INSTITUTO NACIONAL DE ASOCIATIVISMO
Y ECONOMÍA SOCIAL

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

ÍNDICE

Introducción

El Instituto Nacional de Asociativismo y Economía Social (INAES), se compromete a establecer medidas de control y seguridad orientadas a proteger la gestión de la seguridad de la información, con el objeto de propiciar la continuidad de los sistemas, minimizar los riesgos de las amenazas y contribuir al eficiente cumplimiento de los objetivos de la organización; todo ello enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión del Organismo. Para cumplir con ello, se desarrolla el presente marco normativo “Política de Seguridad de la Información”.

La Política de Seguridad de la Información (PSI), nos brinda un marco para proteger la información y garantizar la continuidad de las operaciones de los sistemas de información, el compromiso manifiesto de las máximas autoridades de este organismo para promover la difusión, consolidación y cumplimiento de la política de seguridad adoptada, con el fin que estos principios lleguen a formar parte de la cultura organizacional.

La presente Política de Seguridad de la Información (PSI) será 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.

Se declaran inicialmente las políticas generales de seguridad de la información. Posteriormente como anexos, las políticas particulares y directrices, para consolidar la gestión de la seguridad de la información dentro del organismo. De esta manera se da cumplimiento a la Decisión Administrativa N° 641/2021, la cual establece en la sección V. DIRECTRICES, punto 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...”.

El presente documento se redactó según la política de seguridad de la información modelo indicada en la Disposición N° 1/2022 de la Dirección Nacional de Ciberseguridad y alineada con los requisitos mínimos de seguridad de la información para organismos según la Decisión Administrativa N° 641/2021 JGM. Como también se encuentra alineada al código de buenas prácticas de controles para la seguridad de la información de la Norma ISO/IEC 27002:2013.

Objetivos

Establecer un marco de referencia para la protección de la información y continuidad de los procesos y/o servicios, a través del resguardo de la confidencialidad, conservación de la integridad y mantenimiento de la disponibilidad de la información y de todos los recursos tecnológicos del Organismo, utilizados en la transmisión, procesamiento y almacenamiento, frente a posibles amenazas internas o externas, deliberadas o accidentales.

Alcance

La presente Política de Seguridad de la Información se dicta en cumplimiento de las disposiciones legales vigentes y deberá ser conocida y cumplida por todo el Organismo -funcionarios y personal-, sea cual fuere su nivel escalafonario, su situación de revista o modalidad contractual.

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

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.

Marco Normativo

El marco normativo de la presente Política de Seguridad de la Información se encuentra alineado respecto a la Legislación de la República Argentina.
Leyes relacionadas a la Ciberseguridad:

- Ley 26.388 de Delitos informáticos
- Ley 25.326 de Protección de Datos Personales
- Decreto Reglamentario N° 1558/2001

- Ley 25.506 de Firma Digital
- Decreto Reglamentario N° 2628/2002
- Ley 26.904 de Grooming
- Ley 11.723 Propiedad Intelectual y Ley 25.036 Modificatoria de Ley 11.723

Normativa vinculada a las funciones de la Dirección Nacional de Infraestructuras Críticas de la Información y Ciberseguridad:

- Decisión Administrativa 641/2021. Establece los requisitos mínimos de seguridad de la información para organismos públicos.
- Disposición 1/2022 Dirección Nacional de Ciberseguridad JGM. Aprueba el "Modelo Referencial de Política de Seguridad de la Información".
- Disposición 6/2021. Creación del Comité Asesor para el Desarrollo e Implementación de aplicaciones seguras.
- Disposición 1/2021. Centro Nacional de Respuestas a Incidentes Informáticos (CERT.ar) en el ámbito de la Dirección Nacional de Ciberseguridad.
- Resolución 580/2011. Creación del Programa Nacional de Protección de Infraestructuras Críticas de Información y Ciberseguridad.
- Resolución 1523/2019. Definición de Infraestructuras Críticas.

Otras normativas relacionadas a la Ciberseguridad:

- Decreto 577/2017. Creación del Comité de Ciberseguridad.
- Decreto 480/2019. Modificación del Decreto 577/2017.
- Resolución 829/2019. Aprobación de la Estrategia Nacional de Ciberseguridad.
- Resolución 141/2019. Presidencia del Comité de Ciberseguridad.

Normativa internacional:

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

Revisión y Actualización

El organismo se compromete a revisar la PSI anualmente, adaptándola a nuevas exigencias organizativas o del entorno, así como a comunicar 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 área de ciberseguridad será la responsable de llevar adelante las revisiones sean periódicas o ad-hoc, dejándose constancia de ellas en el presente documento.
Quien ejerza el cargo de responsable del área aprobará las nuevas versiones, que serán comunicadas en tiempo y forma a todos los alcanzados para su cumplimiento.

Lineamientos específicos

Siguiendo los lineamientos contemplados en el Anexo I “REQUISITOS MÍNIMOS DE SEGURIDAD DE LA INFORMACIÓN PARA LOS ORGANISMOS DEL SECTOR PÚBLICO NACIONAL” aprobado por la Decisión Administrativa N° 641/21, se establecen catorce (14) directrices para organizar la presente Política de Seguridad de la Información:

- Gestión de las Políticas y Normativas de Seguridad
- Política Organizativa
- Política de Recursos Humanos
- Política de Gestión de Activos
- Política de Control de Accesos
- Política de Criptografía
- Política Físico y Ambiental
- Política de Seguridad en las Operaciones
- Política en la Gestión de la Comunicación
- Política de Adquisición, Desarrollo y Mantenimiento de Sistemas
- Política con relación a los Proveedores

- Política de Gestión de Incidentes de Seguridad
- Política de Gestión de la Continuidad
- Política de Cumplimiento

Gestión de las Políticas y Normativas de Seguridad

La presente Política de Seguridad de la Información, deberá ser cumplida por todo el personal prestatario de servicios en el ámbito del Organismo, tanto funcionarios jerárquicos, administrativos, operativos y técnicos, sea cual fuere su modalidad de contratación, nivel escalafonario y situación de revista. Como también deberá ser utilizada como base para establecer el conjunto de normas, procedimientos, lineamientos y guías acordes a los procesos que se llevan adelante en el Organismo, en su plataforma tecnológica y demás recursos de los que disponga.

Se establecen una serie de políticas de seguridad específicas, incluidas como anexos en el presente documento, las cuales indican objetivos, responsabilidades y políticas detalladas aplicables a áreas particulares y también de cumplimiento con carácter obligatorio, se indican además documentos modelos y glosario de términos.

La Política de Seguridad de la Información, será revisada anualmente de forma regular con el objeto de permitir su constante actualización. La actividad de revisión incluye oportunidades de mejoras, en respuesta a los cambios organizacionales, a cambios significativos en procesos críticos o a cambios normativos, legales, de terceros, tecnológicos o de otra índole. Los cambios en la Política de Seguridad de la Información deberán ser aprobados por la máxima autoridad de la jurisdicción o en quien ella delegue esa facultad.

Política Organizativa de la Seguridad

El organismo apoyará e impulsará las iniciativas de seguridad que se propongan con el objeto de preservar la confidencialidad, integridad y disponibilidad de la información que se gestiona y almacena.

Se establecerán responsables del cumplimiento de los distintos procesos y funciones asociados a la seguridad de los sistemas de información dentro del Organismo, como

también la supervisión de los aspectos inherentes a la seguridad tratados en la presente política.
Se designarán, propietarios de la información y propietarios de activos, quienes serán responsables por el resguardo de estos.
Se establecerá la segregación de las funciones asignando distintos perfiles o áreas de responsabilidad para evitar tener conflictos de intereses.
Se promoverá el contacto con otros organismos públicos y entidades privadas para el intercambio de experiencias en materias de seguridad, con el objeto de actualizar e intercambiar conocimientos relativos a seguridad y promover la capacitación continua.

Se contemplará la seguridad de la información en todos los proyectos tecnológicos que lleve adelante en el Organismo.

Se establecerán requisitos de seguridad para el uso de dispositivos móviles, al igual que requisitos para implementar el trabajo remoto.

Política de Uso Aceptable de los Recursos de Tecnología de la Información

Se establecen directivas para el uso adecuado de la información, los sistemas informáticos y entorno tecnológico que posee el Organismo, se especifican acciones consideradas prohibidas con respecto al uso del correo electrónico, Internet y demás recursos tecnológicos de hardware y/o de software, cedidos para su uso laboral al personal del Organismo. Se establecen pautas de conducta para regular el uso de los recursos informáticos que se utilizan.

Política de Recursos Humanos

Se establecerá, la aceptación del cumplimiento del acuerdo de confidencialidad y de la Política de Seguridad de la Información en la contratación. Y durante la relación laboral, la responsabilidad del debido cuidado de los activos tecnológicos cedidos para sus labores y la devolución de estos al finalizar el vínculo laboral con el Organismo.

La Coordinación de Recursos Humanos en las etapas de inducción de los agentes, notificará la existencia y el deber de cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan.

Deberán existir procesos disciplinarios a los agentes que hayan cometido una apertura en la seguridad de la información en conformidad con la normativa vigente del organismo y atendiendo en cada caso la situación de revista y forma de contratación de cada agente. Todas las direcciones velarán e impulsarán el cumplimiento de la política de seguridad de la información. Asimismo, deberán establecer claramente los niveles, perfiles o permisos para acceder a la información y sistemas para todo personal a su cargo, definiendo los perfiles de trabajo y/o permisos en las áreas de su incumbencia.

Los directores y/o jefes de unidades organizativas son responsables ante la desvinculación o cambio de función del personal, que el conocimiento que estos posean sea documentado y transferido apropiadamente, antes de proceder a su desvinculación o cambio de función para evitar afectar el normal funcionamiento de las tareas en su ausencia.

Se establece el compromiso de concientizar y capacitar al personal en temas referidos a las buenas prácticas en seguridad de la información en la Coordinación de Servicios Digitales e Informáticos. Como también el de promover el entrenamiento especializado y frecuente de quienes desarrollan funciones en áreas de seguridad de la información del Organismo.

Política de Gestión de Activos

Se establecerá la existencia de un inventario de activos actualizado, debiendo designar responsables. Si bien la implementación de los controles de seguridad, gestión técnica u operativa podrá ser delegada a personal especializado, el responsable seguirá teniendo a su cargo el activo que le ha sido asignado.

Se establecerá el compromiso de devolución de activos asignados previa a su desvinculación, antes de la finalización del vínculo laboral, contrato o acuerdo con el Organismo.

Se definen normas de uso de los activos de tecnología según las pautas declaradas en la Política de Uso de los Activos de los Recursos de Tecnología de la Información y la devolución de estos cuando el agente se desvincule laboralmente o cuando sea necesario su entrega debido a un cambio en sus funciones.

Se establecerá el tratamiento apropiado para la eliminación de forma segura de los activos de información sobre cualquier medio que pueda contener información del Organismo.

Política de Control de Accesos

Se controlará el acceso a las redes, servicios, información y a los recursos tecnológicos del Organismo, a través de la existencia de directivas y procedimientos que reglamentan la gestión de usuarios y la gestión de permisos de acceso a la información y a los recursos tecnológicos del Organismo.

Se restringirá el acceso a la información, en concordancia con la clasificación de esta, sobre la base de la premisa rectora, “Todo acceso está prohibido, a menos que se permita explícitamente” mediante la autorización formalizada de cada dirección indicando los perfiles y permisos de acceso del personal a su cargo a los sistemas y/o recursos de información que sean requeridos para las actividades y tareas que cada empleado o funcionario deba llevar adelante.

Se establecerá el seguimiento de las cuentas con privilegios especiales y la revisión de los permisos de acceso configurados en los sistemas mediante auditorias periódicas, controlando que estos coincidan con los perfiles y permisos informados por cada dirección del Organismo.

Se establecerá la gestión segura de las contraseñas y/o dispositivos de autenticación, como también las responsabilidades de los usuarios sobre el uso de estos, por lo cual se establecerá que los agentes, funcionarios y demás usuarios deberán hacer un uso responsable de sus dispositivos y datos de autenticación. Se declara que se encuentra estrictamente prohibido compartir los mismos.

Se establecerá que los sistemas de administración de contraseñas apliquen contraseñas de calidad, por lo cual se deberán establecer criterios de complejidad como ser longitud mínima, caracteres, mayúsculas, minúsculas y caracteres numéricos o especiales para su conformación y cambios de forma periódica. Se promoverá el uso de gestores de almacenamiento de contraseñas para los usuarios finales mediante aplicaciones específicas para tal fin.

Se prohíbe que personal no autorizado haga uso de programas especiales con capacidades de anulación de los sistemas de control y seguridad.

Se promoverá el inicio de sesión seguro mediante la implementación de dos o más factores de autenticación para acceder a los sistemas y servicios cuando sea posible. Se limitará el acceso al código fuente de los programas del Organismo solo al personal autorizado.

Se monitorea, inspecciona y controla el tráfico de datos en las redes del Organismo, comunicaciones internas, como también toda comunicación externa entrante hacia las redes del Organismo y toda comunicación saliente hacia Internet con el objeto de verificar que no se violen las políticas de seguridad establecidas.

Política en la Gestión de la Criptografía

Se establecerá el uso de la criptografía para asegurar la información y las comunicaciones, el resguardo de las contraseñas, en el almacenamiento de las copias de seguridad, en el cifrado de dispositivos móviles, en las conexiones de trabajo remoto, en la comunicación de los servicios expuestos a Internet y en toda transmisión de datos, dentro y fuera del ámbito del Organismo.

Se establece el uso de certificados digitales en todos los sitios de Internet que publica el Organismo para asegurar un canal de comunicación cifrado.

Política Físico Ambiental

Se controlará la identificación, ingreso y egreso físico a las dependencias del Organismo, con el objeto de evitar el acceso no autorizado, daño o hurto a las instalaciones e interferencias en las actividades del Organismo.

Se definen perímetros de seguridad y controles extras, para proteger las áreas consideradas como críticas, definiéndose inicialmente éstas como las áreas ocupadas por las oficinas de las autoridades superiores del Organismo, Sala de Comunicaciones, Centro de Procesamiento de Datos, Instalaciones de los Grupos Electrógenos e Instalaciones de Aire Acondicionado, considerando que la exposición, mal funcionamiento o puesta fuera de

servicio de las mismas, pueda afectar el normal desempeño de los sistemas de información del Organismo. A estos fines se establecerán controles adicionales, a través de la existencia de distintos niveles de accesos biométricos, control de seguridad física permitiendo solo el acceso autorizado, seguimiento y control mediante cámaras de seguridad, prohibición de grabaciones de video y fotografías sin la debida autorización y acompañamiento por personal del Organismo ante la ejecución de trabajos por parte de proveedores.

Se asegura la continuidad operacional del suministro de energía eléctrica y del control ambiental en el centro de procesamiento de datos y sala de comunicaciones, como también la existencia de controles de seguridad para asegurar la protección del cableado de transmisión de datos.

Se establecerá la existencia del inventario de activos físicos que procesan información, indicando su localización física y asignación organizacional y personal para su uso. Se establecerá el registro de las personas y de los activos que son retirados fuera de las instalaciones del Organismo, la adopción de controles y medidas de seguridad extras para el equipamiento informático que es utilizado fuera del Organismo, con el objeto de minimizar el impacto ante la pérdida o robo de este.

Se propiciará el mantenimiento periódico del equipamiento informático y destrucción segura de los dispositivos de almacenamiento, cuando el equipamiento no pueda ser reutilizado o donado, con el objeto de no exponer información residual, considerada privada o confidencial en el equipo informático.

Se adoptará la política de escritorios limpios, con el objeto de proteger documentación en papel u otro medio de almacenamiento de información reservada, confidencial o secreta que pudiera existir en el área de trabajo, evitando de este modo su pérdida y divulgación no deseada. Se adoptará también la política de pantallas limpias, a fin de reducir los riesgos de acceso no autorizado y/o fuga de información desde el equipo informático que se encontrase desatendido.

Política de Seguridad en las Operaciones

Se declararán responsables de las operaciones, quienes deberán documentar procedimientos para gestionar las principales tareas operativas en las instalaciones de

procesamiento de información. Se redactará documentación de gestión de cambios, como requisito previo a la implementación de los cambios en la infraestructura y/o sistemas de procesamiento de información.

Se evaluarán periódicamente las necesidades de capacidad operacional de los sistemas y la proyección de futuras demandas, con el objeto de garantizar que el crecimiento no ponga en riesgo las actividades operativas ante la falta de recursos.

En los procesos de desarrollo de software, se definirán entornos separados e independientes entre sí, con el objeto de generar software seguro, sin defectos o fallos en el servicio que ofrecen y evitar problemas de indisponibilidad.
Se protegerán los sistemas tecnológicos contra todo tipo de código malicioso, mediante la ejecución de análisis periódicos preventivos de detección y eliminación de malware en las estaciones de trabajo, servidores, como también controles de detección y eliminación de malware en las conexiones de internet y correo electrónico.

La información y los sistemas se deberán resguardar de manera periódica y programada mediante la generación de copias de seguridad y pruebas de restauración.

Se sincronizan los relojes de todos los sistemas para el correcto registro de los eventos de los usuarios y sistemas; respecto de accesos, fallas, instalación y ejecución de software, alertas de seguridad y cualquier otra actividad relevante. Dichos registros de eventos se almacenarán de forma segura para futuras consultas o actividades de auditoría, teniendo especial cuidado con los registros de eventos de usuarios con privilegios administrativos para evitar su manipulación.

La instalación de software está supeditada conforme a los procedimientos, autorizaciones, conformidades y pruebas previas pertinentes antes que los mismos sean puestos en producción y solo podrá ser efectuado por personal autorizado.

Se evaluará la seguridad de los sistemas publicados, mediante pruebas periódicas de evaluación de vulnerabilidades y elaboración de informes de remediación y mejoría para su corrección.

Política en la Gestión de las Comunicaciones

Se monitoreará, registrará, controlará y restringirá el acceso a las redes que integran la infraestructura de telecomunicaciones del Organismo, independientemente del medio de transmisión implementado.

Se segregará y restringirá el tráfico de red de acuerdo con los perfiles y permisos asignados a los usuarios, que fueran declarados por los responsables de las distintas unidades organizativas.

Se controlará el tráfico hacia y desde Internet con el objeto de evitar que la navegación transgreda las normas establecidas en la Política de Uso Aceptable de los Recursos de Tecnología del Información.

Se promoverá que la autenticación de los usuarios sea realizada implementando múltiples factores de autenticación para asegurar la identidad de los usuarios antes que estos acceden remotamente a las redes de la Organismo.

Se implementarán dispositivos de red redundantes para mantener la alta disponibilidad en los servicios de red.

El intercambio de información con entidades externas se deberá realizar a través conexiones cifradas de extremo a extremo y se deberá promover la implementación de certificados digitales para la validación de las dos partes intervinientes y de este modo asegurar la confidencialidad, integridad y la autenticidad de la información que se transmite y envía hacia redes externas.

En los acuerdos entre el Organismo y otras entidades públicas o privadas, relativos al intercambio de información, se especificarán consideraciones técnicas de seguridad para la transferencia segura de datos entre ambas partes, como también se establecerán acuerdos de confidencialidad para la protección de la información que se comparte.

Se considera al correo electrónico un servicio crítico, por lo cual se implementan medidas de protección mediante sistemas redundantes para la gestión del correo electrónico y sistemas de seguridad antimalware y filtros anti-spam, con el objeto de detectar archivos

adjuntos maliciosos o correos fraudulentos que intenten robar o dañar los activos de información.

La utilización de servicios de Internet será monitoreada y controlada, con el objeto de evitar que el uso indebido de dichos servicios afecte el rendimiento de la infraestructura de comunicaciones o pongan en riesgo la seguridad de esta ante la descarga e instalación de archivos. Razón por la cual el uso de Internet, al igual que el uso del correo electrónico laboral estará sujeta a las condiciones de uso descriptas en la Política de Uso Aceptable de los Recursos de la Tecnología de la Información.

Política de Adquisición, Desarrollo y Mantenimiento de Sistemas

En toda adquisición de sistemas informáticos, como también en todos los proyectos de desarrollo de software, tanto propios o de terceros, se deberá establecer la inclusión de requerimientos de seguridad, como también la existencia de directivas de seguridad para el desarrollo de aplicaciones, las cuales describen requerimientos básicos de seguridad a considerar en todo desarrollo.

Se considera a la seguridad de la información como una parte importante en los ciclos de vida de los procesos de desarrollo y adquisición, por lo cual se deberá contemplar la seguridad en todos los niveles de la arquitectura, negocios, datos, aplicaciones y tecnología; equilibrando la necesidad de la seguridad con la accesibilidad.

Se deberán establecer controles para asegurar los sistemas del Organismo expuestos a Internet, con el objeto de protegerlos contra actividades fraudulentas, modificaciones y divulgación de datos no autorizados, intercepción, vulneración de la confidencialidad, suplantación de identidad y cualquier otra amenaza existente.

Se deberán evaluar, validar y documentar los cambios, con el objeto de minimizar los riesgos de modificaciones indebidas que pudieran comprometer las operaciones en el entorno productivo, respetando las instancias de desarrollo, pruebas y producción e incorporando de este modo efectivos controles cruzados o por oposición.

Se deberán realizar evaluaciones de seguridad en busca de vulnerabilidades sobre desarrollos de software nuevos o modificaciones, propios o de terceros y del sistema

operativo de la plataforma en la que está implementada la misma antes que los mismos sean puestos en producción.

Se deberán establecer programas de ejecución de pruebas funcionales que permitan evaluar los requisitos funcionales y el cumplimiento de estos en los sistemas desarrollados. Se declara que todo algoritmo o código fuente desarrollado internamente o por terceros es de propiedad exclusiva del Organismo, estando prohibida su copia parcial, total y distribución de esta a terceros sin la debida autorización.

Se deberán usar datos de prueba de manera segura para las pruebas funcionales.
La modificación, actualización o eliminación de los datos operativos en producción deberán ser realizadas, solo a través de los sistemas que procesan dichos datos. Se considerarán excepciones, debiendo ser las mismas documentadas e informadas a las partes interesadas siendo estos los propietarios de la información, los responsables de la gestión funcional y técnica y el responsable de los procesos a los cuales afecte la modificación manual, debiéndose registrar detalladamente dicha modificación.

Política con relación a los Proveedores

Se incluirán los niveles de servicio (SLA) y acuerdos de confidencialidad en los contratos o convenios con los proveedores.

Se establece que todo cambio a realizar por lo proveedores sobre los sistemas e infraestructura deberá ser planificado e informado previamente al personal técnico del área de competencia, para su evaluación, cálculo del riesgo que implica dicho cambio y confirmación de ejecución por parte del personal técnico del Organismo; para lo cual se establece la gestión de cambios.

Los proveedores que accedan físicamente a las instalaciones para dar soporte se deberán identificar, registrar sus ingresos y deberán estar siempre acompañados por personal técnico del Organismo dentro de las instalaciones de la Organismo.

Se deberán controlar las implementaciones de los proveedores, monitorear su cumplimiento y la gestión en los cambios, con el fin de asegurar que los servicios que se presten cumplan con todos los requerimientos acordados previamente.

Política de Gestión de Incidentes de Seguridad

Se establece que la Coordinación de Servicios Digitales e Informáticos tiene la autoridad para acceder a todo sistema o dispositivo de la infraestructura tecnológica involucrada en alertas o incidentes de seguridad que considere apropiado, para evitar que escale y pudiera afectar la disponibilidad, confidencialidad o integridad de la información y de los recursos tecnológicos del Organismo

El personal del Organismo, cuando descubra fallas o debilidades, detecte alertas o incidentes de seguridad, tiene la obligación de informarlo a la Coordinación de Servicios Digitales e Informáticos.

Se deberán establecer procesos documentados y asignación de responsabilidades para la adecuada gestión de respuesta a incidentes de seguridad de la información. Se deberá incluir la recopilación y registro de evidencia para su evaluación inicial, análisis del incidente y acciones de remediación, comunicación del estado de situación del proceso de resolución del incidente, registro formal de las acciones realizadas y cierre del incidente, cuando sea necesario se realizará un análisis forense y/o post-incidente, para confirmar la causa y aprender del mismo.

Se deberán documentar procedimientos para la correcta adquisición de imágenes forenses y preservación de la información que pudiera servir como evidencia, ya sea para implementar una medida disciplinaria interna o iniciar una acción legal.

Política de Gestión de la Continuidad

A fin de contrarrestar la pérdida de la continuidad operativa, se deberá desarrollar e implantar el plan de contingencia para asegurar la continuidad de los procesos del Organismo, para que las operaciones se puedan restaurar en los plazos requeridos.

Para garantizar que los planes operativos de restauración de las operaciones sean ordenados y consistentes entre sí, se deberá tener en cuenta la priorización de los procesos críticos, la asignación de responsabilidades, la identificación de las amenazas que pudieran ocasionar interrupciones en los procesos, la documentación de la estrategia de continuidad de las actividades consecuente con los objetivos y prioridades acordados, la comunicación

y capacitación del personal, en materia de procedimientos y procesos de emergencia acordados y de recuperación.

Se deberán realizar pruebas y revisiones de los planes de continuidad de las operaciones con el objeto de mantenerlos actualizados ante cambios en los procesos de negocio y en la tecnología involucrada.

Para minimizar el riesgo de la pérdida de la continuidad operativa se deberán implementar arquitecturas y/o componentes redundantes en las instalaciones de procesamiento y transmisión de la información.

Política de Cumplimiento Normativo y Técnico

Se respetan los requisitos contractuales, regulatorios y legales vigentes. Los empleados aceptan conocer y cumplir con lo dispuesto por la Ley 25.164 (Ley Marco de Regulación de Empleo Público Nacional), Ley 25.188 (Ética en el Ejercicio de la Función Pública), Decreto 41/99 (Código de Ética de la Función Pública), Ley 11.723 (Ley de Propiedad Intelectual), Ley N° 25.506 (Ley de Firma Digital) y Ley 26.388 (Ley de Delitos Informáticos).

Se establece la protección de los registros de datos contra pérdida, destrucción, acceso no autorizado, publicación no autorizada, degradación del medio de almacenamiento, obsolescencia del formato o medio de almacenamiento.

Se respeta la privacidad de la información personal por lo cual se informa y detallan las actividades que serán objeto de control y monitoreo, a fin de no violar el derecho a la privacidad del empleado. A su vez los empleados conocen las restricciones al tratamiento de los datos y de la información que administran con motivo del ejercicio de sus funciones, por lo cual firman el Acuerdo de Confidencialidad.

Se verifica periódicamente que los sistemas de información cumplan con lo establecido por la Política de Seguridad de la Información, normas y procedimientos de seguridad; las que incluirán la revisión de los sistemas en producción. Esta verificación comprende pruebas de evaluación de vulnerabilidades y/o pruebas de penetración, cuyo objetivo es la detección de vulnerabilidades en los sistemas y la infraestructura.

Se establecen auditorias de cumplimiento en los sistemas de información, infraestructura tecnológica y en los procesos existentes, como también de la revisión independiente del estado de la seguridad realizada por la Unidad de Auditoría Interna o Especialistas de Seguridad externos al Organismo para garantizar la eficacia de los controles implementados.

ANEXO - Términos y Definiciones

Seguridad de la Información

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.

- 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.

- Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

Adicionalmente, deben considerarse los conceptos de:

- Auditabilidad: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

- 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.

- 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.

- Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el organismo.
- No repudio: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

- 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.

A los efectos de una correcta interpretación de la presente Política, se realizan las siguientes definiciones:

- Activo: Información, conocimiento sobre los procesos, el personal, hardware, software y cualquier otro recurso involucrado en el tratamiento de los datos, que tenga valor para la organización.
- Amenaza: Una causa potencial de un incidente no deseado, el cual puede ocasionar daños a un sistema u organización.
- Control**:** Medio para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras organizacionales, las cuales pueden ser de naturaleza administrativa, técnica, de gestión, o legal.

NOTA. Control es también utilizado como sinónimo de salvaguarda o de contramedida.

- Contraseñas Críticas: En los diferentes ambientes de procesamiento existen cuentas de usuarios con las cuales es posible efectuar actividades críticas como ser instalación de plataformas o sistemas, habilitación de servicios, actualización de software, configuración de componentes informáticos, etc. Dichas cuentas no serán de uso habitual (diario), sino que sólo serán utilizadas ante una necesidad específica de realizar alguna tarea que lo requiera y se encontrarán protegidas por contraseñas con un mayor nivel de complejidad que el habitual.

- 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 esta, la probabilidad de que ocurran y su potencial impacto en la operatoria del organismo.

- Gestión de Riesgos: Actividades coordinadas para dirigir y controlar una organización en lo que concierne al riesgo.

NOTA. La gestión de riesgos usualmente incluye la evaluación de riesgos, el tratamiento de riesgos, la aceptación de riesgos y la comunicación de riesgos.

- Incidente de Seguridad: Un incidente de seguridad es un evento adverso en un sistema de computadoras, o red de computadoras, que puede comprometer o compromete la confidencialidad, integridad y/o disponibilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

- 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.

- Riesgo: Combinación de la probabilidad de ocurrencia de un evento y sus consecuencias o impacto.

- 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 la UTN 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.

- Tratamiento de Riesgos: Proceso de selección e implementación de medidas para modificar el riesgo.

- Vulnerabilidad: Una debilidad de un activo o grupo de activos que puede ser aprovechada por una amenaza.

- Inducción: Es el proceso por el cual un empleado adquiere los conocimientos necesarios para manejarse dentro de la empresa e integrarse plenamente en su funcionamiento.

- Ad-hoc: significa "para este propósito" o "para esto". Es una frase latina que a menudo se utiliza para indicar que un determinado acontecimiento es temporal y es destinado a ese propósito específico.

- SLA: Un acuerdo de nivel de servicio (Service Level Agreement) es un contrato que establece las responsabilidades y obligaciones entre una empresa y su cliente. Entre otras cosas, define sin lugar a duda las expectativas que deberán cumplirse entre ambas partes sobre la calidad del servicio prestado.

- Obsolescencia: Es el proceso de volverse obsoleto, anticuado, ya no de uso general, o ya no útil, o la condición de estar en tal estado.

- Malware o “software malicioso”: Es un término amplio que describe cualquier programa o código malicioso que es dañino para los sistemas.

República Argentina - Poder Ejecutivo Nacional
1983/2023 - 40 AÑOS DE DEMOCRACIA

Hoja Adicional de Firmas
Anexo

Número: IF-2023-11033879-APN-CSDI#INAES

CIUDAD DE BUENOS AIRES
Lunes 30 de Enero de 2023

Referencia: EX-2023-11005920- -APN-CSDI#INAES - Política de Seguridad de la Información INAES.

El documento fue importado por el sistema GEDO con un total de 23 pagina/s.

Digitally signed by Esteban Jose Piemontese
Date: 2023.01.30 17:26:46 ART
Location: Ciudad Autónoma de Buenos Aires

Esteban Jose Piemontese
Coordinador
Coordinación de Servicios Digitales e Informáticos
Instituto Nacional de Asociativismo y Economía Social

Digitally signed by Gestion Documental Electronica
Date: 2023.01.30 17:27:21 -03:00