Ministerio de Economía

Política de Seguridad de la Información

VERSIÓN 1.2

Ministerio de Economía	POLÍTICA	Versión: 1.2 Vigencia: 23-02-21	SI-POL-01
Política de Seguridad de la Información		Confeccionó: DGTIyC Revisó/Conformó: CSI Aprobó: Ministro de Economía	

Tabla de contenidos

SOBRE EL DOCUMENTO 6

GESTIÓN DE VERSIONES 6

1.CLÁUSULA: INTRODUCCIÓN 7

1.1 Alcance de la Política de Seguridad de la Información (PSI) 7

2.CLÁUSULA:TÉRMINOS Y DEFINICIONES 7

2.1 Seguridad de la Información 7
2.2 Evaluación de Riesgos 8
2.3 Tratamiento de Riesgos. 8
2.4 Gestión de Riesgos 8
2.5 Comité de Seguridad de la Información (CSI) 8
2.6 Responsable de Seguridad de la Información (RSI) 8
2.7 Responsable de Área Informática 9
2.8 Incidente de Seguridad 9
2.9 Riesgo 9
2.10 Amenaza 9
2.11Vulnerabilidad 9
2.12 Control 9

3. CLÁUSULA: ESTRUCTURA DE LA POLÍTICA 9

4. CLÁUSULA: EVALUACIÓN Y TRATAMIENTO DE RIESGOS 9

4.1 Evaluación de los Riesgos de Seguridad 10
4.2 Tratamiento de los Riesgos de Seguridad 10

5. CLÁUSULA: POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN (PSI) 11

5.1 Objetivo 11
5.2 Política de Seguridad de la información(PSI) 13

6. CLÁUSULA: ORGANIZACIÓN 14

Generalidades 15
Objetivo 15
Alcance 15
Responsabilidad 15
6.1 Categoría: Organización interna 16
6.2 Categoría: Dispositivos móviles y trabajo remoto 18
7. CLÁUSULA: RECURSOS HUMANOS 21
Generalidades 21
Objetivo 21
Alcance 21
Responsabilidad 21
7.1 Categoría: Antes del empleo 22
7.2 Categoría: Durante el empleo 23
7.3 Categoría: Cese del empleo o cambio de puesto de trabajo 24

8. CLÁUSULA: GESTIÓN DE ACTIVOS 25

Generalidades 25
Objetivo 26
Alcance 26
RESPONSABILIDAD 26
8.1 Categoría: Responsabilidad sobre los activos 26
8.2 Categoría: Clasificación de la información 28
8.3 Categoría: Gestión de medios 29

9. CLÁUSULA: GESTIÓN DE ACCESOS 31

Generalidades 31
Objetivo 32
Alcance 32
Responsabilidad 32
9.1 CATEGORÍA: REQUERIMIENTOS PARA LA GESTIÓN DE ACCESO 34
Objetivo 34
9.2 CATEGORÍA: ADMINISTRACIÓN DE GESTIÓN DE USUARIAS/OS 34
Objetivo 34
9.3 CATEGORÍA: RESPONSABILIDADES DE LA/EL USUARIA/O 37
Objetivo 37
9.4 CATEGORÍA: CONTROL DE ACCESO A SISTEMAS Y APLICACIONES 38
Objetivo 38
9.5 CATEGORÍA: CONTROL DE ACCESO AL SISTEMA OPERATIVO 42
Objetivo 42

10. CLÁUSULA: CRIPTOGRAFÍA 44

Generalidades 44
Objetivos 44
Alcance 44
Responsabilidad 44
10.1 CATEGORÍA: CUMPLIMIENTO DE REQUISITOS LEGALES 45
Objetivo 45

11. CLÁUSULA: FÍSICA Y AMBIENTAL 47

Generalidades 47
Objetivo 47
Alcance 47
Responsabilidad 48
11.1 CATEGORÍA: ÁREAS SEGURAS 48
Objetivo 48
11.2 CATEGORÍA: SEGURIDAD DE LOS EQUIPOS 51
Objetivo 51

12. CLÁUSULA: SEGURIDAD EN LAS OPERACIONES 56

Generalidades 56
Objetivo 56
Responsabilidad 56
12.1 CATEGORÍA: PROCEDIMIENTOS Y RESPONSABILIDADES OPERATIVAS 57

Objetivo *57*
12.2 CATEGORÍA: PROTECCIÓN CONTRA EL MALWARE (CÓDIGO MALICIOSO) 58
Objetivo *58*
12.3 CATEGORÍA: RESGUARDO (BACKUP) 59
Objetivo *59*
12.4 CATEGORÍA: REGISTRO Y MONITOREO 60
Objetivo *60*
12.5 CATEGORÍA: CONTROL DE SOFTWARE OPERACIONAL 61
Objetivo *61*
12.6 CATEGORÍA: ADMINISTRACIÓN DE VULNERABILIDADES TÉCNICAS 62
Objetivo *62*
12.7 CATEGORÍA: CONSIDERACIONES SOBRE LA AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN 63
Objetivo *63*

13. CLÁUSULA: GESTIÓN DE COMUNICACIONES 63

Generalidades 63
Objetivo 63
Alcance 64
Responsabilidad 64
13.1 CATEGORÍA: GESTIÓN DE LA RED 64
Objetivo *64*
13.2 CATEGORÍA: TRANSFERENCIA DE INFORMACIÓN 65
Objetivo *65*

14. CLÁUSULA: ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS 66

Generalidades 66
Objetivo 67
Alcance 67
Responsabilidad 67
14.1 CATEGORÍA: REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS 67
Objetivo *67*
14.2 CATEGORÍA: SEGURIDAD EN LOS SISTEMAS DE APLICACIÓN 69
Objetivo *69*
14.3 CATEGORÍA: SEGURIDAD DE LOS ARCHIVOS DEL SISTEMA 70
Objetivo *70*
14.4 CATEGORÍA: SEGURIDAD DE LOS PROCESOS DE DESARROLLO Y SOPORTE 72
Objetivo *72*
14.5 CATEGORÍA: GESTIÓN DE VULNERABILIDADES TÉCNICAS 74
Objetivo *74*
Información Complementaria *74*
Ambiente de Desarrollo *75*
Ambiente de Pruebas *75*
Ambiente de Producción *75*

15. CLÁUSULA: RELACIONES CON PROVEEDORES 75

Generalidades 75
Objetivo 76
Alcance 76

Responsabilidad 76
15.1 Categoría: Seguridad de la información en las relaciones con la/el proveedora/or 76
Objetivo *76*
15.2 Categoría: Administración de prestación de servicios de proveedoras/es 78
Objetivo *78*

16. CLÁUSULA: GESTIÓN DE INCIDENTES DE SEGURIDAD 79

Generalidades 79
Objetivo 79
Alcance 79
Responsabilidad 79
16.1 Categoría: Informe de los eventos y debilidades de la seguridad de la información 80
Objetivo *80*
16.2 Categoría: Gestión de los Incidentes y mejoras de la seguridad de la información 80
Objetivo *80*

17. CLÁUSULA: GESTIÓN DE LA CONTINUIDAD 82

Generalidades 82
Objetivo 82
Responsabilidad 82
17.1 Categoría: Gestión de continuidad del Ministerio 83
Objetivo *83*
Actividades del Ministerio *84*
17.2 Categoría: Redundancias 86
Objetivo *86*

18. CLÁUSULA: CUMPLIMIENTO 86

Generalidades 86
Objetivos 87
Alcance 87
Responsabilidad 87
18.1 Categoría: Cumplimiento de Requisitos Legales 87
Objetivo *87*
Derecho de Propiedad intelectual del Software *88*
18.2 Categoría: Revisiones de la Política de Seguridad y la Compatibilidad Técnica 92
Objetivo *92*
18.3 Categoría: Consideraciones de Auditorías de Sistemas 93
Objetivo *93*

Sobre el Documento

Documento	Código	Versión
Política de Seguridad de la Información	SI-POL-01	1.2

Elaboró: DGTIyC	Revisó/Conformó: CSI	Aprobó: Ministro de Economía
Fecha: 15-08-2018	**Fecha:** 23-02-2021	**Fecha:**

Gestión de Versiones

Aspectos que cambiaron en el documento	Detalles de los cambios efectuados	Responsable de la solicitud del cambio	Fecha del Cambio	Versión
Adopción del Documento.	Redacción.	Director/a General	15-08-2018	1
Ajuste del Documento.	Cambios para mejorar la comprensión del texto.	Director/a General	10-04-2019	1.1
Modificaciones y adecuaciones al funcionamiento y particularidades del Ministerio. Ajustes de lenguaje inclusivo.	Actualizaciones, correcciones y ajustes.	Director/a General	23-02-2021	1.2

1. Cláusula: Introducción

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

En ese sentido, la Seguridad de la Información protege a la información de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información y de la operación del Ministerio, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos del Organismo.

Es importante que los principios de la Política de Seguridad de la Información (PSI) sean parte de la cultura organizacional. Para esto, se debe asegurar un compromiso manifiesto de las máximas autoridades del Ministerio y de los/las titulares de Unidades Organizativas para la difusión, consolidación y cumplimiento de esta política.

1.1 Alcance de la Política de Seguridad de la Información (PSI)

La PSI 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 del Ministerio.

Debe ser conocida y cumplida por toda la planta de personal del Ministerio, tanto se trate de funcionarias/os políticas/os como técnicas/os, administrativas/os y operativas/os, y sea cual fuere su nivel jerárquico y su situación de revista.

2. Términos y Definiciones

2.1 Seguridad de la Información

La Seguridad de la Información se entiende como la preservación de las siguientes características:

- **Confidencialidad**: Garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a ésta.
- **Integridad**: Salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- **Disponibilidad**: Garantiza que las/los usuarias/os autorizadas/os tengan acceso a la información y a los recursos relacionados con ésta, toda vez que lo requieran.

Adicionalmente, deben considerarse los conceptos de:

- **Autenticidad**: Validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el/la emisor/a para evitar suplantación de identidades.
- **Auditabilidad**: Todos los eventos de un sistema deben poder ser registrados para su control posterior.
- **Protección a la duplicación**: Asegura que una transacción sólo se realiza una (1) 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**: Refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
- **Legalidad**: Cumplimiento del ordenamiento jurídico (leyes, reglamentaciones, procedimientos, etc.) al que está sujeto el Ministerio, y en particular, aquel que hace a la seguridad.
- **Confiabilidad de la Información**: La información generada debe ser adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

2.1.1 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, clasificación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.
- **Tecnología de la Información**: Se refiere al hardware y software operados por el Ministerio, o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Ministerio, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.
- **Propietaria/o de la Información**: Define a la persona responsable de la integridad, confidencialidad y disponibilidad de una cierta información.

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 su procesamiento, la probabilidad de que ocurran y su potencial impacto en la operatoria del Ministerio.

2.3 Tratamiento de Riesgos

Proceso de selección e implementación de medidas para modificar el riesgo.

2.4 Gestión de Riesgos

Actividades coordinadas para dirigir y controlar una organización en lo que concierne al riesgo.

NOTA. La Gestión de Riesgos usualmente incluye la evaluación de riesgos, el tratamiento de riesgos, la aceptación de riesgos y la comunicación de riesgos.

2.5 Comité de Seguridad de la Información (CSI)

El CSI es un cuerpo integrado por representantes de todas las áreas sustantivas del Ministerio, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

2.6 Responsable de Seguridad de la Información (RSI)

Es quien cumple la función de supervisar, planificar, desarrollar, controlar y gestionar las políticas, procedimientos y acciones de cumplimiento de la PSI y de asesorar en materia de Seguridad de la Información a los integrantes del Ministerio que así lo requieran.

2.7 Responsable del Área Informática

Es el/la titular de la Dirección General de Tecnologías de la Información y las Comunicaciones (DGTIyC) dependiente de la Subsecretaría de Administración y Normalización Patrimonial de la Secretaría Legal y Administrativa del Ministerio de Economía, quien tiene las funciones y responsabilidades asignadas por la normativa vigente.

En lo que respecta a los Sistemas de Administración Financiera, sus accesos, desarrollo, mantenimiento y administración, la responsabilidad es de la Dirección General de Sistemas Informáticos de Administración Financiera

(DGSIAF) dependiente de la Subsecretaría de Presupuesto de la Secretaría de Hacienda del citado Ministerio, conforme las funciones y responsabilidades asignadas por la normativa vigente.

En aquellas materias que sean de carácter compartido entre la DGTIyC y la DGSIAF, las decisiones serán adoptadas por consenso entre las dos (2) áreas informáticas, en el ámbito de sus respectivas competencias.

2.8 Incidente de Seguridad

Un Incidente de Seguridad es un evento adverso en un sistema de información, ya sean computadoras, red de computadoras u otros medios que contengan información, que puede comprometer o compromete la confidencialidad, integridad y/o disponibilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

2.9 Riesgo

Combinación de la probabilidad de ocurrencia de un evento y sus consecuencias o impacto.

2.10 Amenaza

Una causa potencial de un incidente no deseado, el cual puede ocasionar daños a un sistema u organización.

2.11 Vulnerabilidad

Una debilidad de un activo o grupo de activos que puede ser aprovechada por una amenaza.

2.12 Control

Medio para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras organizacionales, las cuales pueden ser de naturaleza administrativa, técnica, de gestión, o legal.

NOTA. Control es también utilizado como sinónimo de salvaguarda o de contramedida.

3. Cláusula: Estructura de la política

Esta Política se divide en dos (2) partes, y guarda la siguiente estructura:

- Cuatro (4) cláusulas introductorias, con los términos generales y el establecimiento de la evaluación y el tratamiento de los riesgos;
- Catorce (14) cláusulas que abarcan los diferentes aspectos o dominios de la Seguridad de la Información. Se presentan de manera sistemática y consistente.

Cada cláusula contiene un número de categorías o grupo de controles de seguridad principales.

4. Cláusula: Evaluación y tratamiento de Riesgos

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

Es por ello que resulta imprescindible gestionar los riesgos del Ministerio, como pilar fundamental para la gestión de seguridad.

Objetivo

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

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

Alcance

La PSI se aplica a toda la información administrada en el Ministerio, cualquiera sea el soporte en que se encuentre.

Responsabilidad

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

El RSI junto con los Titulares de Unidades Organizativas son responsables del desarrollo del proceso de gestión de riesgos de seguridad de la información.

4.1 Evaluación de los Riesgos de Seguridad

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

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

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

4.2 Tratamiento de los Riesgos de Seguridad

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

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

a) Mitigar los riesgos mediante la aplicación de controles apropiados para reducir los riesgos;
b) Aceptar los riesgos de manera objetiva y consciente, siempre y cuando éstos satisfagan claramente la política y los criterios de aceptación de riesgos del Ministerio;
c) Evitar los riesgos, eliminando las acciones que dan origen a la ocurrencia de éstos;
d) Transferir los riesgos asociados a otras partes interesadas, por ejemplo: compañías de seguro o proveedoras/es.

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

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

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

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

5. Cláusula: Política de Seguridad de la Información (PSI)

5.1 Objetivo

Proteger los recursos de información del Ministerio 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 la PSI, identificando los recursos y las partidas presupuestarias correspondientes, sin que ello implique necesariamente la asignación de partidas adicionales.

Mantener la PSI del Ministerio actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

Alcance

Esta política se aplica en todo el ámbito del Ministerio, y a la totalidad de los procesos, ya sean internos o externos vinculados al Ministerio a través de contratos o acuerdos con terceros.

Responsabilidad

Todos/as los/las Directores/as Nacionales o Generales o equivalentes, titulares de Unidades Organizativas, tanto se trate de autoridades políticas o personal técnico y sea cual fuere su nivel jerárquico son responsables de la implementación de esta PSI dentro de sus áreas de responsabilidad, así como del cumplimiento de dicha PSI por parte de su equipo de trabajo.

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

La/El Ministra/o de Economía aprueba la PSI y es responsable de la autorización de sus modificaciones.

El CSI del Ministerio de Economía:

- Revisa y propone la PSI y las funciones generales en materia de seguridad de la información a la máxima autoridad del Ministerio para su aprobación;
- Monitorea cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes;

- Toma conocimiento y supervisa la investigación y monitoreo de los incidentes relativos a la seguridad;

- Aprueba las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área (se refiere a dar curso a las propuestas relativas a la seguridad de la información del Ministerio presentadas por parte de las áreas de acuerdo a sus competencias, elevándolas a la máxima autoridad del Ministerio para su aprobación), así como acuerda y aprueba metodologías y procesos específicos relativos a seguridad de la información;

- Garantiza que la seguridad sea parte del proceso de planificación de la información; evalúa y coordina la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios;

- Promueve la difusión y apoyo a la seguridad de la información dentro del Ministerio y coordina el proceso de administración de la continuidad de las actividades del Organismo.

- Coordina el proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de la información del Ministerio frente a interrupciones imprevistas.

La/El Coordinadora/or del CSI es la/el responsable de:

- Coordinarlas acciones del CSI;

- Impulsar la implementación y cumplimiento de la PSI.

El RSI:

- Cumple funciones relativas a la seguridad de los sistemas de información del Ministerio, lo cual incluye la supervisión de todos los aspectos inherentes a los temas tratados en la PSI.

Las/Los Propietarias/os de la información y Propietarias/os de activos son responsables de:

- Clasificar la información de acuerdo con el grado de sensibilidad y criticidad;

- Documentar y mantener actualizada la clasificación efectuada;

- Definir qué usuarias/os deben tener permisos de acceso a la información de acuerdo a sus funciones y competencia.

La/ El Responsable del Área de Recursos Humanos o quien desempeñe esas funciones, cumplirá la función de:

- Notificar a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la PSI y de todas las normas, procedimientos y prácticas que de ella surjan;

- Asimismo, tiene a su cargo la notificación de la PSI 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 continua en materia de seguridad.

La/El Responsable del Área Informática cumple la función de cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología del Ministerio. Por otra parte, tiene 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.

La/El Responsable del Área Legal o Jurídica verifica el cumplimiento de la PSI en la gestión de los contratos, acuerdos u otra documentación del Ministerio con las/los empleadas/os y, en caso de existir, con los terceros. Asimismo, asesora en materia legal al Ministerio, en lo que se refiere a la seguridad de la información.

La Unidad de Auditoría Interna (UAI), o en su defecto quien sea propuesto por el CSI 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 la PSI y por las normas, procedimientos y prácticas que de ella surjan (Ver Cláusula 18: Cumplimiento).

5.2 Política de Seguridad de la información (PSI)

Objetivo

Proporcionar a las autoridades la dirección y soporte para la seguridad de la información en concordancia con los requerimientos, normas y regulaciones relevantes. El CSI debe establecer claramente la dirección de la política en línea con los objetivos.

5.2.1 Control: Documento de la PSI

El documento de la PSI es conformado por el CSI, aprobado por la/el Ministra/o, publicado y comunicado a las/los empleadas/os y las partes externas relevantes.

Esta PSI se conforma por 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 del Ministerio y establecer un marco gerencial para controlar su implementación.

Gestión de Activos

Destinado a mantener una adecuada protección de los activos del Ministerio.

Recursos Humanos

Orientado a reducir los riesgos de error humano, comisión de ilícitos contra el Ministerio o uso inadecuado de instalaciones.

Física y Ambiental

Destinado a impedir accesos no autorizados, daños e interferencia a las sedes e información del Ministerio.

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.

Gestión de Accesos

Orientado a controlar el acceso lógico a la información.

Adquisición. Desarrollo y Mantenimiento de los Sistemas

Orientado a garantizar la incorporación de medidas de seguridad en los sistemas de información desde su especificación, adquisición, desarrollo y/o implementación y durante su mantenimiento.

Gestión de Incidentes de seguridad

Orientado a administrar todos los eventos que atenten contra la confidencialidad, integridad y disponibilidad de la información y los activos tecnológicos.

Gestión de Continuidad

Orientado a contrarrestar las interrupciones de las actividades y proteger los procesos críticos de los efectos de fallas significativas o desastres.

Cumplimiento

Destinado a impedir infracciones y violaciones de las leyes del Derecho Civil y Penal; de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos; y de los requisitos de seguridad.

A fin de asegurar la implementación de las medidas de seguridad comprendidas en la PSI, el Ministerio identifica los recursos necesarios e indica formalmente las partidas presupuestarias correspondientes. Lo expresado anteriormente no implica necesariamente la asignación de partidas presupuestarias adicionales.

La PSI aprobada se comunicará mediante la/el Responsable del Área de Recursos Humanos.

5.2.2 Control: Revisión de la PSI

El responsable de las actividades de desarrollo, evaluación y revisión de la PSI será el CSI.

La actividad de revisión debe incluir las oportunidades de mejoras, en respuesta a los cambios, entre otros, organizacionales, normativos, legales, de terceros, tecnológicos.

Las mejoras tenidas en cuenta deben quedar registradas y tener las aprobaciones de las/los responsables.

El CSI debe revisarla a intervalos planeados y prever el tratamiento de caso de los cambios no planeados, a efectos de mantener actualizada la política.

Asimismo, debe efectuar 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.

6. Organización

Generalidades

La presente PSI establece la administración de la seguridad de la información como parte fundamental de los objetivos y actividades del Ministerio. Por ello se define formalmente un ámbito de gestión para efectuar tareas tales como la aprobación de la PSI, la coordinación de su implementación y la asignación de funciones y responsabilidades.

Asimismo, se contempla 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 Ministerio 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 considera 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 deben establecer las medidas adecuadas para la protección de la información.

Objetivo

- Administrar la seguridad de la información dentro del Ministerio 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 del Ministerio.

Alcance

- Esta PSI se aplica a todos los recursos del Ministerio 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/La Coordinador/a del CSI es el/la responsable de impulsar la implementación de la PSI.

El CSI tiene a cargo el mantenimiento y la presentación para la aprobación de la PSI ante la máxima autoridad del Ministerio, 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.

La/El RSI asiste al personal del Ministerio en materia de seguridad de la información y coordina la interacción con Organismos especializados. Asimismo, junto con las/los propietarias/os de la información, analiza el riesgo de los accesos de terceros a la información del Ministerio y verifica la aplicación de las medidas de seguridad necesarias para su protección.

Las/Los Responsables de las Unidades Organizativas autorizan la incorporación de nuevos recursos de procesamiento de información a las áreas de su incumbencia.

La UAI o en su defecto quien sea propuesto por el CSI es responsable de realizar revisiones independientes sobre la vigencia y el cumplimiento de la PSI.

La/El Responsable del Área de Administración, con la colaboración de la/el Responsable del Área Jurídica, incluye en los contratos con proveedoras/es de servicios de tecnología y cualquier otra/o proveedora/or de bienes o servicios cuya actividad afecte directa o indirectamente a los activos de información, la obligatoriedad del cumplimiento de la PSI y de

todas las normas, procedimientos y prácticas relacionadas. Asimismo, notifica a las/los proveedoras/es sobre las modificaciones que se efectúen a la PSI del Ministerio.

6.1 Categoría: Organización interna

Objetivo

Manejar la seguridad de la información dentro del Ministerio.

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

El/La Ministro/a aprueba la PSI y asigna los roles de seguridad. El CSI coordina y revisa la implementación de la seguridad en todo el Ministerio.

6.1.1 Control: Compromiso de la dirección con la seguridad de la información

La dirección apoya la seguridad de la información a través de una dirección clara, mostrando compromiso, asignando roles y reconociendo responsabilidades explícitas.

Formular, revisa y aprueba la PSI, y corrobora los beneficios de su implementación.

La seguridad de la información es una responsabilidad del Ministerio compartida por todas las Autoridades políticas y Directoras/es Nacionales o Generales o equivalentes. Para ello se crea el CSI, integrado por representantes de todas las áreas mencionadas, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad de la información. Éste cuenta con un/a Coordinador/a, con la misión de impulsar la implementación de la PSI.

6.1.2 Control: Coordinación de la seguridad de la información

La coordinación de la seguridad de la información involucra la cooperación y colaboración de Directoras/es Nacionales o Generales o equivalentes, usuarias/os, administradoras/es, diseñadoras/es de aplicación, auditoras/es y personal de seguridad, y capacidades especializadas en áreas como seguros, temas legales, recursos humanos, tecnologías de información (TI) o gestión del riesgo.

Esta actividad debe:

a) Asegurar que las actividades de seguridad sean ejecutadas en conformidad con la PSI;

b) Identificar cómo manejar las no conformidades;

c) Aprobar las metodologías y procesos para la seguridad de la información; por ejemplo, la evaluación del riesgo y la clasificación de la información;

d) Identificar cambios significativos en las amenazas y la exposición de la información y los medios de procesamiento de la información ante amenazas;

e) Evaluar la idoneidad y coordinar la implementación de los controles de la seguridad de información;

f) Promover de manera efectiva la educación, capacitación y conocimiento de la seguridad de la información a través de toda la organización;

g) Evaluar la información recibida del monitoreo y revisar los incidentes de seguridad de la información, y recomendar las acciones apropiadas en respuesta a los incidentes de seguridad de información identificados;

h) Mantener contacto con los organismos nacionales encargados de la seguridad de la información e integrar una red nacional de seguimiento de incidentes de seguridad de la información.

6.1.3 Control: Asignación de responsabilidades de la seguridad de la información

La asignación de responsabilidades de la seguridad de la información debe ejecutarse en forma alineada a la PSI.

La máxima autoridad del Ministerio asigna las funciones relativas a la seguridad informática del Ministerio a quien sea designado, en adelante el "RSI", quien tendrá a cargo las funciones relativas a la seguridad de los sistemas de información del Ministerio, lo cual incluye la supervisión de todos los aspectos inherentes a seguridad informática tratados en la presente PSI.

El CSI propone a la autoridad que corresponda para su aprobación la definición y asignación de las responsabilidades que surgen de la presente PSI.

Oportunamente se detallarán los procesos de seguridad, en un documento posterior, indicándose en cada caso las/los responsables del cumplimiento de los aspectos de esta PSI aplicables a cada caso.

De igual forma, oportunamente se detallarán las/los propietarias/os de la información, quienes son las/los Responsables de las Unidades Organizativas a cargo del manejo de la referida información.

Cabe aclarar que, si bien las/los propietarias/os pueden delegar la administración de sus funciones a personal idóneo a su cargo, conservan la responsabilidad de su cumplimiento.

La delegación de la administración por parte de las/los propietarias/os de la información debe ser documentada por éstos y proporcionada al RSI.

6.1.4 Control: Autorización para instalaciones de procesamiento de información

Los nuevos recursos de procesamiento de información deben estar autorizados por las/los Responsables de las Unidades Organizativas involucradas, considerando su propósito y uso, conjuntamente con la/el RSI, a fin de garantizar que se cumpla toda la PSI y los requerimientos de seguridad pertinentes.

Las siguientes guías deben ser consideradas para el proceso de autorización:

a) Cumplir con los niveles de aprobación vigentes en la organización, incluso la/el responsable del ambiente de seguridad de la información, asegurando el cumplimiento de las políticas y requerimientos;

b) Cuando corresponda, se verificará el hardware y software para garantizar su compatibilidad con los componentes de otros sistemas del Ministerio;

c) El uso de recursos personales de procesamiento de información en el lugar de trabajo puede ocasionar nuevas vulnerabilidades. En consecuencia, su uso debe ser evaluado en cada caso por la/el RSI y debe ser autorizado por la/el Responsable del Área Informática y por el/la Director/a Nacional (o equivalente) responsable del área al que se destinen los recursos.

6.1.5 Control: Acuerdos de confidencialidad

Se deben definir, implementar y revisar regularmente los acuerdos de confidencialidad o de no divulgación para la protección de la información del Ministerio. Dichos acuerdos deben responder a los requerimientos de confidencialidad o no divulgación del Ministerio, los cuales deben ser revisados periódicamente. Asimismo, deben cumplir con toda legislación o normativa que alcance al Ministerio en materia de confidencialidad de la información.

Dichos acuerdos deben celebrarse tanto con el personal del Ministerio como con aquellos terceros que se relacionen de alguna manera con su información, inclusive si la información no se encuentra en un sistema computarizado.

6.1.6 Control: Contacto con otros organismos

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

Oficina Nacional de Tecnologías de Información (ONTI) dependiente de la Subsecretaría de Tecnologías de la Información y las Comunicaciones de la Secretaría de Innovación Pública de la Jefatura de Gabinete de Ministros:

Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC). Es una unidad de respuesta ante incidentes en redes y sistemas, que centraliza y coordina los esfuerzos ante los incidentes de seguridad que afecten a los recursos informáticos del Sector Público.

Dirección Nacional de Protección de Datos Personales de la Agencia de Acceso a la Información Pública, organismo descentralizado en el ámbito de la Jefatura de Gabinete de Ministros. En los intercambios de información de seguridad no se debe divulgar información sensible (de acuerdo a lo definido en la normativa vigente, por ejemplo, ley 25.326) o confidencial perteneciente al Ministerio 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 de la información cuyo personal está obligado a mantener la confidencialidad de los temas que trata.

6.1.7 Control: Contacto con grupos de interés especial

La/El RSI es la/el encargada/o de coordinar los conocimientos y las experiencias disponibles en el Ministerio a fin de brindar ayuda en la toma de decisiones en materia de seguridad. Ésta/e debe obtener asesoramiento de otros Organismos.

Con el objeto de optimizar su gestión, se habilita al RSI el contacto con las Unidades Organizativas de todas las áreas del Ministerio.

Debe considerar ser miembro de grupos de interés especial para:

a) Adquirir nuevos conocimientos acerca de las mejores prácticas y estar actualizado;

b) Asegurar que la concientización acerca de la seguridad de la información esté actualizada y completa;

c) Recibir alertas tempranas, avisos y recomendaciones ante ataques y vulnerabilidades;

d) Proporcionar vínculos adecuados durante el tratamiento de los incidentes de seguridad de la información.

6.1.8 Control: Revisión independiente de la seguridad de la información

La UAI o en su defecto quien sea propuesto por el CSI debe realizar revisiones independientes sobre la vigencia, implementación y gestión de la PSI, a efectos de garantizar que las prácticas del Ministerio reflejan adecuadamente sus disposiciones.

Estas revisiones deben incluir las oportunidades de evaluación de mejoras y las necesidades de cambios de enfoque en la seguridad, incluyendo políticas y objetivos de control.

Se deben registrar y reportar todas estas actividades.

6.2 Categoría: Dispositivos móviles y trabajo remoto

Objetivo

Asegurar la seguridad de la información cuando se utiliza medios de computación y teletrabajo móviles y/o remotos.

La protección requerida se debe conmensurar con los riesgos que causan estas maneras de trabajo específicas. Cuando se utiliza computación móvil, se deben considerar los riesgos de trabajar en un ambiente desprotegido y se debe aplicar una protección apropiada. En el caso del teletrabajo, la organización debe aplicar protección al lugar del teletrabajo y asegurar que se establezcan los arreglos adecuados para esta manera de trabajar.

6.2.1 Control: Dispositivos móviles

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

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

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

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

a) La protección física necesaria;

b) El acceso seguro a los dispositivos;

c) La utilización segura de los dispositivos en lugares públicos;

d) El acceso a los sistemas de información y servicios del Ministerio a través de dichos dispositivos;

e) Las técnicas criptográficas a utilizar para la transmisión de información clasificada;

f) Los mecanismos de resguardo de la información contenida en los dispositivos;

g) La protección contra software malicioso.

La utilización de dispositivos móviles incrementa la probabilidad de ocurrencia de incidentes del tipo de pérdida, robo o hurto. En consecuencia, debe entrenarse especialmente al personal que los utilice. Se deben desarrollar normas y procedimientos sobre los cuidados especiales a observar durante el uso de dispositivos móviles, que contemplen 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 Ministerio 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 deben confeccionar procedimientos que permitan a la/el usuaria/o del dispositivo reportar rápidamente cualquier incidente sufrido y mitigar los riesgos a los que eventualmente estuvieran expuestos los sistemas de información del Ministerio, los que incluyen:

a) Revocación de las credenciales afectadas;

b) Notificación a grupos de trabajo donde potencialmente se pudieran haber comprometido recursos.

6.2.2 Control: Trabajo remoto

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

El trabajo remoto puede ser autorizado por la/el Responsable de la Unidad Organizativa, o superior jerárquico correspondiente, a la cual pertenezca la/el usuaria/o solicitante, conjuntamente con la/el RSI, 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.

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 Ministerio, la sensibilidad de la información a la que se accede y que pasa a través del vínculo 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 autorizado por el Ministerio en los dispositivos utilizados para el teletrabajo.

Los controles y disposiciones comprenden:

a) 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 Ministerio y los sistemas internos y servicio a los cuales el trabajador remoto está autorizado a acceder;

b) Proveer de un adecuado equipo de comunicación, con inclusión de métodos para asegurar el acceso remoto;

c) Incluir seguridad física;

d) Definir reglas y orientación respecto del acceso de terceros al equipamiento e información;

e) Proveer el hardware y el soporte y mantenimiento del software;

f) Definir los procedimientos de "backup" y de continuidad de las operaciones;

g) Efectuar auditoría y monitoreo de la seguridad;

h) Realizar la anulación de las autorizaciones, derechos de acceso y devolución del equipo cuando finalicen las actividades remotas;

i) Asegurar el reintegro del equipamiento en las mismas condiciones en que fue entregado, en el caso en que cese la necesidad de trabajar en forma remota.

Se deben implementar procesos de auditoría específicos para los casos de accesos remotos, sujetos a revisaciones regulares. Se debe llevar un registro de incidentes a fin de corregir eventuales fallas en la seguridad de este tipo de accesos.

7. Cláusula: Recursos Humanos

Generalidades

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

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

La implementación de la PSI tiene como meta minimizar la probabilidad de ocurrencia de incidentes. Es por ello que resulta necesario implementar un mecanismo que permita reportar las debilidades y los incidentes tan pronto como sea posible, a fin de subsanarlos y evitar eventuales replicaciones. Por lo tanto, es importante analizar las causas del incidente producido y aprender de éste, 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 e incluirlas en los acuerdos de confidencialidad a firmarse y verificar su cumplimiento durante el desempeño de la persona como agente.

Garantizar que las/los usuarias/os estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para respaldar la PSI en el transcurso de sus tareas normales.

Establecer Compromisos de Confidencialidad con todo el personal y usuarias/os 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 PSI se aplica a todo el personal del Ministerio, cualquiera sea su situación de revista, y al personal externo que efectúe tareas dentro del ámbito del Ministerio.

Responsabilidad

La/El Responsable del Área de Recursos Humanos debe incluir las funciones relativas a la seguridad de la información en las descripciones de puestos de las/los empleadas/os, informar a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la PSI, gestionar los Compromisos de Confidencialidad con el personal y coordinar las tareas de capacitación de usuarias/os respecto de la presente PSI.

La/El Responsable del Área Jurídica participa en la confección del Compromiso de Confidencialidad a firmar por las/los empleadas/os y terceras/os que desarrollen funciones en el Ministerio, en el asesoramiento sobre las sanciones a ser aplicadas por incumplimiento de la presente PSI y en el tratamiento de incidentes de seguridad que requieran de su intervención.

7.1 Categoría: Antes del empleo

Objetivo

Asegurar que las/los empleadas/os, contratistas y terceras/os entiendan sus responsabilidades y sean idóneos para los roles para los cuales son considerados y reducir el riesgo de robo, fraude y mal uso de los recursos.

Las responsabilidades de seguridad deben ser comunicadas previa efectivización de la relación de empleo, en las definiciones de trabajo y condiciones del empleo.

7.1.1 Control: Funciones y responsabilidades

Las funciones y responsabilidades en materia de seguridad deben incorporarse en la descripción de las responsabilidades de los puestos de trabajo.

Éstas incluyen las responsabilidades generales relacionadas con la implementación y el mantenimiento de la PSI, y las responsabilidades específicas vinculadas a la protección de cada uno de los activos o la ejecución de procesos o actividades de seguridad determinadas.

Se deben definir y comunicar claramente los roles y responsabilidades de seguridad a los/las candidatos/as para el puesto de trabajo durante el proceso de preselección.

7.1.2 Control: Investigación de antecedentes

Se deben llevar a cabo controles de verificación del personal en el momento en que se solicita el puesto. Estos controles incluyen todos los aspectos que indiquen las normas que a tal efecto alcanzan al Ministerio.

Los chequeos de verificación deben incluir:

a) Disponibilidad de referencias de carácter satisfactorias;

b) Chequeo del currículum vitae del postulante;

c) Confirmación de títulos académicos y profesionales mencionados por el postulante;

d) Acreditación de su identidad.

7.1.3 Control: Términos y condiciones de contratación

Como parte de sus términos y condiciones iniciales de empleo, las/los empleadas/os, cualquiera sea su situación de revista, deben firmar un Compromiso de Confidencialidad o no divulgación en lo que respecta al tratamiento de la información del Ministerio. La copia firmada del Compromiso debe ser retenida en forma segura por el Área de Recursos Humanos u otra competente.

Asimismo, mediante el Compromiso de Confidencialidad las/los empleadas/os declaran conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo.

Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad de la/el empleada/o.

Se debe desarrollar un procedimiento para la suscripción del Compromiso de Confidencialidad donde se incluyan aspectos sobre:

- Suscripción inicial del Compromiso por parte de la totalidad del personal. Revisión anual del contenido del Compromiso.
- Método de re-suscripción en caso de modificación del texto del Compromiso.
- Los términos y condiciones de empleo establecerán la responsabilidad de la/el empleada/o en materia de seguridad de la información.

- Cuando corresponda, los términos y condiciones de empleo establecen que estas responsabilidades se extienden más allá de los límites de la sede del Ministerio y del horario normal de trabajo.
- Los derechos y obligaciones de la/el empleada/o relativos a la seguridad de la información, por ejemplo, en relación con las leyes de Propiedad Intelectual o la legislación de protección de datos, se deben estar aclarados e incluidos en los términos y condiciones de empleo.

7.2 Categoría: Durante el empleo

Objetivo

Asegurar que las/los usuarias/os empleadas/os, contratistas y terceras personas estén al tanto de las amenazas e inquietudes de la seguridad de la información, sus responsabilidades y obligaciones, y estén equipadas para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir el riesgo de error humano.

7.2.1 Control: Responsabilidad de la dirección

La dirección debe solicitar a las/los empleadas/os, contratistas y usuarias/os de terceras partes que apliquen la seguridad en concordancia con las políticas y procedimientos establecidos por la organización, cumpliendo con lo siguiente:

a) Estar adecuadamente informados de sus roles y responsabilidades de seguridad de la información antes de que se le otorgue el acceso a información sensible o a los sistemas de información;

b) Ser provistos de guías para establecer las expectativas de seguridad de su rol dentro del Ministerio;

c) Ser motivados para cumplir con las políticas de seguridad del Ministerio;

d) Alcanzar un nivel de conciencia sobre la seguridad acorde con sus roles y responsabilidades dentro del Ministerio;

e) Cumplir con las condiciones y términos del empleo, los cuales incluyen las PSI del Ministerio y métodos adecuados de trabajo;

f) Mantener las habilidades adecuadas.

g) Fomentar la capacitación

Si las/los empleadas/os, contratistas y usuarias/os no son conscientes de sus responsabilidades de seguridad, pueden causar daños considerables al Ministerio. Un personal motivado tiene más probabilidades de ser más confiable y causar menos incidentes de seguridad de la información.

7.2.2 Control: Concientización, formación y capacitación en seguridad de la información

Todas/os las/los empleadas/os del Ministerio y, cuando sea pertinente, las/los usuarias/os externos y las/los terceras/os que desempeñen funciones en el Ministerio, deben recibir una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos del Ministerio. 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 o el material impreso.

La/El Responsable del Área de Recursos Humanos es el encargado de coordinar las acciones de capacitación que surgen de la presente PSI.

Cada seis (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.

Áreas Responsables del Material de Capacitación

El área responsable del material de capacitación es la Dirección General de Recursos Humanos dependiente de la Subsecretaría de Administración y Normalización Patrimonial de la Secretaría Legal y Administrativa del Ministerio de Economía..

Adicionalmente, las áreas responsables de generar el material de capacitación deben disponer de información sobre seguridad de la información para la Administración Pública Nacional en la Coordinación de Emergencias en Redes Teleinformáticas para complementar los materiales por ellas generados.

El personal que ingrese al Ministerio debe recibir el material, indicándosele el comportamiento esperado en lo que respecta a la seguridad de la información, antes de serle otorgados los privilegios de acceso a los sistemas que correspondan.

Por otra parte, se deben arbitrar 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.

7.2.3 Control: Proceso disciplinario

Se debe seguir el proceso disciplinario formal contemplado en las normas estatutarias, escalafonarias y convencionales que rigen al personal de la Administración Pública Nacional para las/los empleadas/os que violen la Política, Normas y Procedimientos de Seguridad del Ministerio.

El proceso disciplinario también se puede utilizar para disuadir a las/los empleadas/os, contratistas y terceras/os que incumplan con las políticas y procedimientos de la seguridad del Ministerio o incurrir en cualquier otro incumplimiento de la seguridad.

7.3 Categoría: Cese del empleo o cambio de puesto de trabajo

Objetivo

Cuando el egreso se produjere por alguno de los causales establecidos en la normativa vigente, se debe controlar la devolución en buen estado de los equipos asignados y que se eliminen todos los permisos de acceso a la información.

7.3.1 Control: Responsabilidad del cese o cambio

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

Puede ser necesario informar a las/los empleadas/os, contratistas y terceras/os de los cambios en el personal y los acuerdos de operación.

7.3.2 Control: Devolución de activos

Todas/os las/los empleadas/os, contratistas y usuarias/os de terceras partes deben devolver todos los activos de la organización en su poder (software, documentos corporativos, equipamiento, dispositivos de computación móviles, tarjetas de crédito, tarjetas de ingreso, etc.) tras la terminación de su empleo, contrato, o acuerdo.

En los casos donde la/el empleada/o, contratista y usuarias/os tengan un conocimiento que es importante para las operaciones actuales, dicho conocimiento debe ser documentado y transferido al Ministerio.

7.3.3 Control: Retiro de los derechos de acceso

Se deben revisar los derechos de acceso de un individuo a los activos asociados con los sistemas y servicios de información tras la desvinculación, y de ser necesario, removerlos.

Con el cambio de un empleo deben removerse todos los derechos de acceso que no fueron aprobados para el nuevo empleo, comprendiendo esto accesos lógicos y físicos, llaves, tarjetas de identificación, instalaciones de procesamiento de la información, suscripciones, y remoción de cualquier documentación que lo identifique como un miembro corriente del Ministerio.

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

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

a) Si la terminación o cambio es iniciado por la/el empleada/o, contratista o usuaria/o de tercera parte, o por la gestión y la razón de la finalización;

b) Las responsabilidades actuales de la/el empleada/o, contratista o cualquier otra usuaria/o;

c) El valor de los activos accesibles actualmente.

8. Cláusula: Gestión de Activos

Generalidades

El Ministerio debe tener un conocimiento preciso 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 usuaria/o, material de capacitación, procedimientos operativos o de soporte, planes de continuidad y contingencia, información archivada, etc.
- Recursos de software: software de aplicaciones, sistemas operativos, herramientas de desarrollo y publicación de contenidos, utilitarios, etc.
- Activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles, teléfonos celulares, tabletas), equipos de comunicaciones (routers, PABXs, máquinas de fax, contestadores automáticos, switches de datos, módems, etc.), medios magnéticos (cintas, discos, dispositivos móviles de almacenamiento de datos -pendrives, discos externos, etc.-), otros equipos técnicos (equipos de CCTV, impresoras, lectores biométricos, relacionados con el suministro eléctrico, unidades de aire acondicionado, controles automatizados de acceso, etc.), 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.

Generalmente, 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 el Ministerio.

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, grabada como audio o video. 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 su confidencialidad 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 PSI se aplica a toda la información administrada en el Ministerio, cualquiera sea el soporte en que se encuentre.

Responsabilidad

Las/Los Propietarias/os de los Activos son las/los encargadas/os de identificarlos y clasificarlos de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada, de definir las funciones que deben tener permisos de acceso a los activos y son responsables de mantener los controles adecuados para garantizar su seguridad.

La/El RSI 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 Propietaria/o de la Información debe supervisar que el proceso de clasificación y rótulo de información de su área de competencia se cumpla de acuerdo a lo establecido en la presente PSI.

8.1 Categoría: Responsabilidad sobre los activos

Objetivo

Todos los activos deben ser inventariados y contar con una/un propietaria/o nombrada/o.

Las/Los propietarias/as deben identificar todos los activos y se deben asignar la responsabilidad por el mantenimiento de los controles apropiados. La implementación de controles específicos puede ser delegada por la/el propietaria/o conforme sea apropiado, pero la/el propietaria/o sigue siendo responsable por la protección apropiada de los activos.

8.1.1 Control: Inventario de activos

Se deben identificar los activos de información del Ministerio. Existen muchos tipos de activos, que incluyen:

a) Información: bases de datos, archivos de datos, documentación, contratos, acuerdos;

b) Activos de software: software de aplicaciones, software de sistemas, herramientas de desarrollo, y utilitarios;

c) Activos físicos: equipamiento de computación, equipamiento de comunicaciones, medios removibles y otros equipamientos;

d) Instalaciones: edificios, ubicaciones físicas, tendido eléctrico, red de agua y gas, etc.;

e) Servicios: servicios de cómputo y de comunicaciones, servicios generales, por ejemplo: calefacción, iluminación, energía, y aire acondicionado;

f) Personas, y sus calificaciones, habilidades y experiencia;

g) Activos intangibles, tales como la reputación y la imagen del Ministerio.

El inventario debe actualizarse ante cualquier modificación de la información registrada y revisado con una periodicidad de seis (6) meses.

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

8.1.2 Control: Propiedad de los activos

Toda la información y los activos junto a sus medios de procesamiento de información son propiedad de un/a responsable designado/a en el Ministerio.

Las/Los propietarias/os designadas/os de los activos identificados deben cumplir sus funciones de propietaria/o, esto es:

a) Informar sobre cualquier cambio que afecte el inventario de activos;

b) Clasificar los activos en función a su valor;

c) Definir los requisitos de seguridad de los activos;

d) Velar por la implementación y el mantenimiento de los controles de seguridad requeridos en los activos.

Cabe aclarar que, si bien las/los propietarias/os pueden delegar la administración de sus funciones a personal idóneo a su cargo, conservan la responsabilidad de su cumplimiento. La delegación de la administración por parte de las/los propietarias/os de los activos debe ser documentada por éstos y proporcionada al RSI.

8.1.3 Control: Uso aceptable de los activos

Se deben identificar, documentar e implementar reglas para el uso aceptable de la información y los activos asociados con las instalaciones de procesamiento de la información.

Todas/os las/los empleadas/os, contratistas y usuarias/os de terceras partes deben seguir las reglas para el uso aceptable de la información y los activos asociados con las instalaciones de su procesamiento, incluyendo:

a) Correo electrónico,

b) Sistemas de gestión,

c) Estaciones de trabajo,

d) Dispositivos móviles,

e) Herramientas y equipamiento de publicación de contenidos, etc.

8.2 Categoría: Clasificación de la información

Objetivo

Asegurar que la información reciba un nivel de protección apropiado.

La información debe ser clasificada para indicar la necesidad, prioridades y grado de protección esperado cuando se la maneja.

La información tiene diversos grados de confidencialidad e importancia. Algunos ítems pueden requerir un nivel de protección adicional o manejo especial. Se debe utilizar un esquema de clasificación de información para definir un conjunto apropiado de niveles de protección y comunicar la necesidad de medidas de uso especiales.

8.2.1 Control: Directrices de clasificación

Para clasificar un activo de información, se deben evaluar las tres (3) características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad.

A continuación, se establece la metodología de clasificación de la información propuesta en función a cada una de las mencionadas características:

Confidencialidad:

1. Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleada/o del Ministerio o no. PUBLICO
2. Información que puede ser conocida y utilizada por todos las/los empleadas/os del Ministerio y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para el Ministerio, el Sector Público Nacional o terceros/as. RESERVADA - USO INTERNO
3. Información que sólo puede ser conocida y utilizada por un grupo de empleada/os, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas al Ministerio, al Sector Público Nacional o a terceros/as. RESERVADA – CONFIDENCIAL
4. Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleada/os, generalmente de la alta dirección del Ministerio, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves a éste, al Sector Público Nacional o a terceros/as. RESERVADA - SECRETA

Integridad:

1. Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operatoria del Ministerio.
2. Información cuya modificación no autorizada puede repararse, aunque podría ocasionar pérdidas leves para el Ministerio, el Sector Público Nacional o terceros/as.
3. Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas para el Ministerio, el Sector Público Nacional o terceros/as.
4. Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves al Ministerio, al Sector Público Nacional o a terceros/as.

Disponibilidad:

1. Información cuya inaccesibilidad no afecta la operatoria del Ministerio.
2. Información cuya inaccesibilidad permanente durante una (1) semana podría ocasionar pérdidas significativas para el Ministerio, el Sector Público Nacional o terceros/as.

3. Información cuya inaccesibilidad permanente durante un (1) día podría ocasionar pérdidas significativas al Ministerio, al Sector Público Nacional o a terceros/as.
4. Información cuya inaccesibilidad permanente durante una (1) hora podría ocasionar pérdidas significativas al Ministerio, al Sector Público Nacional o a terceros/as.

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

Se debe asignar 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 supera el uno (1).

CRITICIDAD MEDIA: alguno de los valores asignados es dos (2).

CRITICIDAD ALTA: alguno de los valores asignados es tres (3).

Sólo la/el Propietaria/o de la información puede asignar o cambiar su nivel de clasificación, cumpliendo con los siguientes requisitos previos:

- Asignarle una fecha de efectividad;
- Comunicárselo a la/el depositaria/o del recurso;
- Realizar los cambios necesarios para que las/los usuarias/os conozcan la nueva clasificación.

Luego de clasificada la información, su propietaria/o identifica los recursos asociados (sistemas, equipamiento, servicios, etc.) y los perfiles funcionales que deben tener acceso a ésta.

En adelante se menciona como "información clasificada" (o "datos clasificados") a aquella que se encuadre en los niveles 2, 3 o 4 de Confidencialidad.

8.2.2 Control: Etiquetado y manipulación de la información

Se deben definir procedimientos para el rotulado y manejo de información, de acuerdo al esquema de clasificación definido. Éstos contemplan los recursos de información tanto en formatos físicos como electrónicos e incorporan 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.).
- Transmisión a través de mecanismos de intercambio de archivos (FTP, almacenamiento masivo remoto, etc.).

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

8.3 Categoría: Gestión de medios

Objetivo

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

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

8.3.1 Control: Administración de Medios Informáticos Removibles

La/El Responsable del Área Informática, con la asistencia del RSI, debe implementar procedimientos para la administración de medios informáticos removibles, como cintas, discos, pendrives e informes impresos. El cumplimiento de los procedimientos se hará de acuerdo a la cláusula "9.1 Categoría: Requerimientos para la Gestión de Acceso".

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

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

b) Requerir autorización para retirar cualquier medio del Ministerio 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 proveedoras/es y la criticidad de la información almacenada.

8.3.2 Control: Eliminación de Medios de Información

La/El Responsable del Área Informática, junto con el RSI debe definir procedimientos para la eliminación segura de los medios de soporte de información respetando la normativa vigente.

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

a) Documentos en papel;

b) Voces, videos u otras grabaciones;

c) Papel carbónico;

d) Informes de salida;

e) Cintas de impresora de un (1) solo uso;

f) Cintas magnéticas;

g) Discos u otros dispositivos removibles;

h) Medios de almacenamiento óptico (todos los formatos incluyendo todos los medios de distribución de software del fabricante o proveedora/or);

i) Listados de sistemas;

j) Datos de prueba;

k) Documentación del sistema.

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

8.3.3 Control: Seguridad de los Medios en Tránsito

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

a) La utilización de medios de transporte o servicios de mensajería confiables. La/El Propietaria/o de la Información a transportar debe determinar qué servicio de mensajería utilizar conforme la criticidad de la información a transmitir;

b) Suficiente embalaje para envío de medios a través de servicios postales o de mensajería, siguiendo las especificaciones de los/las fabricantes o proveedoras/es;

c) La adopción de controles especiales, cuando resulte necesario, a fin de proteger la información sensible contra divulgación o modificación no autorizadas. Entre los ejemplos se incluyen: i) Uso de recipientes cerrados. ii) Entrega en mano;

c) Embalaje a prueba de apertura no autorizada (que revele cualquier intento de acceso);

d) En casos excepcionales, división de la mercadería a enviar en más de una (1) entrega y envío por diferentes rutas.

9. Cláusula: Gestión de Accesos

Generalidades

El acceso a la información por medio de un sistema de restricciones y excepciones 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 las/los usuarias/os de todos los niveles, desde el registro inicial de nuevas/os usuarias/os hasta la privación final de derechos de las/los usuarias/os que ya no requieren el acceso.

La cooperación de las/los usuarias/os es esencial para la eficacia de la seguridad, por lo tanto, es necesario concientizarlos 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 usuarias/os por medio de técnicas de autenticación y autorización.

Controlar la seguridad en la conexión entre la red del Ministerio y otras redes públicas o privadas. Registrar y revisar eventos y actividades críticas llevadas a cabo por las/los usuarias/os en los sistemas.

Concientizar a las/los usuarias/os 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 PSI 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 Ministerio, cualquiera sea la función que desempeñen.

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

Responsabilidad

La/El RSI está a cargo de:

- Definir normas y procedimientos para la gestión de accesos a todos los sistemas, bases de datos y servicios de información multiusuaria/o; 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 (logs); y el ajuste de relojes de acuerdo a un estándar preestablecido;
- Definir pautas de utilización de Internet para todos las/los usuarias/os;
- 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 periódicamente la asignación de privilegios a usuarias/os;
- Analizar y sugerir medidas a ser implementadas para efectivizar el control de acceso a Internet de las/los usuarias/os;
- Verificar el cumplimiento de las pautas establecidas, relacionadas con control de accesos, registración de usuarias/os, administración de privilegios, administración de contraseñas, utilización de servicios de red, autenticación de usuarias/os 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 (físicos y lógicos), subdivisión de redes, control de conexiones a la red, control de ruteo de red, etc.;
- Concientizar a las/los usuarias/os sobre el uso apropiado de contraseñas y de equipos de trabajo;
- Verificar periódicamente el cumplimiento de los procedimientos de revisión de registros de auditoría;
- Asistir a las/los usuarias/os que corresponda en el análisis de riesgos a los que se expone la información y los componentes del ambiente informático que le sirven de soporte.

Las/Los Propietarias/os de la Información están 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 usuarias/os a ser registrados en los sistemas de procesamiento de su incumbencia y la periodicidad de su revisión.

- Aprobar y solicitar la asignación de privilegios a usuarias/os e informar los cambios cuando resulte pertinente (baja, cambio de área).;
- 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.

Las/Los Propietarias/os de la Información junto con la UAI o en su defecto quien sea propuesto/a por el CSI, debe definir un cronograma de depuración de logs y registros de auditoría en línea en función a normas vigentes y a sus propias necesidades.

Las/Los Responsable de las Unidades Organizativas, junto con la/el RSI, 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, autorizan el acceso de las/los usuarias/os a su cargo a los servicios y recursos de red y a Internet.

La/El Responsable del Área Informática cumple las siguientes funciones:

- Implementar procedimientos para la activación y desactivación de derechos de acceso a las redes;
- Analizar e implementar los métodos de autenticación y control de acceso definidos en los sistemas, bases de datos y servicios;
- Evaluar el costo y el impacto de la implementación de “enrutadores”, “gateways” y/o "firewalls" 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 (logs) de usuarias/os de acuerdo a lo definido por las/los propietarias/as de la información, así como su depuración;
- 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 usuarias/os (Ej.: biometría, verificación de firma, uso de autenticadores de hardware);
- Definir e implementar la configuración que debe efectuarse para cada servicio de red, de manera de garantizar la seguridad en su operatoria;
- Analizar las medidas a ser implementadas para efectivizar el control de acceso a Internet de las/los usuarias/os;
- 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 UAI o en su defecto quien sea propuesto/a por el CSI, debe tener acceso a los registros de eventos a fin de colaborar en el control y efectuar recomendaciones sobre modificaciones a los aspectos de seguridad.

El CSI debe aprobar el análisis de riesgos de la información efectuado. Asimismo, debe aprobar el período definido para el mantenimiento de los registros de auditoría generados.

9.1 Categoría: Requerimientos para la Gestión de Acceso

Objetivo

Controlar el acceso a la información. Se debe controlar el acceso a la información, medios de procesamiento de la información y procesos sobre la base de los requerimientos del Ministerio y de seguridad. Las reglas de control del acceso deben tomar en cuenta las políticas para la divulgación y autorización de la información.

9.1.1 Control: Política de Gestión de Accesos

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

a) Identificar los requerimientos de seguridad de cada una de las aplicaciones;

b) Identificar toda la información relacionada con las aplicaciones;

c) Establecer criterios coherentes entre esta Política de Control de Acceso y la Política de Clasificación de Información de los diferentes sistemas y redes (Ver cláusula 8: Gestión de Activos);

d) Identificar la legislación aplicable y las obligaciones contractuales con respecto a la protección del acceso a datos y servicios;

e) Definir los perfiles de acceso de usuarias/os estándar, comunes a cada categoría de puestos de trabajo;

f) Administrar los derechos de acceso en un ambiente distribuido y de red, que reconozcan todos los tipos de conexiones y dispositivos disponibles.

9.1.2 Control: Reglas de Gestión de Acceso

Las reglas de control de acceso especificadas, deben:

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 de la/el usuaria/o (Ver cláusula 8: Gestión de Activos);

d) Controlar los cambios en los permisos de usuaria/o que son iniciados automáticamente por el sistema de información y aquellos que son iniciados por la/el administradora/or;

e) Controlar las reglas que requieren la aprobación de la/el administradora/or o de la/el Propietaria/o de la Información de que se trate, antes de entrar en vigencia, y aquellas que no requieren aprobación.

9.2 Categoría: Administración de Gestión de Usuarias/os

Objetivo

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

Los procedimientos deben abarcar todas las etapas en el ciclo de vida del acceso de la/el usuaria/o, desde el registro inicial de usuarias/os nuevas/os hasta la baja final de las/los usuarias/os que ya no requieren acceso a los sistemas y servicios de información.

9.2.1 Control: Registración de Usuarias/os

La/El RSI debe definir un procedimiento formal de registro de usuaria/os para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información multiusuaria/o, el cual debe comprender:

a) Utilizar identificadores de usuarias/os únicas/os, de manera que se pueda identificar a las/los usuarias/os por sus acciones evitando la existencia de múltiples perfiles de acceso para un/a mismo/a empleado/a. El uso de identificadores grupales no debe ser permitido bajo ninguna circunstancia;

b) Verificar que la/el usuaria/o tiene autorización de la/el Propietaria/o 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 de la/el usuaria/o y es coherente con la PSI del Ministerio, por ejemplo, que no compromete la segregación de funciones;

d) Entregar a las/los usuarias/os un detalle escrito de sus derechos de acceso;

e) Requerir que las/los usuarias/os firmen declaraciones señalando que comprenden y aceptan las condiciones para el acceso;

f) Garantizar que las/los proveedoras/es de servicios no otorguen acceso hasta que se hayan completado los procedimientos de autorización;

g) Mantener un registro formal actualizado de todas las personas registradas para utilizar el servicio;

h) Cancelar inmediatamente los derechos de acceso de las/los usuarias/os que cambiaron sus tareas, o de aquellas/os a las/los que se les revocó la autorización, se desvincularon del Ministerio o sufrieron la pérdida/robo de sus credenciales de acceso;

i) Efectuar revisiones periódicas con el objeto de:

   a) Cancelar identificadores y cuentas de usuarias/os redundantes.

   b) Inhabilitar cuentas inactivas por más de sesenta (60) días.

   c) Eliminar cuentas inactivas por más de ciento veinte (120) días.

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

j) Garantizar que los identificadores de usuarias/os redundantes no se asignen a otras/os usuarias/os;

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

9.2.2 Control: Gestión de Privilegios

Se debe limitar y controlar la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas.

Los sistemas multiusuaria/o que requieren protección contra accesos no autorizados deben prever una asignación de privilegios controlada mediante un proceso de autorización formal. Se deben tener en cuenta los siguientes pasos:

a) Identificar los privilegios asociados a cada producto del sistema, por ejemplo, sistema operativo, sistema de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los productos.

b) Asignar los privilegios a individuos sobre la base de la necesidad de uso y evento por evento, por ejemplo, el requerimiento mínimo para su rol funcional.

c) Mantener un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no deben ser otorgados hasta que se haya completado el proceso formal de autorización.

d) Establecer un período de vigencia para el mantenimiento de los privilegios (en base a la utilización que se les dará a los mismos) luego del cual éstos serán revocados.

e) Promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a las/los usuarias/os.

Las/Los Propietarias/os de la Información son las/los encargadas/os de aprobar la asignación de privilegios a usuarias/os y solicitar su implementación, bajo la supervisión de la/el RSI.

9.2.3 Control: Gestión de Contraseñas de Usuaria/o

La asignación de contraseñas se controla a través de un proceso de administración formal, respetando los siguientes pasos:

a) Requerir que las/los usuarias/os 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 las/los usuarias/os cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al sistema. Las contraseñas provisorias, que se asignan cuando las/los usuarias/os olvidan su contraseña, sólo deben suministrarse una vez acreditada la identidad de la/el usuaria/o.

c) Generar contraseñas provisorias seguras para otorgar a las/los usuarias/os. Se debe evitar la participación de terceros/as o el uso de mensajes de correo electrónico sin protección (texto claro) en el mecanismo de entrega de la contraseña y las/los usuarias/os deben dar acuse de recibo formal cuando la reciban.

d) Almacenar las contraseñas sólo en sistemas informáticos protegidos.

e) Utilizar otras tecnologías de autenticación y autorización de usuarias/os, 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 esas herramientas se puede disponer cuando la evaluación de riesgos realizada por la/el RSI conjuntamente con la/el Responsable del Área de Informática y la/el Propietaria/o de la Información lo determine necesario, adecuado y/ o justificado.

f) Configurar los sistemas de tal manera que:

   a) Las contraseñas sean del tipo “password fuerte” y tengan una cantidad a definir mínima de caracteres.

   b) Suspendan o bloqueen permanentemente a la/el usuaria/o luego de una cantidad a definir máxima de intentos de entrar con una contraseña incorrecta (debe pedir la rehabilitación ante quien corresponda).

   c) Solicitar el cambio de la contraseña a intervalos regulares. Dicho intervalo deberá definirse.

   d) Impedir que las últimas contraseñas sean reutilizadas. La cantidad mínima de últimas contraseñas deberá definirse.

   e) Establecer un tiempo de vida mínimo para las contraseñas, el cual deberá definirse.

   f) Todos los parámetros mencionados anteriormente serán definidos en un documento aparte por el RSI, el cual deberá ser actualizado con una frecuencia no mayor a un (1) año.

9.2.4 Control: Administración de Contraseñas Críticas

En los diferentes ambientes de procesamiento existen cuentas de usuarias/os 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 son de uso habitual (diario), sino que sólo pueden ser utilizadas ante una necesidad específica de realizar alguna tarea que lo requiera y se deben proteger por contraseñas con un mayor nivel de complejidad que el habitual. La/El RSI debe definir procedimientos para la administración de dichas contraseñas críticas que contemplen lo siguiente:

a) Definir las causas que justifican el uso de contraseñas críticas, así como el nivel de autorización requerido.

b) Las contraseñas seleccionadas deben ser seguras, y su definición efectuada como mínimo por dos (2) 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 deben resguardarse debidamente.

d) La utilización de las contraseñas críticas debe registrarse, documentando las causas que determinaron su uso, así como la/el responsable de las actividades que se efectúen con éstas.

e) Cada contraseña crítica se renovará una vez utilizada y se debe definir un período luego del cual ésta será renovada en caso de que no se la haya utilizado.

f) Todas las actividades que se efectúen con las cuentas críticas se deben registrar para luego ser revisadas. Dicho registro debe ser revisado posteriormente por la/el RSI y permanecer a disposición de la UAI, en caso de que lo requiera.

9.2.5 Control: Revisión de Derechos de Acceso de Usuarias/os

A fin de mantener un control eficaz del acceso a los datos y servicios de información, la/el Propietaria/o de la Información de que se trate debe revisar, a intervalos regulares de seis (6) meses, los derechos de acceso de las/los usuarias/os, mediante un proceso formal. Se deben contemplar los siguientes controles:

a) Revisar los derechos de acceso de las/los usuarias/os a intervalos de seis (6) meses.

b) Revisar las autorizaciones de privilegios especiales de derechos de acceso a intervalos de tres (3) meses.

c) Revisar las asignaciones de privilegios a intervalos de seis (6) meses, a fin de garantizar que no se obtengan privilegios no autorizados.

9.3 Categoría: Responsabilidades de la/el Usuaria/o

Objetivo

Evitar el acceso de usuarias/os no autorizados, evitar poner en peligro la información y evitar el robo de información y los medios de procesamiento de la información.

La cooperación de las/los usuarias/os autorizadas/os es esencial para una seguridad efectiva.

Las/Los usuarias/os deben estar al tanto de sus responsabilidades para mantener controles de acceso efectivos, particularmente con relación al uso de claves secretas y la seguridad del equipo de la/el usuaria/o.

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

9.3.1 Control: Uso de Contraseñas

Las/Los usuarias/os 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 una/un usuaria/o, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.

Las/Los usuarias/os 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 la/el Responsable del Activo de Información de que se trate, que:

   i. Sean fáciles de recordar.

   ii. 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.

   iii. No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.

   iv. Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.

   v. Cambiar las contraseñas provisorias en el primer inicio de sesión ("log on").

   vi. Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.

   vii. Notificar de acuerdo a lo establecido en la cláusula 16: Gestión de Incidentes de Seguridad, cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

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

9.4 Categoría: Control de Acceso a Sistemas y Aplicaciones

Objetivo

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

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

El acceso de la/el usuaria/o a las redes y servicios de las redes no deben comprometer la seguridad de los servicios de la red asegurando:

a) Que existan las interfaces apropiadas entre la red del Ministerio y las redes de otras organizaciones y redes públicas;

b) Se apliquen los mecanismos de autenticación apropiados para las/los usuarias/os y el equipo;

c) El control del acceso de la/el usuaria/o a la información sea obligatorio.

9.4.1 Control: Política de Utilización de los Servicios de Red

Las conexiones no seguras a los servicios de red pueden afectar a todo el Ministerio, por lo tanto, se debe controlar el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que las/los usuarias/os que tengan acceso a las redes y a sus servicios no comprometan su seguridad.

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

Este control es particularmente importante para las conexiones de red a aplicaciones que procesen información clasificada o aplicaciones críticas, o a usuarias/os 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 Ministerio.

Para ello se deben desarrollar procedimientos para la activación y desactivación de derechos de acceso a las redes, los cuales deben comprender:

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, 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 PSI debe ser coherente con la Política de Gestión de Accesos del Ministerio.

9.4.2 Control: 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 Ministerio, o para el uso no autorizado de servicios de información. Por esto, el camino de las comunicaciones debe ser controlado.

Se deben limitar las opciones de elección de la ruta entre la terminal de usuaria/o y los servicios a los cuales ésta/e se encuentra autorizada/o a acceder, mediante la implementación de controles en diferentes puntos.

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

a) Asignar números telefónicos o líneas en forma dedicada.

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 las/los usuarias/os.

d) Evitar la navegación ilimitada por la red.

e) Imponer el uso de sistemas de aplicación y/o "gateways" de seguridad específicos para usuarias/os externos de la red.

f) Controlar activamente las comunicaciones con origen y destino autorizados a través de un "gateway", por ejemplo, utilizando "firewalls" y generando alertas ante eventos no previstos.

g) Restringir el acceso a redes, estableciendo dominios lógicos separados, por ejemplo, redes privadas virtuales para grupos de usuarias/os dentro o fuera del Ministerio.

Los requerimientos relativos a caminos forzados se deben basar en la Política de Control de Accesos del Ministerio. La/El RSI, conjuntamente con la/el Propietaria/o de la Información de que se trate realizará una evaluación de riesgos a fin de determinar los mecanismos de control que corresponda en cada caso.

9.4.3 Control: Autenticación de Usuarias/os para Conexiones Externas

Las conexiones externas son de gran potencial para accesos no autorizados a la información del Ministerio. Por consiguiente, el acceso de usuarias/os remotos está sujeto al cumplimiento de procedimientos de autenticación. Existen diferentes métodos de autenticación, algunos de los cuales brindan un mayor nivel de protección que otros. La/El RSI,

conjuntamente con la/el Propietaria/o de la Información de que se trate, realizará una evaluación de riesgos a fin de determinar el mecanismo de autenticación que corresponda en cada caso.

La autenticación de usuarias/os 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:
   i. Asignación de la herramienta de autenticación.
   ii. Registro de los poseedores de autenticadores.
   iii. Mecanismo de rescate al momento de la desvinculación del personal al que se le otorgó.
   iv. 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:
   i. Establecimiento de las reglas con la/el usuaria/o.
   ii. 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 de la/el usuaria/o de red, a fin de constatar el origen de la conexión.

Los procedimientos y controles de rellamada, o dial-back, pueden brindar protección contra conexiones no autorizadas a las instalaciones de procesamiento de información del Ministerio. Al aplicar este tipo de control, el Ministerio no debe utilizar servicios de red que incluyan desvío de llamadas. Si por alguna causa es preciso mantener el desvío de llamadas, no es posible aplicar el control de rellamada. Asimismo, es importante que el proceso de rellamada garantice que se produzca a su término una desconexión real del lado del Ministerio.

En caso de utilizarse sistemas de Voz sobre IP, deben ajustarse los controles a fin de que no sean utilizados para efectuar comunicaciones no autorizadas (ej.: bloqueo de puertos).

9.4.4 Control: 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 Ministerio. Por consiguiente, las conexiones a sistemas informáticos remotos deben ser autenticadas. Esto es particularmente importante si la conexión utiliza una red que está fuera de control de la gestión de seguridad del Ministerio. 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 usuarias/os remotos, cuando éstos están conectados a un servicio informático seguro y compartido.

9.4.5 Control: 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, deben ser protegidos por un mecanismo de seguridad apropiado, con las mismas características del punto "9.4.3 Control: Autenticación de Usuarias/os para Conexiones Externas". También para este caso debe tenerse en cuenta el punto "9.4.2 Control: Camino Forzado".

9.4.6 Control: Subdivisión de Redes

Para controlar la seguridad en redes extensas se pueden dividir en dominios lógicos separados.

Para esto se definirán y documentarán los perímetros de seguridad que sean convenientes.

Estos perímetros se implementan 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 de acuerdo a la Política de Control de Accesos.

La subdivisión en dominios de la red debe tomar en cuenta criterios tales 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 Gestión de Accesos y los requerimientos de acceso (9.1 Categoría: Requerimientos para la Gestión de Acceso), la/el Responsable del Área Informática debe evaluar el costo relativo y el impacto en el desempeño que ocasione la implementación de enrutadores o "gateways" adecuados para subdividir la red. Luego debe decidir, junto con la/el RSI, el esquema más apropiado a implementar.

9.4.7 Control: Acceso a Internet

El acceso a Internet solo puede ser utilizado con propósitos autorizados o con el destino por el cual fue provisto.

La/El RSI debe definir procedimientos para solicitar y aprobar accesos a Internet. Los accesos deben ser autorizados formalmente por la/el Responsable de la Unidad Organizativa a cargo del personal que lo solicite. Asimismo, se deben definir las pautas de utilización de Internet para todas/os las/los usuarias/os.

Se debe evaluar la conveniencia de utilizar el registro de los accesos de las/los usuarias/os a Internet con el objeto de realizar revisiones de los accesos efectuados o analizar casos particulares. Dicho control debe ser comunicado a las/los usuarias/os de acuerdo a lo establecido en el punto 6.1.5 Control: Acuerdos de confidencialidad. Para ello, la/el RSI junto con la/el Responsable del Área de Informática deben analizar las medidas a ser implementadas para efectivizar dicho control, como ser la instalación de "firewalls", "proxies", etc.

9.4.8 Control: Conexión a la Red Sobre la base de lo definido en el punto "9.1 Categoría: Requerimientos para la Gestión de Accesos", se deben implementar controles para limitar la capacidad de conexión de las/los usuarias/os. Dichos controles se pueden implementar en los "gateways" que separen los diferentes dominios de la red. Algunos ejemplos de los entornos a los 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: Ruteo de Red

En las redes compartidas, especialmente aquellas que se extienden fuera de los límites del Ministerio, se deben incorporar controles de ruteo, para asegurar que las conexiones informáticas y los flujos de información no violen la 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 Control: Seguridad de los Servicios de Red

La/El RSI junto con la/el Responsable del Área informática deben definir las pautas para garantizar la seguridad de los servicios de red del Ministerio, tanto públicos como privados.

Para ello se han de tener 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 presentarse.
- Instalar periódicamente las actualizaciones de seguridad.

Dicha configuración debe ser revisada periódicamente por la/el RSI.

9.5 Categoría: Control de Acceso al Sistema Operativo

Objetivo

Evitar el acceso no autorizado a los sistemas operativos.

Se deben utilizar medios de seguridad para impedir el acceso a los sistemas operativos a las/los usuarias/os no autorizadas/os. Los medios deben tener la capacidad para:

a) Autenticar a las/los usuarias/os autorizadas/os, en concordancia con una política de control de acceso definida;

b) Registrar los intentos exitosos y fallidos de autenticación del sistema;

c) Registrar el uso de los privilegios especiales del sistema;

d) Emitir alarmas cuando se violen las políticas de seguridad del sistema;

e) Proporcionar los medios de autenticación apropiados;

f) Cuando sea apropiado, restringir el tiempo de conexión de las/los usuarias/os.

9.5.1 Control: Identificación Automática de Terminales

La/El RSI junto con la/el Responsable del Área Informática debe realizar una evaluación de riesgos a fin de determinar el método de protección adecuado para el acceso al Sistema Operativo.

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

a) El método de identificación automática de terminales utilizado.

b) El detalle de transacciones permitidas por terminal o dispositivo.

9.5.2 Control: Procedimientos de Conexión de Terminales.

El acceso a los servicios de información sólo es permitido a través de un proceso de conexión seguro. El procedimiento de conexión en un sistema informático debe estar 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 una/un usuaria/o no autorizada/o.

El procedimiento de identificación debe:

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 las/los usuarias/os autorizadas/os pueden acceder a la computadora.

c) Evitar dar mensajes de ayuda que pudieran asistir a usuarias/os no autorizadas/os 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:

   i. Registrar los intentos no exitosos.

   ii. Impedir otros intentos de identificación, una vez superado el límite permitido.

   iii. 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:

   i. Fecha y hora de la conexión exitosa anterior.

   ii. Detalles de los intentos de conexión no exitosos desde la última conexión exitosa.

9.5.3 Control: Identificación y Autenticación de las/los Usuarias/os

Todos las/los usuarias/os (incluido personal de soporte técnico, como las/los operadoras/es, administradoras/es de red, programadoras/es de sistemas y administradoras/es de bases de datos) deben tener un identificador único (ID de usuaria/o) solamente para su uso personal exclusivo, de manera que las actividades puedan rastrearse con posterioridad hasta llegar a la/el agente responsable, a fin de garantizar la trazabilidad de las transacciones. Los identificadores de usuarias/os no deben dar ningún indicio del nivel de privilegio otorgado.

Si se utiliza un método de autenticación físico (por ejemplo, autenticadores de hardware), debe 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 Control: Sistema de Administración de Contraseñas

Las contraseñas constituyen uno de los principales medios de validación de la autoridad de una/un usuaria/o 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 las/los usuarias/os seleccionen y cambien sus propias contraseñas (luego de cumplido el plazo mínimo de mantenimiento de éstas) 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 Control: Uso de Contraseñas”.

d) Imponer cambios en las contraseñas en aquellos casos en que las/los usuarias/os mantengan sus propias contraseñas.

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

f) Evitar mostrar las contraseñas en pantalla cuando son ingresadas.

10. Cláusula: Criptografía

Generalidades

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

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

Objetivos

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

Alcance

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

Responsabilidad

La/El RSI, junto con la/el Propietaria/o de la Información, deben definir en función a la criticidad de la información, los requerimientos de protección mediante métodos criptográficos. Luego, la/el RSI define junto con la/el Responsable del Área de Sistemas, los métodos de encripción a ser utilizados.

Asimismo, la/el RSI hade cumplir las siguientes funciones:

- Definir los procedimientos de administración de claves.
- Verificar el cumplimiento de los controles establecidos para el desarrollo y mantenimiento de sistemas.
- Garantizar el cumplimiento de los requerimientos de seguridad para el software.
- Definir procedimientos para el control de cambios a los sistemas; la verificación de la seguridad de las plataformas y bases de datos que soportan e interactúan con los sistemas; el control de código malicioso; y la definición de las funciones del personal involucrado en el proceso de entrada de datos.

10.1 Categoría: Cumplimiento de Requisitos Legales

Objetivo

Se deben utilizar sistemas y técnicas criptográficas para la protección de la información en base a un análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad. Se debe desarrollar una política sobre el uso de controles criptográficos. Se debe establecer una gestión de claves para sostener el uso de técnicas criptográficas.

10.1.1 Control: Política de Utilización de Controles Criptográficos

El Ministerio establece la presente Política de uso de controles criptográficos, a fin de determinar su correcto uso. Para ello se indica que:

a) Se deben utilizar controles criptográficos en los siguientes casos:

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

ii. Para la transmisión de información clasificada, fuera del ámbito del Ministerio.

iii. Para el resguardo de información, cuando así surja de la evaluación de riesgos realizada por la/el Propietaria/o de la Información y la/el RSI.

b) Se deben establecer 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) La/El Responsable del Área Informática deberá proponer la asignación de funciones oportunamente, mediante un documento específico;

d) Se deberán redactar las normas y procedimientos necesarios para describir los algoritmos de firma a utilizar, como así también la longitud de clave a emplear, debiéndose verificar esta condición periódicamente con el objeto de efectuar las actualizaciones correspondientes.

10.1.2 Control: Cifrado

El/La Propietaria/o de la Información y la/el RSI deben llevar a cabo una evaluación de riesgos para identificar 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 Ministerio en materia criptográfica, se deben considerar los controles aplicables a la exportación e importación de tecnología criptográfica.

10.1.3 Control: 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 (2) claves relacionadas de manera única, donde una clave, denominada privada, se utiliza para crear una firma y la otra, denominada pública, para verificarla.

Se deben tomar 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.

Se recomienda que las claves criptográficas utilizadas para firmar digitalmente no sean empleadas en procedimientos de cifrado de información. Dichas claves deben ser resguardadas bajo el control exclusivo de su titular.

Las firmas y certificados digitales se rigen por la legislación vigente (Ley N° 25.506 –texto actualizado-, los decretos 892 del 1º de noviembre de2017 y 182 del 11 de marzo de 2019 y sus normas modificatorias o complementarias), que determina las condiciones bajo las cuales una firma digital es legalmente válida.

En algunos casos podría ser necesario establecer acuerdos especiales para respaldar el uso de las firmas digitales. A tal fin se debe obtener asesoramiento legal con respecto al marco normativo aplicable y la modalidad del acuerdo a implementar. (Ver Cláusula 10.1.1: Control: Política de utilización de controles criptográficos).

10.1.4 Control: Servicios de No Repudio

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

10.1.5 Control: Protección de claves criptográficas

Se debe implementar un sistema de administración de claves criptográficas para respaldar la utilización por parte del Ministerio de los dos (2) tipos de técnicas criptográficas, a saber:

a) Técnicas de clave secreta (criptografía simétrica), cuando (2) dos o más actores comparten la misma clave y ésta se utiliza tanto para cifrar información como para descifrarla;

b) Técnicas de clave pública (criptografía asimétrica), cuando cada usuaria/o tiene un par de claves: una (1) clave pública (que puede ser revelada a cualquier persona) utilizada para cifrar y una (1) clave privada (que debe mantenerse en secreto) utilizada para descifrar. Las claves asimétricas utilizadas para cifrado no deben ser las mismas que se utilizan para firmar digitalmente.

Todas las claves deben ser protegidas contra modificación y destrucción. Las claves secretas y privadas deben ser protegidas contra copia o divulgación no autorizada. Se deben aplicar con éste propósito los algoritmos criptográficos oportunamente definidos.

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

10.1.6 Control: Protección de Claves criptográficas: Normas y procedimientos

Se deben redactar las normas y procedimientos necesarios para:

a) Generar claves para diferentes sistemas criptográficos y diferentes aplicaciones;

b) Generar y obtener certificados de clave pública de manera segura;

c) Distribuir claves de forma segura a las/los usuarias/os que corresponda, incluyendo información sobre cómo deben activarse cuando se reciban;

d) Almacenar claves, incluyendo la forma de acceso a éstas por parte de las/los usuarias/os autorizadas/os;

e) Cambiar o actualizar claves, incluyendo reglas sobre cuándo y cómo deben cambiarse las claves;

f) Revocar claves, incluyendo cómo deben retirarse o desactivarse éstas, por ejemplo, cuando las claves están comprometidas o cuando una/un usuaria/o se desvincula del Ministerio (en cuyo caso las claves también deben archivarse);

g) Recuperar claves pérdidas o alteradas como parte de la administración de la continuidad de las actividades del Ministerio, por ejemplo, para la recuperación de la información cifrada;

h) Archivar claves, por ejemplo, para la información archivada o resguardada;

i) Destruir claves;

j) Registrar y auditar las actividades relativas a la administración de claves.

A fin de reducir la probabilidad de compromiso, las claves deben tener fechas de inicio y caducidad de vigencia, definidas de manera que sólo puedan ser utilizadas por el lapso de doce (12) meses.

Además de la administración segura de las claves secretas y privadas, debe tenerse en cuenta la protección de las claves públicas. Este problema es abordado mediante el uso de un certificado de clave pública. Este certificado se generará de forma que vincule de manera única la información relativa a la/el propietaria/o del par de claves pública/privada con la clave pública.

En consecuencia, es importante que el proceso de administración de los certificados de clave pública sea absolutamente confiable. Este proceso debe ser llevado a cabo por una entidad denominada Autoridad de Certificación (AC) o Certificador.

11. Cláusula: 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 Ministerio. Asimismo, pretende evitar al máximo el riesgo de accesos físicos no autorizados, mediante el establecimiento de perímetros de seguridad.

Se distinguen tres (3) 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 Ministerio 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 Ministerio como en instalaciones próximas a su sede 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 Ministerio.

Dichos procesos deben ser ejecutados bajo estrictas normas de seguridad y de preservación de la información almacenada en éstos. Así también se debe tener en cuenta la aplicación de dichas normas en equipamiento perteneciente al Ministerio, pero situado físicamente fuera de éste("housing"), así como en equipamiento ajeno que albergue sistemas y/o preste servicios de procesamiento de información al Ministerio ("hosting").

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

Gran cantidad de información manejada en las oficinas se encuentra almacenada en papel, por lo que es necesario establecer pautas de seguridad para la conservación de dicha documentación y para su destrucción cuando así lo requiera.

Objetivo

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

Proteger el equipamiento de procesamiento de información crítica del Ministerio ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados. Asimismo, contemplar su protección en su traslado y permanencia fuera de las áreas protegidas, por motivos de mantenimiento u otros.

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

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

Proporcionar protección proporcional a los riesgos identificados.

Alcance

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

Responsabilidad

La/El RSI debe definir junto con la/el Responsable del Área Informática y las/los Propietarias/os de la Información, según corresponda, las medidas de seguridad física y ambiental para el resguardo de los activos críticos, en función a un análisis de riesgos, y debe controlar su implementación. Asimismo, debe verificar el cumplimiento de las disposiciones sobre seguridad física y ambiental indicadas en la presente Cláusula.

La/el Responsable del Área Informática asiste al RSI en la definición de las medidas de seguridad a implementar en áreas protegidas, y coordina su implementación. Asimismo, controla el mantenimiento del equipamiento informático de acuerdo a las indicaciones de proveedoras/es tanto dentro como fuera de las instalaciones del Ministerio.

Las/Los Responsables de Unidades Organizativas definen los niveles de acceso físico del personal del Ministerio a las áreas restringidas bajo su responsabilidad.

Las/Los Propietarias/os de la Información autorizan formalmente el trabajo fuera de las instalaciones con información de su incumbencia a las/los empleadas/os del Ministerio cuando lo crean conveniente.

La UAI o en su defecto quien sea propuesto por el CSI revisa los registros de acceso a las áreas protegidas.

Todo personal del Ministerio 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.

11.1 Categoría: Áreas Seguras

Objetivo

Evitar el acceso físico no autorizado, daño e interferencia con la información y los locales del Ministerio.

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

11.1.1 Control: Perímetro de seguridad física

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

El Ministerio debe utilizar 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 son definidas por la/el Responsable del Área Informática con el asesoramiento de la/el RSI, de acuerdo a la evaluación de riesgos efectuada.

Se deben considerar e implementar 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 deben implementar los medios alternativos de control de acceso físico al área o edificio que serán establecidos oportunamente, mediante un documento específico. El acceso a dichas áreas y edificios debe estar restringido exclusivamente al personal autorizado. Los métodos implementados deben registrar cada ingreso y egreso en forma precisa.

d) 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.

e) Identificar claramente todas las puertas de incendio de un perímetro de seguridad.

Un área segura puede ser una oficina con llave, o varias oficinas rodeadas por una barrera de seguridad física interna continua. Pueden ser necesarios barreras y perímetros adicionales para controlar el acceso físico entre las áreas con diferentes requerimientos de seguridad, dentro del mismo perímetro de seguridad

La/El RSI debe llevar un registro actualizado de los sitios protegidos, indicando:

a) Identificación del Edificio y Área.

b) Principales elementos a proteger.

c) Medidas de protección física

11.1.2 Control: Controles físicos de entrada

Las áreas protegidas se deben resguardar mediante el empleo de controles de acceso físico, determinados por la/el RSI junto con la/el Responsable del Área Informática, a fin de permitir el acceso sólo al personal autorizado. Estos controles de acceso físico deben tener, 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 permite 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 deben utilizar los siguientes controles de autenticación para autorizar y validar todos los accesos: listado de personas habilitadas y tarjeta inteligente o control biométrico. Se debe mantener un registro protegido para permitir auditar todos los accesos.

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

d) Revisar y actualizar cada seis (6) meses los derechos de acceso a las áreas protegidas, los que deben ser documentados y firmados por la/el Responsable de la Unidad Organizativa de la que dependa.

e) Revisar los registros de acceso a las áreas protegidas. Esta tarea la realiza la UAI o en su defecto quien sea propuesto por el CSI.

11.1.3 Control: Seguridad de oficinas, despachos, instalaciones

Para la selección y el diseño de un área protegida se debe tener 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 debe tomar en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad. Asimismo, se deben considerar las amenazas a la seguridad que representan los edificios y zonas aledañas, por ejemplo, filtración de agua desde otras instalaciones.

Las áreas protegidas del Ministerio son definidas por el Área de Gestión de Accesos con el asesoramiento de la/el RSI con base en la criticidad de los activos procesados en el lugar.

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 sean discretos y ofrezcan 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, lo que podría comprometer la información;

d) Establecer que las puertas y ventanas permanecerán cerradas cuando no haya vigilancia. Se debe agregar 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: cámaras, sensores de movimiento y cerrojos con tarjeta inteligente o control biométrico. Éstos deben ser instalados según estándares profesionales y probados periódicamente. Estos mecanismos de control comprenden todas las puertas exteriores y ventanas accesibles;

f) Separar las instalaciones de procesamiento de información administradas por el Ministerio de aquellas administradas por terceros/as. Esta separación podrá realizarse, dentro de las áreas protegidas, mediante el uso de racks con llave;

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 lugares seguros definidos oportunamente, a una distancia prudencial de las áreas protegidas del Ministerio. Los suministros tales como los útiles de escritorio no serán trasladados al área protegida hasta que sean requeridos;

i) Almacenar los equipos redundantes y la información de resguardo (backup) en un sitio seguro y distante del lugar de procesamiento, para evitar daños ocasionados ante eventuales contingencias en el sitio principal.

11.1.4 Control: Protección contra amenazas externas y de origen ambiental

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

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

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

a) Los materiales peligrosos o combustibles deben ser almacenados a una distancia segura del área asegurada. Los suministros a granel como papelería no deben almacenarse en el área asegurada;

b) El equipo de reemplazo y los medios de respaldo deben ubicarse a una distancia segura para evitar el daño de un desastre que afecte el local principal;

c) Se debe proporcionar equipo contra-incendios ubicado adecuadamente.

11.1.5 Control: Trabajo en áreas seguras

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/as sin supervisión.

c) Bloquear físicamente e inspeccionar periódicamente las áreas protegidas desocupadas.

d) Limitar el acceso al personal del servicio de soporte externo a las áreas protegidas o a las instalaciones de procesamiento de información sensible. Este acceso, como el de cualquier otra persona ajena que requiera acceder al área protegida, se otorga solamente cuando sea necesario y se encuentre autorizado y monitoreado. Se debe mantener 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 hayan sido formalmente autorizadas por la/el Responsable de dicha área o la/el Responsable del Área Informática y la/el RSI.

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

11.1.6 Control: Áreas de acceso público, de carga y descarga

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

Para ello se deben establecer controles físicos conforme a los siguientes lineamientos:

a) Limitar el acceso a las áreas de depósito, desde el exterior de la sede del Ministerio, 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.

f) Cuando fuese posible, el material entrante debe estar segregado o separado en las diferentes partes que lo constituyan.

11.2 Categoría: Seguridad de los equipos

Objetivo

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

Se debe proteger el equipo de amenazas físicas y ambientales.

11.2.1 Control: emplazamiento y protección de equipos

El equipamiento debe ser 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 los eventos que sean definidos oportunamente.

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

Revisar regularmente las condiciones ambientales para verificar que éstas no afecten de manera adversa el funcionamiento de las instalaciones de procesamiento de la información. En los centros de procesamiento de información, esta revisión se realizará mediante sensores que, ante alguna novedad, envíen automáticamente reportes. Para la revisión presencial, se seguirá el procedimiento que oportunamente se disponga a tal fin.

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

11.2.2 Control: Instalaciones de suministro

El equipamiento debe estar protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía debe estar de acuerdo con las especificaciones del fabricante o proveedora/or de cada equipo. Para asegurar la continuidad del suministro de energía, se deben contemplar las siguientes medidas de control:

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

b) Contar con un suministro de energía interrumpible (UPS) para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas del Ministerio. Las UPS cuentan con medios por los cuales pueden comunicar a los equipos la detección de una falla en el suministro de energía. Esto debe implementarse, para que ante un incidente cada equipo pueda decidir si procede a un apagado controlado o continúa operando. La determinación de dichas operaciones críticas es el resultado del análisis de impacto realizado por la/el RSI conjuntamente con las/los Propietarias/os de la Información con incumbencia. Los planes de contingencia deben contemplar las acciones que han de emprenderse ante una falla de la UPS. Los equipos de UPS deben ser inspeccionados y probados periódicamente para asegurar que funcionan correctamente y que tienen la autonomía requerida;

c) Montar un generador de respaldo para los casos en que el procesamiento deba continuar ante una falla prolongada en el suministro de energía. Debe realizarse un análisis de impacto de las posibles consecuencias ante una interrupción prolongada del procesamiento, con el objeto de definir qué componentes es necesario abastecer de energía alternativa. Dicho análisis debe ser realizado por la/el RSI conjuntamente con las/los Propietarias/os de la Información. Se debe disponer 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 debe asegurar que el tiempo de funcionamiento de la UPS permita su encendido manual. Los generadores deben ser inspeccionados y probados periódicamente para asegurar que funcionen según lo previsto.

Asimismo, se debe procurar 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 debe proveer de iluminación de emergencia en caso de producirse una falla en el suministro principal de energía.

Se debe implementar protección contra descargas eléctricas en todos los edificios y líneas de comunicaciones externas de acuerdo a las normativas vigentes.

Las opciones para lograr la continuidad de los suministros de energía incluyen múltiples alimentaciones para evitar fallas en el suministro de energía.

11.2.3 Control: Seguridad del cableado

El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información deben estar protegidos contra intercepción o daño, mediante las siguientes acciones:

a) Cumplir con los requisitos técnicos vigentes de la República Argentina;

b) Utilizar piso ducto o cableado embutido en la pared, siempre que sea posible, cuando corresponda a las instalaciones de procesamiento de información o alternativas que defina el área responsable;

c) Proteger el cableado de red contra intercepción no autorizada o daño mediante el uso de conductos o 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.

De ser posible, para los sistemas sensibles o críticos identificados por la DGTIyC en base al relevamiento realizado con los/las Propietarios/as de la Información o referentes de las unidades organizativas, se deben implementar los siguientes controles adicionales:

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;

11.2.4 Control: Mantenimiento de los equipos de procesamiento crítico

Se debe realizar 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 la/el proveedora/or y con la autorización formal del Responsables del Área Informática. El Área de Informática debe mantener un listado actualizado del equipamiento con el detalle de la frecuencia con la que se realiza 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 Ministerio para su mantenimiento;

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

11.2.5 Control: Seguridad de los equipos fuera de las instalaciones

El uso de equipamiento destinado al procesamiento de información, fuera del ámbito del Ministerio debe ser autorizado por la/el responsable patrimonial. En el caso de que en éste se almacene información clasificada, debe ser aprobado además por su Propietaria/o. La seguridad provista debe ser equivalente a la suministrada dentro del ámbito del Ministerio para un propósito similar, teniendo en cuenta los riesgos de trabajar fuera de éste.

Se deben respetar permanentemente las instrucciones del fabricante respecto del cuidado del equipamiento. Asimismo, se debe mantener una adecuada cobertura de seguro para proteger el equipamiento fuera del ámbito del Ministerio, cuando sea conveniente.

Los riesgos de seguridad, por ejemplo: daño, robo o intercepción; puede variar considerablemente entre los edificios y debe ser tomado en cuenta para evaluar los controles apropiados.

11.2.6 Control: Reutilización o retiro seguro de equipos

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

Los dispositivos que contengan información confidencial deben requerir una evaluación de riesgo para determinar si los ítems debieran ser físicamente destruidos en lugar de enviarlos a reparar o descartar.

11.2.7 Control: Retirada de materiales propiedad del Ministerio

El equipamiento, la información y el software no pueden ser retirados de la sede del Ministerio sin autorización formal.

Periódicamente se deben llevar a cabo comprobaciones puntuales para detectar el retiro no autorizado de activos del Ministerio, a cargo del Área Responsable del Patrimonio. El personal debe tener conocimiento de la posibilidad de realización de dichas comprobaciones.

Las/Los empleadas/os deben saber que se llevan a cabo chequeos inesperados, y los chequeos se deben realizar con la debida autorización de los requerimientos legales y reguladores.

11.2.8 Control: Políticas de Pantallas Limpias

Las/Los usuarias/os deben garantizar que los equipos desatendidos estén protegidos adecuadamente.

Los equipos instalados en áreas de usuarias/os, por ejemplo, estaciones de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos.

La/El RSI debe coordinar con el Área de Recursos Humanos las tareas de concientización a todas/os las/los usuarias/os y contratistas, acerca de los requerimientos y procedimientos de seguridad, para la protección de equipos desatendidos, así como de sus funciones en relación a la implementación de dicha protección.

Las/Los usuarias/os deben cumplir 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 pantalla 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.

11.2.9 Control: Políticas de Escritorios Limpios

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

Se deben aplicar 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 Ministerio (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. Éstas 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). Las/Los responsables de cada área deben mantener un registro de las contraseñas o copia de las llaves de seguridad utilizadas en el sector a su cargo. Tales elementos deben protegerse en sobre cerrado o caja de seguridad para impedir accesos no autorizados, debiendo dejarse constancia de todo acceso a éstas, 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. Verificar que las impresoras no guarden en memoria local documentos impresos, o aparejarlas para que los borren una vez impresos.

12. Cláusula: Seguridad en las Operaciones

Generalidades

La proliferación de software malicioso, como virus, troyanos, etc., hace necesario que se adopten medidas de prevención, a efectos de evitar la ocurrencia de tales amenazas.

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

Objetivo

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

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

Alcance

Todas las instalaciones de procesamiento de información del Ministerio.

Responsabilidad

La/El RSI tiene a su cargo, entre otros:

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

La/El Responsable del Área Informática tiene a su cargo lo siguiente:

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

La/El RSI junto con la/el Responsable del Área Informática y la/el Responsable del Área Jurídica del Ministerio deben evaluar los contratos y acuerdos con terceros/as para garantizar la incorporación de consideraciones relativas a la seguridad de la información involucrada en la gestión de los productos o servicios prestados.

Cada Propietaria/o de la Información, junto con la/RSI y la/el Responsable del Área Informática, debe determinar los requerimientos para resguardar la información por la cual es responsable. Asimismo, debe aprobar los servicios de mensajería autorizados para transportar la información cuando sea requerido, de acuerdo a su nivel de criticidad.

La UAI o en su defecto quien sea propuesto por el CSI, debe revisar las actividades que no hayan sido posibles segregar. Asimismo, debe revisar los registros de actividades del personal operativo.

12.1 Categoría: Procedimientos y Responsabilidades operativas

Objetivo

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

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

12.1.1 Control: Documentación de los Procedimientos operativos

Se deben documentar y mantener actualizados los procedimientos operativos identificados en esta política y sus cambios deben ser autorizados por la/el RSI.

Los procedimientos especifican 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.

Adicionalmente se debe preparar 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 finalización de la ejecución de los sistemas;

e) Programación y ejecución de procesos;

f) Gestión de servicios;

g) Resguardo de información;

h) Gestión de incidentes de seguridad en el ambiente de procesamiento y comunicaciones;

i) Remplazo o cambio de componentes del ambiente de procesamiento y comunicaciones.

12.1.2 Control: Cambios en las Operaciones

Se deben definir procedimientos para el control de los cambios en el ambiente operativo y de comunicaciones.

Todo cambio debe ser evaluado previamente en aspectos técnicos y de seguridad.

La/El RSI debe controlar que los cambios en los componentes operativos y de comunicaciones no afecten su

seguridad ni de la información que soportan. La/El Responsable del Área Informática debe evaluar el posible impacto operativo de los cambios previstos y verificar su correcta implementación.

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

Los procedimientos de control de cambios contemplan 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 éstos.

12.1.3 Control: Planificación de la Capacidad

La/El Responsable del Área Informática, o el personal que éste designe, debe efectuar el monitoreo de las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuados. Para ello, debe tomar en cuenta además los nuevos requerimientos de los sistemas, así como las tendencias actuales y proyectadas en el procesamiento de la información del Ministerio para el período estipulado de vida útil de cada componente. Asimismo, debe informar 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.

12.1.4 Control: Separación de entornos de desarrollo, pruebas y operacionales

Los ambientes de desarrollo, prueba y operaciones, siempre que sea posible, deben estar separados preferentemente en forma física, y se deben definir y documentar las reglas para la transferencia de software desde el estado de desarrollo hacia el estado productivo. Para ello, se deben tener en cuenta los siguientes controles:

a) Ejecutar el software de desarrollo y de producción 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 de producción, cuando no sean indispensables para su funcionamiento;

d) Utilizar sistemas de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas. Prohibir a las/los usuarias/os compartir contraseñas en estos sistemas. Las interfaces de los sistemas deben identificar claramente a qué instancia se está realizando la conexión;

e) Definir Propietarias/os de la Información para cada uno de los ambientes de procesamiento existentes;

f) El personal de desarrollo no debe tener acceso al ambiente productivo. De ser extrema dicha necesidad, se debe establecer un procedimiento de emergencia para la autorización, documentación y registro de dichos accesos.

12.2 Categoría: Protección contra el malware (código malicioso)

Objetivo

Proteger la integridad del software y la integración. Se requiere tomar precauciones para evitar y detectar la introducción de códigos maliciosos y códigos móviles no autorizados. El software y los medios de procesamiento de la información son vulnerables a la introducción de códigos maliciosos; como ser, entre otros, virus Troyanos, bombas lógicas, etc. Las/Los usuarias/os deben estar al tanto de los peligros de los códigos maliciosos. Cuando sea apropiado, las/los responsables deben introducir controles para evitar, detectar y eliminar los códigos maliciosos y controlar los códigos móviles.

12.2.1 Control: Control contra el malware (código malicioso)

La/El RSI debe definir controles de detección y prevención para la protección contra software malicioso. La/El Responsable del Área Informática, o el personal designado por éste, debe implementar dichos controles.

La/El RSI debe desarrollar procedimientos adecuados de concientización de usuarias/os en materia de seguridad, controles de acceso al sistema y administración de cambios. Estos controles deben considerar establecer políticas y procedimientos formales que contemplen las siguientes acciones:

a) Prohibir la instalación y uso de software no autorizado por el Ministerio (Ver 18.1.2 Control: Derechos de Propiedad Intelectual);

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 (ej.: dispositivos portátiles), señalando las medidas de protección a tomar;

c) Instalar y actualizar periódicamente software de detección y reparación de virus, examinando computadoras y medios informáticos, como medida precautoria y rutinaria;

d) Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles (probar dichas actualizaciones en un entorno de prueba previamente si es que constituyen cambios críticos a los sistemas);

e) Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos del Ministerio, 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 antivirus (rogues) y las cadenas falsas (hoax) y de cómo proceder frente a éstos;

i) Redactar normas de protección y habilitación de puertos de conexión de dispositivos móviles y sus derechos de acceso.

12.2.2 Control: Código Móvil

En caso de que el código móvil sea autorizado, se debe garantizar que la configuración asegure que el código móvil autorizado opere de acuerdo a una configuración de seguridad claramente definida, previniendo que el código móvil no autorizado sea ejecutado. Asimismo, se implementarán acciones para la protección contra acciones maliciosas resultantes de la ejecución no autorizada de código móvil, como ser:

a) Ejecución del código móvil en un ambiente lógicamente aislado;

b) Bloqueo del uso de código móvil;

c) Bloqueo de la recepción de código móvil;

d) Activación de medidas técnicas como sea disponible en un sistema específico para asegurar que el código móvil es gestionado;

e) Control de los recursos disponibles para el acceso del código móvil;

f) Implementación de controles criptográficos para autenticar de forma unívoca el código móvil.

12.3 Categoría: Resguardo (backup)

Objetivo

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

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

12.3.1 Control: Resguardo de la Información

La/El Responsable del Área Informática, la/el RSI y las/os Propietarias/os de la Información deben determinar los requerimientos para resguardar cada software o dato en función de su criticidad. En base a ello, se debe definir y documentar un esquema de resguardo de la información.

La/El Responsable del Área Informática debe disponer y controlar la realización de dichas copias, así como la prueba periódica de su restauración e integridad. Para esto se debe contar con instalaciones de resguardo que garanticen la disponibilidad de toda la información y del software crítico del Ministerio. Los sistemas de resguardo deben probarse periódicamente, asegurándose que cumplen con los requerimientos de los planes de continuidad de las actividades del organismo, según el punto (ver también Cláusula 17.1 Categoría: Gestión de Continuidad del Ministerio).

Se deben definir procedimientos para el resguardo de la información, que deben 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 remplazo de los medios de almacenamiento de las copias de resguardo, una vez concluida la posibilidad de ser reutilizados, de acuerdo a lo indicado por la/el proveedora/or, 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 éstas y los procedimientos documentados de restauración, a una distancia suficiente como para evitar daños provenientes de un desastre en el sitio principal. Se deben retener al menos tres (3) generaciones o ciclos de información de resguardo para la información y el software esenciales para el Ministerio. Para la definición de información mínima a ser resguardada en el sitio remoto, se debe tener en cuenta el nivel de clasificación otorgado a ésta, en términos de disponibilidad 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.

12.4 Categoría: Registro y Monitoreo

Objetivo

Detectar las actividades de procesamiento de información no autorizadas.

Se deben monitorear los sistemas y se deben reportar los eventos de seguridad de la información.

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

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

12.4.1 Control: Registro de eventos

Se deben producir y mantener registros de auditoría en los cuales se registren las actividades, excepciones, y eventos de seguridad de la información de las/los usuarias/os, por un período acordado para permitir la detección e investigación de incidentes.

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

a) Identificación de las/los usuarias/os;

b) Fechas, tiempos, y detalles de los eventos principales, por ejemplo, inicio y cierre de sesión;

c) Identidad del equipo o la ubicación si es posible;

d) Registros de intentos de acceso al sistema exitosos y fallidos;

e) Registros de intentos de acceso a los datos u otro recurso, exitosos y rechazados;

f) Cambios a la configuración del sistema;

g) Uso de privilegios;

h) Uso de utilitarios y aplicaciones de sistemas;

i) Archivos accedidos y el tipo de acceso;

j) Direcciones de redes y protocolos;

k) Alarmas que son ejecutadas por el sistema de control de accesos;

l) Activación y desactivación de los sistemas de protección, tales como sistemas antivirus y sistemas de detección de intrusos.

12.4.2 Control: Protección del registro de información

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

a) Alteraciones de los tipos de mensajes que son grabados;

b) Edición o eliminación de archivos de registro;

c) Exceso de la capacidad de almacenamiento de los archivos de registro, resultando en la falla para registrar los eventos o sobrescribiendo eventos registrados en el pasado.

12.4.3 Control: Registro del Administrador y del Operador

Se deben registrar y revisar periódicamente en particular las actividades de las/los administradoras/es y operadoras/es de sistema incluyendo:

a) Cuenta de administración u operación involucrada;

b) Momento en el cual ocurre un evento (éxito o falla);

c) Información acerca del evento (por ejemplo, los archivos manipulados) o las fallas (por ejemplo, los errores ocurridos y las acciones correctivas tomadas);

d) Procesos involucrados.

12.4.4 Control: Sincronización de Relojes

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

12.5 Categoría: Control de Software Operacional

Objetivo

Garantizar la seguridad de los archivos del sistema.

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

12.5.1 Control: Instalación de software en sistemas operacionales

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

- Toda aplicación desarrollada por el Ministerio o por un/a tercero/a debe tener una/un única/o Responsable designada/o formalmente por la/el Responsable del Área Informática.
- Ningún/na programador/a o analista de desarrollo y mantenimiento de aplicaciones puede acceder a los

ambientes de producción.

- La/El Responsable del Área Informática, propone para su aprobación por parte del superior jerárquico que corresponda, la asignación de la función de "implementador" al personal de su área que considere adecuado, quien tendrá como funciones principales:

  ◦ Coordinar la implementación de modificaciones o nuevos programas en el ambiente de Producción.

  ◦ Asegurar que los sistemas aplicativos en uso, en el ambiente de Producción, sean los autorizados y aprobados de acuerdo a las normas y procedimientos vigentes.

  ◦ Instalar las modificaciones, controlando previamente la recepción de la prueba aprobada por parte de la/el Analista Responsable, del sector encargado del testeo y de la usuaria/o final.

  ◦ Rechazar la implementación en caso de encontrar defectos y/o si faltara la documentación estándar establecida.

Otros controles a realizar son:

a) Guardar sólo los ejecutables en el ambiente de producción.

b) Llevar un registro de auditoría de las actualizaciones realizadas.

c) Retener las versiones previas del sistema, como medida de contingencia.

d) Definir un procedimiento que establezca los pasos a seguir para implementar las autorizaciones y conformidades pertinentes, las pruebas previas a realizarse, etc.

e) Denegar, cuando correspondiere, permisos de modificación al implementador sobre los programas fuentes bajo su custodia.

Evitar que la función de implementador sea ejercida por personal que pertenezca al sector de desarrollo o mantenimiento.

12.6 Categoría: Administración de vulnerabilidades técnicas

Objetivo

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

12.6.1 Control: Administración de vulnerabilidades técnicas

Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición del Ministerio a tales vulnerabilidades y se tomarán las medidas necesarias para tratar los riesgos asociados.

Para ello se debe contar con un inventario de software donde se detalle información de versiones de éste, así como datos de la proveedora/or y responsable interno.

El proceso de gestión de las vulnerabilidades técnicas debe comprender:

a) Definición de roles y responsabilidades asociados con la gestión de vulnerabilidades técnicas;

b) Procedimientos de identificación de vulnerabilidades técnicas potenciales;

c) Definición de una línea de tiempo para reaccionar ante las notificaciones de las vulnerabilidades técnicas potencialmente relevantes;

d) Definición de prioridades para la atención de necesidades relacionadas con actualizaciones de seguridad;

e) Identificación de los riesgos asociados y las acciones a llevar a cabo ante vulnerabilidades identificadas;

f) Identificación de los riesgos asociados a la instalación de parches;

g) Aprobación y evaluación de los parches antes de que sean instalados para garantizar que son efectivos y que no resultan en efectos secundarios que no puedan ser tolerados;

h) Consideración de controles alternativos en caso de inexistencia de parches;

i) Generación y mantenimiento de un registro de auditoría para todos los procedimientos emprendidos;

j) Seguimiento y evaluación regular del proceso de gestión de las vulnerabilidades técnicas para garantizar su efectividad y eficiencia;

12.6.2 Control: Restricciones en la instalación de software

Se deben establecer e implementar:

- Las reglas que rigen la instalación de software por parte de las/los usuarias/os y poner en vigencia una política estricta sobre qué tipo de software pueden instalar las/los usuarias/os.

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

12.7 Categoría: Consideraciones sobre la auditoría de los sistemas de información

Objetivo

Minimizar el impacto de las actividades de auditoría en los sistemas operacionales.

12.7.1 Control: Controles de auditoría de los sistemas de información

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

Se deben contemplar los siguientes puntos:

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

b) Controlar el alcance de las verificaciones. Esta función es realizada por la/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: i) Eliminar archivos transitorios. ii) Eliminar entidades ficticias y datos incorporados en archivos maestros. iii) Revertir transacciones. iv) 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 UAI o en su defecto quien sea propuesto por el CSI debe completar el formulario que oportunamente la UAI envíe a las áreas involucradas.

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: i) Fecha y hora. ii) Puesto de trabajo. iii) Usuario. iv) Tipo de acceso. v) Identificación de los datos accedidos. vi) Estado previo y posterior. vii) Programa y/o función utilizada.

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

13. Cláusula: Gestión de Comunicaciones

Generalidades

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

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

Objetivo

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

comunicaciones.

Alcance

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

Responsabilidad

La/El RSI tiene a su cargo, entre otros:

- Definir y documentar una norma clara con respecto al uso del correo electrónico;
- Controlar los mecanismos de distribución y difusión de información dentro del Ministerio;
- Desarrollar procedimientos adecuados de concientización de usuarias/os en materia de seguridad, controles de acceso al sistema y administración de cambios;
- Verificar el cumplimiento de las normas, procedimientos y controles establecidos.

La/El Responsable del Área Informática tiene a su cargo lo siguiente:

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

La/El RSI junto con la/el Responsable del Área Informática y la/el Responsable del Área Jurídica del Ministerio deben evaluar los contratos y acuerdos con terceros/as para garantizar la incorporación de consideraciones relativas a la seguridad de la información involucrada en la gestión de los productos o servicios prestados.

Cada Propietaria/o de la Información, junto con la/el RSI y la/el Responsable del Área Informática, debe determinar los requerimientos para resguardar la información por la cual es responsable. Asimismo, debe aprobar los servicios de mensajería autorizados para transportar la información cuando sea requerido, de acuerdo a su nivel de criticidad.

La UAI o en su defecto quien sea propuesto por el CSI, debe revisar las actividades que no hayan sido posibles segregar e informarlas oportunamente al resto de las áreas. Asimismo debe revisar los registros de actividades del personal operativo.

13.1 Categoría: Gestión de la Red

Objetivo

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

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

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

13.1.1 Control: Redes

La/El RSI debe definir controles para garantizar la seguridad de los datos y los servicios conectados en las redes del Ministerio 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 la/el responsable establecido en el punto “6.1.3 Control: Asignación de responsabilidad de la 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.

La/El Responsable del Área Informática debe implementar dichos controles.

13.1.2 Control: Seguridad de Servicio de red

La/El RSI junto con la/el Responsable del Área Informática deben definir las pautas para garantizar la seguridad de los servicios de red del Ministerio, tanto públicos como privados.

Para ello se deben tener 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 la/el RSI.

13.2 Categoría: Transferencia de información

Objetivo

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

Los intercambios de información dentro de las organizaciones se deben basar en una política formal de intercambio, seguida en línea con los acuerdos de intercambio, y debe cumplir con cualquier legislación relevante (ver Cláusula 18: Cumplimiento).

Se deben establecer los procedimientos y estándares para proteger la información y los medios físicos que contiene la información en tránsito.

13.2.1 Control: Procedimientos y controles de intercambio de la información

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

a) Protección de la información intercambiada de la intercepción, copiado, modificación, de que sea mal dirigida, y de su destrucción;

b) Detección y protección contra el código malicioso que puede ser transmitido a través del uso de comunicaciones electrónicas;

c) Definición del uso aceptable de las instalaciones de comunicación electrónicas;

d) Uso seguro de comunicaciones inalámbricas;

e) Responsabilidades de la/el empleada/o, contratista y cualquier otra/o usuaria/o de no comprometer a la organización, por ejemplo, a través de la difamación, hostigamiento, personificación, reenvío de cadenas de comunicación epistolar, compras no autorizadas y cualquier otro medio (ej.: redes sociales);

f) Uso de técnicas criptográficas para proteger la confidencialidad, integridad y la autenticidad de la información;

g) Directrices de retención y eliminación para toda la correspondencia en concordancia con las leyes y regulaciones relevantes, locales y nacionales;

h) Instrucción del personal sobre las precauciones que deben tomar a la hora de transmitir información del Ministerio.

13.2.2 Control: Acuerdos de Intercambio de Información

Cuando se realicen acuerdos entre organizaciones para el intercambio de información y software, se debe especificar el grado de sensibilidad de la información del Ministerio involucrada y las consideraciones de seguridad sobre ésta. Se deben tener 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, exposición o divulgación no autorizada 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.).

13.2.3 Control: Seguridad de la Mensajería

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

Se deben considerar las siguientes medidas de seguridad en los mensajes electrónicos:

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

13.2.4 Control: Acuerdos de confidencialidad.

Se deben definir, implementar y revisar regularmente los acuerdos de confidencialidad o de no divulgación para la protección de la información del Ministerio. Dichos acuerdos deben responder a los requerimientos de confidencialidad o no divulgación del Ministerio, los cuales deben ser revisados periódicamente. Asimismo, deben cumplir con toda legislación o normativa que alcance al Ministerio en materia de confidencialidad de la información.

Dichos acuerdos deben celebrarse tanto con el personal del Ministerio como con aquellos/as terceros/as que se relacionen de alguna manera con su información.

14. Cláusula: Adquisición, desarrollo y mantenimiento de sistemas

Generalidades

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

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

Dado que los analistas y programadores tienen el conocimiento total de la lógica de los procesos en los sistemas, se deben implementar controles que eviten maniobras dolosas por parte de estas personas u otras que puedan operar sobre los sistemas, bases de datos y plataformas de software de base (por ejemplo, operadores que puedan manipular los datos y/o atacantes que puedan comprometer/alterar la integridad de las bases de datos) y en el caso de que se lleven a cabo, identificar rápidamente a la/el responsable.

Asimismo, es necesaria una adecuada administración de la infraestructura de base, Sistemas Operativos y Software de Base, en las distintas plataformas, para asegurar una correcta implementación de la seguridad, ya que en general los aplicativos se asientan sobre este tipo de software.

Objetivo

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

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

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

Alcance

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

Responsabilidad

La/El RSI junto con la/el Propietaria/o de la Información y la UAI deben definir los controles a ser implementados en los sistemas desarrollados internamente o por terceros/as, en función de una evaluación previa de riesgos.

La/El RSI, junto con la/el Propietaria/o de la Información debe definir en función a la criticidad de la información, los requerimientos de protección mediante métodos criptográficos. Luego, la/el RSI debe definir junto con la/el Responsable del Área de Sistemas los métodos de cifrado a ser utilizados.

Asimismo, la/el RSI cumple las siguientes funciones:

- Definir los procedimientos de administración de claves;
- Verificar el cumplimiento de los controles establecidos para el desarrollo y mantenimiento de sistemas;
- Garantizar el cumplimiento de los requerimientos de seguridad para el software;
- Definir procedimientos para: el control de cambios a los sistemas; la verificación de la seguridad de las plataformas y bases de datos que soportan e interactúan con los sistemas; el control de código malicioso y la definición de las funciones del personal involucrado en el proceso de entrada de datos.

La/el Responsable del Área Informática, debe proponer para su aprobación por parte del superior jerárquico que corresponda, la asignación de funciones de "implementadora/or" y "administradora/or de programas fuentes" al personal de su área que considere adecuado, cuyas responsabilidades se detallan en la presente cláusula. Asimismo, debe verificar el cumplimiento de las definiciones establecidas sobre los controles y las medidas de seguridad a ser incorporadas a los sistemas.

El Área de Sistemas debe proponer quiénes realizan la administración de las técnicas criptográficas y claves.

La/El Responsable del Área de Administración debe incorporar aspectos relacionados con el licenciamiento, la calidad del software y la seguridad de la información en los contratos con terceros/as por el desarrollo de software. La/El Responsable del Área Jurídica debe participar en dicha tarea.

14.1 Categoría: Requerimientos de Seguridad de los Sistemas

Objetivo

Garantizar que la seguridad sea una parte integral de los sistemas de información.

Los sistemas de información incluyen sistemas de operación, infraestructura, aplicaciones operativas, productos de venta masiva, servicios y aplicaciones desarrolladas por la/el usuaria/o. El diseño e implementación del sistema de información que soporta el proceso operativo puede ser crucial para la seguridad. Se deben identificar y acordar los requerimientos de seguridad antes del desarrollo y/o implementación de los sistemas de información.

14.1.1 Control: Análisis y Especificaciones de los Requerimientos de seguridad

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

Los requerimientos para nuevos sistemas o mejoras a los existentes deben especificar la necesidad de controles. Estas

especificaciones deben considerar los controles automáticos a incorporar al sistema, como así también controles manuales de apoyo.

Se deben tener en cuenta las siguientes consideraciones:

a) Definir un procedimiento para que durante las etapas de análisis y diseño del sistema se incorporen a los requerimientos los correspondientes controles de seguridad. Este procedimiento debe incluir una etapa de evaluación de riesgos previa al diseño, para definir los requerimientos de seguridad e identificar los controles apropiados. En esta tarea deben participar las áreas usuarias, de sistemas, de seguridad informática y auditoría, especificando y aprobando los controles automáticos a incorporar al sistema y las necesidades de controles manuales complementarios.
Las áreas involucradas pueden solicitar certificaciones y evaluaciones independientes para los productos a utilizar.

b) Evaluar los requerimientos de seguridad y los controles requeridos, teniendo en cuenta que éstos deben ser proporcionales en costo y esfuerzo al valor del bien que se quiere proteger y al daño potencial que pudiera ocasionar a las actividades realizadas;

c) Considerar que los controles introducidos en la etapa de diseño, son significativamente menos costosos de implementar y mantener que aquellos incluidos durante o después de la implementación.

14.1.2 Control: Seguridad de servicios aplicativos en redes públicas

Se deben controlar los mecanismos de distribución y difusión tales como documentos, computadoras, dispositivos de computación móvil, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general (analógica o digital), multimedia, servicios o instalaciones postales, equipos de fax, etc.

Al interconectar dichos medios, se deben considerar las implicancias en lo que respecta a la seguridad y a las actividades propias del Ministerio, 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 Ministerio, 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 Ministerio, como la comunicación de órdenes o autorizaciones;

f) Categorías de personal y contratistas o terceros/as a los que se permite el uso del sistema y las ubicaciones desde las cuales se puede acceder a éste;

g) Restricción de acceso a determinadas instalaciones a específicas categorías de usuarias/os;

h) Identificación de la posición o categoría de las/los usuarias/os, por ejemplo, empleadas/os del Ministerio o contratistas, en directorios accesibles por otras/os usuarias/os;

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.

14.1.3 Control: Protección de servicios de aplicativos

Se deben tomar 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 Ministerio 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 ciertas normas de la jurisdicción en la cual se localiza el sistema o en la cual tiene lugar la transacción electrónica. Se debe implementar un proceso de autorización formal antes de que la información se ponga a disposición del público, estableciéndose en todos los casos los/las encargados/as de dicha aprobación.

Todos los sistemas de acceso público deben prever que:

a) La información se obtenga, procese y proporcione de acuerdo a la normativa vigente, en especial la Ley de Protección de Datos Personales;

b) La información que se ingresa al sistema de publicación, o aquella que éste procesa, sea procesada en forma completa, exacta y oportuna;

c) La información sensible o confidencial 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 éste se conecta;

e) La/El responsable de la publicación de información en sistemas de acceso público sea claramente identificado;

f) La información se publique teniendo en cuenta las normas establecidas al respecto;

g) Se garantice la validez y vigencia de la información publicada.

14.2 Categoría: Seguridad en los Sistemas de Aplicación

Objetivo

Para evitar la pérdida, modificación o uso inadecuado de los datos pertenecientes a los sistemas de información, se deben establecer controles y registros de auditoría, verificando:

a) La validación efectiva de datos de entrada;

b) El procesamiento interno;

c) La autenticación de mensajes (interfaces entre sistemas);

d) La validación de datos de salida.

14.2.1 Control: Validación de Datos de Entrada

Se debe definir 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 debe considerar los siguientes controles:

a) Control de secuencia;

b) Control de monto límite por operación y tipo de usuaria/o;

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 deben llevar a cabo las siguientes acciones:

a) Definir un procedimiento para realizar revisiones periódicas de contenidos de campos claves o archivos de datos, definiendo quién lo realiza, en qué forma, con qué método, quiénes deben ser informados del resultado, etc.;

b) Definir un procedimiento que explicite las alternativas a seguir para responder a errores de validación en un aplicativo;

c) Definir un procedimiento que permita determinar las responsabilidades de todo el personal involucrado en el proceso de entrada de datos.

14.2.2 Control: Controles de Procesamiento Interno

Se debe definir 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 deben implementar:

a) Procedimientos que permitan identificar el uso y localización en los aplicativos de funciones de incorporación y eliminación que realizan cambios en los datos;

b) Procedimientos que establezcan los controles y verificaciones necesarios para prevenir la ejecución de programas fuera de secuencia o cuando falle el procesamiento previo;

c) Procedimientos que establezcan la revisión periódica de los registros de auditoría o alertas de forma de detectar cualquier anomalía en la ejecución de las transacciones;

d) Procedimientos que realicen la validación de los datos generados por el sistema;

e) Procedimientos que verifiquen la integridad de los datos y del software cargado o descargado entre computadoras;

f) Procedimientos que controlen la integridad de registros y archivos;

g) Procedimientos que verifiquen la ejecución de los aplicativos en el momento adecuado;

h) Procedimientos que aseguren el orden correcto de ejecución de los aplicativos, la finalización programada en caso de falla, y la detención de las actividades de procesamiento hasta que el problema sea resuelto.

14.2.3 Control: Autenticación de Mensajes

Cuando una aplicación tenga previsto el envío de mensajes que contengan información clasificada, se deben implementar los controles criptográficos determinados en el punto 10.1.1 Control: Política de Utilización de Controles Criptográficos.

14.2.4 Control: Validación de Datos de Salidas

Se deben establecer procedimientos para validar la salida de los datos de las aplicaciones, incluyendo:

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

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

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

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

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

14.3 Categoría: Seguridad de los Archivos del Sistema

Objetivo

Se debe garantizar que los desarrollos y actividades de soporte a los sistemas se lleven a cabo de manera segura, controlando el acceso a sus archivos.

14.3.1 Control: 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 por el Ministerio o por un/a tercero/a tiene una/un única/o Responsable designada/o formalmente por la/el Responsable del Área Informática;
- Ningún programador o analista de desarrollo y mantenimiento de aplicaciones puede acceder a los ambientes de producción;
- La/El Responsable del Área Informática debe proponer para su aprobación por parte del superior jerárquico que corresponda la asignación de la función de "implementador" al personal de su área que considere adecuado, quien tiene como funciones principales:
    - Coordinar la implementación de modificaciones o nuevos programas en el ambiente de Producción;
    - Asegurar que los sistemas aplicativos en uso, en el ambiente de Producción, sean los autorizados y

aprobados de acuerdo a las normas y procedimientos vigentes;

- Instalar las modificaciones, controlando previamente la recepción de la prueba aprobada por parte de la/el Analista Responsable, del sector encargado del testeo y de la usuaria/o final;
- 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 a la/el implementadora/or sobre los programas fuentes bajo su custodia;

f) Evitar que la función de implementador/a sea ejercida por personal que pertenezca al sector de desarrollo o mantenimiento.

14.3.2 Control: Protección de los Datos de Prueba del Sistema

Las pruebas de los sistemas se deben efectuar sobre datos extraídos del ambiente operativo.

Para proteger los datos de prueba se deben establecer normas y procedimientos que contemplen lo siguiente:

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. Solicitar autorización formal para realizar una copia de la base operativa como base de prueba, llevando registro de tal autorización.

Eliminar inmediatamente, una vez completadas las pruebas, la información operativa utilizada.

14.3.3 Control: Cambios a Datos Operativos

La modificación, actualización o eliminación de los datos operativos deben realizarse a través de los sistemas que procesan dichos datos y de acuerdo al esquema de control de accesos implementado en éstos. Una modificación 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 deben considerar como excepciones. La/El RSI debe definir procedimientos para la gestión de dichas excepciones contemplando lo siguiente:

a) Se debe generar una solicitud formal para la realización de la modificación, actualización o eliminación del dato;

b) La/El Propietaria/o de la Información afectada y la/el RSI deben aprobar la ejecución del cambio evaluando las razones por las cuales se solicita;

c) Se deben generar cuentas de usuarias/os de emergencia para ser utilizadas en la ejecución de excepciones. Éstas deben estar protegidas mediante contraseñas, sujetas al procedimiento de administración de contraseñas críticas y habilitadas sólo ante un requerimiento de emergencia y por el lapso que ésta dure;

d) Se debe designar un/a encargado/a de implementar los cambios, el/la cual no puede ser personal del área de Desarrollo. En el caso de que esta función no pueda ser segregada se deben aplicar controles adicionales de acuerdo a lo establecido en la Cláusula 7: Recursos Humanos;

e) Se deben registrar todas las actividades realizadas con las cuentas de emergencia. Dicho registro debe ser revisado posteriormente por la/el RSI.

14.3.4 Control: Acceso a las Bibliotecas de programas fuentes

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

a) La/El Responsable del Área Informática debe proponer para su aprobación por parte del superior jerárquico que corresponda la función de “administradora/or de programas fuentes” al personal de su área que considere

adecuado, quien tendrá en custodia los programas fuentes y debe:

i. Proveer al Área de Desarrollo los programas fuentes solicitados para su modificación, manteniendo en todo momento la correlación programa fuente/ejecutable;

ii. Llevar un registro actualizado de todos los programas fuentes en uso, indicando nombre del programa, programador/a, Analista Responsable que autorizó, versión, fecha de última modificación y fecha/hora de compilación y estado (en modificación, en producción);

iii. Verificar que el/la 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;

iv. Administrar las distintas versiones de una aplicación;

v. Asegurar que un mismo programa fuente no sea modificado simultáneamente por más de un/a desarrollador/a.

b) Denegar a la/el "administradora/or de programas fuentes" permisos de modificación sobre los programas fuentes bajo su custodia;

c) Establecer que todo programa objeto o ejecutable en producción tenga un único programa fuente asociado que garantice su origen;

d) Establecer que el/la implementador/a de producción debe efectuar la generación del programa objeto o ejecutable que estará en producción (compilación), a fin de garantizar tal correspondencia;

e) Desarrollar un procedimiento que garantice que toda vez que se migre a producción el módulo fuente, se cree el código ejecutable correspondiente en forma automática;

f) Evitar que la función de "administradora/or de programas fuentes" sea ejercida por personal que pertenezca al Sector de Desarrollo y/o Mantenimiento;

g) Prohibir la guarda de programas fuentes históricos (que no sean los correspondientes a los programas operativos) en el ambiente de producción;

h) Prohibir el acceso a todo/a operador/a y/o usuaria/o 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 Ministerio en los procedimientos que surgen de la presente política.

14.4 Categoría: Seguridad de los Procesos de Desarrollo y Soporte

Objetivo

Esta política provee seguridad al software y a la información del sistema de aplicación, por lo tanto, se deben controlar los entornos y el soporte dado a éstos.

14.4.1 Control: Procedimiento de Control de Cambios

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

Para ello se debe establecer un procedimiento que incluya las siguientes consideraciones:

a) Verificar que los cambios sean propuestos por usuarias/os autorizadas/os y respete los términos y condiciones que surjan de la licencia de uso;

b) Mantener un registro de los niveles de autorización acordados;

c) Solicitar la autorización de la/el Propietaria/o de la Información, en caso de tratarse de cambios a sistemas de procesamiento de ésta;

d) Efectuar un análisis de riesgos del cambio;

e) Determinar los requisitos de seguridad para el cambio;

f) Analizar el impacto de los cambios sobre los controles de seguridad existentes;

g) Obtener aprobación formal por parte de la/el Responsable del Área Informática para las tareas detalladas, antes que comiencen las tareas;

h) Solicitar la revisión de la/el RSI para garantizar que no se violen los requerimientos de seguridad que debe cumplir el software;

i) Efectuar las actividades relativas al cambio en el ambiente de desarrollo;

j) Obtener la aprobación por parte de la/el usuaria/o autorizada/o y del área de pruebas mediante pruebas en el ambiente correspondiente;

k) Actualizar la documentación para cada cambio implementado, tanto de los manuales de usuarias/os como de la documentación operativa;

l) Mantener un control de versiones para todas las actualizaciones de software;

m) Garantizar que la implementación se llevará a cabo minimizando la discontinuidad de las actividades y sin alterar los procesos involucrados;

n) Informar a las áreas usuarias antes de la implementación de un cambio que pueda afectar su operatoria;

o) Garantizar que sea el/la implementador/a quien efectúe el pasaje de los objetos modificados al ambiente operativo, de acuerdo a lo establecido en "14.3.1 Control: Software Operativo".

Oportunamente se presentará un esquema modelo de segregación de ambientes de procesamiento.

14.4.2 Control: Revisión Técnica de los Cambios en el Sistema Operativo

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

Para ello, se debe definir un procedimiento que incluya:

a) Revisar los procedimientos de integridad y control de aplicaciones para garantizar que no hayan sido comprometidas por el cambio;

b) Garantizar que los cambios en el Sistema Operativo sean informados con anterioridad a la implementación;

c) Asegurar la actualización del Plan de Continuidad de las Actividades del Ministerio.

14.4.3 Control: Restricción del Cambio de Paquetes de Software

En caso de considerarlo necesario la modificación de paquetes de software suministrados por proveedoras/es, y previa autorización del Responsable del Área Informática, se debe:

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

b) Determinar la conveniencia de que la modificación sea efectuada por el Ministerio, por la/el proveedora/or o por una tercera/o;

c) Evaluar el impacto que se produciría si el Ministerio 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.

14.4.4 Control: 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 la/el usuaria/o.

En este sentido, se deben redactar normas y procedimientos que incluyan:

a) Adquirir programas a proveedoras/es acreditados o productos ya evaluados;

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

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

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

e) Ejecutar controles y pruebas de evaluación de seguridad periódicamente en

producción.

14.4.5 Control: Desarrollo Externo de Software

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

a) Acuerdos de licencias, propiedad de código y derechos conferidos (Ver 18.1.2 Derechos de Propiedad Intelectual);

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

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

d) Verificación del cumplimiento de las condiciones de seguridad;

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

14.5 Categoría: Gestión de vulnerabilidades técnicas

Objetivo

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

14.5.1 Control: Vulnerabilidades técnicas

Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición del Ministerio a tales vulnerabilidades y tomar las medidas necesarias para tratar los riesgos asociados.

Para ello se debe contar con un inventario de software donde se detalle información de sus versiones, así como datos de la/el proveedora/or y responsable interna/o.

El proceso de gestión de las vulnerabilidades técnicas debe comprender:

a) Definición de roles y responsabilidades asociados con la gestión de vulnerabilidades técnicas;

b) Procedimientos de identificación de vulnerabilidades técnicas potenciales;

c) Definición de una línea de tiempo para reaccionar ante las notificaciones de las vulnerabilidades técnicas potencialmente relevantes;

d) Definición de prioridades para la atención de necesidades relacionadas con actualizaciones de seguridad;

e) Identificación de los riesgos asociados y las acciones a llevar a cabo ante vulnerabilidades identificadas;

f) Identificación de los riesgos asociados a la instalación de parches;

g) Aprobación y evaluación de los parches antes de que sean instalados para garantizar que son efectivos y que no resultan en efectos secundarios que no puedan ser tolerados;

h) Consideración de controles alternativos en caso de inexistencia de parches;

i) Generación y mantenimiento de un registro de auditoría para todos los procedimientos emprendidos;

j) Seguimiento y evaluación regular del proceso de gestión de las vulnerabilidades técnicas para garantizar su efectividad y eficiencia.

Información Complementaria

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 una/un proveedora/or 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 instalen 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 (3) ambientes que debe ser adaptado a las características propias de cada Ministerio, teniendo en cuenta las capacidades instaladas, los recursos y el equipamiento existente.

Ambiente de Desarrollo

Es donde se desarrollan los programas fuentes y donde se almacena toda la información relacionada con el análisis y diseño de los sistemas. El/La analista o programador/a (desarrollador) tiene total dominio sobre el ambiente. Puede recibir alguna fuente para modificar, quedando registrado en el sistema de control de versiones que administra la/el "administradora/or de programas fuentes".

El/La desarrollador/a 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 a la/el implementadora/or de ese ambiente.

Ambiente de Pruebas

El/La implementador/a de este ambiente recibe el programa y la documentación respectiva y realiza una prueba general con un lote de datos para tal efecto, junto con la/el usuaria/o 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 correctos de acuerdo a las especificaciones y considera que la documentación presentada es completa, entonces remite el programa fuente a la/el implementador/a de producción por medio del sistema de control de versiones y le entrega las instrucciones. Caso contrario, vuelve atrás el ciclo devolviendo el programa a la/el desarrolladora/or, 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 la/el "administradora/or de programas fuentes" y donde se dejan los datos de la/el programadora/or que hizo la modificación, fecha, hora y tamaño de los programas fuentes y objetos o ejecutables.

El/La "implementador/a" 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.

Deben aplicarse procedimientos de la misma naturaleza y alcance para las modificaciones de cualquier otro elemento que forme parte del sistema, por ejemplo: modelo de datos de la base de datos o cambios en los parámetros, etc. Las modificaciones realizadas al software de base (Sistemas Operativos, Motores de bases de datos, Productos middleware) deben cumplir idénticos pasos, sólo que las implementaciones las realizan los/las propias/os administradoras/es.

Cabe aclarar que tanto el personal de desarrollo como la/el proveedora/or 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.

15. Cláusula: Relaciones con Proveedores

Generalidades

Las/Los proveedoras/es del Ministerio deben ser gestionadas/os en lo que respecta a los aspectos de seguridad que tienen que ver con el establecimiento y el acuerdo de todos los requisitos de seguridad de la información del Ministerio.

Objetivo

Establecer y mantener el nivel acordado de seguridad de información y prestación de servicios conforme a los acuerdos de la/el proveedora/or.

Alcance

Los dos (2) grandes puntos del alcance son:

- Asegurar la protección de la información del Ministerio que es accedida por las/los proveedoras/es, cumpliendo con el nivel de seguridad establecido.
- El mantenimiento del nivel acordado de seguridad de información y prestación de servicios conforme a los acuerdos de la/el proveedora/or.

Responsabilidad

La/El RSI, junto con la/el Propietaria/o de la Información, deben definir en función a la criticidad de la información, los requerimientos de protección en lo referente al acceso de la información de las/los proveedoras/es durante todo su ciclo de vida con el Ministerio.

Asimismo, todo responsable de las áreas legales, compras o que gestionen los contratos con proveedoras/es, debe garantizar que en éstos se definan y se acuerden los niveles de seguridad establecidos por el Ministerio.

15.1 Categoría: Seguridad de la información en las relaciones con la/el proveedora/or

Objetivo

Garantizar y asegurar la protección de la información del Ministerio que es accedida por las/los proveedoras/es, cumpliendo con el nivel de seguridad establecido.

15.1.1 Control: Política de seguridad de la información para las relaciones con proveedoras/es

Se deben acordar los requisitos de seguridad de la información para mitigar los riesgos asociados al acceso de las/los proveedoras/es a los activos del Ministerio con la/el proveedora/or y se deben documentar debidamente.

El Ministerio debe identificar e imponer controles de seguridad de la información para abordar específicamente el acceso de las/los proveedoras/es a la información del Ministerio en una política.

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

a) La identificación y la documentación de los tipos de proveedoras/es, es decir, los servicios de Tecnologías de Información (TI), las utilidades de logística, los servicios financieros, los componentes de la infraestructura de Tecnologías de Información (TI) y a quiénes autoriza el Ministerio para acceder a su información;

b) Un proceso y ciclo de vida estandarizado para administrar las relaciones con las/los proveedoras/es;

c) La definición de los tipos de acceso a la información que se les permite a los distintos tipos de proveedoras/es y el monitoreo y control del acceso;

d) Requisitos mínimos de seguridad de la información para cada tipo de información y tipo de acceso para servir de base para los acuerdos individuales con las/los proveedoras/es en base a las necesidades del Ministerio y los requisitos y su perfil de riesgo;

e) Procesos y procedimientos para monitorear la adherencia a los requisitos de seguridad de información establecidos para cada tipo de proveedora/or y tipo de acceso, incluida la revisión de terceros/as y la validación de productos;

f) Controles de precisión y nivel de detalles para garantizar la integridad de la información o el procesamiento de información que entrega cualquiera de las partes;

g) Tipos de obligaciones aplicables a las/los proveedoras/es para proteger la información;

h) Manejo de incidentes y contingencias asociadas con el acceso a las/los proveedoras/es, incluidas las responsabilidades del Ministerio y las/los proveedoras/es;

i) Resiliencia y, en caso de ser necesario, disposiciones de recuperación y contingencia para garantizar la disponibilidad de la información o el procesamiento de información proporcionado por cualquiera de las partes;

j) Capacitación de concientización para el personal del Ministerio involucrado en las adquisiciones sobre políticas, procesos y procedimientos correspondientes;

k) Capacitación de concientización para el personal del Ministerio que interactúa con el personal de las/los proveedoras/es en cuanto a las reglas adecuadas sobre el compromiso y el comportamiento en base al tipo de proveedora/or y el nivel de acceso de la/el proveedora/or a los sistemas y la información del Ministerio;

l) Las condiciones sobre los controles y requisitos de seguridad de la información se documentarán en un acuerdo firmado por ambas partes;

m) Administración de las transiciones necesarias de información, instalaciones de procesamiento de información y cualquier otra cosa que se deba mover y, garantizando que se mantiene la seguridad de la información a través de todo el período de transición.

15.1.2 Control: Abordar la seguridad dentro de los acuerdos de la/el proveedora/or

Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedora/or que puede acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de Tecnologías de Información (TI) para la información del Ministerio.

Se deben establecer y documentar acuerdos con las/los proveedoras/es para garantizar que no existen malos entendidos entre el Ministerio y la/el proveedora/or en cuanto a las obligaciones de ambas partes para cumplir con los requisitos de seguridad de la información pertinentes.

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

a) Descripción de la información que se debe proporcionar o a la que se debe acceder y los métodos para proporcionar o acceder a la información;

b) Clasificación de la información de acuerdo al esquema de clasificación del Ministerio; y si es necesario también realizar el mapeo entre el esquema propio del Organismo y el esquema de clasificación de la/el proveedora/or;

c) Requisitos legales y normativos, incluida la protección de datos personales, los derechos de propiedad intelectual y una descripción de sobre cómo se garantizará que se cumplen;

d) Obligación de cada parte contractual de implementar un conjunto de controles acordados incluido el control de acceso, la revisión de desempeño, el monitoreo, los informes y la auditoría;

e) Reglas de uso aceptable de la información, incluido el uso inaceptable en caso de ser necesario;

f) Una lista explícita del personal autorizado para acceder o recibir la información o los procedimientos o condiciones del Ministerio para su autorización y el retiro de la autorización, para el acceso a o la recepción de la información del Ministerio al personal de la/el proveedora/or;

g) Políticas de seguridad de la información pertinentes al contrato específico;

h) Requisitos y procedimientos de la administración de incidentes (en especial la notificación y la colaboración durante la remediación de incidentes);

i) Requisitos de capacitación y concientización para procedimientos específicos y requisitos de seguridad de la información, es decir, para la respuesta ante incidentes y procedimientos de autorización;

j) Normativas pertinentes para la subcontratación, incluidos los controles que se deben implementar;

k) Socios de acuerdos pertinentes, incluida una persona de contacto para los asuntos de seguridad de la información;

l) Requisitos de selección, si existe alguno, para el personal de la/el proveedora/or para realizar los procedimientos de selección y notificación si no se ha completado la selección o si los resultados dan pie a dudas o inquietudes;

m) Derecho a auditar los procesos y los controles de la/el proveedora/or relacionados al acuerdo;

n) Procesos de resolución de defectos y resolución de conflictos;

o) Obligación de la/el proveedora/or a entregar periódicamente un informe independiente sobre la efectividad de

los controles y un acuerdo sobre la corrección oportuna de los asuntos pertinentes indicados en el informe;

p) Obligaciones de la proveedora/or para cumplir con los requisitos de seguridad del Ministerio.

15.1.3 Control: Cadena de suministro de tecnologías de la información y comunicaciones

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

Se deben incluir los siguientes temas en los acuerdos con la/el proveedora/or sobre la seguridad de la cadena de suministro:

a) Definir los requisitos de seguridad de la información que se aplican a la adquisición de tecnologías, productos o servicios de información y comunicación además de los requisitos de seguridad de la información para las relaciones con la/el proveedora/or;

b) Para los servicios de tecnología de información y comunicación que requieren que las/los usuarias/os propaguen los requisitos de seguridad del Ministerio en toda la cadena de suministro si las/los proveedoras/es realizan subcontrataciones para partes del servicio de tecnología de información y comunicación proporcionados al Ministerio;

c) Para los productos de tecnología de información y comunicación que requieren que los proveedores propaguen las prácticas de seguridad correspondientes a través de toda la cadena de suministro si estos productos incluyen componentes comprados a otras/os proveedoras/es;

d) Implementación de un proceso de monitoreo y métodos aceptables para validar que los productos y servicios de tecnología de información y comunicación adhieren a los requisitos de seguridad establecidos;

e) Implementación de un proceso para identificar los componentes de los productos o servicios que son fundamentales para mantener la funcionalidad y que, por lo tanto, requiere una mayor atención y escrutinio cuando se desarrollan fuera del Ministerio, especialmente si la/el proveedora/or del nivel superior externaliza los aspectos de los componentes de productos o servicios a otras/os proveedoras/es;

f) Obtención de una garantía de que los componentes críticos y su origen se pueden rastrear en toda la cadena de suministros;

g) Obtener la garantía de que los productos de tecnología de información y comunicación entregados funcionan según lo esperado sin ninguna función inesperada o no deseada;

h) Definición de las reglas para compartir la información en cuanto a la cadena de suministro y cualquier posible problema y compromiso entre el Ministerio y las/los proveedoras/es;

i) Implementación de procesos específicos para administrar el ciclo de vida de los componentes de tecnología de información y comunicación junto con la disponibilidad y los riesgos de seguridad asociados. Esto incluye los riesgos de los componentes que ya no están disponibles debido a que las/los proveedoras/es ya no están en el negocio o a que ya no proporcionan estos componentes debido a los avances de la tecnología.

15.2 Categoría: Administración de prestación de servicios de proveedoras/es

Objetivo

Garantizar el mantenimiento del nivel acordado de seguridad de información y prestación de servicios conforme a los acuerdos de la/el proveedora/or.

15.2.1 Control: Supervisión y Revisión de los servicios de la/el proveedora/or

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

El Ministerio debe mantener control suficiente y visión general de todos los aspectos de seguridad para la información sensible o crítica, o de las instalaciones de procesamiento de información accedidas, procesadas o gestionadas por una tercera parte. Se recomienda que la organización asegure que se mantenga la visibilidad de las actividades de seguridad como gestión de cambios, identificación de vulnerabilidades y reporte/respuesta de

incidentes de seguridad de información a través de un proceso de reportes claro y definido, con formato y estructura.

15.2.2 Control: Gestión de cambios a los servicios de la proveedora/or

Se deben gestionar los cambios en la provisión de los servicios, incluyendo el mantenimiento y las mejoras de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los sistemas y procesos del negocio involucrados y la revaluación de los riesgos.

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

- Los cambios realizados por la organización para implementar:
  - Mejoras a los servicios corrientes ofrecidos;
  - Desarrollo de cualquier aplicación y sistemas nuevos;
  - Modificaciones o actualizaciones de las políticas y procedimientos del Ministerio;
  - Nuevos controles para resolver los incidentes de la seguridad de la información y para mejorar la seguridad;
- Cambios en los servicios de las terceras partes para implementar:
  - Cambios y mejoras de las redes;
  - Uso de nuevas tecnologías;
  - Adopción de nuevos productos o nuevas versiones/publicaciones;
  - Nuevas herramientas de desarrollo y ambientes;
  - Cambios de las ubicaciones físicas de las instalaciones de servicio;
  - Cambio de las/los proveedoras/es.

16. Cláusula: Gestión de Incidentes de Seguridad

Generalidades

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

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

Objetivo

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

Alcance

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

Responsabilidad

El CSI es responsable de implementar los medios y canales necesarios para que la/el RSI maneje los reportes de incidentes y anomalías de los sistemas. Asimismo, dicho Comité, debe tomar conocimiento, efectuar el seguimiento de la investigación, controlar la evolución e impulsar la resolución de los incidentes relativos a la seguridad.

La/el RSI tiene a cargo el seguimiento, documentación y análisis de los incidentes de seguridad reportados, así como su comunicación al CSI, a las/os Propietarias/os de la Información y al Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC). Asimismo, la/el RSI y el Área de Gestión de Recursos Humanos son responsables de comunicar fehacientemente los procedimientos de Gestión de Incidentes a las/los empleadas/os y contratadas/os al inicio de la relación laboral.

La/El Responsable del Área Jurídica debe participar en el tratamiento de incidentes de seguridad que requieran de su intervención.

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

16.1 Categoría: Informe de los eventos y debilidades de la seguridad de la información

Objetivo

Asegurar que los eventos y debilidades de la seguridad de la información asociados con los sistemas de información sean comunicados de una manera que permita que se realice una acción correctiva oportuna.

16.1.1 Control: Reporte de los eventos de la seguridad de información

Los incidentes relativos a la seguridad deben ser comunicados a través de las autoridades o canales apropiados tan pronto como sea posible.

Se debe establecer 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 debe contemplar que, ante la detección de un supuesto incidente o violación de la seguridad, la/el RSI sea informado tan pronto como se haya tomado conocimiento. Este debe indicar los recursos necesarios para la investigación y resolución del incidente, y se hará cargo de su monitoreo.

Asimismo, debe mantener al CSI al tanto de la ocurrencia de incidentes de seguridad.

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

Todas/os las/los empleadas/os y contratistas deben conocer fehacientemente el procedimiento de comunicación de incidentes de seguridad y deben informar formalmente éstos tan pronto hayan tomado conocimiento de su ocurrencia.

16.1.2 Control: Reporte de las debilidades de la seguridad

Las/Los usuarias/os de servicios de información, al momento de tomar conocimiento directo o indirectamente acerca de una debilidad de seguridad, son responsables de registrar y comunicar formalmente éstas al RSI.

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

16.1.3 Control: Comunicación de Anomalías del Software

Se deben establecer procedimientos para la comunicación de anomalías de software, los cuales deben 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 de modo formal al RSI o a la/el Responsable del activo de que se trate.

Se prohíbe a las/los usuarias/os quitar el software que supuestamente tiene una anomalía, a menos que estén autorizados formalmente para hacerlo. La recuperación debe ser realizada por personal experimentado, adecuadamente habilitado.

16.2 Categoría: Gestión de los Incidentes y mejoras de la seguridad de la información

Objetivo

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

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

16.2.1 Control: Responsabilidades y procedimientos

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

a) Contemplar y definir todos los tipos probables de incidentes relativos a seguridad, incluyendo como mínimo:
    i. Fallas operativas;
    ii. Código malicioso;
    iii. Intrusiones;
    iv. Fraude informático;
    v. Error humano;
    vi. Catástrofes naturales.

b) Comunicar formalmente los incidentes a través de autoridades o canales apropiados tan pronto como sea posible.

c) Contemplar los siguientes puntos en los procedimientos para los planes de contingencia normales (diseñados para recuperar sistemas y servicios tan pronto como sea posible):
    i. Definición de las primeras medidas a implementar;
    ii. Análisis e identificación de la causa del incidente;
    iii. Planificación e implementación de soluciones para evitar su repetición, si fuera necesario;
    iv. Comunicación formal con las personas afectadas o involucradas con la recuperación del incidente;
    v. Notificación de la acción a la autoridad y/u Organismos pertinentes.

d) Registrar pistas de auditoría y evidencia similar para:
    i. Análisis de problemas internos;
    ii. Uso como evidencia en relación con una probable violación contractual o infracción normativa, o en marco de un proceso judicial (Ver cláusula 10.1. Categoría: Cumplimiento de Requisitos Legales).

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:
    i. Acceso a los sistemas y datos existentes sólo al personal claramente identificado y autorizado;
    ii. Documentación de todas las acciones de emergencia emprendidas en forma detallada;
    iii. Comunicación de las acciones de emergencia a la/el titular de la Unidad Organizativa y revisión de su cumplimiento;
    iv. Constatación de la integridad de los controles y sistemas del Ministerio en un plazo mínimo.

f) En los casos en los que se considere necesario, se debe solicitar la participación de la/el Responsable del Área Jurídica del Ministerio en el tratamiento de incidentes de seguridad ocurridos.

16.2.2 Control: Aprendiendo a partir de los incidentes de la seguridad de la información

Se debe definir un proceso que permita documentar, cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y anomalías. Esta información se debe utilizar para identificar aquellos que sean recurrentes o de alto impacto.

Esto debe ser evaluado a efectos de establecer la necesidad de mejorar o agregar controles para limitar la frecuencia,

daño y costo de casos futuros.

16.2.3 Control: Procesos Disciplinarios

Se debe seguir el proceso disciplinario formal contemplado en las normas estatutarias, escalafonarias y convencionales que rigen al personal de la Administración Pública Nacional, para las/los empleadas/os que violen la Política, Normas y Procedimientos de Seguridad del Ministerio(Ver Cláusula 18: Cumplimiento).

17. Cláusula: Gestión de la Continuidad

Generalidades

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

El desarrollo e implementación de planes de contingencia es una herramienta básica para garantizar que las actividades del Ministerio 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 eventuales interrupciones de las actividades del Ministerio y asegurar la reanudación oportuna de las operaciones indispensables.

Objetivo

Minimizar los efectos de las posibles interrupciones de las actividades normales del Ministerio (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 Ministerio con el establecimiento de planes que incluyan al menos las siguientes etapas:

a) Notificación/Activación: Consiste en la detección y determinación del daño y la activación del plan;

b) Reanudación: Consiste en la restauración temporal de las operaciones y recuperación del daño producido al sistema original;

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

Asegurar la coordinación con el personal del Ministerio y los contactos externos que deben participar en las estrategias de planificación de contingencias. Asignar funciones para cada actividad definida.

Alcance

Esta política se aplica a todos los procesos críticos identificados del Ministerio.

Responsabilidad

La/El RSI debe participar activamente en la definición, documentación, prueba y actualización de los planes de contingencia.

Las/Los Propietarias/os de la Información y la/el RSI cumplen las siguientes funciones:

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

Las/Los Responsables de Procesos deben revisar periódicamente los planes bajo su incumbencia, como así también identificar cambios en las disposiciones relativas a las actividades del Ministerio aún no reflejadas en los planes de continuidad.

Las/Los administradoras/es de cada plan deben verificar el cumplimiento de los procedimientos implementados para llevar a cabo las acciones contempladas en cada plan de continuidad.

El CSI tiene a cargo la coordinación del proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de información del Ministerio frente a interrupciones imprevistas.

17.1 Categoría: Gestión de continuidad del Ministerio

Objetivo

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

17.1.1 Control: Proceso de Administración de la continuidad del Ministerio

El CSI es responsable de la coordinación del desarrollo de los procesos que garanticen la continuidad de las actividades del Ministerio.

El CSI tiene a cargo la coordinación del proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de información del Ministerio frente a interrupciones imprevistas, lo cual incluye las siguientes funciones:

a) Identificar y priorizar los procesos críticos de las actividades del Ministerio.

b) Asegurar que todos los/las integrantes del Ministerio comprendan los riesgos que ésta 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 Ministerio.

c) Elaborar y documentar una estrategia de continuidad de las actividades del Ministerio consecuente con los objetivos y prioridades acordados.

d) Proponer planes de continuidad de las actividades del Ministerio de conformidad con la estrategia de continuidad acordada.

e) Establecer un cronograma de pruebas periódicas de cada uno de los planes de contingencia, proponiendo una asignación de funciones para su cumplimiento.

f) Coordinar actualizaciones periódicas de los planes y procesos implementados.

g) Considerar la contratación de seguros que podrían formar parte del proceso de continuidad de las actividades del Ministerio.

h) Proponer las modificaciones a los planes de contingencia.

17.1.2 Control: Continuidad de las Actividades y Análisis de los impactos

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

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

electrónicos vitales, etc.

Esta actividad debe ser llevada a cabo con la activa participación de las/los propietarias/as de los procesos y recursos de información de que se trate y la/el RSI, considerando todos los procesos de las actividades del Ministerio y no limitándose a las instalaciones de procesamiento de la información.

Según los resultados de la evaluación de esta actividad, se debe desarrollar un plan estratégico para determinar el enfoque global con el que se aborda la continuidad de las actividades del Ministerio. Una vez que se ha creado este plan, éste debe ser propuesto por el CSI a la máxima autoridad del Ministerio para su aprobación.

17.1.3 Control: Elaboración e implementación de los planes de continuidad de las actividades del Ministerio

Las/Los propietarias/as de procesos y recursos de información, con la asistencia de la/el RSI deben elaborar los planes de contingencia necesarios para garantizar la continuidad de las actividades del Ministerio. Estos procesos deben ser propuestos por el CSI.

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

a) Identificar y acordar respecto a todas las funciones y procedimientos de emergencia.

b) Analizar los posibles escenarios de contingencia y definir las acciones correctivas a implementar en cada caso.

c) Implementar procedimientos de emergencia para permitir la recuperación y restablecimiento en los plazos requeridos. Se debe dedicar especial atención a la evaluación de las dependencias de actividades externas y a los contratos vigentes.

d) Documentar los procedimientos y procesos acordados.

e) Instruir adecuadamente al personal, en materia de procedimientos y procesos de emergencia acordados, incluyendo el manejo de crisis.

f) instruir al personal involucrado en los procedimientos de reanudación y recuperación en los siguientes temas:

   i. Objetivo del plan.

   ii. Mecanismos de coordinación y comunicación entre equipos (personal involucrado).

   iii. Procedimientos de divulgación.

   iv. Requisitos de la seguridad.

   v. Procesos específicos para el personal involucrado.

   vi. Responsabilidades individuales.

   vii. Probar y actualizar los planes, guardando evidencia formal de las pruebas y sus resultados. Asimismo, el proceso de planificación debe concentrarse en los objetivos de las actividades requeridas del Ministerio, por ejemplo, restablecimiento de los servicios a las/los usuarias/os en un plazo aceptable. Deben considerarse los servicios y recursos que permiten 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.

17.1.4 Control: Marco para la Planificación de la Continuidad de las Actividades del Ministerio

Se debe mantener un solo marco para los planes de continuidad de las actividades del Ministerio, a fin de garantizar que éstos sean uniformes e identificar prioridades de prueba y mantenimiento.

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

La/El administradora/or de cada Plan de Continuidad es la/el encargada/o de coordinar las tareas definidas en éste.

Las modificaciones deben ser propuestas por el CSI para su aprobación.

El marco para la planificación de la continuidad de las actividades del Ministerio debe tener 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 ponerlos en marcha;

b) Definir los procedimientos de emergencia que describan las acciones a emprender una vez ocurrido un incidente que ponga en peligro las operaciones del Ministerio 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 Ministerio o de servicios de soporte a ubicaciones transitorias alternativas, y para el restablecimiento de los procesos en los plazos requeridos;

d) Redactar los procedimientos de recuperación que describan las acciones a emprender para restablecer las operaciones normales del Ministerio;

e) Definir un cronograma de mantenimiento que especifique cómo y cuándo será probado el plan, y el proceso para su mantenimiento;

f) Efectuar actividades de concientización e instrucción al personal, diseñadas para propiciar la comprensión de los procesos de continuidad de las actividades y garantizar que los procesos sigan siendo eficaces;

g) Documentar las responsabilidades y funciones de las personas, describiendo las/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/a responsable de declarar el estado de contingencia, lo cual dará inicio al plan.

Las/Los Administradoras/es de los Planes de Contingencia son designadas/os por el CSI.

El cumplimiento de los procedimientos implementados para llevar a cabo las acciones contempladas en cada Plan de Continuidad deben contarse entre las responsabilidades de las/los Administradoras/es 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 las/los proveedoras/es de servicios.

17.1.5 Control: Ensayo, Mantenimiento y Reevaluación de los Planes de continuidad del Ministerio

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

- El CSI debe establecerá un cronograma de pruebas periódicas de cada uno de los planes de contingencia;
- El cronograma indica quienes son las/los responsables de llevar a cabo cada una de las pruebas y de elevar el resultado obtenido al citado Comité.

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

a) Efectuar pruebas de discusión de diversos escenarios (discutiendo medidas para la recuperación de las actividades 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 Ministerio, el personal, el equipamiento, las instalaciones y los procesos pueden afrontar las interrupciones.

Para las operaciones críticas del Ministerio se deben tomar en cuenta, además, los siguientes mecanismos:

a) Efectuar pruebas de recuperación en un sitio alternativo (ejecutando los procesos de las actividades del Ministerio en paralelo, con operaciones de recuperación fuera del sitio principal);

b) Realizar pruebas de instalaciones y servicios de proveedoras/es (garantizando que los productos y servicios de proveedoras/es externos cumplan con los compromisos contraídos).

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

Los Planes de Continuidad de las actividades del Ministerio serán elaborados oportunamente en un documento

posterior, y deben ser revisados y actualizados periódicamente, para garantizar su eficacia permanente. Se deben incluir procedimientos en el Programa de Administración de Cambios del Ministerio para garantizar que se aborden adecuadamente los tópicos de continuidad de las actividades.

La periodicidad de revisión de los planes de contingencia es de doce (12) meses.

Cada Responsables de Procesos debe asegurar las revisiones periódicas de cada uno de los Planes de Continuidad de su incumbencia, como así también de la identificación de cambios en las disposiciones relativas a las actividades del Ministerio aún no reflejadas en dichos planes.

Debe prestarse especial atención a los cambios de:

a) Personal;

b) Direcciones o números telefónicos;

c) Estrategia del Ministerio;

d) Ubicación, instalaciones y recursos;

e) Legislación;

f) Contratistas, proveedoras/es y clientas/es críticos;

g) Procesos, o procesos nuevos / eliminados;

h) Tecnologías;

i) Requisitos operacionales;

j) Requisitos de seguridad;

k) Hardware, software y otros equipos (tipos, especificaciones, y cantidad);

l) Requerimientos de los sitios alternativos;

m) Registros de datos vitales.

Todas las modificaciones efectuadas deben ser propuestas por el CSI para su aprobación por el superior jerárquico que corresponda.

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

17.2 Categoría: Redundancias

Objetivo

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

17.2.1 Control: Disponibilidad de las instalaciones de procesamiento de la información

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

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

18. Cláusula: Cumplimiento

Generalidades

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

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

El Área Jurídica del Ministerio es responsable de encuadrar jurídicamente la formulación e implementación de la política.

Objetivos

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

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

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 éste, 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 Ministerio.

Alcance

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

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

Responsabilidad

La/El RSI cumple las siguientes funciones:

- Definir normas y procedimientos para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual y a la conservación de registros;
- Realizar revisiones periódicas de todas las áreas del Ministerio 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;
- Garantizar la seguridad y el control de las herramientas utilizadas para las revisiones de auditoría.

La/El Responsable del Área Jurídica del Ministerio, con la asistencia de la/el RSI cumplen las siguientes funciones:

- Definir y documentar claramente todos los requisitos normativos y contractuales pertinentes para cada sistema de información;
- Redactar un Compromiso de Confidencialidad a ser firmado por todo el personal.

Las/Los Responsables de Unidades Organizativas deben velar por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos en la presente política, dentro de su área de responsabilidad.

Todas/os las/los empleadas/os de los mandos medios y superiores deben conocer, comprender, dar a conocer, cumplir y hacer cumplir la presente política y la normativa vigente.

18.1 Categoría: Cumplimiento de Requisitos Legales

Objetivo

Evitar las violaciones a cualquier ley; regulación estatutaria, reguladora o contractual; y cualquier requerimiento de seguridad.

El diseño, operación, uso y gestión de los sistemas de información pueden estar sujetos a requerimientos de seguridad estatutarios, reguladores y contractuales.

18.1.1 Control: Identificación de la Legislación Aplicable

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

18.1.2 Control: Derechos de Propiedad Intelectual

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

Las/Los empleadas/os únicamente podrán utilizar material autorizado por el Ministerio.

El Ministerio solo podrá autorizar el uso de material producido por éste, o material autorizado o suministrado a éste por su titular, conforme los términos y condiciones acordadas 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 deben 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/as utilicen su producto o procedimiento.

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 al equipamiento específico y su copia a la creación de copias de resguardo solamente.

La/El RSI, con la asistencia del Área Jurídica, debe analizar los términos y condiciones de la licencia, e implementar 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 usuarias/os;

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/as;

i) Utilizar herramientas de auditoría adecuadas;

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

18.1.3 Control: Protección de los Registros del Ministerio

Los registros críticos del Ministerio se deben proteger 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 Ministerio.

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

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

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

Si se seleccionan medios de almacenamiento electrónicos, se deben incluir 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 éstos contra eventuales pérdidas ocasionadas por futuros cambios tecnológicos.

Los sistemas de almacenamiento de datos deben ser 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, de acuerdo a lo que se defina en tal sentido oportunamente.

El sistema de almacenamiento y manipulación debe garantizar 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 Ministerio.

A fin de cumplir con estas obligaciones, se deben tomar 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 deben tener presente las siguientes normas:

- Ética en el Ejercicio de la Función Pública. Ley Nº 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/la funcionario/a público/a 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 artículo 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 una funcionario/a o de otra persona en el interés del servicio público. Si el culpable fuere el/la mismo/a depositario/a, 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 del 30 de abril de 1996: Reglamenta el artículo 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;
- Ley de Propiedad Intelectual N° 11.723: Protege los derechos de autor de las obras científicas, literarias y artísticas, incluyendo las compilaciones de datos o de otros materiales;
- Ley N° 25.506 y su reglamentación: Establece que la exigencia legal de conservar documentos, registros o datos, también queda satisfecha con la conservación de los correspondientes documentos digitales firmados digitalmente, según los procedimientos que determine la reglamentación, siempre que sean accesibles para su

posterior consulta y permitan determinar fehacientemente el origen, destino, fecha y hora de su generación, envío y/o recepción;

- Código Penal: Sanciona a aquel que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos (artículo 183).

18.1.4 Control: Protección de Datos y Privacidad de la Información Personal

Todas/os las/los empleadas/os deben conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan conocimiento con motivo del ejercicio de sus funciones.

El Ministerio debe redactar un "Compromiso de Confidencialidad", el cual debe ser suscrito por todos los/las funcionarios/as públicos/as y contratistas. La copia firmada del compromiso será retenida en forma segura por el Ministerio.

Mediante este instrumento la/el empleada/o se compromete a utilizar la información solamente para el uso específico al que se ha destinado y a no comunicar, diseminar o de alguna otra forma hacer pública la información a ninguna persona, firma, compañía o tercera persona, salvo autorización previa y escrita de la/el Responsable del Activo de que se trate. A través del "Compromiso de Confidencialidad" se debe advertir a la/el empleada/o 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 de la empleada/o.

En particular, se deben tener presente las siguientes normas:

- Ley Marco de Regulación de Empleo Público Nacional Nº 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 las/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 Nº 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 Nº 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/as;
- 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 abriere o accediere indebidamente a una comunicación electrónica o indebidamente la suprimiere o desviare (artículo 153), al que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido (artículo 153 bis), al que el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros. (artículo 155), al que teniendo noticias de un secreto cuya divulgación pueda causar daño, lo revelare sin justa causa (artículo 156), al funcionario público que revelare hechos, actuaciones o documentos que por la ley deben quedar secretos (artículo 157), al que a sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales, ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley e ilegítimamente insertare o hiciere insertar datos en un archivo de datos

personales (artículo 157 bis), al que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos (artículo 183), 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 (artículos 222 y 223).

Asimismo, debe considerarse lo establecido en el decreto 1172 del 3 de diciembre de 2003, que regula el acceso a la información pública por parte de los ciudadanos.

18.1.5 Control: Prevención del Uso Inadecuado de los Recursos de Procesamiento de Información

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

Todas/os las/los empleadas/os 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 Nº 25.164: Prohíbe hacer uso indebido o con fines particulares del patrimonio estatal;
- Convenio Colectivo de Trabajo General: Obliga a las/los agentes a no hacer uso indebido o con fines particulares del patrimonio estatal;
- Ética en el Ejercicio de la Función Pública. Ley Nº 25.188: Obliga a las personas que se desempeñen en la función pública a proteger y conservar la propiedad del Estado Nacional 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;
- Código Penal: Sanciona a aquel que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños (artículo 183).

18.1.6 Control: Regulación de Controles para el Uso de Criptografía

Al utilizar firmas digitales o electrónicas se debe considerar lo dispuesto en la ley 25.506 y sus normas reglamentarias y complementarias, 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 Wassenaar, que establece un listado de materiales y tecnologías de doble uso, cuya comercialización puede ser considerada peligrosa.

El decreto 603 del 9 de abril de 1992 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 al área competente del Ministerio de Defensa, a fin de saber si el material exportable requiere algún tratamiento especial.

18.1.7 Control: 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, la evidencia presentada debe cumplir con lo establecido por las normas procesales. Para lograr la validez de la evidencia, el Ministerio debe garantizar que sus sistemas de información cumplen con la normativa y 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 ésta. Esta pista se establece

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 para garantizar su disponibilidad. Se debe mantener un registro de todas las acciones realizadas durante el proceso de copia. Se debe almacenar 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 por lo tanto se deben tomar todos los recaudos establecidos para la obtención y preservación de la evidencia.

Se debe 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 las/los agentes públicos. Este Decreto debe ser complementado por lo dispuesto en la Ley de Procedimientos Administrativos N° 19.549 y por toda otra normativa aplicable, incluido el Código Penal, el que sanciona a quien sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público (artículo 255).

18.1.8 Control: Delitos Informáticos

Todas/os las/os empleadas/os deben conocer la existencia de la ley 26.388 de Delitos Informáticos, a partir de cuyo dictado se castigan penalmente ciertas conductas cometidas mediante medios informáticos. En tal sentido, las/los agentes públicos deben conocer con exactitud el alcance de los nuevos tipos penales introducidos por la norma mencionada.

Cabe señalar que la mayoría de las conductas descritas por dicha norma vinculada ya han sido señaladas en los apartados precedentes.

18.2 Categoría: Revisiones de la Política de Seguridad y la Compatibilidad Técnica

Objetivo

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

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

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

18.2.1 Control: Cumplimiento de la Política de Seguridad

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

La/El RSI realizará revisiones periódicas de todas las áreas del Ministerio 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) Propietarias/os de información.

d) Usuarias/os.

Las/Los Propietarias/os de la Información deben brindar apoyo a la revisión periódica del cumplimiento de la política, normas, procedimientos y otros requisitos de seguridad aplicables.

18.2.2 Control: Verificación de la Compatibilidad Técnica

La/El RSI debe verificar 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 debe volcar en un informe técnico para su ulterior interpretación por parte de los/las especialistas. Para ello, la tarea puede ser realizada por un/a profesional experimentado/a (en forma manual o con el apoyo de herramientas de software), o por un paquete de software automatizado que genere reportes que pueden ser interpretados por un/a especialista técnico/a.

La verificación del cumplimiento comprende pruebas de penetración y tiene 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 deben tomar los recaudos necesarios en el caso de pruebas de penetración exitosas que comprometan la seguridad del sistema.

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

18.3 Categoría: Consideraciones de Auditorías de Sistemas

Objetivo

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

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

Con relación a las auditorías, son de aplicación las Normas de Control Interno para Tecnologías de Información, aprobadas por la resolución 48 del 5 de mayo de2005 de la Sindicatura General de la Nación (SIGEN), organismo descentralizado en el ámbito de la Presidencia de la Nación.

18.3.1 Controles de Auditoría de Sistemas

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

Se deben contemplar los siguientes puntos:

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

b) Controlar el alcance de las verificaciones. Esta función debe ser realizada por la/el responsable de auditoría;

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

   i. Eliminar archivos transitorios;
   ii. Eliminar entidades ficticias y datos incorporados en archivos maestros;
   iii. Revertir transacciones;
   iv. Revocar privilegios otorgados

d) Identificar claramente los recursos de tecnologías de información (TI) para llevar a cabo las verificaciones, los cuales deben ser puestos a disposición de los auditores. A tal efecto, la Unidad de Auditoría o en su defecto quien sea propuesto por el CSI debe completar el formulario que oportunamente se establezca, el cual debe ser puesto en conocimiento de las áreas involucradas;

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:

   i. Fecha y hora;
   ii. Puesto de trabajo;
   iii. Usuario;

iv. Tipo de acceso;

v. Identificación de los datos accedidos;

vi. Estado previo y posterior;

vii. Programa y/o función utilizada;

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

18.3.2 Control: Protección de los Elementos Utilizados por la Auditoría de Sistemas

Se debe proteger 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 éstos.

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

Se deben tomar los recaudos necesarios a efectos de cumplir las normas de auditoría dispuestas por la Sindicatura General de la Nación.

18.3.3 Control: Sanciones Previstas por Incumplimiento

Se debe sancionar administrativamente a quien viole lo dispuesto en la presente PSI conforme a lo previsto por las normas estatutarias, escalafonarias y convencionales que rigen al personal de la Administración Pública Nacional y, en caso de corresponder, se deben realizar las acciones correspondientes ante el o los Organismos pertinentes.

Las sanciones sólo pueden imponerse mediante un acto administrativo que así lo disponga cumpliendo las formalidades impuestas por los preceptos constitucionales, la Ley de Procedimiento Administrativo Nº 19.549 y demás normativas específicas aplicables.

Amén de las sanciones disciplinarias o administrativas, la/el agente que no da debido cumplimiento a sus obligaciones pueden incurrir también en responsabilidad civil o patrimonial —cuando ocasiona un daño que debe ser indemnizado— y/o en responsabilidad penal —cuando su conducta constituye un comportamiento considerado delito por el Código Penal y leyes especiales.

República Argentina - Poder Ejecutivo Nacional
2021 - Año de Homenaje al Premio Nobel de Medicina Dr. César Milstein

Hoja Adicional de Firmas
Anexo

Número: IF-2021-19601238-APN-SLYA#MEC

CIUDAD DE BUENOS AIRES
Viernes 5 de Marzo de 2021

Referencia: Política de Seguridad de la Información - Código SI-POL-01 - versión 1.2.

El documento fue importado por el sistema GEDO con un total de 94 pagina/s.

Digitally signed by TANUZ Rita Haydee
Date: 2021.03.05 11:30:33 ART
Location: Ciudad Autónoma de Buenos Aires

Rita Haydee Tanuz
Secretaria
Secretaría Legal y Administrativa
Ministerio de Economía

Digitally signed by Gestion Documental Electronica
Date: 2021.03.05 11:30:46 -03:00