República Argentina - Poder Ejecutivo Nacional
Las Malvinas son argentinas

Anexo

Número: IF-2022-09912113-APN-DNCIB#JGM

CIUDAD DE BUENOS AIRES
Martes 1 de Febrero de 2022

Referencia: ANEXO MODELO REFERENCIAL DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

ANEXO

MODELO REFERENCIAL DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

I. INTRODUCCIÓN

Una Política de Seguridad de la Información (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/alta gerencia 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.

La DA antes citada determina en su anexo y como primera directriz lo siguiente:

"1. Política de Seguridad de la Información del organismo

Los organismos deben desarrollar una Política de Seguridad de la Información compatible con la responsabilidad primaria y las acciones de su competencia, sobre la base de una evaluación de los riesgos que pudieran afectarlos. Los términos de dicha política deben ser consistentes con las directrices del presente documento.

Dicha política debe ser:

- *aprobada por las máximas autoridades del organismo o por el funcionario a quien se le ha delegado la función.*
- *notificada y difundida a todo el personal y a aquellos terceros involucrados cuando resulte pertinente y en*

los aspectos que corresponda.

- *cumplida por todos los agentes y funcionarios del organismo.*
- *revisada y eventualmente actualizada, con una periodicidad no superior a DOCE (12) meses.*
- *utilizada como base para establecer un conjunto de normas, procedimientos, lineamientos y guías acordes a los procesos que se llevan adelante en el organismo, su plataforma tecnológica y demás recursos de los que disponga.*
- *informada a la Dirección Nacional de Ciberseguridad una vez aprobada."*

La PSI del organismo deberá cumplir con lo dispuesto precedentemente en todos los casos.

Con el fin de orientar a los organismos para la elaboración de sus PSI, la Dirección Nacional de Ciberseguridad de la Subsecretaría de Tecnologías de la Información y las Comunicaciones de la Secretaría de Innovación Pública elaboró un modelo referencial, que se incluye como Sección II de este documento. Este modelo podrá ser adaptado por cada organismo en función de sus competencias, los riesgos a los que se expone, los recursos disponibles, el marco normativo interno y externo que sea aplicable y demás características particulares de la entidad, para cumplimentar este requerimiento.

En consiguiente, las disposiciones que se describen a continuación podrán utilizarse como base para la elaboración de las respectivas políticas a dictarse por cada organismo alcanzado por la DA N° 641/2021, debiendo ser interpretadas como un compendio de buenas prácticas en materia de seguridad de la información recomendadas.

La Dirección Nacional de Ciberseguridad no recomienda la utilización textual de este documento como PSI del organismo, sin una revisión y ajuste previo. Como sección III se presentan una serie de lecturas adicionales o complementarias sugeridas, que podrán consultarse junto a otras fuentes que el organismo quiera utilizar para la redacción de su propia Política.

II. MODELO REFERENCIAL DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Introducción

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 y del Estado Nacional en su conjunto.

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. En este aspecto, el Estado puede proveer los servicios en forma directa o ejercer un rol regulatorio que lo obliga a velar por la seguridad de los datos y servicios tratados.

Objeto

La presente Política de Seguridad de la Información (en adelante, 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.

El objetivo principal de esta PSI 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.

Alcance

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.

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

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 PSI.

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.

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.

/Denominación del área/ será la responsable de llevar adelante las revisiones sean periódicas o ad-hoc, dejándose constancia de ellas en el presente documento. /Denominación del cargo o rol/ será responsable de la aprobación 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 /día, mes y año/.

Lineamientos específicos

Organización de la Seguridad de la Información:

El organismo asigna a la /denominación del área/ 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 PSI. Dicha unidad organizativa 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. Asímismo, requerirá a las áreas competentes la inclusión en contratos, Términos de Referencia o instrumentos similares, cláusulas que contemplen el cumplimiento de la presente PSI.

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 agentes y funcionarios 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 empleados, funcionarios y demás usuarios, 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.

Uso de herramientas criptográficas

Se utilizan sistemas y técnicas criptográficas 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.

Para ello, se requiere el cifrado de toda la información crítica, especialmente cuando ésta sea transmita fuera del organismo o se encuentre contenida en medios de almacenamiento que se trasladen fuera de la institución. Asimismo, se protegen las claves criptográficas durante todo su ciclo de vida y se utilizan certificados digitales válidos en los sitios web institucionales.

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. 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 empleados y funcionarios, 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 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 empleados detecten un evento que podría constituir un incidente de seguridad, lo deben comunicar a /área o autoridad competente/. 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 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.

III. BIBLIOGRAFÍA DE CONSULTA O COMPLEMENTARIA

A continuación, se citan algunos sitios web con información relacionada o complementaria:

- Instituto Argentina de Normalización y Certificación - IRAM - https://www.iram.org.ar/
- ISO - https://www.iso.org/home.html– INCIBE – Política
- Instituto de Ciberseguridad de España de Seguridad para PyMEs - https://www.incibe.es/protege-tu-empresa/herramientas/politicas
- Ministerio de TIC de Colombia - Elaboración de la política general de seguridad y privacidad de la información - https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf
- ISO27000.es - https://www.iso27000.es/
- NIST – Cybersecurity Framework – Policy Template Guide - https://www.cisecurity.org/wp-content/uploads/2020/07/NIST-CSF-Policy-Template-Guide-2 020-0720-1.pdf
- SANS Institute – Security Policies: where to begin – Laura Wills - https://sansorg.egnyte.com/dl/sOmMKofHbS
- SANS Institute – Security Policies Templates - https://www.sans.org/information-security-policy/

Digitally signed by Gestion Documental Electronica
Date: 2022.02.01 17:43:49 -03:00

Gustavo Raúl SAIN
Director Nacional
Dirección Nacional de Ciberseguridad
Jefatura de Gabinete de Ministros

Digitally signed by Gestion Documental Electronica
Date: 2022.02.01 17:43:50 -03:00