Ministerio de Educación
Presidencia de la Nación

MINISTERIO DE EDUCACIÓN DE LA NACIÓN

POLITICAS DE SEGURIDAD DE LA INFORMACION

VERSIÓN 1.0

Contenido

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. INTRODUCCIÓN

1.1. Objetivo

En el marco del cumplimiento por lo dispuesto en la Decisión Administrativa (DA) N°641/2021, se elabora la presente política para ser aprobada por las autoridades y comunicada a todos los involucrados.

El presente documento “Política de Seguridad de la Información” (en adelante PSI) del Ministerio de Educación de la Nación, tiene por objeto proteger los datos y los recursos utilizados para su tratamiento, que define la postura del organismo respecto al comportamiento que se espera de empleados, autoridades y terceros que tomen contacto con dichos datos y/o recursos para su protección.

La política recoge las medidas de seguridad establecidas con el fin de asegurar la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de los sistemas de información y de los datos, cuando sean tratados por los agentes, funcionarios, trabajadores en el ejercicio de sus funciones, y aquellos prestadores de servicios y/o reparticiones públicas que el Ministerio de Educación requiera para acometer sus objetivos.

Es de máxima importancia que los principios de la PSI sean parte de la cultura organizacional, para lo cual se debe asegurar el compromiso manifiesto de los directivos del organismo, de los titulares de las distintas unidades organizativas para la difusión del mismo y de todos los funcionarios y agentes para la consolidación y cumplimiento de la presente política.

1.2. Alcance

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 de técnicas/os, administrativas/os y operativas/os, y sea cual fuere su nivel jerárquico y su situación de revista, como así también por terceros que establezcan algún tipo de relación contractual con el organismo.

2. TÉRMINOS Y DEFINICIONES

2.1. Seguridad de la Información

Se entiende como “Seguridad de la Información” a la preservación de las siguientes características:

- **Confidencialidad:** Garantizar que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- **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.

2.2. Definición:

- **Principio de seguridad de la información**: Integran este principio, la confidencialidad, integridad y disponibilidad de la información.
- **Autenticidad**: Validez de la información en tiempo, forma y distribución. 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 posterior control
- **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 de Educación, y particularmente aquel que hace a la seguridad de la información.
- **Privilegio**: Para sistemas multiusuario o de red, indica las características, derechos o servicios que permite a un usuario realizar ciertas actividades o acciones.
- **Información**: Referente 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. La información es el activo más importante de todo organismo.
- **Contabilidad de la información**: La información generada debe ser adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.
- **Dato**: Una unidad de información.

- **Datos Sensibles**: Los datos sensibles personales: son los que refieren al origen racial o étnico, ideológico, creencias religiosas o filosóficas, afiliación sindical, salud o vida sexual y se les aplican normas más estrictas para su tratamiento. Los datos sensibles organizacionales: son los que se refieren a temas propios de un organismo, cuya difusión pública aumentaría el riesgo de amenazas a la información.
- **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.
- **Sensibilización**: Implica un proceso que tiene como objetivo principal impactar sobre el comportamiento de los usuarios y reforzar buenas prácticas en materia de seguridad de la información.
- **Filtración de información**: Divulgaciones no autorizadas de información que pueden dar lugar a robos o fugas de datos
- **Programas maliciosos o Malware:** Programas peligrosos como virus, gusanos, troyanos y programas espía.
- **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 puedan comprometer o comprometan 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.
- **Riesgo:** Combinación de la probabilidad de ocurrencia de un evento y sus consecuencias o impactos.
- **Amenaza:** Una causa potencial de un incidente no deseado, el cual puede ocasionar daños a un sistema u organismo.
- **Vulnerabilidad:** Debilidad de un activo o grupo de activos que puede es aprovechada por una amenaza.
- **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.
- **Gestión de Riesgos**: Actividades coordinadas para dirigir y controlar una organización en lo que concierne al riesgo. Esta incluye la evaluación de riesgos, tratamiento de riesgos y aceptación de riesgos.
- **Evaluación de Riesgos**: Se entiende por evaluación de riesgos a la evaluación de 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 organismo.

3. GESTIÓN DE RIESGOS

Dado que todo organismo se encuentra expuesto a riesgos en materia de seguridad, y que no existe la seguridad absoluta, es necesario conocer cuál es el mapa de riesgos al cual se enfrenta el Ministerio y tomar las acciones pertinentes para mitigar los efectos negativos. Es por ello resulta imprescindible gestionar los riesgos del Ministerio como base fundamental para la gestión de la seguridad de la información.

3.1. Objetivo:

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

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

3.2. Alcance:

Las presentes políticas de seguridad de la información serán de aplicación obligatoria a toda información administrada en el organismo, ya sea cualquiera el soporte en el que se encontrare.

3.3. Responsabilidad

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

3.4. Evaluación de Riesgos

El organismo evaluará sus riesgos identificándolos, cuantificándolos y priorizándolos en función de los criterios de aceptación y de sus objetivos de control relevantes. Los resultados obtenidos guiarán y determinarán la apropiada acción de la dirección y prioridades para gestionar e implementar los controles necesarios para la protección de dichos riesgos.

Se deberá realizar la evaluación de riesgos periódicamente, a fin de tratar los cambios en los requerimientos de seguridad y en las situaciones de riesgo, ya sean por los cambios producidos en los activos, amenazas, vulnerabilidades, impactos y valoración de riesgos. Se deberá realizar la evaluación de los mismos cada vez que ocurran cambios significativos.

El alcance de la evaluación podría incluir a organismo en su completitud, a sólo una parte del mismo, un sistema de información particular, componentes específicos de un sistema o servicios.

3.5. Tratamiento de los Riesgos de Seguridad

Para cada uno de los riesgos identificados durante la evaluación, se deberán tomar decisiones para su tratamiento. Las opciones para el tratamiento de riesgos incluyen:

3.5.1. Mitigar los riesgos, mediante la aplicación de controles apropiados a fin de reducir los mismos.
3.5.2. Aceptar los riesgos de manera objetiva y consciente, siempre y cuando estos satisfagan la política y los criterios de aceptación del organismo.
3.5.3. Evitar los riesgos, eliminando las acciones que dan origen a su ocurrencia.
3.5.4. Transferir los riesgos asociados a otras partes interesadas, como ser compañías de seguro o proveedores de servicios.

4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN (PSI)

4.1. Objetivo

La presente PSI establece las directrices y líneas de actuación en materia de Seguridad de la Información que establecen el modo en que el Ministerio de Educación de la Nación debe gestionar y proteger los datos a los cuales da tratamiento, los recursos tecnológicos que utiliza y los servicios que brinda.

Los objetivos específicos deben asegurar el principio de seguridad de la información y proveer un esquema de gestión destinado a implementar y mantener un nivel de Seguridad de la Información acorde a los riesgos que se presentan y cuyo propósito es:

4.1.1. Asegurar el mantenimiento de la confiabilidad con quienes se comparten redes públicas y privadas.
4.1.2. Garantizar la seguridad de la información.
4.1.3. Adoptar todas las medidas en cumplimiento del marco normativo aplicable.
4.1.4. Poner de manifiesto la postura del Organismo en lo que respecta a la prevención, atención y seguimiento de incidentes de Seguridad de la Información.
4.1.5. Informar que se habilitan y disponen los mecanismos necesarios para el tratamiento adecuado coordinado de la seguridad física y lógica de la información del organismo
4.1.6. Provocar la adopción paulatina de los conceptos de seguridad por parte del personal del organismo mediante un plan de concientización y acorde a la cultura organizacional.
4.1.7. Cumplir con la legislación aplicable en materia de seguridad de la información.

4.2. Alcance

Esta política se aplica a todos los miembros, agentes y funcionarios del Ministerio, y a la totalidad de los procesos, individuos y/u organizaciones, internos o externo vinculados al Ministerio a través de contratos o acuerdos con terceros.

4.3. Responsabilidad

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

El Comité de Seguridad de la Información (CSI):

Será quien efectúe tareas tales como la aprobación de la Política de Seguridad de la Información, coordinar su implementación, asignar funciones y responsabilidades, administrar la seguridad de la información dentro del Ministerio de Educación y garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información del Organismo.

El Comité de Seguridad de la Información se encontrará integrado por representantes de las áreas sustantivas del Ministerio de Educación de la Nación destinado a garantizar el apoyo manifiesto sobre las iniciativas de seguridad.

Funciones:

- Revisar y proponer al ministro de Educación, para su aprobación, la Política de Seguridad de la Información (PSI) conforme a la DA 641/21.
- Efectuar periódicas revisiones de las PSI y gestionar la aprobación de las modificaciones que se efectúen.
- Monitorear los cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
- Seguimiento de las actividades relativas a la seguridad de la información, dentro de cada área: análisis de riesgos, monitoreo de incidentes, supervisión de la investigación, implementación de controles y administración de la continuidad.
- Impulsar procesos de concientización y capacitación de los usuarios.
- Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.
- Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y procesos específicos relativos a la seguridad de la información.
- Propiciar que la seguridad sea parte del proceso de planificación informática del organismo.
- Implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
- Promover la difusión y apoyo a la seguridad de la información dentro del organismo.
- Coordinar el proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de la información del organismo frente a interrupciones imprevistas.
- Supervisión de la normativa y procedimientos para la aplicación de las PSI.

Cómo máxima autoridad del organismo, el Ministro de Educación será quien apruebe las PSI y sus modificatorias.

Los Secretarios, Subsecretarios, Directores Nacionales o Generales, Directores o equivalentes, responsables de las Unidades Organizativas, tanto se trate de autoridades políticas o personal técnico y sea cual fuere su nivel jerárquico, serán los responsables de la implementación y cumplimiento de la PSI dentro de sus áreas de responsabilidad.

Los mismos son responsables de clasificar la información según su grado de sensibilidad y criticidad, documentar y mantener actualizada la clasificación mencionada y definir a los usuarios que tendrán permisos de acceso a la información, de acuerdo con sus funciones y competencias.

Se determina que cada Secretario, Subsecretario, Director Nacional o General, responsables de Unidades Organizativas o equivalentes son responsables primarios de la información de uso y manejo de sus áreas, pudiendo delegar la administración de la misma a personal idóneo a su cargo, pero conservando la responsabilidad primaria de la misma.

La delegación de la administración por parte de los responsables primarios será documentada y proporcionada al Responsable del CSI.

4.4. Revisión

La presente Política de Seguridad de la Información, será revisada y actualizada anualmente por parte del CSI con el objeto de permitir su constante actualización. La actividad de revisión incluye oportunidades de mejoras, en respuesta a los cambios organizacionales, tanto en los procesos críticos o normativos, legales, de terceros, tecnológicos o de otra índole.

4.5. Cumplimiento

La presente Política de Seguridad de la Información, deberá ser cumplida por todo el personal, tanto se trate de funcionarios jerárquicos, administrativos, operativos y técnicos, sea cual fuere su modalidad de contratación, nivel escalafonario y situación de revista.

Las PSI, deberán ser utilizadas como base para establecer un conjunto de normas, procedimientos, lineamientos y guías acordes a los procesos que se lleven adelante en el organismo, ya sea desde una plataforma tecnológica como de los demás recursos de los que disponga.

Una vez generada, actualizada, modificada, revisada y aprobadas las PSI, las mismas serán informadas a la Dirección Nacional de Ciberseguridad de la Secretaría de Innovación Publica de la Jefatura de Gabinete de Ministros.

5. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD

5.1. Objetivo

Desarrollar e implementar un marco organizativo para la efectiva gestión y operación de la seguridad de la información en el organismo, por lo cual, será asignando a un área del organismo con competencia en la materia las responsabilidades relativas a la seguridad de la información.

Establecer un marco gerencial para iniciar y controlar la implementación de las PSI, como también establecer y distribuir las funciones y responsabilidades de los miembros integrantes del Comité de Seguridad.

Fomentar la consulta y cooperación con organismos especializados para la obtención de asesoría en materia de seguridad. Por lo cual el responsable del CSI podrá mantener contactos con los siguientes organismos especializados en temas relativos a la seguridad informática:

5.1.1. Oficina Nacional de Tecnologías de la Información (ONTI)
5.1.2. Cert.ar (Equipo de Respuesta ante Emergencias Informáticas Nacional)
5.1.3. Dirección Nacional de Firma Digital e Infraestructura Tecnológica
5.1.4. Dirección Nacional de Protección de Datos Personales de la Agencia de acceso a la información pública

En caso de darse dichos intercambios de información, no será divulgada información confidencial perteneciente al organismo a personas no autorizadas. Los fines de dicha acción será pura y exclusivamente con fines de asesoramiento o de transmisión de experiencias, solo se permitirá cuando se haya firmado un acuerdo de Compromiso de Confidencialidad previo o con aquellas organizaciones especializadas en temas relativos a la seguridad informática y cuyo personal este obligado a mantener la confidencialidad de los temas que tratan.

5.2. Responsabilidad

El/La Coordinador/a del CSI es el/la responsable de impulsar la implementación de la PSI.

El CSI será quien genere, revise, actualice y proponga la presentación de las PSI para su a la máxima autoridad del Ministerio.

5.3. Organización Interna

El/La Coordinador/a del CSI es el/la responsable de:

- Coordinar las acciones del CSI.
- Impulsar la implementación y cumplimiento de la PSI.

El/La Secretario/a Técnico/a de Seguridad de la Información:

- Cumplirá funciones relativas a la recepción de designaciones de representantes, modificaciones y/o cualquier otra circunstancia vinculada a la conformación del comité.
- Comunicará convocatorias a reuniones ordinarias y extraordinarias. Comunicará la creación de comisiones y será el responsable de la comunicación institucional.

El/La Responsable del área de Gestión Informática:

- Cumplirá la función de cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología del organismo.

El/La Responsable del área de Recursos Humanos:

- Notificará a todo el personal del cumplimiento de las PSI y de todas las normas, procedimientos y prácticas que de ella surjan.
- Implementará actas compromiso sobre la confidencialidad de la información y notificar la responsabilidad sobre el tratamiento de la información a los usuarios.
- Notificará a las áreas correspondientes las bajas de personal para proceder a realizar la desafectación de los accesos a la información y equipamiento físico del organismo.

El/La Responsable del área de la Seguridad Edilicia:

- Cubrirá los requerimientos ambientales que permitan que los recursos informáticos del organismo funcionen en forma segura. Estas actividades deberán ser coordinadas conjuntamente con el Responsable de Gestión Informática.
- Deberá definir e implementar acciones de mantenimiento edilicias, puestos de trabajo y oficinas en las cuales se ubiquen equipos de procesamiento de la información, donde se almacene o archive información ya sea en el formato papel, o digital.
- Deberá atender tareas relativas a la seguridad y controles de acceso físico al ámbito del Ministerio de Educación de la Nación.

El/La Responsable del área Legal o Jurídica:

- Verificará el cumplimiento de la PSI, acuerdos, contratos y otras documentaciones del organismo con los empleados y terceros.
- Trabajará conjuntamente con el Responsable de la Unidad de Auditoría Interna concernientes a la generación de contratos con proveedores de servicios de tecnología y cualquier proveedor de bienes o servicios cuya actividad afecte directa o indirectamente a los activos de información, la obligatoriedad del cumplimiento de la PSI y de toda normativa, procedimientos y practicas relacionadas que de ella emanen.

El/La Responsable de la Unidad de Auditoría Interna:

- Realizará las prácticas periódicas de auditoría sobre los sistemas y actividades vinculadas con la tecnología de información.

Los Responsables de las Unidades Organizativas:

- Deberán conocer, cumplir y dar a conocer al personal que tienen a su cargo, las PSI, normativas, procedimientos y prácticas relacionadas que surjan de la misma.

5.4. 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 no divulgación. Así mismo, deben cumplir con toda la 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 terceros que se relacionen de alguna manera con su información, independientemente del tipo de formato en el cual dicha información se encontrare.

5.5. Acceso al trabajo remoto

El trabajo remoto utiliza una tecnología de comunicación por la cual permite al personal trabajar de manera remota desde un lugar externo al Ministerio que posea acceso a internet.

El trabajo remoto deberá ser solicitado por el/la Responsable de la Unidad Organizativa o superior jerárquico correspondiente, a la cual pertenezca el/la usuario/a al Director de Gestión Informática mediante una comunicación oficial a través de la plataforma GDE.

La Dirección de Gestión Informática (DGIN) analizará el pedido y adoptará las medidas que correspondan en materia de seguridad de modo de cumplir con la política, normas y procedimientos existentes.

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

a) Los requerimientos de seguridad de comunicaciones, tomando en cuenta las necesidades 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.
b) La amenaza de acceso no autorizado a información o recursos por parte de otras personas que utilizan el lugar, como por ejemplo familiares y amigos.
c) Evitar la instalación / desinstalación de software no autorizado por el Ministerio en los dispositivos utilizados para el teletrabajo, dado que los mismos son otorgados por el organismo para tal fin, salvo caso contrario en que la DGIN autorice el uso del dispositivo propiedad de un tercero, caso en el cual el/la usuario/a deberá comprometerse mediante un acuerdo de confidencialidad o no divulgación.
d) Definir el trabajo permitido, el horario de conexión, 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 servicios a los cuales el trabajador remoto está autorizado a acceder.
e) Proveer de un adecuado equipo de comunicación, con inclusión de métodos para asegurar el acceso remoto.
f) Definir normas sobre el acceso de terceros al equipamiento e información.
g) Realizar la anulación de las autorizaciones, derechos de acceso y devolución del equipo, para el caso de que hayan sido provistos por el organismo, cuando finalicen las actividades remotas.
h) Solicitar al usuario un consentimiento sobre las normas a efectuar durante el transcurso en que dure su condición de trabajo remoto en cuanto a materia de seguridad y política de uso de los activos de información.

6. SEGURIDAD INFORMATICA DE LOS RECURSOS HUMANOS

6.1. Objetivo

Dado que 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 el desarrollo de sus funciones en cuanto a seguridad y confidencialidad de la información, se instruirá sobre el mismo y se definirán sanciones que se aplicarán en caso de incumplimiento en alguna de las políticas desarrolladas.

Se detallan los objetivos principales:

Reducir los riesgos de error humano, ilícitos e impericias dadas por el uso inadecuado de las instalaciones, recursos y acceso no autorizado de la información.

Dar a conocer las responsabilidades del personal desde su etapa de reclutamiento en materia de seguridad. Las mismas serán incluidas en los acuerdos de confidencialidad a firmarse y serán verificados su cumplimiento durante el desempeño del personal como agentes del organismo, cualquiera sea su modalidad de contratación o situación de revista.

Concientizar que las/los usuarias/os estén al corriente de las amenazas y vulnerabilidades de seguridad de la información y que se encuentren instruidos para que respalden las PSI durante la realización de sus funciones.

6.2. Responsabilidad

EL/La Responsable de la Dirección de Recursos Humanos deberá incluir las funciones relativas a la seguridad de la información en las descripciones de los puestos de las/los empleadas/os, informar a todo el personal ingresante al organismo de sus obligaciones respecto del cumplimiento de la PSI y gestionar los Compromisos de Confidencialidad para con todo el personal independientemente de la modalidad de contratación o fuente de financiamiento.

En los casos en los cuales, el tipo de contratación sea por fuentes externas al organismo, Los/Las Responsables de las distintas Unidades Organizativas serán los responsables de informar a la Dirección de Recursos Humanos, el personal que tienen bajo su cargo y el tipo de contratación cada vez que efectúe una modificación.

6.3. Control y Verificación del Personal para contratar

La dirección de Recursos Humanos deberá llevar a cabo controles de verificación del personal al momento de la solicitud del puesto de trabajo. Dichos controles deberán incluir aspectos como la acreditación de identidad, confirmación de títulos académicos y profesionales mencionados por el postulante y antecedentes penales entre otros.

6.4. 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 la Dirección de Recursos Humanos.

Mediante el compromiso de confidencialidad el empleado declarará conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo. Estas actividades serán detalladas para su conocimiento y notificadas a fin de no violar el derecho de privacidad del empleado. Los términos y condiciones de empleo establecerán la responsabilidad del/la empleado/a en materia de seguridad de la información. En los casos en los cuales corresponda, los términos y condiciones de empleo establecerán que estas responsabilidades se entenderán más allá de los límites de la sede del Ministerio y del horario laboral.

Los derechos y obligaciones de la/el empleada/o relativos a la seguridad de la información, en relación con las leyes de propiedad intelectual o protección de datos, deben estar aclarados e incluidos en los términos y condiciones laborales.

El responsable de la Dirección de Recursos Humanos desarrollará un procedimiento para la notificación inicial del compromiso de confidencialidad por parte de la totalidad del personal como también deberá tener en cuenta las notificaciones en caso de modificación del texto compromiso.

6.5. Controles durante la contratación

La dirección de Recursos Humanos deberá asegurar que las/los usuarias/os, empleadas/os, contratistas/os y terceras partes estén al tanto de las amenazas e inquietudes de la seguridad de la información, sus responsabilidades y obligaciones para apoyar la política de seguridad de la información del organismo durante todo el transcurso de su actividad laboral y para reducir el riesgo de error humano.

Por lo cual, la dirección de Recursos Humanos deberá 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 el organismo.

Teniendo en cuenta los siguientes aspectos:

- Informar adecuadamente respecto a los roles y responsabilidades antes de que el organismo le otorgue el acceso a información sensible o a sistemas de información independientemente del formato en el cual este se encuentre.
- Motivar el cumplimiento de las PSI.
- Fomentar un nivel de conciencia sobre la seguridad de la información, acorde a los roles y responsabilidades.
- Cumplir con las condiciones y términos del empleo, los cuales incluyen las PSI, políticas de uso, métodos y buenas prácticas de trabajo.
- Fomentar la capacitación en materia de seguridad de la información.

6.6. Sanciones: Proceso Disciplinario.

Se seguirá el proceso disciplinario formal contemplado en las normas estatutarias, escalafonarias y convencionales que rigen al personal de la APN para las/los empleadas/os que violen la Política, Normas y Procedimientos de Seguridad del organismo.

6.7. Desvinculación o cambio en el puesto de trabajo

Cuando el egreso se produjere por alguno de los causales establecidos en la normativa vigente, se controlará la devolución en buen estado de los equipos tecnológicos asignados como también se eliminarán todos los permisos de acceso a la información.

La dirección de Recursos Humanos informará inmediatamente de realizada la baja del agente a la dirección de Gestión Informática para que realice las acciones pertinentes.

Para el caso de desvinculación del personal, la DGIN revisará los derechos de acceso asociados con los sistemas y servicios de información a fin de removerlos.

En cuanto las modificaciones de funciones por cambios en el puesto de trabajo, una vez notificada la DGIN por parte de RRHH, se tomarán las medidas necesarias para restringir todos los accesos de información, tanto accesos lógicos como físicos, no correspondientes aplicando el principio del mínimo privilegio.

Para nuevos accesos en el nuevo puesto de trabajo, se deberán solicitar mediante comunicación oficial a través de la plataforma GDE a el/la directora/director de Gestión Informática y deberá ser solicitado por el/la responsable de la unidad organizativa en la cual presta sus nuevas funciones el agente.

Tras la desvinculación contractual, todos los/las empleados/as, contratistas y usuarias/os de terceras partes deben devolver todos los activos de la organización que se encuentren en su poder (ya sea software, documentos, equipamiento, dispositivos móviles, tarjetas bancarias, tarjetas de ingreso, etc.) De igual manera, si los mismos tienen conocimiento de contraseñas para cuentas que continuarán activas, éstas deberán ser modificadas tras la finalización o cambio de empleo, contrato o acuerdo.

7. GESTION DE ACTIVOS

Se entiende como activo de información a cualquier información o sistema relacionado con el tratamiento de la misma, que tenga valor para el organismo. Pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones.

Dichos activos de información deben ser clasificados según el nivel de sensibilidad y criticidad que contienen o bien de acuerdo con la funcionalidad que cumplen y catalogados en función a ello, con el objeto de establecer los mecanismos en que han de ser tratados y protegidos.

Se tendrán en cuenta algunos aspectos como el factor tiempo, dado que la clasificación de la información podría verse modificada durante el transcurso del tiempo hasta el punto de dejar de ser sensible y crítica.

De igual modo durante el transcurso del tiempo, la información podría adoptar diversas formas, encontrarse tanto integrada en sistemas informáticos como encontrarse externamente, almacenada en dichos sistemas o en medios extraíbles, transmitida e impresa o escrita en papel, como también grabada como video o audio. Estos diversos formatos en los cuales se puede contener información serán contemplados para garantizar los principios de la seguridad de la información (confidencialidad, integridad y disponibilidad).

En los casos en los cuales la información podría pasar a ser obsoleta, se contemplará su eliminación mediante una destrucción segura.

7.1. Objetivos

Clasificar la información para señalar la sensibilidad y criticidad de los mismos, a fin de establecer niveles de protección y realizar el tratamiento adecuado.

7.2. Inventario de Activos

La DGIN identificará los activos importantes asociados a cada sistema de información, sus respectivos propietarios y su ubicación. El responsable de cada unidad organizativa deberá informar sobre los activos de información que utiliza y ante cualquier modificación que se produzca deberá notificar al Coordinador de Seguridad de la Información a fin de modificar o establecer nuevas políticas, procedimientos o normas asociadas a la misma.

7.3. Clasificación de la Información

Para clasificar un activo de información, se evaluarán las 3 características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad.

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

7.3.1. Confidencialidad

1: Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleada/o del organismo o no. **PUBLICO**

2: Información que puede ser conocida y utilizada por todos/as los/las empleados/as 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 empleados/as, 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 empleados/as, generalmente de la alta dirección del Ministerio, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves a éste, al Sector Publico Nacional o a terceros/as. **RESERVADA-SECRETA**

7.3.2. 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, Sector Público Nacional o terceros/as.

7.3.3. 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.

Dentro de las pérdidas mencionadas se contemplan las mensurables (materiales) y las no mensurables (imagen, valor de la información, obligaciones contractuales o públicas, disposiciones legales, etc.)

Se asignará a la información un valor por cada uno de los criterios antes mencionados para luego clasificarlos dentro 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).

La/el propietaria/o de la información puede asignar o cambiar su nivel de clasificación, cumpliendo con los siguientes requisitos:

- Asignarle una fecha de efectividad a la información.
- Comunicarlo 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 propietario/a identificará los recursos asociados, tales como sistemas, equipamiento, servicios, etc. Y los perfiles asociados a los mismos que deban tener privilegios de acceso.

Se definirán procesos para el rotulado y manejo de información de acuerdo con el esquema de clasificación definido. Los mismos contemplarán los activos de información tanto en formatos físicos como electrónicos e incorporarán las siguientes actividades de procesamiento: copia, almacenamiento, transmisión por correo, fax, correo electrónico, transmisión oral mediante telefonía fija, móvil, correo de voz o contestadores automáticos, transmisión a través de mecanismos de intercambio de archivos mediante ftp, almacenamiento masivo remoto.

7.4. Eliminación de medios de información

Se deben 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:

- Documentos en papel
- Voces, videos u otras grabaciones
- Papel carbónico
- Informes de salida
- cintas magnéticas
- discos u otros medios removibles
- almacenamiento óptico
- listados de sistemas
- datos de prueba
- documentación de sistemas

8. AUTENTICACIÓN, AUTORIZACIÓN Y CONTROL DE ACCESOS

Para impedir el acceso no autorizado a los sistemas de información se implementarán procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos estarán documentados, comunicados y controlados en cuanto a su cumplimiento. Los cuales comenzarán a implementarse con los nuevos usuarios solicitados a partir del 1 de enero del 2023.

Dichos procedimientos comprenderán todas las etapas del ciclo de vida de los accesos de las/los usuarias/os de todos los niveles, desde la generación de nuevos usuarios hasta la privación final de derechos.

8.1. Objetivos

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

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

Otorgar mecanismos de seguridad de la información al utilizar dispositivos móviles para el uso de trabajo remoto.

Concientizar a los usuarios respecto de su responsabilidad frente al uso de contraseñas y dispositivos tecnológicos.

8.2. Política de control de accesos

La Dirección de Gestión Informática, será la encargada de:

- Definir normas y procedimientos para la gestión de accesos de los sistemas, bases de datos y servicios de información.
- Analizar e implementar los métodos de autenticación y control de acceso definidos en los sistemas, base de datos y servicios.
- Establecer los procesos para el acceso, uso y control de las instalaciones de procesamiento de la información.
- Definirá las pautas de acceso a internet en puertos específicos por fuera del estándar, su prohibición y su habilitación en casos excepcionales y mediante la debida justificación a la apertura de estos, la cual deberá ser solicitada mediante comunicación oficial a través de la plataforma GDE.

- Realizar la asignación, modificación y control de los privilegios de usuarios utilizando el principio de “necesidad de saber”.
- Implementar procedimientos para la activación y desactivación de derechos de acceso a la red del organismo.

Las/Los propietarias/os de la información, se encargarán de:

- Aprobar y solicitar la asignación de privilegio de usuarios e informar los cambios cuando resulte pertinente ya seas por baja o cambio de área o funciones.
- 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 eventos y actividades de usuarios a ser registrados en los sistemas de procesamiento de su incumbencia y la periodicidad de revisión.

8.3. Reglas de Gestión de Acceso

Las reglas de control de acceso especificadas deben:

- Indicar expresamente si las reglas son obligatorias u optativas
- 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”
- 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.

8.4. Administración de Gestión de Usuarios

8.4.1. Registro de Usuarios

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

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

Verificar que el usuario posee autorización del propietario de la información para el uso del sistema, base de datos o servicio de información.

Verificar que el nivel de acceso otorgado al usuario sea adecuado según el propósito de sus funciones y sea coherente con la PSI como por ejemplo que no comprometa la segregación de funciones.

Entregar a los usuarios un detalle escrito sobre sus derechos de acceso.

Requerir que los usuarios firmen declaraciones señalando que comprenden y aceptan las condiciones para el acceso.

Garantizar que los proveedores de servicios no otorguen el acceso hasta que se hayan completado los procedimientos de autorización. En todo caso contractual con terceros, la DGIN deberá intervenir y/o tener conocimiento sobre los servicios prestados a las distintas unidades organizativas.

Mantener un registro formal de las personas registradas para el uso de los distintos servicios. Por lo cual se requiere para su cumplimiento el trabajo coordinado por parte de la DRRHH y de la DGIN para mantener dicho registro actualizado.

Cancelar de manera inmediata los privilegios de acceso d ellos usuarios que modificaron sus funciones, o de aquellos a los cuales se les revocó la autorización, se desvincularon del organismo o sufrieron la pérdida o robo de sus credenciales de acceso.

Efectuar revisiones periódicas con el objeto de:

- Cancelar cuentas de usuario redundantes, en caso de que existieran.
- Bloquear cuentas inactivas por más de 180 días.
- Eliminar las cuentas inactivas por más de 365 días.

Revisar periódicamente la lista de incidencias de las cuentas de usuario con el objeto de detectar los riesgos para evaluar las acciones pertinentes y en base a la clasificación de distintos niveles:

- Para riesgo bajo, notificar al usuario por mail institucional y proceder al bloqueo de la cuenta en caso de falta de respuesta luego de transcurrido los 5 días hábiles.
- Para riesgo medio, notificar al usuario por mail institucional y proceder al bloqueo de la cuenta en caso de falta de respuesta luego de transcurrido los 2 días hábiles.
- Para riesgo alto, proceder al bloqueo de la cuenta de forma inmediata.
- Para todos los casos el desbloqueo de cualquier cuenta de usuario se realizará por comunicación oficial mediante la plataforma GDE al/la director/a de Gestión Informática.

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

8.4.2. Gestión de privilegios

Se procederá a limitar y controlar la asignación y uso de privilegios, debido a que su uso inadecuado resulta ser el factor más importante que contribuye a la falla de los sistemas.

Para los sistemas multiusuario que requieren protección contra accesos no autorizados se preverá una asignación de privilegios controlada mediante un proceso de autorización formal, tomando en consideración los siguientes pasos:

a) Identificar los privilegios asociados a cada producto del sistema, como lo son el sistema operativo y los sistemas de gestión de bases de datos y aplicaciones.
b) Asignar los privilegios a individuos sobre la base de la necesidad de uso y evento por evento, como lo es el requerimiento mínimo para su rol funcional.
c) Mantener un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no serán otorgados hasta que se haya completado el proceso formal de autorización.
d) Se mantendrá un período de vigencia para el mantenimiento de los privilegios (según el uso que se les dará a los mismos) luego serán revocados.

Los propietarios de la información serán quienes deberán aprobar la asignación de privilegios a los usuarios, solicitar su implementación e indicar los recursos a acceder.

8.4.3. Gestión de contraseñas

La asignación de contraseñas se controlará mediante un proceso de administración formal y respetando los siguientes pasos:

a) Requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto y las contraseñas de los grupos de trabajo, para el caso de que existieran, exclusivamente entre los miembros del grupo. Dicha declaración podrá encontrarse incluida en el Acta Compromiso de Confidencialidad.
b) Garantizar, dentro de lo posible y siempre que la tecnología aplicada lo permita, que los usuarios cambien sus claves iniciales que les han sido asignadas la primera vez que ingresan al sistema, como el caso del correo institucional
c) Las contraseñas provisoras que se asignan cuando los usuarios olvidan su contraseña, sólo se entregarán una vez acreditada la identidad del mismo.
d) Generar contraseñas provisorias seguras para otorgar a los usuarios. Se debe evitar la participación de terceros o el uso de mensajes de correo electrónico sin protección (texto plano) en el mecanismo de entrega de contraseñas y los usuarios deberán dar acuse de recibo cuando lo reciban.
e) Almacenar las contraseñas sólo en sistemas informáticos protegidos.
f) Utilizar otras tecnologías de autenticación y autorización de usuarios, como ser la biométrica (huellas, facial, etc.), verificación de firma, uso de autenticadores de hardware (tarjetas de circuito integrado), etc.
g) Configurar los sistemas para que:
    - Las contraseñas sean “password fuerte” y tengan una cantidad mínima a definir de caracteres.
    - Suspendan o bloqueen permanentemente al usuario luego de una cantidad a definir máxima de intentos fallidos de autenticación. Se pedirá la rehabilitación ante quien corresponda mediante mecanismos formales.
    - Solicitar cambio de clave en intervalos regulares. Dicho intervalo será a definir.
    - Impedir que las últimas contraseñas sean reutilizadas. La cantidad mínima será a definir.
    - Establecer el tiempo de vida mínimo para las contraseñas. El tiempo será a definir.
    - Los parámetros antes mencionados serán definidos en un anexo por parte de la DGIN, el cual se actualizará con una frecuencia no mayor a 1 (un) año.

8.4.4. Administración de contraseñas críticas

Dada la amplitud en los diferentes ambientes de procesamiento, existen cuentas de usuarios con los cuales es posible efectuar tareas críticas tales como la instalación de plataformas o sistemas, habilitación de servicios, actualización de software, configuración de componentes informáticos, etc. Las cuentas mencionadas que no son de uso habitual, sino que pueden ser utilizadas ante la necesidad específica de realizar tareas que lo requieran y deben ser protegidas por contraseñas con un nivel mayor de complejidad a la habitual, deberán regirse por procedimientos que contemplen lo siguiente:

- Definir las causas que justifican el uso de contraseñas críticas, así como el nivel de autorización requerido.
- Resguardar debidamente las contraseñas y los nombres de las cuentas críticas.
- Registrar el uso de contraseñas críticas, así como el responsable que las utiliza.
- Se registrarán todas las actividades realizadas con las cuentas críticas para luego realizar su revisión. Dicho registro debe ser revisado posteriormente y permanecer para disposición de la UAI en caso de que lo requiera.

8.4.5. Revisión de derechos de acceso de usuarios

Para mantener un eficaz control del acceso a los datos y servicios de información, el propietario de la información deberá en intervalos regulares de seis (6) meses, revisar los derechos de acceso de los usuarios mediante un proceso formal donde contemplará los siguientes controles:

- Revisar los derechos de acceso de los usuarios a intervalos de seis (6) meses.
- Revisar las autorizaciones de privilegios especiales de derechos de acceso a intervalos tres (3) meses.
- Revisar las asignaciones de privilegios a intervalos de seis (6) meses a fin de garantizar que no se obtengan privilegios no autorizados.

8.5. Responsabilidad del usuario

A fin de evitar el acceso de usuarios no autorizados, evitar poner en peligro la información, y evitar el robo de información y los medios de procesamiento de la información es esencial fomentar sobre la responsabilidad y la cooperación de los usuarios autorizados para una seguridad efectiva.

Por lo cual los usuarios 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 del usuario.

Deberán implementar escritorios y pantalla limpios a fin de reducir el riesgo de acceso no autorizado o daño a papeles, medios y medios de procesamiento de información.

Dado que las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información, se deberán tener en cuenta las siguientes directivas:

a) Los usuarios deberán seguir las buenas prácticas de seguridad en la selección y uso de contraseñas.
b) Mantener las contraseñas en secreto
c) Pedir el cambio de contraseña siempre que exista un posible indicio de que la cuenta de usuario se encuentra comprometida.
d) Seleccionar contraseñas de calidad según las prescripciones informadas por la DGIN:

- Fáciles de recordar
- No se encuentren basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona.
- No tenga caracteres idénticos consecutivos, o grupos totalmente numéricos o totalmente alfabéticos.
- Cambiar contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.
- Cambiar las contraseñas provisorias en el primer inicio de sesión (“log on”).
- Evitar incluir contraseñas en los procesos automatizados de inicio de sesión.
- Notificar a la DGIN, de acuerdo con lo establecido en el ítem de Gestión de Incidentes de Seguridad, cualquier incidente relacionado con sus contraseñas, ya sean pérdidas, robos o indicio de pérdida de confidencialidad.

Para todos los usuarios que necesitan acceder a múltiples servicios o plataformas y requieran mantener múltiples conexiones, deberán acceder con contraseñas diferentes para cada uno de los servicios. En aquellos casos en que el usuario requiera utilizar una única contraseña para los diversos servicios deberá notificarlo a la DGIN (quien lo someterá a análisis)

En cuanto a los equipos desatendidos o desafectados que se encuentran ubicados físicamente en áreas de usuarios serán los mismos usuarios quienes deberán garantizar que dicho equipamiento sea protegido adecuadamente.

Los equipos que se encuentren instalados en áreas de usuarios, como ser las estaciones de trabajo, requieren una protección contra accesos no autorizados cuando los mismos se encuentren sin uso. Para lo cual los usuarios deberán concluir las sesiones activas al finalizar las tareas, a menos que puedan protegerse mediante un mecanismo de bloqueo adecuado, como un protector de pantalla protegido con contraseña.

8.6. Control de Acceso a Sistemas y Aplicaciones mediante el acceso a la Red

8.6.1. Política de utilización de los servicios de red

Las conexiones no seguras a los servicios de red pueden afectar la operatoria del organismo, por lo cual, desde la DGIN se controlará el acceso a los servicios de red tanto internos como externos, con el propósito de garantizar que los usuarios que tengan acceso a las redes y a los servicios ofrecidos por el organismo no comprometan la seguridad de los mismos.

La DGIN tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal del titular de una unidad organizativa que lo solicite para personal a su cargo.

Este control es importante para las conexiones cuyo acceso a aplicaciones procesan información clasificada o aplicaciones críticas, o a usuarios que utilicen el acceso desde sitios de alto riesgo, como ser áreas públicas o externas que se encuentren fuera de la administración y control del Ministerio.

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

- Identificar las redes y servicios a los cuales se permite el acceso.
- Realizar normas y procedimientos de autorización para determinar las personas, las redes y servicios a los cuales se le otorgará el acceso.
- Establecer controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios.

8.6.2. Acceso a la Red

Las redes se encuentran diseñadas para permitir el máximo alcance de distribución de recursos y flexibilidad en la elección de la ruta a utilizar. Características que pueden ofrecer oportunidades para el acceso no autorizado a aplicaciones, o servicios de información. Por lo cual las comunicaciones deben ser controladas.

Desde la DGIN, se implementarán las acciones correspondientes a fin de limitar las opciones de elección de la ruta entre la terminal de usuario y los servicios a los cuales éste se encuentra autorizado a acceder.

A continuación, se enumeran aspectos a considerar:

- Asignar números telefónicos o líneas, en forma dedicada.
- Evitar la navegación ilimitada por la red.
- Establecer conexión automática de puertos a gateways de seguridad o firewalls.
- Imponer el uso de gateways de seguridad o firewall a usuarios externos de la red.
- Controlar activamente las comunicaciones con origen y destino autorizados a través de un Gateway de seguridad, firewall o sistema de autenticación.
- Restringir el acceso a redes estableciendo dominios lógicos separados, tales como redes privadas virtuales.
- Conexiones del tipo VPN Ipsec ofrecidos por la DGIN, ya seas mediante hardware o software controlado y bajo un sistema de licencias actualizados.

8.6.3. Autenticación de usuarios para conexiones externas

Las conexiones externas son un punto focal para accesos no autorizados a la información del organismo. Por lo cual, el acceso de usuarios remotos se encontrará sujeto al cumplimiento de procedimientos de autenticación. Dado que existen diferentes métodos de autenticación, los cuales algunos brindan un mayor nivel de protección que otros, la DGIN realizará un análisis de riesgos a fin de determinar el mecanismo de autenticación correspondiente según sea el caso.

La autenticación de usuarios remotos podrá llevarse a cabo utilizando:

a) Un método de autenticación físico (tokens) para lo cual deberá implementarse un procedimiento que incluirá la asignación de la herramienta de autenticación, registro de los poseedores de autenticadores, mecanismo de recupero del bien al momento de la desvinculación del personal y un método de revocación de acceso del autenticador, en caso de comprometida la seguridad del mismo.
b) Un protocolo de autenticación (desafío/respuesta), para lo cual deberá implementarse un procedimiento que incluya el establecimiento de las reglas

con el usuario y un establecimiento de un ciclo de vida de las reglas para su renovación.

Para todos los casos los servicios autorizados serán los ofrecidos por la DGIN.

8.6.4. Protección de puertos

La dirección de Gestión Informática restringirá los puertos de uso, bloqueando aquellos considerados como puntos focales para posibles ataques y manteniendo solamente abiertos aquellos que sean estrictamente necesarios.

Para el caso en el cual una unidad organizativa deba acceder a un puerto que se encuentre cerrado, deberá dirigir su solicitud a la DGIN mediante una comunicación oficial, indicando la dirección ip y/o url al igual que la justificación que arbitra la apertura de dicho puerto. La solicitud será sujeta a evaluación por la DGIN.

8.6.5. Subdivisión de redes

La dirección de Gestión Informática para controlar la seguridad en la red interna del organismo dividirá la misma en segmentos lógicos separados. Esta separación se producirá mediante la configuración de redes privadas virtuales (VLANS) a fin de minimizar la superficie de ataque.

Para la división lógica de la red, se tomarán en cuenta criterios como ser: los requerimientos de seguridad comunes a ciertos grupos de dispositivos vinculados a una misma red, mayor exposición de un grupo a peligros externos, separación física u otros criterios de segregación o aglutinamiento.

8.7. Control de Acceso al Sistemas Operativo

Con el objeto de evitar el acceso no autorizado a los sistemas operativos, se utilizarán mecanismos de seguridad con capacidad de:

a) Autenticar a los usuarios autorizados, 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 privilegios especiales del sistema.
d) Emitir alarmas cuando las políticas de seguridad del sistema sean violadas.
e) Proporcionar medios de autenticación apropiados.
f) Restringir el tiempo de conexión de los usuarios ante la falta de actividad.

8.7.1. Identificación y Autenticación de usuarios

Todos los usuarios deben tener un identificador único (ID de usuario) para su uso personal exclusivo, de forma tal que las actividades puedan ser rastreadas con posterioridad, con el fin de garantizar la trazabilidad de las transacciones. Los ID no deben dar ningún indicio del nivel de privilegio otorgado.

Para el caso en que la autenticación utilice algún medio físico (autenticadores de hardware), se deberán implementar procedimientos que incluyan:

a) Asignar la herramienta de autenticación
b) Registrar los poseedores de autenticadores.
c) Recupero del autenticador al momento de la desvinculación del personal.
d) Revocar el acceso del autenticador para el caso en el que se vea comprometida la seguridad del mismo.

8.7.2. Administración de Contraseñas

Dado que las contraseñas constituyen uno de los principales medios de validación de la autoridad de un usuario para acceder a un servicio informático, los sistemas de administración de contraseñas deben constituir una herramienta eficaz e interactiva que garantice la calidad de las mismas:

Se deberá:

a) Imponer el uso de contraseñas individuales.
b) Permitir que los usuarios cambien sus propias contraseñas individuales e incluir un procedimiento para contemplar errores de ingreso.
c) Imponer una selección de contraseñas de calidad, según el punto 8.5.d.
d) Imponer los cambios de contraseñas cuando se detecten que podrían haber sido vulneradas.
e) Evitar mostrar las contraseñas en pantalla cuando sean ingresadas.

9. USO DE HERRAMIENTAS CRIPTOGRAFICAS

Se establecerá el uso de la criptografía para asegurar la información, en el resguardo de las contraseñas, en el almacenamiento de las copias de seguridad, en las conexiones de trabajo remoto y en las comunicaciones de los servicios expuestos a internet, tales como SSL y TLS.

9.1. Firma Digital

Las firmas digitales proporcionan un medio de protección de la autenticidad e integridad el cual se aplica a cualquier documento electrónico.

Su implementación se basa en 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 resguardar las claves privadas para proteger la confidencialidad de la información.

De igual manera es importante proteger la integridad de la clave pública, la cual se provee mediante un certificado.

Las firmas y certificados digitales se rigen bajo la Ley de Firma Digital 25.506, los decretos 892 del 1° de noviembre del 2017 y 182 del 11 de marzo de 2019 y sus normas modificatorias o complementarias, las cuales determinan las condiciones bajo las cuales una firma digital es legalmente válida.

En cuanto al término no repudio, es uno de los más importantes en la firma digital.

El **no repudio** provee garantía al receptor de una comunicación en cuanto a que el mensaje fue originado por el emisor y no por alguien que se hizo pasar por este. Además, previene que el remitente o emisor del mensaje afirme que él no envió el mensaje.

Por lo cual, al firmar digitalmente un documento, este se encuentra vinculado exclusivamente a la persona firmante y la identifica unívocamente.

En algunos casos podría ser necesario establecer en el organismo la firma digital, para lo cual deberán implementarse los procesos basados en el punto 8.7.1

9.2. Múltiple factor de autenticación

El organismo deberá implementar siempre y cuando le sea posible, autenticación de múltiples factores (MFA) para sus sistemas o servicios.

La autenticación de múltiples factores es un componente de gestión de acceso que requiere que los usuarios demuestren su identidad utilizando al menos dos factores de verificación diferentes antes de obtener el acceso a un sitio web, servicio de correo, aplicación u otro recurso en línea.

A continuación, se detallan los factores de autenticación que se utilizan en MFA

Factor de conocimiento: “Algo que se Conoce” como suele ser una contraseña, un PIN, una frase de paso o un conjunto de preguntas de seguridad y sus correspondientes respuestas que sólo conoce la persona.

Factor de posesión: “Algo que se posee” tales como tokens, tarjetas inteligentes que generan contraseñas de un solo uso o código de acceso (OTP), como también la instalación de una aplicación de autenticación, la cual genera claves de seguridad OTP.

Factor de inherencia: “Algo que usted es” tales como lo son los datos biométricos que pueden abarcar desde las huellas dactilares, los escaneos de retina, el reconocimiento facial, reconocimiento de voz o hasta los comportamientos de un individuo como lo son la intensidad o la rapidez con que la persona teclea o desliza el dedo en pantalla.

Se deberán utilizar al menos dos tecnologías diferentes para lograr la autenticación multifactor, de al menos dos grupos tecnológicos diferentes para el proceso de autenticación.

9.3. Cifrado en los dispositivos de almacenamiento

Siempre y cuando sea posible, el organismo deberá implementar mecanismos de cifrado en las unidades de almacenamiento, como por ejemplo Bitlocker.

Pudiendo implementar, siempre y cuando la tecnología instalada lo permita, un dispositivo de hardware (chip) llamado TPM (Trusted Plataform Module) que se encuentra integrado en la placa mother del servidor o computadora. El TPM genera claves de cifrado y almacena en su memoria parte de dicha clave y parte en el disco; el TPM detecta cambios de hardware de forma que un atacante no pueda acceder al disco manipulando el hardware de la computadora mientras el sistema se encuentra sin conexión.

Para los casos en los cuales no fuera posible utilizar TPM, se podrá implementar unidades flash USB o integrar dicha solución con los servicios de dominio de Active Directory (AD DS) para proporcionar una administración centralizada de claves.

10. FISICA Y AMBIENTAL

A fin de minimizar los riesgos por daños e interferencias a la información y brindar continuidad en las operaciones del organismo, se distinguen algunos conceptos a tener en cuenta tales como la protección física de los accesos, la protección ambiental y el transporte, protección y mantenimiento del equipamiento involucrado a la documentación concerniente.

Mediante el establecimiento de perímetros de seguridad en áreas restringidas; tales como lo son las instalaciones de procesamiento de información crítica o sensible del organismo; facilitará la implementación de controles a dichas áreas de accesos físicos no autorizados.

Mediante el control de los factores ambientales en las áreas de procesamiento de información, permitirá garantizar el correcto de dicho equipamiento como también minimizar las interrupciones de servicio.

En cuanto a 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.

10.1. 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 utilizará perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información, de suministro de energía eléctrica, de aire acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información.

Un perímetro de seguridad se encuentra delimitado por una barrera, por ejemplo, cercada por una pared, con una puerta de acceso controlado por dispositivo de autenticación, o con puerta bajo llave y/o candado, o mediante un escritorio u oficina de recepción atendidos por personal.

En cuanto a la fortaleza de cada barrera, en las áreas donde se realice procesamiento de información, deberá ser definida conjuntamente por la Dirección de Gestión Informática y la Dirección de Servicios y Mantenimiento.

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) Para aquellos casos en que las áreas restringidas no sean de procesamiento de información, como ser los accesos de ingreso a las sedes, se deberá verificar la existencia de un área de recepción atendida por personal. El acceso a dichas áreas y edificios debe estar restringido exclusivamente al personal autorizado. En cuanto a los ingresos de invitados o terceros ajenos al organismo, se deberá implementar un procedimiento de autorización que habilite su ingreso. 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 la Dirección de Servicios y Mantenimiento deberá 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

10.2. Controles físicos de entrada

Las áreas protegidas se deben resguardar mediante el empleo de controles de acceso físico, determinados por la Dirección de Recursos Humanos, La Dirección de Servicios y Mantenimiento y la Dirección de Gestión Informática (si el medio de control fuera mediante algún recurso tecnológico o el acceso fuera hacia un centro de procesamiento de datos), 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.

10.3. 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 y separada del área asegurada. Los suministros a granel como papelería no deben almacenarse en el área asegurada;

b) Se debe proporcionar equipo contraincendios ubicado adecuadamente.

10.4. 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 acceso a los mismos:

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.

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

10.5. Instalaciones de suministro eléctrico

El recurso tecnológico considerado crítico para mantener la operatoria del organismo, como ser servidores, activos de red, accesos biométricos, debe estar protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas.

Para asegurar la continuidad del suministro de energía, se deben contemplar las siguientes medidas de control:

a) 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 sobre la detección de una falla en el suministro de energía. Dicha alerta permitirá que ante un incidente se proceda a un apagado controlado. Los equipos de UPS deben ser inspeccionados y probados periódicamente para asegurar que funcionan correctamente y que tienen la autonomía requerida.

b) Montar un generador de respaldo para los casos en que el procesamiento deba continuar ante una falla prolongada en el suministro de energía y sea de carácter crítico. 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 Dirección de Servicios y Mantenimiento conjuntamente con la Dirección de Gestión Informática. 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 de acuerdo con 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.

10.6. 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 canalizaciones metálicas independientes.

10.7. 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/la responsable de la dirección de Gestión Informática. El mismo deberá mantener un listado actualizado del equipamiento de la infraestructura desplegada.

b) Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento informático.

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.

10.8. Seguridad de los equipos fuera de las instalaciones

El uso de equipamiento destinado al procesamiento de información, que fuera utilizado fuera del ámbito del organismo debe ser autorizado por la/el responsable patrimonial. 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, ya seas contra daño o robo 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.

10.9. Políticas de Escritorios Limpios

Se debe adoptar 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 haya 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.

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.

11. SEGURIDAD OPERATIVA

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

Por lo cual se deberán definir procedimientos para el control de los procesos operativos documentados, los sistemas e instalaciones de procesamiento de información, y verificar su cumplimiento de forma tal que no afecten la seguridad de la información.

11.1. Documentación de los procedimientos operativos

Se deberá documentar y mantener actualizados los procedimientos operativos a fin de garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de información.

La documentación de dichos procedimientos deberá ser referida a las siguientes actividades:

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

11.2. Cambio en las operaciones

Se deberán definir procedimientos para el control de los cambios en el ambiente operativo y de las comunicaciones. Todo cambio debe ser evaluado en aspectos técnicos y de seguridad.

Se deberá llevar un registro con toda la información relevante de cada cambio implementado.

Los procedimientos de control de cambios contemplan los siguientes aspectos:

- Identificación y registro de cambios significativos
- Evaluación del posible impacto de dichos cambios
- Aprobación formal de los cambios propuestos
- Planificación del proceso de cambio
- Prueba del nuevo escenario
- Comunicación de detalles de cambios a todas las personas pertinentes

11.3. Planificación de la Capacidad

La dirección de Gestión Informática deberá 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. Se deberán tomar en cuenta los nuevos requerimientos de los sistemas, como también las tendencias actuales y futuras. Asimismo, deberá informar las necesidades detectadas a las autoridades competentes.

11.4. Separación de entornos de desarrollo, prueba y producción

Los ambientes de desarrollo, prueba y producción deben estar separados, siempre que sea posible, de manera física, y se deben definir y documentar las reglas para la transferencia de software desde el estado de desarrollo hacia el estado de producción.

Se deberán tener en cuenta los siguientes controles:

- Ejecutar el software de desarrollo y de producción en diferentes ambientes, equipos o directorios.
- Separar las actividades de desarrollo y prueba en entorno distintos.
- Impedir el acceso a los compiladores, editores y otros utilitarios del sistema en el ambiente de producción, cuando el mismo no sea indispensable para su funcionamiento.
- Utilizar sistemas de autenticación y autorización independientes para los distintos ambientes, así como perfiles de acceso a los sistemas.
- Prohibir a los usuarios compartir claves en los sistemas.

- Las interfaces de los sistemas deben identificar a que instancia se está realizando la conexión.
- El personal de desarrollo no debe tener acceso al ambiente de producción. En caso de que por necesidad el personal de desarrollo deba acceder, se establecerá un procedimiento para la autorización, documentación y registro de dichos accesos.

11.5. Protección contra código malicioso (malware)

Se deberán desarrollar procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios en los mismos.

Se deberán establecer políticas y procedimientos que contemplen las siguientes acciones:

- Prohibir la instalación y uso de software no autorizado por el Ministerio.
- Redactar procedimientos para evitar los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas, o por cualquier medio como ser dispositivos externos.
- Instalar y actualizar periódicamente el software antivirus y realizar análisis periódicos de las unidades de almacenamiento.
- Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles. Realizar dichas actualizaciones en entornos de pruebas.
- Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.
- Redactar normas de protección y habilitación de puertos de conexión de dispositivos móviles y sus derechos de acceso.

11.6. Resguardo de la información (Backup)

A fin de mantener la integridad y disponibilidad de la información y los medios de procesamiento de información, se deberán establecer procedimientos de respaldo de la información, y realizar prácticas de restauración de la misma.

Se deberán definir procedimientos para el resguardo de la información, que deben considerar los siguientes aspectos:

- Definir un esquema de rotulo de las copias de resguardo, que permita contar con toda la información necesaria para identificar cada una de ellas y administrarlas debidamente.
- Establecer un esquema de remplazo de los medios de almacenamiento de las copias de resguardo, una vez concluida la posibilidad de ser reutilizado.
- Almacenar en una ubicación remota las copias de resguardo de la información junto con los registros de éstos y los procedimientos documentados de recuperación, a una distancia suficiente.
- Asignar a la información de resguardo un nivel de protección física y ambiental.

- Probar de forma periódica los medios de resguardo mediante pruebas de recuperación.

11.7. Registro y Monitoreo

Se deberán detectar las actividades de procesamiento de información no autorizados.

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

Utilizar una bitácora de operador y registrar las fallas para asegurar que se identifiquen los problemas en los sistemas de información.

11.8. Registro de eventos

Se deben producir y mantener registros en los cuales se registren actividades, excepciones y eventos de seguridad de la información de las/los usuarias/os.

Se debe evaluar en los registros la siguiente información:

- Identificación de las/los usuarias/os
- Fechas, tiempos y detalles de los eventos principales, tales como inicio y cierre de sesión.
- Identidad del equipo o la ubicación si es posible.
- Registro de intentos de acceso al sistema exitosos y fallidos.
- Cambios en la configuración de los sistemas
- Uso de privilegios de usuario
- Uso de utilitarios y aplicaciones del sistema
- Archivos accedidos y tipos de acceso
- Alarmas ejecutadas por el sistema de control de accesos.

11.9. Sincronización de relojes

Se deberán mantener los equipos bajo una correcta configuración de los relojes, a fin de garantizar la exactitud de los registros de logs. De todos los sistemas. Se podrá utilizar un protocolo de sincronización de los relojes contra una fuente externa de dato.

11.10. Control sobre el desarrollo de software

Se deben definir los controles a realizar durante la implementación de los sistemas en producción, a fin de minimizar el riesgo de alteración de los mismos.

Toda aplicación desarrollada, ya sea por el organismo o por un tercero contratado deberá tener a un responsable designado.

Ni los analistas, ni los desarrolladores, ni quienes realicen el mantenimiento de las aplicaciones podrán tener acceso a los ambientes de producción.

Se deberán llevar registros de las actualizaciones realizadas y versionados.

La dirección de Gestión Informática designará en la función de “Project Manager” al personal que considere adecuado, quien cumplirá las siguientes funciones:

- Coordinar la implementación de modificaciones o nuevos programas en el ambiente de producción.
- Asegurar que los sistemas en el ambiente de producción sean los autorizados y aprobados de acuerdo a las normas y procedimientos vigentes.
- Controlar las modificaciones a impactar en el ambiente de producción, controlando previamente las pruebas realizadas en los ambientes de prueba.
- Rechazar toda implementación, en caso de encontrar errores y/o ante la falta de la documentación necesaria o prestablecida.

11.11. Restricciones en la instalación de software

Se deberán establecer e implementar reglas sobre que tipo de software pueden instalar los usuarios. Dado que la instalación no controlada de software en dispositivos tecnológicos puede iniciar la introducción de vulnerabilidades y fuga de información, falta de integridad u otros incidentes de seguridad de la información.

12. SEGURIDAD EN LAS COMUNICACIONES

Las comunicaciones establecidas permiten el intercambio de información, el cual debe encontrarse regulado para garantizar los principios de la seguridad de la información que se emiten o reciben por distintos canales.

12.1. Gestión de Red

La Dirección de Gestión Informática deberá definir las pautas a fin de garantizar la seguridad de los servicios de la red del Ministerio.

Para lo cual deberá tener en cuenta:

- Mantener instalados y habilitados sólo aquellos servicios que sean utilizados.
- Realizar segmentación de redes por tipo de servicios, unidades organizativas o zonas geográficas.
- Definir el uso aceptable de las instalaciones de comunicación electrónicas.
- El uso seguro en las comunicaciones inalámbricas.
- Definir conexiones VPN para modalidades referidas a teletrabajo (usuario remoto y LAN) o para realizar la vinculación entre dos sitios (sitio de prestador externo y LAN), encontrándose este último sujeto a las definiciones técnicas y siempre y cuando no seas necesario otro tipo de enlace con mayor performance en el ancho de banda.

12.2. Transferencia de información

Para aquellos casos en los cuales se realicen acuerdos entre organismos públicos o privados (organizaciones, instituciones, fundaciones, etc.) para el intercambio de información bajo cualquier tipo de formato en el cual se encontrare (papel, digital, incluida en sistemas, software, etc.) se deberá especificar el grado de sensibilidad de la información involucrada y las consideraciones de seguridad sobre ésta.

Se deberá tener en cuenta los siguientes aspectos:

- Responsabilidades gerenciales por el control, notificaciones de transmisión, envíos y recepciones.
- Procedimientos de notificación de emisión, transmisión, envío y recepción.
- Normas o técnicas para el empaquetado (formato papel) o método de encriptación (formato digital).
- Información sobre la propiedad de la información suministrada y las condiciones de su uso.
- Normas o técnicas para la grabación y/o lectura de la información.

12.3. Seguridad en la mensajería

La mensajería electrónica como el correo electrónico, el intercambio de datos electrónicos (EDI) entre dos sistemas informáticos, la mensajería instantánea y las redes sociales cumplen un rol importante en las comunicaciones y poseen diferentes riesgos para los cuales deben considerarse medidas de seguridad:

- Protección de mensajes por el acceso no autorizado, modificaciones o denegación de servicio.
- Una correcta asignación de la dirección y transporte del mensaje.
- Confiabilidad y disponibilidad de los servicios.
- Consideraciones legales, como lo es la firma digital.
- Obtención de aprobación previa antes del uso de los servicios.

12.4. Acuerdos de Confidencialidad

Se deberá definir, implementar y revisar regularmente los acuerdos de confidencialidad o de no divulgación de la información del organismo. Así mismo deberán cumplir con la legislación o normativa vigente que alcance o competa al Ministerio. Dichos acuerdos se deberán celebrar tanto con el personal del organismo como con aquellos/as terceros/as que se relaciones de alguna manera con su información.

13. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

La seguridad de la información debe contemplarse como parte integral de los sistemas de información en todas las fases del ciclo de vida del sistema.

Dado que los sistemas de información incluyen servicios de operación, infraestructura IT, aplicaciones operativas, productos del tipo contable, etc. Será crucial identificar y acordar los requerimientos de seguridad antes del desarrollo y/o implementación de los sistemas de información.

13.1. Requerimientos de seguridad

Se deberán tener en cuenta algunas consideraciones a incorporar en los sistemas de información, ya sean propios, internos al organismo como a los sistemas desarrollados por terceros.

- Definir un procedimiento para que durante las etapas de análisis y diseño del sistema se incorporen a los requerimientos los controles necesarios de seguridad. Se deberá incluir una evaluación de riesgos previo al diseño, para definir los requerimientos de seguridad e identificar los controles apropiados.
- Evaluar los requerimientos de seguridad y los controles requeridos, teniendo en cuenta que éstos deben ser proporcionales en su relación costo y beneficio, analizando el activo de información que se quiere proteger y el daño potencial que pudiera ocasionar las actividades realizadas en pos de su seguridad.
- Limitar el acceso a la información para aquellos proyectos considerados sensibles.
- Categorizar a los usuarios a los cuales se les permite el uso del sistema, con distintos niveles de privilegios y limitar las ubicaciones desde las cuales pueden acceder a las mismas.
- Ningún programador o analista de desarrollo y mantenimiento de aplicaciones puede acceder a los ambientes de producción.
- Utilizar un sistema de control de versionados para el desarrollo de aplicaciones.
- Llevar un registro de las actualizaciones realizadas.
- Retener las versiones previas del sistema como medida de contingencia.
- La DGIN deberá designar al personal de su área que considere adecuado para que cumpla con la función de “Project Manager”. Dentro de las funciones del mismo se encontrarán:
    - Coordinar la implementación de nuevas modificaciones o nuevos sistemas en el ambiente de producción.
    - Asegurar que los sistemas aplicativos en uso, en el ambiente de producción, sean autorizados y aprobados de acuerdo a las normas y procedimientos vigentes.
    - Rechazar la implementación en caso de encontrar defectos y/o si faltara la documentación estándar establecida.
    - Controlar los permisos de modificación sobre los programas fuentes bajo su custodia.

- Realizar pruebas de los sistemas sobre datos extraídos del ambiente de producción a fin de trabajar sobre un lote de datos aproximados a un contexto real.
- Para la realización de pruebas se deberá prohibir el uso de bases de datos operativas, en el caso en que no fuera posible se deberán despersonalizar los datos antes de su uso.
- Luego de realizadas las pruebas, en el ambiente de prueba, se deberá eliminar la información operativa utilizada para tales efectos.

- Realizar copias de respaldo de los programas fuentes cumpliendo los requisitos de seguridad establecidos por el organismo en los procedimientos que surgen de la presente política.
- En caso de ser necesario realizar un cambio en el sistema operativo, donde se encuentren alojados los sistemas, se deberán revisar los procedimientos de integridad y control de aplicaciones para garantizar que no hayan sido comprometidas por el cambio.
- En caso de considerar necesaria la modificación de paquetes de software, retener el software original realizando los cambios sobre una copia identificada y documentando exhaustivamente los pasos realizados.

13.2. Desarrollo Externo

Para los casos en los cuales se considere la tercerización del desarrollo de software, se deberán establecer normas y procedimientos que contemplen los siguientes aspectos:

- Acuerdos de licencias, propiedad de código y derechos conferidos
- Requerimientos contractuales con respecto a la calidad y seguridad del código y la existencia de garantías.
- Verificación del cumplimiento de las condiciones de seguridad.
- Acuerdos de custodia de las fuentes del software y cualquier otra información requerida en caso de quiebra y/o inhabilidad de la tercera parte. O Deberá ser entregadas los códigos fuentes para que el organismo preste custodia del mismo una vez desarrollado el producto o al realizar actualizaciones sobre el mismo.

13.3. Gestión de Vulnerabilidades

Se deberá obtener información oportuna y precisa acerca de las vulnerabilidades técnicas de los sistemas de información utilizados para evaluar la exposición ante tales vulnerabilidades y tomar las medidas a fin de tratar los riesgos asociados.

Se deberá contar con un inventario de software donde se detalle información de sus versiones, como datos de los proveedores y responsables.

El proceso de gestión de vulnerabilidades deberá contemplar:

- La definición de roles y responsabilidades asociados con la gestión de vulnerabilidades técnicas.
- Procedimientos de identificación de vulnerabilidades técnicas potenciales.
- Definición de prioridades para la atención de necesidades relacionadas con actualizaciones de seguridad.
- Identificación de los riesgos asociados a la instalación de parches.

13.4. Ambientes

Toda aplicación generada en el sector de desarrollo o adquirida a través de un prestador, 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. Por lo cual 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.

Se deberá adaptar en tres (3) ambientes teniendo en cuenta las capacidades instaladas, los recursos y el equipamiento existente.

Ambiente de Desarrollo:

Donde se desarrollan los programas fuente y donde se almacena toda la información relacionada con el análisis y diseño de los sistemas. El/La Analista o programador/a (desarrollador) tendrá total dominio sobre el ambiente. Podrán recibir alguna fuente para modificar, quedando registrado en el sistema de control de versionado. En el mismo realizará las pruebas con los datos de la "base de datos" del entorno de desarrollo. Cuando lo considere, lo pasará al ambiente de prueba junto con la documentación necesaria que le entregara al implementador de dicho ambiente.

Ambiente de Pruebas:

En este ambiente, se recibirá el programa y la documentación respectiva y se realizará una prueba general con un lote de datos para tal efecto.

El testeador realizará las pruebas con los datos de la "base de datos" del ambiente de pruebas. Si no se detectaran errores de ejecución y los resultados de rutinas son correctos y si considera que la documentación presentada se encuentra completa, entonces remitirá el programa fuente al ambiente de producción por medio del sistema de control de versiones. Caso contrario volverá hacia atrás devolviendo el sistema al ambiente de desarrollo junto con las observaciones pertinentes.

Ambiente de Producción:

Ambiente en el cual se ejecutan los sistemas y se encuentran los datos productivos. Los programas fuentes certificados se guardarán en un repositorio de fuentes de producción, almacenándolos mediante n sistema de control de versionado. Se registrarán los datos del programador, las modificaciones realizadas, fecha, hora y tamaño de los programas fuente y objetos o ejecutables.

Tanto el personal de desarrollo, como los proveedores de aplicativos tercerizados 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. Salvo en casos excepcionales, se debe documentar adecuadamente la autorización, trabajos realizados y un monitoreo constante en todo momento de este.

14. RELACION CON PROVEEDORES

Asegurar la protección de la información del Ministerio que es accedida por los/las proveedores/as, cumpliendo con el nivel de seguridad establecido.

Dichos requisitos de seguridad de la información deberán ser acordados para mitigar los riesgos asociados al acceso de los/las proveedores/as y deberán documentarse debidamente.

Los proveedores que deban acceder físicamente a las instalaciones para dar soporte se deberán identificar, registrar sus ingresos y estar siempre acompañados por personal del Ministerio de Educación.

Se deberán identificar e incluir en los acuerdos los niveles de servicio SLA y acuerdo de compromisos de confidencialidad en todo contrato o convenio con los proveedores.

Se deberán incluir en las contrataciones, en caso de corresponder, el detalle de los contactos (teléfonos, correos electrónicos y página web) de asistencia de soporte técnico y el nivel de escalamiento correspondiente.

Se deberá establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor/a que puede acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de Tecnologías de Información (IT).

Se definen a continuación los términos para incluir en los acuerdos antes mencionados:

- 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.
- Clasificación de la información de acuerdo con el esquema de 7.3 “Clasificación de la Información” de la presente política de seguridad.
- Requisitos legales y normativos, incluida la protección de datos personales y los derechos de propiedad intelectual.
- Reglas de uso aceptable de la información, incluido el uso inaceptable en caso de ser necesario.
- Una lista explícita del personal (externo) autorizado para acceder o recibir la información o los procedimientos o condiciones del Ministerio.
- Políticas de seguridad de la información pertinentes al contrato específico.
- Normativas pertinentes para la subcontratación en caso de que esto suceda, como podría llegar a suceder en los casos de empresas Partner, es decir para los servicios 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.

15. GESTION DE INCIDENTES DE SEGURIDAD

Es necesario que el organismo cuente con capacidad de gestión de incidentes de seguridad de la información que permitan realizar la detección de incidentes, llevar a cabo su tratamiento y poder realizar una prevención de futuros incidentes similares.

Por lo cual se deberán adoptar las medidas necesarias para prevenir, detectar, gestionar, resolver y reportar los incidentes de seguridad que puedan afectar a los activos de información.

15.1. Reporte de Eventos de Seguridad de la Información

Todo el personal del organismo es responsable de reportar a la DGIN las debilidades e incidentes de seguridad que oportunamente detecten.

Los incidentes ocurridos en el organismo y relativos a la seguridad de la información deberán ser comunicados a través de las autoridades o canales apropiados tan pronto como sea posible.

Se deberá establecer un procedimiento formal de comunicación y 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 seguridad sea informado debidamente a la DGIN tan pronto se haya tomado conocimiento.

Sin perjuicio de informar a otros organismos de competencia, la DGIN deberá comunicar a la Dirección Nacional de Ciberseguridad todo incidente o violación de la seguridad que involucre recursos informáticos.

15.2. Gestión de incidentes y mejoras de la seguridad de la información

Se deberá establecer los procedimientos para el manejo de los eventos y debilidades en la seguridad de la información una vez que han sido reportados.

Se deberán contemplar y definir todos los tipos probables de incidentes relativos a la seguridad incluyendo:

- Fallas operativas
- Código malicioso
- Intrusiones
- Fraude informático
- Error humano
- Catástrofes naturales.

Se deberá contemplar en los planes de contingencia los siguientes puntos:

- Definición de las primeras medidas a implementar
- Análisis e identificación de la causa del incidente
- Planificación e implementación de soluciones para evitar su repetición, si es que esto fuera posible.
- Comunicación formal con los afectados o involucrados en la recuperación del incidente.
- Notificación de las acciones realizadas a las autoridades u organismos pertinentes.

Se deberá registrar pistas de auditoría y evidencia, para implementar controles luego de realizadas las acciones de recuperación.

16. GESTION DE CONTINUIDAD

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

Esto permitirá mantener la continuidad de la operatoria y mantener planes prioritarios, coordinados y probados. Así mismo permitirá preparar a la organización para responder ante el impacto de las incidencias.

Se deberá ejecutar un plan a fin de minimizar los efectos de las posibles interrupciones de las actividades cotidianas, ya sean estas, resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos, para proteger los procesos críticos mediante la combinación de controles preventivos y acciones de recuperación.

Dichos planes deberán contener al menos las siguientes etapas:

- Notificación/Activación: Consiste en detectar y determinar el daño y la activación del plan.
- Reanudación: Consiste en restaurar temporalmente las operaciones diarias y realizar la recuperación del daño producido al sistema.
- Recuperación: Consiste en la restauración de las capacidades de proceso del sistema en las condiciones normales.

16.1. Continuidad de las actividades y análisis de los impactos

Se deberán contemplar los siguientes aspectos a fin de establecer un Plan de Continuidad:

- Priorización de los procesos críticos del organismo.
- Identificar los eventos (amenazas) que puedan ocasionar interrupciones en las actividades diarias, como ser la falla de equipamiento, interrupción del suministro de energía eléctrica, incendio, ilícitos, etc.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones, evaluar la magnitud del daño y el período de recuperación.
- Identificar los controles preventivos en los centros de procesamiento de datos y racks de comunicaciones, tales como detectores de humo, fuego, humedad, derrame de líquidos, fallas de suministro eléctrico, etc. Como así también identificar los controles preventivos en todos los aspectos lógicos de acceso a la información.
- Documentación, comunicación y capacitación al personal, mediante procedimientos y procesos relacionados con la recuperación de la operatoria del organismo.

16.2. Elaboración e implementación de los planes de continuidad

Se deberán elaborar planes de contingencia para garantizar la continuidad de las actividades del Ministerio y se deberán abarcar los siguientes puntos:

- Analizar los posibles escenarios de contingencia y definir las acciones correctivas a implementar en cada caso.
- Implementar procedimientos de emergencia para permitir la recuperación y restablecimiento de los servicios en el menor tiempo posible.
- Documentar los procedimientos y procesos acordados.
- Documentar las evidencias de las pruebas realizadas en el ambiente de simulacro, que deberá realzarse de manera periódica.
- Instruir al personal adecuadamente, en materia de procedimientos y procesos de contingencia.
- Efectuar pruebas de recuperación técnica, realizar ensayos completos probando que el Ministerio, el personal, el equipamiento, las instalaciones y los procesos pueden afrontar las interrupciones.
- Todas las pruebas efectuadas deberán ser documentadas, resguardándose la evidencia formal de la ejecución y de los resultados obtenidos.

17. CUMPLIMIENTO

El diseño, la operación, el uso y administración de los sistemas de información se encuentran regulados por disposiciones legales y contractuales. Por lo cual se deberá cumplir con las disposiciones legales, normativas y contractuales vigentes a fin de evitar sanciones administrativas.

17.1. Derechos de la propiedad intelectual

Se deberán 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 este, 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 deberán tener presentes:

- 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.

17.2. 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. Por lo cual se deberá analizar los términos y condiciones de las licencias e implementar los siguientes controles:

- 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.
- Divulgar las políticas de adquisición de software y las disposiciones de la Ley de Protección Intelectual, y notificar la determinación de tomar acciones disciplinarias contra el personal que las infrinja.
- Mantener un adecuado registro de activos.
- Conservar pruebas y evidencias de propiedad de licencias, discos maestros, manuales, etc.
- Implementar controles para evitar el exceso del número máximo permitido de usuarios.
- Verificar que sólo se instalen productos con licencia, o software autorizado, como podría ser el caso del software libre.
- Elaborar y divulgar un procedimiento para el mantenimiento de condiciones adecuadas con respecto a las licencias.
- Elaborar y divulgar un procedimiento relativo a la eliminación o transferencia de software a terceros.
- Utilizar herramientas de auditorías adecuadas.
- Cumplir con los términos y condiciones establecidos para obtener software e información en redes públicas.

17.3. Protección de los Registros del Ministerio

Los registros críticos del organismo se deben proteger contra pérdida, destrucción y falsificación. Algunos registros podrían requerir una retención segura para cumplir requisitos legales o normativos, como así también para respaldar actividades esenciales del organismo.

Los registros se deberán 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, como ser papel, medios magnéticos u ópticos, y el lugar de almacenamiento, ya sea local e interno al organismo o almacenamiento en nube.

Las claves criptográficas asociadas con archivos cifrados deberán mantenerse en forma segura y estar disponibles para su uso por parte de personas autorizadas cuando esto resultare necesario.

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 con 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 resultasen necesarios para el organismo.

Se deberán tener en cuenta:

- Ley N° 25.188: "Ética en el Ejercicio de la Función Pública", 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.
- Decreto 41/99: "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 ART 255: Sanciona a quien sustrajere, ocultare, destruyere o inutilizare objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un/a funcionario/a o de otra persona en el interés del servicio público. Si el culpable fuere el/la mismo/a depositario/a, sufrirá las sanciones que el organismo determine según sea el caso y según la reglamentación vigente.
- Ley N° 24.624 ART 30: Autoriza el archivo y la conservación en soporte electrónico u óptico indeleble de la documentación financiera, de personal y de control de la APN 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 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 ART 183: Sanciona a aquel que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos.

17.4. Protección de datos y Privacidad de la Información Personal

Todo el personal del organismo deberá conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan acceso con motivo del ejercicio de sus funciones.

Se deberá redactar un "Compromiso de Confidencialidad", el cual deberá ser suscrito por todos los que tengan acceso a información clasificada como Confidencial o Secreta. Mediante este instrumento el subscriptor se comprometerá a utilizar la información solamente para el uso específico al que está destinada y a no comunicar, diseminar o de alguna otra forma hacer pública la información a ninguna persona, firma, compañía o tercera persona, salvo autorización previa y escrita del responsable del Activo de que se trate.

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

Se deberán tener en cuenta:

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

- Código Penal: Sanciona a aquel que teniendo noticias de un secreto cuya divulgación pueda causar daño, lo revelare sin justa causa (Art. 156), al funcionario público que revelare hechos, actuaciones o documentos que por la ley deben quedar secretos (Art. 157), al que revelare secretos políticos o militares concernientes a la seguridad, a los medios de defensa o a las relaciones exteriores de la Nación, o al que por imprudencia o negligencia diere a conocer los secretos mencionados anteriormente, de los que se hallare en posesión en virtud de su empleo u oficio (Art. 222 y 223). Resolución HCS 120/06 y otra normativa aplicable al personal de la UNC.

17.5. 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 para el cual fueron provistos debe ser considerada como uso indebido.

Todos/as los/las empleados/as deben conocer el alcance preciso del uso adecuado de los recursos informáticos y deben respetarlo. En particular se debe respetar lo dispuesto por las siguientes normas:

- Ley Marco de Regulación de Empleo Público Nacional. Ley 25.164: Prohíbe hacer uso indebido o con fines particulares del patrimonio estatal.
- Convenio Colectivo de Trabajo General: Obliga a las/los agentes a no hacer uso indebido o con fines particulares del patrimonio estatal.
- Ética en el Ejercicio de la Función Pública. Ley 25.188: Obliga a las personas que se desempeñen en la función pública a proteger y conservar la propiedad del Estado y sólo emplear sus bienes con los fines autorizados.
- Código de Ética de la Función Pública: Obliga al funcionario público a proteger y conservar los bienes del Estado y utilizar los que le fueran asignados para el desempeño de sus funciones de manera racional, evitando su abuso, derroche o desaprovechamiento.
- Código Penal ART 183: 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.

17.6. Delitos Informáticos

Todos/as los/las empleados/as 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 el presente documento.

17.7. Cumplimiento de la Política de Seguridad de la Información

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 Unidad de Auditoría Interna realizará revisiones periódicas de todas las áreas del organismo a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad.

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

17.8. Controles de Auditoría de Sistemas

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

Se contemplarán los siguientes puntos:

- Acordar con el Área que corresponda los requerimientos de auditoría.
- Controlar el alcance de las verificaciones. Esta función será realizada por el responsable de auditoría.
- Limitar las verificaciones a un acceso de sólo lectura del software y datos de producción. Caso contrario, se tomarán los resguardos necesarios a efectos de aislar y contrarrestar los efectos de las modificaciones realizadas, una vez finalizada la auditoría. Por ejemplo:
    - Eliminar archivos transitorios.
    - Eliminar entidades ficticias y datos incorporados en archivos maestros.
    - Revertir transacciones.

    - Revocar privilegios otorgados.
- Identificar claramente los recursos de tecnologías de información para llevar a cabo las verificaciones, los cuales serán puestos a disposición de los auditores. A tal efecto, el responsable de la Unidad de Auditoría Interna completará y mantendrá actualizado el formulario que oportunamente se establezca, el cual deberá ser puesto en conocimiento de las áreas involucradas.
- Identificar y acordar los requerimientos de procesamiento especial o adicional.
- Monitorear y registrar todos los accesos, a fin de generar una pista de referencia. Los datos a resguardar deben incluir como mínimo:
    - Fecha y hora.
    - Puesto de trabajo.
    - Usuario.
    - Tipo de acceso.
    - Identificación de los datos accedidos.
    - Estado previo y posterior.
    - Programa y/o función utilizada.

- Documentar todos los procedimientos de auditoría, requerimientos y responsabilidades

17.9. Protección de los elementos utilizados por la Auditoría de Sistemas

Se deberá 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 deberán tomar los recaudos necesarios a efectos de cumplir las normas de auditoría dispuestas por la Sindicatura General de la Nación.

17.10. Sanciones Previstas por Incumplimiento

Se sancionará 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 N° 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 puede 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.

18. ANEXO I

18.1. Modelo de Declaración Jurada sobre la Confidencialidad de la Información

DECLARACION JURADA CONFIDENCIALIDAD

En virtud de los servicios prestados en la Dirección General de Informática, dependiente de la Subsecretaria de Gestión Administrativa, del Ministerio de Educación de la Nación, …… con DNI……. Cargo de revista…… o responsable de la firma de la cual representa……. ……
Me comprometo, mediante la suscripción de la presente a guardar la máxima reserva y secreto sobre los datos e información, a los que acceda en virtud de las tareas encomendadas, a observar y garantizar la confidencialidad, integridad y secreto de dichos datos adoptando las máximas medidas de seguridad, para evitar su divulgación.
El compromiso que se asume, subsistirá mientras se mantenga la relación con el Estado Nacional (bajo cualquier modalidad) y aún después de finiquitada la misma; asumiendo la responsabilidad penal, administrativa y civil que por dolo o negligencia pudiera ocasionar la difusión y divulgación de los datos e información que se debe resguardar.

En la Ciudad Autónoma de Buenos Aires a los días del mes de de 2022

19. ANEXO II

19.1 Modelo de Carta Compromiso en el Uso de Recursos Tecnológicos

En virtud de los servicios prestados en la Dirección General de Informática, dependiente de la Subsecretaria de Gestión Administrativa, del Ministerio de Educación de la Nación, YO ……. con DNI…….Cargo de revista……. Me comprometo, mediante la suscripción de la presente a cuidar del bien y/o servicio recibido y realizar una óptima utilización y buen uso del recurso tecnológico.

Asumo la responsabilidad de utilizarlos en las actividades relacionadas con mis funciones dentro del organismo.

Declaro que conozco las recomendaciones de uso, custodia y cuidado de los equipos electrónicos y la responsabilidad en el uso del internet y la utilización de las tecnologías de la información y las comunicaciones TIC.

El compromiso que se asume subsistirá mientras se mantenga la relación con el Estado Nacional (bajo cualquier modalidad). Luego de finiquitada la misma; asumo la responsabilidad de notificar a la Dirección de Gestión Informática sobre dicha situación para que puedan realizar la baja de los servicios correspondientes y me comprometo a realizar la entrega de los bienes tecnológicos recibidos bajo mi nombre.

Cualquier daño que sufran dichos recursos a causa de un uso indebido de los mismos será mi responsabilidad.

Firmado a los ____ días del mes de _____ del año _____ en la ciudad de _____

República Argentina - Poder Ejecutivo Nacional
Las Malvinas son argentinas

Hoja Adicional de Firmas
Informe gráfico firma conjunta

Número: IF-2022-139107936-APN-DGIN#ME

CIUDAD DE BUENOS AIRES
Martes 27 de Diciembre de 2022

Referencia: Políticas de Seguridad de la Información

El documento fue importado por el sistema GEDO con un total de 65 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2022.12.22 19:07:13 -03:00

Galdys Patricia BOTTI
Auditor
Unidad de Auditoría Interna
Ministerio de Educación

Digitally signed by Gestion Documental Electronica
Date: 2022.12.26 12:50:42 -03:00

Nahuel Ivan Sifon
Asesor Administrativo
Dirección General de Asuntos Jurídicos
Ministerio de Educación

Digitally signed by Gestion Documental Electronica
Date: 2022.12.26 14:22:58 -03:00

Tomas CIOCCI
Director Nacional
Dirección Nacional de Evaluación, Información y Estadística Educativa
Ministerio de Educación

Digitally signed by Gestion Documental Electronica
Date: 2022.12.26 14:33:18 -03:00

Juan Pablo BENSADON
Director
Dirección de Asistencia Técnico Administrativa
Ministerio de Educación

Digitally signed by Gestion Documental Electronica
Date: 2022.12.26 14:45:28 -03:00

Martín Ricardo FUNES
Coordinador Técnico Administrativo
Secretaría de Educación
Ministerio de Educación

Digitally signed by Gestion Documental Electronica
Date: 2022.12.26 14:51:38 -03:00

Viviana ALONSO
Gabinete
Dirección Nacional de Fortalecimiento del Sistema Formador
Ministerio de Educación

Digitally signed by Gestion Documental Electronica
Date: 2022.12.26 15:13:35 -03:00

Gustavo PELTZER
Director Nacional
Instituto Nacional de Educación Tecnológica
Ministerio de Educación

Digitally signed by Gestion Documental Electronica
Date: 2022.12.26 15:26:34 -03:00

Andrea Cecilia ESCANDE
Directora Nacional
Dirección Nacional de Presupuesto e Información Universitaria
Ministerio de Educación

Digitally signed by Gestion Documental Electronica
Date: 2022.12.26 17:15:27 -03:00

Gonzalo Tomás PÉREZ
Asistente administrativo
Unidad Gabinete de Asesores
Ministerio de Educación

Digitally signed by Gestion Documental Electronica
Date: 2022.12.27 12:25:33 -03:00

Marcela RODRIGUEZ O CONNOR
Directora
Dirección de Servicios y Mantenimiento
Ministerio de Educación

Digitally signed by Gestion Documental Electronica
Date: 2022.12.27 12:42:02 -03:00

Andrea KEMELMAJER
Directora
Dirección de Contrataciones
Ministerio de Educación

Digitally signed by Gestion Documental Electronica
Date: 2022.12.27 14:37:45 -03:00

Juan Pablo Pale
Director General
Dirección General de Administración
Ministerio de Educación

Digitally signed by Gestion Documental Electronica
Date: 2022.12.27 14:43:18 -03:00

Hector Omar MEDINA
Asistente administrativo
Dirección de Recursos Humanos
Ministerio de Educación

Digitally signed by Gestion Documental Electronica
Date: 2022.12.27 14:46:17 -03:00

LORENA MABEL ALMIRON
Asistenta administrativa
Dirección de Gestión Informática
Ministerio de Educación

Digitally signed by Gestion Documental Electronica
Date: 2022.12.27 14:46:28 -03:00

VANESA DANIELA OUBIÑAS
Técnico Informático
Dirección de Gestión Informática
Ministerio de Educación

Digitally signed by Gestion Documental Electronica
Date: 2022.12.27 14:50:36 -03:00

EDGARDO DAMIAN BOMBARA
Director
Dirección de Gestión Informática
Ministerio de Educación

Digitally signed by Gestion Documental Electronica
Date: 2022.12.27 14:50:39 -03:00