BIBLIOTECA NACIONAL MARIANO MORENO

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Versión 1.0

Fecha	Versión	Cargo	Responsable	Acción
01/03/2022	1.0	xx	xx	Creación de la PSI

Referente a los Usuarios

Referente a la Organización

REFERENTES A LOS USUARIOS

1. Política de Seguridad de la Información

1.1 Introducción

El avance de las nuevas tecnologías es un fenómeno del cuál nuestro Organismo, Biblioteca Nacional Mariano Moreno(en adelante el "Organismo") no puede quedar exenta, más aún cuando la información tiene un rol preponderante en el inventario de activos de la empresa. Entendemos que dichas exigencias generan grandes demandas para que se integren los sistemas de información del Organismo.

Una Política de Seguridad de la Información (en adelante PSI) es un documento central para la protección de los datos y de los recursos utilizados para su tratamiento, que define la postura de una organización respecto al comportamiento que espera de empleados, autoridades y terceros que tomen contacto con dichos datos y/o recursos, para su protección.

En el marco de lo dispuesto por la Decisión Administrativa (DA) N° 641/2021, los Organismos alcanzados por la norma deben elaborar y aprobar una PSI. Dicha política debe ser aprobada por las autoridades y comunicada a todos los involucrados. Contar con un documento formal y debidamente informado es además, una buena práctica incorporada a todos los estándares y recomendaciones internacionales.

Las PSI protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos del Organismo.

Es importante que los principios de la PSI sean parte de la cultura organizacional. Para esto, se debe asegurar un compromiso manifiesto de los Directivos del Organismo, de los titulares de Unidades Organizativas para la difusión, y de todos los funcionarios y agentes para la consolidación y cumplimiento de la presente Política.

1.2 Declaración de la Política de Seguridad de la Información

La gestión efectiva de la Seguridad de la Información es una responsabilidad compartida por todos los miembros del Organismo. Dicha responsabilidad se debe asumir en una actitud proactiva y colaborativa tendiente a la protección de los activos comerciales de la empresa, entre los cuales se encuentra el objeto de la presente política: la información.

La información es un activo que, como otros bienes y servicios requeridos para el cumplimiento de los objetivos del organismo, resulta esencial para el desarrollo de las actividades de competencia. En consecuencia, necesita ser protegida adecuadamente.

Dicha información puede presentarse en diversos formatos (impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos o como contenido multimedial, entre otros). Por lo tanto y sin perjuicio del formato en que se encuentre y del soporte que se utilice, debe estar apropiadamente protegida desde su creación, durante todo su ciclo de vida y hasta su eventual destrucción, desuso o archivo definitivo.

La Seguridad de la Información es la protección de la información de un rango amplio de amenazas, con el objeto de minimizar los riesgos a los que se encuentra expuesta y asegurar la continuidad de la operación normal del organismo. Tiene por objetivos la preservación de la confidencialidad, integridad y disponibilidad de la información.

Dicho estado de protección adecuada se logra implementando un conjunto de mecanismos de seguridad o controles que incluyen entre otros, procesos, políticas, procedimientos, estructuras organizacionales, software y hardware. Se necesita establecer, implementar, monitorear, revisar y mejorar estos mecanismos para fortalecer el cumplimiento de los objetivos de seguridad específicos. Esto se debe realizar en forma coordinada con otros procesos de gestión del organismo.

Del mismo modo, los procesos, sistemas y redes de apoyo son también activos importantes. Definir, lograr, mantener y mejorar la Seguridad de la Información es esencial para preservarlos, mantener la eficacia en la operación, cumplir con el marco legal y las normas internas, y preservar la imagen institucional del Organismo.

Los organismos, como cualquier organización enfrentan amenazas de seguridad en sus sistemas y redes de información, cada vez más frecuentes y sofisticadas. La Seguridad de la Información es importante para el desarrollo de actividades del sector público y para proteger las infraestructuras críticas de información que proveen servicios esenciales a la sociedad.

Consideramos entonces como objetivo de la presente política, establecer los principios, medidas y controles adecuados y tendientes a garantizar la Integridad, Confidencialidad y Disponibilidad de la información, adoptándose los principios de la debida diligencia y debido cuidado de la información.

1.3 Objetivo de la Política de Seguridad de la Información

La presente PSI establece las directrices y líneas de actuación en materia de Seguridad de la Información que establecen el modo en que el Organismo debe gestionar y proteger los datos a los que da tratamiento, los recursos tecnológicos que utiliza y los servicios que brinda. Detalla también lineamientos respecto a la comunicación de esta Política a los funcionarios y empleados bajo cualquier modalidad de contratación y demás involucrados internos y externos, así como respecto a su implementación en todas las dependencias de la jurisdicción.

Los objetivos específicos de la Política de Seguridad de la Información son asegurar la información en sus tres pilares fundamentales para el Organismo:

- **Disponibilidad:** Para asegurar que los usuarios autorizados tienen acceso a la información y los procesos, sistemas y redes que la soportan, cuando se requiera.
- **Integridad:** Para preservar que la información no ha sido alterada ni modificada de forma no autorizada, asegurando su veracidad y completitud.
- **Confidencialidad:** Para asegurar que la información solo sea accedida por aquellos que cuenten con la autorización respectiva.

Dichos objetivos deben 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:

- Asegurar el mantenimiento de la confiabilidad con quienes se comparten redes públicas y privadas.
- Garantizar que la información está segura.
- Adoptar todas las medidas en cumplimiento del marco normativo aplicable.
- Poner de manifiesto la postura del Organismo en lo que respecta a la prevención, atención y seguimiento de incidentes de Seguridad de la Información.
- Informar que se habilitan y disponen los mecanismos necesarios para el tratamiento adecuado y

coordinado de la Seguridad Física y Lógica de la información del Organismo.

- Provocar la adopción paulatina de los conceptos de seguridad por parte del Organismo a través de un plan de implementación gradual y acorde con la cultura del Organismo.
- Cumplir con la legislación aplicable en materia de Seguridad de la Información.

1.4 Alcance

Esta Política aplica a todos los miembros, agentes y funcionarios del Organismo, como así también a otros procesos, individuos y/u organizaciones, internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

1.5 Disposiciones Generales

Esta PSI se aplica en todo el ámbito del organismo, a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros. Todo el personal deberá respetar las normas, estándares, guías de mejores prácticas y procedimientos de Seguridad de la Información derivadas de la presente política.

Debe ser comunicada fehacientemente y cumplida por todos los funcionarios y agentes que lo integran, cualquiera sea su modalidad de vinculación y contractual y las fuentes de financiamiento correspondientes. En su alcance se encuentran tanto el personal que desempeñe funciones directivas como administrativas o técnicas, cualquiera sea su vínculo/relación contractual, su nivel jerárquico, su situación de revista y las tareas que desempeñe.

Asimismo, debe ser conocida y cumplida por todas aquellas personas, ya sean internos o externos, vinculadas a la entidad a través de contratos, convenios, acuerdos o algún otro instrumento válido para establecer la relación con terceros, en la medida en que les sea aplicable y en las secciones que le corresponden.

Toda información relacionada con un proceso deberá ser clasificada conforme al estándar correspondiente en cuanto a su grado de sensibilidad para el Organismo.

El personal será responsable de proteger la información y recursos bajo su custodia, que sean propiedad del Organismo, siguiendo las normas, estándares, guías de mejores prácticas y procedimientos definidos para tales efectos por el Organismo.

Todo incidente de Seguridad de la Información deberá ser tratado con la mayor discreción posible, reportándose de acuerdo a los protocolos vigentes y buscando en todo momento preservar la reputación del Organismo.

Las infracciones, incumplimientos o prácticas inapropiadas o contrarias a las obligaciones establecidas en las normas, estándares, guías de mejores prácticas y procedimientos de Seguridad de la Información derivadas de la presente política, serán pasible de sanción disciplinaria de acuerdo a la normativa vigente en materia de recursos Humanos.

Los principios de la Seguridad de la Información, en base a la normativa vigente, que son adoptados por el organismo comprendidos en el inciso a) del artículo 8 la Ley N° 24.156, son la Confidencialidad, la Integridad y la Disponibilidad de la información a la que le dan tratamiento y de los activos de información utilizados para su gestión. La protección de los derechos de los titulares de los datos personales procesados, así como de

la información propia del organismo, es un objetivo central de esta PSI.

Todo el personal deberá cumplir con la normativa vigente y relación a Seguridad de la Información, especialmente con la Ley 25.326 y las resoluciones que emita el Organismo de control la "Agencia de Acceso a la Información Pública (AAIP)".

Los contenidos de este documento están alineados y se complementan con el resto de las políticas y normativas internas del organismo, que entiende la importancia de gestionar eficazmente la Seguridad de la Información. En consecuencia, declara su compromiso y total apoyo a la gestión de la Seguridad de la Información como parte integrante de la gestión del resto de los procesos establecidos en su ámbito.

Asimismo, sus autoridades se comprometen a liderar la mejora continua de los procesos de gestión de Seguridad de la Información, asegurando su eficacia y eficiencia. Las personas alcanzadas por esta PSI reciben una concientización periódica y pertinente a su función, respecto del compromiso que asumen para cumplir con esta PSI. Para ello, se asignan los recursos necesarios.

En el mismo sentido, el Organismo se compromete a cumplir con la normativa legal y reglamentaria aplicable a todos los niveles, así como a adaptarse a futuras normas y requisitos del contexto interno o externo y a aquellos que emanan de la vinculación con terceros involucrados.

El incumplimiento de esta política tendrá como resultado la aplicación de sanciones disciplinarias, conforme a la magnitud y característica del aspecto no cumplido, de acuerdo con la normativa aplicable al organismo.

Al respecto y de acuerdo a la normativa vigente, se establece como falta el incumplimiento de los lineamientos y disposiciones de esta PSI, por parte de los agentes y funcionarios, en función de lo dispuesto por el régimen sancionatorio establecido en la Ley Marco de Regulación de Empleo Público Nacional N° 25.164, su Decreto Reglamentario N° 1421/02 y sus normas modificatorias y complementarias. Para ello, se establece una graduación en las responsabilidades y sanciones administrativas que se aplicarán de acuerdo con la gravedad de la infracción cometida, sin perjuicio de las acciones legales que pudieran corresponder.

El organismo establece sus requisitos de Seguridad de la Información en base a la evaluación y posterior gestión de riesgos de seguridad sobre sus activos de la información.

1.6 Revisión y actualización

El Organismo se compromete a revisar esta PSI anualmente, adaptándola a nuevas exigencias organizativas o del entorno, así como a comunicarla a su planta de personal y a los terceros involucrados. También dispondrá las medidas necesarias para que esté a disposición de los alcanzados en todo momento.

Adicionalmente, procederá a su revisión y eventual modificación, cada vez que se produzca un cambio significativo en la plataforma tecnológica, una modificación de la normativa vigente aplicable, un cambio en los objetivos estratégicos del organismo o cualquier otro evento que lo amerite.

Área de Informática será la responsable de llevar adelante las revisiones sean periódicas, dejándose constancia de ellas en el presente documento. La Dirección y/o el Comité de Seguridad será responsable de la aprobación de las nuevas versiones, que serán comunicadas en tiempo y forma a todos los alcanzados para su cumplimiento.

1.7 Términos y Definiciones

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

- **Confidencialidad:** se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- **Integridad:** se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- **Disponibilidad:** se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.
- Adicionalmente, deberán considerarse los conceptos de:
- **Autenticidad:** busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- **Auditabilidad:** define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
- **Protección a la duplicación:** consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
- **No repudio:** se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
- **Legalidad:** referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.
- **Confiabilidad de la Información:** es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.
- A los efectos de una correcta interpretación de la presente Política, se realizan las siguientes definiciones:
- **Información:** se refiere a toda comunicación o representación de conocimiento como datos personales y/o cualquier información o datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
- **Sistema de Información:** se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.
- **Tecnología de la Información:** se refiere al hardware y software operados por el Organismo o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.
- **Evaluación de Riesgos:** se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria del Organismo.
- **Administración de Riesgos:** se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.
- **Comité de Seguridad de la Información:** el Comité de Seguridad de la Información, es un cuerpo integrado por representantes de todas las áreas sustantivas del Organismo, destinado a garantizar el

apoyo manifiesto de las autoridades a las iniciativas de seguridad. Además cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de Seguridad de la Información a los integrantes del Organismo que así lo requieran.

- **Propietario de la información:** entre sus funciones se encuentran la clasificación de la información de acuerdo con el grado de sensibilidad y criticidad de la misma, la definición de qué usuarios deben tener permisos de acceso a la información de acuerdo a sus funciones y competencia.
- **Incidente de Seguridad:** un incidente de seguridad es un evento adverso en un sistema de computadoras, o red de computadoras, que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

1.8 Normas, estándares, guías, procedimientos y anexos

Se consideran como obligatorias y parte de las presentes políticas, todas las normas, estándares, guías de mejores prácticas y procedimientos de Seguridad de la Información. A continuación, se categorizan las normas fundamentales que forman parte de la estructura normativa, de acuerdo a la Decisión Administrativa Nº 641/2021:

1. **Organización de la seguridad:** tiene por objetivo establecer, regular y organizar la administración y gestión de la Seguridad de la Información del Organismo. Se asigna las responsabilidades relativas a la Seguridad de la Información y la mejor forma de coordinar todas las actividades tendientes a la implementación de la presente PSI.
2. **Recursos humanos:** El personal es considerado un recurso fundamental para la protección de la información. Este control tiene por objetivo educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su jerarquía en el Organismo, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de Seguridad de la Información, así como las posibles consecuencias y sanciones ante casos de incumplimiento.
3. **Gestión de activos:** tiene por objetivo determinar cuáles son los activos del Organismo, clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información.
4. **Gestión y control de accesos:** tiene por objetivo gestionar los procesos de identificación, autenticación y autorización para impedir el acceso no autorizado a los sistemas de información, a través de la implementación de procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información.
5. **Uso de herramientas criptográficas:** tiene como objetivo la gestión de las técnicas y algoritmos criptográficos para la protección de la información del Organismo, con el fin de preservar su Confidencialidad, Integridad, Autenticidad y no repudio, tanto para su almacenamiento como para su transmisión.
6. **Seguridad física y ambiental:** tiene por objetivo brindar el marco mínimo de seguridad en materia de protección física de accesos, la protección ambiental, protección y mantenimiento de equipamiento y documentación. Se busca proteger las instalaciones y activos físicos, incluyendo sus puestos de trabajo, en función de la criticidad de la información que éstos gestionan, mediante el establecimiento de

perímetros de seguridad, áreas protegidas y controles ambientales.

7. **Seguridad operativa:** tiene como objetivo que las operaciones del Organismo se desarrollen en forma segura, en todas las instalaciones de procesamiento de información, asignándose las debidas responsabilidades y desarrollando procedimientos acordes para minimizar los riesgos de acceso, cambios no autorizados, pérdida de información y control de la actividad de administradores, operadores y usuarios con privilegios.
8. **Gestión de comunicaciones:** tiene por objetivo determinar los criterios de seguridad a cumplirse en materia de comunicaciones del Organismo, tanto internas como con el exterior, asegurando el correcto flujo de las operaciones.
9. **Adquisición de sistemas, desarrollo y mantenimiento de sistemas de información:** tiene por objetivo identificar, documentar y aprobar los requerimientos de seguridad a incorporar durante todas las etapas de desarrollo e implementación de las aplicaciones y sistemas. Se debe aplicar una metodología de desarrollo seguro para todas las aplicaciones que se desarrollen internamente e incorporar requerimientos y evaluaciones de seguridad en el proceso de contratación de aplicaciones a terceros.
10. **Relación con proveedores:** tiene por objetivo incluir cláusulas vinculadas a la seguridad de la información en los pliegos de bases y condiciones. Estas disposiciones consideran los aspectos pertinentes a la protección de la información y los servicios que se brinden, desde el inicio del proceso contractual hasta su finalización. Los requisitos a incluir son acordes a la criticidad de la información y los servicios, la evaluación de riesgos y el cumplimiento de todas las normas legales y contractuales aplicables.
11. **Gestión de incidentes de seguridad:** tiene por objetivo administrar todos los eventos que atenten contra la Confidencialidad, Integridad y Disponibilidad de la información y los activos de información. Se adoptan las medidas necesarias para prevenir, detectar, gestionar, resolver y reportar los incidentes de seguridad que puedan afectar los activos de información. Las debilidades en los procesos son debidamente comunicadas, identificadas y minimizadas de forma tal que se apliquen las acciones correctivas en el menor tiempo posible
12. **Gestión de la Continuidad:** tiene por objetivo el desarrollo e implementación de planes de contingencia que permitan que, ante incidentes de seguridad, el Organismo pueda restablecerse dentro de los plazos requeridos. Se contemplan todos los aspectos de seguridad requeridos en los procedimientos de continuidad de la gestión del organismo que se desarrollan, especialmente cuando se trate de información, servicios o sistemas críticos. Se realizan análisis de impacto y se identifican las ventanas de recuperación requeridas en los procesos críticos
13. **Cumplimiento:** tiene por objetivo determinar y cumplir requisitos legales, normativos y contractuales pertinentes a cada sistema de información, los cuáles deben estar debidamente definidos y documentados a fin de que los mismos sean cumplidos por parte del Organismo. Se promueve el acatamiento de las políticas y normas de seguridad que se aprueban en su ámbito y dar cumplimiento a las recomendaciones correspondientes a los hallazgos de las auditorías internas y externas que se realicen, adoptando las medidas correctivas que correspondan.

1.9 Sanciones Previstas por Incumplimiento

El incumplimiento de la PSI tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud

y característica del aspecto no cumplido.

En aquellos casos en los cuáles un empleado realice alguna de las conductas prohibidas de manera expresa o implícita en las presentes PSI, se procederá a la aplicación de la sanción que corresponda.

El Procedimiento y régimen de sanciones aplicable, será en concordancia y bajo los mismos criterios establecidos en un manual de procedimientos de Recursos Humanos del Organismo.

La gravedad de las sanciones se determinará por quien el Organismo determine, teniendo en especial consideración las circunstancias del hecho, su publicidad a terceros, las responsabilidades del empleado infractor, y todo otro elemento del caso en concreto relativo al hecho.

Las sanciones dictaminadas serán adecuadamente notificadas al empleado infractor, dejándose constancia de la misma en su legajo personal.

2. Políticas sobre Activos de Información

2.1 Introducción

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

Frecuentemente, la información deja de ser sensible o crítica después de un cierto período de tiempo, por ejemplo, cuando la información se ha hecho pública. Estos aspectos deben tenerse en cuenta, puesto que la clasificación por exceso puede traducirse en gastos adicionales innecesarios para el Organismo.

Las pautas de clasificación deben prever y contemplar el hecho de que la clasificación de un ítem de información determinado no necesariamente debe mantenerse invariable por siempre, y que ésta puede cambiar de acuerdo con una Política predeterminada.

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

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

2.2 Clasificación de la información

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

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

2.2.1 Confidencialidad

- **Nivel 0 – Pública:** Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado del Organismo o no.
- **Nivel 1- Reservada o de uso interno:** Información que puede ser conocida y utilizada por todos los empleados del Organismo y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para el Organismo.
- **Nivel 2 – Reservada confidencial:** Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas al Organismo.
- **Nivel 3 – Secreta:** Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección del Organismo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves al mismo.

2.2.2 Integridad

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

2.2.3 Disponibilidad

- **Nivel 0:** Información cuya inaccesibilidad no afecta la operatoria del Organismo.
- **Nivel 1:** Información cuya inaccesibilidad permanente durante más de una semana podría ocasionar pérdidas significativas para el Organismo.
- **Nivel 2:** Información cuya inaccesibilidad permanente durante más de un día podría ocasionar pérdidas significativas para el Organismo.
- **Nivel 3:** Información cuya inaccesibilidad permanente durante más de una hora podría ocasionar pérdidas significativas para el Organismo.

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

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

- **Criticidad Baja:** ninguno de los valores asignados supera el 1.
- **Criticidad Media:** alguno de los valores asignados es 2
- **Criticidad Alta:** alguno de los valores asignados es 3

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

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

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

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

2.3 Uso adecuado de activos físicos y de información

2.3.1 Introducción

La Seguridad de la Información se basa en la capacidad para preservar su integridad, confidencialidad y disponibilidad, por parte de los elementos involucrados en su tratamiento: equipamiento, software, procedimientos, así como de los recursos humanos que utilizan dichos componentes. En este sentido, es fundamental educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación de revista, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad. De la misma forma, es necesario definir las sanciones que se aplicaran en caso de incumplimiento.

2.3.2 Objetivos

1. Definir de forma clara las reglas sobre el uso adecuado de los sistemas, recursos y todo tipo de activos físicos y de información pertenecientes al Organismo.
2. Informar y educar sobre el uso adecuado que debe darse a los recursos informáticos provistos por el Organismo.
3. Explicitar las responsabilidades en materia de Seguridad de la Información a todo el personal del Organismo, a fin de que puedan desempeñar de una forma más segura sus tareas, a fin de evitar riesgos de error humano, comisión de ilícitos, uso inadecuado de los activos físicos, y manejo no autorizado de los activos de información.

2.3.3 Obligaciones generales

El usuario se compromete a observar y cumplir la presente Política de Seguridad de la Información así como a tomar conocimiento y cumplir todas sus normas, protocolos y anexos vinculados y vigentes del Organismo.

- Los activos físicos y de información provistos por el Organismo en función a la relación laboral, se entiende que son titularidad del empleador, independientemente del otorgamiento de accesos (nombre de usuario y clave) que se realicen al usuario.
- El Organismo podrá monitorear el manejo y tratamiento de la información por parte del usuario a través del empleo de distintos medios y herramientas que permitirán controlar que la utilización de los activos físicos y de información sean conforme a las pautas establecidas en el presente compromiso.
- El empleador podrá, ante la detección de conductas o comportamientos irregulares, iniciar una investigación interna que permita determinar la gravedad y magnitud de las infracciones del empleado, reservándose el derecho de tomar las medidas sancionatorias y disciplinarias que estime correspondientes.

2.3.4 Uso adecuado

Los activos físicos y de información solamente pueden ser utilizados a fines de cumplir los objetivos, satisfacer necesidades y ejecutar tareas vinculadas con el Organismo. En especial, se debe tener en cuenta las siguientes normas de uso:

1. Se debe conservar toda la información en los equipos centralizados de procesamiento de datos del Organismo y resguardar toda la documentación e información de acuerdo a las Políticas de Seguridad de la Información, utilizando siempre la estación de trabajo asignada. En caso de utilizar una estación de trabajo distinta a la indicada, deberá solicitarse autorización por escrito.

2. Adoptar claves y contraseñas seguras, de acuerdo a las buenas prácticas en la generación de Contraseñas establecidas en las Políticas de Seguridad de la Información.
3. Realizar las copias de seguridad de los activos de información siguiendo las normas establecidas por el Organismo.
4. Ante la detección de cualquier tipo de incidente de seguridad, o hecho sospechoso o anormal en la utilización de los activos físicos o de información, el usuario deberá reportarlo ante el área de Informática, siguiendo el protocolo de reporte de incidentes de seguridad.
5. Los usuarios de los sistemas de información solamente pueden acceder a los activos de sistemas de información para los cuales han sido explícitamente autorizados por el propietario del activo.
6. Los usuarios pueden utilizar los sistemas de información únicamente para las actividades para las cuales han sido autorizados; es decir, para las cuales les han sido otorgados derechos de acceso.
7. Los equipos, la información o software, independientemente de su formato o soporte de almacenamiento, no pueden ser retirados de las instalaciones sin el permiso escrito previo del responsable de los Activos de Información que corresponda. En caso de estar autorizado, el usuario que retire los activos físicos o de información del establecimiento, será responsable del cuidado tanto de la integridad de los dispositivos físicos, como de la integridad y confidencialidad de la información almacenada en los mismos.
8. Al finalizar un contrato de empleo, o de otro tipo, o bien al alcanzarse los objetivos para los cuáles fueron asignados determinados activos físicos o de información, el usuario debe devolver todos esos activos al Responsable de Activos de Información que corresponda.
9. Sólo se puede acceder a Internet a través de la red local del Organismo, con la infraestructura y protección de cortafuegos adecuadas. El Área de Informática puede bloquear el acceso a determinadas páginas de Internet para usuarios individuales, grupos de usuarios o para todos los empleados del Organismo. Si el acceso a algunas páginas Web está bloqueado, el usuario puede elevar una petición escrita a su superior solicitando autorización para acceder a dichas páginas. El usuario no debe intentar eludir por su cuenta esa restricción.
10. El usuario debe considerar a toda la información recibida a través de Internet como no verificada o no confiable. Ese tipo de información puede ser utilizado con fines comerciales solamente después de haber verificado su autenticidad y veracidad.
11. El usuario debe seguir las recomendaciones establecidas en las Políticas de pantalla y escritorio limpio.
12. En caso que algún empleado quiera utilizar su propio dispositivo móvil con finalidades laborales dentro o fuera del Organismo, previamente deberá solicitar autorización por escrito, identificando el dispositivo y aceptando las Políticas de Uso de Dispositivos Móviles No Corporativos.

2.3.5 Actividades prohibidas

Está prohibido utilizar los activos de información de manera tal que ocasionen algún tipo de daño directo o indirecto sobre el Organismo, o bien, su utilización de tal forma que pueda o pudiera provocar un incidente de seguridad que tenga consecuencias sobre la confidencialidad, integridad o disponibilidad de la información del Organismo. A modo enunciativo, más no taxativo, el usuario acepta y comprende que está prohibido:

1. Permitir que otra persona utilice sus derechos de acceso; es decir, su nombre de usuario; y no debe utilizar el nombre de usuario y/o clave de otra persona. El uso de nombres de usuario grupales está prohibido. El propietario de la cuenta de usuario es su usuario, que es responsable de su uso y de todas las transacciones realizadas con dicha cuenta de usuario.

2. Utilizar todo tipo de cuentas de servicios (correo electrónico, redes sociales, etc.) que sean personales y ajenos a los otorgados por el Organismo. En el caso de no contar con una cuenta corporativa, al momento de iniciarse los servicios a prestarse, deberá pedir autorización e indicar cuál será la cuenta de correo que se utilizará durante la prestación de los servicios.
3. El uso e instalación de todo tipo de software, licenciado o no, que no se encuentre expresamente habilitado por el Área de Informática para el desarrollo de las funciones en las estaciones de trabajo. En caso de que, para la realización de una determinada actividad encargada por un superior, sea necesaria la utilización de un software no habilitado, deberá realizarse un pedido de autorización por escrito, indicando la funcionalidad requerida.
4. Realizar copias no autorizadas del software que pertenece al Organismo, excepto en los casos permitidos por ley, por el fabricante o por el Responsables de Activos de Información. Los usuarios no deben copiar software ni otros materiales originales de otras fuentes, y son responsables por todas las consecuencias que pudieran surgir bajo la ley de propiedad intelectual.
5. Difundir al público o personas no autorizadas, cualquier tipo de información privada, clasificada o confidencial perteneciente al Organismo.
6. El envío de cualquier tipo de mensaje ajeno a las actividades del Organismo (spam, cadenas de mails, etc.), desde o hacia las cuentas de correo corporativas.
7. El envío de archivos adjuntos de extensiones no permitidas por el Área de Informática del Organismo.
8. Modificar la configuración de los clientes de correo del Organismo o enviar correo utilizando como remitente direcciones que no se le hayan sido asignadas
9. Acceder a Internet mediante módems, Internet móvil, red inalámbrica u otros dispositivos de acceso directo a Internet que no sean provistos por el Organismo.
10. Participar en actividades que puedan ser utilizadas para eludir controles de seguridad de los sistemas de información.

2.3.6 Responsabilidades del Usuario

2.3.6.1 Uso de Contraseñas seguras

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

Los usuarios deben cumplir las siguientes directivas:

a) Mantener las contraseñas en secreto.

b) Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.

c) Seleccionar contraseñas de calidad, de acuerdo a las prescripciones informadas por el responsable del Activo de Información de que se trate, que:

- Sean fáciles de recordar.
- No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo, nombres, números de teléfono, fecha de nacimiento, etc.

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

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

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

f) Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, autoguardado en navegadores de internet, o aquellas almacenadas en una tecla de función o macro.

g) Notificar cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

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

El usuario entiende y comprende que su contraseña debe ser secreta y no debe ser revelada a compañeros de trabajo ni otras personas externas, comprendiendo que toda actividad realizada con su usuario será su responsabilidad.

2.3.6.2 Reporte de incidentes de Seguridad de la Información

Un incidente de Seguridad de la Información se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la Política de Seguridad de la Información.

El reporte de los incidentes permite responder a los mismos en forma sistemática, minimizar su ocurrencia, facilitar una recuperación rápida y eficiente de las actividades minimizando la pérdida de información y la interrupción de los servicios, mejorar continuamente el marco de seguridad y el proceso de tratamiento de incidentes, y manejar correctamente los aspectos legales que pudieran surgir durante este proceso.

Al presentarse un fallo o incidente de Seguridad de la Información, el usuario entiende y comprende que deberá comunicarlo de inmediato con el Área de Informática, en caso de no poder contactarse envíe un correo electrónico a **seguridad.informatica@bn.gob.ar.**

La información mínima que debe proveer es:

- Nombre y Apellido
- Área
- Interno y/o correo electrónico
- Fecha y hora de la detección
- Recurso o activo afectado
- Ubicación
- Descripción del incidente.

2.3.7 Monitoreo y auditoría del uso de los activos físicos y de información

El Organismo, en concordancia con la potestad de dirección y control de la Ley N.º 20.744 de Contrato de Trabajo, que en su art. 70 confiere la facultad de ejercer controles personales sobre los trabajadores destinados a la protección de los bienes del Organismo, salvaguardando la dignidad del trabajador, a través del presente

documento informa y define expresamente el ejercicio de dichos controles, de acuerdo a lo siguiente:

a) El usuario acepta y comprende que todos los datos creados, almacenados, enviados o recibidos a través del sistema de información, o de otro sistema de comunicación, del Organismo, incluyendo diversas aplicaciones, correo electrónico, Internet, fax, etc., independientemente de si es personal o no, se considera propiedad del Organismo y estará sujeto a los sistemas de monitoreo y control que tendrán como finalidad la verificación del cumplimiento de las obligaciones y responsabilidades establecidas en las Políticas de Seguridad de la Información por parte de todo el personales del Organismo (internos y externos).

b) El usuario acepta y comprende que en los casos que se considere necesario, el Comité de Seguridad de la Información estará autorizado para el acceso y auditoría de todas las cuentas corporativas asignadas al usuario investigado con la finalidad de salvaguardar los intereses del Organismo. El usuario entiende y acepta que dichas auditorías sobre las cuentas corporativas no serán consideradas una violación de privacidad o expectativa de privacidad del usuario.

c) El usuario acepta y comprende que toda utilización de los recursos del Organismo, tanto activos físicos como de información, con propósitos no autorizados o ajenos al destino para el cual fueron provistos podrá ser considerado como uso indebido o inadecuado, con sus consecuentes sanciones disciplinarias.

d) El Organismo se reserva el derecho de monitorear y auditar en todo momento los recursos corporativos de todo el Organismo, entendiendo como monitoreo a aquel tipo de control general sobre los datos de tráfico, sin acceso a los contenidos, que podrán o no ser automatizados, destinados tanto a la detección del fraude corporativo como de la comisión de acciones irregulares o prohibidas por parte de los usuarios. Se considerarán controles de monitoreo, de manera enunciativa y no restrictiva:

   - Filtros de spam
   - Filtros antispyware
   - Logs de sitios visitados (sin trazado de usuario)
   - Logs de software antimalware
   - Logs de impresiones realizadas
   - Análisis sobre transferencia de datos en la red.
   - Otros a definir por el personal del Área de Informática de acuerdo a la tecnología disponible en el Organismo.

e) El Organismo se reserva el derecho de acceder, sólo en casos de excepción y por orden escrita de la Dirección, a los contenidos de los recursos informáticos corporativos. Serán considerados casos de excepción, aquellos donde para resguardar los intereses del Organismo sea indispensable tomar conocimiento del contenido de los datos de las cuentas corporativas. Son casos de excepción, a modo enunciativo y no restrictivo cuando:

   - Existiese sospecha fundada de la comisión de infracciones graves a las Políticas de Seguridad de la Información;
   - Existiese sospecha fundada sobre la comisión de delitos informáticos;
   - Existiese sospecha de infidelidad laboral;
   - Existiese imposibilidad física o psíquicamente imposibilitado del usuario para continuar realizando las actividades designadas con normalidad;

- Existiese un riesgo grave o inminente para el Organismo que requiera el acceso a dicha información corporativa.
- En todos los casos, el Organismo guardará registros de todas las actividades realizadas, a través de los procedimientos adecuados para su conservación e integridad, con el objeto de poder ser utilizada como evidencia para la aplicación de procedimientos internos de sanciones, o para facilitar el acceso a la justicia por exigencias legales.

3. Control de Acceso

Los recursos informáticos y de comunicaciones puestos por el Organismo a disposición de sus empleados están destinados a ser utilizados en el desarrollo de las actividades diarias.

El Organismo se reserva el derecho de acceder a todos los equipos y sistemas utilizados en el desarrollo de sus negocios, con fines de soporte operacional y/o para la protección de sus activos.

2.1 Lineamientos para el Control de Accesos

Todo sistema de Tecnología de la Información (IT), red y aplicación debe tener mecanismos de seguridad definidos e implementados, para proveer un nivel apropiado de protección a la información que maneja.

Para que una persona tenga acceso a sistemas o aplicaciones, sus derechos de acceso deben ser expresamente autorizados y su identidad verificada.

Está estrictamente prohibido compartir las claves de acceso a los sistemas, las mismas deben ser mantenidas en secreto y seguras en forma permanente.

Se deben implementar procedimientos para controlar la utilización de los derechos de acceso a las aplicaciones y para asegurar que el nivel de acceso otorgado es consistente con las funciones de cada usuario.

Los usuarios de sistemas de IT, redes y aplicaciones, deben ser responsables del uso seguro de sus dispositivos y datos de autenticación (usuarios, claves de acceso, PINs, etc.).

2.2 Administración del Acceso de Usuario

Todos los recursos de Tecnología de la Información del Organismo (hardware y software) son provistos para su uso y cumplimiento de los objetivos del Organismo y deben ser utilizados exclusivamente para ello, un uso personal razonable está permitido si cumple con las restricciones dictadas por esta Política, como ser:

- Se realice fuera de su horario de trabajo para que no interfiera ni con su productividad, ni con la de otros empleados.
- No consuma recursos que compitan con la producción (ej. consumo excesivo de Internet)
- No signifique un riesgo legal al Organismo (ej. violación de derechos de autor u otro).
- No consuma recursos que signifiquen cargos para el Organismo (ej. impresiones, papel, comunicaciones telefónicas no vinculadas a la actividad laboral, medios magnéticos, etc.).
- No está permitido el uso de dispositivos personales o de terceros en el Organismo, ni conectarlos a los recursos de IT del Organismo. Pueden ser autorizadas excepciones, a criterio del Área de Informática. En este caso, las previsiones de esta Política se deben aplicar tanto al uso como al almacenamiento de cualquier información en ese dispositivo.
- No está permitida la instalación, actualización y/o utilización de software que no esté debidamente autorizado y homologado por el Área de Informática.
- No está permitida la apertura de equipos y/o estaciones de trabajo, impresoras, escáner, o cualquier otro

dispositivo informático por parte de los usuarios.

- No está permitido realizar actividades usando equipamiento o sistemas de la empresa que este fuera del alcance de la tarea diaria.

2.3 Sistemas de Control de Acceso

El acceso a los sistemas informáticos debe ser controlado y restringido a usuarios autorizados solamente, de manera de minimizar el riesgo de accesos indebidos.

Los dispositivos de seguridad de una aplicación deben ser capaces de identificar y verificar la identidad de cada usuario autorizado, mediante mecanismos de autenticación definidos por los responsables de Gestión de Accesos.

Las directrices para la implementación de sistemas de Control de Acceso se encuentran definidas en la Política de Control de Acceso.

2.4 Monitoreo del Acceso a los Sistemas y su Uso

Los accesos a los sistemas serán registrados y monitoreados para asegurar el cumplimiento de las normas de acceso.

El Área de Informática debe definir el alcance de todas las actividades de monitoreo y control. Las mismas deben ser documentadas y reflejar los riesgos asociados.

4. Seguridad Física y Ambiental

2.5 Seguridad Física de la Información

Todos los recursos de tecnología informática que son críticos para la continuidad del Organismo deben ser físicamente asegurados.

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

Se debe proteger el equipo de amenazas físicas y ambientales.

La responsabilidad por la protección de las computadoras de escritorio, notebook y los dispositivos móviles que se utilizan dentro de las oficinas del Organismo, que en algunos casos contienen y procesan información crítica, es responsabilidad de los usuarios a quienes han sido asignados. El acceso físico a los sistemas de Tecnología de Información, incluyendo la infraestructura de comunicaciones, debe estar limitado a los empleados autorizados. Todos los Servidores se deben mantener en un área de acceso restringido y controlado.

Si la información o el equipamiento informático son sacados de las oficinas con la debida autorización, sigue aun siendo propiedad de la empresa, y como tal, deberá ser usado en las actividades para las que fue autorizado.

Cada vez que el personal deje su oficina o escritorio, se debe asegurar que ninguna información confidencial u otro material sensitivo queden desprotegidos. El manejo de la información impresa y de los medios de almacenamiento deberán cumplir los requerimientos definidos.

2.6 Medios Removibles

Cuando se utilicen medios removibles (disco, cinta, CD/DVD, Pen drive u otro medio de almacenamiento) para almacenar o transportar información sensible o altamente sensible se debe almacenar en forma cifrada.

Los medios removibles se deben mantener con un nivel de seguridad física acorde al nivel de protección que la información almacenada requiera.

2.7 Comunicaciones escritas y por voz

Toda la información en formato físico, escrita o impresa debe ser clasificada de acuerdo a sus requerimientos de seguridad. Esta información incluye registros de papel y comunicaciones (e-mail, mensajería instantánea, etc.).

Cuando la información escrita es transferida y almacenada, la clasificación de la información debe ser claramente indicada.

La información de clasificación *confidencial o estrictamente confidencial* no se debe transmitir a través de teléfono, mensajería instantánea, chat o correo electrónico sin cifrado.

2.8 Destrucción de información

El descarte de los medios requiere un tratamiento acorde con el nivel de clasificación de Seguridad de la Información almacenada.

Para el caso de la información confidencial y estrictamente confidencial el medio debe ser físicamente destruido o debidamente borrado.

5. Gestión de Comunicaciones y Operaciones

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

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

Las comunicaciones establecidas permiten el intercambio de información, que deberá estar regulado para garantizar las condiciones de Confidencialidad, Integridad y Disponibilidad de la información que se emite o recibe por los distintos canales.

2.9 Procedimientos y Responsabilidades Operativas

Se documentarán y mantendrán actualizados los procedimientos operativos identificados en esta Política y sus cambios serán autorizados por el Comité de Seguridad de la Información.

Los procedimientos especificarán instrucciones para la ejecución detallada de cada tarea, incluyendo pero no limitado a:

1. Requerimientos de programación de procesos, interdependencias con otros sistemas, tiempos de inicio de las primeras tareas y tiempos de terminación de las últimas tareas.
2. Instrucciones para el manejo de errores u otras condiciones excepcionales que puedan surgir durante la ejecución de tareas.
3. Restricciones en el uso de utilitarios del sistema.
4. Personas de soporte a contactar en caso de dificultades operativas o técnicas imprevistas.
5. Instrucciones especiales para el manejo de “salidas”, como el uso de papelería especial o la administración de salidas confidenciales, incluyendo procedimientos para la eliminación segura de salidas fallidas de tareas.
6. Reinicio del sistema y procedimientos de recuperación en caso de producirse fallas en el sistema.

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

1. Instalación y mantenimiento de equipamiento para el procesamiento de información y comunicaciones.
2. Instalación y mantenimiento de las plataformas de procesamiento.
3. Monitoreo del procesamiento y las comunicaciones.
4. Inicio y finalización de la ejecución de los sistemas.
5. Programación y ejecución de procesos.
6. Gestión de servicios.
7. Resguardo de información.
8. Gestión de incidentes de seguridad en el ambiente de procesamiento y comunicaciones.

9. Reemplazo o cambio de componentes del ambiente de procesamiento y comunicaciones.
10. Uso del correo electrónico.

2.10 Control de cambios en las operaciones

Se definirán procedimientos para el control de los cambios en el ambiente operativo y de comunicaciones. Todo cambio deberá ser evaluado previamente en aspectos técnicos y de seguridad.

El Comité de Seguridad de la Información controlará que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de los mismos ni de la información que soportan. El responsable del Área Informática evaluará el posible impacto operativo de los cambios previstos y verificará su correcta implementación.

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

Los procedimientos de control de cambios contemplarán los siguientes puntos:

1. Identificación y registro de cambios significativos.
2. Evaluación del posible impacto de dichos cambios.
3. Aprobación formal de los cambios propuestos.
4. Planificación del proceso de cambio.
5. Prueba del nuevo escenario.
6. Comunicación de detalles de cambios a todas las personas pertinentes.
7. Identificación de las responsabilidades por la cancelación de los cambios fallidos y la recuperación respecto de los mismos.

2.11 Planificación y aprobación de sistemas

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

Sugerirán criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, solicitando la realización de las pruebas necesarias antes de su aprobación definitiva. Se deben considerar los siguientes puntos:

1. Verificar el impacto en el desempeño y los requerimientos de capacidad de las computadoras.
2. Garantizar la recuperación ante errores.
3. Preparar y poner a prueba los procedimientos operativos de rutina según normas definidas.
4. Garantizar la implementación de un conjunto acordado de controles de seguridad.

5. Confeccionar disposiciones relativas a la continuidad de las actividades del Organismo.
6. Asegurar que la instalación del nuevo sistema no afectará negativamente los sistemas existentes, especialmente en los períodos pico de procesamiento.
7. Considerar el efecto que tiene el nuevo sistema en la seguridad global del Organismo.
8. Disponer la realización de entrenamiento en la operación y/o uso de nuevos sistemas.

2.12 Cifrado de Información

El cifrado de los datos es necesario para proteger los datos sensibles almacenados en los dispositivos, los que son transferidos a través de las redes de comunicaciones, o los que son protegidos en los medios de backups.

Los esquemas de cifrado deberán ser aplicados en base a los niveles de exposición al riesgo y las reglas de este deberán ser estipuladas en el Estándar de Cifrado, a definirse por el Área de Informática.

Para lograr un adecuado cifrado deberán usarse algoritmos y longitudes de llaves confiables, los cuales deberán ser continuamente actualizados para mantener su compatibilidad con los últimos avances técnicos.

2.13 Controles contra el software malicioso

El Área de Informática definirá controles de detección y prevención para la protección contra software malicioso. El responsable del Área de Sistemas, o el personal designado por éste, implementarán dichos controles.

El Área de Informática desarrollará procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.

Estos controles deberán considerar las siguientes acciones:

1. Prohibir el uso de software no autorizado por el Organismo.
2. Redactar procedimientos para evitar los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas, o por cualquier otro medio, señalando las medidas de protección a tomar.
3. Instalar y actualizar periódicamente software de detección y eliminación de malware, examinado dispositivos y medios informáticos, como medida precautoria y rutinaria.
4. Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles (probar dichas actualizaciones en un entorno de prueba previamente si es que constituyen cambios críticos a los sistemas).
5. Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos del Organismo, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.
6. 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.
7. Redactar procedimientos para verificar toda la información relativa a software malicioso, garantizando que los boletines de alerta sean exactos e informativos.

8. Concientizar al personal acerca de la problemática del software malicioso, como lo son troyanos, falsos antivirus, ransomware, entre otras amenazas, y de cómo proceder frente a los mismos.

2.14 Mantenimiento y resguardo de la información

El Área de Informática y los Propietarios de Información determinarán los requerimientos para resguardar cada software o dato en función de su criticidad. En base a ello, se definirá y documentará un esquema de resguardo de la información.

El responsable del Área Informática dispondrá y controlará la realización de dichas copias, así como la prueba periódica de su restauración. Para esto se deberá contar con instalaciones de resguardo que garanticen la disponibilidad de toda la información y del software crítico del Organismo. Los sistemas de resguardo deberán probarse periódicamente, asegurándose que cumplen con los requerimientos de los planes de continuidad de las actividades del Organismo.

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

1. Definir un esquema de identificación de las copias de resguardo, que permita contar con toda la información necesaria para reconocer cada una de ellas y administrarlas debidamente.
2. Establecer un esquema de reemplazo de los medios de almacenamiento de las copias de resguardo, una vez concluida la posibilidad de ser reutilizados, de acuerdo a lo indicado por el proveedor, y asegurando la destrucción de los medios desechados.
3. Almacenar en una ubicación remota copias recientes de información de resguardo junto con registros exactos y completos de las mismas y los procedimientos documentados de restauración, a una distancia suficiente como para evitar daños provenientes de un desastre en el sitio principal. Para la definición de información mínima a ser resguardada en el sitio remoto, se deberá tener en cuenta el nivel de clasificación otorgado a la misma, en términos de disponibilidad y requisitos legales a los que se encuentre sujeta.
4. Asignar a la información de resguardo un nivel de protección física y ambiental según las normas aplicadas en el sitio principal. Extender los mismos controles aplicados a los dispositivos en el sitio principal al sitio de resguardo.
5. Probar periódicamente los medios de resguardo.
6. Verificar y probar periódicamente los procedimientos de restauración garantizando su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos.
7. Los procedimientos de realización de copias de resguardo y su almacenamiento deberán respetar las disposiciones de la regulación sobre control de registros de la presente política.

2.15 Registro de actividades y fallas en los sistemas de operación

El Comité de Seguridad de la Información asegurará el registro de las actividades realizadas en los sistemas, incluyendo según corresponda:

1. Tiempos de inicio y cierre del sistema.
2. Errores del sistema y medidas correctivas tomadas.

3. Intentos de acceso a sistemas, recursos o información crítica o acciones restringidas
4. Ejecución de operaciones críticas
5. Cambios a información crítica

El Comité de Seguridad de la Información desarrollará y verificará el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas.

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

1. Revisión de registros de fallas para garantizar que las mismas fueron resueltas satisfactoriamente.
2. Revisión de medidas correctivas para garantizar que los controles no fueron comprometidos, y que las medidas tomadas fueron autorizadas.
3. Documentación de la falla con el objeto de prevenir su repetición o facilitar su resolución en caso de reincidencia.

2.16 Seguridad del Correo Electrónico

2.16.1 Riesgos de Seguridad

Se implementarán controles para reducir los riesgos de incidentes de seguridad en el correo electrónico, contemplando los siguientes aspectos:

1. La posible interceptación de comunicaciones electrónicas y el consecuente acceso a los mensajes.
2. La posible recepción de código malicioso en un mensaje de correo, el cual afecte la seguridad del dispositivo receptor o de la red a la que se encuentra conectada.
3. El uso inadecuado por parte del personal.
4. Las consideraciones legales, como la necesidad potencial de contar con prueba de origen, envío, entrega y aceptación.
5. Las implicancias de la publicación externa de listados de personal, accesibles al público.
6. El acceso de usuarios remotos a las cuentas de correo electrónico.

2.16.2 Política de Correo Electrónico

El Área de Informática definirá y documentará normas y procedimientos claros con respecto al uso del correo electrónico, que incluya al menos los siguientes aspectos:

1. Medidas de seguridad para el correo electrónico.
2. Protección de archivos adjuntos de correo electrónico.
3. Uso de técnicas criptográficas para proteger la confidencialidad e integridad de los mensajes electrónicos.
4. Retención de mensajes que, si se almacenaran, pudieran ser usados en caso de litigio.
5. Controles adicionales para examinar mensajes electrónicos que no pueden ser autenticados.
6. Aspectos operativos para garantizar el correcto funcionamiento [illegible]

información transmitida y recibida, cantidad de destinatarios, tamaño máximo del buzón del usuario, etc.).

7. Definición de los alcances del uso del correo electrónico por parte del personal del Organismo.
8. Potestad del Organismo para auditar los mensajes recibidos o emitidos por los servidores del Organismo, lo cual se incluirá en el “Compromiso de Confidencialidad”.

2.17 Seguridad en dispositivos móviles y trabajo remoto

2.17.1 Dispositivos Móviles

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

Se deberá tener en cuenta en este sentido, cualquier dispositivo móvil y/o removible, incluyendo: notebooks, laptop, teléfonos celulares y sus tarjetas de memoria, dispositivos de almacenamiento removibles, tales como CDs, DVDs, pendrive, y cualquier dispositivo de almacenamiento de conexión USB, tarjetas de identificación personal (control de acceso), dispositivos criptográficos, cámaras digitales, etc.

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

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

1. La protección física necesaria
2. El acceso seguro a los dispositivos
3. La utilización de los dispositivos en lugares públicos.
4. El acceso a los sistemas de información y servicios del Organismo a través de dichos dispositivos.
5. Las técnicas criptográficas a utilizar para la transmisión de información clasificada.
6. Los mecanismos de resguardo de la información contenida en los dispositivos.
7. La protección contra software malicioso.

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

1. Proteger el dispositivo mediante algún control de acceso (Contraseña, Pin, Patrón, Huella, etc.)
2. Mantener cifrada la información clasificada.
3. Permanecer siempre cerca del dispositivo.
4. No dejar desatendidos los equipos.
5. No llamar la atención acerca de portar un equipo valioso.
6. No poner identificaciones del Organismo en el dispositivo, salvo los estrictamente necesarios.
7. No poner datos de contacto técnico en el dispositivo.

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

1. Revocación de las credenciales afectadas
2. Notificación a grupos de Trabajo donde potencialmente se pudieran haber comprometido recursos.

2.17.2 Trabajo Remoto

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

El trabajo remoto sólo será autorizado por el responsable del área correspondiente, a la cual pertenezca el usuario solicitante, conjuntamente con el Área de Informática, cuando se verifique que son adoptadas todas las medidas que correspondan en materia de Seguridad de la Información, de modo de cumplir con la política, normas y procedimientos existentes.

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

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

1. El ambiente de trabajo remoto propuesto.
2. Los requerimientos de seguridad de comunicaciones, tomando en cuenta la necesidad de acceso remoto a los sistemas internos del Organismo, la sensibilidad de la información a la que se accederá y que pasará a través del vínculo de comunicación y la sensibilidad del sistema interno.
3. La amenaza de acceso no autorizado a información o recursos por parte de otras personas que utilizan el lugar, por ejemplo, familia y amigos.
4. Evitar la instalación de software no autorizada por el Organismo.

Los controles y disposiciones comprenden:

1. Proveer de mobiliario para almacenamiento y equipamiento adecuado para las actividades de trabajo remoto.
2. Definir el trabajo permitido, el horario de trabajo, la clasificación de la información que se puede almacenar en el equipo remoto desde el cual se accede a la red del Organismo y los sistemas internos y servicio a los cuales el trabajador remoto está autorizado a acceder.
3. Proveer de un adecuado equipo de comunicación, con inclusión de métodos para asegurar el acceso remoto.
4. Incluir seguridad física.
5. Definir reglas y orientación respecto del acceso de terceros al equipamiento e información.
6. Proveer el hardware, el soporte y el mantenimiento del software.
7. Definir los procedimientos de backup y de continuidad de las operaciones.
8. Efectuar auditoría y monitoreo de la seguridad.
9. Realizar la anulación de las autorizaciones, derechos de acceso y devolución del equipo cuando finalicen las actividades remotas.

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

Se implementarán procesos de auditoría específicos para los casos de accesos remotos, que serán revisados regularmente. Se llevará un registro de incidentes a fin de corregir eventuales fallas en la seguridad de este tipo de accesos.

2.18 Administración de vulnerabilidades técnicas

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

Se obtendrá información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, la exposición de la empresa a tales vulnerabilidades evaluadas, y se tomarán las medidas necesarias para tratar los riesgos asociados.

Se deben establecer e implementar las reglas que rigen la instalación de software por parte de los usuarios y poner en vigencia una política estricta sobre qué tipo de software pueden instalar los usuarios.

6. Gestión de incidentes

Se establecen directrices, funciones y procedimientos de manejo de incidentes garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad.

Se consideran:

1. Los tipos probables de incidentes relativos a seguridad
2. La comunicación de los incidentes a través de canales gerenciales apropiados tan pronto como sea posible.
3. La consideración de los siguientes aspectos en los procedimientos diseñados para recuperar sistemas y servicios tan pronto como sea posible:
    - Definición de las primeras medidas a implementar
    - Análisis e identificación de la causa del incidente.
    - Planificación e implementación de soluciones para evitar la repetición del mismo, si fuera necesario.
    - Comunicación con las personas afectadas o involucradas con la recuperación, del incidente.
    - Notificación de la acción a la autoridad y/u Organismos pertinentes.
4. El registro de pistas de auditoría y evidencia similar para:
    - Análisis de problemas internos.
    - Uso como evidencia en relación con una probable violación contractual o infracción normativa, o en marco de un proceso judicial.
    - Negociación de compensaciones por parte de los proveedores de software y de servicios.
5. La implementación de controles detallados y formalizados de las acciones de recuperación respecto de las violaciones de la seguridad y de corrección de fallas del sistema, garantizando:
    - Acceso a los sistemas y datos existentes sólo al personal claramente identificado y autorizado.
    - Documentación de todas las acciones de emergencia emprendidas en forma detallada.
    - Comunicación de las acciones de emergencia al titular de la Unidad Organizativa y revisión de su cumplimiento.
    - Constatación de la integridad de los controles y sistemas del Organismo en un plazo mínimo.

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

REFERENTE A LA ORGANIZACIÓN

7. Organización de la Seguridad

2.19 Interna

Se describen a continuación los principales roles de la seguridad informática en el Organismo:

1. **Comité de Seguridad de la Información:** El Comité de Seguridad de la Información, es un cuerpo integrado por representantes de todas las áreas sustantivas del Organismo, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.
2. Además cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de Seguridad de la Información a los integrantes del Organismo que así lo requieran.
3. **Propietario de la información:** referente designado, entre sus funciones se encuentran la clasificación de la información de acuerdo con el grado de sensibilidad y criticidad de la misma, la definición de qué usuarios deben tener permisos de acceso a la información de acuerdo a sus funciones y competencia.
4. **Administrador:** son aquellos puestos asociados con la implementación de reglas de Seguridad de la Información. Entre las funciones se incluye la ejecución de las acciones necesarias para la implementación de las especificaciones de seguridad información (técnicas, administrativas y asociadas con el personal).
5. **Usuario:** Los usuarios de la información y de los sistemas utilizados para su procesamiento son responsables de conocer, dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente.
6. **Auditor:** responsable de realizar verificaciones independientes, practicando auditorías periódicas sobre los sistemas y actividades vinculadas con la tecnología de información, debiendo informar sobre el cumplimiento de las especificaciones y medidas de Seguridad de la Información establecidas por la Política de Seguridad de la Información y por las normas, procedimientos y prácticas que surjan. Con el apoyo del Comité de Seguridad de la Información o de quien el decida.
7. Los roles, responsabilidades como los mecanismos de implementación de la estructura para la gestión de la Seguridad de la Información, se detallan en la documentación asociada a cada proceso.

2.20 Seguridad en el acceso por parte de terceros

Cuando exista la necesidad de otorgar acceso a terceras partes a información del Organismo, el Área de Informática y el Propietario de la Información de que se trate, llevarán a cabo y documentarán una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta, entre otros aspectos:

- El tipo de acceso requerido (físico/lógico y a qué recurso).
- Los motivos para los cuales se solicita el acceso.
- El valor de la información.
- Los controles empleados por la tercera parte.
- La incidencia de este acceso en la Seguridad de la Información del Organismo.
- Si dentro de la Información existen datos personales propios de Organismo o de terceros.

En todos los contratos cuyo objeto sea la prestación de servicios a título personal bajo cualquier modalidad

jurídica que deban desarrollarse dentro del Organismo, se establecerán los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, restringiendo al mínimo necesario, los permisos a otorgar.

Se cita a modo de ejemplo:

1. Personal de mantenimiento y soporte de hardware y software.
2. Limpieza, “catering”, guardia de seguridad y otros servicios de soporte tercerizados.
3. Pasantías y otras designaciones de corto plazo.
4. Consultores, asesores, productores y prestadores.

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

2.21 Requerimientos de Seguridad en Contratos o Acuerdos con Terceros

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

1. Cumplimiento de la Política de Seguridad de la Información del Organismo.
2. Protección de los activos del Organismo, incluyendo procedimientos para proteger los bienes del Organismo, abarcando los activos físicos, la información y el software.

8. Política de Seguridad en Recursos Humanos

El responsable del Área de Recursos Humanos incluirá las funciones relativas a la Seguridad de la Información en las descripciones de puestos de los empleados, informará a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información, gestionará los Compromisos de Confidencialidad con el personal y coordinará las tareas de capacitación de usuarios respecto de la presente Política.

El responsable del Área Legal participará en la confección del Compromiso de Confidencialidad a firmar por los empleados y terceros que desarrollen funciones en el Organismo, en el asesoramiento sobre las sanciones a ser aplicadas por incumplimiento de la presente Política y en el tratamiento de incidentes de seguridad que requieran de su intervención.

2.22 Antes de la relación laboral

Las funciones y responsabilidades en materia de seguridad serán incorporadas en la descripción de las responsabilidades de los puestos de trabajo.

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

Se definirán y comunicarán claramente los roles y responsabilidades de seguridad a los candidatos para el puesto de trabajo durante el proceso de preselección.

RRHH o quien este determine llevarán a cabo controles de verificación del personal en el momento en que se solicita el puesto. Estos controles incluirán todos los aspectos que indiquen las normas que, a tal efecto, alcanzan al Organismo.

Los chequeos de verificación deben incluir:

1. Disponibilidad de referencias de carácter satisfactorias.
2. Chequeo del currículum vitae del postulante.
3. Confirmación de títulos académicos y profesionales mencionados por el postulante.
4. Acreditación de su identidad.
5. Análisis de identidad digital.

2.23 Durante la relación laboral

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

El responsable del Área de Recursos Humanos será el encargado de coordinar las acciones de capacitación que surjan

de la presente Política.

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

El personal que ingrese al Organismo recibirá el material, indicándosele el comportamiento esperado en lo que respecta a la Seguridad de la Información, antes de serle otorgados los privilegios de acceso a los sistemas que correspondan.

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

2.24 Proceso disciplinario

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

El proceso disciplinario también se puede utilizar como un elemento disuasivo para evitar que los empleados, contratistas y terceros violen la políticas y procedimientos de la seguridad del Organismo.

2.25 Cese de la relación laboral o cambio de puesto de trabajo

Las responsabilidades para realizar la desvinculación o cambio de puesto deben ser claramente definidas y asignadas, incluyendo requerimientos de seguridad y responsabilidades legales a posteriori, cuando sea apropiado, las responsabilidades contenidas dentro de cualquier acuerdo de confidencialidad, y los términos y condiciones de empleo con continuidad por un periodo definido de tiempo luego de la finalización del trabajo del empleado, contratista o usuario de tercera parte. Puede ser necesario informar a los empleados, contratistas y terceros de los cambios en el personal y los acuerdos de operación.

Todos los empleados, contratistas y usuarios de terceras partes deben devolver todos los activos del Organismo en su poder (software, documentos corporativos, equipamiento, dispositivos de computación móviles, tarjetas de crédito, tarjetas de ingreso, etc.) tras la terminación de su empleo, contrato, o acuerdo.

En los casos donde el empleado, contratista y usuarios tengan conocimiento que es importante para las operaciones actuales, esa información debe ser documentada y transferida al Organismo.

Se revisarán los derechos de acceso de un individuo a los activos asociados con los sistemas y servicios de información tras la desvinculación. Esto determinará si es necesario remover los derechos de acceso.

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

Si un empleado, contratista o usuario de tercera parte que se está desvinculando tiene conocimiento de contraseñas para cuentas que permanecen activas, estas deben ser cambiadas tras la finalización o cambio de empleo, contrato o acuerdo.

Se evaluará la reducción o eliminación de los derechos de acceso a los activos de la información y a las instalaciones de procesamiento de la información antes de que el empleo termine o cambie, dependiendo de factores de riesgos.

tales como:

1. Si el termino o cambio es iniciado por el empleado, contratista o usuario de tercera parte, o por la gestión y la razón de la finalización.
2. Las responsabilidades actuales del empleado, contratista o cualquier otro usuario.
3. El valor de los activos accesibles actualmente.

9. Adquisición, Desarrollo y Mantenimiento de Sistemas

Se debe garantizar que la seguridad sea una parte integral de los sistemas de información.

Se deben identificar y acordar los requerimientos de seguridad antes del desarrollo y/o implementación de los sistemas de información, así como del todo el ciclo de vida del desarrollo de software (SDLC).

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

1. La validación efectiva de datos de entrada y salida.
2. El procesamiento interno.
3. La autenticación de mensajes (interfaces entre sistemas).
4. La validación de datos de salida.
5. Modelado de amenazas.
6. Capacitación del personal relacionado con el desarrollo de software.
7. Pruebas de seguridad en ambientes de testing, QA y relacionado.
8. Pruebas periódicas de seguridad en entornos de producción.

Se garantizará que los desarrollos y actividades de soporte a los sistemas se lleven a cabo de manera segura, controlando el acceso a los archivos del mismo y la adecuada separación de ambientes (desarrollo, testing, producción, etc.).

Se controlarán los entornos y el soporte dados al software y a la información del sistema de aplicación.

10. Política de Continuidad de la Gestión

2.26 Introducción

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

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

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

2.27 Proceso de la Administración de la Continuidad del Organismo

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

Este Comité tendrá a cargo la coordinación del proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de información del Organismo frente a interrupciones imprevistas, lo cual incluye las siguientes funciones:

1. Identificar y priorizar los procesos críticos de las actividades del Organismo.
2. Asegurar que todos los integrantes del Organismo comprendan los riesgos que la misma enfrenta, en términos de probabilidad de ocurrencia e impacto de posibles amenazas, así como los efectos que una interrupción puede tener en la actividad del Organismo.
3. Elaborar y documentar una estrategia de continuidad de las actividades del Organismo consecuente con los objetivos y prioridades acordados.
4. Proponer planes de continuidad de las actividades del Organismo de conformidad con la estrategia de continuidad acordada.
5. Establecer un cronograma de pruebas periódicas de cada uno de los planes de contingencia, proponiendo una asignación de funciones para su cumplimiento.
6. Coordinar actualizaciones periódicas de los planes y procesos implementados.
7. Considerar el análisis y la contratación de seguros, que podrían formar parte del proceso de continuidad de las actividades del Organismo.
8. Proponer las modificaciones a los planes de contingencia.

2.28 Continuidad de las Actividades y Análisis de los Impactos

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

Identificar los eventos (amenazas) que puedan ocasionar interrupciones en los procesos de las actividades, por ejemplo, fallas en el equipamiento, comisión de ilícitos, interrupción del suministro de energía eléctrica, inundación e incendio, desastres naturales, destrucción edilicia, atentados, etc.

Evaluar los riesgos para determinar el impacto de dichas interrupciones, tanto en términos de magnitud de daño como del período de recuperación. Dicha evaluación debe identificar los recursos críticos, los impactos producidos por una interrupción, los tiempos de interrupción aceptables o permitidos, y debe especificar las prioridades de recuperación.

Identificar los controles preventivos, como por ejemplo sistemas de supresión de fuego, detectores de humo y fuego, contenedores resistentes al calor y a prueba de agua para los medios de backup, los registros no electrónicos vitales, etc.

Esta actividad será llevada a cabo con la activa participación de los propietarios de los procesos y recursos de información de que se trate y del Área de Informática, considerando todos los procesos de las actividades del Organismo y no limitándose a las instalaciones de procesamiento de la información.

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

11.Política de Cumplimiento Legal

2.29 Introducción

El diseño, operación, uso y administración de los sistemas de información están regulados por disposiciones legales y contractuales las cuales Organismo cumple.

Los requisitos normativos y contractuales pertinentes a cada sistema de información deben estar debidamente definidos y documentados de forma tal de facilitar el cumplimiento por parte del Organismo y sus empleados.

El Área Legal del Organismo, será responsable de encuadrar jurídicamente la formulación e implementación de la política.

2.30 Identificación de normativa aplicable

El Responsable de Seguridad de la Información, con la asistencia del Área Jurídica, serán los encargados de implementar los siguientes controles:

1. Elaborar, divulgar y asegurar la aceptación fehaciente de un documento legal que informe sobre las condiciones de uso de los recursos informáticos del Organismo, incluyendo cláusulas de confidencialidad sobre la información y destacándose las potestades de control y monitoreo que se reserva el Organismo. Todos los empleados deben conocer el alcance preciso del uso adecuado de los recursos informáticos y deben respetarlo.
2. Elaborar y divulgar las políticas de privacidad, tanto para personal interno como externo que acceda a servicios o información del Organismo.
3. Identificar, inscribir y asegurarse que todas las bases de datos personales que posee el Organismo cumplan con todas las obligaciones y principios vigentes en la normativa sobre protección de datos personales.
4. Al menos una vez por año, realizar una revisión y actualización de la normativa vigente aplicable, especialmente en materia de protección de datos personales.
5. Llevar un registro de las obligaciones legales contraídas contractualmente, que deberá ser controlado y actualizado en cooperación el Área Jurídica.

A continuación, se detalla un listado de la normativa considerada como aplicable al momento de la elaboración de las presentes políticas.

2.31 Derechos de Propiedad Intelectual

En materia de Propiedad Intelectual, Organismo cumple con la siguiente normativa aplicable:

1. **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.
2. **Ley de Marcas N° 22.362:** Protege la propiedad de una marca y la exclusividad de su uso.

3. **Ley de Patentes de Invención y Modelos de Utilidad N° 24.481:** Protege el derecho del titular de la patente de invención a impedir que terceros utilicen su producto o procedimiento.

El Responsable de Seguridad de la Información, con la asistencia del Área Jurídica, serán los encargados de analizar los términos y condiciones de las licencias, e implementarán los siguientes controles:

1. 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.
2. Divulgar las políticas de adquisición de software y las Disposiciones de la Ley de Propiedad
3. Intelectual, y notificar la determinación de tomar acciones disciplinarias contra el personal que las infrinja.
4. Verificar que sólo se instalen productos con licencia y software autorizado.
5. Mantener un adecuado registro de activos.
6. Conservar pruebas y evidencias de propiedad de licencias, discos maestros, manuales y llaves durante el plazo de uso de las mismas.
7. Implementar controles para evitar el exceso del número máximo permitido de usuarios en los sistemas.
8. Elaborar y divulgar un procedimiento para el mantenimiento de condiciones adecuadas con respecto a las licencias.
9. Elaborar y divulgar un procedimiento relativo a la eliminación o transferencia de software a terceros.
10. Utilizar herramientas de auditoría adecuadas que permitan que, ante el caso de un incidente de seguridad, se pueda identificar los detalles del mismo (fecha, usuario, servicios, etc.)
11. Cumplir con los términos y condiciones establecidos para obtener software e información en redes públicas.
12. En el caso de desarrollo interno de software, garantizar que los mismos se realicen siguiendo las buenas prácticas de desarrollo seguro.
13. En el caso de desarrollo interno de software, identificar y verificar que todos los empleados vinculados a las tareas de desarrollo se encuentren debidamente categorizados para la realización de dichas tareas.

2.31.1 Guarda y Protección de los Registros del Organismo

En materia de Guarda y Protección de Registros, Organismo cumple con la siguiente normativa aplicable:

- **Art. 328 del Código Civil y Comercial de la Nación**: Establece que deberá conservarse por el plazo mínimo de 10 años cualquier información relativa a: a) los libros contables, contándose el plazo desde el último asiento; b) los demás registros, desde la fecha de la última anotación practicada sobre los mismos; y c) los instrumentos respaldatorios, desde su fecha.
- **Decreto 1397/79 (Art. 48) y RG 2746/10 (Art. 42) – AFIP:** Establece la obligación de guarda de comprobantes y documentos que acrediten las operaciones vinculadas a su actividad, por un término de hasta 5 años después de operada la prescripción del período fiscal a que se refiere.
- **Código Penal (Art. 255):** Sanciona a quien sustrajere, ocultare, destruyere o inutilizare objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario o de otra persona en el interés del servicio público. Si el culpable fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo.

- **Ley 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
- **Decreto N.º 41.223/1934:** Reglamenta la Ley 11.723 de Propiedad Intelectual.
- **Ley de Firma Digital N° 25.506:** 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 2do párrafo):** Sanciona a aquel que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos.
- **Ley de Confidencialidad sobre Información y Productos N.º 24.766:** que estén legítimamente bajo control de una persona y se divulgue indebidamente de manera contraria a los usos comerciales honestos.
- Decisión Administrativa Nº 641/2021, los "Requisitos Mínimos De Seguridad De La Información Para Los Organismos Del Sector Público Nacional" y el deber de que cada organismo apruebe un "Plan de Seguridad" que establezca los plazos en que dará cumplimiento a cada uno de esos "requisitos mínimos", plazos que no deberán exceder la fecha del 31 de diciembre de 2022.

El Responsable de Seguridad de la Información, con la asistencia del Área Jurídica, serán los encargados de analizar los términos y condiciones de la licencia, e implementará los siguientes controles:

1. Elaborar y divulgar los lineamientos para la retención, almacenamiento, manipulación y eliminación de registros e información.
2. Preparar un cronograma de retención identificando los tipos esenciales de registros y el período durante el cual deben ser retenidos.
3. Mantener un inventario de programas fuentes de información clave.
4. Implementar adecuados controles para proteger la información y los registros esenciales contra pérdida, destrucción y falsificación.
5. Clasificar los registros se clasificarán en diferentes tipos, por ejemplo, registros contables, registros de base de datos, registros de auditoría y procedimientos operativos, cada uno de ellos detallando los períodos de retención y el tipo de medios de almacenamiento, por ejemplo, papel, microfichas, medios magnéticos u ópticos.
6. Considerar la posibilidad de degradación de los medios utilizados para el almacenamiento de los registros. Los procedimientos de almacenamiento y manipulación se implementarán de acuerdo con las recomendaciones del fabricante.
7. En el proceso de selección de medios de almacenamiento electrónicos, se incluirán los procedimientos para garantizar la capacidad de acceso a los datos (tanto legibilidad de formato como medios) durante todo el período de retención, a fin de salvaguardar los mismos contra eventuales pérdidas ocasionadas por futuros cambios tecnológicos.
8. Los sistemas de almacenamiento de datos serán seleccionados de modo tal que los datos requeridos puedan recuperarse de una manera que resulte aceptable para el caso de pedidos de la justicia.
9. El sistema de almacenamiento y manipulación deberá garantizar una clara identificación de los

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

2.31.2 Protección de Datos y Privacidad de la Información Personal

En materia de Protección de Datos y Privacidad de la Información Personal, Organismo cumple con la siguiente normativa aplicable:

- Constitución de la Nación Argentina: Modificada en 1994. Art. 19 y 43 (Habeas Data).
- **Contrato de Trabajo. Ley 20.744:** el Capítulo VII "De los derechos y deberes de las partes" establece diferentes derechos y obligaciones a ser tenidos en cuenta, tanto por parte del empleador como de los empleados.
- **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.
- **Decreto Reglamentario 1.558/2001:** reglamenta la Ley de Protección de los Datos Personales
- **Convenio Colectivo de Trabajo General:** dispone que todos los agentes deben observar el deber de fidelidad que se derive de la índole de las tareas que le fueran asignadas y guardar la discreción correspondiente, con respecto a todos los hechos e informaciones de los cuales tenga conocimiento en el ejercicio o con motivo del ejercicio de sus funciones.
- **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 (Art. 153 y 153 bis):** sanciona a aquel que abriere o accediere indebidamente a una comunicación electrónica o indebidamente la suprimiere o desviare (Art. 153), al que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido (Art. 153 bis) , al que el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros.
- **Código Penal (Art. 155):** sanciona al que teniendo noticias de un secreto cuya divulgación pueda causar daño, lo revelare sin justa causa.
- **Código Penal (Art. 157 bis):** sanciona al que a sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales, ilegítimamente proporcionare o revelare a otra información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley e ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.
- **Código Penal (Art. 183 2do párrafo):** sanciona al que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos.
- **Ley de Confidencialidad sobre Información y Productos N.º 24.766:** que estén legítimamente bajo control de una persona y se divulgue indebidamente de manera contraria a los usos comerciales honestos.

- **Ley de Derechos del Paciente en su Relación con los Profesionales e Instituciones de la Salud Nº 26.529:** que regula los derechos del paciente sobre su historia clínica y el consentimiento informado luego de recibir la información sobre su tratamiento.
- **Ley de Actos Discriminatorios Nº 23.592:** sanciona a quienes realicen por cualquier medio actos discriminatorios determinados por motivos de raza, religión, nacionalidad, ideología, opinión política o gremial, sexo, posición económica, condición social o caracteres físicos.
- **Ley Nº 21.173 (Art. 1071 bis CC):** sanciona al que arbitrariamente se entrometa en la vida ajena, publique retratos, difunda correspondencia, mortifique a otros en sus costumbres o sentimientos, o perturbe de cualquier modo su intimidad.

Disposiciones de la Agencia de Acceso a la Información Pública:

- **Disposición Nº 2/2003:** habilita el Registro Nacional de Bases de Datos y dispone la realización del Primer Censo Nacional de Bases de Datos.
- **Disposición Nº 1/2004:** implementa, con carácter obligatorio, el Primer Censo Nacional de Archivos, Registros, Bases o Bancos de Datos Privados.
- **Disposición Nº 4/2004:** homologa el Código de Ética de la Asociación de Marketing Directo e Interactivo de Argentina (AMDIA).
- **Disposición Nº 2/2005:** implementa el Registro Nacional de Bases de Datos y los formularios de inscripción.
- **Disposición Nº 7/2005:** aprueba la "Clasificación de Infracciones" y la "Graduación de las Sanciones" a aplicar ante violaciones a las normas de la Ley 25.326 y sus reglamentaciones.
- **Disposición Nº 2/2006:** implementa el Relevamiento Integral de Bases de Datos Personales del Estado Nacional.
- **Disposición Nº 11/2006:** aprueban las "Medidas de Seguridad para el Tratamiento y Conservación de los Datos Personales Contenidos en Archivos, Registros, Bancos y Bases de Datos Públicos no estatales y Privados". (derogada por Resolución 47/2018)
- **Disposición Nº 2/2008:** crea el Repertorio de Jurisprudencia sobre Hábeas Data en el ámbito de la DNPDP y de libre consulta.
- **Disposición Nº 3/2008:** crea el Centro de Jurisprudencia, Investigación y Promoción de la Protección de los Datos Personales en el ámbito de la DNPDP.
- **Disposición Nº 3/2012:** aprueba las Normas de Inspección e Instructivo del Formulario de Inspección de la DNPDP y deroga la Disposición DNPDP N° 05/2008.
- **Disposición Nº 6/2008:** aprueba el Procedimiento de Control en la Ejecución de Formularios de Consentimiento Informado en ensayos de farmacología clínica.
- **Disposición Nº 7/2008:** aprueba la "Guía de Buenas Prácticas en Políticas de Privacidad para las Bases de Datos del Ámbito Público" y el texto modelo de "Convenio de Confidencialidad".
- **Disposición Nº 10/2008:** establece que los responsables y usuarios de bancos de datos públicos o privados, deberán incluir información específica legal en su página web y en toda comunicación o publicidad, y en los formularios utilizados para la recolección de datos.
- **Disposición Nº 4/2009:** establece que la opción para el ejercicio del derecho de retiro o bloqueo

contemplada en el artículo 27, inciso 3, de la Ley 25.326, deberá aparecer en toda comunicación que se efectúe con fines publicitarios, junto con el mecanismo previsto para su ejercicio.

- **Disposición Nº 7/2010:** crea el Centro de Asistencia a las Víctimas de Robo de Identidad en el Ámbito de la Dirección Nacional de Protección de Datos Personales.
- **Disposición Nº 12/2010:** establece que al tratarse datos destinados a difusión pública que contengan datos sensibles o referente a menores, incapaces y asuntos de familia deberán aplicarse procedimientos de disociación y de protección a fin de evitar la identificación del titular del dato.
- **Disposición Nº 17/2010:** establece el sistema informativo denominado "Base Informática para la Comunicación Electrónica Interjurisdiccional sobre Datos Personales en Información Crediticia".
- **Disposición Nº 24/2010:** crea el Registro Nacional de Documentos de Identidad Cuestionados.
- **Disposición Nº 3/2012:** aprueba el "Formulario de Inspección" y el "Instructivo del Formulario de Inspección".
- **Disposición Nº 4/2012:** sustituye el art. 7° de la Disposición DNPDP Nº 02/05 estableciendo que no será necesaria la renovación anual cuando la cantidad de personas en el total de las bases de datos sea menor a 5.000, y se declare que no se realiza tratamiento de datos sensibles.
- **Resolución 47/2018** "Medidas de seguridad recomendadas para el tratamiento y conservación de los datos personales en medios informatizados y no informatizados".
- **Disposición Nº 10/2015 de la Agencia de Acceso a la Información Pública (DNPDP)**, que aprueba las condiciones de licitud para las actividades de recolección y tratamiento de imágenes digitales de personas con fines de seguridad y videovigilancia.
- **Disposición Nº15/2018 de la Agencia de Acceso a la Información Pública (DNPDP),** actualiza el cartel de VIDEOVIGILANCIA para utilizar en las zonas donde se usen cámaras. Actualiza y complementa la Disp. 10/2015 de la AAIP.
- **Disposición Nº 2009622/2016 de la Agencia de Acceso a la Información Pública**, que aclara cómo se debe cumplir con la obligación de dar acceso a los titulares a sus datos personales cuando éstos son recolectados por cámaras de videovigilancia.

2.31.3 Firma Digital y Documentos Electrónicos

En materia de Firma Digital y Documentos Electrónicos, el Organismo cumple con la siguiente normativa aplicable:

- **Ley Nº 25.506 de Firma Digital:** regula la utilización de la Firma Digital y Firma Electrónica en la República Argentina.
- **Decreto Reglamentario Nº 2.628/02:** Reglamenta la Ley Nº 25.506 de Firma Digital.
- **Ley Nº 4.736 de la Ciudad Autónoma de Buenos Aires:** Regula la eficacia jurídica y valor probatorio de la firma digital en la Ciudad de Buenos Aires.
- **Decreto Nº 1028/2003:** disuelve el Ente Administrador de Firma Digital creado por el Decreto 2628/2002 y lo reemplaza por la Oficina Nacional de Tecnologías de Información (ONTI) de la Subsecretaría de la Gestión Pública.
- **Decisión Administrativa Nº 6/2007 de la Jefatura de Gabinete de Ministros:** establece el marco normativo de Firma Digital aplicable al otorgamiento y revocación de licencias a los certificadores

que así lo soliciten.

2.31.4 Delitos Informáticos y Ciberseguridad

En materia de Delitos Informáticos y Ciberseguridad, el Organismo cumple con la siguiente normativa aplicable:

- Código Penal de la Nación Argentina.
- **Ley de Delitos Informáticos Nº 26.388:** modifica y agrega distintos artículos en el Código Penal Argentino, tipificando diferentes delitos informáticos.
- **Ley Nº 26.904 de Grooming:** incorpora el art. 131 del Código Penal que pena con prisión de 6 meses a 4 años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma.

2.32 Recolección de Evidencia

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

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

Para lograr la calidad y totalidad de la evidencia es necesario que se cumplan las siguientes condiciones:

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

2.33 Excepciones de Responsabilidad

En determinadas ocasiones especiales, podrán considerarse exceptuados de responsabilidad ante el incumplimiento de determinadas obligaciones impuestas por las presentes Políticas de Seguridad:

1. En casos de empleados que realicen actividades por orden escrita de la Gerencia. En estos casos, el empleado probando la orden escrita, quedará exento de responsabilidad y será la Gerencia quien responda por las infracciones cometidas.
2. En casos de empleados que pertenezcan al Área de Informática, pueden estar exentos de seguir algunas de las restricciones y/o obligaciones establecidas en las presentes políticas, siempre que sea necesario para cumplir con las responsabilidades a su cargo, o bien, ante las actividades de urgencia que se requieran para mantener bajo control eventos no programados.

Siempre que fuera posible, las excepciones deben ser solicitadas siguiendo el procedimiento correspondiente y en el caso que sea necesario, anexando además la documentación sobre la cual se funda la petición. Las excepciones presentadas formalmente, deben ser revisadas y aprobadas por la Gerencia o autoridad designada para tal función.

2.34 Aceptación de la Política

Todo el personal, agentes, funcionarios y otras personas, organismos y/o empresas relacionadas con la actividad del Organismo deben aceptar y adherir a esta política de Seguridad de la Información, por lo cuál debe ser puesta a disposición para su lectura, comprensión y aceptación.

El incumplimiento de la Política y/o Normas de Seguridad de la Información descriptas podrá dar lugar a la aplicación de medidas disciplinarias.

2.35 Vigencia y actualización de la Política

La presente Política de Seguridad tendrán vigencia indefinida a partir de su publicación.

Asimismo, podrá ser revisada y actualizada de acuerdo con la evaluación de riesgos, y ante la implementación de nuevos programas y/o sistemas, cambios en las operaciones, actualizaciones tecnológicas y nuevas relaciones con terceros.

Las actualizaciones de la Política serán adecuadamente notificadas a los usuarios, entrando en vigencia 30 días posteriores a su aprobación por el Directorio y puesta en conocimiento a los empleados.

Los empleados, asumen entre sus responsabilidades laborales, examinar periódicamente las Políticas de Seguridad, ya que, notificadas las modificaciones durante el plazo establecido, se presumirá el debido conocimiento de tales cambios.

En caso de que las modificaciones sean de una entidad tal que requieran la renovación del consentimiento del personal para la entrada en vigencia, se establecerá un procedimiento de aceptación que facilite la aceptación individual por parte de los empleados.

Anexo 1: Consentimiento informado para personal interno

A través de la presente, a los …… días del mes de …….. del año ……, el Sr./Sra. ……, DNI …… en mi situación de empleado, agente o funcionario del Organismo, declaro:

1. Haber leído y entendido las Políticas de Seguridad de la Información, con los que expreso mi acuerdo.
2. Declaro entender y comprender todos y cada uno de los puntos relacionados al tratamiento adecuado de la información, así como al uso adecuado de los recursos informáticos que se me proveen para el desarrollo de mis tareas laborales.
3. Haber recibido una capacitación creada por profesionales de Seguridad Informática, donde se me han explicado debidamente sobre los detalles y significados relativos a la redacción de las Políticas de Seguridad.
4. Haber tenido oportunidad de hacer preguntas y todas ellas me han sido contestadas completa y satisfactoriamente a mi entender y comprensión.
5. Haber sido correctamente informado sobre la aplicación de las Políticas de Seguridad, así como sus consecuencias ante eventuales infracciones (sanciones).
6. Haber leído y ser correctamente informado sobre el Manual de Tratamiento de Datos Personales, el cual acepto en todos sus términos.

NOMBRE Y APELLIDO: ……

DNI: ……

FIRMA: ……

República Argentina - Poder Ejecutivo Nacional
Las Malvinas son argentinas

Hoja Adicional de Firmas
Anexo

Número: IF-2022-27301779-APN-BNMM#MC

CIUDAD DE BUENOS AIRES
Martes 22 de Marzo de 2022

Referencia: ANEXO I - POLITICAS DE SEGURIDAD DE LA INFORMACION V.1.0

El documento fue importado por el sistema GEDO con un total de 50 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2022.03.22 12:57:13 -03:00

Juan Sasturain
Director
Biblioteca Nacional Mariano Moreno
Ministerio de Cultura

Digitally signed by Gestion Documental Electronica
Date: 2022.03.22 12:57:13 -03:00