POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

(PSI)

Introducción

La SUPERINTENDENCIA DE SEGUROS DE LA NACIÓN (SSN) reconoce que 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 sus actividades y debe, en consecuencia, ser protegida adecuadamente. La protección se extiende a todo el ciclo de vida de la información, a todos los formatos en los que se encuentre y soporte que se utilice, con el fin de preservar la confidencialidad, integridad y disponibilidad de la información.

Dicho estado de protección se logra estableciendo, implementado, monitoreando, revisando y mejorando un conjunto de mecanismos de seguridad o controles que incluyen, entre otros, procesos, políticas, procedimientos, estructuras organizacionales, software y hardware. El objeto de estos mecanismos y controles es el de minimizar los riesgos a los que se encuentra expuesta la información, así como asegurar la continuidad de las operaciones del organismo.

En función de lo expuesto, la preservación de los activos de información resulta esencial, tanto para garantizar el normal desarrollo de las actividades de la SSN, como para cumplir con el marco legal y preservar la imagen institucional del organismo y del Estado Nacional en su conjunto.

Consideraciones generales

Objetivos

La presente Política de Seguridad de la Información (PSI) establece las directrices y líneas de actuación en materia de seguridad de la información que fijan 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. Asimismo, detalla lineamientos respecto a la comunicación de esta Política y sobre su implementación.

Los objetivos de la PSI son:

- Orientar y enmarcar las acciones de fortalecimiento del Sistema de Gestión de Seguridad de la Información que lleve adelante la SSN.
- Fomentar el desarrollo de una cultura de seguridad de la información en la organización.

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 ser políticas, procedimientos, cláusulas contractuales y acuerdos con empleados y terceros.

Alcance

Esta PSI se aplica en todo el ámbito del organismo, a sus recursos y a la totalidad de los procesos.

Su cumplimiento es obligatorio para la totalidad de los/las funcionarios/as y agentes que integran el organismo, cualquiera sea su modalidad de contratación y las fuentes de financiamiento correspondientes.

Asimismo, la PSI debe ser conocida y cumplida por todas aquellas personas, ya sean internas o externas, 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.

Marco normativo

La presente Política de Seguridad de la Información se encuentra alineada con la Legislación de la República Argentina que regula aspectos que hacen a la seguridad de la información.

Leyes y decretos relacionados con la seguridad de la información y con la protección de datos personales:

- Ley 26.388 de Delitos informáticos
- Ley 25.326 de Protección de Datos Personales y Decreto Reglamentario N° 1558/2001
- Ley 25.506 de Firma Digital y Decreto Reglamentario N° 2628/2002
- Ley 26.904 de Grooming.
- Ley 11.723 Propiedad Intelectual y Ley 25.036 Modificatoria de Ley 11.723

- Decreto 577/2017. Creación del Comité de Ciberseguridad.

Selección de resoluciones y disposiciones relevantes:

- Decisión Administrativa 641/2021. Establece los requisitos mínimos de seguridad de la información para organismos públicos
- Disposición DNCIB 1/2022. Aprueba el “Modelo Referencial de Política de Seguridad de la Información”.
- Disposición DNCIB 8/2021. Guía Introductoria a La Seguridad para el Desarrollo de Aplicaciones Web.
- Disposición DNCIB 7/2021 Dirección Nacional de Ciberseguridad “Registro de Puntos Focales en Ciberseguridad del Sector Público Nacional”
- Disposición DNCIB 6/2021. Creación del Comité Asesor para el Desarrollo e Implementación de aplicaciones seguras.
- Disposición DNCIB 1/2021. Centro Nacional de Respuestas a Incidentes Informáticos (CERT.ar) en el ámbito de la Dirección Nacional de Ciberseguridad.
- Resolución JGM 580/2011. Creación del Programa Nacional de Protección de Infraestructuras Críticas de Información y Ciberseguridad.
- Resolución JGM 1523/2019. Definición de Infraestructuras Críticas.
- Resolución JGM 829/2019. Aprobación de la Estrategia Nacional de Ciberseguridad.

Estándares internacionales referidos a las buenas prácticas de seguridad de la información:

- Norma ISO/IEC 27002:2013 Código de Buenas Prácticas de Controles para la Seguridad de la Información.

Principios básicos

Los principios adoptados por el organismo para orientar las acciones de preservación de la seguridad de la información son:

Confidencialidad	de modo que únicamente quienes estén autorizadas accedan a la información.
Integridad	de modo que la exactitud de los datos transportados o almacenados sea protegida de la modificación, pérdida o destrucción, garantizándose la no alteración de los mismos.
Disponibilidad	de modo que los datos e información estén accesibles por los usuarios o procesos autorizados cuando así lo requieran.
Autenticidad	de modo que se asegure la identidad del emisor de la información que se envíe, a través de una validación que evite la suplantación de identidades.

Asimismo, la protección de los derechos de los titulares de los datos personales procesados es un objetivo central de esta PSI.

La SSN declara su compromiso y 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. En este sentido, sus autoridades se comprometen a liderar la mejora continua de los procesos de gestión de seguridad de la información, asegurando su eficacia y eficiencia.

Incumplimiento

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 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 agentes y funcionarias y funcionarios, de acuerdo al 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.

Vigencia

La PSI entrará en vigencia a partir de su fecha de aprobación y mantendrá la misma de manera indefinida hasta tanto se apruebe una en su reemplazo.

Revisión y actualización

El organismo se compromete a revisar esta PSI con una periodicidad mínima anual, adaptándola a nuevas exigencias organizativas o del entorno, así como a comunicarla a su personal y a los terceros involucrados.

Asimismo, la SSN se compromete a realizar las revisiones adicionales que sean necesarias ante cambios significativos a nivel normativo, tecnológico y/o de otra índole que requieran una adaptación de la presente Política.

Es responsabilidad del Comité de Seguridad de la Información llevar adelante las revisiones, sean periódicas o ad-hoc, de la PSI, así como poner a disposición de la máxima autoridad del organismo los documentos elaborados para su consideración y aprobación.

Lineamientos específicos

Organización de la seguridad de la información

La SSN asignó al Comité de Seguridad de la Información (CSI)[1] las funciones de planificación en materia de seguridad de la información y de supervisión de la investigación y monitoreo de los incidentes relativos a la seguridad de la información. La planificación comprende la propuesta de programas, proyectos y metodologías, su monitoreo y evaluación, así como la promoción de la difusión y apoyo a la seguridad de la información dentro del organismo. Es función propia del CSI la elaboración de la PSI, así como su revisión y propuesta de modificatorias.

El CSI es la principal instancia responsable de la planificación de la seguridad de los sistemas de información del organismo, en los términos del art. 5° de la DA 641/21, sin perjuicio de las responsabilidades propias que asigna la estructura orgánico-funcional vigente. Su presidencia está a cargo del/de la titular de la Gerencia de Coordinación General. El CSI podrá ser asistido en sus actividades por las Comisiones de Seguridad de la Información que a estos efectos cree.

La Subgerencia de Tecnologías de la Información y de las Comunicaciones, dependiente de la Gerencia de Coordinación General, tiene a su cargo la organización de las actividades tendientes a la implementación de la presente PSI y su titular es, a su vez, el punto focal designado ante la Dirección Nacional de Ciberseguridad (DNCIB), conforme lo requiere la Disposición DNCIB 7/21.

Seguridad informática de los recursos humanos

La SSN procurará que su personal se encuentre debidamente concientizado a través de programas específicos. En lo que hace al personal técnico, el organismo procurará el acceso a capacitación adecuada a sus funciones. Las acciones que se adopten en materia de seguridad de la información no podrán afectar los derechos individuales de los empleados, especialmente aquellos relacionados con la privacidad.

Cuando el organismo lo considere necesario, de acuerdo al marco legal aplicable, se requerirá a los agentes, funcionarios y a los terceros que interactúen con el organismo, de acuerdo a su competencias, la firma de un acuerdo de confidencialidad. Así también, se procurará incluir en la etapa de inducción de los agentes los aspectos de seguridad.

Gestión de activos

El organismo adoptará las medidas necesarias para contar con los activos de información inventariados, de forma tal que permita su clasificación en función de la criticidad. Se registrará al responsable de cada activo, así como su ubicación, permitiendo de esta manera una adecuada gestión y protección de los activos de información. El concepto de activos abarca tanto al hardware

[1] Resolución SSN 677/22.

como el software y a 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.

El organismo exige a todos los/las agentes y funcionarios/as que se desvinculan la devolución de los activos de información en su poder. En el mismo sentido, se compromete a establecer e implementar los procedimientos adecuados para la destrucción segura de cualquier medio que pueda contener información crítica o datos personales.

Autenticación, autorización y control de acceso

El organismo implementa los procedimientos necesarios para autenticar a los usuarios de los dispositivos y sistemas en uso. Asimismo, adopta el principio de mínimo privilegio en materia de acceso a los activos de información. Es responsabilidad de todo el personal con privilegios que le permitan otorgar o modificar el acceso a otras personas a los activos de información velar por el cumplimiento de este principio, verificando que estas últimas tengan un motivo válido para solicitar el acceso en razón de su rol y/o funciones.

Los 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, fijándose revisiones periódicas.

Los empleados, funcionarios y terceros destinatarios de esta Política son responsables del uso adecuado de los dispositivos y datos de autenticación otorgados por el organismo para el cumplimiento de sus funciones. El organismo adoptará las acciones necesarias, entre las cuáles se encuentra la difusión de la PSI, para procurar que el personal incorpore las medidas de cuidado necesarias, tanto dentro como fuera del organismo.

Uso de herramientas criptográficas

El organismo requerirá el cifrado de todas las unidades propias que alojen información considerada crítica. A su vez, para su transmisión fuera del organismo se cumplirá con las medidas y canales (como ser, el Sistema de Gestión Documental Electrónica –GDE-) que establece la normativa vigente como de cumplimiento obligatorio para los organismos de la Administración Pública Nacional. Las claves criptográficas se protegerán durante todo su ciclo de vida.

Se utilizan certificados digitales válidos en el sitio web institucional y en las aplicaciones web que se desarrollen.

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, áreas protegidas y controles ambientales, 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.

Seguridad operativa

El organismo adopta 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. Para ello, se compromete a desarrollar e implementar procedimientos acordes que permitan el desarrollo seguro de las operaciones del organismo, así como el control de la actividad de administradores y operadores.

Seguridad de las comunicaciones

El organismo asigna cuentas institucionales a todo el personal, quienes están obligados a utilizarlas para toda comunicación vinculada a sus funciones. El personal es informado por sus respectivas autoridades sobre los riesgos de incumplir este requerimiento.

La SSN adopta medidas 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.

Adquisición de sistemas, desarrollo y mantenimiento de sistemas de información

El organismo se compromete a adoptar medidas de seguridad para proteger por defecto y desde el diseño todas las aplicaciones que se desarrollen con medios propios o a través de terceros. Asimismo, se compromete a establecer, adoptar, incorporar y requerir el empleo de buenas prácticas en materia de desarrollo seguro. A estos fines, se promoverá la capacitación permanente de quienes desarrollen funciones de desarrollo de software e infraestructura.

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 los contratantes. 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 se compromete a adoptar las medidas necesarias para prevenir, detectar, gestionar, resolver y reportar los incidentes de seguridad que puedan afectar a sus activos de información. Entre otras medidas, la de poner a disposición un canal de comunicación centralizado para el registro de los eventos que puedan constituir un incidente de seguridad, al que deberán informar los empleados del organismo. De producirse el incidente, y que éste hubiera afectado información o datos personales de terceros, 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 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.

Estructura normativa de seguridad de la información

Agrupamiento de las normas específicas de seguridad de la información

La SSN se compromete a establecer la normativa específica de seguridad de la información necesaria para el cumplimiento de la presente Política, la que se agrupa en las siguientes categorías:

- **Normas referidas a los activos de información y exigencias técnicas**. Se establecerán los criterios aplicables a los activos de información y las exigencias técnicas de seguridad adecuadas para el organismo en materia de gestión de activos, seguridad física y ambiental; criptografía; gestión de comunicaciones y operaciones; control de acceso; sobre adquisición, desarrollo y mantenimiento de sistemas de información; sobre gestión de incidentes; y sobre administración de proveedores.
- **Normas referidas a la gestión de personas.** Con el objeto de favorecer un uso adecuado de la información y de los sistemas que la apoyan, se desarrollarán normas de seguridad de la información vinculadas a la gestión de las personas, las que deberán encontrarse alineadas, entre otras, con la normativa aplicable en la materia.
- **Normas referidas al cumplimiento**. Se desarrollará la normativa de seguridad de la información asociada al cumplimiento de disposiciones legales, regulatorias o contractuales. A partir de dichas normas, se deberán implementar medidas preventivas y correctivas que consideren el riesgo por incumplimiento.

Aprobación y difusión de las normas

La normativa específica de seguridad de la información de la SSN, así como cualquier modificación de la misma, será aprobada por la máxima autoridad del organismo o autoridad competente.

La normativa específica, así como esta Política, será comunicada al personal del organismo, de manera pertinente, accesible y comprensible. El texto íntegro y actualizado de la presente Política se pondrá y mantendrá a disposición de los interesados en la Intranet del organismo y en el sistema KRONOS.

Anexo. Glosario

Activos de información

Toda información o sistema relacionado con su tratamiento que tenga valor para la organización. Pueden consistir en documentos, datos, aplicaciones, equipos informáticos, personal o cualquier otro componente. Los activos de información son susceptibles de ataques deliberados o accidentales.

Amenaza

Causa potencial de un incidente no deseado, que puede dar lugar a daños a un sistema o proceso.

Ataque

Intento de destruir, exponer, alterar, inhabilitar, acceder sin autorización, hacer uso no autorizado y/o cualquier otra acción prohibida sobre un activo de información.

Ataque informático

Ciberataque.

Autenticación

Procedimiento que se realiza para comprobar que alguien es quién dice ser cuando accede a un dispositivo o sistema.

Ciberataque

Intento deliberado de obtener acceso a un sistema informático sin autorización sirviéndose de diferentes técnicas y vulnerabilidades para la realización de actividades con fines maliciosos, como el robo de información, extorsión del propietario o simplemente daños al sistema.

Confidencialidad

Propiedad que refiere a que los datos e información se mantengan inaccesibles y se revelen únicamente a personas, entes o procesos autorizados.

Control

Los medios para gestionar el riesgo, incluidos políticas, procedimientos, directrices, prácticas o estructuras organizativas, que pueden ser de naturaleza administrativa, técnica, de gestión o jurídica.

Control de acceso

Medios que se emplean para asegurar que el acceso a los activos de información se encuentre restringido a las personas autorizadas.

Disponibilidad

Propiedad que refiere a que los datos e información sean accesibles y se encuentren listos para su uso a demanda de una persona o ente autorizado.

Evento de seguridad de la información

Actividad o serie de actividades sospechosas que ameritan ser analizadas desde la perspectiva de la seguridad de la información.

Incidente de seguridad de la información

Evento o serie de eventos de seguridad de la información, no deseados o inesperados, que comprometen la seguridad de la información y amenazan la operación del negocio.

Información

Es un conjunto de datos organizados que portan, transmiten o arrojan un significado.

Integridad

Propiedad que refiere a la exactitud y completitud de la información.

Mínimo privilegio

Principio por el cual a cada usuario de un sistema se le otorga el conjunto de privilegios más restrictivos (o la autorización más baja) necesarios para el desempeño de sus tareas autorizadas.

Recurso

Cualquier activo que posibilite generar, almacenar, publicar o transmitir información.

Riesgo

Efecto de la incertidumbre sobre el logro de los objetivos de seguridad de la información.

Sistema de información

Aplicaciones, servicios, activos de tecnología de la información y todo otro componente empleado para tratar información.

Vulnerabilidad

Debilidad de un activo, grupo de activos o de un control que puede ser materializada por una o más amenazas.

República Argentina - Poder Ejecutivo Nacional
Las Malvinas son argentinas

Hoja Adicional de Firmas
Informe gráfico

Número: IF-2022-138513863-APN-GCG#SSN

CIUDAD DE BUENOS AIRES
Lunes 26 de Diciembre de 2022

Referencia: Anexo Política de Seguridad de la Información

El documento fue importado por el sistema GEDO con un total de 14 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2022.12.26 14:34:43 -03:00

Maria Alejandra Campolonghi
Subgerenta
Gerencia de Coordinación General
Superintendencia de Seguros de la Nación

Digitally signed by Gestion Documental Electronica
Date: 2022.12.26 14:34:44 -03:00