

## **PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE CORALINA.**

---

## ESTRUCTURA DEL DOCUMENTO “PLAN DE TRATAMIENTO DE RIESGOS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE CORALINA”

### Índice

1. INTRODUCCIÓN.....	2
1.1. Alcance.....	2
2. TÉRMINOS Y DEFINICIONES.....	2
2.1. Seguridad de la Información.....	3
2.2. Evaluación de Riesgos .....	3
2.3. Administración de Riesgos.....	3
2.4. Comité de Seguridad de la Información .....	3
2.5. Responsable de Seguridad Informática.....	4
2.6. Incidente de Seguridad.....	4
3. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.....	4
3.1. Aspectos Generales.....	6
3.2. Sanciones Previstas por Incumplimiento.....	7
4. ORGANIZACIÓN DE LA SEGURIDAD .....	7
4.1. Infraestructura de la Seguridad de la Información.....	8
4.1.1. Comité de Seguridad de la Información .....	8
4.1.2. Asignación de Responsabilidades en Materia de Seguridad de la Información ...	9
4.2. Seguridad Frente al Acceso por Parte de Terceros .....	10
4.2.1. Identificación de Riesgos del Acceso de Terceras Partes .....	10
4.2.2. Requerimientos de Seguridad en Contratos o Acuerdos con Terceros.....	11
4.3. Tercerización .....	11
4.3.1. Requerimientos de Seguridad en Contratos de Tercerización .....	11
5. CLASIFICACIÓN Y CONTROL DE ACTIVOS.....	12
5.1. Inventario de activos.....	13
<b>7. SEGURIDAD FÍSICA Y AMBIENTAL.....</b>	<b>13</b>
7.6. Ubicación y Protección del Equipamiento y Copias de Seguridad .....	13
7.7. Suministros de Energía .....	14
7.8. Seguridad del Cableado .....	15
7.9. Mantenimiento de Equipos.....	15
7.11. Desafectación o Reutilización Segura de los Equipos. ....	16
<b>8. GESTIÓN DE COMUNICACIONES Y OPERACIONES .....</b>	<b>16</b>
8.3. Protección Contra Software Malicioso .....	16
8.3.1. Controles Contra Software Malicioso .....	16
8.4. Mantenimiento .....	16
8.4.1. Resguardo de la Información .....	16
8.4.2. Registro de Actividades del Personal Operativo.....	17
8.4.3. Registro de Fallas.....	18
8.5. Administración de la Red .....	18
8.5.1. Controles de Redes.....	18
8.6. Administración y Seguridad de los Medios de Almacenamiento .....	18
8.6.1. Administración de Medios Informáticos Removibles.....	18
8.6.2. Eliminación de Medios de Información.....	19
8.7.3. Seguridad del Gobierno Electrónico.....	19
8.7.4. Seguridad del Correo Electrónico.....	20
8.7.4.1. Riesgos de Seguridad.....	20
8.7.4.2. Política de Correo Electrónico.....	20

8.7.5. Seguridad de los Sistemas Electrónicos de Oficina.....	21
<b>9. CONTROL DE ACCESOS .....</b>	<b>22</b>
9.2.2. Administración de Privilegios.....	22
9.2.3. Administración de Contraseñas de Usuario .....	22
9.2.4. Administración de Contraseñas Críticas .....	23
9.3. Responsabilidades del Usuario.....	23
9.3.1. Uso de Contraseñas.....	23
9.4.6. Subdivisión de Redes.....	24
9.4.7. Acceso a Internet.....	24
9.4.8. Control de Conexión a la Red .....	25
9.4.10. Seguridad de los Servicios de Red .....	25
9.5.3. Identificación y Autenticación de los Usuarios .....	25
9.5.4. Sistema de Administración de Contraseñas .....	26
9.8. Computación Móvil y Trabajo Remoto.....	26
9.8.1. Computación Móvil .....	26

## 1. Introducción

### 1.1. Alcance

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

Debe ser conocida y cumplida por toda la planta de personal de la Corporación, tanto se trate de funcionarios como contratistas, y sea cual fuere su nivel jerárquico y cargo asignado.

## 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 de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- **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 sujeta la Corporación.
- **Confiable 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 Corporación o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la Corporación, 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 y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria de la Corporación.

## 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 la 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 Corporación, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

## 2.5. Responsable de Seguridad Informática

Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes del Organismo 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 Corporación 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 del Organismo.

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 funcionarias de la Corporación y de los Sub Directores de cada área para la difusión, consolidación y cumplimiento de la presente Política.

### Objetivo

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

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 Corporación actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

### Alcance

Esta Política se aplica en todo el ámbito de la Corporación, 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 Directores Generales, Sub Directores o equivalentes, jefes de Departamentos En la Corporación, 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 Corporación, el área a la cual se encuentre afectado y cualquiera sea el nivel de las tareas que desempeñe.

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

El Comité de Seguridad de la Información del Organismo, procederá a revisar y proponer a la máxima autoridad del Organismo para su aprobación la Política de Seguridad de la Información y las funciones generales en materia de seguridad de la información; monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las Política de Seguridad de la Información

amenazas más importantes; tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad; aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área, 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 Corporación y coordinar el proceso de administración de la continuidad de las actividades del Organismo.

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

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

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

El Responsable del Área de Recursos Humanos o quién desempeñe esas funciones, cumplirá la función 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 Compromisos de Confidencialidad (entre otros) y las tareas de capacitación continúa en materia de seguridad.

El Responsable del Área Informática cumplirá la función de cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología del Organismo. Por otra parte, tendrá la función de efectuar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada, 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.

### 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 Corporación 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 Corporación.
- Seguridad Física y Ambiental.  
Destinado a impedir accesos no autorizados, daños e interferencia a las sedes e información de la Corporación.
- 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 de la Corporación  
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 los requisitos de seguridad.

A fin de asegurar la implementación de las medidas de seguridad comprendidas en esta Política, la Corporación identificará los recursos necesarios e indicará formalmente las partidas presupuestarias correspondientes, como anexo a la presente Política.

El Comité de Seguridad de la Información revisará (indicar periodicidad no mayor a un año) 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.

## **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 Corporación.

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

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

Por otro lado, debe tenerse en cuenta que ciertas actividades de la Corporación 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 Corporación y establecer un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades.

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



## Alcance

Esta Política se aplica a todos los recursos de la Corporación 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 Comité de Seguridad de la Información tendrá a cargo el mantenimiento y la presentación para la aprobación de la presente Política, ante la Dirección General de la Corporación, el seguimiento de acuerdo a las incumbencias propias de cada área de las actividades relativas a la seguridad de la información (análisis de riesgos, monitoreo de incidentes, supervisión de la investigación, implementación de controles, administración de la continuidad, impulsión de procesos de concientización, etc.) y la proposición de asignación de funciones.

El Responsable de Seguridad Informática asistirá al personal de la Corporación en materia de seguridad de la información.

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

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

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 Corporación.

## 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 Corporación compartida por todas las Autoridades políticas y Directores Nacionales o Generales, Gerentes o equivalentes, por lo cual se crea el Comité de Seguridad de la Información, integrado por representantes de todos los

Directores mencionados, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad. El mismo contará con un Coordinador, quien cumplirá la función de impulsar la implementación de la presente Política.

## Conformación del Comité de Seguridad de la Información

Área / Dirección Representante

Este Comité tendrá entre sus funciones:

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

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

La Dirección General, asigna las funciones relativas a la Seguridad Informática de la Corporación al Ing. de sistemas, en adelante el “Responsable de Seguridad Informática”, quien tendrá a cargo las funciones relativas a la seguridad de los sistemas de información de la Corporación, lo cual incluye la supervisión de todos los aspectos inherentes a seguridad informática 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:

proceso	Responsable
Seguridad en las Comunicaciones y las Operaciones	
Control de Acceso a recursos informaticos e información.	
Seguridad en el Desarrollo y Mantenimiento de Sistemas	

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.

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

El uso de recursos personales de procesamiento de información en el lugar de trabajo puede ocasionar nuevas vulnerabilidades. En consecuencia, su uso será evaluado en cada caso por el Responsable de Seguridad Informática y deberá ser autorizado por el Responsable del Área Informática y por la sub dirección de planeación.

## 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 Corporación, el Responsable de Seguridad Informática y el Propietario de la Información de que se trate, llevarán a cabo y documentarán una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta, entre otros aspectos:

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

En todos los contratos cuyo objeto sea la prestación de servicios a título personal bajo cualquier modalidad jurídica que deban desarrollarse dentro de la Corporación, 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.
- c) Pasantías y otras designaciones de corto plazo.
- d) Consultores.

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

### 4.2.2. Requerimientos de Seguridad en Contratos o Acuerdos con Terceros

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

- a) Cumplimiento de la Política de seguridad de la información de la Corporación.
- b) ~~Protección de los activos del Organismo, incluyendo:~~ \_\_\_\_\_

- Procedimientos para proteger los bienes del Organismo, abarcando los activos físicos, la información y el software. Organización de la Seguridad
- Procedimientos para determinar si ha ocurrido algún evento que comprometa los bienes, por ejemplo, debido a pérdida o modificación de datos.
- Controles para garantizar la recuperación o destrucción de la información y los activos al finalizar el contrato o acuerdo, o en un momento convenido durante la vigencia del mismo.
- Restricciones a la copia y divulgación de información.
- c) Descripción de los servicios disponibles.
- 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 PC de la corporación, contemplarán además de los puntos especificados en (“Requerimientos de Seguridad en Contratos o Acuerdos con Terceros”, los siguientes aspectos:

- a) Forma en que se cumplirán los requisitos legales aplicables.
- b) Medios para garantizar que todas las partes involucradas en la tercerización,

incluyendo los subcontratistas, están al corriente de sus responsabilidades en materia de seguridad.

- c) Forma en que se mantendrá y comprobará la integridad y confidencialidad de los activos del Organismo.
- d) Controles físicos y lógicos que se utilizarán para restringir y delimitar el acceso a la información sensible del Organismo.
- 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 tercer izado.
- g) Derecho a la auditoría por parte del Organismo sobre los aspectos tercer izados 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. Clasificación y Control de Activos

## 5. Clasificación y Control de Activos

### Generalidades

El Organismo 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, etc.).

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

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

Por último, la información puede pasar a ser obsoleta y por lo tanto, ser necesario eliminarla. La destrucción de la información es un proceso que debe asegurar la confidencialidad de la misma hasta el momento de su eliminación.

## Objetivo

Garantizar que los activos de información reciban un apropiado nivel de protección.  
Clasificar la información para señalar su sensibilidad y criticidad.  
Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

## Alcance

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

## Responsabilidad

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

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

Cada Propietario de la Información supervisará que el proceso de clasificación y rótulo de información de su área de competencia sea cumplimentado de acuerdo a lo establecido en la presente Política.

### 5.1. Inventario de activos

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

## 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.

### 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

Incendio

Explosivos

Humo

Inundaciones o filtraciones de agua (o falta de suministro)

Polvo

Vibraciones

Efectos químicos

Interferencia en el suministro de energía eléctrica  
(cortes de suministro, variación de tensión)

Radiación electromagnética

Derrumbes

- e) Revisar regularmente las condiciones ambientales para verificar que las mismas no afecten de manera adversa el funcionamiento de las instalaciones de procesamiento de la información. Esta revisión se realizará cada: 6 meses
- f) Considerar asimismo el impacto de las amenazas citadas en el punto d) que tengan lugar en zonas próximas a la sede de la Corporación.

### 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 cada equipo. Para asegurar la continuidad del suministro de energía, se contemplarán las siguientes medidas de control:

- a) Disponer de múltiples enchufes o líneas de suministro para evitar un único punto de falla en el suministro de energía.
- b) Contar con un suministro de energía 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 con incumbencia. Los planes de contingencia contemplarán las acciones que han de emprenderse ante una falla de la UPS. Los equipos de UPS serán inspeccionados y probados periódicamente para asegurar que funcionan correctamente y que tienen la autonomía requerida.

c) Montar un generador de respaldo para los casos en que el procesamiento deba continuar ante una falla prolongada en el suministro de energía. Deberá realizarse un análisis de impacto de las posibles consecuencias ante una interrupción prolongada del procesamiento, con el objeto de definir 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 descargas eléctricas en todos los edificios y líneas de comunicaciones externas de acuerdo a las normativas vigentes.

## 7.8. Seguridad del Cableado

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

- a) Cumplir con los requisitos técnicos vigentes.
- b) Utilizar piso ducto 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 interceptación no autorizada.
- 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.
  - a) Instalar conductos blindados y recintos o cajas con cerradura en los puntos terminales y de inspección.
  - b) Utilizar rutas o medios de transmisión alternativos.

## 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 equipamiento de la sede del Organismo para su mantenimiento.
- e) Eliminar la información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.

### **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.

## **8. Gestión de Comunicaciones y Operaciones**

### **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 la Corporación
- 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, como medida precautoria y rutinaria.
- d) Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles (probar dichas actualizaciones en un entorno de prueba previamente si es que constituyen cambios críticos a los sistemas).
- e) Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos de la Corporación, 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 del Área Informática y de Seguridad Informática 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 crítico del Organismo. Los sistemas de resguardo deberán probarse periódicamente, asegurándose que cumplen con los requerimientos de los planes de continuidad de las actividades de la Corporación,

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, y asegurando la destrucción de los medios desechados.
- c) Almacenar en una ubicación remota copias recientes de información de resguardo junto con registros exactos y completos de las mismas y los procedimientos documentados de restauración, a una distancia suficiente como para evitar daños provenientes de un desastre en el sitio principal. Se deberán retener al menos tres generaciones o ciclos de información de resguardo para la información y el software Gestión de Comunicaciones y Operaciones.  
esenciales para la Corporación. 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.
- 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.

#### **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 propuesto 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,
- 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 implementará dichos controles.

## 8.6. Administración y Seguridad de los Medios de Almacenamiento

### 8.6.1. Administración de Medios Informáticos Removibles

El Responsable del Área Informática, con la asistencia del Responsable de Seguridad Informática, implementará procedimientos para la administración de medios informáticos removibles, como cintas, discos, casetes e informes impresos. 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 la Corporación el Organismo. (Ver 7.11. Desafectación o Reutilización Segura de los Equipos.).
- 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.

### 8.6.2. Eliminación de Medios de Información

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

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, toner y cartuchos 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. Gestión de Comunicaciones y Operaciones
- k) Documentación del sistema.

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

### 8.7.3. Seguridad del Gobierno Electrónico

El Responsable de Seguridad Informática verificará que los procedimientos de aprobación de Software del punto “**Aprobación del Sistema**” incluyan los siguientes aspectos para las Aplicaciones de Gobierno Electrónico:

- a) Autenticación: Nivel de confianza recíproca suficiente sobre la identidad del usuario y la Corporación.
- b) Autorización: Niveles de Autorización adecuados para establecer disposiciones, emitir

o firmar documentos clave, etc.. Forma de comunicarlo al otro participante de la transacción electrónica.

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

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 interceptación 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.
- f) Las consideraciones legales, como la necesidad potencial de contar con prueba de origen, envío, entrega y aceptación.
- g) Las implicancias de la publicación externa de listados de personal, accesibles al público.
- h) El acceso de usuarios remotos a las cuentas de correo electrónico.
- i) El uso inadecuado por parte del personal.

##### **8.7.4.2. Política de Correo Electrónico**

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

- a) Protección contra ataques al correo electrónico, por ejemplo virus, interceptación, etc.

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

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

Entender al correo electrónico como una herramienta más de trabajo provista al empleado a fin de ser utilizada conforme el uso al cual está destinada, faculta al empleador a implementar sistemas de controles destinados a velar por la protección y el buen uso de sus recursos. Esta facultad, sin embargo, deberá ejercerse salvaguardando la dignidad del trabajador y su derecho a la intimidad. Por tal motivo, el Organismo debe informar claramente a sus empleados: a) cuál es el uso que el organismo espera que los empleados hagan del correo electrónico provisto por el organismo; y b) bajo qué condiciones los mensajes pueden ser objeto de control y monitoreo.

### **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 las actividades que desarrollan determinadas personas, por ejemplo, aquellas que trabaja en proyectos sensibles.
- e) La aptitud del sistema para dar soporte a las aplicaciones del Organismo, como la comunicación de órdenes o autorizaciones.
- f) Categorías de personal y contratistas o terceros a los que se permite el uso del sistema

y las ubicaciones desde las cuales se puede acceder al mismo.

- g) Restricción de acceso a determinadas instalaciones a específicas categorías de usuarios.
- h) Identificación de la posición o categoría de los usuarios, por ejemplo, empleados del Organismo o contratistas, en directorios accesibles por otros usuarios.
- i) Retención y resguardo de la información almacenada en el sistema.
- j) Requerimientos y disposiciones relativos a sistemas de soporte de reposición de información previa.

## 9. Control de Accesos

### 9.2.2. Administración de Privilegios

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

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

### 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. Esta declaración bien puede estar incluida en el Compromiso de Confidencialidad
- b) Garantizar que los usuarios cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al sistema. Las contraseñas provisorias, que se asignan cuando los usuarios olvidan su contraseña, sólo debe suministrarse una vez identificado el usuario.
- c) Generar contraseñas provisorias seguras para otorgar a los usuarios. Se debe evitar la

participación de terceros o el uso de mensajes de correo electrónico sin protección (texto claro) en el mecanismo de entrega de la contraseña y los usuarios deben dar acuse de recibo cuando la reciban.

- d) Almacenar las contraseñas sólo en sistemas informáticos protegidos.
- e) Utilizar otras tecnologías de autenticación y autorización de usuarios, como ser la biométrica (por ejemplo, verificación de huellas dactilares), verificación de firma, uso de autenticadores de hardware (como las tarjetas de circuito integrado), etc.. El uso de esa herramienta se dispondrá cuando la evaluación de riesgos realizada por el Responsable de Seguridad Informática conjuntamente con el Responsable del Área de Informática y el Propietario de la Información lo determine necesario (o lo justifique).
- f) Configurar los sistemas de tal manera que:
  - las contraseñas tengan al menos 6 caracteres,
  - suspendan o bloqueen permanentemente al usuario luego de su retiro de la Corporación.
  - solicitar el cambio de la contraseña cada 45
  - impedir que las últimas 3 contraseñas sean reutilizadas,

#### 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 Control de Accesos

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.
- 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.

### 9.3. Responsabilidades del Usuario

#### 9.3.1. Uso de Contraseñas



Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas.

Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.

Los usuarios deben cumplir las 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. Control de Accesos
  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 provisionales en el primer inicio de sesión (“log on”).
- f) Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.
- g) Notificar de acuerdo a lo establecido en 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.

#### 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 y para bloquear el acceso no autorizado.

La subdivisión en dominios de la red tomará en cuenta criterios como los requerimientos de seguridad común 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.

el Responsable del Área Informática evaluará el costo relativo y el impacto en el desempeño que ocasione la implementación de enrutadores o gateways adecuados 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 formalmente por el Responsable de la Sub Dirección de Planeación. 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. 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**

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

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.

#### **9.4.10. 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.
- Instalar periódicamente las actualizaciones de seguridad.

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

#### **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 específica. 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 “Uso de Contraseñas”.
- d) Imponer cambios en las contraseñas en aquellos casos en que los usuarios mantengan sus propias contraseñas, según lo señalado en el punto “Uso de Contraseñas”.
- e) Obligar a los usuarios a cambiar las contraseñas provisionales en su primer procedimiento de identificación, en los casos en que ellos seleccionen sus contraseñas.
- f) Mantener un registro de las últimas contraseñas utilizadas por el usuario, y evitar la reutilización de las mismas.
- g) Evitar mostrar las contraseñas en pantalla, cuando son ingresadas.
- h) Almacenar en forma separada los archivos de contraseñas y los datos de sistemas de aplicación.
- i) Almacenar las contraseñas en forma cifrada utilizando un algoritmo de cifrado unidireccional.
- j) Modificar todas las contraseñas predeterminadas por el vendedor, una vez instalado el software y el hardware (por ejemplo, claves de impresoras, hubs, routers, etc.).
- k) Garantizar que el medio utilizado para acceder/utilizar el sistema de contraseñas, asegure que no se tenga acceso a información temporal o en tránsito de forma no protegida.

### **9.8. 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 de la Corporación.

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, ya que deberán incluirse todos los dispositivos que pudieran contener información confidencial de la Corporación 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 Control de Accesos 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, salvo los estrictamente necesarios.
- 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 pudieran haber comprometidos recursos.