Institución Tecnológica Colegio
Mayor de Bolívar
Comité de Seguridad de la Información

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

INSTITUCIÓN TECNOLÓGICA
COLEGIO MAYOR DE BOLÍVAR

- ABRIL 2017 -

Institución Tecnológica Colegio
Mayor de Bolívar

Comité de Seguridad de la Información

ÍNDICE

6. SEGURIDAD DEL PERSONAL

6.1. **Seguridad en la Definición de Puestos de Trabajo y la Asignación de Recursos**

6.1.1. Incorporación de la Seguridad en los Puestos de Trabajo
6.1.2. Control y Política del Personal
6.1.3. Compromiso de Confidencialidad
6.1.4. Términos y Condiciones de Empleo

6.2. **Capacitación del Usuario**

6.2.1. Formación y Capacitación en Materia de Seguridad de la Información
6.3. Respuesta a Incidentes y Anomalías en Materia de Seguridad
6.3.1. Comunicación de Incidentes Relativos a la Seguridad
6.3.2. Comunicación de Debilidades en Materia de Seguridad
6.3.3. Comunicación de Anomalías del Software
6.3.4. Aprendiendo de los Incidentes

7. SEGURIDAD FÍSICA Y AMBIENTAL

7.1. Perímetro de Seguridad Física
7.2. Controles de Acceso Físico
7.3. Protección de Oficinas, Recintos e Instalaciones
7.4. Desarrollo de Tareas en Áreas Protegidas
7.5. Aislamiento de las Áreas de Recepción y Distribución
7.6. Ubicación y Protección del Equipamiento y Copias de Seguridad
7.7. Suministros de Energía
7.8. Seguridad del Cableado
7.9. Mantenimiento de Equipos
7.10. Seguridad de los Equipos Fuera de las Instalaciones
7.11. Desafectación o Reutilización Segura de los Equipos.
7.12. Políticas de Escritorios y Pantallas Limpias
7.13. Retiro de los Bienes

8. GESTIÓN DE COMUNICACIONES Y OPERACIONES

8.1. **Procedimientos y Responsabilidades Operativas**

8.1.1. Documentación de los Procedimientos Operativos
8.1.2. Control de Cambios en las Operaciones
8.1.3. Procedimientos de Manejo de Incidentes
8.1.4. Separación de Funciones
8.1.5. Separación entre Instalaciones de Desarrollo e Instalaciones Operativas
8.1.6. Gestión de Instalaciones Externas

8.2. **Planificación y Aprobación de Sistemas**

Institución Tecnológica Colegio
Mayor de Bolívar

Comité de Seguridad de la Información

1. INTRODUCCIÓN

La información es un recurso que, como el resto de los activos, tiene valor parala comunidad universitaria y por consiguiente debe ser debidamente protegida, garantizando la continuidad de los sistemas de información, minimizando los riesgos de daño y contribuyendo de esta manera, a una mejor gestión de la Institución.

Para que estos principios de la Política de Seguridad de la Información sean efectivos, resulta necesaria la implementación de una Política de Seguridad de la Información que forme parte de la cultura organizacional de la Institución, lo que implica que debe contarse con el manifiesto compromiso de todos los funcionarios de una manera u otra vinculados a la gestión, para contribuir a la difusión, consolidación y cumplimiento.

Como consecuencia de lo expuesto, la Institución Tecnológica COLMAYOR Bolívar se ha abocado a la tarea de implementar sus propias políticas de seguridad de la información, basándose en las características establecidas en el Modelo de Política de Seguridad de la Información del Gobierno central (GEL) publicado por el Ministerio de las Tecnologías MinTic.

Así mismo, con el propósito de que dicha implementación pueda realizarse en forma ordenada y gradual, la Institución ha encomendado a su Comité de Seguridad de la Información, la tarea de elaborar y coordinar la ejecución de un Plan de Acción para el año 2017 que fije objetivos vinculados a los temas institucionales..

2. TÉRMINOS Y DEFINICIONES

Con el objeto de precisar el alcance de los principales conceptos utilizados en este documento, se transcriben las definiciones que sobre los mismos se han incluído en el Modelo de Política de Seguridad de la Información GEL.

2.1. Seguridad de la Información: La seguridad de la información se entiende como la preservación de las siguientes características:

- **Confidencialidad**: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- **Integridad**: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- **Disponibilidad**: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, deberán considerarse los conceptos de:

- **Autenticidad**: busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar 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 sólo 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 reci- bido información alegue ante terceros que no la envió o recibió.
- **Legalidad**: referido al cumplimiento de las leyes, normas, reglamenta- ciones o disposiciones a las que está sujeto el Organismo.
- **Confiabilidad de la Información**: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las mis- iones y funciones.

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

2.3. 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.

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

2.5. Comité de Seguridad de la Información: El Comité de Seguridad de la Información, es un cuerpo integrado por representantes de todas las áreas sustantivas de la Institución, desti- nado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

2.6. Responsable de Seguridad Informática: Es la persona que cumple la función de su- pervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes de la Institución que así lo requieran.

3. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

3.1. Objetivos:

a) Proteger los recursos de información de la Institución 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.

b) 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.

c) Mantener la Política de Seguridad de la Institución actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

3.2. Sanciones Previstas por Incumplimiento: El incumplimiento de la disposiciones establecidas por las Políticas de Seguridad de la Información tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud y característica del aspecto no cumplido.

4. ORGANIZACIÓN DE LA SEGURIDAD

Son sus objetivos:

a) Administrar la seguridad de la información dentro de la Institución y es tablecer un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades.

b) Fomentar la consulta y cooperación con Organismos especializados para la obtención de asesoría en materia de seguridad de la información.

c) Garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información de la Institución.

4.1. Infraestructura de la Seguridad de la Información

4.1.1. Comité de Seguridad de la Información: El Modelo de la Seguridad y Privacidad de la Información del MinTic lo define como un cuerpo integrado por representantes de todas las áreas sustantivas de la Institución, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

La Rectoría de la Institución creó el Comité de Seguridad de la Información **ComSI** mediante la Resolución Nº XXXX el X de XXXXXX de XXXX, con los siguientes objetivos:

1) Revisar y proponer a la Rectora de esta Institución para su consideración y posterior aprobación, las políticas de seguridad de la información y las funciones generales en materia de seguridad de la información que fuera convenientes y apropiadas para esta Institución.

2) Monitorear cambios significativos en los riesgos que afectan a los recursos de la información de esta Institución frente a posibles amenazas, sean internas o externas.

3) Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes, relativos a la seguridad, que se produzcan en el ámbito de esta Institución.

4) Aprobar las principales iniciativa para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada sector, así como acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información

5) Evaluar y coordinar la implementación de controles específicos de seguridad se la información para los sistemas o servicios de esta Institución, sean preexistente o nuevos.

6) Promover la difusión y apoyo a la seguridad de la información dentro de la Institución, como así, coordinar el proceso de administración de la continuidad de las actividades.

4.1.2. Asignación de Responsabilidades en Materia de Seguridad de la Información

El Rector de la Institución Tecnológica COLMAYOR Bolívar deberá asigna las funciones relativas a la Seguridad Informática de la Institución a ....., en adelante el “Responsable de Seguridad Informática”, quien tendrá a cargo las funciones relativas a la seguridad de los sistemas de información de la Institución, lo cual incluye la supervisión de todos los

aspectos inherentes a seguridad informática tratados en la presente Política.

El Comité de Seguridad de la Información propondrá a la autoridad que corresponda para su aprobación, la definición y asignación de las responsabilidades que surjan de los procesos de seguridad que se detallan a continuación, indicando en cada caso el/los responsable/s del cumplimiento de los aspectos de esta Política aplicables a cada caso:

a) Seguridad del Personal
b) Seguridad Física y Ambiental
c) Seguridad en las Comunicaciones y las Operaciones
d) Control de Accesos
e) Seguridad en el Desarrollo y Mantenimiento de Sistemas
f) Planificación de la Continuidad Operativa

Así mismo, el Comité de Seguridad de la Información propondrá a la autoridad que corresponda para su aprobación, la definición y asignación de las responsabilidades de los propietarios de la información que se definan, quienes serán los responsables de las unidades organizativas a cargo del manejo de la misma.

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

4.1.3. Proceso de Autorización para Instalaciones de Procesamiento de Información

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

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

4.1.4. Asesoramiento Especializado en Materia de Seguridad de la Información

El Responsable de Seguridad Informática será el encargado de coordinar los

conocimientos y las experiencias disponibles en la Institución, a fin de brindar ayuda en la toma de decisiones en materia de seguridad. Éste podrá obtener asesoramiento de otros Organismos.

4.1.5. Cooperación entre Organismos

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

- Ministerio de Tecnologías de la Información y las Comunicaciones – MinTic
- El Grupo de Respuesta a Emergencias Cibernéticas de Colombia – colCERT
- Dirección Nacional de Protección de Datos Personales. SIC

4.1.6. Revisión Independiente de la Seguridad de la Información

La Unidad de Control Interno o en su defecto quien sea propuesto por el Comité de Seguridad de la Información realizará revisiones independientes sobre la vigencia e implementación de las Políticas de Seguridad de la Información, a efectos de garantizar que las prácticas de la Institución reflejan adecuadamente sus disposiciones.

4.2. Seguridad Frente al Acceso por Parte de Terceros

4.2.1. Identificación de Riesgos del Acceso de Terceras Partes

Cuando exista la necesidad de otorgar acceso a terceras partes a información de la Institución, 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 qué 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 de la Institución.

En todos los contratos cuyo objeto sea la prestación de servicios a título personal bajo cualquier modalidad jurídica que deban desarrollarse dentro de la

Institución, se establecerán los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, restringiendo al mínimo necesario, los permisos a otorgar.

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.

4.2.2. 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 de la Institución.
b) Protección de los activos de la Institución, incluyendo:
   • Procedimientos para proteger los bienes de la Institución, abarcando los activos físicos, la información y el software.
   • Procedimientos para determinar si ha ocurrido algún evento que comprometa los bienes, por ejemplo, debido a pérdida o modificación de datos.
   • Controles para garantizar la recuperación o destrucción de la información y los activos al finalizar el contrato o acuerdo, o en un momento convenido durante la vigencia del mismo.
   • Restricciones a la copia y divulgación de información.
c) Descripción de los servicios disponibles.
d) Nivel de servicio esperado y niveles de servicio aceptables.
e) Permiso para la transferencia de personal cuando sea necesario.
f) Obligaciones de las partes 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:
   a. Métodos de acceso permitidos, y el control y uso de identificadores únicos como identificadores de usuario y contraseñas de usuarios.
   b. Proceso de autorización de accesos y privilegios de usuarios.
   c. 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 surgi- das 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 hard- ware 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 administrado- res 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.

4.3. Tercerización

4.3.1. Requerimientos de Seguridad en Contratos de Tercerización

Los contratos o acuerdos de tercerización total o parcial para la administración y con- trol de sistemas de información, redes y/o ambientes de PC de la Institución, contemplarán además de los puntos especificados en (“SLA o ANS 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 de la Institución.

d) Controles físicos y lógicos que se utilizarán para restringir y delimitar el

acceso a la información sensible de la Institución.

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 auditoría por parte de la Institución sobre los aspectos tercerizados en forma directa o a través de la contratación de servicios ad hoc.

Se debe prever la factibilidad de ampliar los requerimientos y procedimientos de seguridad con el acuerdo de las partes.

5. CLASIFICACIÓN Y CONTROL DE ACTIVOS

Son sus objetivos:

a) Garantizar que los activos de información reciban un apropiado nivel de protección.

b) Clasificar la información para señalar su sensibilidad y criticidad.

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

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

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.

El Responsable de Seguridad Informática es el encargado de asegurar que los lineamientos para la utilización de los recursos de la tecnología de información contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan.
Cada Propietario de la Información supervisará que el proceso de clasificación y rótulo de información de su área de competencia sea cumplimentado de acuerdo a lo establecido en la presente Política.

5.1. 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 revisado con una periodicidad no mayor a 6 meses.

El encargado de elaborar el inventario y mantenerlo actualizado es cada Responsable de Unidad Organizativa.

5.2. 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:

a) confidencialidad,

b) integridad,

c) disponibilidad.

5.3. 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 tan- to en formatos físicos como electrónicos e incorporarán las siguientes actividades de procesa- miento de la información:

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

6. SEGURIDAD DEL PERSONAL

Son sus objetivos:

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

b) 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.

c) Garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para respaldar la Política de Seguridad de la Institución en el transcurso de sus tareas normales.

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

e) 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.

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

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 Responsable de Seguridad Informática tiene a cargo el seguimiento, documentación y análisis de los incidentes de seguridad reportados así como su comunicación al Comité de Seguridad de la Información, a los propietarios de la información.

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 participará en la confección del Compromiso de Confidencialidad a firmar por los empleados y terceros que desarrollen funciones en la Institución, 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 de la Institución es responsable del reporte de debilidades e incidentes de seguridad que oportunamente se detecten.

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

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

6.1.2. 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 a la Institución.

6.1.3. Compromiso de Confidencialidad

Como parte de sus términos y condiciones iniciales de empleo, los empleados, cualquiera sea su situación de vinculación, firmarán un Compromiso de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información de la Institución. 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 declarará 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.

6.1.4. Términos y Condiciones de Empleo

Los términos y condiciones de empleo establecerán la responsabilidad del empleado en materia de seguridad de la información. Cuando corresponda, los términos y condiciones de empleo establecerán que estas responsabilidades se extienden más allá de los límites de la sede de la Institución y del horario normal de trabajo.

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

6.2. Capacitación del Usuario

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

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

6.3. Respuesta a Incidentes y Anomalías en Materia de Seguridad

6.3.1. Comunicación de Incidentes Relativos a la Seguridad

Los incidentes relativos a la seguridad serán comunicados a través de canales 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.

6.3.2. 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.

6.3.3. Comunicación de Anomalías del Software

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

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

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

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

La recuperación será realizada por personal experimentado, adecuadamente habilitado.

6.3.4. Aprendiendo de los Incidentes

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

7. SEGURIDAD FÍSICA Y AMBIENTAL

Son sus objetivos:

a) Prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones e información de la Institución.

b) Proteger el equipamiento de procesamiento de información crítica de la Institución, 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.

c) Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información de la Institución.

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

e) Proporcionar protección proporcional a los riesgos identificados.

Esta Política se aplica a todos los recursos físicos relativos a los sistemas de información de la Institución: instalaciones, equipamiento, cableado, Documentación, medios de almacenamiento, etc.

El Responsable de Seguridad Informática definirá junto con el Responsable del Área 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 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 de la Institución.

Los Responsables de Unidades Académicas definirán los niveles de acceso físico del personal de la Institución 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 de la Institución cuando lo crean conveniente.

Todo el personal de la Institución 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.

7.1. 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 oficinas de la Institución y de las instalaciones de procesamiento de información.

El Organismo utilizará perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información, de suministro de energía eléctrica, de aire acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información. 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 Informática con el asesoramiento del Responsable de Seguridad Informática, de acuerdo a la evaluación de riesgos efectuada.

7.2. Controles de Acceso Físico

Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por el Responsable de Seguridad Informática junto con el Responsable del Área Informática, a fin de permitir el acceso sólo al personal autorizado.

7.3. Protección de Oficinas, Recintos e Instalaciones

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

7.4. Desarrollo de Tareas en Áreas Protegidas

Para incrementar la seguridad de las áreas protegidas, se establecerán controles y lineamientos adicionales, que incluyan controles para el personal que trabaja en el área protegida, así como para las actividades de terceros que tengan lugar allí.

7.5. 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.

7.6. 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,

7.7. Suministros de Energía

El equipamiento estará protegido con respecto a las posibles fallas en el suministro de energía otras anomalías eléctricas. El suministro de energía estará de acuerdo con las especificaciones del fabricante o proveedor de cada equipo.

7.8. Seguridad del Cableado

El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información estará protegido contra intercepción o daño.

7.9. Mantenimiento de Equipos

Se realizará el mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanentes, teniendo en cuenta a tal efecto:

a) la realización de tareas de mantenimiento preventivo al equipamiento, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal del Responsables del Área Informática.

b) el establecimiento de la práctica de que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.

c) la registración de todas las fallas -supuestas y/o reales- y de todo el mantenimiento preventivo y correctivo realizado.

d) la registración del retiro de equipamiento para su mantenimiento de la sede de la Institución.

e) la eliminación de toda información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.

7.10. Seguridad de los Equipos Fuera de las Instalaciones

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

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

7.11. Desafectación o Reutilización Segura de los Equipos

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

7.12. 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 instala- ciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.

7.13. Retiro de los Bienes

El equipamiento, la información y el software no serán retirados de la sede de l a Institución sin autorización formal. Periódicamente, se llevarán a cabo comprobaciones puntuales para detectar el retiro no autorizado de activos de la Institución.

8. GESTIÓN DE COMUNICACIONES Y OPERACIONES

Son sus objetivos:

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

b) Establecer responsabilidades y procedimientos para su gestión y operación, incluyen- do instrucciones operativas, procedimientos para la respuesta a incidentes y separación de funciones.

Cada Propietario de la Información, junto con el Responsable de Seguridad Informática y el Responsable del Área 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.

8.1. Procedimientos y Responsabilidades Operativas

8.1.1. 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.

8.1.2. 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 Informática evaluará el posible impacto operativo de los cambios previstos y verificará su correcta implementación.

8.1.3. 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 seguridad.

8.1.4. Separación de Funciones

Se contemplará la separación de la gestión o ejecución de tareas o áreas de responsabilidad, en la medida de que la misma reduzca 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.

En los casos en los que este método de control no se pudiera cumplirse, se imple- mentarán controles tales como el monitoreo de las actividades y/o la elaboración de registros de auditoría y control periódico de los mismos.

8.1.5. 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.

8.1.6. Gestión de Instalaciones Externas

En el caso de tercerizar la administración de las instalaciones de procesamiento, se acordarán controles con el proveedor del servicio que se incluirán en el contrato de tercerización.

8.2. Planificación y Aprobación de Sistemas

8.2.1. Planificación de la Capacidad

El Responsable del Área Informática, o el personal que éste designe, efectuará el monitoreo de las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas, 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 de la Institución 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.

8.2.2. Aprobación del Sistema

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

8.3. Protección Contra Software Malicioso

8.3.1. 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 Informática, o el personal designado por éste, implementará dichos controles.

Generalización

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.

8.4. Mantenimiento

8.4.1. Resguardo de la Información

El Responsable del Área Informática y el de Seguridad Informática junto al Responsable del Área 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.

8.4.2. Registro de Actividades del Personal Operativo

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

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

8.4.3. Registro de Fallas

El Responsable del Área 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.

8.5. Administración de la Red

8.5.1. Controles de Redes

El Responsable de Seguridad Informática definirá controles para garantizar la seguridad de los datos y los servicios conectados en las redes de la Institución, contra el acceso no autorizado. El Responsable del Área Informática implementará dichos controles.

8.6. Administración y Seguridad de los Medios de Almacenamiento

8.6.1. Administración de Medios Informáticos Removibles

El Responsable del Área Informática, con la asistencia del Responsable de Seguridad Informática, implementará procedimientos para la administración de medios informáticos removibles, como

cintas, discos, casetes e informes impresos.

8.6.2. Eliminación de Medios de Información

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

8.6.3. Procedimientos de Manejo de la Información

Se definirán procedimientos para el manejo y almacenamiento de la información de acuerdo a lo establecido en el capítulo 5 – "Clasificación y Control de Activos".

8.6.4. Seguridad de la Documentación del Sistema

La documentación del sistema puede contener información sensible, por lo que se considerarán los recaudos para su protección, de almacenar la documentación del sistema en forma segura y 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.

8.7. Intercambios de Información y Software

8.7.1. 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 de la Institución y las consideraciones de seguridad sobre la misma.

8.7.2. 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, suficiente embalaje para el envío y la adopción de controles especiales, cuando resulte necesario, a fin de proteger la información sensible contra divulgación o modificación no autorizadas.

8.7.3. Seguridad del Gobierno Electrónico

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

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

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.

8.7.4. Seguridad del Correo Electrónico

8.7.4.1. 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 autoriza- dos 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 de la Institución.

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.

8.7.4.2. Política de Correo Electrónico

El Responsable de Seguridad Informática junto con el Responsable del Área 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 (Ver 10.3. Controles Criptográficos).

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 de la Institución.

8.7.5. 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.

8.7.6. 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.

8.7.7. Otras Formas de Intercambio de Información
Se implementarán normas, procedimientos y controles para proteger el intercambio de información a través de medios de comunicaciones de voz, fax y vídeo.

9. CONTROL DE ACCESOS

Son sus objetivos:

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

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

c) Controlar la seguridad en la conexión entre la red de la Institución y otras redes públicas o privadas.

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

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

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

9.1. Requerimientos para el Control de Acceso

9.1.1. Política de Control de Accesos

9.1.2. Reglas de Control de Acceso

9.2. 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.

9.2.1. 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,

9.2.2. 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.

9.2.3. Administración de Contraseñas de Usuario

La asignación de contraseñas se controlará a través de un proceso de administración formal.

9.2.4. Administración de Contraseñas Críticas

Existen cuentas de usuarios con las cuales es posible efectuar actividades críticas como ser instalación de plataformas o sistemas, habilitación de servicios, actualización de software, configuración de componentes informáticos, etc.. Dichas cuentas no serán de uso habitual (diario), sino que sólo serán utilizadas ante una necesidad específica de realizar alguna tarea que lo requiera y se encontrarán protegidas por contraseñas con un mayor nivel de complejidad que el habitual.

El Responsable de Seguridad Informática definirá procedimientos para la administración de dichas contraseñas críticas.

9.2.5. Revisión de Derechos de Acceso de Usuarios

A fin de mantener un control eficaz del acceso a los datos y servicios de información, el Propietario de la Información de que se trate, llevará a cabo un proceso formal, a intervalos regulares de no más a 6 meses, a fin de revisar los derechos de acceso de los usuarios.

9.3. Responsabilidades del Usuario

9.3.1. Uso de Contraseñas

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

9.3.2. Equipos Desatendidos en Áreas de Usuarios

Los usuarios deberán garantizar que los equipos desatendidos sean protegidos adecuadamente. Los equipos instalados en áreas de usuarios, por ejemplo estacio- nes de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos.

El Responsable de Seguridad Informática debe coordinar con el Área de Recursos Humanos las tareas de concientización a todos los usuarios y contratistas, acerca de los requerimientos y procedimientos de seguridad, para la protección de equi- pos desatendidos, así como de sus funciones en relación a la implementación de dicha protección.

9.4. Control de Acceso a la Red

9.4.1. Política de Utilización de los Servicios de Red
Se controlará el acceso a los servicios de red tanto internos como externos. El Responsable del Área Informática tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal del titular de una Unidad Organizativa que lo solicite para personal de su incumbencia.

9.4.2. Camino Forzado
El camino de las comunicaciones será controlado. Se limitarán las opciones de elección de la ruta entre la terminal de usuario y los servicios a los cuales el mis- mo se encuentra autorizado a acceder, mediante la implementación de controles en diferentes puntos de la misma.

9.4.3. Autenticación de Usuarios para Conexiones Externas
El Responsable de Seguridad Informática, conjuntamente con el Propietario de la Información de que se trate, realizarán una evaluación de riesgos a fin de determi- nar el mecanismo de autenticación que corresponda en cada caso.

9.4.4. Autenticación de Nodos
Una herramienta de conexión automática a una computadora remota podría brindar un medio para obtener acceso no autorizado a una aplicación de la Uni- versidad. Por consiguiente, las conexiones a sistemas informáticos remotos serán autenticadas.

9.4.5. Protección de los Puertos (Ports) de Diagnóstico Remoto
Los puertos de diagnóstico proporcionan un medio de acceso no autorizado. Por consiguiente, serán protegidos por un mecanismo de seguridad apropiado

9.4.6. Subdivisión de Redes
Se definirán y documentarán los perímetros de seguridad que sean convenientes, que se implementarán mediante la instalación de "gateways" con funcionalidades de "firewall" o redes privadas virtuales, para filtrar el tráfico entre los dominios
y para bloquear el acceso no autorizado.

9.4.7. Acceso a Internet
El acceso a Internet será utilizado con propósitos autorizados o con el destino por el cual fue provisto. El Responsable de Seguridad Informática definirá procedi- mientos para solicitar y aprobar accesos a Internet. Los

accesos serán autorizados formalmente por el Responsable de la Unidad Organizativa a cargo del personal que lo solicite. Asimismo, se definirán las pautas de utilización de Internet para todos los usuarios.

9.4.8. Control de Conexión a la Red
Se podrán implementar controles para limitar la capacidad de conexión de los usuarios, de acuerdo a las políticas que se establecen a tal efecto. Dichos controles se podrán implementar en los "gateways" que separan los diferentes dominios de la red.

9.4.9. Control de Ruteo de Red
Se incorporarán controles de ruteo, para asegurar que las conexiones informáticas y los flujos de información no violen la Política de Control de Accesos. Estos con- troles contemplarán mínimamente la verificación positiva de direcciones de origen y destino.

9.4.10. Seguridad de los Servicios de Red
El Responsable de Seguridad Informática junto con el Responsable del Área In- formática definirán las pautas para garantizar la seguridad de los servicios de red de la Institución, tanto de los públicos como los privados.

9.5. Control de Acceso al Sistema Operativo

9.5.1. Identificación Automática de Terminales
El Responsable de Seguridad Informática junto con el Responsable del Área Informática realizarán una evaluación de riesgos a fin de determinar el método de protección adecuado para el acceso al Sistema Operativo.

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

9.5.3. Identificación y Autenticación de los Usuarios
Todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán un identificador único (ID de usuario) solamente para su uso perso- nal exclusivo. Los identificadores de usuario no darán ningún indicio del nivel de privilegio otorgado.

9.5.4. Sistema de Administración de Contraseñas El sistema de administración de contraseñas debe:

a) Imponer el uso de contraseñas individuales para determinar

responsabili- dades.

b) Permitir que los usuarios seleccionen y cambien sus propias contraseñas (luego de cumplido el plazo mínimo de mantenimiento de las mismas) e incluir un procedimiento de confirmación para contemplar los errores de ingreso.

c) Imponer una selección de contraseñas de calidad según lo señalado en el punto “Uso de Contraseñas”.

d) Imponer cambios en las contraseñas en aquellos casos en que los usuarios mantengan sus propias contraseñas, según lo señalado en el punto “Uso de Contraseñas”.

e) Obligar a los usuarios a cambiar las contraseñas provisorias en su primer procedimiento de identificación, en los casos en que ellos seleccionen sus contraseñas.

f) Mantener un registro de las últimas contraseñas utilizadas por el usuario, y evitar la reutilización de las mismas.

g) Evitar mostrar las contraseñas en pantalla, cuando son ingresadas.

h) Almacenar en forma separada los archivos de contraseñas y los datos de sistemas de aplicación.

i) Almacenar las contraseñas en forma cifrada utilizando un algoritmo de cifrado unidireccional.

j) Modificar todas las contraseñas predeterminadas por el vendedor, una vez instalado el software y el hardware (por ejemplo claves de impresoras, switcs, routers, etc.).

k) Garantizar que el medio utilizado para acceder/utilizar el sistema de contraseñas, asegure que no se tenga acceso a información temporal o en tránsito de forma no protegida.

9.5.5. Uso de Utilitarios de Sistema

Existen programas utilitarios que podrían tener la capacidad de pasar por alto los controles de sistemas y aplicaciones. Su uso será limitado y minuciosamente controlado.

9.5.6. Alarmas Silenciosas para la Protección de los Usuarios

Se considerará la provisión de alarmas silenciosas para los usuarios que podrían ser objetos de coerción. La decisión de suministrar una alarma de esta índole se basará en una evaluación de riesgos que realizará el Responsable de Seguridad Informática junto con el Responsable del Área Informática.

9.5.7. Desconexión de Terminales por Tiempo Muerto

El Responsable de Seguridad Informática, junto con los Propietarios de la

Información de que se trate definirán cuáles se consideran terminales de alto riesgo. o que sirven a sistemas de alto riesgo. Las mismas se apagarán después de un periodo definido de inactividad, por un lapso que responderá a los riesgos de seguridad del área y de la información que maneje la terminal.

Para las PC's, se implementará la desconexión por tiempo muerto, que limpie la pantalla y evite el acceso no autorizado, pero que no cierra las sesiones de aplicación o de red. Por otro lado, si un usuario debe abandonar su puesto de trabajo momentáneamente, activará protectores de pantalla con contraseñas.

9.5.8. Limitación del Horario de Conexión

Se implementará un control de esta índole para aplicaciones informáticas sensibles, especialmente aquellas terminales instaladas en ubicaciones de alto riesgo.

9.6. Control de Acceso a las Aplicaciones

9.6.1. Restricción del Acceso a la Información

Los usuarios de sistemas de aplicación, con inclusión del personal de soporte, tendrán acceso a la información y a las funciones de los sistemas de aplicación de conformidad con la Política de Control de Acceso definida, sobre la base de los requerimientos de cada aplicación, y conforme a la Política de la Institución para el acceso a la información

9.6.2. Aislamiento de los Sistemas Sensibles

Los sistemas sensibles podrían requerir de un ambiente informático dedicado (aislado). La sensibilidad puede señalar que el sistema de aplicación debe ejecutarse en una computadora dedicada, que sólo debe compartir recursos con los sistemas de aplicación confiables, o no tener limitaciones.

9.7. Monitoreo del Acceso y Uso de los Sistemas

9.7.1. Registro de Eventos

Se generarán registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad. Los registros de auditoría deberán incluir la identificación del usuario, la fecha y hora de inicio y terminación, la identidad o ubicación de la terminal, un registro de intentos exitosos y fallidos de acceso al sistema y un registro de intentos exitosos y fallidos de acceso a datos y otros recursos.

9.7.2. Monitoreo del Uso de los Sistemas

9.7.2.1. Procedimientos y Áreas de Riesgo

Se desarrollarán procedimientos para monitorear el uso de las instalaciones de procesamiento de la información, a fin de garantizar que los usuarios sólo estén desempeñando actividades que hayan sido autorizadas explícitamente.

9.7.2.2. Factores de Riesgo

Los Propietarios de la Información manifestarán la necesidad de registrar aquellos eventos que consideren críticos para la operatoria que se encuentra bajo su responsabilidad.

9.7.2.3. Registro y Revisión de Eventos

Se implementará un procedimiento de registro y revisión de los registros de auditoría, orientado a producir un informe de las amenazas detectadas contra los sistemas y los métodos utilizados.
La periodicidad de dichas revisiones será definida por los Propietarios de la Información y el Responsable de Seguridad Informática, de acuerdo a la evaluación de riesgos efectuada.

9.7.3. Sincronización de Relojes

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

9.8. Computación Móvil y Trabajo Remoto

9.8.1. Computación Móvil

Se desarrollarán procedimientos adecuados para estos dispositivos, que abarquen la protección física necesaria, el acceso seguro a los dispositivos, la utilización de los dispositivos en lugares públicos. el acceso a los sistemas de información y servicios de la Institución a través de dichos dispositivos, las técnicas criptográficas a utilizar para la transmisión de información clasificada, los mecanismos de resguardo de la información contenida en los dispositivos y la protección contra software malicioso.

9.8.2. Trabajo Remoto

El trabajo remoto sólo será autorizado por el Responsable de la Unidad

Organizativa, o superior jerárquico correspondiente, a la cual pertenezca el usuario solicitante, conjuntamente con el Responsable de Seguridad Informática, cuando se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con la política, normas y procedimientos existentes.

10. DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Son sus objetivos:

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

b) 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.

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

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 de Datos que integren cualquiera de los ambientes administrados por la Institución en donde residan los desarrollos mencionados.

El Responsable de Seguridad Informática junto con el Propietario de la Información y la Unidad de Control Interno, 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, definirán 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 Sistemas, los métodos de encripción a ser utilizados.

10.1. Requerimientos de Seguridad de los Sistemas

10.1.1. 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.

10.2. Seguridad en los Sistemas de Aplicación

10.2.1. 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.

10.2.2. 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 pro cesamiento y/o vicios por procesos de errores.

10.2.3. Autenticación de Mensajes
Cuando una aplicación tenga previsto el envío de mensajes que contengan información clasificada, se implementarán controles criptográficos.

10.2.4. Validación de Datos de Salidas
Se establecerán procedimientos para validar la salida de los datos de las aplicaciones, incluyendo:

a) Comprobaciones de la razonabilidad para probar si los datos de salida son plausibles.

b) Control de conciliación de cuentas para asegurar el procesamiento de todos los datos.

c) Provisión de información suficiente, para que el lector o sistema de procesamiento subsiguiente determine la exactitud, totalidad, precisión y clasificación de la información.

d) Procedimientos para responder a las pruebas de validación de salidas.

e) Definición de las responsabilidades de todo el personal involucrado en el proceso de salida de datos.

10.3. Controles Criptográficos

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

10.3.1. Política de Utilización de Controles Criptográficos Se utilizarán controles criptográficos en los siguientes casos:

1. Para la protección de claves de acceso a sistemas, datos y servicios.

2. Para la transmisión de información clasificada, fuera del ámbito de la Institución.

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

10.3.2. Cifrado

Mediante la evaluación de riesgos que llevará a cabo el Propietario de la Información y el Responsable de Seguridad Informática, se identificará el nivel requerido de protección, tomando en cuenta el tipo y la calidad del algoritmo de cifrado utilizado y la longitud de las claves criptográficas a utilizar.

10.3.3. Firma Digital

Se tomarán recaudos para proteger la confidencialidad de las claves privadas. Asimismo, es importante proteger la integridad de la clave pública. Esta protección se provee mediante el uso de un certificado de clave pública.

10.3.4. Servicios de No Repudio

Estos servicios se utilizarán cuando sea necesario resolver disputas acerca de la ocurrencia de un evento o acción. Su objetivo es proporcionar herramientas para evitar que aquél que haya originado una transacción electrónica niegue haberla efectuado.

10.3.5. Administración de Claves

10.3.5.1. Protección de Claves Criptográficas

Se implementará un sistema de administración de claves criptográficas para respaldar su utilización por parte de la Institución. Todas las claves serán protegidas contra modificación y destrucción, y las claves secretas y priva- das serán protegidas contra copia o divulgación no autorizada. Se proporcionará una protección adecuada al equipamiento utilizado para generar, alma- cenar y archivar claves, considerándolo crítico o de alto riesgo.

10.4. Seguridad de los Archivos del Sistema

Se garantizará que los desarrollos y actividades de soporte a los sistemas se lleven a cabo de manera segura, controlando el acceso a los archivos del mismo.

10.4.1. Control del Software Operativo
Toda aplicación, desarrollada por el Organismo o por un tercero tendrá un único Responsable designado formalmente por el Responsable del Área Informática. Ningún programador o analista de desarrollo y mantenimiento de aplicaciones podrá acceder a los ambientes de producción.

El Responsable del Área Informática, propondrá para su aprobación por parte del superior jerárquico que corresponda, la asignación de la función de "implementador" al personal de su área que considere adecuado.

10.4.2. Protección de los Datos de Prueba del Sistema
Las pruebas de los sistemas se efectuarán sobre datos extraídos del ambiente operativo. Para proteger los datos de prueba se establecerán normas y procedimientos a tal efecto.

10.4.3. Control de Cambios a Datos Operativos
La modificación, actualización o eliminación de los datos operativos serán realiza- dos a través de los sistemas que procesan dichos datos y de acuerdo al esquema de control de accesos implementado en los mismos.

10.4.4. Control de Acceso a las Bibliotecas de Programas Fuentes
El Responsable del Área Informática, propondrá para su aprobación por parte del superior jerárquico que corresponda la función de "administrador de programas fuentes" al personal de su área que considere adecuado, quien tendrá en custodia los programas fuentes

10.5. Seguridad de los Procesos de Desarrollo y Soporte

10.5.1. Procedimiento de Control de Cambios
Se implementarán controles estrictos durante la implementación de cambios imponiendo el cumplimiento de procedimientos formales. Éstos garantizarán que se cumplan los procedimientos de seguridad y control, respetando la división de funciones.

10.5.2. Revisión Técnica de los Cambios en el Sistema Operativo
Toda vez que sea necesario realizar un cambio en el Sistema Operativo, los sistemas serán revisados para asegurar que no se produzca un impacto en su funciona- miento o seguridad.

10.5.3. Restricción del Cambio de Paquetes de Software
La modificación de paquetes de software suministrados por proveedores,

previa autorización del Responsable del Área Informática, deberá:

a) Analizar los términos y condiciones de la licencia a fin de determinar si las modificaciones se encuentran autorizadas.

b) Determinar la conveniencia de que la modificación sea efectuada por la Institución, por el proveedor o por un tercero.

c) Evaluar el impacto que se produce si el Organismo se hace cargo del mantenimiento.

d) Retener el software original realizando los cambios sobre una copia perfectamente identificada, documentando exhaustivamente por si fuera necesario aplicarlo a nuevas versiones.

10.5.4. Canales Ocultos y Código Malicioso

Se redactarán normas y procedimientos que incluyan:

a) Adquirir programas a proveedores acreditados o productos ya evaluados.

b) Examinar los códigos fuentes (cuando sea posible) antes de utilizar los programas.

c) Controlar el acceso y las modificaciones al código instalado.

d) Utilizar herramientas para la protección contra la infección del software con código malicioso.

10.5.5. Desarrollo Externo de Software

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

a) Acuerdos de licencias, propiedad de código y derechos conferidos.

b) Requerimientos contractuales con respecto a la calidad del código y la existencia de garantías.

c) Procedimientos de certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan auditorías, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software establecidos, etc.

d) Verificación del cumplimiento de las condiciones de seguridad contempladas en el punto 4.3.1. Requerimientos de Seguridad en Contratos de Tercerización.

e) Acuerdos de custodia de los fuentes del software (y cualquier otra información requerida) en caso de quiebra de la tercera parte.

11. ADMINISTRACIÓN DE LA CONTINUIDAD DE LAS ACTIVIDADES DE LA

Comité de Seguridad de la Informacion

INSTITUCIÓN

Son sus objetivos:

a) Minimizar los efectos de las posibles interrupciones de las actividades normales de la Institución (sean éstas resultado de desastres naturales, accidentes, fallas en el equipa- miento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.

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

c) Maximizar la efectividad de las operaciones de contingencia de la Institución con el establecimiento de planes que incluyan al menos las siguientes etapas:

1) Notificación / Activación: Consistente en la detección y determinación del daño y la activación del plan.

2) Reanudación: Consistente en la restauración temporal de las operaciones y recuperación del daño producido al sistema original.

3) Recuperación: Consistente en la restauración de las capacidades de proceso del sistema a las condiciones de operación normales.

d) Asegurar la coordinación con el personal de la Institución y los contactos externos que participarán en las estrategias de planificación de contingencias. Asignar funciones para cada actividad definida.

e)

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 de la Institución.
- 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 de la Institución.
- Elaborar los planes de contingencia necesarios para garantizar la continuidad de las actividades de la Institución.

11.1. Proceso de la Administración de la Continuidad de la Institución

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 de la Institución.

11.2. Continuidad de las Actividades y Análisis de los Impactos

Se establece la necesidad de contar con un Plan de Continuidad de las Actividades de la Institución que contemple los siguientes puntos:

- Identificar los eventos (amenazas) que puedan ocasionar interrupciones en los procesos de las actividades.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones, tanto en términos de magnitud de daño como del período de recuperación.
- Identificar los controles preventivos.

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 de la Institución y no limitándose a las instalaciones de procesamiento de la información.

11.3. Elaboración e Implementación de los Planes de Continuidad de las Activida- des de la Institución

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 de la Institución. Estos procesos deberán ser propuestos por el Comité de Seguridad de la Información

11.4. Marco para la Planificación de la Continuidad de las Actividades de la Institución

Se mantendrá un solo marco para los planes de continuidad de las actividades de la institución, 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.

11.5. Ensayo, Mantenimiento y Reevaluación de los Planes de Continuidad de la Institución

El Comité de Seguridad de la Información establecerá un cronograma de pruebas periódicas de cada uno de los planes de contingencia.

12. CUMPLIMIENTO

Son sus objetivos:

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

b) Garantizar que los sistemas cumplan con la política, normas y procedimientos de seguridad de la Institución.

c) 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.

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

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

f) Determinar los plazos para el mantenimiento de información y para la recolección de evidencia de la Institución.

12.1. Cumplimiento de Requisitos Legales

12.1.1. Identificación de la Legislación Aplicable

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

12.1.2. Derechos de Propiedad Intelectual

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

12.1.2.1. Derecho de Propiedad Intelectual del Software

El Responsable de Seguridad Informática, con la asistencia

del Área Le- gal, analizará los términos y condiciones de la licencia, e implementará los siguientes controles:

a) Definir normas y procedimientos para el cumplimiento del derecho de propiedad intelectual de software que defina el uso legal de productos de información y de software.

b) Divulgar las políticas de adquisición de software y las disposiciones de la Ley de Propiedad Intelectual, y notificar la determinación de tomar acciones disciplinarias contra el personal que las infrinja.

c) Mantener un adecuado registro de activos.

d) Conservar pruebas y evidencias de propiedad de licencias, discos maestros, manuales, etc.

e) Implementar controles para evitar el exceso del número máximo permitido de usuarios.

f) Verificar que sólo se instalen productos con licencia y software autorizado.

g) Elaborar y divulgar un procedimiento para el mantenimiento de condiciones adecuadas con respecto a las licencias.

h) Elaborar y divulgar un procedimiento relativo a la eliminación o transferencia de software a terceros.

i) Utilizar herramientas de auditoría adecuadas.

j) Cumplir con los términos y condiciones establecidos para obtener software e información en redes públicas.

12.1.3. Protección de los Registros de la Institución

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

12.1.4. Protección de Datos y Privacidad de la Información Personal

Todos los empleados deberán conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan conocimiento con motivo del ejercicio de sus funciones. La Institución redactará un "Compromiso de Confidencialidad", el cual deberá ser suscrito por todos los empleados. La copia firmada del compromiso será retenida en forma segura por la Institución.

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

Los recursos de procesamiento de información de la Institución se suministran con un propósito determinado. Toda utilización de estos

recursos con propósitos no autorizados o ajenos al destino por el cual fueron provistos debe ser considerada como uso indebido. Todos los empleados deben conocer el alcance preciso del uso adecuado de los recursos informáticos y deben respetarlo.

12.1.6. Regulación de Controles para el Uso de Criptografía
Al utilizar firmas digitales o electrónicas, se deberá considerar lo dispuesto por la Ley 527 del 1999 y su decreto reglamentario Decreto 2364 de 2012, que establecen las condiciones bajo las cuales una firma digital es legalmente válida.

12.1.7. Recolección de Evidencia
Es necesario contar con adecuada evidencia para respaldar una acción contra una persona u organización. Siempre que esta acción responda a una medida disciplinaria interna, la evidencia necesaria estará descrita en los procedimientos internos.

12.2. Revisiones de la Política de Seguridad y la Compatibilidad Técnica

12.2.1. Cumplimiento de las Políticas de Seguridad
Cada Responsable de Unidad Organizativa, velará por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos, dentro de su área de responsabilidad.
El Responsable de Seguridad Informática, realizará revisiones periódicas de todas las áreas de la Institución a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad. Entre las áreas a revisar se incluyen las siguientes:

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

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

12.2.2. Verificación de la Compatibilidad Técnica
El Responsable de Seguridad Informática verificará periódicamente que los sistemas de información cumplan con la política, normas y procedimientos de seguridad, las que incluirán la revisión de los sistemas en producción a fin de garantizar que los controles de hardware y software hayan sido correctamente implementados.

12.3. Consideraciones de Auditorías de Sistemas

12.3.1. Controles de Auditoría de Sistemas

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

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

Se protegerá el acceso a los elementos utilizados en las auditorías de sistemas, o sea archivos de datos o software, a fin de evitar el mal uso o el compromiso de los mismos. Dichas herramientas estarán separadas de los sistemas en producción y de desarrollo, y se les otorgará el nivel de protección requerido. Se tomarán los recaudos necesarios a efectos de cumplimentar las normas de auditoría dispuestas por la NAGA – Norma Auditoria Generalmente Aceptadas

12.4. Sanciones Previstas por Incumplimiento

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