**POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN ANMAC 2022.**

## 1. INTRODUCCION.

La presente política de Seguridad de la Información se dicta en cumplimiento de las disposiciones legales vigentes y debe ser conocida y cumplida por toda la planta de trabajadores/as del Organismo sea cual fuere su nivel jerárquico, su situación de revista y la modalidad de contratación.

La información, los procesos, los sistemas, como así también, los recursos humanos son activos muy importantes para la Agencia. Definir, lograr, sostener y mejorar la seguridad de la información debe ser esencial para mantener una eficacia y eficiencia en la operación de las actividades, el cumplimiento normativo y la reputación del Organismo.

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

## 2. OBJETO.

La presente Política de Seguridad de la Información 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/las funcionarios/as y los/las trabajadores/as, contratados/as por diferentes modalidades y demás involucrados internos/as y externos/as, así como respecto a su implementación en todas las dependencias de la jurisdicción.

El objetivo principal de esta Política es definir el propósito, la dirección, los principios, las reglas básicas y los mecanismos de comunicación para la protección de la información del organismo, así como de los recursos utilizados en su tratamiento.

El presente documento se dicta en cumplimiento de las disposiciones legales vigentes, tanto externas al organismo, como leyes nacionales, decretos

resoluciones y disposiciones que sean aplicables a los datos, los sistemas informáticos y el ambiente tecnológico que utiliza, así como internas de la propia entidad, como políticas, procedimientos, cláusulas contractuales, acuerdos con empleados y terceros, etc.

Una adecuada gestión de la seguridad de la información permite proteger los recursos de información y la tecnología utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar la confidencialidad, integridad, disponibilidad de la información, así como el cumplimiento de las normas aplicables.

## 3. TIPOS DE ACTIVOS DE INFORMACIÓN

Los activos por proteger, mediante el cumplimiento de la Política de Seguridad de la Información, son:

- La información propiamente dicha, en sus múltiples formatos (papel, digital, imagen, audio, video).
- Equipos, Sistemas e Infraestructura que soportan los diferentes formatos de información.
- Las personas que utilizan la información, y que tienen el conocimiento de los procesos del organismo.

## 4. ALCANCE

Esta Política de Seguridad 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.

Debe ser comunicada fehacientemente y cumplida por todos los/as funcionarios/as y trabajadores/as 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, operativas 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 le sea aplicable y en las secciones que le corresponden.

Este documento alcanza todas las actividades relacionadas con la generación, procesamiento, almacenamiento, transmisión, traslado y consumo de la información necesaria para la Agencia Nacional de Materiales Controlados en cualquiera de sus tipos de activos.

Dichas actividades pueden desarrollarlas funcionarios/as, trabajadores/as bajo cualquier modalidad de contratación, contratistas, entidades asociadas y/o usuarios/as de terceras partes relacionados y demás involucrados internos y externos.

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

## 5. DEFINICIONES

A los efectos de una correcta interpretación de la presente Política, se deben tener en cuenta las siguientes definiciones:

- Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

- Sistema de información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

- Tecnología de la información: Se refiere al hardware y software operados por un 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.

- Confidencialidad: Garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a ésta, impidiendo su divulgación a personas o entidades no autorizadas.
- Integridad: Salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento, de acuerdo con las pautas fijadas por el organismo y por las regulaciones externas.
- Disponibilidad: Garantiza que las/los usuarias/os autorizadas/os tengan acceso a la información y a los recursos relacionados con ésta, toda vez que lo requieran.
- Eficacia: Garantizar el cumplimiento de los objetivos planificados. En particular, que la información y sus procesos relacionados sean relevantes y pertinentes para el desarrollo de la actividad; y que la información se presente en forma correcta, coherente, completa y oportuna.
- Eficiencia: Garantizar la optimización del uso de recursos en las actividades relacionadas con la información y su protección.
- Clasificación de la Información: Contribuir a la eficacia y eficiencia de la protección de la información determinando el valor para la ANMaC de los distintos activos de información, como un paso previo a la gestión de riesgos y a la aplicación de controles de seguridad.
- Propietario de la Información: Define a la persona responsable de la integridad, confidencialidad y disponibilidad de una cierta información.
- Evaluación de Riesgos: evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de su procesamiento, la probabilidad de que ocurran y su potencial impacto en la operatoria del Organismo.
- Tratamiento de riesgos: Proceso de selección e implementación de medidas para modificar el riesgo.
- Gestión de riesgos: Actividades coordinadas destinadas a gestionar riesgos. Usualmente incluye la evaluación, el tratamiento, la aceptación y la comunicación de estos, a fin de contribuir a la eficacia y eficiencia de la protección de la información.
- Amenaza: Una causa potencial de un incidente no deseado que puede ocasionar daños a un sistema u organismo.

- Vulnerabilidad: Una debilidad de un activo o grupo de activos que puede ser aprovechada por una amenaza.
- Control: Medio para gestionar el riesgo, incluyendo políticas y procedimientos.
- Autenticidad: Asegurar la validez de la información en tiempo, forma y distribución. Asimismo, garantizar el origen de la información, validando el emisor para evitar suplantación de identidades.
- Auditabilidad: Todos los eventos de un sistema deben poder ser registrados para su control posterior.
- Protección a la duplicación: Asegurar que una transacción solo se realice 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: Toma de medidas para evitar que un organismo que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
- Legalidad: Cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto al organismo.
- Confiabilidad de la información: La información generada debe ser adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

## 6. PRINCIPIOS BÁSICOS

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 Política de Seguridad de la Información.

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 Política reciben una concientización periódica y pertinente a su función, respecto del compromiso que asumen para cumplir con la presente. Para ello, se asignan los recursos necesarios, tanto humanos, cognitivos, como materiales, de capital y financieros para lograr la mejora progresiva.

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 Política, por parte de los/as agentes y funcionarios/as, 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.

## 7. REVISION Y ACTUALIZACION

El organismo se compromete a revisar esta Política de Seguridad de la Información 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.

El Comité de Seguridad de la Información será el responsable de llevar adelante las revisiones sean periódicas o ad-hoc, dejándose constancia de ellas en el presente documento. El/la Director/a de Sistemas y el/la Coordinador/a de Recursos Humanos serán responsables de la propuesta e implementación de las nuevas versiones, que serán comunicadas en tiempo y forma a todos los alcanzados para su cumplimiento.

La fecha programada de la próxima revisión es el 01 de junio de 2023.

## 8. GESTIÓN DE RIESGOS SOBRE LOS ACTIVOS DE INFORMACIÓN

Se deben identificar claramente todos los activos de información, elaborando y manteniendo un inventario de ellos. El Comité de Seguridad de la Información (punto 9.1) deberá decidir el tratamiento que se llevará a cabo frente a los riesgos y documentar adecuadamente dichas decisiones. Las posibles opciones para el tratamiento de los riesgos son:

a) Mitigar los riesgos mediante la aplicación de controles apropiados para reducir los efectos de aquellos.

b) Aceptar los riesgos de manera objetiva y consciente, siempre y cuando estos satisfagan claramente la política y los criterios de aceptación de riesgos del organismo.

c) Evitar los riesgos eliminando las acciones que los originan.

d) Transferir los riesgos asociados a otras partes interesadas, por ejemplo: compañías de seguro o proveedores.

La política de seguridad de la información propende a minimizar los riesgos de la gestión de la información preservando las siguientes características:

- Confidencialidad: se garantiza que la información sea accesible solo a aquellas personas autorizadas a tener acceso a ella.

- Integridad: se salvaguarda la exactitud y la totalidad de la información y los métodos de procesamiento.
- Disponibilidad: se garantiza que los/as usuarios/as autorizados/as tengan acceso a la información y a los recursos relacionados con ella, toda vez que lo requieran.

## 9. DE LAS RESPONSABILIDADES

El/La Directora/a Ejecutivo/a, el/la Subdirector/a Ejecutivo/a, todos/as los/las Directores/as Nacionales o Generales o equivalentes, Coordinadores/as, titulares de Unidades Organizativas, tanto se trate de autoridades políticas o personal técnico y sea cual fuere su nivel jerárquico, son responsables de la implementación de esta Política de Seguridad de la Información dentro de sus áreas de responsabilidad, así como del cumplimiento de la misma, por parte de su equipo de trabajo.

### 9.1 RESPONSABILIDADES BÁSICAS DEL COMITÉ DE SEGURIDAD DE INFORMACIÓN

- Revisar y proponer a la máxima autoridad del organismo para su aprobación las modificaciones/actualizaciones de la Política de Seguridad de la Información y las funciones generales en materia de seguridad de la información.
- Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
- Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.
- Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo con las competencias y responsabilidades asignadas a cada área, así como acordar y aprobar metodologías y procesos específicos relativos a seguridad de la información.
- Garantizar que la seguridad de la información sea parte del proceso de planificación de la información; evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.

- Promover la difusión y el apoyo a la seguridad de la información dentro del organismo y coordinar el proceso de administración de la continuidad de las actividades del organismo.
- Coordinar el proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de la información de la Agencia frente a interrupciones imprevistas.
- Definir procedimientos para el control de cambios a los procesos operativos documentados, los sistemas e instalaciones de procesamiento de información, y verificar su cumplimiento, de manera que no afecten la seguridad de la información.
- Establecer criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, contemplando la realización de las pruebas necesarias antes de su aprobación definitiva. Verificar que dichos procedimientos de aprobación de software incluyan aspectos de seguridad para todas las aplicaciones.
- Definir procedimientos para el manejo de incidentes de seguridad y para la administración de los medios de almacenamiento.
- Definir y documentar una norma clara con respecto al uso del correo electrónico, redes sociales, intranet y sistema de gestión documental electrónica.
- Definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso y para garantizar la seguridad de los datos y los servicios conectados en las redes del organismo.
- Desarrollar procedimientos adecuados de concientización de usuarios/as en materia de seguridad, controles de acceso al sistema y administración de cambios.
-Verificar el cumplimiento de las normas, procedimientos y controles establecidos.
- Administrar los medios técnicos necesarios para permitir la segregación de los ambientes de procesamiento.
- Monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad, a fin de evitar potenciales amenazas a la seguridad del sistema o a los servicios del usuario/a.

- Controlar la realización de las copias de resguardo de información, así como la prueba periódica de su restauración.
- Controlar la extracción de información para su resguardo confidencial.
- Desarrollar y verificar el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas.

**9.2. RESPONSABILIDAD DEL COORDINADOR DEL COMITÉ DE SEGURIDAD DE LA INFORMACION**

La Dirección Ejecutiva designará un Coordinador/a del Comité de Seguridad de la Información, quien tendrá la responsabilidad de:

- Coordinar las acciones del Comité de Seguridad de la Información.
- Impulsar la implementación y el cumplimiento de la Política de Seguridad de la Información.

**9.3 LOS RESPONSABLES DE LA DIRECCIÓN DE SISTEMAS Y DE LA COORDINACIÓN DE INFORMÁTICA.**

Cumplirán la función de cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología del organismo Asimismo, tendrá la función de efectuar las tareas de control, desarrollo, resguardo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases.

El/la responsable de la Dirección de Sistemas definirá junto con el responsable de la Dirección de Administración, según corresponda, las medidas de seguridad física y ambiental para el resguardo de los activos críticos, en función de un análisis de riesgos, y controlará su implementación. Asimismo, verificará el cumplimiento de las disposiciones sobre seguridad física y ambiental indicadas en el presente y controlará el mantenimiento del equipamiento informático de acuerdo con las indicaciones de proveedores, tanto dentro como fuera del organismo.

**9.4 EL/LA RESPONSABLE DE LA DIRECCIÓN DE ASUNTOS JURÍDICOS**

Verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación del organismo con SNS

empleados/as y con terceras personas. Asimismo, asesorará en materia legal al organismo, en lo que se refiere a la seguridad de la información.

Deberá promover el deslinde de la responsabilidad que correspondiere (civil, penal y/o disciplinaria) y, en su caso, desarrollar proyectos de sanciones ante el incumplimiento de la presente y, elevarlos a consideración de la Dirección Ejecutiva.

**9.5 EL/LA RESPONSABLE DE LA DIRECCIÓN DE ADMINISTRACIÓN**

Definirá junto con el/la responsable de la Dirección de Sistemas, las medidas de seguridad física y ambiental para el resguardo de los activos críticos, en función de un análisis de riesgos, y controlará su implementación.

Es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la tecnología de información, debiendo informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por la Política de Seguridad de la Información y por las normas, procedimientos y prácticas que de ella surja.

**9.6 EL/LA RESPONSABLE DE LA COORDINACIÓN DE RECURSOS HUMANOS**

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

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

- Tiene a su cargo la notificación de la Política de Seguridad de la Información a todo el personal, de los cambios que en ella se produzcan, la implementación de la suscripción de los Compromisos de Confidencialidad (entre otros) y las tareas de capacitación continua en materia de seguridad.

**9.6.2.- RESPONSABILIDAD DE LA COORDINACIÓN DE RECURSOS HUMANOS DURANTE EL EMPLEO**

El área de Recursos Humanos solicitará a los trabajadores/as, contratistas y usuarios/as de terceras partes que apliquen la seguridad en concordancia con las políticas y procedimientos establecidos cumpliendo con lo siguiente:

- Estar adecuadamente informados de sus roles y responsabilidades de seguridad de la información antes de que se les otorgue el acceso a información sensible o a los sistemas de información.
- Estar provistos de guías para establecer las expectativas de seguridad de su rol dentro del organismo.
- Tener la suficiente motivación para cumplir con las políticas de seguridad del organismo.
- Cumplir con las condiciones y términos del empleo, los cuales incluyen las políticas de seguridad de la información del organismo y métodos adecuados de trabajo.

**9.6.3- RESPONSABILIDAD DE LA COORDINACIÓN DE RECURSOS HUMANOS ANTE LA DESVINCULACIÓN O CAMBIO DE PUESTO DE UN AGENTE**

Al momento del cese de las actividades de un trabajador/a o del cambio de puesto en el organismo, deberá comunicar fehacientemente este hecho al Comité de Seguridad de la Información y al responsable de la Dirección de Sistemas, quien deberá bloquear todos los accesos de esa persona a la red y desafectar todos sus privilegios en caso de desvinculación. Si el agente sufriera un cambio de puesto dentro del organismo, se le deberán actualizar sus roles y permisos en función de la nueva asignación.

**9.7 RESPONSABILIDAD DE LA COORDINACION DE ACCESO A LA INFORMACION Y CONTROL DE LA GESTION.**

Revisar y proponer los cambios que estime necesarios para alcanzar la mejora progresiva del acceso y resguardo de la información que utilizan los/as agentes del Organismo, contratados bajo cualquier modalidad.

**9.8 RESPONSABILIDADES DEL USUARIO**

Todo usuario/a tiene prohibido facilitar el acceso a personas no autorizadas, poner en peligro la información y el robo de información y los medios de procesamiento de la información. La cooperación de los usuarios/as autorizados/as es esencial para una seguridad efectiva. Los/as usuarios/as deben estar al tanto de sus responsabilidades para mantener controles de acceso efectivos, particularmente con relación al uso de claves secretas y la seguridad del equipo del usuario/a. Asimismo, se deberán 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/a y, consecuentemente, un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.

## 10. LINEAMIENTOS ESPECIFICOS

### Organización de la Seguridad de la Información

El organismo asigna al Comité de Seguridad de la Información las responsabilidades relativas a la seguridad de la información, que tendrá a su cargo la coordinación de todas las actividades tendientes a la implementación de la presente Política.

Dicho Comité velará por una adecuada segregación de funciones, por un abordaje de la seguridad de la información en todos los proyectos y programas del organismo y por el establecimiento de adecuados procedimientos de seguridad, en base a un plan de tratamiento de riesgos.

Las autoridades del organismo se comprometen a impulsar las iniciativas que el área competente proponga con el objetivo de preservar la confidencialidad, integridad y disponibilidad de la información que gestiona. Asimismo, requerirá a las áreas competentes la inclusión en contratos, Términos de Referencia o instrumentos similares, cláusulas que contemplen el cumplimiento de la presente Política.

### Seguridad Informática de los Recursos Humanos

El personal es considerado un recurso central para la protección de la información, motivo por lo cual es adecuadamente entrenado en caso del personal técnico y concientizado a través de programas específicos, para quienes no realizan actividades de ese tenor. A tal fin, se establecen las medidas necesarias en los procesos de selección de personal, durante la vinculación laboral y al momento de la desvinculación, pudiendo inclusive

excederlo. En todo momento se protegen los derechos individuales de los empleados, especialmente aquellos relacionados con la privacidad.
Se establece la obligatoriedad de la suscripción de compromisos de confidencialidad en función de las responsabilidades que correspondan y a las funciones que se desarrollen. Los permisos de acceso son otorgados en función de cada perfil de trabajo y se mantienen actualizados.

**Gestión de Activos**

La gestión y protección efectiva de los activos en función de su clasificación por criticidad es una prioridad para el organismo. Entre los activos se incluyen tanto el hardware como el software y los dispositivos de comunicación, los elementos de apoyo, la información y los datos en sí mismos, cualquiera sea el soporte y formato en el que se encuentren. Para la clasificación se tienen en cuenta la confidencialidad, integridad y disponibilidad de los datos, así como las funciones que soporta el activo y la normativa aplicable.
Se llevan inventarios actualizados y se exige a todos los/as agentes y funcionarios/as que se desvinculan la devolución de los activos de información en su poder. En el mismo sentido, se procede a una destrucción segura de cualquier medio que pueda contener información crítica o datos personales, para lo cual, se cuenta con procedimientos adecuados.

**Autenticación, autorización y control de Acceso**

El organismo adopta los mecanismos necesarios para que solo el personal autorizado acceda a los activos de información, bajo la premisa básica de que *"Todo está prohibido a menos que se permita expresamente"* para a aquellos activos considerados críticos. El acceso a la información se establecerá en base a la *"necesidad de saber"*, es decir que quienes accedan deben tener un motivo válido para hacerlo en razón de su rol y/o funciones y usando una política de "Mínimo Privilegio". Estos privilegios se otorgan en forma expresa, son autorizados por los niveles competentes y se gestionan adecuadamente las altas y bajas de las cuentas y permisos de acceso, con revisiones

periódicas. Se requiere a los/as trabajadores/as, funcionarios/as y demás usuarios/as, el uso responsable de los dispositivos y datos de autenticación otorgados por el organismo para el cumplimiento de sus funciones, que no los compartan y que los mantengan siempre seguros, tanto dentro como fuera del organismo.

**Seguridad física y ambiental**

El organismo protege sus 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 y áreas protegidas, en la medida en que se considere necesario.
Además, se monitorean los accesos físicos para permitir solo ingresos y egresos debidamente autorizados y se mantiene un registro actualizado de los activos físicos que procesan información. Se implementan y hacen cumplir medidas de seguridad para los activos físicos que deben llevarse fuera del organismo, manteniéndose el registro correspondiente.

**Seguridad operativa**

Las operaciones del organismo se desarrollan en forma segura, en todas las instalaciones de procesamiento de información, asignándose las debidas responsabilidades y desarrollando procedimientos acordes. Se adoptan medidas para minimizar los riesgos de acceso y cambios no autorizados o pérdida de información y para proteger las instalaciones y plataformas tecnológicas contra infecciones de código malicioso.
Las vulnerabilidades son gestionadas de manera apropiada y se controla la actividad de administradores y operadores.

**Seguridad de las comunicaciones**

El organismo adopta las medidas necesarias para proteger adecuadamente la información que se comunica por sus redes informáticas y para minimizar los

riesgos que pudieran afectar la infraestructura de soporte. Toda información que se transfiere fuera del organismo, incluyendo la que se transmite a través de los servicios de correo electrónico es protegida de acuerdo a su nivel de criticidad.

Se asignan cuentas institucionales a todos los/as trabajadores/as y funcionarios/as, quienes están obligados a utilizarlas para toda comunicación vinculada a sus funciones. Dicho personal es informado por sus respectivas autoridades sobre los riesgos de incumplir este requerimiento, y se les exige la firma de acuerdos de confidencialidad y no divulgación, en los casos en los que el organismo lo considere necesario.

**Adquisición de sistemas, desarrollo y mantenimiento de sistemas de información**

El organismo adopta las medidas de seguridad necesarias para proteger por defecto y desde el diseño todas las aplicaciones que se desarrollen internamente, utilizando una metodología de desarrollo seguro, e incorpora requerimientos y evaluaciones de seguridad en el proceso de contratación de aplicaciones a terceros. Esto se aplica especialmente a aquellas que se utilicen para brindar servicios o realizar trámites por parte de la ciudadanía e involucren el tratamiento de datos personales.

Se evalúa la seguridad de las aplicaciones antes de ponerlas productivas.

**Relación con proveedores**

El organismo incluye en los pliegos de bases y condiciones particulares cláusulas vinculadas a la seguridad de la información, de cumplimiento efectivo y obligatorio por parte de los cocontratantes. 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.

**Gestión de incidentes de seguridad**

El organismo adopta las medidas necesarias para prevenir, detectar, gestionar, resolver y reportar los incidentes de seguridad que puedan afectar sus 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.
Cuando los/as empleados/as detecten un evento que podría constituir un incidente de seguridad, lo deben comunicar a la Dirección de Sistemas –o el área que en un futuro la reemplace-. De producirse el incidente, y que éste hubiera afectado información o datos personales de terceras personas, el organismo informará públicamente tal ocurrencia, de acuerdo a lo dispuesto por la normativa vigente.

**Aspectos de seguridad para la continuidad de la gestión**

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.

**Cumplimiento**

El organismo cumple las disposiciones legales, normativas y contractuales que le son aplicables y promueve el acatamiento de las políticas y normas de seguridad que se aprueban en su ámbito. En el mismo sentido, atiende y da cumplimiento a las recomendaciones correspondientes a los hallazgos de las auditorías internas y externas que se realicen, adoptando las medidas correctivas que correspondan

República Argentina - Poder Ejecutivo Nacional
Las Malvinas son argentinas

**Hoja Adicional de Firmas**
**Informe gráfico**

**Número:** IF-2022-44112404-APN-DNAAJYM#ANMAC

CIUDAD DE BUENOS AIRES
Miércoles 4 de Mayo de 2022

**Referencia:** POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN ANMAC 2022

---

El documento fue importado por el sistema GEDO con un total de 17 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2022.05.04 17:06:39 -03:00

Miguel Alfredo La Scalea
Coordinador
Dirección Nacional de Administración, Asuntos Jurídicos y Modernización
Agencia Nacional de Materiales Controlados

Digitally signed by Gestion Documental Electronica
Date: 2022.05.04 17:06:40 -03:00