1. Introducción

Este modelo de política de seguridad está basado en el **Modelo de Política de Seguridad de los Sistemas de Información para Organismos de la Administración Pública Nacional Argentina.** Redactado por la subsecretaria de la gestión pública. En éste documento se redactarán las políticas de seguridad que se aplicaran dentro de la Universidad Nacional del Comahue, cuyo órgano de control es la Dirección General de Tecnología de la Información, Subsecretaría de Tecnologías de la Información.

1.1. Alcance

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

Debe ser conocida y cumplida por toda la planta de personal de la Universidad , tanto se trate de Autoridades, Docentes, No docentes y alumnos. Sea cual fuere su nivel jerárquico y su situación de revista. Las políticas comprenden tanto a la Administración Central como así también a todas las unidades académicas, facultades, organismos autónomos dependientes de la Universidad Nacional del Comahue.

2. Términos y Definiciones

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

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 y utilidad 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 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 la Universidad.

- **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 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.

- **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 la Universidad para llevar a cabo una función propia de la Universidad, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

2.2. Evaluación de Riesgos

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

2.3. 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 los sistemas de información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

2.4. 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 Universidad, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

2.5. Responsable de Seguridad Informática

Es la persona del área TI de la organización 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 Universidad que así lo requieran.

2.6. Incidente de Seguridad

Un incidente de seguridad es un evento adverso en un sistema de computadoras, o red de computadoras, 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.

3. Política de Seguridad de la Información

Generalidades

La información es un recurso que, como el resto de los activos, tiene valor para la Universidad y por consiguiente debe ser debidamente protegida.

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

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

Para esto, se debe asegurar un compromiso manifiesto de las máximas Autoridades de la Universidad y de los medios necesarios para la difusión, consolidación y cumplimiento de la presente Política.

Objetivo

Proteger los recursos de información de la Universidad 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 de la Universidad actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

Alcance

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

Responsabilidad

Todos los Directores Nacionales o Generales, Gerentes o equivalentes, titulares de Unidades Organizativas, tanto se trate de autoridades políticas o técnicas y 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 de la Universidad, cualquiera sea su situación de revista, el área a la cual se encuentre afectado y cualquiera sea el nivel de las tareas que desempeñe.

Las máximas autoridades de la Universidad emiten esta Política y son responsables de la autorización de sus modificaciones.

El **Comité de Seguridad de la Información** de la Universidad , procederá a revisar y proponer a la máxima autoridad del organismo para su aprobación modificaciones a la Política de Seguridad de la Información y las responsabilidades 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, así como acordar y aprobar metodologías y procesos específicos relativos a seguridad de la información; garantizar que la seguridad sea parte del proceso de planificación de la información; evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios; promover la difusión y apoyo a la seguridad de la información dentro de la Universidad y coordinar el proceso de administración de la continuidad de las actividades de la Universidad

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

El **Responsable de Seguridad Informática** tiene la responsabilidad de supervisar todos los aspectos inherentes a los temas tratados en la presente Política, lo cual incluye verificar el cumplimiento de la misma y orientar y asesorar a las dependencias de la Universidad respecto a su implementación. Asimismo es responsable de asegurar que la utilización de los recursos de la tecnología de información contemple los requerimientos de seguridad establecidos según la criticidad de la información que procesan.

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 **Área de Recursos Humanos** o quién desempeñe esas funciones, es responsable de notificar a todo el personal que ingresa 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. Asimismo, tendrá a su cargo la notificación de la presente Política a todo el personal, de los cambios que en ella se produzcan, la implementación de la suscripción de los Acuerdos de Confidencialidad y las tareas de capacitación continua en materia de seguridad.

El **Responsable del Área Informática** tiene la responsabilidad de cumplir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología del Organismo. Por otra parte tendrá la responsabilidad de efectuar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas aprobada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases.

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

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

La **Unidad de Auditoría Interna**, o en su defecto quien sea designado por el Comité de Seguridad de la Información es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la tecnología de información, debiendo informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta Política y por las normas, procedimientos y prácticas que de ella surjan (Ver ". Cumplimiento").

La presente descripción de roles y responsabilidades, no exime a cada sector de la responsabilidad del cumplimiento de las funciones que le son propias, ni de las responsabilidades específicas que emanen de los próximos capítulos.

Política

3.1. Aspectos Generales

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

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

- **Clasificación y Control de Activos**
  Destinado a mantener una adecuada protección de los activos de la Universidad.

- **Seguridad del Personal**
  Orientado a reducir los riesgos de error humano, comisión de ilícitos contra la Universidad o uso inadecuado de instalaciones.

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

- **Gestión de las Comunicaciones y las Operaciones**
  Dirigido a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y medios de comunicación.

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

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

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

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

A fin de asegurar la implementación de las medidas de seguridad comprendidas en esta Política, el Organismo identificará los recursos necesarios e indicará formalmente las partidas presupuestarias correspondientes, como anexo a la presente Política. Lo expresado anteriormente no implicará necesariamente la asignación de partidas presupuestarias adicionales.

El Comité de Seguridad de la Información revisará anualmente la presente Política, a efectos de

mantenerla actualizada. Asimismo efectuará toda modificación que sea necesaria en función a posibles cambios que puedan afectar su definición, como ser, cambios tecnológicos, variación de los costos de los controles, impacto de los incidentes de seguridad, etc.

3.2. Sanciones Previstas por Incumplimiento

El incumplimiento de la Política de Seguridad de la Información tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud y característica del aspecto no cumplido (Ver "12.4. Sanciones Previstas por Incumplimiento").

4. Organización de la Seguridad

Generalidades

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

Por ello, se definirá formalmente un ámbito de gestión para efectuar tareas 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 la Universidad pueden requerir que terceros accedan a información interna, o bien puede ser necesaria la tercerización de ciertas funciones relacionadas con el procesamiento de la información. En estos casos se considerará que la información puede ponerse en riesgo si el acceso de dichos terceros se produce en el marco de una inadecuada administración de la seguridad, por lo que se establecerán las medidas adecuadas para la protección de la información.

Objetivo

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

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

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

Alcance

Esta Política se aplica a todos los recursos de la Universidad y a todas sus relaciones con terceros

que impliquen el acceso a sus datos, recursos y/o a la administración y control de sus sistemas de información.

Responsabilidad

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

El área de Tecnologías de la Información de la Universidad tendrá a cargo la presentación y el mantenimiento de la presente Política, la coordinación de las actividades relativas a la seguridad de la información (análisis de riesgos, monitoreo de incidentes, supervisión de la investigación, implementación de controles, administración de la continuidad, impulsión de procesos de concientización, etc.) y la asignación de funciones y responsabilidades.

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

Los Responsables de las Unidades Organizativas serán responsables de autorizar la incorporación de nuevos recursos de procesamiento de información a las áreas de su incumbencia.

La Unidad de Auditoría Interna o en su defecto quien sea designado por el Comité de Seguridad de la Información será responsable de realizar revisiones independientes sobre la vigencia y el cumplimiento de la presente Política.

El Responsable del Área de Administración será responsable 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. El Responsable del Área Legal participará en dicha tarea. Asimismo, notificará a los proveedores sobre las modificaciones que se efectúen a la Política de Seguridad de la Información de la Universidad.

Política

4.1. Infraestructura de la Seguridad de la Información

4.1.1. Comité de Seguridad de la Información

La seguridad de la información es una responsabilidad de la Universidad compartida por todas las Autoridades políticas, técnicas y administrativas, por lo cual se crea el Comité de Seguridad de la Información, integrado por representantes de los sectores mencionados, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad, el que será presidido por el rector de la Universidad Nacional del Comahue, quien deberá asignar funciones y responsabilidades específicas relativas a la seguridad de la información para todo el Organismo.

Conformación del Comité de Seguridad de la Información

Área / Dirección	Representante

Este Comité tendrá entre sus funciones:

- 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.
- Garantizar que la seguridad sea parte del proceso de planificación de la información.
- Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
- Promover la difusión y apoyo a la seguridad de la información dentro de la Universidad.

El Secretario General coordinará las actividades del Comité de Seguridad de la Información.

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

El Presidente del Comité de Seguridad de la Información, asigna las funciones relativas a la Seguridad Informática en el ámbito de toda la Universidad al responsable del área TI del organismo, en adelante el "Responsable de Seguridad Informática", quien tendrá a cargo la supervisión de todos los aspectos inherentes a los temas tratados en la presente Política.

A continuación se detallan los procesos de seguridad, indicándose en cada caso el/los responsable/s del cumplimiento de los aspectos de esta Política aplicables a cada caso, el Responsable de Seguridad Informática asignará estas responsabilidades:

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

De igual forma, seguidamente se designan los propietarios de la información, quienes serán los Responsables de las Unidades Organizacionales a cargo del manejo de la misma:

Información	Propietario	Recursos asociados	Procesos involucrados	Administrador
Contable	.....	Sistemas de información, equipamiento, bases de datos, comunicaciones, ...	.....	.....
Presupuesto	.....	.....	.....	.....
Inventario				
.....				
.....				

El Comité de Seguridad de la Información definirá y documentará las responsabilidades que le corresponderán a cada funcionario como resultado de la precedente asignación. 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 del Organismo.

El uso de recursos personales de procesamiento de información en el lugar de trabajo puede ocasionar nuevas vulnerabilidades. En consecuencia, su uso será evaluado en cada caso por el Responsable de Seguridad Informática y deberá ser autorizado por el Director o responsable del área al que se destinen los recursos.

4.1.4. Asesoramiento Especializado en Materia de Seguridad de la Información

El Responsable de Seguridad Informática será el encargado de coordinar los conocimientos y las experiencias disponibles en el Organismo a fin de brindar ayuda en la toma de decisiones en materia de seguridad. Éste podrá obtener asesoramiento de otros Organismos (Ver "4.1.5. Cooperación entre Organismos"). Con el objeto de optimizar su gestión, se habilitará al Responsable de Seguridad Informática el contacto con las Unidades Organizativas de todas las Áreas del

Organismo.

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 podrá mantener contacto con organismos especializados en temas relativos a la seguridad informática.

En los intercambios de información de seguridad, no se divulgará información confidencial perteneciente al Organismo a personas no autorizadas.

El intercambio de información confidencial para fines de asesoramiento o de transmisión de experiencias, sólo se permite cuando se haya firmado un Acuerdo de Confidencialidad previo o con aquellas Organizaciones especializadas en temas relativos a la seguridad informática cuyo personal está obligado a mantener la confidencialidad de los temas que trata.

4.1.6. Revisión Independiente de la Seguridad de la Información

La Unidad de Auditoría Interna o en su defecto quien sea designado por el Comité de Seguridad de la Información realizará revisiones independientes sobre la vigencia e implementación de la Política de Seguridad de la Información, a efectos de garantizar que las prácticas del Organismo 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 Universidad, 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 del Organismo.

En todos los contratos cuyo objeto sea la prestación de servicios a título personal bajo cualquier modalidad jurídica que deban desarrollarse dentro del Organismo, 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) Limpieza, "catering", 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 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 general de seguridad de la información de la Universidad.
b) Protección de los activos de la Universidad, incluyendo:
   - Procedimientos para proteger los bienes de la Universidad, 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.
   - Procedimientos para garantizar la integridad y disponibilidad de la información.
   - 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.

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 control de sistemas de información, redes y/o ambientes de PC de la Universidad, contemplarán además de los puntos especificados en "4.2.2. 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 de la Universidad.
d) Controles físicos y lógicos que se utilizarán para restringir y delimitar el acceso a la información sensible de la Universidad.
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 del Universidad 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

Generalidades

La Universidad debe tener un acabado conocimiento sobre los activos que posee como parte importante de la administración de riesgos. Algunos ejemplos de activos son:

- 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, aire acondicionado, etc.).

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

Frecuentemente, la información deja de ser sensible o crítica después de un cierto período 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 la Universidad.

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 ésta 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.
- Designar a los propietarios de la información existente en el Organismo.
- 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 la Universidad Nacional del Comahue, cualquiera sea el soporte en que se encuentre.

Responsabilidad

Los propietarios de la información son los encargados de clasificar la información de su propiedad de acuerdo con el grado de sensibilidad y criticidad de la misma, 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 la utilización de los recursos de la tecnología de información contemple 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.

Política

5.1. Inventario de activos

Se identificará 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 de 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: confidencialidad, integridad y confidencialidad.

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

- **Confidencialidad**:

    0- Información de dominio público que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado de la Universidad o no. SIN CLASIFICAR
    1- Información que puede ser conocida y utilizada por todos los empleados y algunos colaboradores externos autorizados, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para la Universidad. RESERVADA – USO INTERNO

2- Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas a la Universidad. RESERVADA - CONFIDENCIAL
3- Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección de la Universidad, y cuya divulgación o uso no autorizados podría ocasionar graves pérdidas al mismo. RESERVADA - SECRETA

- **Integridad**:

0- Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operatoria de la Universidad.
1- Información cuya modificación no autorizada puede repararse aunque podría ocasionar pérdidas leves para la Universidad.
2- Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas para la Universidad.
3- Información cuya modificación no autorizada no podría repararse, ocasionando graves pérdidas para la Universidad.

- **Disponibilidad**:

0- Información cuya inaccesibilidad no afecta la operatoria de la universidad.
1- Información cuya inaccesibilidad permanente durante 2 semanas podría ocasionar pérdidas significativas para la Universidad.
2- Información cuya inaccesibilidad permanente durante 2 días podría ocasionar pérdidas significativas para la Universidad.
3- Información cuya inaccesibilidad permanente durante 2 horas podría ocasionar pérdidas significativas para la Universidad.

Al referirse a pérdidas, se contemplan aquellas mensurables (materiales) y no mensurables (imagen, valor estratégico de la información, obligaciones contractuales o públicas, etc.).

Se asignará a la información un valor por cada uno de estos criterios. Luego, se clasificará la información en una de las siguientes categorías:

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

Sólo el Propietario de la Información puede asignar o cambiar su nivel de clasificación, cumpliendo con los siguientes requisitos previos:

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

Luego de clasificada la información, el propietario de la misma identificará los recursos asociados (sistemas, equipamiento, servicios, etc.) y los perfiles funcionales que deberán tener acceso a la misma.

En adelante se mencionará como "información clasificada" (o "datos clasificados") a aquella que se encuadre en los niveles 1, 2 o 3 de Confidencialidad.

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 tanto en formatos físicos como electrónicos e incorporarán 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.).

6. Seguridad del Personal

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, sin perjuicio de que éstos se presenten de todos modos. 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 de los mismos. 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

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, incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado.

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

Establecer Acuerdos 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 de la Universidad Nacional del Comahue, cualquiera sea su situación de revista, y al personal externo que efectúe tareas dentro del ámbito de la Universidad.

Responsabilidad

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 Acuerdos 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 y 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, supervisará la investigación, controlará la evolución e impulsará la resolución de los incidentes relativos a la seguridad.

El Responsable del Área Legal participará activamente en la confección del Acuerdo de Confidencialidad a firmar por los empleados, 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 Organismo es responsable del reporte de debilidades e incidentes de seguridad.

Política

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

6.1.1. Inclusión de la Seguridad en las Responsabilidades de 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 por la implementación y el mantenimiento de la Política de Seguridad, y las responsabilidades específicas por 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 Universidad.

6.1.3. Acuerdos de Confidencialidad

Como parte de sus términos y condiciones iniciales de empleo, los empleados, cualquiera sea su situación de revista, firmarán un Acuerdo de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información de la Universidad. La copia firmada del Acuerdo deberá ser retenida en forma segura por el Área de Recursos Humanos o por quien defina el Comité de Seguridad de la Información.

El "Acuerdo de Confidencialidad" deberá advertir que determinadas actividades pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad del empleado.

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

a) Suscripción inicial del Acuerdo por parte de la totalidad del personal.
b) Revisión del contenido del Acuerdo cada 1 año.
c) Método de resuscripción en caso de modificación del texto del Acuerdo.

6.1.4. Términos y Condiciones de Empleo

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

Las responsabilidades y derechos legales del empleado, 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.

También se incluirá la responsabilidad por la clasificación y administración de los sistemas y datos de la Universidad. Cuando corresponda, los términos y condiciones de empleo establecerán que estas responsabilidades se extienden más allá de los límites de la sede del Organismo y del horario normal de trabajo.

6.2. Capacitación del Usuario

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

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

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

Cada 6 meses se revisará el material correspondiente a la capacitación, a fin de evaluar la pertinencia de su actualización, de acuerdo al estado del arte de ese momento.

Las siguientes áreas serán encargadas de producir el material de capacitación

Áreas Responsables del Material de Capacitación
Área de capacitación

El personal que ingrese a la Universidad, recibirá el material indicando el comportamiento esperado en lo que respecta a la seguridad de la información, antes de serle otorgados los privilegios de acceso a los sistemas que correspondan.

Por otra parte, se arbitrarán los medios técnicos necesarios para comunicar a todo el personal, eventuales modificaciones o novedades en materia de seguridad, que deban ser tratadas con un orden preferencial.

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 o medios de comunicación oficiales 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 asignará los recursos necesarios para la investigación y resolución del incidente, y se encargará de su monitoreo.

Todos los empleados y contratistas deben conocer el procedimiento de comunicación de incidentes de seguridad, y deben informar de los mismos tan pronto hayan tomado conocimiento de su ocurrencia.

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.

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

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.

Se prohíbe a los usuarios quitar el software que supuestamente tiene una anomalía, a menos que estén autorizados formalmente para hacerlo. 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.

6.3.5. Procesos Disciplinarios

Se seguirá el proceso disciplinario formal contemplado en las normas estatutarias, escalafonarias y

convencionales que rigen al personal de la Administración Publica Nacional, para los empleados que violen la política, normas y procedimientos de seguridad del Organismo (Ver "12.4. Sanciones Previstas por Incumplimiento").

7. Seguridad Física y Ambiental

Generalidades

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

El control de los factores ambientales permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio. Deben contemplarse tanto los riesgos en las instalaciones del Organismo 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 Organismo. 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 Organismo pero situado físicamente fuera del mismo ("housing") así como en equipamiento ajeno que albergue sistemas y/o preste servicios de procesamiento de información al Organismo ("hosting").

La información almacenada en los sistemas de procesamiento y la documentación contenida en diferentes medios de almacenamiento, son susceptibles de ser recuperadas de los mismos 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 de la Universidad .

Proteger el equipamiento de procesamiento de información crítica de la Universidad ubicándolas 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 (ej.: "housing" y "hosting").

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

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 de la Universidad Nacional del Comahue y de todas las unidades académicas: instalaciones, equipamiento, cableado, medios de almacenamiento, etc.

Responsabilidad

El Responsable de Seguridad Informática definirá junto con los propietarios de información 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 del Organismo.

Los Responsables de Unidades Organizativas definirán los niveles de acceso físicos del personal de su incumbencia a las áreas restringidas.

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

La Unidad de Auditoría Interna o en su defecto quien sea designado por el Comité de Seguridad de la Información revisará los registros de acceso a las áreas protegidas.

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

Política

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 sedes del Organismo y de las instalaciones de procesamiento de información.

La Universidad 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 de Seguridad Informática (con asesoramiento a personal especializado), quienes lo definirán 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). 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.
c) Verificar la existencia de un área de recepción atendida por personal. Si esto no fuera posible se implementarán los siguientes medios alternativos de control de acceso físico al área o edificio.
d) El acceso a dichas áreas y edificios estará restringido exclusivamente al personal autorizado. Los métodos implementados registrarán cada ingreso y egreso en forma precisa.
e) Extender las barreras físicas 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.

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. Estos controles de acceso físico tendrán, por lo menos, las siguientes características:

a) Supervisar o inspeccionar a los visitantes a áreas protegidas y registrar la fecha y horario de su ingreso y egreso. Sólo se permitirá el acceso mediando propósitos específicos y autorizados 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 utilizarán 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 control biométrico, etc.). Se mantendrá un registro protegido para permitir auditar todos los accesos.

c) Revisar y actualizar cada 6 meses los derechos de acceso a las áreas protegidas, los que serán documentados y firmados por el Responsable de la Unidad Organizativa de la que dependa.

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

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, por ejemplo, filtración de agua desde otras instalaciones.

El Responsable de Seguridad Informática junto con el Responsable del Área Informática definirán los sitios clasificados como áreas protegidas de la Universidad Nacional del Comahue

Áreas Protegidas

Se establecen las siguientes medidas de protección para áreas protegidas:

a) Ubicar las instalaciones críticas en lugares a los cuales no pueda acceder personal no autorizado.
b) Establecer que los edificios o sitios donde se realicen actividades de procesamiento de

información serán discretos y ofrecerán un señalamiento mínimo de su propósito, sin signos obvios, exteriores o interiores.
c) Ubicar las funciones y el equipamiento de soporte, por ejemplo: impresoras, fotocopiadoras, máquinas de fax, adecuadamente dentro del área protegida para evitar solicitudes de acceso, el cual podría comprometer la información.
d) Establecer que las puertas y ventanas permanecerán cerradas cuando no haya vigilancia. Se agregará protección externa a las ventanas, en particular las que se encuentran en planta baja o presenten riesgos especiales.
e) Implementar los siguientes mecanismos de control para la detección de intrusos: alarmas y detectores de movimientos. Los mismos serán instalados según estándares profesionales y probados periódicamente. Estos mecanismos de control comprenderán todas las puertas exteriores y ventanas accesibles.
f) Separar las instalaciones de procesamiento de información administradas por la Universidad de aquellas administradas por terceros.
g) Restringir el acceso público a las guías telefónicas y listados de teléfonos internos que identifican las ubicaciones de las instalaciones de procesamiento de información sensible.
h) Almacenar los materiales peligrosos o combustibles en los siguientes lugares seguros a una distancia prudencial de las áreas protegidas.
i) Almacenar los equipos redundantes y la información de resguardo (back up) en un sitio seguro y distante del lugar de procesamiento, para evitar daños ocasionados ante eventuales contingencias en el sitio principal.

7.4. Desarrollo de Tareas en Áreas Protegidas

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

a) Dar a conocer al personal la existencia del área protegida, o de las actividades que allí se llevan a cabo, sólo si es necesario para el desarrollo de sus funciones.
b) Evitar la ejecución de trabajos por parte de terceros sin supervisión, tanto por razones de seguridad, como para evitar la posibilidad de que se lleven a cabo actividades maliciosas.
c) Bloquear físicamente e inspeccionar periódicamente las áreas protegidas desocupadas.
d) Limitar el acceso al personal del servicio de soporte externo a las áreas protegidas o a las instalaciones de procesamiento de información sensible. Este acceso, como el de cualquier otra persona ajena que requiera acceder al área protegida, será otorgado solamente cuando sea necesario y se encuentre autorizado y monitoreado. Se mantendrá un registro de todos los accesos de personas ajenas.
e) Pueden requerirse barreras y perímetros adicionales para controlar el acceso físico entre áreas con diferentes requerimientos de seguridad, y que están ubicadas dentro del mismo perímetro de seguridad.
f) Impedir el ingreso de equipos de computación móvil, fotográficos, de vídeo, audio o cualquier otro tipo de equipamiento que registre información, a menos que el Responsable de Seguridad Informática, lo autorice formalmente mediante los respectivos acuerdos.
g) Prohibir comer, beber y fumar dentro de las instalaciones de procesamiento de la información.

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.

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

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

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, 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	Llaves y control de ingreso
Incendio	Alarma de Incendios
Explosivos	Seguridad perimetral
Humo	Alarma de detección de humo
Inundaciones o filtraciones de agua (o falta de suministro)	Controles periódicos del área de servicios
Polvo	Controles periódicos del área de limpieza
Vibraciones	Controles periódicos del área de servicios
Efectos químicos	Controles periódicos del área de servicios
Interferencia en el suministro de energía eléctrica (cortes de suministro, variación de tensión)	Controles periódicos del área de servicios

Radiación electromagnética	Controles periódicos del área de servicios
Derrumbes	Controles periódicos del área de servicios

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. Esta revisión se realizará con la siguiente periodicidad: seis meses.
f) Considerar asimismo el impacto de las amenazas citadas en el punto d) que tengan lugar en zonas próximas a la sede del Organismo.

7.7. 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 los equipos. 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 ininterrumpible (UPS) para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas del Organismo. La determinación de dichas operaciones críticas, será el resultado del análisis de impacto realizado por el Responsable de Seguridad Informática conjuntamente con los propietarios de la información. Los planes de contingencia contemplarán las acciones que han de emprenderse ante una falla de la UPS. Los equipos de UPS serán inspeccionados y probados periódicamente para asegurar que funcionan correctamente y que tienen la autonomía requerida.
c) Montar un generador de respaldo para los casos en que el procesamiento deba continuar ante una falla prolongada en el suministro de energía. Deberá realizarse un análisis de impacto de las posibles consecuencias ante una interrupción prolongada del procesamiento, con el objeto de definir qué componentes será necesario abastecer de energía alternativa. 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 período prolongado. Cuando el encendido de los generadores no sea automático, se asegurará que el tiempo de funcionamiento de la UPS permita el encendido manual de los mismos. Los generadores serán inspeccionados y probados periódicamente para asegurar que funcionen según lo previsto.

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

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, mediante las siguientes acciones:

a) Cumplir con los requisitos técnicos vigentes de la República Argentina.
b) Utilizar pisoducto o cableado embutido en la pared, siempre que sea posible, cuando corresponda a las instalaciones de procesamiento de información.
c) Proteger el cableado de red contra intercepción no autorizada o daño mediante los siguientes controles: el uso de conductos evitando trayectos que atraviesen áreas públicas.
d) Separar los cables de energía de los cables de comunicaciones para evitar interferencias.
e) Proteger el tendido del cableado troncal (backbone) mediante la utilización de ductos blindados.

7.9. 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 sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.
c) Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.
d) Registrar el retiro de equipos de la sede del Organismo para su mantenimiento.
e) Eliminar la información confidencial que contenga cualquier equipo 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 Universidad, será autorizado por el Propietario de la Información almacenada en el mismo. La seguridad provista debe ser equivalente a la suministrada dentro del ámbito del Organismo para un propósito similar, teniendo en cuenta los riesgos de trabajar fuera de la misma.

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

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 instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera 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 Organismo (preferentemente en una caja fuerte o gabinete a prueba de incendios) cuando no está en uso, especialmente cuando no hay personal en la oficina.
c) Desconectar de la red / sistema / servicio las computadoras personales, terminales e impresoras asignadas a funciones críticas, cuando están desatendidas. Las mismas deben ser protegidas mediante cerraduras de seguridad, contraseñas u otros controles cuando no están en uso (como por 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 encontrarán 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 envío de correo postal y las máquinas de fax no atendidas.
e) Bloquear las fotocopiadoras (o protegerlas de alguna manera del uso no autorizado) fuera del horario normal de trabajo.
f) Retirar inmediatamente la información sensible o confidencial, una vez impresa.

7.13. Retiro de los Bienes

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

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

8. 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 Organismo, estableciendo procedimientos que aseguren la calidad de los procesos que se implementen en el ámbito operativo, a fin de minimizar los riesgos de incidentes producidos por la manipulación de información operativa.

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

Las comunicaciones establecidas permiten el intercambio de información, que 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

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

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

Alcance

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

Responsabilidad

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 prueba 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.
- Definir y documentar una norma clara con respecto al uso del correo electrónico.

- Controlar los mecanismos de distribución y difusión de información dentro del Organismo.
- Definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso y para garantizar la seguridad de los datos y los servicios conectados en las redes del Organismo.
- Desarrollar procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.
- Verificar el cumplimiento de las normas, procedimientos y controles establecidos.

El Responsable del Área 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 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 Informática y el Responsable del Área Legal del Organismo evaluarán los contratos y acuerdos con terceros para garantizar la incorporación de consideraciones relativas a la seguridad de la información afectada en la gestión de los productos o servicios prestados.

Política

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.

Los procedimientos especificarán instrucciones para la ejecución detallada de cada tarea, incluyendo:

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

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

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

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, asignando responsabilidades.

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.

8.1.3. Procedimientos de Manejo de Incidentes

Se establecerán responsabilidades y procedimientos de manejo de incidentes garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad (Ver también 6.3.1 – "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

   1) Fallas operativas
   2) Código malicioso
   3) Intrusiones
   4) Fraude informático
   5) Error humano
   6) Catástrofes naturales

b) Comunicar los incidentes a través de canales oficiales apropiados tan pronto como sea posible, de acuerdo a lo indicado en 6.3.1 – "Comunicación de Incidentes Relativos a la Seguridad".

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):

   1) Definición de primeras medidas
   2) Análisis e identificación de la causa del incidente.
   3) Planificación e implementación de soluciones para evitar la repetición del mismo, si fuera necesario.
   4) Comunicación con las personas afectadas o involucradas con la recuperación, del incidente.
   5) Notificación de la acción a la autoridad y/u Organismos pertinentes.

d) Registrar pistas de auditoría y evidencia similar para:

   1) Análisis de problemas internos.
   2) Uso como evidencia en relación con una probable violación contractual o infracción normativa, o en el caso de un proceso judicial, por ejemplo por aplicación de legislación sobre protección de datos (Ver "12.1.

Cumplimiento de Requisitos Legales").

3) 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:

1) Acceso a los sistemas y datos existentes sólo al personal claramente identificado y autorizado.
2) Documentación de todas las acciones de emergencia emprendidas en forma detallada.
3) Comunicación de las acciones de emergencia al titular de la Unidad Organizativa y revisión de su cumplimiento.
4) Constatación de la integridad de los controles y sistemas del Organismo en un plazo mínimo.

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

8.1.4. 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:

a) Monitoreo de las actividades.
b) Registros de auditoría y control periódico de los mismos.
c) Supervisión por parte de la Unidad de Auditoría Interna o en su defecto quien sea designado por el Comité de Seguridad de la Información, 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 la auditoría de seguridad, tomando recaudos para que ninguna persona pueda realizar actividades en áreas de responsabilidad única sin ser monitoreada, y la independencia entre el inicio de un evento y su autorización, considerando los siguientes puntos:

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

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.

Para ello, se tendrán en cuenta los siguientes controles:

a) Ejecutar el software de desarrollo y de operaciones, en diferentes ambientes de operaciones, equipos, o directorios.
b) Separar las actividades de desarrollo y prueba, en entornos diferentes.
c) Impedir el acceso a los compiladores, editores y otros utilitarios del sistema en el ambiente operativo, cuando no sean indispensables para el funcionamiento del mismo.
d) Utilizar sistemas de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas. Prohibir a los usuarios compartir contraseñas en estos sistemas. Las interfaces de los sistemas identificarán claramente a qué instancia se está realizando la conexión.
e) Definir propietarios de la información para cada un de los ambientes de procesamiento existentes.
f) 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 "8.1.4. Separación de Funciones".

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 y se incluirán en el contrato, contemplando las siguientes cuestiones específicas (Ver "4.3.1. Requerimientos de Seguridad en Contratos de Tercerización"):

a) Identificar las aplicaciones sensibles o críticas que convengan retener en el Organismo.
b) Obtener la aprobación de los propietarios de aplicaciones específicas.
c) Identificar las implicancias para la continuidad de los planes de las actividades del Organismo.
d) Especificar las normas de seguridad y el proceso de medición del cumplimiento.
e) Asignar responsabilidades específicas y procedimientos para monitorear con eficacia todas las actividades de seguridad.
f) Definir las responsabilidades 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 Organismo.

8.2. Planificación y Aprobación de Sistemas

8.2.1. Planificación de la Capacidad

El Responsable del Área Informática, o el personal designado por éste, deberá monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad, a fin de garantizar un procesamiento y almacenamiento adecuados. Para ello tomará en cuenta además los nuevos requerimientos de los sistemas así como las tendencias actuales y proyectadas en el procesamiento de la información del Organismo para el período estipulado de vida útil de cada componente. Asimismo, informará las necesidades detectadas a las autoridades competentes para que puedan identificar y evitar potenciales cuellos de botella, que podrían plantear una amenaza a la seguridad o a la continuidad del procesamiento, y puedan planificar una adecuada acción correctiva.

8.2.2. Aprobación del Sistema

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

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

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.

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:

a) Prohibir el uso de software no autorizado por el Organismo ("12.1.2.1. Derecho de Propiedad Intelectual del Software").
b) 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.
c) Instalar y actualizar periódicamente software de detección y reparación de virus, examinado computadoras y medios informáticos, tanto como medida precautoria como rutinaria.
d) Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles (probar dichas actualizaciones en un entorno de prueba previamente si es que constituyen cambios críticos a los sistemas).
e) Revisar periódicamente el contenido de software y datos de los sistemas que sustentan procesos críticos del Organismo investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.
f) Verificar, antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.
g) Redactar procedimientos para verificar toda la información relativa a software malicioso, garantizando que los boletines de alerta sean exactos e informativos.
h) Concientizar al personal acerca del problema de los falsos virus (hoax) y de cómo proceder frente a los mismos.

8.4. Mantenimiento

8.4.1. Resguardo de la Información

El Responsable de Seguridad Informática junto con 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 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 critico del Organismo. Los sistemas de resguardo deberán probarse periódicamente, asegurándose que cumplen con los requerimientos de los planes de continuidad de las actividades del organismo, según el punto – "11.5. Ensayo, Mantenimiento y Reevaluación de los Planes de Continuidad del Organismo." de esta política.

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

a) Definir un esquema de rótulo de las copias de resguardo, que permita contar con toda la información necesaria para identificar cada una de ellas y administrarlas debidamente.
b) Establecer un esquema de reemplazo de los medios de almacenamiento de las copias de resguardo, una vez concluida la posibilidad de ser reutilizados, de acuerdo a lo indicado por el proveedor.
c) Almacenar en una ubicación remota un nivel mínimo de información de resguardo, junto

con registros exactos y completos de las copias de resguardo y los procedimientos documentados de restauración, a una distancia suficiente como para evitar daños provenientes de un desastre en el sitio principal. Se deberán retener al menos tres generaciones o ciclos de información de resguardo para la información y el software esenciales para el Organismo. Para la definición de información mínima a ser resguardada en el sitio remoto, se deberá tener en cuenta el nivel de clasificación otorgado a la misma, en términos de disponibilidad (Ver "5.2. Clasificación de la información") y requisitos legales a los que se encuentre sujeta.

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

Los procedimientos de realización de copias de resguardo y su almacenamiento deberán respetar las disposiciones del punto – "Clasificación y Control de Activos" y – "12.1.3. Protección de los Registros del Organismo" de la presente Política.

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

La Unidad de Auditoría Interna o en su defecto quien sea designado por el Comité de Seguridad de la Información contrastará los registros de actividades del personal operativo con relación a los procedimientos operativos.

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.

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

a) Revisión de registros de fallas para garantizar que las mismas fueron resueltas satisfactoriamente.
b) Revisión de medidas correctivas para garantizar que los controles no fueron

comprometidos, y que las medidas tomadas fueron autorizadas.

c) Documentación de la falla con el objeto de prevenir su repetición o facilitar su resolución en caso de reincidencia.

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 del Organismo, contra el acceso no autorizado, considerando la ejecución de las siguientes acciones:

a) Establecer los procedimientos para la administración del equipamiento remoto, incluyendo los equipos en las áreas usuarias, la que será llevada a cabo por el responsable establecido en el punto – "4.1.2. Asignación de Responsabilidades en Materia de Seguridad de la Información".

b) Establecer controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados. Implementar controles especiales para mantener la disponibilidad de los servicios de red y computadoras conectadas.

c) Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información.

El Responsable del Área Informática, será responsable de la implementación de 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 el asesoramiento del Responsable de Seguridad Informática, implementará procedimientos para la administración de medios informáticos removibles, como cintas, discos, casetes e informes impresos. El cumplimiento de los procedimientos se hará de acuerdo al capítulo – "Control de Accesos".

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

a) Eliminar de forma segura los contenidos, si ya no son requeridos, de cualquier medio reutilizable que ha de ser retirado o reutilizado por el Organismo.

b) Requerir autorización para retirar cualquier medio del Organismo y realizar un control de todos los retiros a fin de mantener un registro de auditoría.

c) Almacenar todos los medios en un ambiente seguro y protegido, de acuerdo con las especificaciones de los fabricantes o proveedores.

Se documentarán todos los procedimientos y niveles de autorización, en concordancia con el capítulo – "Clasificación y Control de Activos".

8.6.2. Eliminación de Medios de Información

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

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

a) Documentos en papel.
b) Voces u otras grabaciones.
c) Papel carbónico.
d) Informes de salida.
e) Cintas de impresora de un solo uso.
f) Cintas magnéticas.
g) Discos o casetes removibles.
h) Medios de almacenamiento óptico (todos los formatos incluyendo todos los medios de distribución de software del fabricante o proveedor).
i) Listados de programas.
j) Datos de prueba.
k) Documentación del sistema.

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

8.6.3. Procedimientos de Manejo de la Información

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

Se contemplarán en los procedimientos las siguientes acciones:

a) Incluir en la protección a documentos, sistemas informáticos, redes, computación móvil, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general, multimedia, servicios e instalaciones postales, uso de máquinas de fax y cualquier otro ítem potencialmente sensible.
b) Restringir el acceso para identificar al personal no autorizado
c) Mantener un registro formal de los receptores autorizados de datos
d) Garantizar que los datos de entrada son completos, que el procesamiento se lleva a cabo correctamente y que se aplica la validación de salidas.
e) Proteger los datos en espera ("colas").
f) Conservar los medios de almacenamiento en un ambiente que concuerde con las especificaciones de los fabricantes o proveedores.

8.6.4. 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:

a) Almacenar la documentación del sistema en forma segura
b) Restringir el acceso a la documentación del sistema al personal estrictamente necesario. Dicho acceso será autorizado por el Propietario de la Información del 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, estos especificarán el grado de sensibilidad de la información del Organismo involucrada y las consideraciones de seguridad sobre la misma. Se tendrán en cuenta los siguientes aspectos:

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

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:

a) La utilización de medios de transporte o servicios de mensajería confiables. El Propietario de la Información a transportar aprobará los servicios de mensajería autorizados.
b) Suficiente embalaje para envío de medios a través de servicios postales o de mensajería, siguiendo las especificaciones de los fabricantes o proveedores.
c) Adoptar controles especiales, cuando resulte necesario, a fin de proteger la información sensible contra divulgación o modificación no autorizadas. Entre los ejemplos se incluyen:
    1) Uso de recipientes cerrados.
    2) Entrega en mano.
    3) Embalaje a prueba de apertura no autorizada (que revele cualquier intento de acceso).
    4) En casos excepcionales, división de la mercadería a enviar en más de una entrega y envío por diferentes rutas.

8.7.3. Seguridad del Gobierno Electrónico

El Responsable de Seguridad Informática verificará que los procedimientos de aprobación de Software del punto "8.2.2. 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 Organismo.
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**: Evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
i) **Órdenes**: Protección que requiere para mantener la confidencialidad, integridad y no repudio de la información sobre trámites y para evitar la pérdida o duplicación de transacciones.
j) **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 – "10.3.1. Política de Utilización de Controles Criptográficos." y tomando en cuenta el cumplimiento de los requisitos legales emanados de toda la normativa vigente.

Se documentarán los acuerdos de gobierno electrónico entre partes que comprometan a las mismas a respetar los términos y condiciones acordados, incluyendo los detalles de autorización, requiriéndose otros acuerdos con proveedores de servicios de información y de redes que aporten beneficios adicionales.

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

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 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 Organismo, por ejemplo, el efecto del incremento en la velocidad de envío o el efecto de enviar mensajes formales de persona a persona en lugar de mensajes entre organizaciones.
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 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 (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.).

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.

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

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

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 que podría dañar la reputación del Organismo 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 con leyes, normas y estatutos 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. El Comité de Seguridad de la Información designará a los responsables de dicha aprobación.

Todos los sistemas de acceso público deberán prever que:

a) La información se obtenga de acuerdo con la legislación de protección de datos.
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.

Asimismo, se garantizará la validez y vigencia de la información publicada, con el objeto de preservar la imagen de la Universidad.

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, contemplando las siguientes acciones:

a) Concientizar al personal sobre la toma de debidas precauciones, por ejemplo no revelar información sensible como para evitar ser escuchado o interceptado, al hacer una llamada telefónica, por:

   1) Personas cercanas, en especial al utilizar teléfonos móviles.
   2) Terceros que tengan acceso a la comunicación mediante la Intervención de la línea telefónica, y otras formas de escucha subrepticias, a través del acceso físico al aparato o a la línea telefónica, o mediante equipos de barrido de frecuencias al utilizar teléfonos móviles análogos.
   3) Terceros en el lado receptor.

b) Recordar al personal que no sostengan conversaciones confidenciales en lugares públicos u oficinas abiertas y lugares de reunión con paredes delgadas.

c) No dejar mensajes en contestadores automáticos puesto que éstos pueden ser escuchados por personas no autorizadas, almacenados en sistemas públicos o almacenados incorrectamente como resultado de un error de discado.

d) Recordar al personal los problemas ocasionados por el uso de máquinas de fax, en particular:

   1) El acceso no autorizado a sistemas incorporados de almacenamiento de mensajes con el objeto de recuperarlos.
   2) La programación deliberada o accidental de equipos para enviar mensajes a determinados números.
   3) El envío de documentos y mensajes a un número equivocado por errores de discado o por utilizar el número almacenado equivocado.

9. Control de Accesos

Generalidades

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

Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de

todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso.

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 identificación y autenticación.

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

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

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

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

Alcance

La Política definida en este documento se aplica a todas las formas de acceso de aquellos a quienes se les haya otorgado permisos sobre los sistemas de información, bases de datos o servicios de información del Organismo, cualquiera sea la función que desempeñe.

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

Responsabilidad

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 Responsable 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 a los servicios y recursos de red y a Internet de los usuarios a su cargo.

El Responsable del Área Informática será responsable de:
- Implementar procedimientos para la activación y desactivación de derechos de acceso a las redes.
- 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 identificación y autenticación de usuarios (biometría, verificación de firma, uso de autenticadores de hardware).
- Definir e implementar la configuración que debe efectuarse para cada servicio de red, de manera

de garantizar la seguridad en su operatoria.
- Analizar las medidas a ser implementadas para efectivizar el control de acceso a Internet de los usuarios.
- Otorgar acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal correspondiente.
- Efectuar un control de los registros de auditoría generados por los sistemas operativos y de comunicaciones.

La Unidad de Auditoría Interna o en su defecto quien sea designado por el Comité de Seguridad de la Información, tendrá acceso a los registros de eventos a fin de colaborar en el control y efectuar recomendaciones sobre modificaciones a los aspectos de seguridad.

El Comité de Seguridad de la Información aprobará el análisis de riesgos de la información efectuado, la implementación de técnicas de identificación y autenticación de usuarios y alarmas silenciosas. Asimismo, aprobará el período definido para el mantenimiento de los registros de auditoría generados.

Política

9.1. Requerimientos para el Control de Acceso

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

9.1.2. Reglas de Control de Acceso

Las reglas de control de acceso especificadas, deberán:

a) Indicar expresamente si las reglas son obligatorias u optativas
b) Establecer reglas sobre la premisa "Todo debe estar prohibido a menos que se permita expresamente" y no sobre la premisa inversa de "Todo está permitido a menos que se prohíba expresamente".
c) Controlar los cambios en los rótulos de información que son iniciados automáticamente

por herramientas de procesamiento de información, de aquellos que son iniciados a discreción del usuario (Ver ". Clasificación y Control de Activos").

d) Controlar los cambios en los permisos de usuario que son iniciados automáticamente por el sistema de información y aquellos que son iniciados por el administrador.

e) Controlar las reglas que requieren la aprobación del administrador o del Propietario de la Información de que se trate, antes de entrar en vigencia, y aquellas que no requieren aprobación.

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. Registración de Usuarios

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

a) Utilizar identificadores de usuario únicos, de manera que se pueda vincular y hacer responsables 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 son 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 Organismo, 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 Organismo o sufrieron la perdida/robo de sus credenciales de acceso.

i) Efectuar revisiones periódicas con el objeto de:
   - cancelar identificadores y cuentas de usuario redundantes
   - inhabilitar cuentas inactivas por más de ..... (indicar período no mayor a 60 días)
   - eliminar cuentas inactivas por más de..... (indicar período no mayor a 120 días)

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

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

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

9.2.2. Administración de Privilegios

Se limitará y controlará la asignación y uso de privilegios (cualquier característica o servicio de un sistema de información multiusuario que permita que el usuario pase por alto los controles de sistemas o aplicaciones), 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 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, lo cual será controlado por el Responsable de Seguridad Informática, y solicitar su implementación.

9.2.3. 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 acusar recibo de la recepción de la misma.

d) Almacenar las contraseñas sólo en sistemas informáticos protegidos.

e) Utilizar otras tecnologías de identificación y autenticación de usuarios, como la biométrica (por ejemplo verificación de huellas dactilares), verificación de firma y uso de autenticadores de hardware (como las tarjetas de circuito integrado). Para ello, el Comité de Seguridad de la Información dispondrá, cuando la evaluación de riesgos realizada por el Responsable de Seguridad Informática conjuntamente con el Responsable del Área de Informática lo determine, el uso de estas herramientas.

f) Configurar los sistemas operativos de red de tal manera que:
   - las contraseñas tengan ..... (especificar cantidad no menor a 8 caracteres),
   - suspendan o bloqueen permanentemente al usuario luego de ..... (especificar cantidad no mayor a 3) intentos de entrar con una contraseña incorrecta (deberá pedir la rehabilitación al responsable de administración de seguridad),
   - solicitar el cambio de la contraseña cada ..... (especificar lapso no mayor a 45 días),
   - impedir que las últimas ..... (especificar cantidad no menor a 12) contraseñas no sean reutilizadas,
   - establecer un tiempo de vida mínimo de ..... (especificar cantidad no mayor a 3) días para las contraseñas.

9.2.4. Administración de Contraseñas Críticas

En los diferentes ambientes de procesamiento 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 que contemplen lo siguiente:

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

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 .....

(indicar periodicidad no mayor a seis meses), a fin de revisar los derechos de acceso de los usuarios. Se deberán contemplar los siguientes controles:

a) Revisar los derechos de acceso de los usuarios a intervalos de seis meses y después de cualquier cambio.
b) Revisar las autorizaciones de privilegios especiales de derechos de acceso a intervalos de tres meses.
c) Revisar las asignaciones de privilegios a intervalos de seis meses, a fin de garantizar que no se obtengan privilegios no autorizados.

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. También permiten la identificación de las actividades realizadas en los sistemas de información.

Los usuarios deben cumplir las siguientes directivas:

a) Mantener las contraseñas en secreto.
b) Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
c) Seleccionar contraseñas de calidad, de acuerdo a las prescripciones informadas por el Responsable del Activo de Información de que se trate, que:
    1. Sean fáciles de recordar.
    2. No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo nombres, números de teléfono, fecha de nacimiento, etc.
    3. No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.
d) Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.
e) Cambiar las contraseñas provisorias en el primer inicio de sesión ("log on").
f) Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquéllas almacenadas en una tecla de función o macro.
g) Notificar de acuerdo a lo establecido en 6.3.1 – "Comunicación de Incidentes Relativos a la Seguridad", cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

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

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 estaciones de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos durante un período extenso de tiempo.

El Responsable de Seguridad Informática debe disponer las tareas de concientización a todos los usuarios y contratistas, acerca de los requerimientos y procedimientos de seguridad, para la protección de equipos desatendidos, así como de sus responsabilidades por la implementación de dicha protección.

Los usuarios cumplirán con las siguientes pautas:

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

9.4. Control de Acceso a la Red

9.4.1. Política de Utilización de los Servicios de Red

Las conexiones no seguras a los servicios de red pueden afectar a todo el Organismo, por lo tanto, se controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos.

El Responsable del Área Informática tendrá a cargo el otorgamiento acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal de un titular de una Unidad Organizativa que lo solicite para personal de su incumbencia.

Este control es particularmente importante para las conexiones de red a aplicaciones que procesen información clasificada o aplicaciones críticas, o a usuarios que utilicen el acceso desde sitios de alto riesgo, por ejemplo, áreas públicas o externas que están fuera de la administración y del control de seguridad del Organismo.

Para ello, se desarrollarán procedimientos para la activación y desactivación de derechos de acceso a las redes, los cuales comprenderán:

a) Identificar las redes y servicios de red a los cuales se permite el acceso.
b) Realizar normas y procedimientos de autorización para determinar las personas y, las redes y servicios de red a los cuales se les otorgará el acceso.

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

Esta Política será coherente con la Política de Control de Accesos del Organismo (Ver "9.1.1. Política de Control de Accesos").

9.4.2. Camino Forzado

Las redes están diseñadas para permitir el máximo alcance de distribución de recursos y flexibilidad en la elección de la ruta a utilizar. Estas características también pueden ofrecer oportunidades para el acceso no autorizado a las aplicaciones del Organismo, o para el uso no autorizado de servicios de información. Por esto, 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 mismo se encuentra autorizado a acceder, mediante la implementación de controles en diferentes puntos de la misma.

A continuación se enumeran algunos ejemplos a considerar en caso de implementar estos controles a los sistemas existentes:

a) Asignar, números IPs.
b) Establecer la conexión automática de puertos a gateways de seguridad o a sistemas de aplicación específicos.
c) Limitar las opciones de menú y submenú de cada uno de los usuarios.
d) Evitar la navegación ilimitada por la red.
e) Imponer el uso de sistemas de aplicación y/o gateways de seguridad específicos para usuarios externos de la red.
f) Controlar activamente las comunicaciones con origen y destino autorizados a través de un gateway, por ejemplo utilizando firewalls.
g) Restringir el acceso a redes, estableciendo dominios lógicos separados, por ejemplo, redes privadas virtuales para grupos de usuarios dentro o fuera del Organismo.

Los requerimientos relativos a caminos forzados se basarán en la Política de Control de Accesos del Organismo (Ver "9.1.1. Política de Control de Accesos"). El Responsable de Seguridad Informática, conjuntamente con el Propietario de la Información de que se trate, realizarán una evaluación de riesgos a fin de determinar los mecanismos de control que corresponda en cada caso.

9.4.3. Autenticación de Usuarios para Conexiones Externas

Las conexiones externas son de gran potencial para accesos no autorizados a la información del Organismo. Por consiguiente, el acceso de usuarios remotos estará sujeto al cumplimiento de procedimientos de autenticación. Existen diferentes métodos de autenticación, algunos de los cuales brindan un mayor nivel de protección que otros. El Responsable de Seguridad Informática, conjuntamente con el Propietario de la Información de que se trate, realizarán una evaluación de riesgos a fin de determinar el mecanismo de autenticación que corresponda en cada caso.

La autenticación de usuarios remotos puede llevarse a cabo utilizando:

a) Un método de autenticación físico (por ejemplo tokens de hardware), para lo que debe implementarse un procedimiento que incluya:

- Asignación de la herramienta de autenticación.
- Registro de los poseedores de autenticadores.
- Mecanismo de rescate al momento de la desvinculación del personal al que se le otorgó.
- Método de revocación de acceso del autenticador, en caso de compromiso de seguridad.

b) Un protocolo de autenticación (por ejemplo desafío / respuesta), para lo que debe implementarse un procedimiento que incluya:

- Establecimiento de las reglas con el usuario.
- Establecimiento de un ciclo de vida de las reglas para su renovación.

c) También pueden utilizarse líneas dedicadas privadas o una herramienta de verificación de la dirección del usuario de red, a fin de constatar el origen de la conexión.

Los procedimientos y controles de re-llamada o dial-back, pueden brindar protección contra conexiones no autorizadas y no deseadas a las instalaciones de procesamiento de información del Organismo. Al aplicar este tipo de control, el Organismo no debe utilizar servicios de red que incluyan desvío de llamadas o, si lo hacen, deben inhabilitar el uso de dichas herramientas para evitar las debilidades asociadas con la misma. Asimismo, es importante que el proceso de re-llamada garantice que se produzca una desconexión real del lado del Organismo.

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 del Organismo. Por consiguiente, las conexiones a sistemas informáticos remotos serán autenticadas. Esto es particularmente importante si la conexión utiliza una red que está fuera de control de la gestión de seguridad del Organismo. En el punto anterior se mencionan algunos ejemplos de autenticación y de cómo puede lograrse. La autenticación de nodos puede servir como un medio alternativo de autenticación de grupos de usuarios remotos, cuando éstos están conectados a un servicio informático seguro y compartido.

9.4.5. Protección de los Puertos (Ports) de Diagnóstico Remoto

Muchas computadoras y sistemas de comunicación son instalados y administrados con una herramienta de diagnóstico remoto. Si no están protegidos, estos puertos de diagnóstico proporcionan un medio de acceso no autorizado. Por consiguiente, serán protegidos por un mecanismo de seguridad apropiado, con las mismas características del punto – "9.4.3. Autenticación de Usuarios para Conexiones Externas". También para este caso deberá tenerse en cuenta el punto "9.4.2. Camino Forzado".

9.4.6. Subdivisión de Redes

Para controlar la seguridad en redes extensas, se podrán dividir en dominios lógicos separados. Para esto se definirán y documentarán los perímetros de seguridad que sean convenientes. Estos perímetros se implementarán mediante la instalación de "gateways" con funcionalidades de "firewall" o redes privadas virtuales, para filtrar el tráfico entre los dominios (Ver "9.4.8. Control de Conexión a la Red" y "9.4.9. Control de Ruteo de Red") y para bloquear el acceso no autorizado de acuerdo a la Política de Control de Accesos (Ver "9.1. Requerimientos ").

La subdivisión en dominios de la red tomará en cuenta criterios como los requerimientos de seguridad comunes de grupos de integrantes de la red, la mayor exposición de un grupo a peligros externos, separación física, u otros criterios de aglutinamiento o segregación preexistentes.

Basándose en la Política de Control de Accesos y los requerimientos de acceso (Ver "9.1. Requerimientos "), el Responsable del Área Informática evaluará el costo relativo y el impacto en el desempeño que ocasione la implementación de enrutadores o gateways adecuados (Ver "9.4.8. Control de Conexión a la Red" y "9.4.9. Control de Ruteo de Red") para subdividir la red. Luego decidirá, junto con el Responsable de Seguridad Informática el esquema más apropiado a implementar.

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 procedimientos para solicitar y aprobar accesos a Internet. Los accesos serán autorizados por el Responsable de la Unidad Organizativa a cargo del empleado solicitante. Asimismo, se definirán las pautas de utilización de Internet para todos los usuarios.

Se evaluará la conveniencia de generar un registro de los accesos de los usuarios a Internet, con el objeto de realizar revisiones de los accesos efectuados o analizar casos particulares. Dicho control será comunicado a los usuarios de acuerdo a lo establecido en el punto – "6.1.3. Acuerdos de Confidencialidad". Para ello, el Responsable de Seguridad Informática junto con el Responsable del Área de Informática analizarán las medidas a ser implementadas para efectivizar dicho control, como ser la instalación de "firewalls", "proxies", etc.

9.4.8. Control de Conexión a la Red

Sobre la base de lo definido en el punto "9.1. Requerimientos ", se implementarán controles para limitar la capacidad de conexión de los usuarios. Dichos controles se podrán implementar en los "gateways" que separen los diferentes dominios de la red (Ver "9.4.6. Subdivisión de Redes").

Algunos ejemplos de los entornos a las que deben implementarse restricciones son:

a) Correo electrónico.
b) Transferencia de archivos.

c) Acceso interactivo.
d) Acceso a la red fuera del horario laboral.

9.4.9. Control de Ruteo de Red

En las redes compartidas, especialmente aquellas que se extienden de los límites del Organismo, se incorporarán controles de ruteo, para asegurar que las conexiones informáticas y los flujos de información no violen la Política de Control de Accesos (Ver "9.1.1. Política de Control de Accesos"). Estos controles contemplarán mínimamente la verificación positiva de direcciones de origen y destino. Adicionalmente, para este objetivo pueden utilizarse diversos métodos incluyendo entre otros autenticación de protocolos de ruteo, ruteo estático, traducción de direcciones y listas de control de acceso.

9.4.10. Seguridad de los Servicios de Red

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

Para ello se tendrán en cuenta las siguientes directivas:

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

Dicha configuración será revisada periódicamente por el Responsable de Seguridad Informática.

9.5. Control de Acceso al Sistema Operativo

9.5.1. Identificación Automática de Terminales

El Responsable de Seguridad Informática realizará una evaluación de riesgos a fin de determinar el método de protección adecuado del acceso al Sistema Operativo. Esta evaluación contará con la aprobación del Comité de Seguridad de la Información.

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

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

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.

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

El procedimiento de identificación deberá:

a) Mantener en secreto los identificadores de sistemas o aplicaciones hasta tanto se haya llevado a cabo exitosamente el proceso de conexión.
b) Desplegar un aviso general advirtiendo que sólo los usuarios autorizados pueden acceder a la computadora.
c) Evitar dar mensajes de ayuda que pudieran asistir a un usuario no autorizado durante el procedimiento de conexión.
d) Validar la información de la conexión sólo al completarse la totalidad de los datos de entrada. Si surge una condición de error, el sistema no debe indicar que parte de los datos es correcta o incorrecta.
e) Limitar el número de intentos de conexión no exitosos permitidos y:
   - Registrar los intentos no exitosos.
   - Impedir otros intentos de identificación, una vez superado el límite permitido.
   - Desconectar conexiones de comunicaciones de datos.
f) Limitar el tiempo máximo permitido para el procedimiento de conexión. Si este es excedido, el sistema debe finalizar la conexión.
g) Desplegar la siguiente información, al completarse una conexión exitosa:
   - Fecha y hora de la conexión exitosa anterior.
   - Detalles de los intentos de conexión no exitosos desde la última conexión exitosa.

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 personal exclusivo, de manera que las actividades puedan rastrearse con posterioridad hasta llegar al individuo responsable. Los identificadores de usuario no darán ningún indicio del nivel de privilegio otorgado.

En circunstancias excepcionales, cuando existe un claro beneficio para el Organismo, podrá utilizarse un identificador compartido para un grupo de usuarios o una tarea especifica. Para casos de esta índole, se documentará la justificación y aprobación del Propietario de la Información de que se trate.

Si se utilizará un método de autenticación físico (por ejemplo autenticadores de hardware), deberá implementarse un procedimiento que incluya:

a) Asignar la herramienta de autenticación.
b) Registrar los poseedores de autenticadores.
c) Rescatar el autenticador al momento de la desvinculación del personal al que se le otorgó.
d) Revocar el acceso del autenticador, en caso de compromiso de seguridad.

9.5.4. Sistema de Administración de Contraseñas

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

El sistema de administración de contraseñas debe:

a) Imponer el uso de contraseñas individuales para determinar responsabilidades.
b) Permitir que los usuarios seleccionen y cambien sus propias contraseñas (luego de cumplido el plazo mínimo de mantenimiento de 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 9.3.1 – "9.3.1. Uso de Contraseñas".
d) Imponer cambios en las contraseñas en aquellos casos en que los usuarios mantengan sus propias contraseñas, según lo señalado en el punto 9.3.1 – "9.3.1. Uso de Contraseñas".
e) Obligar a los usuarios a cambiar las contraseñas temporarias en su primer procedimiento de identificación, en los casos en que ellos seleccionen sus contraseñas.
f) Mantener un registro de las últimas contraseñas del 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, hubs, routers, etc.).

9.5.5. Uso de Utilitarios de Sistema

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

a) Utilizar procedimientos de autenticación para utilitarios del sistema.
b) Separar entre utilitarios del sistema y software de aplicaciones.
c) Limitar el uso de utilitarios del sistema a la cantidad mínima viable de usuarios fiables y autorizados.

d) Evitar que personas ajenas al Organismo tomen conocimiento de la existencia y modo de uso de los utilitarios instalados en las instalaciones informáticas.
e) Establecer autorizaciones para uso ad hoc de utilitarios de sistema.
f) Limitar la disponibilidad de utilitarios de sistema, por ejemplo durante el transcurso de un cambio autorizado.
g) Registrar todo uso de utilitarios del sistema.
h) Definir y documentar los niveles de autorización para utilitarios del sistema.
i) Remover todo el software basado en utilitarios y software de sistema innecesarios.

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, con aprobación del Comité de Seguridad de la Información. En este caso, se definirán y asignarán responsabilidades y procedimientos para responder a la activación de una alarma silenciosa.

9.5.7. Desconexión de Terminales por Tiempo Muerto

El Responsable de Seguridad Informática, junto con los propietarios de información definirán cuáles se consideran terminales de alto riesgo, por ejemplo áreas públicas o externas fuera del alcance de la gestión de seguridad del Organismo, o que sirven a sistemas de alto riesgo. Las mismas se apagarán después de un periodo definido de inactividad, para evitar el acceso de personas no autorizadas. Esta herramienta de desconexión por tiempo muerto deberá limpiar la pantalla de la terminal y deberá cerrar tanto la sesión de la aplicación como la de red, después de un periodo definido de inactividad. El lapso por tiempo muerto responderá a los riesgos de seguridad del área y de los usuarios de 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 agente debe abandonar su puesto de trabajo momentáneamente, activará protectores de pantalla con contraseñas, a los efectos de evitar que terceros puedan ver su trabajo o continuar con la sesión de usuario habilitada.

9.5.8. Limitación del Horario de Conexión

Las restricciones al horario de conexión deben suministrar seguridad adicional a las aplicaciones de alto riesgo. La limitación del periodo durante el cual se permiten las conexiones de terminales a los servicios informáticos reduce el espectro de oportunidades para el acceso no autorizado. Se implementará un control de esta índole para aplicaciones informáticas sensibles, especialmente aquellas terminales instaladas en ubicaciones de alto riesgo, por ejemplo áreas publicas o externas que estén fuera del alcance de la gestión de seguridad del Organismo.

Entre los controles que se deben aplicar, se enuncian:

a) Utilizar lapsos predeterminados, por ejemplo para transmisiones de archivos en lote, o sesiones interactivas periódicas de corta duración.
b) Limitar los tiempos de conexión al horario normal de oficina, de no existir un requerimiento operativo de horas extras o extensión horaria.
c) Documentar debidamente los agentes que no tienen restricciones horarias y las razones de su autorización. También cuando el Propietario de la Información autorice excepciones para una extensión horaria ocasional.

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 del Organismo para el acceso a la información, (Ver "9.1. Requerimientos ").

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

a) Proveer una interfaz para controlar el acceso a las funciones de los sistemas de aplicación. El Propietario de la Información involucrada será responsable de la adjudicación de accesos a las funciones. En el caso de que las actividades involucradas en el otorgamiento de acceso revistan un carácter técnico elevado, las mismas serán llevadas a cabo por personal del área de sistemas, conforme a una autorización formal emitida por el Propietario de la Información.
b) Restringir el conocimiento de los usuarios acerca de la información o de las funciones de los sistemas de aplicación a las cuales no sean autorizados a acceder, con la adecuada edición de la documentación de usuario.
c) Controlar los derechos de acceso de los usuarios, por ejemplo, lectura, escritura, supresión y ejecución.
d) Garantizar que las salidas de los sistemas de aplicación que administran información sensible, contengan sólo la información que resulte pertinente para el uso de la salida, y que la misma se envíe solamente a las terminales y ubicaciones autorizadas.
e) Revisar periódicamente dichas salidas a fin de garantizar la remoción de la información redundante.
f) Restringir el acceso a la información por fuera del sistema encargado de su procesamiento, es decir, la modificación directa del dato almacenado.

9.6.2. Aislamiento de los Sistemas Sensibles

Los sistemas sensibles podrían requerir de un ambiente informático dedicado (aislado). Algunos sistemas de aplicación son suficientemente sensibles a pérdidas potenciales y requieren un tratamiento especial. 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. Son aplicables las siguientes consideraciones:

a) Identificar y documentar claramente la sensibilidad de un sistema de aplicación. Esta tarea será llevada a cabo por el administrador de la aplicación (Ver ". Clasificación y Control de Activos").
b) Identificar y acordar con el administrador de la aplicación sensible cuando la aplicación ha de ejecutarse en un ambiente compartido, los sistemas de aplicación con los cuales ésta compartirá los recursos.
c) Coordinar con el Responsable del Área informática, qué servicios estarán disponibles en el entorno donde se ejecutará la aplicación, de acuerdo a los requerimientos de operación y seguridad especificados por el administrador de la aplicación.
d) Considerar la seguridad en la administración de las copias de respaldo de la información que procesan las aplicaciones.
e) Considerar las mismas precauciones de seguridad y privacidad, en la elaboración del plan de continuidad y/o contingencia de la ejecución de la aplicación. Ejemplo: el equipamiento alternativo o las instalaciones de emergencia donde restablecer la aplicación.

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:

a) Identificación del usuario.
b) Fecha y hora de inicio y terminación.
c) Identidad o ubicación de la terminal, si se hubiera dispuesto identificación automática para la misma (Ver "9.5.1. Identificación Automática de Terminales").
d) Registros de intentos exitosos y fallidos de acceso al sistema.
e) Registros de intentos exitosos y fallidos de acceso a datos y otros recursos.

En todos los casos, los registros de auditoría serán archivados preferentemente en un equipo diferente al que los genere y conforme los requerimientos de la Política de Retención de Registros (Ver "12.1.7. Recolección de Evidencia").

Los propietarios de la información definirán un cronograma de depuración de registros en línea en función a normas vigentes, y a sus propias necesidades. Esto será aprobado por el Comité de Seguridad de la Información.

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.

Todos los empleados deben conocer el alcance preciso del uso adecuado de los recursos informáticos, y se les advertirá que determinadas actividades pueden ser objeto de control y monitoreo (Ver "12.1.5. Prevención del Uso Inadecuado de los Recursos de Procesamiento de Información").

El alcance de estos procedimientos deberá corresponderse a la evaluación de riesgos que realice el Responsable del Área Informática y el Responsable de Seguridad Informática (Ver "10.4.1. Control del Software Operativo").

Entre las áreas que deben tenerse en cuenta se enumeran las siguientes:

a) Acceso no autorizado, incluyendo detalles como:
   1. Identificación del usuario.
   2. Fecha y hora de eventos clave.
   3. Tipos de eventos.
   4. Archivos a los que se accede.
   5. Utilitarios y programas utilizados.

b) Todas las operaciones con privilegio, como:
   1. Utilización de cuenta de supervisor.
   2. Inicio y cierre del sistema.
   3. Conexión y desconexión de dispositivos de Ingreso y Salida de información o que permitan copiar datos.
   4. Cambio de fecha/hora.
   5. Cambios en la configuración de la seguridad.
   6. Alta de servicios.

c) Intentos de acceso no autorizado, como:
   1. Intentos fallidos.
   2. Violaciones de la Política de Accesos y notificaciones para "gateways" de red y "firewalls".
   3. Alertas de sistemas de detección de intrusiones.

d) Alertas o fallas de sistema como:
   1. Alertas o mensajes de consola.
   2. Excepciones del sistema de registro.
   3. Alarmas del sistema de administración de redes.
   4. Accesos remotos a los sistemas.

9.7.2.2. Factores de Riesgo

Entre los factores de riesgo que se deben considerar se encuentran:

a) La criticidad de los procesos de aplicaciones.
b) El valor, la sensibilidad o criticidad de la información involucrada.
c) La experiencia acumulada en materia de infiltración y uso inadecuado del sistema.
d) El alcance de la interconexión del sistema (en particular las redes públicas).

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.

Si el volumen de la información contenida en alguno de los registros fuera muy grande, el procedimiento indicará cuales de los registros más significativos se copiarán automáticamente en registros auxiliares.

Por otra parte, el Responsable del Área Informática, podrá disponer la utilización de herramientas de auditoría o utilitarios adecuados para llevar a cabo el control de los registros.

En la asignación de responsabilidades en materia de seguridad de la información (Ver "4.1. Infraestructura de la Seguridad de la Información"), se deberá separar las funciones entre quienes realizan la revisión y aquellos cuyas actividades están siendo monitoreadas.

Las herramientas de registro deberán contar con los controles de acceso necesarios, a fin de garantizar que no ocurra:

a) La desactivación de la herramienta de registro.
b) La alteración de mensajes registrados.
c) La edición o supresión de archivos de registro.
d) La saturación de un medio de soporte de archivos de registro.
e) La falla en los registros de los eventos.
f) La sobre escritura de los registros.

La Unidad de Auditoría Interna o en su defecto quien sea designado por el Comité de Seguridad de la Información, tendrá acceso a los registros de eventos a fin de colaborar en el control y efectuar recomendaciones sobre modificaciones a los aspectos de seguridad. Adicionalmente podrían evaluar las herramientas, pero no tendrán libre acceso a ellas.

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 de cualquier variación significativa.

9.8. Computación Móvil y Trabajo Remoto

9.8.1. Computación Móvil

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

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

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

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

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

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

a) Permanecer siempre cerca del dispositivo.
b) No dejar desatendidos los equipos.
c) No llamar la atención acerca de portar un equipo valioso.
d) No poner identificaciones del Organismo en el dispositivo.
e) No poner datos de contacto técnico en el dispositivo.
f) Mantener cifrada la información clasificada.

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

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

9.8.2. Trabajo Remoto

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

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

Estos casos serán de excepción y serán contemplados en situaciones que justifiquen la imposibilidad de otra forma de acceso y urgencia del mismo tales como horarios del Organismo, solicitudes de la Superioridad, etc.

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

a) La seguridad física existente en el sitio de trabajo remoto, tomando en cuenta la seguridad física del edificio y del ambiente local.
b) El ambiente de trabajo remoto propuesto.
c) Los requerimientos de seguridad de comunicaciones, tomando en cuenta la necesidad de acceso remoto a los sistemas internos del Organismo, la sensibilidad de la información a la que se accederá y que pasará a través del vinculo de comunicación y la sensibilidad del sistema interno.
d) La amenaza de acceso no autorizado a información o recursos por parte de otras personas que utilizan el lugar, por ejemplo, familia y amigos.
e) Evitar la instalación / desinstalación de software no provisto por el Organismo.

Los controles y disposiciones comprenden:

a) Proveer de mobiliario para almacenamiento y equipamiento adecuado para las actividades de trabajo remoto.
b) Definir el trabajo permitido, el horario de trabajo, la clasificación de la información que se puede almacenar en el equipo remoto desde el cual se accede a la red del Organismo y los sistemas internos y servicio a los cuales el trabajador remoto está autorizado a acceder.
c) Proveer de un adecuado equipo de comunicación, con inclusión de métodos para asegurar el acceso remoto.
d) Incluir seguridad física.
e) Definir reglas y orientación para cuando familiares y visitantes accedan al equipo e información.
f) Proveer el hardware y el soporte y mantenimiento del software.
g) Definir los procedimientos de backup y de continuidad de las operaciones.
h) Efectuar auditoría y monitoreo de la seguridad.
i) Realizar la anulación de las autorizaciones, derechos de acceso y devolución del equipo cuando finalicen las actividades remotas.

Se implementarán procesos de auditoría específicos para los casos de accesos remotos, que serán

revisados regularmente. Se llevará un registro de incidentes a fin de corregir eventuales fallas en la seguridad de este tipo de accesos.

10. Desarrollo y Mantenimiento de Sistemas

Generalidades

El desarrollo y mantenimiento de las aplicaciones, tanto comerciales como propias, es un punto crítico de la seguridad.

Durante el análisis y diseño de los procesos que soportan estas aplicaciones se debe 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, encontrar rápidamente al responsable.

Asimismo, una adecuada administración de la infraestructura de base, Sistemas Operativos y Software de Base, en las distintas plataformas, asegura 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 los cuales éstos se apoyan.

Definir los métodos de protección de información crítica.

Alcance

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

Responsabilidad

El Responsable de Seguridad Informática junto con el Propietario de la Información y la Unidad de Auditoría Interna, definirán los controles a ser implementados en los sistemas desarrollados o

adquiridos, 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.

Asimismo, el Responsable de Seguridad Informática será responsable de:
- Desarrollar 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 que debe cumplir 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 responsabilidades del personal involucrado en el proceso de entrada de datos.

El Responsable del Área Informática, asignará formalmente las 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 Comité de Seguridad de la Información designará los responsables de la administración de las técnicas criptográficas y claves.

El Responsable del Área de Administración será responsable de incorporar 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

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, sean estos propios, nuevos, mejoras a los existentes o paquetes comerciales.

Los requerimientos para nuevos sistemas o mejoras a los existentes especificarán las necesidades 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 de sistemas, 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 de los productos a utilizar.

b) Evaluar los requerimientos de seguridad y los controles requeridos, en términos que éstos deben ser proporcionales en costo y esfuerzo, al valor del bien que se quiere proteger y al daño potencial 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.

10.2. Seguridad en los Sistemas de Aplicación

Para evitar la pérdida, modificaciones o uso inadecuado de los datos en los sistemas de información, se establecerán controles y registros de auditoría, controlando:

a) La validación de datos de entrada.
b) La validación de datos de salida.
c) El procesamiento interno.

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.

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, quienes 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.

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 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. Procedimientos que establezcan los controles y verificaciones necesarios para prevenir la ejecución de programas fuera de secuencia o cuando falle el procesamiento previo.
b) Procedimientos que establezca la revisión periódica de los registros de auditoría de forma de detectar cualquier anomalía en la ejecución de las transacciones.
c) Procedimientos que realice la validación de los datos generados por el sistema.
d) Procedimientos que verifique la integridad de los datos o software cargados o descargados entre computadoras.
e) Procedimientos que controle la integridad de registros y archivos.
f) Procedimientos que verifique la ejecución de los aplicativos en el momento adecuado.
g) Procedimientos que asegure 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.

10.2.3. Autenticación de Mensajes

Cuando una aplicación tenga previsto el envío de mensaje que contengan información clasificada, se implementarán los controles criptográficos determinados en el punto – "10.3. 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) Verificaciones físicas de la información que brinda el sistema, que actúen como un control por oposición.
b) Control de conciliación de cuentas para asegurar el procesamiento de todos los datos, etc..

10.3. Controles Criptográficos

Se utilizarán sistemas y técnicas criptográficas para la protección de la información en base a un análisis de riesgo efectuado y para la cual otros controles no suministran una adecuada protección

de la confidencialidad e integridad.

10.3.1. Política de Utilización de Controles Criptográficos.

El Organismo determina la presente Política de uso de controles criptográficos, a fin de determinar el correcto uso de los mismos. Para ello se establece que:

a) Se utilizarán controles criptográficos en las siguientes ocasiones:
   1) Para la protección de claves de acceso a sistemas, datos y servicios.
   2) Para la transmisión de información clasificada, fuera del ámbito del Organismo.
   3) Para el resguardo de información, cuando así surja de la evaluación de riesgos correspondiente, que será realizada por el Propietario de la Información y el Responsable de Seguridad Informática.

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

c) El Comité de Seguridad de la Información asigna a las siguientes funciones:

Función	Cargo
Implementación de la Política de Controles Criptográficos	
Administración de Claves	

d) Se utilizarán los siguientes algoritmos de cifrado y tamaños de clave:

1) Cifrado Simétrico

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

2) Cifrado Asimétrico

Utilizar Para	Algoritmo	Longitud de Clave
Para certificados utilizados en servicios relacionados a la firma digital (certificación de hora digital, almacenamiento seguro de documentos electrónicos, etc.)	RSA	2048 bits

	DSA	2048 bits
	ECDSA	210 bits
Para certificados de Certificador o de información de estado de certificados	RSA	2048 bits
	DSA	2048 bits
	ECDSA	210 bits
Para certificados de usuario (personas físicas o jurídicas)	RSA	1024 bits
	DSA	1024 bits
	ECDSA	190 bits

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.

Al implementar la Política del Organismo en materia criptográfica, se considerarán los controles aplicables a la exportación e importación de tecnología criptográfica (Ver "12.1.6. Regulación de Controles para el Uso de Criptografía").

10.3.3. Firma Digital

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

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.

Los algoritmos de firma utilizados, como así también la longitud de clave a emplear, son las enumeradas en el punto – "10.3.1. Política de Utilización de Controles Criptográficos.", en el cuadro de cifrado asimétrico.

Se recomienda que las claves criptográficas utilizadas para realizar firmas digitales no sean empleadas en procedimientos de cifrado de información y sean resguardadas bajo el control exclusivo de su titular.

Al utilizar firmas digitales, se considerará la legislación pertinente (Ley 25.506, el Decreto Nº 2628/02 y el conjunto de normas complementarias que fijan o modifican competencias y establecen procedimientos) que describa las condiciones bajo las cuales una firma digital es legalmente vinculante. Por ejemplo, en el caso del comercio electrónico, es importante conocer la situación jurídica de las firmas digitales. (Ver "12.1.6. Regulación de Controles para el Uso de Criptografía")

Podría ser necesario establecer contratos de cumplimiento obligatorio u otros acuerdos para respaldar el uso de las mismas, cuando el marco legal sea inadecuado. Se deberá obtener asesoramiento legal con respecto a las leyes y normas que podrían aplicarse al uso de firmas digitales que pretende realizar el Organismo (Ver ". Cumplimiento").

10.3.4. Servicios de No Repudio

Estos servicios se utilizarán cuando sea necesario resolver disputas acerca de la ocurrencia o no de un evento o acción. Su objetivo es proporcionar herramientas para evitar que aquel que haya originado una transacción electrónica niegue haberlo hecho.

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 uso por parte del Organismo de los dos tipos de técnicas criptográficas, los cuales son:

a) Técnicas de clave secreta (criptografía simétrica), cuando dos o más actores comparten la misma clave y esta se utiliza tanto para cifrar información como para descifrarla.
b) Técnicas de clave publica (criptografía asimétrica), cuando cada usuario tiene un par de claves: una clave pública (que puede ser revelada a cualquier persona) utilizada para cifrar y una clave privada (que debe mantenerse en secreto) utilizada para descifrar.

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

Las técnicas criptográficas enumeradas en el punto – "10.3.1. Política de Utilización de Controles Criptográficos.", serán aplicadas con este propósito.

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

10.3.5.2. Normas, Procedimientos y Métodos

Se redactarán las normas y procedimientos necesarios para:

a) Generar claves para diferentes sistemas criptográficos y diferentes aplicaciones.
b) Generar y obtener certificados de clave publica de manera segura.

c) Distribuir claves a los usuarios que corresponda de forma segura, incluyendo cómo deben activarse las claves cuando se reciben.
d) Almacenar claves, incluyendo la forma de acceso a las mismas por parte de los usuarios autorizados.
e) Cambiar o actualizar claves, incluyendo reglas sobre cuándo y cómo deben cambiarse las claves.
f) Ocuparse de las claves comprometidas.
g) Revocar claves, incluyendo cómo deben retirarse o desactivarse las mismas, por ejemplo cuando las claves están comprometidas o cuando un usuario se desvincula del Organismo (en cuyo caso las claves también deben archivarse).
h) Recuperar claves perdidas o alteradas como parte de la administración de la continuidad de las actividades del Organismo, por ejemplo la recuperación de la información cifrada.
i) Archivar claves, por ejemplo, para la información archivada o resguardada.
j) Destruir claves.
k) Registrar (logging) y auditar las actividades relativas a la administración de claves.

A fin de reducir la probabilidad de compromiso, las claves tendrán fechas de entrada y caducidad de vigencia, definidas de manera que sólo puedan ser utilizadas por el lapso de 6 meses.

Además de la administración segura de las claves secretas y privadas, también deberá tenerse en cuenta la protección de las claves públicas. Este problema es abordado mediante el uso de un certificado de clave pública. Estos certificados se generarán de forma que vincule de manera única la información relativa al propietario del par de claves pública / privada con la clave pública.

En consecuencia es importante que el proceso de administración que genera estos certificados sea confiable. Normalmente, este proceso es llevado a cabo por una Autoridad de Certificación (AC), la cual deberá residir en una organización reconocida, con adecuados controles y procedimientos implementados, para ofrecer el nivel de confiabilidad requerido.

El contenido de los acuerdos de nivel de servicios o contratos con proveedores externos de servicios criptográficos, por ejemplo con una autoridad de certificación, deben comprender los tópicos de responsabilidad legal, confiabilidad del servicio y tiempos de respuesta para la prestación de los mismos.

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

Se definen los siguientes controles a realizar durante la implementación del software en producción, a fin de minimizar el riesgo de alteración de los sistemas.

- Toda aplicación, desarrollada internamente o adquirida a un proveedor 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, asignará formalmente la función de "implementador" al personal de su área que considere adecuado, quien tendrá como funciones y responsabilidades principales:

  a) Coordinar la implementación de modificaciones o nuevos programas en el ambiente de Producción.
  b) Asegurar que los sistemas aplicativos en uso, en el ambiente de Producción, son los autorizados y aprobados de acuerdo a las normas y procedimientos vigentes.
  c) Instalar las modificaciones, controlando previamente la recepción de la prueba aprobada por parte del Analista Responsable, del sector encargado del testeo y del usuario final.
  d) Rechazar la implementación en caso de encontrar defectos y/o si faltara la documentación estándar establecida.

Otros controles a realizar son:

a) Guardar sólo los ejecutables en el ambiente de producción.
b) Llevar un registro de auditoría de las actualizaciones realizadas.
c) Retener las versiones previas del sistema, como medida de contingencia.
d) Definir un procedimiento que establezca los pasos a seguir para implementar las autorizaciones y conformes pertinentes, las pruebas previas a realizarse, etc.
e) Denegar permisos de modificación al implementador sobre los programas fuentes bajo su custodia.
f) Evitar, que la función de implementador sea ejercida por alguna persona que pertenezca al sector de desarrollo o mantenimiento.

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 que contemplen lo siguiente:

a) Prohibir el uso de bases de datos operativas. En caso contrario se deben despersonalizar los datos antes de su uso. Aplicar idénticos procedimientos de control de acceso que en la base de producción.
b) Solicitar autorización formal para realizar una copia de la base operativa como base de prueba, llevando registro de tal actuación.
c) Registrar formalmente, tanto el uso como la copia de la información de bases de datos operativas.
d) Eliminar inmediatamente, una vez completadas las pruebas, la información operativa utilizada.

10.4.3. Control de Cambios a Datos Operativos

La modificación, actualización o eliminación de los datos operativos será realizado a través de los sistemas que procesan dichos datos y de acuerdo al esquema de control de accesos implementado en los mismos (Ver "9.2. Administración de Accesos de Usuarios"). Una modificación directa (por fuera de los sistemas) a un dato, almacenado ya sea en un archivo o base de datos, podría poner en riesgo la integridad de la información.

Los casos en los que no fuera posible la aplicación de la precedente política, se considerarán como excepciones. El Responsable de Seguridad Informática definirá procedimientos para la gestión de dichas excepciones que contemplarán lo siguiente:

a) Se generará una solicitud formal para la realización de la modificación, actualización o eliminación del dato.

b) El Propietario de la Información afectada y del Responsable de Seguridad Informática aprobarán la ejecución del cambio evaluando las razones por las cuales se solicita.

c) Se generarán cuentas de usuario de emergencia para ser utilizadas en la ejecución de excepciones. Las mismas serán protegidas mediante contraseñas, sujetas al procedimiento de administración de contraseñas críticas (Ver "9.2.4. Administración de Contraseñas Críticas")

d) Se designará a un responsable de implementar los cambios, el cual no será desarrollador. En el caso de que esta función no pueda ser segregada, se aplicarán controles adicionales de acuerdo a lo establecido en "8.1.4. Separación de Funciones".

e) Se registrarán todas las actividades realizadas con las cuentas de emergencia. Dicho registro será revisado posteriormente por el Responsable de Seguridad.

10.4.4. Control de Acceso a las Bibliotecas de Programas Fuentes

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

a) El Responsable del Área Informática, asignará formalmente la función de "administrador de programas fuentes" al personal de su área que considere adecuado, quien tendrá en custodia los programas fuentes y deberá:

- Proveer al Área de Desarrollo de los programas fuentes solicitados para su modificación, manteniendo en todo momento la correlación programa fuente / ejecutable.
- Llevar un registro actualizado de todos los programas fuentes en uso, indicando nombre del programa, programador, Analista Responsable que autorizó, versión, fecha de última modificación, y fecha / hora de compilación y estado (en modificación, en producción).
- Verificar que el Analista Responsable que autoriza la solicitud de un

programa fuente sea el designado para la aplicación, rechazando el pedido en caso contrario. Registrar cada solicitud aprobada.
- Administrar las distintas versiones de una aplicación.
- Asegurar que un mismo programa fuente no sea modificado simultáneamente por más de un desarrollador.

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

10.5. Seguridad de los Procesos de Desarrollo y Soporte

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

10.5.1. Procedimiento de Control de Cambios

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

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

a) Verificar que los cambios sean propuestos por usuarios autorizados.
b) Mantener un registro de los niveles de autorización acordados.
c) Solicitar la autorización del Propietario de la Información, en caso de tratarse de cambios a sistemas de procesamiento de la misma.
d) Identificar todos los elementos que requieren modificaciones (software, bases de datos, hardware).
e) Revisar los controles y los procedimientos de integridad para garantizar que no serán

comprometidos por los cambios.

f) Obtener aprobación formal por parte del Responsable del Área Informática para las propuestas detalladas antes que comiencen las tareas.
g) Solicitar la revisión del Responsable de Seguridad Informática para garantizar la no violación a los requerimientos de seguridad que debe cumplir el software.
h) Efectuar las actividades relativas al cambio en el ambiente de desarrollo.
i) Obtener la aprobación por parte del usuario autorizado y del área de testing mediante pruebas en el ambiente correspondiente.
j) Actualizar la documentación para cada cambio implementado, tanto de los manuales de usuario como de la documentación operativa.
k) Mantener un control de versiones para todas las actualizaciones de software.
l) Garantizar que la implementación se llevará a cabo minimizando la discontinuidad de las actividades y no alterando los procesos involucrados. Informar a las áreas usuarias antes de la implementación de un cambio que pueda afectar su operatoria.
m) Garantizar que sea el implementador quien efectúe el pasaje al ambiente operativo de los objetos modificados, de acuerdo a lo establecido en – "10.4.1. Control del Software Operativo".

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 funcionamiento o seguridad.

Para ello, se definirá un procedimiento que incluya:

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

10.5.3. Restricción del Cambio de Paquetes de Software

Se prohíbe la modificación de paquetes de software suministrados por proveedores.

En caso de considerarlo esencial, y previa autorización del Responsable del Área Informática, se tendrá en cuenta:

a) Obtener el consentimiento del proveedor en caso de ser necesario.
b) Procurar que sea el proveedor quien realice los cambios requeridos generando una actualización estándar de los programas.
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

Un canal oculto puede exponer información utilizando algunos medios indirectos y desconocidos. El código malicioso está diseñado para afectar a un sistema en forma no autorizada y no requerida por el usuario.

Para revisar este tópico, se redactarán normas y procedimientos que incluya:

a) Comprar 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) Efectuar tareas de monitoreo tendientes a identificar alteraciones al software que indiquen la presencia de código malicioso.
e) Utilizar herramientas preventivas para la protección de 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 de propiedad intelectual (Ver "12.1.2. Derechos de Propiedad Intelectual").
b) Requerimientos contractuales con respecto a la calidad del código.
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.

Anexo

Para cumplir con esta Política, en lo referente a los puntos "Seguridad de los Archivos del Sistema y "Seguridad de los Procesos de Desarrollo y Soporte", se sugiere implementar un modelo de separación de funciones entre los distintos ambientes involucrados.
Toda aplicación generada en el sector de desarrollo o adquirida a un proveedor es, en algún momento, implementada en un ambiente de producción. Los controles de esta transferencia deben ser rigurosos a fin de asegurar que no se instalan programas fraudulentos. Es conveniente implementar algún software para la administración de versiones y para la transmisión de programas entre los ambientes definidos, con un registro asociado para su control.
A continuación se presenta un modelo ideal formado por tres ambientes que debe ser adaptado a las características propias de cada Organismo, con las limitaciones de recursos y equipamiento correspondientes.

- **Ambiente de Desarrollo**

Es donde se desarrollan los programas fuentes. El analista o programador (desarrollador) tiene total dominio sobre el ambiente. Puede recibir algún fuente para modificar, quedando registrado en el sistema de control de versiones que administra el "administrador de programas fuentes".
El desarrollador realiza las pruebas con los datos de la base de desarrollo. Cuando considera que el programa está terminado lo pasa al ambiente de pruebas junto con la documentación requerida que le entregará al implementador de ese ambiente.

- **Ambiente de Pruebas**

El implementador de este ambiente recibe el programa y la documentación respectiva y realiza una prueba general con un lote al efecto, junto con el usuario de ser posible.
El testeador realiza las pruebas con los datos de la base de pruebas. Si no detectan errores de ejecución, los resultados de las rutinas de seguridad son correctas de acuerdo a las especificaciones y considera que la documentación presentada es completa, entonces remite el fuente al implementador de producción por medio del sistema de control de versiones y le entrega las instrucciones. Caso contrario, vuelve atrás el ciclo devolviendo el programa al desarrollador, junto con un detalle de las observaciones.

- **Ambiente de Producción**

Es donde se ejecutan los sistemas y se encuentran los datos productivos. Los programas fuentes certificados se guardan en un repositorio de fuentes de producción, almacenándolos mediante un sistema de control de versiones que maneja el "administrador de programas fuentes" y donde se dejan los datos del programador que hizo la modificación, fecha, hora y tamaño de los programas fuentes y objetos o ejecutables.
El "implementador" compila el programa fuente dentro del ambiente de producción en el momento de realizar el pasaje para asegurar de esta forma que hay una correspondencia biunívoca con el ejecutable en producción y luego se elimina, dejándolo en el repositorio productivo de programas fuentes.

Procedimientos de la misma naturaleza y alcance deberían aplicarse a las modificaciones de cualquier otro elemento que forme parte del sistema, por ejemplo: modelo de datos de la base o cambios en los parámetros, etc. Las modificaciones realizadas al software de base (Sistemas Operativos, Motores de bases de datos, Productos middleware) deberían cumplir idénticos

pasos, sólo que las implementaciones las realizarán los propios administradores.
Cabe aclarar que tanto el personal de desarrollo, como el proveedor de los aplicativos, no deben tener acceso al ambiente de producción, así como tampoco a los datos reales para la realización de las pruebas en el Ambiente de Prueba. Para casos excepcionales, se debe documentar adecuadamente la autorización, los trabajos realizados y monitorearlos en todo momento.

11. Administración de la Continuidad de las Actividades del Organismo

Generalidades

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

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

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

Objetivo

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

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

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

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

Asegurar la coordinación con el personal del Organismo y los contactos externos que participarán en las estrategias de planificación de contingencias. Asignar responsabilidades para cada actividad definida.

Alcance

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

Responsabilidad

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

Los propietarios de los procesos y recursos de información y el Responsable de Seguridad Informática serán responsables de:

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

Cada uno de los propietarios de los procesos y recursos de información, es el responsable de las revisiones periódicas de cada uno de los planes bajo su responsabilidad, como así también de la identificación de cambios en las disposiciones relativas a las actividades del Organismo 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:

- Definir los objetivos organizacionales de las herramientas de procesamiento de información.
- Garantizar que la administración de la continuidad de las actividades del Organismo esté incorporada a los procesos y estructura del mismo.
- Identificar y priorizar los procesos críticos de las actividades del Organismo.
- Asegurar que todos los integrantes del Organismo comprendan los riesgos que la misma enfrenta, en términos de probabilidad de ocurrencia e impacto de posibles amenazas, así como los efectos que una interrupción puede tener en la actividad del Organismo.
- Elaborar y documentar una estrategia de continuidad de las actividades del Organismo consecuente con los objetivos y prioridades acordados.
- Aprobar planes de continuidad de las actividades del Organismo de conformidad con la estrategia de continuidad acordada.
- Establecer un cronograma de pruebas periódicas de cada uno de los planes de contingencia, estableciendo responsables por las mismas.
- Coordinar actualizaciones periódicas de los planes y procesos implementados.
- Considerar la contratación de seguros que podrían formar parte del proceso de continuidad de las actividades del Organismo.
- Aprobar las modificaciones a los planes de contingencia.

Política

11.1. Proceso de la Administración de la Continuidad del Organismo

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

Este Comité tendrá a cargo las siguientes funciones, además de las definidas en el punto – "4.1.1. Comité de Seguridad de la Información":

a) Definir los objetivos organizacionales de las herramientas de procesamiento de información.
b) Garantizar que la administración de la continuidad de las actividades del Organismo esté incorporada a los procesos y estructura del mismo.
c) Identificar y priorizar los procesos críticos de las actividades del Organismo.
d) Asegurar que todos los integrantes del Organismo comprendan los riesgos que la misma enfrenta, en términos de probabilidad de ocurrencia e impacto de posibles amenazas, así como los efectos que una interrupción puede tener en la actividad del Organismo.
e) Elaborar y documentar una estrategia de continuidad de las actividades del Organismo consecuente con los objetivos y prioridades acordados.
f) Aprobar planes de continuidad de las actividades del Organismo de conformidad con la estrategia de continuidad acordada.
g) Coordinar pruebas y actualizaciones periódicas de los planes y procesos implementados.
h) Considerar la contratación de seguros que podrían formar parte del proceso de continuidad de las actividades del Organismo.

11.2. Continuidad de las Actividades y Análisis de los Impactos

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

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

Esta actividad será llevada a cabo con la 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 Organismo y no limitándose a las instalaciones de procesamiento de la información.

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

11.3. Elaboración e Implementación de los Planes de Continuidad de las Actividades del Organismo

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 Organismo. Estos procesos deberán ser aprobados 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 responsabilidades 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:
    1) Objetivo del plan.
    2) Mecanismos de coordinación y comunicación entre equipos (personal involucrado).
    3) Procedimientos de divulgación.
    4) Requisitos de la seguridad.
    5) Procesos específicos para el personal involucrado.
    6) Responsabilidades individuales.
g) Probar y actualizar los planes.

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

11.4. Marco para la Planificación de la Continuidad de las Actividades del Organismo

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

Cada plan de continuidad especificará claramente las condiciones para su puesta en marcha, así como las personas responsables 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 aprobadas por el Comité de Seguridad de la Información.

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

a) Prever las condiciones de implementación de los planes que describan el proceso a seguir (cómo evaluar la situación, qué personas estarán involucradas, etc.) antes de poner en marcha los mismos.
b) Definir los procedimientos de emergencia que describan las acciones a emprender una vez ocurrido un incidente que ponga en peligro las operaciones del Organismo y/o la vida humana. Esto debe incluir disposiciones con respecto a la gestión de las relaciones públicas y a vínculos eficaces a establecer con las autoridades públicas pertinentes, por ejemplo, la policía, bomberos y autoridades locales.
c) Realizar los procedimientos de emergencia que describan las acciones a emprender para el traslado de actividades esenciales del Organismo o de servicios de soporte a ubicaciones transitorias alternativas, y para el restablecimiento de los procesos de negocio en los plazos requeridos.
d) Redactar los procedimientos de recuperación que describan las acciones a emprender para restablecer las operaciones normales del Organismo.
e) Definir un cronograma de mantenimiento que especifique cómo y cuándo será probado el plan, y el proceso para el mantenimiento del mismo.
f) Efectuar actividades de concientización e instrucción al personal, diseñadas para propiciar la comprensión de los procesos de continuidad del negocio y garantizar que los procesos sigan siendo eficaces.
g) Documentar las responsabilidades 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.

Los administradores de los planes de contingencia son:

Plan de Contingencia	Administrador
.....	
.....	

El cumplimiento de los procedimientos implementados para llevar a cabo las acciones

contempladas en cada plan de continuidad, deben contarse entre las responsabilidades de los administradores de cada plan. Las disposiciones de emergencia para servicios técnicos alternativos, como instalaciones de comunicaciones o de procesamiento de información, normalmente se cuentan entre las responsabilidades de los proveedores de servicios.

11.5. Ensayo, Mantenimiento y Reevaluación de los Planes de Continuidad del Organismo.

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

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

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

a) Efectuar pruebas de discusión de diversos escenarios (discutiendo medidas para la recuperación del negocio utilizando ejemplos de interrupciones).
b) Realizar simulaciones (especialmente para entrenar al personal en el desempeño de sus roles de gestión posterior a incidentes o crisis).
c) Efectuar pruebas de recuperación técnica (garantizando que los sistemas de información puedan ser restablecidos con eficacia).
d) Realizar ensayos completos probando que el Organismo, el personal, el equipamiento, las instalaciones y los procesos pueden afrontar las interrupciones.

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

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

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

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

Plan de Contingencia	Revisar cada	Responsable de Revisión

Cada uno de los propietarios de los procesos y recursos de información, es el responsable de las revisiones periódicas de cada uno de los planes bajo su responsabilidad, como así también de la identificación de cambios en las disposiciones relativas a las actividades del Organismo aún no reflejadas en los planes de continuidad.

Todas las modificaciones efectuadas serán aprobadas por el Comité de Seguridad de la Información

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

Deberá prestarse atención, especialmente, a los cambios de:

a) Personal.
b) Direcciones o números telefónicos.
c) Estrategia del Organismo.
d) Ubicación, instalaciones y recursos.
e) Legislación.
f) Contratistas, proveedores y clientes críticos.
g) Procesos, o procesos nuevos / eliminados.
h) Tecnologías.
i) Requisitos operacionales.
j) Requisitos de seguridad.
k) Hardware, software y otros equipos (tipos, especificaciones, y cantidad).
l) Requerimientos de los sitios alternativos.
m) Registros de datos vitales.

12.Cumplimiento

Generalidades

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

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

Es necesario contar con el respaldo de los asesores jurídicos del Organismo, quienes se encargarán de informar las conductas que no se ajustan a derecho.

Objetivos

Cumplir con las disposiciones legales, normativas y contractuales a fin de evitar sanciones administrativas y legales al Organismo y/o al empleado.
Garantizar que los sistemas cumplan con la política, normas y procedimientos de seguridad del Organismo.

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.

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

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

Alcance

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

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

Responsabilidad

El Responsable de Seguridad Informática será responsable de:
- 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.
- Realizar revisiones periódicas de todas las áreas del Organismo a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad.
- Verificar periódicamente que los sistemas de información cumplan la política, normas y procedimientos de seguridad establecidos, pudiendo solicitar la participación de personal externo especializado.
- Coordinar las revisiones de Auditoría y garantizar la seguridad y el control de las herramientas utilizadas para las revisiones.

El Responsable del Área Legal del Organismo, con la asistencia del Responsable de Seguridad Informática serán responsables de:
- Definir y documentar claramente todos los requisitos legales, normativos y contractuales pertinentes para cada sistema de información.
- Redactar un Acuerdo de Confidencialidad a ser firmado por todo el personal.

El Comité de Seguridad de la Información proveerá de los medios necesarios para la resolución de cualquier irregularidad relacionada con la seguridad de la información, ocurrida en el ámbito del Organismo y la individualización de los responsables.

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

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

Políticas

12.1. Cumplimiento de Requisitos Legales

12.1.1. Identificación de la Legislación Aplicable

Se definirán y documentarán claramente todos los requisitos legales, normativos y contractuales pertinentes para cada sistema de información. Del mismo modo se definirán y documentarán los controles específicos y las responsabilidades 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.

Los empleados únicamente podrán utilizar material autorizado por la Universidad.

El Organismo solo podrá autorizar el uso de material producido por el mismo, o material autorizado o suministrado al mismo por quien lo haya desarrollado, conforme los términos y condiciones acordados y lo dispuesto por la normativa vigente.

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

Se deberán tener presentes las siguientes normas:

- *Ley de Propiedad Intelectual N° 11.723:* Protege los derechos de autor de las obras científicas, literarias y artísticas, incluyendo los programas de computación fuente y objeto; las compilaciones de datos o de otros materiales.
- *Ley de Marcas N° 22.362:* Protege la propiedad de una marca y la exclusividad de su uso.
- *Ley de Patentes de Invención y Modelos de Utilidad N° 24.481:* Protege el derecho del titular de la patente de invención a impedir que terceros utilicen su producto o procedimiento.

12.1.2.1. Derecho de Propiedad Intelectual del Software

El software es considerado una obra intelectual que goza de la protección de la Ley 11.723 de Propiedad Intelectual.

Esta ley establece que la explotación de la propiedad intelectual sobre los programas de computación incluirá, entre otras formas, los contratos de licencia para su uso o reproducción.

Los productos de software se suministran normalmente bajo acuerdos de licencia que suelen limitar el uso de los productos a máquinas específicas y su copia a la creación de copias de resguardo solamente.

El Responsable de Seguridad Informática 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 del Organismo

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

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

Tipo de Registro	Sistema de Información	Período de Retención	Medio de Almacenamiento	Responsable

Las claves criptográficas asociadas con archivos cifrados o firmas digitales se mantendrán en forma segura y estarán disponibles para su uso por parte de personas autorizadas cuando resulte necesario (Ver "10.3. Controles Criptográficos").

Se debe considerar la posibilidad de degradación de los medios utilizados para el almacenamiento de los registros. Los procedimientos de almacenamiento y manipulación se implementarán de acuerdo con las recomendaciones del fabricante.(Ver "10.3.1. Política de Utilización de Controles Criptográficos.")

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

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

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

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

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

En particular, se deberán tener presente las siguientes normas:

- *Ética en el Ejercicio de la Función Pública. Ley 25.188:* Establece que las personas que se desempeñen en la función pública deben proteger y conservar la propiedad del Estado y sólo emplear sus bienes con los fines autorizados.
- *Código de Ética de la Función Pública:* Dispone que el funcionario público debe proteger y conservar los bienes del Estado y utilizar los que le fueran asignados para el desempeño de sus funciones de manera racional, evitando su abuso, derroche o desaprovechamiento.
- *Código Penal Art. 255:* Sanciona a quien sustrajere, ocultare, destruyere o inutilizare objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario o de otra persona en el interés del servicio público. Si el culpable fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo.
- *Ley N° 24.624. Artículo 30:* Autoriza el archivo y la conservación en soporte electrónico u óptico indeleble de la documentación financiera, de personal y de control de la Administración Pública Nacional y otorga valor jurídico y probatorio a la documentación existente que se incorpore al Archivo General de la Administración, mediante la utilización de tecnología que garantice la estabilidad, perdurabilidad, inmutabilidad e

inalterabilidad del soporte de guarda físico de la mencionada documentación.

- *Decisión Administrativa 43/96:* Reglamenta el Art. 30 de la Ley 24.624. Determina su ámbito de aplicación, define conceptos y precisa los requisitos de carácter general, los relacionados con los documentos en particular y con el soporte a utilizar en la redacción, producción o reproducción de aquellos.

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.

El Organismo redactará un "Acuerdo de Confidencialidad", el cual deberá ser suscrito por todos los empleados. La copia firmada del acuerdo será retenida en forma segura por el Organismo.

Mediante este acuerdo se comprometerá al empleado a usar la información solamente para el uso específico al que se ha destinado y a no comunicar, diseminar o de alguna otra forma hacer pública la información a ninguna persona, firma, compañía o tercera persona, salvo autorización previa y escrita del Responsable del Activo de que se trate. El "Acuerdo de Confidencialidad" deberá advertir que determinadas actividades pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad del empleado (Ver ". Seguridad del Personal").

En particular, se deberán tener presente las siguientes normas:

- *Ley Marco de Regulación de Empleo Público Nacional. Ley 25.164*: Establece que los Funcionarios Públicos deben observar el deber de fidelidad que se derive de la índole de las tareas que le fueron asignadas y guardar la discreción correspondiente o la reserva absoluta, en su caso, de todo asunto del servicio que así lo requiera.
- *Convenio Colectivo de Trabajo General*: Dispone que todos los agentes deben observar el deber de fidelidad que se derive de la índole de las tareas que le fueran asignadas y guardar la discreción correspondiente, con respecto a todos los hechos e informaciones de los cuales tenga conocimiento en el ejercicio o con motivo del ejercicio de sus funciones.
- *Ética en el Ejercicio de la Función Pública. Ley 25.188:* Obliga a todas las personas que se desempeñen en la función pública a abstenerse de utilizar información adquirida en el cumplimiento de sus funciones para realizar actividades no relacionadas con sus tareas oficiales o de permitir su uso en beneficio de intereses privados.
- *Código de Ética de la Función Pública:* Establece que el funcionario público debe abstenerse de difundir toda información que hubiera sido calificada como reservada o secreta conforme a las disposiciones vigentes, ni la debe utilizar, en beneficio propio o de terceros o para fines ajenos al servicio, información de la que tenga conocimiento con motivo o en ocasión del ejercicio de sus funciones y que no esté destinada al público en general.
- *Protección de Datos Personales. Ley 25.326:* Establece responsabilidades para aquellas personas que recopilan, procesan y divulgan información personal y define criterios para procesar datos personales o cederlos a terceros.
- *Confidencialidad. Ley N° 24.766:* Impide la divulgación a terceros, o su utilización sin previo consentimiento y de manera contraria a los usos comerciales honestos, de

información secreta y con valor comercial que haya sido objeto de medidas razonables para mantenerla secreta.

- *Código Penal:* Sanciona a aquel que teniendo noticias de un secreto cuya divulgación pueda causar daño, lo revelare sin justa causa (Art. 156), al funcionario público que revelare hechos, actuaciones o documentos que por la ley deben quedar secretos (Art. 157), al que revelare secretos políticos o militares concernientes a la seguridad, a los medios de defensa o a las relaciones exteriores de la Nación, o al que por imprudencia o negligencia diere a conocer los secretos mencionados anteriormente, de los que se hallare en posesión en virtud de su empleo u oficio (Art. 222 y 223).

Asimismo, deberá considerarse lo establecido en el Decreto 1172/03, que regula el acceso a la información pública por parte de los ciudadanos.

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

Los recursos de procesamiento de información del Organismo se suministran con un propósito determinado. La utilización de estos recursos con propósitos no autorizados o ajenos al destino por el cual fueron provistos, sin la aprobación del Responsable de la Unidad Organizativa, debe ser considerada como uso indebido.

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

En particular, se debe respetar lo dispuesto por las siguientes normas:

- *Ley Marco de Regulación de Empleo Público Nacional. Ley 25.164*: Prohíbe hacer uso indebido o con fines particulares del patrimonio estatal.
- *Convenio Colectivo de Trabajo General*: Obliga a los agentes a no hacer uso indebido o con fines particulares del patrimonio estatal.
- *Ética en el Ejercicio de la Función Pública. Ley 25.188*: Obliga a las personas que se desempeñen en la función pública a proteger y conservar la propiedad del Estado y sólo emplear sus bienes con los fines autorizados.
- *Código de Ética de la Función Pública*: Obliga al funcionario público a proteger y conservar los bienes del Estado y utilizar los que le fueran asignados para el desempeño de sus funciones de manera racional, evitando su abuso, derroche o desaprovechamiento.

12.1.6. Regulación de Controles para el Uso de Criptografía

Al utilizar firmas digitales, se deberá considerar lo dispuesto por la Ley 25.506 y su decreto reglamentario Decreto 2628/02, que establecen las condiciones bajo las cuales una firma digital es legalmente válida.

Respecto a la comercialización de controles criptográficos, nuestro país ha suscrito el acuerdo Wassennar, que establece un listado de materiales y tecnologías de doble uso, cuya comercialización puede ser considerada peligrosa.

El Decreto 603/92 regula el Régimen de Control de las Exportaciones Sensitivas y de Material Bélico, estableciendo un tratamiento especial para la exportación de determinados bienes que pueden ser comprendidos dentro del concepto de material bélico.

Se debe obtener asesoramiento antes de transferir a otro país información cifrada o controles criptográficos. Para ello se puede consultar a la Dirección General de Política, de la Secretaria de Asuntos Militares, Ministerio de Defensa, a fin de saber si el material exportable requiere algún tratamiento especial.

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.

Cuando la acción implique la aplicación de una ley, tanto civil como penal, la evidencia presentada debe cumplir con lo establecido por las normas procesales. Para lograr la validez de la evidencia, el Organismo garantizará que sus sistemas de información cumplen con los estándares o códigos de práctica relativos a la producción de evidencia válida.

Para lograr la calidad y totalidad de la evidencia es necesaria una sólida pista de la misma. Esta pista se establecerá cumpliendo las siguientes condiciones:

a) Almacenar los documentos en papel originales en forma segura y mantener registros acerca de quién lo halló, dónde se halló, cuándo se halló y quién presenció el hallazgo. Cualquier investigación debe garantizar que los originales no sean alterados.
b) Copiar la información en medios informáticos removibles y la información en discos rígidos o en memoria, para garantizar su disponibilidad. Se mantendrá un registro de todas las acciones realizadas durante el proceso de copia. Se almacenará en forma segura una copia de los medios y del registro.

Cuando se detecta un incidente, puede no resultar obvio si éste derivará en una demanda legal.

El Comité de Seguridad de la Información proveerá de los medios necesarios para la resolución de cualquier irregularidad relacionada con la seguridad de la información, ocurrida en el ámbito del Organismo y la individualización de los responsables.

Se deberá tener presente lo dispuesto por el Reglamento de Investigaciones Administrativas, procedimiento administrativo especial, de naturaleza correctiva interna que constituye garantía suficiente para la protección de los derechos y correcto ejercicio de las responsabilidades impuestas a los agentes públicos. Este Decreto debe ser complementado por lo dispuesto en la Ley N° 19.549 (Ley de Procedimiento Administrativo) y por toda otra normativa aplicable, incluido el Código Penal, el que sanciona a quien sustrajere, ocultare, destruyere o inutilizare objetos destinados a servir de prueba ante la autoridad competente (Art. 255).

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

12.2.1. Cumplimiento de la Política de Seguridad

Cada Responsable de Unidades Organizativas, garantizará 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 del Organismo a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad. Entre las áreas a revisar se incluyen las siguientes:

a) Sistemas de información.
b) Proveedores de sistemas.
c) Propietarios de información y de recursos de información.
d) Usuarios.
e) Gerentes.

Los propietarios de los sistemas de 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. En caso de ser necesario, estas revisiones contemplarán la asistencia técnica especializada.

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

La verificación del cumplimiento comprenderá pruebas de penetración, las cuales podrán contar con la asistencia de especialistas independientes contratados a ese efecto. Esta verificación tendrá como objetivo la detección de vulnerabilidades en el sistema y la verificación de la eficacia de los controles con relación a la prevención de accesos no autorizados. Se tomarán los recaudos necesarios en el caso de pruebas de penetración exitosas que comprometan la seguridad del sistema.

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

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.

Se contemplarán los siguientes puntos:

a) Acordar con el Área que corresponda los requerimientos de auditoría.

b) Controlar el alcance de las verificaciones. Esta función será realizada por el responsable de auditoría.

c) Limitar las verificaciones a un acceso de sólo lectura del software y datos de producción. Caso contrario, se tomarán los resguardos necesarios a efectos de aislar y contrarrestar los efectos de las modificaciones realizadas, una vez finalizada la auditoría. Por ejemplo:

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

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

Recursos de TI a utilizar en la Verificación	
Sistemas de información	.....
Base de datos	.....
Hardware	.....
Software de Auditoría	.....
Medios Magnéticos	.....
Personal de Auditoría	.....
Interlocutores de las Áreas de Informática	.....
Interlocutores de las Áreas Usuarias	.....
Conexiones a Red	.....
.....	.....

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

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

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

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

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 Sindicatura General de la Nación.

12.4. Sanciones Previstas por Incumplimiento

Se sancionará administrativamente a todo aquel que viole lo dispuesto en la presente Política de Seguridad conforme a lo dispuesto por las normas 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.

Índice