento de información crítica del Instituto ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados. Asimismo, contemplar la protección del mismo en su traslado y permanencia fuera de las áreas protegidas, por motivos de mantenimiento u otros. Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información del Instituto.

Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus labores habituales.

Proporcionar protección proporcional a los riesgos identificados.

Alcance

Esta Política se aplica a todos los recursos físicos relativos a los sistemas de información del Instituto: instalaciones, equipamiento, cableado, expedientes, medios de almacenamiento, etc.

Vigencia

Esta Norma de Seguridad Física y Ambiental entrará en vigencia a partir del **01 de Agosto de 2013.**

Responsabilidades

El Responsable de Seguridad Informática definirá junto con el Responsable del Área de Informática y los Propietarios de Información, según corresponda, las medidas de seguridad física y ambiental para el resguardo de los activos críticos, en función a un análisis de riesgos, y controlará su implementación. Asimismo, verificará el cumplimiento de las disposiciones sobre seguridad física y ambiental indicadas en el presente Capítulo.

El Responsable del Área de Informática asistirá al Responsable de Seguridad Informática en la definición de las medidas de seguridad a implementar en áreas protegidas, y coordinará su implementación. Asimismo, controlará el

mantenimiento del equipamiento informático de acuerdo a las indicaciones de proveedores tanto dentro como fuera de las instalaciones del Instituto.

Los Responsables de Unidades Organizativas definirán los niveles de acceso físico del personal del Instituto a las 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 Instituto cuando lo crean conveniente.

Todo el personal del Instituto 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

5.1. Perímetro de Seguridad Física

La protección física se Llevará a cabo mediante la creación de diversas barreras o medidas de control físicas alrededor de las sedes del Instituto y de las instalaciones de procesamiento de información.

El Instituto utilizará perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información, de suministro de energía eléctrica, de aire acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información. Un perímetro de seguridad está delimitado por una barrera, por ejemplo una pared, una puerta de acceso controlado por dispositivo de autenticación o un escritorio u oficina de recepción atendidos por personas. El emplazamiento y la fortaleza de cada barrera estarán definidas por el Responsable del Área de Informática con el asesoramiento del Responsable de Seguridad Informática, de acuerdo a la evaluación de riesgos efectuada.

Se considerarán e implementarán los siguientes lineamientos y controles, según corresponda:

a) Definir y documentar claramente el perímetro de seguridad.
b) Ubicar las instalaciones de procesamiento de información dentro del perímetro de un edificio o área de construcción físicamente sólida (por ejemplo no deben existir aberturas en el perímetro o áreas donde pueda producirse fácilmente una irrupción).
c) Las paredes externas del área deben ser sólidas y todas las puertas que comunican con el exterior deben estar adecuadamente protegidas contra accesos no autorizados, por ejemplo mediante mecanismos de control, vallas,

alarmas, cerraduras, etc.

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 registraran cada ingreso y egreso en forma precisa.
e) Extender las barreras físicas necesarias desde el piso (real) hasta el techo (real), a fin de impedir el ingreso no autorizado y la contaminación ambiental, por ejemplo por incendio, humedad e inundación.
f) Identificar claramente todas las puertas de incendio de un perímetro de seguridad.

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

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

5.2. Controles de Acceso Físico

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

a) Supervisar o inspeccionar a los visitantes a áreas protegidas y registrar la fecha y horario de su ingreso y egreso. Solo se permitirá el acceso mediando propósitos específicos y autorizados e instruyéndose al visitante en el momento de ingreso sobre los requerimientos de seguridad del área y los procedimientos de emergencia.

b) Controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas. Se utilizaran los siguientes controles de autenticación para autorizar y validar todos los accesos: (por ejemplo: personal de guardia con listado de personas habilitadas o por tarjeta magnética o inteligente y número de identificación personal (PIN), etc.). Se mantendrá un registro protegido para permitir auditar todos los accesos.

c) Implementar el uso de una identificación univoca visible para todo el personal del área protegida e instruirlo acerca de cuestionar la presencia de desconocidos no escoltados por personal autorizado y a cualquier persona que no exhiba una identificación visible.

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

e) Revisar los registros de acceso a las áreas protegidas. Esta tarea la realizará el área de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información.

5.3. Protección de Oficinas, Recintos e Instalaciones

Para la selección y el diseño de un área protegida se tendrá en cuenta la posibilidad de dario 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, par ejemplo, filtración de agua desde otras instalaciones.

5.4. Desarrollo de Tareas en Áreas Protegidas

Para incrementar la seguridad de las áreas protegidas, se establecen los siguientes controles y lineamientos adicionales. Esto incluye controles para el personal que trabaja en el área protegida, así coma 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 Elevan a cabo, solo si es necesario para el desarrollo de sus funciones.
b) Evitar la ejecución de trabajos par parte de terceros sin supervisión.
c) Bloquear físicamente e inspeccionar periódicamente las áreas protegidas desocupadas.
d) Limitar el acceso al personal del servicio de soporte externo a las áreas protegidas o a las instalaciones de procesamiento de información sensible. Este acceso, como el de cualquier otra persona ajena que requiera acceder al área protegida, será otorgado solamente cuando sea necesario y se encuentre autorizado y monitoreado. Se mantendrá un registro de todos los accesos de personas ajenas.
e) Pueden requerirse barreras y perímetros adicionales para controlar el acceso físico entre áreas con diferentes requerimientos de seguridad, y que están ubicadas dentro del mismo perímetro de seguridad.
f) Impedir el ingreso de equipos de computación móvil, fotográficos, de video, audio a cualquier otro tipo de equipamiento que registre información, a menos que hayan sido formalmente autorizadas por el Responsable de dicho

área o el Responsable del Área Informática y el Responsable de Seguridad Informática.

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

5.5. Aislamiento de las Áreas de Recepción y Distribución

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

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

a) Limitar el acceso a las áreas de depósito, desde el exterior de la sede del Instituto, solo al personal previamente identificado y autorizado.
b) Desafiar el área de depósito de manera tal que los suministros puedan ser descargados sin que el personal que realiza la entrega acceda a otros sectores del edificio.
c) Proteger todas las puertas exteriores del depósito cuando se abre la puerta interna.
d) Inspeccionar el material entrante para descartar peligros potenciales antes de ser trasladado desde el área de depósito hasta el lugar de uso.
e) Registrar el material entrante al ingresar al sitio pertinente.

5.6. Ubicación y Protección del Equipamiento y Copias de Seguridad

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, por:
   - Amenazas Potenciales Controles
   - Robo o hurto Incendio
   - Explosivos
   - Humo

- Inundaciones o filtraciones de agua (o falta de Suministro)
- Polvo
- Vibraciones
- Efectos Químicos
- Interferencia en el suministro de energía eléctrica (cortes de suministro, variación de tensión)
- Radiación electromagnética
- Derrumbes

e) 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.
f) Considerar asimismo el impacto de las amenazas citadas en el punto d) que tengan lugar en zonas próximas a la sede del Instituto.

5.7. Suministros de Energía

El equipamiento estará protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía estará de acuerdo con las especificaciones del fabricante o proveedor de cada equipo. Para asegurar la continuidad del suministro de energía, se contemplarán las siguientes medidas de control:

a) Disponer de múltiples enchufes o líneas de suministro para evitar un único punto de falla en el suministro de energía.

b) Contar con un suministro de energía interrumpible (UPS) para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas del Instituto. La determinación de dichas operaciones críticas, será el resultado del análisis de impacto realizado por el Responsable de Seguridad Informática 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. Deberá realizarse un análisis de impacto de las posibles consecuencias ante una interrupción prolongada del procesamiento, con el objeto de definir que componentes será necesario abastecer de energía alternativa. Dicho análisis será realizado por el Responsable de Seguridad Informática conjuntamente con los Propietarios de la Información. Se dispondrá de un adecuado suministro de combustible para garantizar que el generador pueda funcionar

por un periodo 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 proveer 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.

5.8. Seguridad del Cableado

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

a) Cumplir con los requisitos técnicos vigentes de la República.
b) Utilizar pisoducto o cableado embutido en la pared, siempre que sea posible, cuando corresponda a las instalaciones de procesamiento de información
c) Separar los cables de energía de los cables de comunicaciones para evitar interferencias.
d) Proteger el tendido del cableado troncal (backbone) mediante la utilización de ductos blindados.
e) Instalar conductos blindados y recintos o cajas con cerradura en los puntos terminales y de inspección.
f) Utilizar rutas o medios de transmisión alternativos.

5.9. Mantenimiento de Equipos

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

a) Someter el equipamiento a tareas de mantenimiento preventivo, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal del Responsables del Área Informática. El Área de Informática mantendrá un listado actualizado del equipamiento con el detalle de la frecuencia en que se realizará el mantenimiento preventivo.
b) Establecer que solo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.
c) Registrar todas las fallas supuestas o reales y todo el mantenimiento

preventivo y correctivo realizado.

d) Registrar el retiro de equipamiento de la sede del Instituto para su mantenimiento.
e) Eliminar la información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.

5.10. Seguridad de los Equipos de las Instalaciones

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

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

Se respetaran permanentemente las instrucciones del fabricante respecto del cuidado del equipamiento. Asimismo, se mantendrá una adecuada cobertura de seguro para proteger el equipamiento fuera del ámbito del Instituto, cuando sea conveniente.

5.11. Desafectación o Reutilización Segura de los Equipos

La información puede verse comprometida par una desafectación o una reutilización descuidada del equipamiento. Los medios de almacenamiento conteniendo material sensible, par ejemplo discos rígidos no removibles, serán físicamente destruidos o sobrescritos en forma segura en lugar de utilizar las funciones de borrado estándar, según corresponda.

5.12. Políticas de Escritorios y Pantallas Limpias.

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, perdida y dario de la información, tanto durante el horario normal de trabajo coma fuera del mismo.

Se aplicarán los siguientes lineamientos:

a) Almacenar bajo llave, cuando corresponda, los documentos en papel y los medios informáticos, en gabinetes y/u otro tipo de mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.
b) Guardar bajo llave la información sensible o crítica del Instituto (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) Desconectar de la red / sistema / servicio las computadoras personales, terminales e impresoras asignadas a funciones criticas, cuando están desatendidas. Las mismas deben ser protegidas mediante cerraduras de seguridad, contraseñas u otros controles cuando no están en uso (coma par ejemplo la utilización de protectores de pantalla con contraseña). Los responsables de cada área mantendrán un registro de las contraseñas o copia de las llaves de seguridad utilizadas en el sector a su cargo. Tales elementos se encontraran protegidos en sobre cerrado o caja de seguridad para impedir accesos no autorizados, debiendo dejarse constancia de todo acceso a las mismas, y de los motivos que llevaron a tal acción.
d) Proteger los puntos de recepción y envió de correo postal y las maquinas de fax no atendidas.
e) Bloquear las fotocopiadoras (o protegerlas de alguna manera del use no autorizado) fuera del horario normal de trabajo.
f) Retirar inmediatamente la información sensible o confidencial, una vez impresa.

5.13. Retiro de los Bienes

El equipamiento, la información y el software no serán retirados de la sede del Instituto sin autorización formal.

6. GESTIÓN DE COMUNICACIONES Y 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 Institutos, 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.

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

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

Objetivo

Es asegurar la operación correcta y segura de los medios de procesamiento de la información, establecer responsabilidades y procedimientos para la gestión y operación de todos los medios de procesamiento de la información.

Alcance

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

Vigencia

Esta Norma de Gestión de comunicaciones y operaciones entrará en vigencia a partir del **01 de Agosto de 2013.**

Responsabilidades

El Responsable de Seguridad Informática 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 las aplicaciones de Gobierno Electrónico.
- Definir procedimientos para el manejo de incidentes de seguridad y para la administración de los medios de almacenamiento.
- Controlar los mecanismos de distribución y difusión de información dentro del Instituto.
- 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 Instituto.
- 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. Gestión de Comunicaciones y Operaciones
- El Responsable del Área de Informática tendrá a su cargo lo siguiente:
- Controlar la existencia de documentación actualizada relacionada con los procedimientos de comunicaciones y 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.
- Desarrollar y verificar el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información r o los sistemas de comunicaciones, que permita tomar medidas correctivas.
- 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.

El Responsable de Seguridad Informática junto con el Responsable del Área de Informática y el Responsable del Área Legal del Instituto 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 Informática y el Responsable del Área de Informática, determinará los requerimientos para resguardar la información por la cual es responsable.

Asimismo, aprobará los servicios de mensajería autorizados para transportar la información cuando sea requerido, de acuerdo a su nivel de criticidad.

El Área de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, revisará las actividades que no hayan sido posibles segregar.

Asimismo, revisará los registros de actividades del personal operativo.

Política

6.1. Procedimientos y Responsabilidades Operativas

6.1.1. Documentación de los Procedimientos Operativos

Se documentarán y mantendrán actualizados los procedimientos operativos identificados en esta Política y sus cambios serán autorizados por el Responsable de Seguridad Informática.
Será el Área de Informática, la responsable de difundir los siguientes antecedentes e información:

- Los contactos de apoyo ante dificultades técnicas u operacionales inesperadas de sistemas informáticos;
- Las exigencias relativas al cumplimiento con las licencias de software y la prohibición del uso de software no autorizado;
- Para protegerse de los riesgos asociados a la obtención de archivos y software a través de la red de telecomunicaciones, o por otros medios, indicando qué medidas de protección se deberán aplicar. Para los efectos de reducir el riesgo de negligencia o mal uso deliberado de los sistemas deberán aplicarse políticas de segregación de funciones.
- Instrucciones para el manejo de errores u otras condiciones excepcionales que puedan surgir durante la ejecución de tareas.
- Instrucciones especiales para el manejo de "salidas", como el uso de papelería especial o la administración de salidas confidenciales,

incluyendo procedimientos para la eliminación segura de salidas fallidas de tareas.

- 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:
  - Instalación y mantenimiento de equipamiento para el procesamiento de información y comunicaciones.
  - Instalación y mantenimiento de las plataformas de procesamiento.
  - Monitoreo del procesamiento y las comunicaciones.
  - Inicio y finalización de la ejecución de los sistemas.
  - Programación y ejecución de procesos.
  - Gestión de servicios.
  - Resguardo de información.
  - Gestión de incidentes de seguridad en el ambiente de procesamiento y comunicaciones.
  - Reemplazo o cambio de componentes del ambiente de procesamiento y comunicaciones.
  - Uso del correo electrónico.

6.1.2. Control de Cambios en las Operaciones

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 Informática controlará que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de los mismos ni de la información que soportan. El Responsable del Área de Informática 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) Identificación y registro de cambios significativos.
b) Evaluación del posible impacto de dichos cambios.
c) Aprobación formal de los cambios propuestos.
d) Planificación del proceso de cambio.
e) Prueba del nuevo escenario.
f) Comunicación de detalles de cambios a todas las personas pertinentes.
g) Identificación de las responsabilidades por la cancelación de los cambios fallidos y la recuperación respecto de los mismos.

6.1.3. Procedimientos de Manejo de Incidentes

Se establecerán funciones y procedimientos de manejo de incidentes garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a Comunicación de Incidentes Relativos a la Seguridad). Se deben considerar los siguientes ítems:

a) Contemplar y definir todos los tipos probables de incidentes relativos a seguridad, incluyendo:
   - Fallas operativas
   - Código malicioso
   - Intrusiones
   - Fraude informático
   - Error humano
   - Catástrofes naturales
b) Comunicar los incidentes a través de canales gerenciales 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):
   - Definición de las primeras medidas a implementar
   - Análisis e identificación de la causa del incidente.
   - Planificación e implementación de soluciones para evitar la repetición del mismo, si fuera necesario.
   - Comunicación con las personas afectadas o involucradas con la recuperación, del incidente.
   - Notificación de la acción a la autoridad y/u Institutos pertinentes.
d) Registrar pistas de auditoría y evidencia similar para:
   - Análisis de problemas internos.
   - Uso como evidencia en relación con una probable violación contractual o infracción normativa, o en marco de un proceso judicial (Ver 12.1. Cumplimiento de Requisitos Legales).
   - Negociación de compensaciones por parte de los proveedores de software y de servicios.
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:
   - Acceso a los sistemas y datos existentes sólo al personal claramente identificado y autorizado.
   - Documentación de todas las acciones de emergencia emprendidas en forma detallada.
   - Comunicación de las acciones de emergencia al titular de la Unidad Organizativa y revisión de su cumplimiento.
   - Constatación de la integridad de los controles y sistemas del Instituto en un plazo mínimo.

En los casos en los que se considere necesario, se solicitará la participación del Responsable del Área Legal del Instituto en el tratamiento de incidentes de seguridad ocurridos.

6.1.4. Separación de Funciones

Se separará la gestión o ejecución de ciertas tareas o áreas de responsabilidad, a fin de reducir el riesgo de modificaciones no autorizadas o mal uso de la información 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, se implementarán controles como:
- Monitoreo de las actividades.
- Registros de auditoría y control periódico de los mismos.
- Supervisión por parte del Área de Auditoría Interna o en su defecto quien sea propuesto a tal efecto, siendo independiente al área que genera las actividades auditadas.

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:
- Separar actividades que requieren connivencia para defraudar, por ejemplo efectuar una orden de compra y verificar que la mercadería fue recibida.
- Diseñar controles, si existe peligro de connivencia de manera tal que dos o más personas estén involucradas, reduciendo la posibilidad de conspiración.

6.1.5. Separación entre Instalaciones de Desarrollo e Instalaciones Operativas

Los ambientes de desarrollo, prueba y operaciones, 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:
- Ejecutar el software de desarrollo y de operaciones, en diferentes ambientes de operaciones, equipos, o directorios.
- Separar las actividades de desarrollo y prueba, en entornos diferentes.

- Impedir el acceso a los compiladores, editores y otros utilitarios del sistema en el ambiente operativo, cuando no sean indispensables para el funcionamiento del mismo.
- 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.
- Definir propietarios de la información para cada uno de los ambientes de procesamiento existentes.
- El personal de desarrollo no tendrá acceso al ambiente operativo. De ser extrema dicha necesidad, se establecerá un procedimiento de emergencia para la autorización, documentación y registro de dichos accesos.

Para el caso que no puedan mantener separados los distintos ambientes en forma física, deberán implementarse los controles indicados en el punto "Separación de Funciones".

6.1.6. Gestión de Instalaciones Externas

En el caso de externalizar la administración de las instalaciones de procesamiento, se acordarán controles con el proveedor del servicio y se incluirán en el contrato, contemplando las siguientes cuestiones específicas:

- Identificar las aplicaciones sensibles o críticas que convenga retener en el Instituto.
- Obtener la aprobación de los propietarios de aplicaciones específicas.
- Identificar las implicancias para la continuidad de los planes de las actividades del Instituto.
- Especificar las normas de seguridad y el proceso de medición del cumplimiento.
- Asignar funciones específicas y procedimientos para monitorear todas las actividades de seguridad.
- Definir las funciones y procedimientos de comunicación y manejo de incidentes relativos a la seguridad.

Dichas consideraciones deberán ser acordadas entre el Responsable de Seguridad Informática, el Responsable del Área de Informática y el Responsable del Área Legal del Instituto.

6.2. Planificación y Aprobación de Sistemas

6.2.1. Planificación de la Capacidad

El Responsable del Área de Informática, o el personal que éste designe, efectuará el monitoreo de las necesidades de capacidad de los sistemas

en operación y proyectar las futuras demandas, 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 Instituto para el período estipulado de vida útil de cada componente. Asimismo, informará las necesidades detectadas a las autoridades competentes para que puedan identificar y evitar potenciales cuellos de botella, que podrían plantear una amenaza a la seguridad o a la continuidad del procesamiento, y puedan planificar una adecuada acción correctiva.

6.2.2. Aprobación del Sistema

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

- Verificar el impacto en el desempeño y los requerimientos de capacidad de las computadoras.
- Garantizar la recuperación ante errores.
- Preparar y poner a prueba los procedimientos operativos de rutina según normas definidas.
- Garantizar la implementación de un conjunto acordado de controles de seguridad.
- Confeccionar disposiciones relativas a la continuidad de las actividades del Instituto.
- Asegurar que la instalación del nuevo sistema no afectará negativamente los sistemas existentes, especialmente en los períodos pico de procesamiento.
- Considerar el efecto que tiene el nuevo sistema en la seguridad global del Instituto.
- Disponer la realización de entrenamiento en la operación y/o uso de nuevos sistemas.

6.3. Protección Contra Software Malicioso

6.3.1. Controles Contra Software Malicioso

El Responsable de Seguridad Informática definirá controles de detección y prevención para la protección contra software malicioso. El Responsable del Área de Informática, o el personal designado por éste, implementarán dichos controles.

El Responsable de Seguridad Informática desarrollará procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.

Estos controles deberán considerar las siguientes acciones:

- Prohibir el uso de software no autorizado por el Instituto
- Redactar procedimientos para evitar los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas, o por cualquier otro medio, señalando las medidas de protección a tomar.
- Instalar y actualizar periódicamente software de detección y reparación de virus, examinado computadoras y medios informáticos, como medida precautoria y rutinaria.
- 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).
- Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos del Instituto, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.
- 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.
- Redactar procedimientos para verificar toda la información relativa a software malicioso, garantizando que los boletines de alerta sean exactos e informativos.
- Concientizar al personal acerca del problema de los falsos virus y de cómo proceder frente a los mismos.

6.4. Mantenimiento

6.4.1. Resguardo de la Información

El Responsable del Área de Informática y el de Seguridad Informática junto al Responsable del Área de Informática y los Propietarios de Información determinarán los requerimientos para resguardar cada software o dato en función de su criticidad. En base a ello, se definirá y documentará un esquema de resguardo de la información.

El Responsable del Área de Informática 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 Instituto. Los sistemas de resguardo deberán probarse

periódicamente, asegurándose que cumplen con los requerimientos de los planes de continuidad de las actividades del Instituto, según el punto "Ensayo, Mantenimiento y Reevaluación de los Planes de Continuidad del Instituto." de esta política.

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

- 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.
- 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 a lo indicado por el proveedor, y asegurando la destrucción de los medios desechados.
- Almacenar en una ubicación remota copias recientes de información de resguardo junto con registros exactos y completos de las mismas y los procedimientos documentados de restauración, a una distancia suficiente como para evitar daños provenientes de un desastre en el sitio principal. Se deberán retener al menos tres generaciones o ciclos de información de resguardo para la información y el software esenciales para el Instituto. 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 requisitos legales a los que se encuentre sujeta.
- 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.
- Probar periódicamente los medios de resguardo.
- Verificar y probar periódicamente los procedimientos de restauración garantizando su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos.

6.4.2. Registro de Actividades del Personal Operativo

El Responsable del Área de Informática asegurará el registro de las actividades realizadas en los sistemas, incluyendo según corresponda:

- Tiempos de inicio y cierre del sistema.
- Errores del sistema y medidas correctivas tomadas.
- Intentos de acceso a sistemas, recursos o información crítica o acciones restringidas.
- Ejecución de operaciones críticas.
- Cambios a información crítica.

6.4.3. Registro de Fallas

El Responsable del Área de Informática desarrollará y verificará el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas.

Se registrarán las fallas comunicadas, debiendo existir reglas claras para el manejo de las mismas, con inclusión de:

- Revisión de registros de fallas para garantizar que las mismas fueron resueltas satisfactoriamente.
- Revisión de medidas correctivas para garantizar que los controles no fueron comprometidos, y que las medidas tomadas fueron autorizadas.
- Documentación de la falla con el objeto de prevenir su repetición o facilitar su resolución en caso de reincidencia.

6.5. Administración de la Red

6.5.1. Controles de Redes

El Servicio deberá asegurar la protección de la información en redes y la protección de la infraestructura de soporte.

El Área de informática implementará controles para asegurar la seguridad de la información en las redes, y proteger los servicios conectados de accesos no autorizados.

En particular, se consideraran los siguientes ítems:

- La responsabilidad operacional para las redes se deberá separar de las operaciones de cómputo;
- Se establecerán las responsabilidades y procedimientos para la gestión del equipo remoto, incluyendo el equipo en las áreas del usuario;
- Se establecerán controles especiales para salvaguardar la confidencialidad y la integridad de la data que pasa a través de la red corporativa;
- Se deberán aplicar registros de ingreso y monitoreo apropiados para permitir el registro de las acciones de seguridad relevantes;
- Las actividades de gestión deberán estar estrechamente coordinadas para optimizar el servicio al Instituto y para asegurar que los controles sean aplicados consistentemente a través de la infraestructura de procesamiento de la información;
- Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información.

6.6. Administración y Seguridad de los Medios de Almacenamiento

6.6.1. Administración de Medios Informáticos Removibles

El Responsable del Área de Informática, con la asistencia del Responsable de Seguridad Informática, implementará procedimientos para la administración de medios informáticos removibles, CDs, DVDs, cintas. Se deberán considerar las siguientes acciones para la implementación de los procedimientos:

- Se deberá establecer los procedimientos para identificar los ítems que requieren de una eliminación segura;
- Requerir autorización para retirar cualquier medio del Instituto y realizar un control de todos los retiros a fin de mantener un registro de auditoría.
- El Comité de Seguridad del Servicio establecerá los procedimientos para el manejo y almacenaje de información para proteger esta información de una divulgación no-autorizada o mal uso.

6.6.2. Eliminación de Medios de Información

El Responsable del Área de Informática, junto con el Responsable de Seguridad Informática definirá procedimientos para la eliminación segura de los medios de información respetando la normativa vigente.

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

- Documentos en papel.
- Voces u otras grabaciones.
- Papel carbónico.
- Informes de salida.
- Cintas de impresora de un solo uso.
- Cintas magnéticas.
- Discos o casetes removibles.
- Medios de almacenamiento óptico (todos los formatos incluyendo todos los medios de distribución de software del fabricante o proveedor).
- Listados de programas.
- Datos de prueba.
- Documentación del sistema.

Asimismo, se debe considerar que podría ser más eficiente disponer que todos los medios sean recolectados y eliminados de manera segura, antes que intentar separar los ítems sensibles.

6.6.3. Procedimientos de Manejo de la Información

Se definirán procedimientos para el manejo y almacenamiento de la información de acuerdo a la clasificación establecida en la Clasificación y Control de Activos.

En los procedimientos se contemplarán las siguientes acciones:
- Incluir en la protección a documentos, sistemas informáticos, redes, computación móvil, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general, multimedia, servicios e instalaciones postales, uso de máquinas de fax y cualquier otro ítem potencialmente sensible.
- Restringir el acceso solo al personal debidamente autorizado
- Mantener un registro formal de los receptores autorizados de datos
- Garantizar que los datos de entrada son completos, que el procesamiento se lleva a cabo correctamente y que se valida las salidas.
- Proteger los datos en espera ("colas").
- Conservar los medios de almacenamiento en un ambiente que concuerde con las especificaciones de los fabricantes o proveedores.

6.6.4. Seguridad de la Documentación del Sistema

La documentación del sistema puede contener información sensible, por lo que se considerarán los siguientes recaudos para su protección:
- Almacenar la documentación del sistema en forma segura.
- Restringir el acceso a la documentación del sistema al personal estrictamente necesario. Dicho acceso será autorizado por el Propietario de la Información relativa al sistema.

6.7. Intercambios de Información y Software

6.7.1. Acuerdos de Intercambio de Información y Software

Cuando se realicen acuerdos entre organizaciones para el intercambio de información y software, se especificarán el grado de sensibilidad de la información del Instituto involucrada y las consideraciones de seguridad sobre la misma. Se tendrán en cuenta los siguientes aspectos:
- Responsabilidades gerenciales por el control y la notificación de transmisiones, envíos y recepciones.
- Procedimientos de notificación de emisión, transmisión, envío y recepción.
- Normas técnicas para el empaquetado y la transmisión.
- Pautas para la identificación del prestador del servicio de correo.

- Responsabilidades y obligaciones en caso de pérdida de datos.
- 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.
- Términos y condiciones de la licencia bajo la cual se suministra el software.
- Información sobre la propiedad de la información suministrada y las condiciones de su uso.
- Normas técnicas para la grabación y lectura de la información y del software.
- Controles especiales que puedan requerirse para proteger ítems sensibles, (claves criptográficas, etc.).

6.7.2. Seguridad de los Medios en Tránsito

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

- 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.
- Suficiente embalaje para envío de medios a través de servicios postales o de mensajería, siguiendo las especificaciones de los fabricantes o proveedores.
- 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:
  - Uso de recipientes cerrados.
  - Entrega en mano.
  - Embalaje a prueba de apertura no autorizada (que revele cualquier intento de acceso).
  - En casos excepcionales, división de la mercadería a enviar en más de una entrega y envío por diferentes rutas.

6.7.3. Seguridad del Gobierno Electrónico

El Responsable de Seguridad Informática verificará que los procedimientos de aprobación de Software del punto "Aprobación del Sistema" incluyan los siguientes aspectos para las aplicaciones de Gobierno Electrónico:

a) **Autenticación**: Nivel de confianza recíproca suficiente sobre la identidad del usuario y el Instituto.

b) **Autorización**: Niveles de Autorización adecuados para establecer disposiciones, emitir o firmar documentos clave, etc. Forma de comunicarlo al otro participante de la transacción electrónica.
c) **Procesos de oferta y contratación pública**: Requerimientos de confidencialidad, integridad y prueba de envío y recepción de documentos clave y de no repudio de contratos.
d) **Trámites en línea**: Confidencialidad, integridad y no repudio de los datos suministrados con respecto a trámites y presentaciones ante el Estado y confirmación de recepción.
e) **Verificación**: Grado de verificación apropiado para constatar la información suministrada por los usuarios.
f) **Cierre de la transacción**: Forma de interacción más adecuada para evitar fraudes.
g) **Protección a la duplicación**: Asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario.
h) **No repudio**: Manera de evitar que una entidad que haya enviado o recibido información alegue que no la envió o recibió.
i) **Responsabilidad**: Asignación de responsabilidades ante el riesgo de eventuales presentaciones, tramitaciones o transacciones fraudulentas.

Las consideraciones mencionadas se implementarán mediante la aplicación de las técnicas criptográficas enumeradas en el punto "Política de Utilización de Controles Criptográficos" y tomando en cuenta el cumplimiento de los requisitos legales emanados de toda la normativa vigente.

Se darán a conocer a los usuarios, los términos y condiciones aplicables.

6.7.4. Seguridad del Correo Electrónico

6.7.4.1. Riesgos de Seguridad

Se implementarán controles para reducir los riesgos de incidentes de seguridad en el correo electrónico, contemplando:
a) La vulnerabilidad de los mensajes al acceso o modificación no autorizados o a la negación de servicio.
b) La posible intercepción y el consecuente acceso a los mensajes en los medios de transferencia que intervienen en la distribución de los mismos.
c) Las posibles vulnerabilidades a errores, por ejemplo, consignación incorrecta de la dirección o dirección errónea, y la confiabilidad y disponibilidad general del servicio.

d) La posible recepción de código malicioso en un mensaje de correo, el cual afecte la seguridad de la terminal receptora o de la red a la que se encuentra conectada.
e) El impacto de un cambio en el medio de comunicación en los procesos del Instituto.
f) Las consideraciones legales, como la necesidad potencial de contar con prueba de origen, envío, entrega y aceptación.
g) Las implicancias de la publicación externa de listados de personal, accesibles al público.
h) El acceso de usuarios remotos a las cuentas de correo electrónico.
i) El uso inadecuado por parte del personal.

6.7.4.2. Política de Correo Electrónico

El Responsable de Seguridad Informática junto con el Responsable del Área de Informática definirán y documentarán normas y procedimientos claros con respecto al uso del correo electrónico, que incluya al menos los siguientes aspectos:

a) Protección contra ataques al correo electrónico, por ejemplo virus, intercepción, etc.
b) Protección de archivos adjuntos de correo electrónico.
c) Uso de técnicas criptográficas para proteger la confidencialidad e integridad de los mensajes electrónicos
d) Retención de mensajes que, si se almacenaran, pudieran ser usados en caso de litigio.
e) Controles adicionales para examinar mensajes electrónicos que no pueden ser autenticados.
f) Aspectos operativos para garantizar el correcto funcionamiento del servicio (ej.: tamaño máximo de información transmitida y recibida, cantidad de destinatarios, tamaño máximo del buzón del usuario, etc.).
g) Definición de los alcances del uso del correo electrónico por parte del personal del Instituto.
h) Potestad del Establecimiento para auditar los mensajes recibidos o emitidos por los servidores del Instituto, lo cual se incluirá en el "Compromiso de Confidencialidad"

Estos dos últimos puntos deben ser leídos a la luz de las normas vigentes que no sólo prohíben a los funcionarios (as) a hacer uso indebido o con fines particulares del patrimonio estatal sino que también imponen la obligación de usar los bienes y recursos del estado con los fines autorizados y de manera racional, evitando su abuso, derroche o desaprovechamiento.

Entender al correo electrónico como una herramienta más de trabajo provista al empleado a fin de ser utilizada conforme el uso al cual está destinada, faculta al empleador a implementar sistemas de controles destinados a velar por la protección y el buen uso de sus recursos.

Esta facultad, sin embargo, deberá ejercerse salvaguardando la dignidad del trabajador y su derecho a la intimidad. Por tal motivo, el Instituto debe informar claramente a sus funcionarios (as): Cuál es el uso que el Instituto espera que los empleados hagan del correo electrónico provisto por el Instituto; y bajo qué condiciones los mensajes pueden ser objeto de control y monitoreo.

6.7.5. Seguridad de los Sistemas Electrónicos de Oficina

Se controlarán los mecanismos de distribución y difusión tales como documentos, computadoras, computación móvil, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general, 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 Instituto, 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 Instituto, 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 trabaja en proyectos sensibles.
e) La aptitud del sistema para dar soporte a las aplicaciones del Instituto, 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 funcionarios (as) del Instituto 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.

6.7.6. Sistemas de Acceso Público

Se tomarán recaudos para la protección de la integridad de la información publicada electrónicamente, a fin de prevenir la modificación no autorizada que podría dañar la reputación del Instituto que emite la publicación. Es posible que la información de un sistema de acceso público, por ejemplo la información en un servidor Web accesible por Internet, deba cumplir conciertas 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 deberán prever que:
a) La información se obtenga, procese y proporcione de acuerdo a la normativa vigente, en especial la Ley de Protección de Datos Personales.
b) La información que se ingresa al sistema de publicación, o aquella que procesa el mismo, sea procesada en forma completa, exacta y oportuna.
c) La información sensible sea protegida durante el proceso de recolección y su almacenamiento.
d) El acceso al sistema de publicación no permita el acceso accidental a las redes a las cuales se conecta el mismo.
e) Se registre al responsable de la publicación de información en sistemas de acceso público.
f) La información se publique teniendo en cuenta las normas establecidas al respecto.
g) Se garantice la validez y vigencia de la información publicada.

7. 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.

La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto es necesario concientizar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

Objetivo

Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.

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

Controlar la seguridad en la conexión entre la red del Instituto 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 Instituto, 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.

Responsabilidades

El Responsable de Seguridad Informática estará a cargo de:

- Definir normas y 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 a un estándar preestablecido.
- Definir pautas de utilización de Internet para todos los usuarios.
- Participar en la definición de normas y procedimientos de seguridad a implementar en el ambiente informático (ej.: sistemas operativos, servicios de red, enrutadores o gateways, etc.) 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, limitación del horario de conexión, registro de eventos, protección de puertos, subdivisión de redes, control de conexiones a la red, control de ruteo de red, etc.
- 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 riesgos a los que se expone la información y los componentes del ambiente informático que sirven de soporte a la misma.

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 a ser implementados en cada caso.
- Definir los eventos y 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.
- Definir un cronograma de depuración de registros de auditoría en línea.

Los Propietarios de la Información junto con el Área de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, definirán un cronograma de depuración de registros en línea en función a normas vigentes y a sus propias necesidades.

Los Responsables de las Unidades Organizativas, junto con el Responsable de Seguridad Informática, 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 Responsable del Área de Informática 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 a lo definido por los propietarios de la información, así como la depuración de los mismos.
- 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 Control de Accesos
- 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 al pedido formal correspondiente.

- Efectuar un control de los registros de auditoría generados por los sistemas operativos y de comunicaciones.

Política

7.1. Requerimientos para el Control de Acceso

7.1.1. Política de Control de Accesos

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

a) Identificar los requerimientos de seguridad de cada una de las aplicaciones.
b) Identificar toda la información relacionada con las aplicaciones.
c) Establecer criterios coherentes entre esta Política de Control de Acceso y la Política de Clasificación de Información de los diferentes sistemas y redes.
d) 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 disponibles.

7.2. Administración de Accesos de Usuarios

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

7.2.1. Registro de Usuarios

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

a) Utilizar identificadores de usuario únicos, de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo empleado. El uso de identificadores grupales sólo debe ser permitido cuando sean convenientes para el trabajo a desarrollar debido a razones operativas.

b) Verificar que el usuario tiene autorización del Propietario de la Información para el uso del sistema, base de datos o servicio de información.
c) Verificar que el nivel de acceso otorgado es adecuado para el propósito de la función del usuario y es coherente con la Política de Seguridad del Instituto, por ejemplo que no compromete la separación de tareas.
d) Entregar a los usuarios un detalle escrito de sus derechos de acceso.
e) Requerir que los usuarios firmen declaraciones señalando que comprenden y aceptan las condiciones para el acceso.
f) Garantizar que los proveedores de servicios no otorguen acceso hasta que se hayan completado los procedimientos de autorización.
g) Mantener un registro formal de todas las personas registradas para utilizar el servicio.
h) Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización, se desvincularon del Instituto o sufrieron la pérdida/robo de sus credenciales de acceso.
i) Garantizar que los identificadores de usuario redundantes no se asignen a otros usuarios.
j) Incluir cláusulas en los contratos de personal y de servicios que especifiquen sanciones si el personal o los agentes que prestan un servicio intentan accesos no autorizados.

7.2.2. Administración de Privilegios

Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente.

Los sistemas multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal. Se deben tener en cuenta los siguientes pasos:
a) Identificar los privilegios asociados a cada producto del sistema, por ejemplo sistema operativo, sistema de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los productos.
b) Asignar los privilegios a individuos sobre la base de la necesidad de uso y evento por evento, por ejemplo el requerimiento mínimo para su rol funcional.

c) Mantener un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no deben ser otorgados hasta que se haya completado el proceso formal de autorización.
d) Establecer un período de vigencia para el mantenimiento de los privilegios (en base a la utilización que se le dará a los mismos) luego del cual los mismos serán revocados.
e) Promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.

Los Propietarios de Información serán los encargados de aprobar la asignación de privilegios a usuarios y solicitar su implementación, lo cual será supervisado por el Responsable de Seguridad Informática.

7.2.3. Administración de Contraseñas de Usuario

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

a) Requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto y las contraseñas de los grupos de trabajo exclusivamente entre los miembros del grupo.
b) Garantizar que 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 deben dar acuse de recibo cuando la reciban.
d) Almacenar las contraseñas sólo en sistemas informáticos protegidos.

8. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SEGURIDAD DE LOS SISTEMAS

Generalidades

El desarrollo y mantenimiento de las aplicaciones es un punto crítico de la seguridad.

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

Dado que los analistas y programadores tienen el conocimiento total 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, 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.

Objetivo

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

Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.

Definir los métodos de protección de la información crítica o sensible.

Alcance

Esta Política se aplica a todos los sistemas informáticos, tanto 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 Instituto en donde residan los desarrollos mencionados.

Responsabilidades

El Responsable de Seguridad Informática junto con el Propietario de la Información y el Área de Auditoría Interna, definirán los controles a ser implementados en los sistemas desarrollados internamente o por terceros, en función de una evaluación previa de riesgos.

El Responsable de Seguridad Informática, junto con el Propietario de la Información, serán quienes definan en función a la criticidad de la información, los requerimientos de protección mediante métodos criptográficos. Luego, el Responsable de Seguridad Informática definirá junto con el Responsable del Área de Informática, los métodos de encriptación a ser utilizados.

Asimismo, el Responsable de Seguridad Informática 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.

El Responsable del Área de Informática, propondrá para su aprobación por parte del superior jerárquico que corresponda, la asignación de funciones de "implementador" y "administrador de programas fuentes" al personal de su área que considere adecuado, cuyas responsabilidades se detallan en el presente capítulo. Asimismo, verificará el cumplimiento de las definiciones establecidas sobre los controles y las medidas de seguridad a ser incorporadas a los sistemas.

El Área de Informática propondrá quiénes realizarán la administración de las técnicas criptográficas y claves.

El Responsable del Área Administrativa 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. El Responsable del Área Legal participará en dicha tarea.

Política

8.1. Requerimientos de Seguridad de los Sistemas

8.1.1. Análisis y Especificaciones de los Requerimientos de Seguridad

Esta Política se implementa para incorporar seguridad a los sistemas de información (propios o de terceros) y a las mejoras o actualizaciones que se les incorporen.

Los requerimientos para nuevos sistemas o mejoras a los existentes especificarán la necesidad de controles. Estas especificaciones deben considerar los controles automáticos a incorporar al sistema, como así también controles 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. En esta tarea deben participar las áreas usuarias, de sistemas, de seguridad informática y auditoría, especificando y aprobando los controles automáticos a incorporar al sistema y las necesidades de controles manuales complementarios. Las áreas involucradas podrán solicitar certificaciones y evaluaciones independientes para los productos a utilizar.
b) Evaluar los requerimientos de seguridad y los controles requeridos, teniendo en cuenta que éstos deben ser proporcionales en costo y esfuerzo al valor del bien que se quiere proteger y al daño potencial que pudiera ocasionar a las actividades realizadas.
c) Considerar que los controles introducidos en la etapa de diseño, son significativamente menos costosos de implementar y mantener que aquellos incluidos durante o después de la implementación.

8.2. Seguridad en los Sistemas de Aplicación

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

a) La validación de datos de entrada.
b) El procesamiento interno.
c) La autenticación de mensajes (interfaces entre sistemas)
d) La validación de datos de salida.

8.2.1. Validación de Datos de Entrada

Se definirá un procedimiento que durante la etapa de diseño, especifique controles que aseguren la validez de los datos ingresados, tan cerca del punto de origen como sea posible, controlando también datos permanentes y tablas de parámetros.

Este procedimiento considerará los siguientes controles:
a) Control de secuencia.
b) Control de monto límite por operación y tipo de usuario.
c) Control del rango de valores posibles y de su validez, de acuerdo a criterios predeterminados.
d) Control de paridad.
e) Control contra valores cargados en las tablas de datos.
f) Controles por oposición, de forma tal que quien ingrese un dato no pueda autorizarlo y viceversa.

Por otra parte, se llevarán a cabo las siguientes acciones:
a) Se definirá un procedimiento para realizar revisiones periódicas de contenidos de campos claves o archivos de datos, definiendo quién lo realizará, en qué forma, con qué método, quiénes deberán ser informados del resultado, etc.
b) Se definirá un procedimiento que explicite las alternativas a seguir para responder a errores de validación en un aplicativo.
c) Se definirá un procedimiento que permita determinar las responsabilidades de todo el personal involucrado en el proceso de entrada de datos.

8.2.2. Controles de Procesamiento Interno

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

Para ello se implementarán:
a) Procedimientos que permitan identificar el uso y localización en los aplicativos, de funciones de incorporación y eliminación que realizan cambios en los datos.
b) Procedimientos que establezcan los controles y verificaciones necesarios para prevenir la ejecución de programas fuera de secuencia o cuando falle el procesamiento previo.
c) Procedimientos que establezcan la revisión periódica de los registros de auditoría de forma de detectar cualquier anomalía en la ejecución de las transacciones.

d) Procedimientos que realicen la validación de los datos generados por el sistema.
e) Procedimientos que verifiquen la integridad de los datos y del software cargado o descargado entre computadoras.
f) Procedimientos que controlen la integridad de registros y archivos.
g) Procedimientos que verifiquen la ejecución de los aplicativos en el momento adecuado.
h) Procedimientos que aseguren el orden correcto de ejecución de los aplicativos, la finalización programada en caso de falla, y la detención de las actividades de procesamiento hasta que el problema sea resuelto.

9. GESTIÓN DE CONTINUIDAD DEL NEGOCIO

Generalidades

La administración de la continuidad del negocio es un proceso crítico que debe involucrar a todos los niveles del Instituto.

Objetivo

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

Mantener la integridad y la disponibilidad de los activos de información y reducir riesgos de perdida en el caso de falla de sistemas, desastre, atenuar las consecuencias eventuales y asegurar la reanudación oportuna de las operaciones indispensables.

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

Maximizar la efectividad de las operaciones de contingencia del Instituto con el establecimiento de planes que incluyan al menos las siguientes etapas:

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

Asegurar la coordinación con el personal del Instituto y los contactos externos 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 que involucran información sensible el Instituto de Neurocirugía.

Vigencia

Esta Norma de Gestión de Continuidad del Negocio entrará en vigencia a partir del **01 de Agosto de 2013.**

Responsabilidades

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

Los Propietarios de la Información y el Responsable de Seguridad Informática cumplirán las siguientes funciones:

- Identificar las amenazas que puedan ocasionar interrupciones de los procesos y/o las actividades del Instituto.
- 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 Establecimiento.
- Elaborar los planes de contingencia necesarios para garantizar la continuidad de las actividades del Establecimiento.

Los Responsables de Procesos revisarán periódicamente los planes bajo su incumbencia, como así también identificar cambios en las disposiciones relativas a las actividades del Instituto aún no reflejadas 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.

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

- Identificar y priorizar los procesos críticos de las actividades del Instituto.
- Asegurar que todos los integrantes del Instituto comprendan los riesgos que la misma enfrenta, en términos de probabilidad de ocurrencia e impacto de posibles amenazas, así como los efectos que una interrupción puede tener en la actividad del Instituto.
- Elaborar y documentar una estrategia de continuidad de las actividades del Instituto consecuente con los objetivos y prioridades acordados.
- Proponer planes de continuidad de las actividades del Instituto de conformidad con la estrategia de continuidad acordada.
- 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 Instituto.
- Proponer las modificaciones a los planes de contingencia.

Política

9.1. Proceso de la Gestión de la Continuidad del Negocio del Instituto de Neurocirugía.

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

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

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

9.2. Continuidad de las Actividades y Análisis de los Impactos

Con el fin de establecer un Plan de Continuidad de las Actividades del Instituto 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 e incendio, desastres naturales, 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 activa participación de los propietarios de los procesos y recursos de información de que se trate y el Responsable de Seguridad Informática, considerando todos los procesos de las actividades del Instituto 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 Instituto. Una vez que se ha creado este plan, el mismo debe ser propuesto por el Comité de Seguridad de la Información a la máxima autoridad del Instituto para su aprobación.

9.3. Elaboración e Implementación de los Planes de Continuidad de las Actividades del Establecimiento.

Los propietarios de procesos y recursos de información, con la asistencia del Responsable de Seguridad Informática, elaborarán los planes de contingencia necesarios para garantizar la continuidad de las actividades del Instituto. Estos procesos deberán ser propuestos por el Comité de Seguridad de la Información.

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:
    - Objetivo del plan.
    - Mecanismos de coordinación y comunicación entre equipos (personal involucrado).
    - Procedimientos de divulgación.
    - Requisitos de la seguridad.
    - Procesos específicos para el personal involucrado.

- Responsabilidades individuales.

g) Probar y actualizar los planes.

Asimismo, el proceso de planificación debe concentrarse en los objetivos de las actividades del Instituto requeridos, 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.

9.4. Marco para la Planificación de la Continuidad de las Actividades del Instituto

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

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

El administrador de cada plan de continuidad será el encargado de coordinar las tareas definidas en el mismo.

Estas modificaciones deberán ser propuestas por el Comité de Seguridad de la Información para su aprobación.

El marco para la planificación de la continuidad de las actividades del Establecimiento, 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 Instituto de Neurocirugía. 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, Carabineros, Policía de Investigaciones, bomberos y autoridades locales.
c) Realizar los procedimientos de emergencia que describan las acciones a emprender para el traslado de actividades esenciales del Instituto 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 Instituto de Neurocirugía.
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.

10. CUMPLIMIENTOS NORMATIVOS

Generalidades

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

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

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

Objetivos

Consolidar la seguridad de la información dentro del Instituto, a través de mecanismos de administración por parte de las unidades, Servicios, grupos e funcionarios asignados a cada función.

Definir en forma clara las responsabilidades de cada funcionario en el contexto de la seguridad de la información.

Cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas al Instituto y/o al funcionario(a) o que incurran en responsabilidad civil o penal como resultado de su incumplimiento.

Garantizar que los sistemas cumplan con la política, normas y procedimientos de seguridad del Instituto.

Revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y 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 el mismo, o los obstáculos que pudieran afectarlo.

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

Alcance

Esta Política se aplica a todo el personal del Instituto.

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

Incluye todos los activos de información que el Instituto posea en la actualidad o en el futuro, de manera que la no mención explícita en la presente política no es argumento suficiente para no proteger activos de información que se encuentren en otras formas. La política cubre toda la información impresa o escrita en papel, almacenada electrónicamente, trasmitida por correo o usando medios electrónicos, mostrada en videos o registros de audio de una conversación.

Vigencia

Esta Norma de Cumplimientos Normativos entrará en vigencia a partir del **01 de Agosto de 2013.**

Responsabilidades

El Responsable de Seguridad Informática cumplirá las siguientes funciones:

Definir normas y procedimientos para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual y a la conservación de registros.

Verificar periódicamente que los sistemas de información cumplan la política, normas y procedimientos de seguridad establecidos.

Garantizar la seguridad y el control de las herramientas utilizadas para las revisiones de auditoría.

El Responsable del Área Legal o Administrativa del Instituto, con la asistencia del Responsable de Seguridad Informática cumplirán las siguientes funciones:

Definir y documentar claramente todos los requisitos normativos y contractuales pertinentes para cada sistema de información.

Redactar un Compromiso de Confidencialidad a ser firmado por todo el personal.

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

El Instituto de Neurocirugía debe conformar un equipo de trabajo ejecutivo para gestionar, evaluar y resolver sobre materias relacionadas a la Seguridad de la Información, el que se denominará "Comité de Seguridad de la Información".

Se crea el rol de "Encargado de Seguridad de la Información", quien debe promover, evaluar y fiscalizar las medidas de seguridad aprobadas por la Dirección.

El Comité de Seguridad de la Información debe reunirse al menos cada tres meses para revisar el estado de la seguridad de la información del Instituto, aprobar y revisar los proyectos de seguridad de la información, aceptar nuevas políticas o modificaciones a las existentes.

El Instituto de Neurocirugía, a través del Encargado de Seguridad, debe establecer medidas de seguridad para prevenir, detectar y responder oportunamente ante posibles daños a la Seguridad de la Información.

El Encargado de Seguridad debe establecer puntos de enlace con encargados de seguridad de otros organismos públicos y especialistas externos en forma periódica.

La Dirección debe definir el nivel de riesgo aceptable para los riesgos que se identifiquen y deberá determinar las acciones a tomar para gestionarlo, a través de alguna de las siguientes alternativas:

- Evitarlo: Cambiando la manera de operar.
- Mitigarlo: Reducir su probabilidad de ocurrencia o las consecuencias: a través de controles apropiados.
- Transferirlo: A otra instancia, como un tercero o seguros.
- Retenerlo: Aceptar el riesgo y vivir con él.

Cualquier cambio en el estado contractual del personal debe ser informado por el área responsable a los administradores de sistemas. Encargado de seguridad y personal de seguridad física, para que puedan realizar las restricciones de acceso a la información que correspondan.