Ministerio de Economía
Presidencia de la Nación

Instituto Nacional de
Estadística y Censos
República Argentina

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Av. Julio A. Roca 609, C1067ABB
Ciudad Autónoma de Buenos Aires, Argentina
Horario de atención de 9:30 a 16:00

ces@indec.gob.ar
Tel.: (54-11) 5031-4632

www indec.gob.ar

INDECArgentina

INDICE

Contenido

Av. Julio A. Roca 609, C1067ABB
Ciudad Autónoma de Buenos Aires, Argentina
Horario de atención de 9:30 a 16:00

ces@indec.gob.ar
Tel.: (54-11) 5031-4632

www indec.gob.ar

INDECArgentina

HISTORIAL DE REVISIONES

Responsable	Fecha	Cambios
Seguridad Informática	04/12/2018	Versión inicial de la Política de Seguridad de la Información (0.95)
Seguridad Informática	25/03/2019	Realineamiento de la política al modelo de la ONTI (0.99)
Procesos y Auditoria	14/04/2019	Sugerencias y Correcciones varias
Seguridad Informática	24/04/2019	Correcciones varias
DI	23/5/2019	Revisión borrador final
Seguridad Informática	22/09/2020	Correcciones varias

RESUMEN

El Instituto Nacional de Estadística y Censos (INDEC) en cumplimiento con la Decisión Administrativa N° 669/2004 de la Jefatura de Gabinete de Ministros, establece la necesidad de contar con una Política de Seguridad de la Información, la cual define directivas orientadas a resguardar la confidencialidad, integridad y disponibilidad de la información, protección de los recursos tecnológicos y la continuidad de las operaciones del Organismo, en conformidad con las leyes y normativas jurídicas vigentes. Se define para ello los siguientes dominios en la declaración de las políticas de seguridad.

Políticas y Normativas de Seguridad

Se establece la “Política de Seguridad de Información” (PSI), aprobada por la máxima autoridad del Organismo, publicada y comunicada a todo el personal.

Se declara la “Política de Uso Aceptable de los Recursos de Tecnología de la Información” (PUA), la cual establece las normas de conducta razonable, que deben observar los agentes y funcionarios del Organismo, cuando utilicen los recursos tecnológicos puestos a su disposición para el desempeño de sus tareas.

Se establecen, además, políticas y normativas complementarias que al igual que las anteriores deberán ser de cumplimiento de carácter obligatorio. Como también la revisión de todas las políticas y normativas de forma regular.

Política Organizativa

Se conforma el “Comité de Seguridad de la Información”, formado por los responsables de las principales áreas sustantivas, el cual será responsable de apoyar e impulsar las políticas, planes y programas referidos a la política de seguridad de la información.

Se conforma también la “Coordinación de Seguridad Informática”, la cual tendrá a su cargo las funciones relativas a la seguridad de los sistemas de información y procesos del Organismo, como también la supervisión de todos los aspectos inherentes a la seguridad tratados en la presente política.

Se establecen responsables en el cumplimiento de los distintos procesos de seguridad. Se designan, propietarios de la información y propietarios de activos, quienes serán responsables por el resguardo de los mismos.

Se apoya 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 contempla la seguridad de la información en todos los proyectos del Organismo.

Se establecen requisitos de seguridad para el uso de dispositivos móviles y el trabajo a distancia, los cuales deben cumplir con ciertas directrices de seguridad, antes que estos accedan a los recursos del Organismo, como también ciertas consideraciones de uso, fuera de las instalaciones.

Política de Recursos Humanos

Se considera fundamental la gestión del ciclo de vida del vínculo laboral de las personas, por lo cual se establecerá la revisión de los antecedentes del postulante antes del empleo, la aceptación de los documentos Acuerdo de Confidencialidad y PUA al inicio del mismo y la devolución de activos al finalizar el vínculo laboral con el Organismo.

Los responsables del área de pertenencia del empleado informarán de la existencia de la PSI y PUA, velarán por el cumplimiento de las normativas vigentes e informarán que el incumplimiento podrá ser pasible del inicio de un proceso administrativo disciplinario.

Se declara el compromiso de concientizar y capacitar al personal en temas referidos a las políticas, procedimientos y buenas prácticas en seguridad informática

Se establece la existencia de un proceso disciplinario para todos aquellos agentes, sea cual fuere su situación de revista en el Organismo, que violen las políticas, normativas y procedimientos de seguridad vigentes.

Política de Gestión de Activos

Se establece la identificación, clasificación y criticidad de los activos de información, físicos y de recursos humanos, mediante un inventario actualizado, designándose responsable de los mismos a los Propietarios de Activos.

Se identifican, documentan y definen normativas de uso de los activos de tecnología según las pautas declaradas en la PUA.

Se definen directrices de clasificación, etiquetado y manipulación de activos de información.

Se establece que el tratamiento de la información, respecto a su almacenamiento, transporte y eliminación se realizará de forma segura.

Política de Control de Accesos

Se controla el acceso a la información y a los recursos tecnológicos del Organismo, por ello se establece la existencia de pautas 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 restringe el acceso a la información, en concordancia con la clasificación de la misma, sobre la base de la premisa rectora, “Todo acceso está prohibido, a menos que se permita explícitamente”.

Se establece la gestión segura de las contraseñas, como también las responsabilidades de los usuarios, sobre el uso de las mismas.

Se monitorea, inspecciona y controla, el tráfico de datos en las redes del Organismo, 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.

Av. Julio A. Roca 609, C1067ABB
Ciudad Autónoma de Buenos Aires, Argentina
Horario de atención de 9:30 a 16:00
ces@indec.gob.ar
Tel.: (54-11) 5031-4632
www indec.gob.ar
INDECArgentina

Política de Criptografía

Se establece el uso de la criptografía para asegurar la información y las comunicaciones, como ser contraseñas, almacenamiento de las copias de resguardo, cifrado de dispositivos móviles, servicios expuestos a Internet y transmisión de datos, dentro y fuera del ámbito del Organismo.

Política Físico y Ambiental

Se controla el ingreso físico a las dependencias del Organismo, con el objeto de evitar el acceso no autorizado, daño a las instalaciones o interferencias en las actividades del Organismo. Se definen, además, perímetros de seguridad y controles, para proteger las áreas consideradas como críticas, considerando que su mal funcionamiento o puesta fuera de servicio, pueda entorpecer el normal desempeño de los sistemas de información del Organismo exponer información que administra dicha área.

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 realiza el mantenimiento periódico del equipamiento informático, control de su entrada y salida de las dependencias del Organismo y destrucción segura cuando el equipamiento no pueda ser reutilizado, con el objeto de no exponer información residual, considerada privada o confidencial en el equipo informático.

Se adopta la política de escritorios limpios, con el objeto de proteger documentación en papel u otro medio de almacenamiento de información que pudiera existir en el área de trabajo, evitando de este modo su pérdida y divulgación no deseada.

Se adopta también la política de pantallas limpias, a fin de reducir los riesgos de acceso no autorizado en un equipo informático que se encontrase desatendido.

Política de Seguridad en las Operaciones

Se establece la evaluación periódica de 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.

Se implementan procedimientos para gestionar tareas operativas y responsables para la ejecución de las mismas.

En los procesos de desarrollo de software, se definen entornos separados entre sí, desarrollo, pruebas funcionales, pruebas de seguridad y producción, con el objeto de generar sistemas seguros.

Se protegen los sistemas tecnológicos contra todo tipo de código malicioso, mediante la ejecución de análisis periódicos preventivos y controles de detección en las estaciones de trabajo, servidores, conexiones de internet y correo electrónico.

La información y los sistemas se resguardan mediante la generación de copias de seguridad de manera periódica y programada.

Se monitorean, registran y auditan los eventos de los usuarios y sistemas, respecto de accesos, fallas, instalación y ejecución de software, alertas de seguridad y cualquier otra actividad relevante.

La instalación de software está supeditada conforme a los procedimientos, autorizaciones, conformidades y pruebas previas pertinentes.

Se evalúa el grado de riesgo de los sistemas publicados, mediante pruebas periódicas de evaluación de vulnerabilidades e informes de remediación y mejoría.

Política en la Gestión de Comunicaciones

Se monitorea, controla, segrega y restringe el tráfico el acceso, independientemente del medio de transmisión implementado, en todas las redes de datos que integran la infraestructura de comunicaciones del Organismo.

Se considera el correo electrónico como un servicio crítico, por lo cual se implementan medidas de protección para su funcionamiento continuo y de manera eficiente.

La utilización de servicios de Internet, es monitoreada y controlada, con el objeto de evitar que el uso indebido de dichos servicios, afecten el rendimiento de la infraestructura de comunicaciones o pongan en riesgo la seguridad de la misma, por lo cual el uso de Internet, al igual que el uso del correo electrónico laboral, estarán sujetos a las condiciones de uso descriptas en la PUA.

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 establece la inclusión de requerimientos de seguridad. Se considerará a la seguridad de la información como una parte integral en los ciclos de vida de los procesos de desarrollo y adquisición.

Se protegen todos los sistemas expuestos a Internet contra actividades fraudulentas, modificaciones y divulgación de datos no autorizados, intercepción, vulneración de la confidencialidad, suplantación de identidad o cualquier otra amenaza existente.

Se realizan pruebas de evaluación de vulnerabilidades en los sistemas e infraestructura del Organismo, con el objeto de detectar debilidades para luego remediarlas.

Se usan datos de prueba de manera segura y siguiendo requisitos de seguridad estipulados en los entornos de desarrollo y pruebas funcionales y de seguridad.

Política en Relación a los Proveedores

Se establecen una serie de requisitos de seguridad para proteger los activos de información que son accedidos por los proveedores, como también los riesgos asociados a los servicios provistos por parte de terceros.

Se controlan las implementaciones de los proveedores, se monitorea 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 con los proveedores.

Política de Gestión de Incidentes de Seguridad

Todo el personal del Organismo, es responsable de informar los incidentes de seguridad cuando los detecten, como también de comunicar las fallas o debilidades descubiertas en los sistemas tecnológicos que usan.

Se establecen responsabilidades y procedimientos para gestionar los incidentes de seguridad, con el fin de garantizar una respuesta rápida, eficaz y sistemática, ante la aparición de los mismos.

Se aplicará un proceso disciplinario contemplado en las normas estatutarias y convencionales que rigen al personal de la Administración Publica Nacional, para los empleados que violen la Política de Seguridad de la Información y la Política de Uso Aceptable de los Recursos de Tecnología de la Información.

Cuando la respuesta a un incidente de seguridad de la información, implique medidas administrativas o legales se establecerán procedimientos complementarios de identificación, adquisición y almacenamiento de evidencia forense.

Política de Gestión de la Continuidad

A fin de contrarrestar la aparición de desastres, se desarrollan e implantan planes de contingencia para asegurar la continuidad de los procesos del Organismo, para que las operaciones se puedan restaurar en los plazos requeridos y manteniendo los requerimientos de seguridad.

Política de Cumplimiento

Se respetan los requisitos contractuales, regulatorios y legales vigentes.

Se aboga por el cumplimiento de las leyes relacionadas a la propiedad intelectual, protección de datos personales, firma digital, delitos informáticos, así como también todo el marco normativo interno de seguridad de la información. Para lo cual se establece realizar revisiones de cumplimiento y de auditoría en los sistemas de información, infraestructura tecnológica y en los procesos existentes.

1 Introducción

Si bien el uso de las actuales tecnologías informáticas, permiten procesar grandes cantidades de información, estas tecnologías están expuestas a múltiples amenazas, más aún, cuando no se cuenta con una correcta gestión de la 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, asegurando de este modo el cumplimiento eficiente de los objetivos del Instituto Nacional de Estadística y Censos (INDEC).

Siendo para ello necesario, el compromiso manifiesto de las máximas autoridades del Organismo y de los titulares de todas las unidades organizativas, 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.

Razón por la cual se decide implementar las siguientes medidas, conforme a la Decisión Administrativa N° 669/2004 de la Jefatura de Gabinete de Ministros que establece la obligatoriedad para los organismos del Sector Público Nacional, de:

- Conformar un Comité de Seguridad en la Información.
- Establecer las funciones del Comité de Seguridad de la Información.
- Designar un coordinador del Comité de Seguridad de la Información.
- Dictar o adecuar la Política de Seguridad conforme la “Política de Seguridad de la Información Modelo”, según Disposición 1/2015 de la Oficina Nacional de Tecnologías de Información.

1.1 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 toda la planta de personal del Organismo, tanto se trate de funcionarios jerárquicos, administrativos, operativos y técnicos, sea cual fuere su nivel escalafonario y su situación de revista.

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 través de acuerdos o contratos con terceros.

1.2 Objetivo

El objetivo de la presente política, es el de proteger los activos de información y de todos los recursos tecnológicos del Organismo, utilizados en su transmisión, procesamiento y almacenamiento, frente a amenazas internas o externas, deliberadas o accidentales.

Mediante la implementación de un adecuado conjunto de controles, que incluyen, políticas, procesos, procedimientos, estructura organizacional, funciones de software y hardware, identificación de recursos y partidas presupuestarias necesarias para alcanzar dichos objetivos.

Av. Julio A. Roca 609, C1067ABB
Ciudad Autónoma de Buenos Aires, Argentina
Horario de atención de 9:30 a 16:00

ces@indec.gob.ar
Tel.: (54-11) 5031-4632

www indec.gob.ar

INDECArgentina

2 Lineamientos

2.1 Principios

La presente política se basa en los principios de confidencialidad, integridad y disponibilidad de la información como también el principio de la continuidad operacional, principios básicos que rigen la Seguridad de la Información.

2.2 Responsabilidad

Es responsabilidad de la Alta Dirección de hacer uso de la Política de Seguridad de la Información, como parte de sus herramientas de gobierno y gestión, como también de apoyar y hacer cumplir los estándares, procedimientos y lineamientos que garanticen su acatamiento.

2.3 Acatamiento

La presente Política de Seguridad de la Información, expresa declaraciones respecto a temáticas inherentes a la seguridad, de acatamiento obligatorio, motivo por el cual se usan términos definitivos como “deberá”, en vez de “debería”. Es decir que no son recomendaciones o sugerencias, sino, declaración que exigen su acatamiento.

2.4 Excepciones

Todas las excepciones a la Política de Seguridad de la Información, deberán ser formalmente documentadas, registradas y revisadas.

La excepción al cumplimiento de la presente Política de Seguridad deberá ser solicitada formalmente por el responsable de la dirección interesada y posteriormente evaluada por la Coordinación de Seguridad Informática, antes de su implementación.

2.5 Marco Normativo

Todas las definiciones de la presente Política de Seguridad de la Información se encuentran alineadas de acuerdo a la Legislación de la República Argentina, respecto a:

- Marco Legal de las Estadísticas Oficiales, Ley N° 17.622
- Protección de Datos Personales, Ley N° 25.326
- Delitos Informáticos, Ley N° 26.388
- Firma Digital, Ley N° 25.506
- Ética en el Ejercicio de la Función Pública, Ley N° 25.188
- Propiedad Intelectual, Ley N° 11.723

- Procedimientos Administrativos, Ley N° 19.549

Como también a los estándares internacionalmente aceptados para la práctica de seguridad de la información, particularmente respecto de:

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

3 Términos y Definiciones

La seguridad de la información se entiende como la preservación de las siguientes tres características:

- **Confidencialidad**: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- **Integridad**: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- **Disponibilidad**: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, deben considerarse los conceptos de:

- **Autenticidad**: busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- **Auditabilidad**: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
- **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:

- **Amenaza**: Es toda acción potencial que puede ocasionar daño o pérdida a un sistema o a la organización.
- **Autenticador**: Es un tipo de dispositivo portátil, que es usado para verificar la identidad de un individuo que desea utilizar un servicio en particular, también conocido como token de autenticación.
- **Backbone**: Cableado troncal de la red de datos, también denominado cableado vertical, que realiza la interconexión entre la sala principal de comunicaciones y cada uno de los gabinetes de comunicación, distribuidos en un cada uno de los pisos de un edificio.

- **Código Malicioso**: Programa malicioso, también llamado código maligno, software malicioso, software dañino o software malintencionado, el cual hace referencia a cualquier tipo de software que trata de infiltrarse sin el consentimiento del usuario para robar información, dañar el sistema afectado o hacer uso de los recursos informáticos para afectar a otros sistemas.
- **Comité de Seguridad de la Información**: Es el cuerpo integrado por los representantes de todas las direcciones sustantivas del Organismo, incluida el área de Seguridad de la Información, con el fin de garantizar el apoyo manifiesto de la alta dirección a las iniciativas de seguridad presentes y futuras.
- **Continuidad operacional**: Refiere a la continuidad de los procesos de negocio en el organismo y su recuperación ante la ocurrencia de un desastre.
- **Contramedida**: Control
- **Control**: Es un 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. Utilizado también como sinónimo de salvaguarda o de contramedida
- **Escrow**: Es un tipo de contrato en el cual, las partes, se comprometen a usar los servicios de un tercero como depositante de los bienes que ofrece cada uno de ellos. Transfiriendo el bien a la otra parte solo si se cumplen las condiciones establecidas previamente.
- **Evaluación de Riesgos**: Se refiere a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria del Organismo.
- **Gestión de Riesgos**: Son las actividades implementadas para dirigir y controlar una organización en lo que concierne al riesgo. 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**: Es un evento adverso en un sistema o red de computadoras, que puede comprometer la confidencialidad, integridad y/o disponibilidad de la información. Pudiendo ser causado por la explotación de alguna vulnerabilidad y que atenta 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.
- **Malware**: Código Malicioso.
- **Propietario de la Información**: Define a la persona responsable de la integridad, confidencialidad y disponibilidad de una cierta información.
- **Remediación**: Proceso que conduce al restablecimiento total o parcial del nivel de seguridad de un sistema, producto de la implementación de una contramedida que

disminuye, mitiga o elimina una amenaza. Por ejemplo, la instalación de actualizaciones de seguridad en un sistema operativo

- **Riesgo**: Es la combinación de la probabilidad de ocurrencia de una amenaza y su impacto si la misma tuviera éxito.
- **Sistema de Información**: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.
- **Tecnología de la Información**: Se refiere al hardware y software operados por el Organismo o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.
- **Tratamiento de Riesgos**: Se refiere a la selección e implementación de controles para modificar el riesgo.
- **Vulnerabilidad**: Es una debilidad existente en un activo que puede ser aprovechada por una amenaza producto de un defecto o mala configuración.

4 Organización del documento Política de Seguridad de la Información

Siguiendo los lineamientos de la política modelo establecida por la ONTI y los dominios definidos en la norma ISO/IEC 27002:2013, se establecen catorce cláusulas 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 las Comunicación
- Política de Adquisición, Desarrollo y Mantenimiento de Sistemas
- Política en Relación a los Proveedores
- Política de Gestión de Incidentes de Seguridad
- Política de Gestión de la Continuidad
- Política de Cumplimiento

5 Gestión de Políticas y Normativas de Seguridad

Objetivo

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

Proporcionar a la Dirección Superior la dirección y soporte para la seguridad de la información en concordancia con los requerimientos y las leyes y regulaciones relevantes. La gerencia debe establecer claramente la dirección de la política en línea con los objetivos.

5.1 Políticas y Normativas de Seguridad

5.1.1 Política de Seguridad de la Información

La presente Política de Seguridad de la Información, una vez aprobada por la máxima autoridad del INDEC, será publicada y comunicada a todos los agentes del organismo y terceras partes relevantes, entrando en vigencia a partir del día siguiente de su publicación oficial.

5.1.2 Políticas y Normativas Complementarias

Deberá existir una “Política de Uso Aceptable de los Recursos de Tecnología de la Información” (PUA), que establecerán las normas de conducta razonable, que deben observar los agentes y funcionarios del Organismo cuando utilicen los recursos informáticos puestos a su disposición, con la finalidad de minimizar todos aquellos riesgos producto del mal uso de los mismos. De la misma manera, podrán existir otra serie de políticas y normativas más detalladas, aplicables en áreas específicas.

Por ello se establecerán las siguientes jerarquías respecto a la documentación de seguridad, a fin de garantizar que los objetivos y medidas establecidos en la presente política de seguridad cuente con un orden establecido:

- **Primer** nivel: Política de Seguridad de la Información.
- **Segundo** nivel: Política de Uso Aceptable de los Recursos de Tecnología de la Información y otras políticas y normativas.
- **Tercer** nivel: Documentación de buenas prácticas, recomendaciones y guías de apoyo referidos a aspectos de seguridad de la información.
- **Cuarto** nivel: Procedimientos de seguridad

5.1.3 Revisión de Políticas

La Política de Seguridad de la Información y la Política de Uso Aceptable de los Recursos de Tecnología de la Información, deberán ser revisadas regularmente cada dos años o cuando

ocurran cambios significativos referidos a las políticas adoptadas y deben ser aprobadas por el Comité de Seguridad de la Información.

La Política de Seguridad de la Información y la Política de Uso Aceptable de los Recursos de Tecnología de la Información deben poseer un dueño, responsable de las actividades de desarrollo, evaluación y revisión de la política.

La actividad de revisión debe incluir las oportunidades de mejoras, en respuesta a los cambios, entre otros, organizacionales, normativos, legales, de terceros o tecnológicos.

6 Política Organizativa

Objetivos

Administrar la seguridad de la información dentro del Organismo y establecer un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades.

Fomentar la consulta y cooperación con Organismos especializados para la obtención de asesoría en materia de seguridad de la información.

Garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información del Organismo.

6.1 Organización Interna

6.1.1 Compromiso de la Dirección del Organismo

La Dirección del Organismo apoyará la seguridad de la información a través de una orientación clara, mostrando compromiso, asignando roles y reconociendo responsabilidades explícitas.

Deberá revisar y aprobar la política de seguridad de la información, como asimismo revisar los beneficios de la implementación de la misma, que fuera elevada previamente por el Comité de Seguridad de la Información.

La seguridad de la información es una responsabilidad del Organismo compartida por todas las Autoridades políticas y Directores Nacionales o Generales, Gerentes o equivalentes, por lo cual se crea el “Comité de Seguridad de la Información”, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad de la información. El mismo contará con un Coordinador, quien cumplirá la función de impulsar la implementación de la presente Política.

Se conformará el Comité de Seguridad de la Información, integrado por los responsables de las siguientes áreas sustantivas:

- Dirección de Gestión
- Dirección Técnica
- Dirección General de Administración y Operaciones
- Dirección de Asuntos Jurídicos
- Dirección de Informática

El mismo deberá contar con un coordinador, quien presentará la evolución de los planes, programas y objetivos de seguridad al Comité para su aprobación y apoyo, cumpliendo tal función el responsable de la Dirección de Informática del Organismo.

El Comité de Seguridad de la Información tendrá entre sus funciones:

a) Revisar y proponer a la máxima autoridad del INDEC para su aprobación, la Política y las funciones generales en materia de Seguridad de la Información.

Av. Julio A. Roca 609, C1067ABB
Ciudad Autónoma de Buenos Aires, Argentina
Horario de atención de 9:30 a 16:00
ces@indec.gob.ar
Tel.: (54-11) 5031-4632
www indec.gob.ar
INDECArgentina

b) Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.

c) Tomar conocimiento y supervisar la investigación y monitoreo de aquellos incidentes relevantes relativos a la seguridad.

d) Evaluar y aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo con las competencias y responsabilidades asignadas a cada área.

e) Acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información.

f) Garantizar que la seguridad sea parte del proceso de planificación informática del Organismo.

g) Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios

h) Promover la difusión y concientización de la seguridad de la información dentro del Organismo.

i) Promover el apoyo y cooperación de los Directores Nacionales, Generales y Coordinadores en toda implementación referida a la seguridad de la información.

j) Coordinar el proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de la información del Organismo frente a interrupciones imprevistas.

6.1.2 Coordinación de Seguridad Informática

Se designará las funciones relativas de seguridad de la información a la “Coordinación de Seguridad Informática”, la cual tendrá a cargo las funciones relativas a la seguridad de los sistemas de información del Organismo y procesos asociados, incluyendo la supervisión de todos los aspectos inherentes a la seguridad tratados en la presente política.

La Coordinación de Seguridad Informática, será responsable de:

Asegurar que las actividades de seguridad sean ejecutadas en conformidad con la Política de Seguridad de la Información.

a) Identificar cómo manejar las no-conformidades.

b) Aprobar las metodologías y procesos para la seguridad de la información; por ejemplo, la evaluación del riesgo y la clasificación de la información.

c) Identificar cambios significativos en las amenazas y la exposición de la información y los medios de procesamiento de la información ante amenazas.

d) Promover de manera eficiente la capacitación y concientización de la seguridad de la información en el Organismo.

e) Evaluar la información recibida del monitoreo y revisar los incidentes de seguridad de la información, y recomendar las acciones apropiadas en respuesta a los incidentes de seguridad de información identificados.

f) Implementar un Sistema de Gestión de Seguridad de la Información (SGSI).

g) Identificar, evaluar y proponer el tratamiento de los riesgos y amenazas a los que se expone la información y los recursos tecnológicos del Organismo.

h) Controlar el acceso a los recursos de tecnológicos.

i) Detectar, analizar, remediar y recolectar evidencia forense de incidentes de seguridad, ante actuaciones que ameriten intervención administrativa o judicial.

6.1.3 Asignación de Responsabilidades de la Seguridad de la Información

Se asignarán responsabilidades en los procesos de seguridad indicados en el presente cuadro:

Proceso de seguridad	Responsable
Apoyo e impulso de la implementación de la Política de Seguridad de la Información	Comité de Seguridad de la Información
Gestión de Incidentes de Seguridad	Coordinación de Seguridad Informática
Seguridad Electrónica	Coordinación de Seguridad Informática (REVISAR)
Seguridad en las Comunicaciones	Coordinación de Seguridad Informática
Seguridad en el SDLC de Sistemas	Dirección de Informática
Planificación de la Continuidad Operativa	Dirección de Informática/Director Técnico/Directo de planificación
Seguridad en la provisión de suministro eléctrico	Coordinación Técnica
Seguridad Ambiental	Coordinación Técnica
Cumplimiento Legal y Normativo	Dirección de Asuntos Jurídicos
Auditorías Internas	Área de Auditoría Interna
Seguridad Física	Recursos Humano o Área de Técnica
Difusión y Cumplimiento	Directores, Coordinadores y empleados
Seguridad de las Personas	Técnica y recursos humanos

6.1.4 Propietarios de la Información

Se designarán propietarios de la información que se procesa y almacena en el Organismo, los cuales deberían ser generalmente los responsables de las Direcciones o Coordinaciones que utilizan dicha información.

Si bien los propietarios de la información podrán delegar la administración de sus funciones a personal idóneo, seguirán conservando la responsabilidad sobre la misma.

La asignación de la responsabilidad de la información deberá ser formalmente documentada y proporcionada a la Coordinación de Seguridad Informática, debiendo registrarse descripción de la información, propietario, procesos involucrados, área, recursos asociados, responsable técnico y cualquier otra información que sea relevante.

6.1.5 Autorización de Equipamiento para Procesamiento de Información

Los nuevos recursos de procesamiento de información deberán ser autorizados por la Dirección de Informática en conjunto con la Coordinación de Seguridad Informática, a fin de garantizar que se cumplan todas las Políticas y requerimientos de seguridad existentes.

El uso de recursos personales de procesamiento de información en el lugar de trabajo puede ocasionar nuevas vulnerabilidades. En consecuencia, su uso será evaluado y autorizado por la Dirección de Informática en conjunto con la Coordinación de Seguridad Informática, siguiendo las directrices del punto 6.2.2 Dispositivos Móviles Personales.

6.1.6 Acuerdo de confidencialidad

Se definirá, implementará y revisará regularmente los acuerdos de confidencialidad o de no divulgación para asegurar la protección de la información del Organismo que deberá ser firmado por la totalidad del personal del organismo, cualquiera sea su situación de revista como también por terceros que tengan relaciones contractuales con el organismo.

Mediante este instrumento el empleado se comprometerá a utilizar la información solamente para el uso específico al que se ha destinado y a no comunicar, diseminar o de alguna otra forma hacer pública la información a ninguna persona, firma, compañía o tercera persona, salvo autorización previa y escrita del Responsable del Activo de que se trate.

Dicho acuerdo debe responder a los requerimientos de confidencialidad o no divulgación, asimismo, deben cumplir con toda legislación o normativa que alcance al Organismo en materia de confidencialidad de la información.

6.1.7 Contacto con otros organismos

A efectos de intercambiar experiencias, obtener asesoramiento o capacitación para el mejoramiento de las prácticas y controles de seguridad, se mantendrán contactos con otros organismos especializados en temas relativos a la seguridad informática.

El intercambio de información confidencial para fines de asesoramiento o de transmisión de experiencias, sólo se permitirá cuando se haya firmado previamente un Acuerdo de Confidencialidad con aquellas organizaciones públicas y privadas especializadas en temas relativos a la seguridad de la Información.

Av. Julio A. Roca 609, C1067ABB
Ciudad Autónoma de Buenos Aires, Argentina
Horario de atención de 9:30 a 16:00
ces@indec.gob.ar
Tel.: (54-11) 5031-4632
www indec.gob.ar
INDECArgentina

6.1.8 Contacto con grupos especializados en seguridad informática

La Coordinación de Seguridad Informática coordinará los conocimientos y las experiencias disponibles en el Organismo en materia de seguridad de la información, promoviendo su capacitación continua.

Para ello promoverá la asistencia y contacto con eventos, grupos, foros o asociaciones especializados de seguridad informática, con el fin de actualizar los conocimientos en materia de seguridad de la información del área, como también poder recibir alertas tempranas, avisos y recomendaciones ante la aparición de nuevas vulnerabilidades o formas de violar la seguridad implementada.

6.1.9 Seguridad de la información en la gestión de proyectos

Se deberá contemplar a la Coordinación de Seguridad Informática en la gestión de proyectos, a efectos de garantizar que se reflejen adecuadamente las disposiciones de la Política de Seguridad de la Información en los mismos.

6.1.10 Segregación de Funciones

Se deberá diseñar el esquema de roles, segregando funciones y áreas de responsabilidades para evitar el conflicto de intereses con el objeto de reducir modificaciones no autorizadas o el mal uso de la información o servicios.

6.2 Dispositivos Móviles y Trabajo Remoto

6.2.1 Dispositivos Móviles del Organismo

Todo dispositivo móvil perteneciente al Organismo (laptop, notebooks, netbooks tabletas, teléfonos celulares, etc.), que pudiera contener información del Organismo, deberá cumplir con medidas seguridad adecuadas para proteger el dispositivo móvil y la información que contiene, contra todos los riesgos derivados del uso del mismo.

Por lo cual se deberán desarrollar procedimientos para asegurar al dispositivo móvil y la información contenida, debiendo tener en cuenta los siguientes conceptos:

a) Protección contra software malicioso del dispositivo móvil.

b) Cifrado de la información en el dispositivo móvil.

c) Mecanismos de borrado seguro de la información en caso de robo o pérdida.

d) Cifrado de las comunicaciones para acceder a los servicios del Organismo.

e) Control de acceso a los recursos a los que accede el dispositivo móvil.

f) Aplicación de las mismas políticas de seguridad que a los equipos no móviles del Organismo.

La utilización de dispositivos móviles en la vía pública, incrementa la probabilidad de ocurrencia de incidentes de pérdida, robo o hurto. En consecuencia, deberá comunicarse al personal que los utilice, sobre los cuidados especiales a observar ante el uso de los mismos, que contemplarán las siguientes recomendaciones:

a) Permanecer cerca del dispositivo, no dejando al mismo desatendido.

b) No llamar la atención acerca de portar un equipo móvil.

c) No poner identificaciones referidas al Organismo en el dispositivo móvil, salvo los estrictamente necesarios.

d) Colocar un teléfono de contacto sin identificación para su recupero.

e) Mantener cifrada la información del dispositivo móvil.

Se confeccionará un procedimiento que permita al poseedor del dispositivo reportar rápidamente cualquier incidente sufrido y de esta manera mitigar los riesgos a los que eventualmente estuviera expuesto el Organismo ante la ocurrencia del incidente, los que incluirán:

a) Revocación de las credenciales afectadas

b) Notificación a la Coordinación de Seguridad Informática.

c) Notificación a los grupos de trabajo donde potencialmente podría haber comprometido dicho incidente.

6.2.2 Dispositivos Móviles Personales

Cuando sea necesario la utilización de equipamiento personal, en las instalaciones del Organismo, este deberá ser evaluado y autorizado por la Coordinación de Seguridad Informática en conjunto con la Dirección de Informática.

Todo dispositivo móvil no perteneciente al Organismo (laptop, notebooks, netbooks tabletas, etc.) deberá cumplir con las medidas de seguridad adecuadas con el fin de proteger los recursos informáticos a los cuales accede. Se deberá desarrollar procedimientos para estos dispositivos, que abarquen los siguientes conceptos:

a) Protección contra software malicioso del dispositivo móvil.

b) Cifrado de las comunicaciones para acceder a los servicios del Organismo.

c) Control de acceso a los recursos a los que se accede desde el dispositivo móvil.

d) Concientización del usuario de las restricciones a las cuales debe adecuarse para que el dispositivo móvil pueda conectarse a los recursos informáticos del Organismo.

e) Auditorías y monitoreo de las actividades efectuadas.

f) Registro de las personas que usan dispositivos no pertenecientes al Organismo.

6.2.3 Trabajo a Distancia

El trabajo a distancia deberá ser autorizado y solicitado por la dirección a la cual pertenezca el usuario, el Coordinador de Seguridad Informática evaluará tal solicitud en conjunto con la Dirección de Informática y solo serán contempladas situaciones que justifiquen la imposibilidad de otra forma de acceso o ante urgencias acaecidas.

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

Los controles y disposiciones comprenden:

a) Asegurar el cifrado de las comunicaciones

b) Concientizar sobre la amenaza de acceso no autorizado a la información o recursos por parte de otras personas que utilizan el espacio de trabajo remoto, por ejemplo, familiar o amigo.

c) Proveer de mobiliario para almacenamiento y equipamiento adecuado para las actividades de trabajo remoto cuando sea necesario

d) Definir el trabajo permitido, el horario de trabajo, la clasificación de la información que se puede almacenar en el equipo remoto desde el cual se accede a la red del Organismo y los sistemas internos y servicio a los cuales el trabajador remoto solo estará autorizado a acceder.

e) Definir reglas y orientación respecto del acceso de terceros al equipamiento e información.

f) Proveer el hardware y el soporte y mantenimiento del software, cuando sea necesario.

g) Efectuar auditorías y monitoreo de las actividades efectuadas remotamente.

h) Realizar la anulación de las autorizaciones, derechos de acceso y devolución del equipo cuando finalicen las actividades remotas.

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

j) Se deberán implementar regularmente procesos de auditoría específicos para los casos de accesos remotos. Se deberá llevar un registro de incidentes a fin de corregir eventuales fallas en la seguridad de este tipo de accesos.

7 Política de Recursos Humanos

Objetivos

Reducir los riesgos de error humano, comisión de ilícitos, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.

Explicitar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos de confidencialidad a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado.

Garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para respaldar la Política de Seguridad del Organismo en el transcurso de sus tareas normales.

Establecer Compromisos de Confidencialidad con todo el personal y usuarios externos de las instalaciones de procesamiento de información.

Establecer las herramientas y mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia.

7.1 Antes del empleo

7.1.1 Funciones y Responsabilidades del Puesto de Trabajo

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

Además, se incluirán las responsabilidades generales relacionadas con la implementación de la Política de Seguridad de la Información, la Política de Uso Aceptable de los Recursos de Tecnología de la Información y las responsabilidades específicas vinculadas a la protección de cada uno de los activos o la ejecución de procesos o actividades a realizar en los puestos de trabajo.

Deberán definirse y comunicarse claramente los roles y responsabilidades de seguridad a los candidatos para el puesto de trabajo durante el proceso de preselección.

7.1.2 Revisión de Antecedentes

Se deberán realizar revisiones de antecedentes referidos a currículum, referencias, títulos académicos, etc., de los postulantes al empleo, en concordancia con el puesto y activos a los cuales tendrá acceso. Teniendo en consideración las regulaciones vigentes, ética y leyes relevantes.

Av. Julio A. Roca 609, C1067ABB
Ciudad Autónoma de Buenos Aires, Argentina
Horario de atención de 9:30 a 16:00
ces@indec.gob.ar
Tel.: (54-11) 5031-4632
www indec.gob.ar
INDECArgentina

7.2 Inicio del empleo

7.2.1 Aceptación de Términos y Condiciones de Contratación

Los nuevos empleados, deberán aceptar firmar los documentos “Acuerdo de Confidencialidad” y “Política de Uso Aceptable de los Recursos de Tecnología de la Información”, por lo cual el empleado declarará conocer y aceptar el control y monitoreo del uso de los recursos tecnológicos que utilizará en el desempeño de sus tareas.

Las copias firmadas deberán ser retenidas en forma segura por la Dirección de Recursos Humanos.

7.3 Durante el empleo

7.3.1 Responsabilidad de la Dirección

Las direcciones en todos los niveles impulsarán que se aplique la política de seguridad de la información en concordancia con las pautas y procedimientos establecidos, por lo que deberán también informar de su existencia y las expectativas de cumplimiento en el desempeño de sus funciones.

7.3.2 Concientización, formación y capacitación en seguridad de la información

Se deberán realizar tareas de capacitación y concientización de las políticas, normativas y procedimientos dirigidos a todos los empleados del Organismo. Dicha capacitación comprenderá requerimientos de seguridad, responsabilidades legales, uso correcto de los dispositivos tecnológicos asignados y el uso correcto de los recursos en general.

7.3.3 Procedimiento disciplinario

El Organismo podrá iniciar un procedimiento administrativo disciplinario, con el objeto de sancionar administrativamente, según las normativas estatutarias, escalafonarias y convencionales que rigen al personal de la Administración Pública Nacional, a todos aquellos empleados, sea cual fuere su situación de revista, que violen las Políticas, Normas y Procedimientos de Seguridad.

Las sanciones podrán imponerse mediante un acto administrativo que así lo disponga cumpliendo las formalidades impuestas por los preceptos constitucionales de la Ley de Procedimiento Administrativo N° 19.549 y demás normativas específicas aplicables.

Los empleados del Organismo, sea cual fuere su nivel escalafonario y su situación de revista, que incumpliera sus obligaciones incurrirán también en responsabilidad civil o patrimonial, si ocasionan daños (cuando ocasione un daño que deba ser indemnizado). Como así también, en responsabilidad penal cuando su conducta se encuentre tipificada y constituya un comportamiento considerado delito por la Ley 26.388 de Delitos Informáticos, Ley 17.622 de Estadística y Censos y demás leyes especiales, siendo la Dirección de Asuntos Jurídicos quien asesorará sobre las

sanciones a ser aplicadas por el incumplimiento de dichas Políticas, Normas y Procedimientos de seguridad.

7.4 Cese del empleo o Cambio de puesto de trabajo

7.4.1 Responsabilidad del Cese o Cambio

Se deberán definir procedimientos y asignar responsabilidades para controlar que los procesos de cambio de función y desvinculación laboral de los empleados, contratistas o terceras personas no afecte el normal desempeño de las actividades del Organismo.

7.4.2 Transferencia de Conocimientos

Todos los empleados, contratistas y usuarios que tengan conocimiento relevante de ciertas operaciones y dicho conocimiento sea desconocido por el personal restante del área donde prestan servicios, deberán documentar dicha información y transferirla al Organismo antes de proceder a su desvinculación.

8 Política de Gestión de Activos

Objetivos

Garantizar que los activos de información reciban un apropiado nivel de protección.

Clasificar la información para señalar su sensibilidad y criticidad.

Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

8.1 Responsabilidad sobre los Activos

8.1.1 Inventario de activos

Se deberá mantener un inventario de activos preciso y actualizado, debiendo ser revisado con una periodicidad no mayor de tres meses, cada activo deberá poseer un propietario asignado.

Para cada uno de los activos identificados, se deberá asignar un propietario.

Todos los activos deberán estar claramente identificados y tipificados según sea:

a) Información: bases de datos, archivos de datos, documentación, contratos, acuerdos.

b) Activos de software: software de aplicaciones, software de sistemas, herramientas de desarrollo, y utilitarios.

c) Activos físicos: equipamiento de computación, equipamiento de comunicaciones, medios removibles y otros equipamientos.

d) Instalaciones: tendido eléctrico, red de agua y gas, etc.

e) Servicios: servicios de cómputo y de comunicaciones, servicios generales, por ejemplo: calefacción, iluminación, energía, y aire acondicionado.

f) Personas, y sus calificaciones, habilidades y experiencia.

g) Activos intangibles, tales como la reputación y la imagen del Organismo.

8.1.2 Propietarios de Activos

Deberá designarse propietarios de los activos registrados, quienes deberán:

a) Informar sobre cualquier cambio que afecte el activo del cual es propietario.

b) Clasificar los activos en función a su sensibilidad y criticidad.

c) Velar por la implementación de controles de seguridad requeridos para proteger los activos.

Los propietarios serán responsables de los activos asignados.

La implementación de los controles de seguridad podrá ser delegada a personal especializado, como también la gestión técnica u operativa, pero el propietario seguirá siendo responsable por los mismos.

8.1.3 Uso Aceptable de Activos de Tecnología

Se identificarán, documentarán y definirán normativas generales para el uso de los activos de tecnología, en el documento “Política de Uso Aceptable de los Recursos de Tecnología de la Información”.

Todos los empleados, sin importar su situación de revista, contratistas y usuarios de terceras partes deberán seguir las reglas establecidas para el uso aceptable de los activos de tecnología de la información.

Toda excepción a la normativa deberá ser autorizada por el máximo responsable del área que solicita la excepción al cumplimiento de dicha normativa.

8.1.4 Devolución de Activos

Todos los empleados, contratistas y usuarios de terceras partes deberán devolver todos los activos (equipamiento tecnológico, software, documentos, tarjetas de ingreso, etc.) que les fueron asignados, inmediatamente en la terminación de su empleo, contrato o acuerdo. Por tal razón deberá existir un Procedimiento de Repliegue de Bienes, como también un Procedimiento de Devolución de Dispositivos Digitales Portátiles, para el adecuado cumplimiento de esta tarea.

8.2 Política de Clasificación de la Información

8.2.1 Directrices de Clasificación de la Información

Se deberán definir procedimientos de clasificación y etiquetado, para determinar la criticidad de la información que se administra en el Organismo, en base a las tres características de seguridad de la información, confidencialidad, integridad y disponibilidad.

8.2.2 Etiquetado y Manipulado de Activos de Información

Se deberá definir procedimientos de etiquetado y de manejo de los activos de información, de acuerdo al esquema de clasificación establecido y criticidad de la información. Los mismos contemplarán los recursos de información tanto en formatos físicos como electrónicos e incorporarán las actividades de procesamiento de la información referidos a copias, almacenamiento, transmisión por correo electrónico, telefonía o transmisiones de datos a través de sistemas de intercambio de archivos.

Para cada uno de los niveles de clasificación, se deben definir los procedimientos de manejo seguros, incluyendo las actividades de procesamiento, almacenaje, transmisión, desclasificación y destrucción.

8.3 Gestión de Soportes de Almacenamiento

8.3.1 Soportes Removibles

Se deberán implementar procedimientos para la gestión de los soportes informáticos extraíbles. Debiendo considerarse aspectos tales como la autorización y registro del retiro de soportes de almacenamiento removibles fuera de los edificios del Organismo.

Se deberán almacenar los soportes de medio extraíbles (cintas magnéticas, discos externos, etc.) en un ambiente seguro y protegido, teniendo en cuenta la criticidad de la información contenida y las especificaciones de los fabricantes o proveedores del soporte de almacenamiento.

8.3.2 Eliminación Segura de Soportes de Información

Se deberán implementar procedimientos para el borrado seguro de la información al declararse la baja el soporte de almacenamiento que lo contiene, como también procedimientos de borrado seguro para las operaciones de reciclado de los dispositivos de almacenamiento, teniendo en cuenta que el mecanismo de eliminación debe contemplar el tipo de dispositivo y la criticidad de la información contenida.

Los procedimientos de eliminación segura deberán considerar elementos de soporte de información, tales como papeles, cintas magnéticas (datos, audio y video), discos magnéticos, dispositivos de almacenamientos ópticos, unidades extraíbles de estado sólido y cualquier otra tecnología o soporte de almacenamiento de datos.

Los medios de almacenamiento, que deseen reutilizarse, pero no puedan serlo, deberán ser destruidos físicamente de manera apropiada, para que la información contenida, no pueda ser recuperada utilizando técnicas forenses.

8.3.3 Tránsito de Soportes de Almacenamiento

Se deberá proteger la información y los soportes de almacenamiento en tránsito, conforme a la sensibilidad y criticidad de la información a transportar. Razón por la cual se deben definir procedimientos de transporte de soportes de almacenamiento, teniendo en cuenta el cifrado de la información contenida en el soporte, utilización de servicios de mensajería confiables, la adopción de embalajes sellados, entrega en mano, o cualquier otro mecanismo para asegurar el soporte de almacenamiento durante el tránsito del mismo.

9 Política de Control de Accesos

Objetivos

Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información. Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.

Controlar la seguridad en la conexión entre la red del Organismo y otras redes públicas o privadas.

Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.

Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.

Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.

9.1 Requerimientos para el Control de Accesos

9.1.1 Política de Gestión de Accesos

Se controlará el acceso a la información y a los recursos tecnológicos del Organismo.

Se definirán procedimientos que tengan en cuenta aspectos tales como:

a) Segregación de las funciones referidas a quien solicita, quien autoriza y quien concede operativamente el acceso.

b) Identificación del propietario de la información, del usuario que requiere el acceso y la aplicación a la cual se desea acceder.

c) Identificación de los requerimientos de seguridad de las aplicaciones y toda información relevante de seguridad, relacionada a las mismas.

d) Existencia de criterios políticas de acceso coherentes con el punto 8.2 Política de Clasificación de la Información.

e) Definición de perfiles de acceso de usuarios en las aplicaciones.

f) Tipos de accesos, informando si son internos o externos, públicos o privados.

g) Requerimientos de revisión periódica de los accesos concedidos.

h) Revocación de los derechos de acceso

i) Administración de cuentas de usuarios y permisos de acceso de los mismos a los sistemas y dispositivos de red del Organismo.

9.1.2 Control de Acceso a las Redes

Se establecerán todas las reglas de acceso, sobre la premisa “Todo acceso a la información y recursos tecnológicos está prohibido, a menos que se permita explícitamente”. Siendo todas las reglas de carácter obligatorio salvo expresamente que se indique lo contrario.

Los usuarios tendrán acceso solo a la red y a los servicios de red que hubieran sido específicamente autorizados.

9.2 Gestión de Acceso de Usuarios

9.2.1 Creación y Eliminación de Cuentas de usuario

Cada usuario deberá tener un identificador unívoco denominado “cuenta de usuario”, el cual será de uso personal y exclusivo, cuyo fin será garantizar la trazabilidad de las operaciones efectuadas por él.

Se deberán definir procedimientos que permitan crear y eliminar cuentas de usuarios, con el fin de otorgar y revocar el acceso a los sistemas, bases de datos y servicios de información, dichos procedimientos deberán:

a) Utilizar nombre de cuentas de usuario identificables, de manera tal, que se pueda determinar inequívocamente las actividades realizadas por dichas cuentas, ya sean cuentas de usuario o cuentas de servicio.

b) Evitar que existan múltiples cuentas de usuario asociadas solo a un individuo, salvo excepciones por cuestiones de seguridad, según se indica en el punto 9.2.3 Gestión de Asignación de Permisos de Acceso con Privilegios Especiales.

c) Evitar la creación y uso de cuentas de usuario genéricas, compartida para un grupo de usuarios o una tarea específica. Esto, será permitido únicamente por razones operativas, debiendo requerir un profundo análisis y autorización de la Coordinación de Seguridad Informática antes de su creación.

d) Los nombres de cuenta de usuario no deberán dar indicios del nivel de privilegios de la misma.

e) Garantizar que los proveedores de servicios no otorguen acceso hasta que se hayan completado los procedimientos de autorización.

f) Mantener un registro formal de todas las personas registradas para utilizar el servicio

g) Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron de funciones, de áreas de pertenencia o se desvincularon del Organismo.

h) Incluir cláusulas en los contratos de personal y de servicios que se especifiquen sanciones si el personal o los agentes que prestan un servicio intentan accesos no autorizados en caso de corresponder, según lo dispuesto en el punto 7.3.3 Proceso disciplinario.

i) Efectuar revisiones periódicas con el objeto de:

- Inhabilitar cuentas de usuarios inactivas por más de tres meses.

- Inhabilitar cuentas de usuarios desvinculados del Organismo
- Eliminar cuentas de usuarios inactivas por más de dos años.
- Eliminar las cuentas de usuarios redundantes o no identificables previo análisis de sus actividades

j) garantizar que los identificadores de usuario redundantes no se asignen a otros usuarios.

En el caso de existir excepciones para evitar inhabilitar o eliminar cuentas de usuario, estas deberán ser debidamente justificadas y aprobadas por la Coordinación de Seguridad Informática.

9.2.2 Gestión de Asignación de Permisos de Acceso

Se controlará la asignación y uso de privilegios a todas las cuentas de todos los sistemas y servicios.

Los Propietarios de Información serán los encargados de aprobar la asignación de los permisos de acceso y solicitar su implementación, que también deberá ser autorizada por la Coordinación de Seguridad Informática.

El proceso de autorización deberá tener en cuenta los siguientes aspectos:

a) Se deberá aplicar el principio de priorización de asignación de menores privilegios.

b) Identificar los niveles de acceso existentes en los sistemas, bases de datos y aplicaciones.

c) Verificar que el nivel de acceso a otorgar sea adecuado al rol del usuario y que no comprometa la segregación de funciones.

d) Establecer un proceso de autorización que registren todos los derechos de acceso asignados.

e) Priorizar que los permisos de acceso se apliquen a Roles en los sistemas, antes de aplicarlos directamente a los usuarios.

9.2.3 Gestión de Asignación de Permisos de Acceso con Privilegios Especiales

La asignación y uso de derechos de acceso con privilegios especiales, deberá seguir la misma política de permisos de acceso definida previamente, pero además se deberá considerar los siguientes aspectos:

a) No deberán utilizarse cuentas de usuarios con derechos de acceso privilegiados para realizar actividades regulares, sino que sólo serán utilizadas ante la necesidad de realizar tareas específicas que lo requieran. Solo deberán ser utilizadas ante necesidades específicas para realizar tareas de contingencia, recupero o reconfiguración que lo requieran.

b) Por lo que un usuario con privilegios especiales debería poseer dos cuentas de usuario, una para sus tareas habituales y otra para realizar estrictamente actividades que requieran permisos especiales.

c) Solo deberán asignarse en caso de necesidad de uso, basado en los requisitos mínimos necesarios para realizar las tareas y estar debidamente documentada

d) Se deberán revisar periódicamente la actividad de los usuarios con derechos de accesos privilegiados, para verificar que solo sean utilizados para las actividades que dieron motivo a su asignación.

9.2.4 Distribución de Contraseñas y de Dispositivos de Acceso

Se deberán establecer procedimientos para la distribución segura de contraseñas o de cualquier otro tipo de dispositivos o mecanismos de autenticación.

Por lo que cual no se deberá enviar por correo electrónico la credencial compuesta por usuario y contraseña en texto plano.

9.2.5 Revisión de Derechos de Acceso de los Usuarios

A fin de mantener un control eficiente del acceso a los datos y servicios de información, la Coordinación de Seguridad Informática, podrá llevar a cabo, procesos formales de revisión de todos los accesos.

Se deberán revisar periódicamente, los derechos de acceso y privilegios asignados a los usuarios, a fin de verificar que los mismas hayan sido autorizadas debidamente.

9.2.6 Revocación y Cambios de Derechos de Acceso

Se deberán implementar procedimientos formales para la de revocación y cambios de derechos de acceso de los usuarios en todos los sistemas y servicios.

Tras la desvinculación del usuario, se deberán eliminar los derechos de acceso a todos los sistemas y servicios de información utilizados por el individuo. Verificando previamente que se pudiera seguir accediendo con otras credenciales activas al sistema o servicio referido.

Ante un cambio de función, se deberán remover todos los derechos de acceso que no fueron aprobados para la nueva función, comprendiendo todos los derechos de accesos lógicos y físicos, como ser llaves, tarjetas de identificación y accesos a instalaciones de procesamiento de la información.

Se deberán cambiar las contraseñas de acceso que pudieran conocer el empleado, contratista o usuario de tercera parte, tras la finalización de su contrato o ante un cambio de función, cuando dicha contraseña formara parte de una credencial de acceso de administración aún activa.

9.3 Responsabilidades del Usuario

9.3.1 Responsabilidad en el uso de las Contraseñas

Los usuarios deberán seguir las buenas prácticas de seguridad referidas al uso de contraseñas en concordancia con la política 9.4.4 Gestión de Contraseñas de Usuarios.

Debiendo cumplir con las siguientes premisas:

a) Mantener las contraseñas en secreto, los usuarios deberán mantener la confidencialidad de las mismas, ya que las contraseñas son consideradas información personal, no debiendo ser compartidas, ni aún con su personal jerárquico.

b) Cuando existiera indicio de que la confidencialidad de la contraseña hubiera sido comprometida, deberá informarlo y solicitar el cambio de la misma, inmediatamente.

c) Seleccionar contraseñas que no estén basadas en datos que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, como ser nombres, números de teléfono, número de oficina, fechas de cumpleaños, etc.

d) No reutilizar o reciclar viejas contraseñas.

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

f) Evitar almacenar contraseñas en papel, archivos de texto, planillas de cálculo o cualquier aplicación cuya función no sea expresamente el almacenamiento seguro de contraseñas.

g) Evitar el uso de gestores de contraseñas que almacenan las contraseñas en Internet.

9.4 Control de Acceso a Sistemas y Aplicaciones

9.4.1 Política de Utilización de los Servicios de Red

Se restringirá y controlará el acceso a los servicios de red tanto internos como externos, en concordancia con el punto 9.2 Gestión de Acceso de Usuarios, para garantizar que los usuarios que accedan a las redes y a sus servicios no comprometan las seguridad de los mismos.

La Coordinación de Seguridad Informática autorizará el acceso a los recursos de red, servicios e información, únicamente mediante un pedido formal del titular de la Dirección propietaria de la información a la cual se pretende acceder.

Se deberán desarrollar procedimientos para conceder o derogar derechos de acceso a la información, identificando las redes y servicios a los cuales se concedió el acceso, teniendo en cuenta los puntos 9.2.2 Gestión de Asignación de Permisos de Acceso y 9.2.3 Gestión de Asignación de Permisos de Acceso con Privilegios Especiales.

9.4.2 Procedimientos Seguros de Inicio de Sesión

El acceso a los servicios de información deberá ser posible, solo a través de un proceso de inicio de sesión segura, no deberá divulgar ningún indicio que provea asistencia a usuarios no autorizados.

En el proceso de inicio seguro deberá:

a) Desplegar un aviso informativo, advirtiendo que sólo los usuarios autorizados pueden iniciar sesión en el equipo informático.

b) Evitar mostrar mensajes de ayuda que pudieran asistir al usuario durante el procedimiento de conexión, que diera indicio del dato erróneo (usuario o contraseña) ante una autenticación incorrecta.

c) Validar la información de la conexión sólo al completarse la totalidad de los datos de entrada. Si surge una condición de error, el sistema no debe indicar que parte de los datos es correcta o incorrecta.

d) Ser condición obligatoria de los usuarios, firmar la “Política de Uso Aceptable de los Recursos de Tecnología de la Información” antes de acceder a los recursos tecnológicos del Organismo, consintiendo mediante esta firma su conocimiento y aceptación.

e) Evitar configurar el equipo informático con credenciales almacenadas que provoquen el inicio de sesión de forma automática.

f) Registrar todas las conexiones exitosas y los intentos de conexión fallidas.

g) Evitar implementaciones que transmitan las contraseñas en texto plano sobre la red de datos.

h) Implementar medidas para la protección ante ataques de fuerza bruta, como ser:

- Bloqueo de la cuenta del usuario, inmediatamente luego de cierto número de reintentos fallidos. Por ejemplo, bloqueo de la cuenta del usuario luego de 5 (cinco) reintentos fallidos.
- Desbloqueo automático de la cuenta luego de cierto tiempo de haberse bloqueado. Por ejemplo, desbloqueo de la cuenta del usuario luego de 10 (diez) minutos de haberse bloqueado

9.4.3 Autentificación de Usuarios para Conexiones Externas

Las conexiones externas representan un gran riesgo a la infraestructura tecnológica del Organismo. Por consiguiente, el acceso de usuarios remotos estará estrictamente limitado y sujeto al cumplimiento de procesos de aprobación, los cuales deberán requerir de la expresa autorización del director del área de pertenencia y de la Coordinación de Seguridad Informática.

Se deberá considerar la implementación de mecanismos de autenticación extras a la credencial de acceso (usuario y contraseña), es decir, el uso de más de un factor de autenticación, mediante métodos de autenticación física (tokens), tarjetas coordenadas, o bien cualquier otro mecanismo que refuerce la identificación de la conexión externa.

Cuando se utilicen mecanismos de autenticación físicos, deben implementarse procedimientos que incluyan, asignación de la herramienta de autenticación, registro de los poseedores de dichos autenticadores, mecanismo de rescate al momento de la desvinculación del personal al que se le otorgó y procedimiento de revocación de acceso del autenticador, en caso de compromiso de seguridad (pérdida o robo).

Las conexiones externas deberán estar cifradas, con algoritmos actualizados, pudiendo ser de dos tipos:

- Conexión cifrada por medio de una Red Privada Virtual (VPN) a la red del Organismo.
- Conexión cifrada al “Portal Web de Acceso Remoto”.

Se deberá asignar preferentemente conectividad al “Portal Web de Acceso Remoto”, salvo pedido expreso que deberá ser evaluado por la Coordinación de Seguridad Informática.

9.4.4 Gestión de Contraseñas de Usuarios

Se deberán implementar sistemas gestores de contraseñas que garanticen la confidencialidad y eficiencia en la administración de las mismas, en concordancia con la política 9.3.1 Responsabilidad en el uso de las Contraseñas y la política 9.2.4 Distribución de Contraseñas y de Dispositivos de Acceso.

Se deberá controlar la gestión de contraseñas mediante un proceso formal que deberá tener en consideración los siguientes aspectos:

a) Se deberán generar mecanismos que permitan a los usuarios cambiar las contraseñas asignadas inicialmente la primera vez que ingresan al sistema. Es decir que los usuarios estarán obligados a cambiar sus contraseñas recibidas inicialmente por parte de los administradores.

b) Cuando se requieran resguardar las contraseñas se deberán utilizar aplicaciones especialmente diseñadas para el almacenamiento seguro de contraseñas, teniendo en cuenta no utilizar aplicaciones que alojen su base de datos de contraseñas en repositorios de Internet.

c) Se establecerán como mínimo las siguientes características básicas de complejidad, longitud mínima de 8 (ocho) caracteres, compuesta por mayúsculas, minúsculas y caracteres numéricos en su conformación.

d) Se deberán configurar procesos que soliciten el cambio de la contraseña cada 1 (uno) año impidiendo la reutilización de las mismas.

e) No se deberán distribuir ni almacenar las contraseñas en texto plano.

f) Las contraseñas deberán almacenarse en sistemas diseñados para tal fin, denominados “gestores de contraseñas”.

g) Se deberán cambiar las contraseñas por defecto de los sistemas y dispositivos luego que hubiera finalizado su instalación inicial.

h) Se deberán cambiar las contraseñas de las cuentas utilizadas por los servicios de soporte externos a la planta del Organismo luego que la tarea de los mismos hubiera finalizado.

Av. Julio A. Roca 609, C1067ABB
Ciudad Autónoma de Buenos Aires, Argentina
Horario de atención de 9:30 a 16:00
ces@indec.gob.ar
Tel.: (54-11) 5031-4632
www indec.gob.ar
INDECArgentina

i) Se deberá implementar el cifrado mediante contraseña en operaciones de Copias de Resguardo y Restauración.

j) Para asegurar el adecuado uso las contraseñas, se deberán registrar y auditar las actividades relativas a la gestión de las mismas.

9.4.5 Gestión de Contraseñas Críticas

Las cuentas administrativas genéricas (administrador, root, admin, etc.) con privilegios especiales para efectuar actividades críticas serán resguardadas de manera especial y solo serán utilizadas ante necesidades específicas para realizar tareas de contingencia, recupero o reconfiguración que lo requieran.

La Coordinación de Seguridad Informática definirá el procedimiento para la administración de contraseñas críticas que contemplará los siguientes aspectos.

a) La conformación de la contraseña crítica deberá poseer un mayor nivel de complejidad que la definida en el punto previo 9.4.4 Gestión de Contraseñas de Usuarios

b) La definición de la misma será efectuada como mínimo por dos personas, de tal manera que ninguna de ellas conozca la contraseña completa.

c) Las partes de las contraseñas serán resguardadas físicamente, en sobres cerrados por duplicado.

d) La utilización de las contraseñas críticas será formalmente registrada, documentando las causas que determinaron su uso, usuario que hizo uso de la misma y las actividades que se realizaron con ella.

e) Las contraseñas críticas se renovarán una vez utilizada, procediendo luego a su resguardo nuevamente.

9.4.6 Detección de Aplicaciones de Riesgo

Se deberán implementar controles para detectar y restringir el uso de sistemas, aplicaciones y utilidades de software que pudieran anular o evitar los controles de seguridad o que pudieran usarse para evaluar la seguridad de la infraestructura tecnológica del Organismo sin haber sido debidamente autorizadas.

9.4.7 Acceso a Internet

El acceso a Internet deberá ser utilizado para propósitos laborales.

Se habilitará el acceso básico a Internet a todos los agentes que cuenten con una cuenta de usuario, estableciéndose pautas de utilización de Internet para todos los usuarios conforme al documento “Política de Uso Aceptable de los Recursos de Tecnología de la Información”.

Se deberán definir procedimientos para solicitar y aprobar accesos a sitios restringidos de Internet. Dichos accesos deberán ser solicitados por el responsable de la Dirección a cargo del personal que lo requiera.

Se registrarán los accesos de todos los usuarios a Internet, con el objeto de realizar revisiones de auditoría o análisis forense ante incidentes de seguridad.

Con el objeto de minimizar el riesgo de violación a la seguridad a través del uso incorrecto del servicio de Internet, se deberán seguir las siguientes pautas de cumplimiento:

a) Queda prohibido acceder a material pornográfico, actividades de apuestas, lúdicas, entretenimiento o pasatiempos de similar tenor, como así también a páginas con contenido contrario a las normas de sentido común y buenas costumbres.

b) Queda prohibido atentar contra los sistemas informáticos y redes de comunicación del Organismo y de terceros.

c) Queda prohibido hacer uso de los repositorios de Internet para almacenar información secreta, privada, confidencial y/o restringida del Organismo.

d) Todos los archivos descargados de Internet deberán ser analizados con herramientas antimalware. Los archivos cifrados que se intenten descargar de Internet que no pudieran analizarse serán bloqueados.

e) Queda prohibida la reproducción de audio y/o video de transmisiones en vivo o bajo demanda de sitios de internet, dado que dicha práctica afecta considerablemente el ancho de banda disponible en el Organismo, degradando el tiempo de respuesta y generando dificultades a las áreas que procesan información Institucional.

f) Queda prohibido bajar o subir información no inherente a las tareas desempeñadas, como así también el uso de programas de mensajería, redes sociales, intercambio de archivos y con otro fin que no sea el laboral.

g) Queda prohibido usar cualquier tipo de mensajería instantánea o web chat para uso personal, a excepción de los específicamente autorizados por la autoridad competente para fines laborales.

h) Toda excepción a las enumeradas previamente debe contar la explicita autorización del responsable de la Dirección a cargo del personal que lo requiera y deberá ser registrada formalmente.

9.4.8 Control de Acceso al Código Fuente

Se deberá restringir y controlar el acceso al código fuente de las aplicaciones de software desarrolladas en el Organismo, con el fin de evitar que sean introducidos cambios sin la debida autorización y control de las áreas involucradas o copia no autorizada del código fuente.

Se deberá definir un responsable de la función de “Administrador de Código Fuentes”, quien tendrá a cargo la custodia de los programas fuentes y deberá llevar un registro actualizado de todos los programas fuentes en uso, indicando nombre del programa, programador, Analista Responsable que autorizó, versión, fecha de última modificación y fecha / hora de compilación y estado (en modificación, en producción).

Se deberá establecer que todo programa objeto o ejecutable en producción tenga un único programa fuente asociado que garantice su origen, es decir que exista trazabilidad de versión entre el programa objeto y el código fuente.

Se deberá establecer la existencia de un implementador de producción, el cual será el responsable del pase a producción.

Se deberá desarrollar un procedimiento que garantice que toda vez que se migre a producción el módulo fuente, se cree el código ejecutable correspondiente en forma automática.

Se deberá prohibir el resguardo de programas fuentes históricos (que no sean los correspondientes a los programas operativos) en el ambiente de producción.

Se deberá prohibir el acceso a todo operador y/o usuario de aplicaciones a los ambientes y a las herramientas que permitan la generación y/o manipulación de los programas fuentes.

Se deberán realizar copias de respaldo de los programas fuentes cumpliendo los requisitos de seguridad establecidos por el Organismo en los procedimientos que surgen de la presente política, teniendo para ello presente, el punto .12.3.1 Copia de Resguardo y Restauración.

9.4.9 Identificación Automática de Estaciones de Trabajo

Se deberá tener en cuenta la identificación automática de las estaciones de trabajo conectadas a la red interna del Organismo, con el objeto de validar las conexiones generadas, debiendo segregarse de la red, aquellas estaciones de trabajo que no estuvieran normalizadas según las directivas de seguridad preestablecidas o que no pudieran identificarse debidamente.

9.4.10 Identificación y Autenticación de los Usuarios

Se deberán seguir expresamente las siguientes directivas:

Todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán un identificador univoco (ID de usuario) solamente para su uso personal exclusivo, de manera que las actividades puedan rastrearse con posterioridad hasta llegar al individuo responsable, a fin de garantizar la trazabilidad de las transacciones. Los identificadores de usuario no darán ningún indicio del nivel de privilegio otorgado.

En circunstancias excepcionales, cuando existe un claro beneficio para el Organismo, podrá utilizarse un identificador compartido para un grupo de usuarios o una tarea específica. Para casos de esta índole, se documentará la justificación y aprobación del Propietario de la Información de que se trate.

Si se utilizará un método de autenticación físico (por ejemplo, autenticadores de hardware), debe implementarse un procedimiento que incluya:

a) Asignar la herramienta de autenticación.

b) Registrar los poseedores de autenticadores.

c) Rescatar el autenticador al momento de la desvinculación del personal al que se le otorgó.

d) Revocar el acceso del autenticador, en caso de compromiso de seguridad.

Av. Julio A. Roca 609, C1067ABB
Ciudad Autónoma de Buenos Aires, Argentina
Horario de atención de 9:30 a 16:00

ces@indec.gob.ar
Tel.: (54-11) 5031-4632

www indec.gob.ar

INDECArgentina

10 Política de Criptografía

Objetivos

Garantizar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, no repudio, la autenticidad y/o la integridad de la información.

10.1 Cumplimiento de Requisitos

10.1.1 Política de Uso de Controles Criptográficos

Se utilizarán sistemas y técnicas criptográficas para el resguardo de la información, con el fin de asegurar una adecuada protección de su confidencialidad. Por lo cual se deberá asegurar la información y las comunicaciones mediante la utilización de controles criptográficos, en los siguientes casos:

- Contraseñas de acceso a sistemas.
- Almacenamiento de Datos, cuando el nivel de protección sea requerido.
- Cifrado de dispositivos móviles.
- Transmisión de información, dentro y fuera del ámbito del Organismo.
- Copias de Resguardo de la Información.
- O bien, producto de la evaluación de riesgo sobre el activo de información que se desea asegurar su confidencialidad

Se deberán utilizar algoritmos de cifrado robustos, que deberán ser validados periódicamente por la Coordinación de Seguridad Informática, con el objeto de evitar el uso de algoritmos de cifrado obsoletos, producto del avance de las técnicas de descifrado.

Al implementar la política de criptografía en el Organismo, se considerarán cuando sea necesario, los controles aplicables a la exportación e importación de tecnología criptográfica.

10.1.2 Firma Digital

Cuando sea necesario asegurar la autenticidad e integridad de los documentos electrónicos, los mismos deberán firmarse digitalmente.

Se deberán tomar los recaudos pertinentes para proteger la confidencialidad de las claves privadas, dichas claves deben ser resguardadas bajo el control exclusivo de su titular. Asimismo, es importante proteger la integridad de la clave pública, mediante el uso de un certificado de clave pública.

Se recomienda que las claves criptográficas utilizadas para firmar digitalmente no sean empleadas en procedimientos de cifrado de información.

Al utilizar firmas y certificados digitales, deberá supeditarse a lo dispuesto por la Ley N° 25.506, el Decreto N° 2628/02 y el conjunto de normas complementarias que fijan o modifican competencias

Av. Julio A. Roca 609, C1067ABB
Ciudad Autónoma de Buenos Aires, Argentina
Horario de atención de 9:30 a 16:00
ces@indec.gob.ar
Tel.: (54-11) 5031-4632
www indec.gob.ar
INDECArgentina

y establecen procedimientos, que describen las condiciones bajo las cuales una firma digital es legalmente válida.

10.1.3 Servicios de No Repudio

Se deberán utilizar los servicios de “no repudio”, cuando sea necesario garantizar transacciones electrónicas que pudieran generar disputas acerca de la ocurrencia y participación en las mismas. Es decir, cuando un individuo que envía el mensaje no pueda negar que es el emisor del mismo (no repudio en origen) y que el receptor no puede negar que recibió dicho mensaje (no repudio en destino), garantizando de este modo, la participación de las partes en dicha comunicación.

10.1.4 Procedimientos para la Gestión de Claves Criptográficas

Se deberá implementar un proceso seguro de administración de claves criptográficas para respaldar la utilización por parte del Organismo de las claves secretas (en criptografía simétrica) y las claves privadas (en criptografía asimétrica), para protegerlas contra modificación, destrucción, copia y divulgación no autorizada.

Se deberán implementar los mecanismos y tomar los recaudos necesarios para proteger la confidencialidad de las claves privadas.

Por lo cual, se deberán redactar procedimientos que estipulen operaciones de:

a) Almacenamiento de claves secretas y privadas, incluyendo la forma de acceso a las mismas por parte de los usuarios autorizados.

b) Renovación y Actualización de claves, incluyendo reglas sobre cuándo y cómo deben cambiarse las claves.

c) Eliminación de claves, incluyendo cómo deben retirarse o desactivarse las mismas, por ejemplo, cuando las claves hayan caducado.

d) Utilización de claves como parte de la administración de la continuidad de las operaciones, por ejemplo, para la recuperación de la información cifrada.

e) Generación e implementación de claves en operaciones de Copias de Resguardo y Restauración.

11 Política Físico y Ambiental

Objetivo

Prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones e información del Organismo.

Proteger el equipamiento de procesamiento de información crítica del Organismo ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados. Asimismo, contemplar la protección del mismo en su traslado y permanencia fuera de las áreas protegidas, por motivos de mantenimiento u otros.

Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información del Organismo.

Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus labores habituales.

Proporcionar protección proporcional a los riesgos identificados.

11.1 Áreas Seguras

11.1.1 Perímetro de seguridad física

Se deberán definir perímetros de seguridad, para proteger las áreas que contienen instalaciones de procesamiento de información, sala de los equipos de comunicaciones., instalaciones de suministro de energía eléctrica, instalaciones de aire acondicionado y cualquier otra área considerada crítica, que su puesta fuera de servicio o mal funcionamiento pueda entorpecer el normal funcionamiento de los sistemas de información del Organismo

11.1.2 Controles físicos de entrada

Todas las instalaciones edilicias del INDEC deberán implementar controles de acceso físico y monitoreo mediante cámaras de seguridad para supervisar la entrada y salida de personas y materiales.

Se deberán registrar fecha, horario y motivo de la visita al ingresar a las áreas protegidas, ya que sólo se permitirá el acceso por propósitos específicos y autorizados. Y se deberá registrar fecha y horario al egresar de dichas áreas.

Se deberá almacenar debidamente los registros de acceso a los efectos de auditorías o investigación de incidentes.

Se controlará y limitará el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas. Se mantendrá un registro protegido para permitir auditar todos los accesos.

Av. Julio A. Roca 609, C1067ABB
Ciudad Autónoma de Buenos Aires, Argentina
Horario de atención de 9:30 a 16:00
ces@indec.gob.ar
Tel.: (54-11) 5031-4632
www indec.gob.ar
INDECArgentina

Se deberá usar una identificación unívoca visible para todo el personal del área protegida e instruirlo acerca de cuestionar la presencia de desconocidos no escoltados por personal autorizado y a cualquier persona que no exhiba una identificación visible.

Se revisarán y actualizarán cada 6 meses los derechos de acceso a las áreas protegidas, dichos procesos serán documentados y firmados por el responsable de la Unidad Organizativa de la que dependa.

Se revisarán los registros de acceso a las áreas protegidas. Esta tarea la realizará la Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información.

11.1.3 Seguridad de oficinas, despachos e instalaciones

Se aplicarán mecanismos extras de control de acceso de seguridad física y/o electrónica a las oficinas y salas del Organismo, también definidas como áreas críticas, considerando la actividad desempeñada o el activo que administran.

Se definirán los siguientes sitios como áreas críticas, dada la actividad desarrollada en las mismas:

- Oficinas de Tesorería.
- Piso de la Alta Dirección.
- Oficinas usadas en la confección del Índice de Precios al Consumidor (IPC).
- Sala de los equipos de comunicaciones.
- Centro de Cómputo

11.1.4 Protección contra amenazas de origen ambiental y externas

Deberán existir controles adecuadamente ubicados de protección física contra incendios.

Deberá existir personal de seguridad física para contrarrestar amenazas de revueltas internas y externas y resguardo las áreas protegidas definidas en los puntos 11.1.2 Controles físicos de entrada y 11.1.3 Seguridad de oficinas, despachos e instalaciones.

11.1.5 Trabajo en áreas críticas

Para incrementar la seguridad de las áreas críticas, se deberán establecer controles y lineamientos adicionales, tanto para el personal del Organismo, como las actividades desarrollas por terceros que tengan lugar en dichas áreas, como ser:

a) Implementar controles extras como ser el monitoreo mediante cámaras de seguridad.

b) Evitar la ejecución de trabajos por parte de terceros sin supervisión de personal del Organismo.

c) Limitar el acceso a las áreas protegidas, solo al personal perteneciente a dichas áreas o cuando sean autorizados por personal responsable de las misma.

d) Considerar impedir el ingreso de dispositivos de almacenamiento portable a menos que sea necesario para el desempeño de sus funciones.

11.1.6 Áreas de acceso público, de carga y descarga

Se deberán establecer controles en las áreas de recepción, carga y descarga a fin de impedir accesos no autorizados a las instalaciones edilicias del Organismo.

Las áreas de recepción, carga y descarga deberán estar aisladas de las instalaciones de procesamiento de información y de las áreas protegidas.

Para ello se establecerán controles físicos que considerarán los siguientes lineamientos:

a) Limitar el acceso a las áreas de depósito, desde el exterior de la sede del Organismo, sólo al personal previamente identificado y autorizado.

b) Diseñar el área de depósito de manera tal, que los suministros puedan ser descargados sin que el personal que realiza la entrega acceda a otros sectores del edificio.

c) Verificar y registrar el material entrante al ingresar a las instalaciones edilicias del Organismo.

d) Inspeccionar el material entrante para descartar peligros potenciales antes de ser trasladado desde el área de depósito hasta el lugar de uso.

11.2 Seguridad de los equipos

11.2.1 Emplazamiento y protección de equipos

El equipamiento deberá ser será ubicado y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas, peligros ambientales y acceso no autorizado, teniendo en cuenta los siguientes puntos:

a) Ubicar el equipamiento en un sitio donde se minimice el acceso innecesario y provea un control de acceso adecuado.

b) Ubicar las instalaciones de procesamiento y almacenamiento de información que procesan datos clasificados, en un sitio que permita la supervisión constante.

c) Adoptar controles adecuados para minimizar el riesgo de amenazas potenciales por robo, hurto, incendio, polvo, calor y radiaciones electromagnéticas.

d) No se debería comer, beber y fumar en proximidad de los equipos de procesamiento de la información como ser el centro de cómputos o la sala de comunicaciones.

11.2.2 Seguridad en el suministro eléctrico

El equipamiento de procesamiento de datos deberá estar protegido ante posibles fallas en el suministro de energía u otras anomalías eléctricas.

Para asegurar la continuidad del suministro de energía, deberá contarse con equipamiento de Suministro de Energía Interrumpible (UPS) y grupo Generador de Energía Eléctrica de respaldo.

Se deberá proveer de iluminación de emergencia en caso de producirse una falla en el suministro principal de energía. Se deberá implementar además protección contra descargas eléctricas en todos los edificios y líneas de comunicaciones externas de acuerdo con las normativas vigentes, adoptando filtros de protección contra rayos a todas las líneas de ingreso de energía eléctrica y comunicaciones.

11.2.3 Seguridad del cableado

El cableado de comunicaciones que transporta datos y brinda apoyo a los servicios de información deberá estar protegido contra intercepción o daño. Por ello, el cableado deberá:

a) Cumplir con los requisitos técnicos vigentes de la República Argentina.

b) Separar los cables de energía de los cables de comunicaciones de datos para evitar interferencias.

c) Proteger el tendido del cableado de red troncal entre los pisos, mediante la utilización de ductos blindados y/o con controles de acceso físicos.

d) Utilizar piso técnico y/o cableado embutido en la pared, siempre que sea posible.

e) Utilizar medios de transmisión alternativos seguros cuando no sea posible asegurar la seguridad en el cableado.

11.2.4 Mantenimiento del equipamiento informático

Se deberán realizar tareas periódicas de mantenimiento preventivo del equipamiento de procesamiento de datos y comunicaciones para asegurar su disponibilidad e integridad permanentes, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal del responsable del Área Informática. El Área de Informática deberá mantener un listado actualizado del equipamiento con el detalle de la frecuencia en que se realizará el mantenimiento preventivo.

Se deberá eliminar la información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.

11.2.5 Seguridad de los equipos fuera de las instalaciones

El uso de equipamiento destinado al procesamiento de información, fuera del ámbito del Organismo, deberá ser autorizado por el responsable patrimonial. En el caso de que en el mismo se almacene información clasificada, debe ser aprobado además por el Propietario de la misma.

Cuando se autorice el uso de equipamiento informático fuera del ámbito de las dependencias del Organismo, el mismo deberá contar con controles de seguridad preventivos ante pérdida, robo, daño o intercepción.

Se deberán respetar permanentemente las instrucciones del fabricante respecto del cuidado del activo. Asimismo, se mantendrá una adecuada cobertura de seguro para proteger el equipamiento fuera del ámbito del Organismo, cuando el activo lo amerite.

11.2.6 Reutilización o Baja de equipamiento informático

Se deberán aplicar operaciones de borrado seguro a todo equipamiento informático, antes de que el mismo sea normalizado para su reutilización, previo resguardo de la información útil y licencias alojadas en dicho equipamiento, teniendo en cuenta las directivas mencionadas en el punto 8.3.2 Eliminación Segura de Soportes de Información.

11.2.7 Retiro de propiedad del organismo

El equipamiento, soportes de almacenamiento, información y software no se deberán retirar o transmitir fuera del ámbito de las dependencias del Organismo sin previa autorización formal.

Se podrán llevar a cabo comprobaciones periódicas para detectar el retiro no autorizado de activos del Organismo.

11.2.8 Pantallas Limpias

Los usuarios deberán cerrar las sesiones de las aplicaciones, sistemas y servicios de red, cuando no estén siendo usadas.

Los usuarios al ausentarse momentáneamente de su puesto de trabajo deberán cerrar la sesión activa o en su defecto, bloquear el equipo informático, para evitar el acceso indebido al mismo en su ausencia.

Se deberá establecer el bloqueo automático de las pantallas, cuando el equipo se encuentre desatendido por más de 5 (cinco) minutos con el objeto de evitar accesos no autorizados a los mismos.

Los usuarios deberán cerrar las sesiones activas al finalizar su jornada laboral y apagar el equipo informático o en su defecto cerrar las sesiones de servicios abiertos y activar el bloqueo del mismo cuando sea solicitado por la Coordinación de Seguridad Informática para realizar tareas de mantenimiento fuera del horario laboral.

11.2.9 Escritorios Limpios

Los usuarios deberán proteger la información no pública que utilizan en sus tareas, no dejando documentación en papel u otro medio de almacenamiento (pendrives, unidades removibles, cd, etc.) sobre su puesto de trabajo sin ningún tipo de control.

Se deberá almacenar bajo llave en gabinetes seguros o cajas fuertes, cuando corresponda, los documentos en papel y soportes de almacenamiento que posean información sensible o crítica, cuando no estén siendo utilizados, especialmente fuera del horario de trabajo.

Se deberá retirar inmediatamente la información sensible o confidencial, una vez impresa.

Se deberán bloquear las fotocopiadoras fuera del horario normal de trabajo y proteger los puntos de recepción y envío de correo postal y las máquinas de fax desatendidas.

12 Política de Seguridad en las Operaciones

Objetivo

Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información.

Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas, procedimientos para la respuesta a incidentes y separación de funciones.

12.1 Procedimientos y Responsabilidades Operativas

12.1.1 Documentación de los Procedimientos Operativos

Los procedimientos operativos deberán ser identificados, documentados, actualizados y puestos a disposición de todos los usuarios que lo requieran. Las responsabilidades referidas a las tareas operativas deberán estar formalmente asignadas.

Los procedimientos especificarán instrucciones para la ejecución detallada de cada tarea, incluyendo:

a) Información que gestiona

b) Requerimientos o interdependencias con otros sistemas.

c) Instrucciones para el manejo de errores u otras condiciones excepcionales que puedan surgir durante la ejecución de tareas.

d) Personas de soporte a quien contactar en caso de dificultades operativas o técnicas imprevistas.

12.1.2 Cambios en las Operaciones

Se deberán definir procedimientos para controlar los cambios en los procesos operativos que pudieran afectar la seguridad en los sistemas de procesamiento del INDEC.

Se deberán almacenar un registro detallado de los cambios para operaciones de auditoría y respuesta de incidentes, conteniendo el mismo toda información relevante a cada cambio implementado.

Se deberá controlar que los cambios a implementar no afecten la seguridad de los procesos asociados ni de la información que administra.

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

Se deberá controlar que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de los mismos ni de la información que soportan. Razón por la cual se deberá

Av. Julio A. Roca 609, C1067ABB
Ciudad Autónoma de Buenos Aires, Argentina
Horario de atención de 9:30 a 16:00
ces@indec.gob.ar
Tel.: (54-11) 5031-4632
www indec.gob.ar
INDECArgentina

evaluar el posible impacto operativo de los cambios previstos y verificar su correcta implementación.

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

Los procedimientos de control de cambios contemplarán los siguientes puntos:

a) Identificación y registro de cambios significativos.

b) Evaluación del posible impacto de dichos cambios.

c) Aprobación formal de los cambios propuestos.

d) Planificación del proceso de cambio.

e) Prueba del nuevo escenario.

f) Comunicación de detalles de cambios a todas las personas pertinentes.

g) Identificación de las responsabilidades por la cancelación de los cambios fallidos y la recuperación respecto de los mismos

12.1.3 Planificación de la Capacidad

Se deberá monitorear y evaluar las necesidades de capacidad operacional actuales de los sistemas y proyectar las futuras demandas, con el objeto de garantizar que el crecimiento no ponga en riesgo las actividades operativas ante la falta de recursos.

12.1.4 Separación de entornos de desarrollo, pruebas y producción

Deberán existir cuatro ambientes diferenciados de trabajo, desarrollo, pruebas, pruebas de seguridad y producción, los cuales deberán estar separados y ser independientes.

Deberán existir procedimientos formales para el traspaso entre estos ambientes, con el fin de reducir el riesgo de cambios no autorizados en los mismos y garantizar la producción de sistemas seguros. Esto controles deberán tener en cuenta los siguientes aspectos:

a) El personal de desarrollo no tendrá acceso al ambiente productivo, oficiando solo como asesor del personal de producción cuando lo requieran.

b) Definir propietarios de la información para cada uno de los ambientes de procesamiento existentes.

c) Ante extrema necesidad, se establecerá un procedimiento formal de emergencia que permita registrar la autorización, acceso y cambio efectuado en el servidor de producción por el personal de desarrollo.

d) El ambiente de producción deberá contar, solo, con el software necesario para el funcionamiento del sistema al que sirve, evitando la existencia de compiladores u otros utilitarios del sistema que pudieran alterar el correcto funcionamiento del mismo.

12.2 Protección contra Código Malicioso

12.2.1 Controles contra Código Malicioso

Se deberán proteger los sistemas tecnológicos mediante la implementación de controles para prevenir, detectar, eliminar y recuperar los sistemas afectados por código malicioso.

Dichos sistemas de detección de código malicioso deberán estar instalados y actualizados en todas las estaciones de trabajo y servidores que conforman la infraestructura tecnológica del Organismo.

Para evitar la ejecución de código malicioso, se deberá controlar toda actividad de lectura y grabación de archivos, en estaciones de trabajo y servidores, todo tráfico de carga y descarga de archivos en los servidores de conexión a Internet y el control en los correos electrónicos con archivos adjuntos o enlaces a sitios web.

Se deberán realizar periódicamente, análisis preventivos para la detección y eliminación de código malicioso en los servidores y estaciones de trabajo.

Como también se deberán implementar las directivas emanadas en la Política de Uso Aceptable de los Recursos de Tecnología de la Información existente.

12.3 Copias de Seguridad

12.3.1 Copia de Resguardo y Restauración

Se definirán procedimientos para el resguardo de la información, que deberá considerar:

a) Definir un esquema de rótulo de las copias de resguardo, que permita contar con toda la información necesaria para identificar y administrar cada una de ellas debidamente.

b) Establecer un esquema de reemplazo de los medios de almacenamiento de las copias de resguardo, una vez concluida la posibilidad de ser reutilizados, de acuerdo a lo indicado por el proveedor y asegurando la destrucción de los medios desechados.

c) Almacenar en una ubicación remota copias de resguardo junto con registros exactos y completos de las mismas y procedimientos documentados de restauración, a una distancia suficiente como para evitar daños provenientes de un desastre en el sitio principal. Teniendo en cuenta el nivel de clasificación otorgado a la información resguardada.

d) Asignar a la información de resguardo, un nivel de protección física y ambiental según los requisitos del proveedor del medio de almacenamiento y las normas aplicadas en el sitio principal.

e) Verificar periódicamente la efectividad de los procedimientos de copias y restauración, asegurándose que cumplan con los requerimientos de los planes de continuidad de las actividades del Organismo, según el punto 0 Objetivo

f) Minimizar los efectos de las posibles interrupciones de las actividades normales del Organismo (sean éstas resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.

Av. Julio A. Roca 609, C1067ABB
Ciudad Autónoma de Buenos Aires, Argentina
Horario de atención de 9:30 a 16:00
ces@indec.gob.ar
Tel.: (54-11) 5031-4632
www indec.gob.ar
INDECArgentina

g) Analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro.

h) Maximizar la efectividad de las operaciones de contingencia del Organismo con el establecimiento de planes que incluyan al menos las siguientes etapas:

i) Notificación/Activación: Consistente en la detección y determinación del daño y la activación del plan.

j) Reanudación: Consistente en la restauración temporal de las operaciones y recuperación del daño producido al sistema original.

k) Recuperación: Consistente en la restauración de las capacidades de proceso del sistema a las condiciones de operación normales.

l) Asegurar la coordinación con el personal del Organismo y los contactos externos que participarán en las estrategias de planificación de contingencias. Asignar funciones para cada actividad definida.

m) Gestión de Continuidad de las Operaciones.

n) Cifrar la Copia de Resguardo, de acuerdo al punto 10.1.1 Política de Uso de Controles Criptográficos.

o) El período de retención de las copias de resguardo deberá ser establecido por medio de una política de retención de acuerdo al tipo de información resguardada y en concordancia con la política 18.1.3 Protección de los Registros del Organismo.

12.4 Registro de Actividad y Monitoreo

12.4.1 Registro de eventos

Se deberán registrar los eventos referidos a la actividad de usuarios y sistemas, eventos asociados a errores y seguridad.

Se deberán almacenar remotamente los eventos de las estaciones de trabajo y servidores críticos, con el objeto de garantizar su integridad y disponibilidad para la detección e investigación de incidentes de seguridad. Los registros de auditoría se almacenarán localmente para las estaciones de trabajo y servidores considerados, no críticos.

Se deberán registrar mínimamente los siguientes datos:

a) Inicio y cierre de sesión;

b) Identificación del usuario

c) Identificación del equipo

d) Direcciones de redes y protocolos

e) Fecha y hora del evento

f) Descripción del evento

g) Registros de intentos de acceso al sistema exitosos y fallidos

h) Registros de intentos de acceso a los datos u otro recurso, exitosos y rechazados

i) Cambios de configuración del sistema

j) Ejecución de aplicaciones de sistemas

k) Archivos accedidos y el tipo de acceso

l) Uso de privilegios

m) Activación y desactivación de los sistemas de protección.

Para el registro de los eventos se debe considerar la política 18.1.3 Protección de los Registros del Organismo

12.4.2 Protección del registro de información de auditoría

Se implementarán controles para la protección de los registros de auditoría almacenados, contra cambios no autorizados, como ser alteración de los mismos o eliminación.

Se deberán implementar controles para evitar fallas por falta de espacio de almacenamiento.

12.4.3 Actividad de los Administradores y Operadores

Se deberá controlar periódicamente la actividad de los usuarios administradores y operadores de sistemas que administren información confidencial, privada o secreta.

Se deberán definir alertas automáticas que informen actividades catalogadas sospechosas, ya sea debido a accesos u operaciones indebidas o fallas de los sistemas.

12.4.4 Sincronización de Relojes

Se deberán sincronizar los relojes de todos los sistemas y equipos informáticos en relación a una o varias fuentes de sincronización únicas de referencia, a fin de garantizar la exactitud de los registros de auditoría.

12.5 Control en la Instalación de Software

12.5.1 Instalación de Software en Producción

Se deberán definir procedimientos para controlar la instalación de software en sistemas operacionales en producción que establezcan los pasos a seguir para validar autorizaciones, conformidades y pruebas previas pertinentes.

Toda aplicación, desarrollada por el Organismo o por un tercero, deberá tener un único responsable designado formalmente por la Dirección de Informática.

Ningún programador o analista de desarrollo podrá acceder a los ambientes de producción, en concordancia con el punto 12.1.4 Separación de entornos de desarrollo, pruebas y producción.

Se debería conservar la versión previa del sistema, como medida de contingencia y control, llevar un registro de auditoría de las actualizaciones efectuadas e instalar sólo los ejecutables en el ambiente de producción.

Se designarán formalmente a los implementadores de los sistemas en producción, evitando que sean los mismos programadores o analista de desarrollo del software que se desea poner en producción.

12.6 Gestión de Vulnerabilidades Técnicas

12.6.1 Vulnerabilidades Técnicas y Remediación

Se deberán efectuar pruebas técnicas y de seguridad, con el objeto de conocer el grado de exposición del sistema antes de desplegarlo en producción, a fin de adoptar las medidas necesarias para minimizar o eliminar los riesgos asociados. Esto también aplica para todo sistema de software desarrollado en el Organismo teniendo en cuenta las directivas de la política 14.2.9 Evaluación de Vulnerabilidades de Seguridad.

Se deberá minimizar los riesgos de actualización, mediante la implementación del control de cambios, imponiendo el cumplimiento de procedimientos formales que garanticen que se cumplan pautas de seguridad y control. Se deberá verificar que los cambios cumplan con los requisitos solicitados y se cuente con las autorizaciones necesarias.

Se deberán establecer roles y responsabilidad asociados a los procesos de identificación de vulnerabilidades técnicas, procedimientos de remediación mediante la instalación de actualizaciones de seguridad, implementación de directrices de configuraciones seguras y controles para asegurar su cumplimiento.

12.6.2 Restricciones en la Instalación de Software

Se declara la prohibición de toda instalación de software, a menos que sea autorizada por la Coordinación de Seguridad Informática, ya que la instalación no controlada de software en sistemas informáticos puede dar pie a la introducción de vulnerabilidades y a la fuga de información, a la falta de integridad u otros incidentes de seguridad de información o bien a la transgresión de derechos de propiedad intelectual.

La instalación de software deberá respetar la Ley de Propiedad Intelectual N° 11.723 y sus decretos asociados, como así también el tipo de licenciamiento designado por el autor del mismo. Por lo que se prohíbe la instalación y uso de cualquier tipo de aplicación y utilidades que active licencias de manera indebida (ver punto 18.1.2 Derechos de Propiedad Intelectual).

12.7 Auditoría de los Sistemas en Producción

12.7.1 Controles de auditoría en los sistemas de información

Se deberá planificar y definir cuidadosamente las actividades de auditoría a realizar sobre los sistemas en producción, con el objeto de minimizar el impacto en los procesos de negocio del Organismo, por esta razón deberán existir procedimientos formales para tal actividad.

Las actividades de auditoría sobre los sistemas en producción deberán tomar los recaudos necesarios que permitan revertir los cambios efectuados en los sistemas en auditados.

Se protegerá el acceso a los elementos utilizados en las auditorías de sistemas, o sea archivos de datos o software, a fin de evitar el mal uso o el compromiso de los mismos.

Dichas herramientas estarán separadas de los sistemas en producción y de desarrollo, y se les otorgará el nivel de protección requerido.

Se tomarán los recaudos necesarios a efectos de cumplimentar las normas de auditoría dispuestas por la Sindicatura General de la Nación.

13 Política en la Gestión de Comunicaciones

Objetivo

Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones.

13.1 Gestión en la Seguridad en las Redes de Datos

13.1.1 Controles en las Redes de Datos

Se deberán restringir las conexiones a los puertos de los dispositivos de red, permitiéndoles conectarse únicamente a los dispositivos con direcciones físicas autorizadas, habilitando de este modo la seguridad de los puertos de conexión.

Se deberán definir controles que inspeccionen los paquetes de datos que se circulan en la red con el objeto de detectar código malicioso que intente vulnerar los sistemas informáticos.

Se deberá controlar la navegación ilimitada de Internet para evitar comprometer el rendimiento y/o estabilidad del acceso a la misma.

Se deberá controlar a los equipos informáticos que se conecten hacia y desde Internet, sea efectuada a través de dispositivos de seguridad que inspeccionan el tráfico saliente y entrante, con el objeto de evitar que la navegación transgreda las normas establecidas en la Política de Uso Aceptable de los Recursos de Tecnología de la Información.

Se deberá controlar el tráfico de datos interno y externo de la red informática mediante dispositivos de seguridad que controlen activamente las comunicaciones con origen y destino autorizados.

Se deberán implementar controles para mantener la alta disponibilidad de los servicios de red y equipamiento informático interconectado.

Se deberá controlar el acceso, administración y uso de los servicios web publicados.

Se deberá mantener instalados y habilitados sólo aquellos servicios que hayan sido autorizados.

13.1.2 Seguridad de los Servicios Activos

La Coordinación de Seguridad Informática definirá las pautas para garantizar la seguridad de los servicios de red del Organismo, dichos servicios activos deberán ser revisados periódicamente, proponiendo recomendaciones cuando sea necesario.

Se deberán seguir expresamente las siguientes directivas:

a) Mantener instalados y habilitados sólo aquellos servicios que sean utilizados.

b) Controlar el acceso lógico a los servicios, tanto su uso. como su administración.

c) Configurar cada servicio de manera segura, siguiendo las recomendaciones de buenas prácticas de seguridad del servicio en cuestión.

Av. Julio A. Roca 609, C1067ABB
Ciudad Autónoma de Buenos Aires, Argentina
Horario de atención de 9:30 a 16:00
ces@indec.gob.ar
Tel.: (54-11) 5031-4632
www indec.gob.ar
INDECArgentina

d) Instalar periódicamente las actualizaciones de seguridad.

e) Evaluar periódicamente la seguridad de los servicios.

13.1.3 Segregación de redes

Con el fin de restringir el acceso indebido a los datos, se deberán segregar el tráfico de datos que circulan por las redes del Organismo, en función de criterios, como ser, estructura organizacional, grupos de servicios utilizados, ubicación u otro. Estos perímetros de seguridad definidos en la segregación de redes deberán ser formalmente definidos y documentados.

13.2 Intercambio de Información con Partes Externas

13.2.1 Procedimientos y Controles de Intercambio de la Información

Se deberán establecer procedimientos para solicitar y aprobar accesos especiales a Internet.

El uso de internet estará sujeto a la Política de Uso Aceptable de los Recursos de Tecnología de la Información, la cual considera aspectos tales como, responsabilidades de los empleados con respecto a la difamación, hostigamiento, personificación, reenvío de cadenas de comunicación de correo electrónico, redes sociales y otros.

La información intercambiada hacia y desde Internet deberá ser protegida contra la intercepción, copiado o modificación.

Los servicios que se exponen hacia Internet deberán estar protegidos ante amenazas externas.

Se deberán implementar controles para la detección de código malicioso que puede ser transmitido desde Internet hacia las redes del Organismo.

Se deberá hacer uso de técnicas criptográficas actualizadas para proteger la confidencialidad, integridad y la autenticidad de la información que se transmite y envía hacia redes externas.

13.2.2 Acuerdos en los Intercambios de Información con Entidades Externas

Cuando se realicen acuerdos entre el INDEC y otros organismos, relativos al intercambio de información y software, se deberá especificar e implementar las consideraciones de seguridad para la transferencia segura de datos entre ambas partes.

13.2.3 Seguridad del Correo Electrónico

El uso del servicio de correo electrónico laboral estará sujeto a la Política de Uso Aceptable de los Recursos de Tecnología de la Información, por lo cual todos los empleados del Organismo deberán aceptar y firmar las pautas de uso declaradas en dicha política, antes de acceder a la cuenta de correo electrónica asignada.

Se deberá proteger el sistema de correo electrónico para evitar el acceso no autorizado, denegación de servicio, correos publicitarios no deseados, suplantación de identidad del remitente y demás amenazas existentes.

El tráfico del sistema de correo electrónico laboral será analizado por sistemas antimalware, con el objeto de detectar archivos binarios maliciosos adjuntos que pusieran en peligro a la infraestructura tecnológica del Organismo.

Se prohíbe adjuntar en la cuenta de correo electrónico laboral binarios ejecutables, cifrados, multimedia de audio y video o archivos de gran tamaño que pudieran degradar el sistema de correo electrónico institucional.

13.2.4 Acuerdo de Confidencialidad en el Intercambio de Información.

Se deberán identificar, revisar y documentar los acuerdos de confidencialidad, para la protección de la información del Organismo que es transferida a entidades externos. Dichos acuerdos deben responder a los requerimientos de confidencialidad o no divulgación del Organismo.

Dichos acuerdos de confidencialidad deberán cumplir con toda legislación o normativa vigente en la administración pública.

14 Política de Adquisición, Desarrollo y Mantenimiento de Sistemas

Objetivo

Asegurar la inclusión de controles de seguridad y validación de datos en la adquisición, desarrollo y mantenimiento de los sistemas de información.

Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.

Definir los métodos de protección de la información crítica o sensible.

Alcance

Esta Política se aplica a todos los sistemas informáticos, tanto los desarrollos propios como los de terceros, y a todos los Sistemas Operativos y/o Software de Base que integren cualquiera de los ambientes administrados por el Organismo en donde residan los desarrollos mencionados.

Responsabilidad

El responsable de Seguridad de la Información junto con el Propietario de la Información y la Unidad de Auditoría Interna, definirán los controles a ser implementados en los sistemas desarrollados internamente o por terceros, en función de una evaluación de riesgos.

El responsable de Seguridad de la Información, junto con el Propietario de la Información, definirá en función a la criticidad de la información, los requerimientos de protección mediante métodos

criptográficos. Luego, el responsable de Seguridad de la Información definirá junto con el responsable del Área de Sistemas, los métodos de encriptación a ser utilizados.

El responsable de Seguridad de la Información cumplirá las siguientes funciones:

- Definir los procedimientos de administración de claves.
- Verificar el cumplimiento de los controles establecidos para el desarrollo y mantenimiento de sistemas.
- Garantizar el cumplimiento de los requerimientos de seguridad para el software.
- Definir procedimientos para: el control de cambios a los sistemas; la verificación de la seguridad de las plataformas y bases de datos que soportan e interactúan con los sistemas; el control de código malicioso; y la definición de las funciones del personal involucrado en el proceso de entrada de datos.

El responsable del Área Informática propondrá para su aprobación, por parte del superior jerárquico que corresponda, la asignación de funciones de “implementador” y “administrador de programas fuentes” al personal de su área que considere idóneo y cuyas responsabilidades se detallan en la presente cláusula. Asimismo, verificará el cumplimiento de las definiciones establecidas sobre los controles y las medidas de seguridad a ser incorporadas a los sistemas.

El Área de Sistemas propondrá quiénes realizarán la administración de las técnicas criptográficas y claves.

El responsable del Área de Administración incorporará aspectos relacionados con el licenciamiento, la calidad del software y la seguridad de la información en los contratos con terceros por el desarrollo de software. El responsable del Área Jurídica participará en dicha tarea.

14.1 Requerimientos de Seguridad de los Sistemas

14.1.1 Análisis y Especificaciones de los Requerimientos de Seguridad

Se deberán incorporar requisitos de seguridad en los sistemas de información (desarrollos propios y de terceros) y en todas las mejoras o actualizaciones que se les incorporen. Razón por la cual, la Coordinación de Seguridad Informática deberá formar parte del ciclo de vida de desarrollo de los sistemas informáticos.

Así también se deben tener en cuenta las siguientes consideraciones:

- Definir un procedimiento para que durante las etapas de análisis y diseño del sistema se incorporen a los requerimientos los correspondientes controles de seguridad. Este procedimiento debe incluir una etapa de evaluación de riesgos previa al diseño para definir los requerimientos de seguridad e identificar los controles apropiados. En esta tarea deben participar las áreas usuarias, de sistemas, de seguridad informática y auditoría, especificando y aprobando los controles automáticos a incorporar al sistema y las necesidades de controles manuales complementarios. Las áreas involucradas podrán solicitar certificaciones y evaluaciones independientes para los productos a utilizar.
- Evaluar los requerimientos de seguridad y los controles requeridos, teniendo en cuenta que éstos deben ser proporcionales en costo y esfuerzo al valor del bien que se quiere proteger y al daño potencial que pudiera ocasionar a las actividades realizadas.

- Hay que considerar y evaluar que los controles en la etapa de diseño son significativamente menos costosos para implementar y mantener que aquellos incluidos durante o después de la implementación de los sistemas.

14.1.2 Seguridad en los Servicios accedidos desde Redes Públicas

Se deberán implementar controles de seguridad que den soporte a todos los sistemas del Organismo, dichos controles deberán ser los seguidamente detallados:

- Vulnerabilidades de la información en los sistemas de oficina, por ejemplo, la grabación de llamadas telefónicas o teleconferencias, la confidencialidad de las llamadas, el almacenamiento de faxes, la apertura o distribución del correo.
- Procedimientos y controles apropiados para administrar la distribución de información, por ejemplo, el uso de boletines electrónicos institucionales.
- Exclusión de categorías de información sensible del Organismo si el sistema no brinda un adecuado nivel de protección.
- Limitación del acceso a la información de las actividades que desarrollan determinadas personas, por ejemplo, aquellas que trabaja en proyectos sensibles.
- La aptitud del sistema para dar soporte a las aplicaciones del Organismo, como la comunicación de órdenes o autorizaciones.
- Categorías de personal y contratistas o terceros a los que se permite el uso del sistema y las ubicaciones desde las cuales se puede acceder al mismo.
- Restricción de acceso a determinadas instalaciones a especificas categorías de usuarios.
- Identificación de la posición o categoría de los usuarios, por ejemplo, empleados del Organismo o contratistas, en directorios accesibles por otros usuarios.
- Retención y resguardo de la información almacenada en el sistema.
- Requerimientos y disposiciones relativos a sistemas de soporte de reposición de información previa.

14.1.3 Protección de la Información en servicios de aplicativos

Se tomarán recaudos para la protección de la integridad de la información publicada electrónicamente a fin de prevenir la modificación no autorizada que podría dañar la reputación del Organismo. Es posible que la información de un sistema de acceso público, por ejemplo, la información en un servidor Web accesible por Internet, deba cumplir con ciertas normas de la jurisdicción en la cual se localiza el sistema o en la cual tiene lugar la transacción electrónica. Se implementará un proceso de autorización formal antes de que la información se ponga a disposición del público, estableciéndose en todos los casos los encargados de dicha aprobación.

Todos los sistemas de acceso público deberán prever que:

- La información se obtenga, procese y proporcione de acuerdo con la normativa vigente, en especial la Ley de Protección de Datos Personales.

- La información que se ingresa al sistema de publicación, o aquella que procesa el mismo, sea procesada en forma completa, exacta y oportuna.
- La información sensible o confidencial sea protegida durante el proceso de recolección y su almacenamiento.
- El acceso al sistema de publicación no permita el acceso accidental a las redes a las cuales se conecta el mismo.
- El responsable de la publicación de información en sistemas de acceso público sea claramente identificado.
- La información se publique teniendo en cuenta las normas establecidas al respecto.
- Se garantice la validez y vigencia de la información publicada.

14.2 Seguridad en Procesos de Desarrollo

14.2.1 Desarrollo Seguro de Software

Se deberá establecer una Política de Requisitos de Seguridad para el Desarrollo Seguro de Software aplicable a todo desarrollo de aplicaciones y sistemas de información dentro del Organismo como así también el realizado por terceros.

Se deberá involucrar a la Coordinación de Seguridad Informática en el ciclo de vida de desarrollo de los sistemas de información desde el inicio con el objeto de validar la arquitectura de seguridad.

Los requisitos mínimos que se deberán considerar son los siguientes:

- Validación de datos de entrada (en el cliente y en el servidor).
- Validación de los datos de salida.
- Identificación de usuarios y origen de las conexiones de accesos.
- Control y Gestión de errores.
- Registro de actividades realizadas.
- Integridad de las transacciones.
- Cifrado de datos.
- Implementación de controles criptográficos cuando se desee transmitir mensajes con información clasificada.
- Otros requisitos de control en seguridad establecidos en la Política de Requisitos de Seguridad para el Desarrollo Seguro determinado por el ONTI en su inciso 14.

Así también se tomarán en cuenta los siguientes controles:

Controles de Procesamiento Interno:

Av. Julio A. Roca 609, C1067ABB
Ciudad Autónoma de Buenos Aires, Argentina
Horario de atención de 9:30 a 16:00
ces@indec.gob.ar
Tel.: (54-11) 5031-4632
www indec.gob.ar
INDECArgentina

Se definirá un procedimiento para que durante la etapa de diseño se incorporen controles de validación a fin de eliminar o minimizar los riesgos de fallas de procesamiento y/o vicios por procesos de errores.

Para ello se implementarán:

- Procedimientos que permitan identificar el uso y localización en los aplicativos, de funciones de incorporación y eliminación que realizan cambios en los datos.
- Procedimientos que establezcan los controles y verificaciones necesarios para prevenir la ejecución de programas fuera de secuencia o cuando falle el procesamiento previo.
- Procedimientos que establezcan la revisión periódica de los registros de auditoría o alertas de forma de detectar cualquier anomalía en la ejecución de las transacciones.
- Procedimientos que realicen la validación de los datos generados por el sistema.
- Procedimientos que verifiquen la integridad de los datos y del software cargado o descargado entre computadoras.
- Procedimientos que controlen la integridad de registros y archivos.
- Procedimientos que verifiquen la ejecución de los aplicativos en el momento adecuado.
- Procedimientos que aseguren el orden correcto de ejecución de los aplicativos, la finalización programada en caso de falla, y la detención de las actividades de procesamiento hasta que el problema sea resuelto.

Control de Validación de Datos de Salidas: Se establecerán procedimientos para validar la salida de los datos de las aplicaciones, incluyendo:

- Comprobaciones de la razonabilidad para probar si los datos de salida son plausibles.
- Control de conciliación de cuentas para asegurar el procesamiento de todos los datos.
- Provisión de información suficiente, para que el lector o sistema de procesamiento subsiguiente determine la exactitud, totalidad, precisión y clasificación de la información.
- Procedimientos para responder a las pruebas de validación de salidas.
- Definición de las responsabilidades de todo el personal involucrado en el proceso de salida de datos.

Control Software Operativo: Se definen los siguientes controles a realizar durante la implementación del software en producción, a fin de minimizar el riesgo de alteración de los sistemas.

- Toda aplicación, desarrollada por el Organismo o por un tercero tendrá un único responsable designado formalmente por el responsable del Área Informática.
- Ningún programador o analista de desarrollo y mantenimiento de aplicaciones podrá acceder a los ambientes de producción.
- El responsable del Área Informática, propondrá para su aprobación por parte del superior jerárquico que corresponda, la asignación de la función de "implementador" al personal de su área que considere adecuado, quien tendrá como funciones principales:
    - Coordinar la implementación de modificaciones o nuevos programas en el ambiente de Producción.
    - Asegurar que los sistemas aplicativos en uso, en el ambiente de Producción, sean los autorizados y aprobados de acuerdo a las normas y procedimientos vigentes.
    - Instalar las modificaciones, controlando previamente la recepción de la prueba aprobada por parte del Analista Responsable, del sector encargado del testeo y del usuario final.
    - Rechazar la implementación en caso de encontrar defectos y/o si faltara la documentación estándar establecida

14.2.2 Procedimiento de Control de Cambios

Para el ciclo de vida de desarrollo de software se deberá elaborar el procedimiento de gestión de cambios con el objeto de minimizar los riesgos de alteración de los sistemas de información. Esto garantizará que se cumplan los procedimientos de seguridad y control, respetando la división de funciones.

Para ello se deberá tomar las siguientes consideraciones:

- Verificar que los cambios sean propuestos por usuarios autorizados y respete los términos y condiciones que surjan de la licencia de uso.
- Mantener un registro de los niveles de autorización acordados.
- Solicitar la autorización del Propietario de la Información, en caso de tratarse de cambios a sistemas de procesamiento de la misma.
- Efectuar un análisis de riesgos del cambio.
- Determinar los requisitos de seguridad para el cambio.
- Analizar el impacto de los cambios sobre los controles de seguridad existentes.
- Obtener aprobación formal por parte del responsable del Área Informática para las tareas detalladas, antes que comiencen las tareas.
- Solicitar la revisión del Responsable de Seguridad de la Información para garantizar que no se violen los requerimientos de seguridad que debe cumplir el software.
- Efectuar las actividades relativas al cambio en el ambiente de desarrollo.

- Obtener la aprobación por parte del usuario autorizado y del área de pruebas mediante pruebas en el ambiente correspondiente.
- Actualizar la documentación para cada cambio implementado, tanto de los manuales de usuario como de la documentación operativa.
- Mantener un control de versiones para todas las actualizaciones de software.
- Garantizar que la implementación se llevará a cabo minimizando la discontinuidad de las actividades y sin alterar los procesos involucrados.
- Informar a las áreas usuarias antes de la implementación de un cambio que pueda afectar su operatoria.

14.2.3 Revisión después de cambios en los Sistemas Operativos

Deberán existir procedimientos de revisión y control para asegurar que no se produzca ningún impacto negativo en el funcionamiento o degradación, en la seguridad de las aplicaciones y sistemas que contiene, cuando se realicen cambios en los Sistemas Operativos por actualizaciones o instalación de componentes.

14.2.4 Restricción del Cambio de Paquetes de Software

Todo cambio en los paquetes de software suministrados por terceros deberá ser controlado de manera estricta. Para ello se deberá:

- Analizar los términos y condiciones de la licencia a fin de determinar si las modificaciones se encuentran autorizadas.
- Determinar la conveniencia de que la modificación sea aplicada o no.
- Evaluar el impacto que produciría el cambio.
- Retener una versión del software original realizando los cambios sobre una copia perfectamente identificada.

14.2.5 Principios de Arquitectura de Ingeniería Segura

Se deberán establecer, documentar, mantener y aplicar los principios de seguridad en ingeniería de sistemas para cualquier labor de implementación en los sistemas de información.

Se deberá diseñar contemplando la seguridad en todos los niveles de la arquitectura -negocios, datos, aplicaciones y tecnología- equilibrando la necesidad de seguridad con la de accesibilidad.

Se deberá analizar la tecnología nueva para conocer sus riesgos de seguridad antes de incluirse como parte del diseño.

14.2.6 Seguridad en los Entornos de Desarrollo

Se deberán implementar controles para proteger adecuadamente los entornos en los que se efectuarán labores de desarrollo e integración de software, abarcando todo el ciclo de vida del desarrollo del sistema y contemplando los recursos humanos, los procesos y las tecnologías asociadas. Dichos controles deberán considerar los siguientes aspectos:

- Segregación entre distintos entornos de desarrollo, según lo señalado en el punto 12.1.4. Separación de entornos de desarrollo, pruebas y producción.
- Seguridad en los datos de prueba y datos en producción que el sistema procesará, almacenará y transmitirá, según los puntos 14.3.1 Protección de los Datos de Prueba y 14.3.2 Cambios a Datos Operativos.
- Control de acceso al código fuente, según punto 9.4.8 Control de Acceso al Código Fuente.
- Monitoreo del cambio en el código y en el entorno que lo almacena, de acuerdo con los puntos 14.2.2 Procedimiento de Control de Cambios, 14.2.3 Revisión después de cambios en los Sistemas Operativos y 14.2.4 Restricción del Cambio de Paquetes de Software.
- Control de los aspectos de seguridad en el desarrollo de sistemas, incluidos en los puntos 14.2.5 Principios de Arquitectura de Ingeniería Segura y 14.2.9 Evaluación de Vulnerabilidades de Seguridad.
- Seguridad en la externalización asociado al desarrollo del sistema según las pautas del punto 14.2.7 Tercerización del Desarrollo de Software.
- Copias de respaldo según lo establecido en el punto 12.3.1 Copia de Resguardo y Restauración.

14.2.7 Tercerización del Desarrollo de Software

Se deberán establecer los requerimientos contractuales de calidad y seguridad del código que incluyan auditorías, una revisión del código para detectar código malicioso, como así también el cumplimiento de los requerimientos de desarrollo mencionados en el punto 14.2.1 Desarrollo Seguro de Software.

Se deberán elaborar acuerdos de licencias, propiedad de código y derechos conferidos.

Se deberá considerar el establecimiento de acuerdos de custodia del código fuente del software por parte de un tercero en caso de quiebra y/o inhabilidad por parte del proveedor del servicio de desarrollo de software.

14.2.8 Evaluación de Requisitos Funcionales

Se deberán establecer programas de ejecución de pruebas funcionales que permita evaluar los requisitos funcionales y el cumplimiento de estos en los sistemas desarrollados.

14.2.9 Evaluación de Vulnerabilidades de Seguridad

Se deberán realizar evaluaciones de seguridad en búsqueda de vulnerabilidades sobre los nuevos sistemas a implementar, sistemas de información utilizados, incluyendo desarrollos propios y de terceros, como también a las plataformas del sistema operativo sobre los cuales están implementados los mismos, con el objeto de detectar canales encubiertos de transmisión de datos no autorizados o cualquier otra vulnerabilidad que atente contra la seguridad.

14.3 Datos de Prueba y Operativos

14.3.1 Protección de los Datos de Prueba

Las pruebas de los sistemas desarrollados podrán efectuarse con datos extraídos del ambiente operativo con autorización previa si los mismos son despersonalizados y enmascarados antes de su uso para evitar exponer información que pueda ser sensible.

Los datos de prueba se deberán eliminar inmediatamente al finalizar las pruebas.

14.3.2 Cambios a Datos Operativos

La modificación, actualización o eliminación de los datos operativos deberán ser realizados, solo a través de los sistemas que procesan dichos datos y de acuerdo con el esquema de control de accesos implementado en los mismos. Cualquier modificación por fuera de los sistemas a un dato almacenado, ya sea en un archivo o base de datos, podría poner en riesgo la integridad de la información.

Todos los casos en los que no fuera posible la aplicación de esta política serán considerados como excepciones. El Responsable de Seguridad Informática es quien definirá los procedimientos para la gestión de dichas excepciones que deberán contemplar lo siguiente:

- Se generará una solicitud formal para la realización de la modificación, actualización o eliminación del dato.
- El Propietario de la Información afectada y el Responsable de Seguridad Informática aprobarán la ejecución del cambio evaluando las razones por las cuales se solicita.
- Se generarán cuentas de usuario de emergencia para ser utilizadas en la ejecución de excepciones. Las mismas serán protegidas mediante contraseñas, sujetas al procedimiento de administración de contraseñas críticas y habilitadas sólo ante un requerimiento de emergencia y por el lapso que ésta dure.
- Se designará un encargado de implementar los cambios, el cual no será personal del área de Desarrollo.
- Se registrarán todas las actividades realizadas con las cuentas de emergencia. Dicho registro será revisado posteriormente por el Responsable de Seguridad de Informática.

Av. Julio A. Roca 609, C1067ABB
Ciudad Autónoma de Buenos Aires, Argentina
Horario de atención de 9:30 a 16:00
ces@indec.gob.ar
Tel.: (54-11) 5031-4632
indec.gob.ar
INDECArgentina

15 Política en Relación a los Proveedores

Objetivo

Establecer y mantener el nivel acordado de seguridad de la información y prestación de los servicios conforme a los acuerdos con el proveedor.

15.1 Seguridad en las Relación con los Proveedores

15.1.1 Seguridad de la Información que es Accedida por los Proveedores

Se deberán documentar y acordar los requisitos de seguridad sobre los activos de información que son accedidos por los proveedores, con el objeto de mitigar los riesgos emergentes al tener acceso a la información y los recursos tecnológicos del Organismo.

Se deberán analizar y definir los riesgos en la provisión del servicio para establecer todos los requisitos de seguridad pertinentes. Para ello se deberá definir con cada proveedor, que información podrá acceder, procesar, almacenar o transmitir.

15.1.2 Seguridad dentro de los Acuerdos de los Proveedores

Se deberán establecer y documentar los acuerdos para garantizar que no existen discrepancias entre el Organismo y el proveedor en cuanto a las obligaciones de ambas partes para cumplir con los requisitos de seguridad de la información establecidos.

Se deberá identificar e incluir en los acuerdos de servicio (SLA) los mecanismos de seguridad, los niveles de servicio y los requisitos de administración de todos los servicios de red contratados a terceros.

A continuación, se definen los términos para incluir en los acuerdos con el fin de poder satisfacer los requisitos de seguridad de la información identificados:

a) Descripción de la información que se debe proporcionar o a la que se debe acceder y los métodos para proporcionar o acceder a la información.

b) Clasificación de la información de acuerdo con el esquema de clasificación del organismo; y si es necesario también realizar el mapeo entre el esquema propio del organismo y el esquema de clasificación del proveedor.

c) Requisitos legales y normativos, incluida la protección de datos personales, los derechos de propiedad intelectual y una descripción de sobre cómo se garantizará si se cumplen.

d) Obligación de cada parte contractual de implementar un conjunto de controles acordados incluido el control de acceso, la revisión de desempeño, el monitoreo, los informes y la auditoría.

e) Reglas de uso aceptable de la información, incluido en uso inaceptable en caso de ser necesario.

f) Una lista explícita del personal autorizado para acceder a/o recibir la información o los procedimientos o condiciones del organismo para su autorización, y el retiro de la autorización para el acceso a/o la recepción de la información del organismo al personal del proveedor.

g) Políticas de Seguridad de la Información pertinentes al contrato específico.

h) Requisitos y procedimientos de la administración de incidentes (en especial la notificación y la colaboración durante la remediación de incidentes).

i) Requisitos de capacitación y concientización para procedimientos específicos y requisitos de seguridad de la información, es decir, para la respuesta ante incidentes y procedimientos de autorización.

j) Normativas pertinentes para la subcontratación, incluidos los controles que se deben implementar.

k) Socios de acuerdos pertinentes, incluida una persona de contacto para los asuntos de seguridad de la información.

l) Requisitos de selección, si existe alguno, para el personal del proveedor para realizar los procedimientos de selección y notificación si no se ha completado la selección o si los resultados dan pie a dudas o inquietudes.

m) Derecho a auditar los procesos y los controles del proveedor relacionados al acuerdo.

n) Procesos de resolución de defectos y resolución de conflictos.

o) Obligación del proveedor a entregar periódicamente un informe independiente sobre la efectividad de los controles y un acuerdo sobre la corrección oportuna de los asuntos pertinentes indicados en el informe.

p) Obligaciones del proveedor para cumplir con la Política de Seguridad de la Información y demás requisitos de seguridad del organismo.

15.1.3 Cadena de suministro de la tecnología de información y comunicación

Se deben incluir en los acuerdos con los proveedores los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones.

Se deben incluir los siguientes temas en los acuerdos con el proveedor sobre la seguridad de la cadena de suministro:

a) Definir los requisitos de seguridad de la información que se aplicarán a la adquisición de tecnologías, productos o servicios de información y comunicación además de los requisitos de seguridad de la información para las relaciones con el proveedor;

b) Para los servicios de tecnología de información y comunicación que requieren que los usuarios propaguen los requisitos de seguridad del organismo en toda la cadena de suministro si los proveedores realizan subcontrataciones para partes del servicio de tecnología de información y comunicación proporcionados al organismo;

Av. Julio A. Roca 609, C1067ABB
Ciudad Autónoma de Buenos Aires, Argentina
Horario de atención de 9:30 a 16:00
ces@indec.gob.ar
Tel.: (54-11) 5031-4632
www indec.gob.ar
INDECArgentina

c) Para los productos de tecnología de información y comunicación que requieren que los proveedores propaguen las prácticas de seguridad correspondientes a través de toda la cadena de suministro si estos productos incluyen componentes comprados a otros proveedores;

d) Implementación de un proceso de monitoreo y métodos aceptables para validar que los productos y servicios de tecnología de información y comunicación se adhieren a los requisitos de seguridad establecidos;

e) Implementación de un proceso para identificar los componentes de los productos o servicios que son fundamentales para mantener la funcionalidad y que, por lo tanto, requiere una mayor atención y escrutinio cuando se desarrollan fuera del organismo, especialmente si el proveedor del nivel superior externalice los aspectos de los componentes de productos o servicios a otros proveedores;

f) Obtención de una garantía de que los componentes críticos y su origen se pueden rastrear en toda la cadena de suministros;

g) Obtener la garantía de que los productos de tecnología de información y comunicación entregados funcionan según lo esperado sin ninguna función inesperada o no deseada;

h) Definición de las reglas para compartir la información en cuanto a la cadena de suministro y cualquier posible problema y compromiso entre el organismo y los proveedores;

i) Implementación de procesos específicos para administrar el ciclo de vida de los componentes de tecnología de información y comunicación junto con la disponibilidad y los riesgos de seguridad asociados. Esto incluye los riesgos de los componentes que ya no están disponibles debido a que los proveedores ya no están en el negocio o a que ya no proporcionan estos componentes debido a los avances de la tecnología.

15.2 Administración de la Prestación de Servicios de Proveedores

15.2.1 Supervisión y Revisión de los Servicios

Se deberá llevar a cabo el seguimiento, control y revisión de los servicios prestados por terceras partes, comprobando que se encuentran adheridos a los términos de seguridad de la información con las condiciones definidas en los acuerdos y que los incidentes de seguridad de la información y los problemas sean manejados en forma apropiada.

Se recomienda que la organización asegure que se mantenga la visibilidad de las actividades de seguridad como gestión de cambios, identificación de vulnerabilidades y reporte/respuesta de incidentes de seguridad de información a través de un proceso de reportes claro y definido, con formato y estructura.

15.2.2 Gestión de Cambios en la Prestación de Servicios

Se deberá llevar la gestión de cambios en la provisión de los servicios, incluyendo el mantenimiento y las mejoras de los procedimientos y controles de seguridad de la información existentes.

El proceso de gestión de servicios de terceros deberá tener en cuenta los siguientes cambios en el Organismo:

- Actualización de las políticas y procedimientos del Organismo
- Actualización de los servicios ofrecidos por del Organismo.
- Actualización de aplicaciones o nuevos sistemas.
- Implementación de nuevos controles de la Seguridad de la Información.

El proceso de gestión deberá, también tener en cuenta los siguientes cambios en el servicio ofrecido por el proveedor:

- Cambios y mejoras de las redes.
- Uso de nuevas tecnologías.
- Adopción de nuevos productos o nuevas versiones/publicaciones.
- Nuevas herramientas de desarrollo y ambientes.
- Cambios de las ubicaciones físicas de las instalaciones de servicio.
- Cambio de los proveedores.

16 Política de Gestión de Incidentes de Seguridad

Objetivo

Garantizar que los eventos de seguridad de la información y las debilidades asociados a los sistemas de información sean comunicados de forma tal que se apliquen las acciones correctivas en el tiempo oportuno.

16.1 Gestión de Incidentes de Seguridad y Mejoras

16.1.1 Responsabilidades y Procedimientos

Se establecerán claramente las responsabilidades y los procedimientos para el manejo de incidentes con el fin de garantizar una respuesta rápida, eficaz y sistemática a los incidentes relativos a la seguridad de la información.

Se deberá contemplar la incorporación en los procedimientos de incidentes de seguridad una definición de las primeras medidas a implementar como ser, identificación, clasificación y análisis de la causa del incidente, la planificación de la solución y recupero de los sistemas afectados, la comunicación formal de las áreas afectadas y la notificación formal al Comité de Seguridad y a la Dirección de Asuntos Jurídicos si fuera necesario.

Seguridad Informática tendrá la autoridad para acceder a todo equipamiento tecnológico involucrado en alertas de seguridad cuando considere que dicho incidente pudiera afectar la disponibilidad, confidencialidad o integridad de la información o los recursos tecnológico del Organismo.

16.1.2 Notificación de los eventos de seguridad de la información

Los incidentes relativos a la seguridad deberán ser comunicados tan pronto como sean detectados mediante el registro de estos en los canales formales siguiendo el procedimiento establecido.

Cuando las áreas usuarias detectasen un incidente de seguridad deberán comunicarlo inmediatamente a la Coordinación de Seguridad Informática, quien procederá a dar respuesta al incidente de seguridad informado.

Se establecerá un procedimiento formal de comunicación y respuesta a incidentes, indicando la acción que ha de emprenderse al recibir un informe sobre incidentes.

Dicho procedimiento deberá contemplar que, ante la detección de un supuesto incidente o violación de la seguridad, el Responsable de Seguridad de la Información sea informado tan pronto como se haya tomado conocimiento. Este indicará los recursos necesarios para la investigación y resolución del incidente, y se encargará de su monitoreo.

Asimismo, se comunicará de manera continua al Comité de Seguridad respecto de la ocurrencia de incidentes de seguridad.

Av. Julio A. Roca 609, C1067ABB
Ciudad Autónoma de Buenos Aires, Argentina
Horario de atención de 9:30 a 16:00
ces@indec.gob.ar
Tel.: (54-11) 5031-4632
www indec.gob.ar
INDECArgentina

Todos los empleados, sea cual fuere su situación contractual, deberán conocer fehacientemente el procedimiento de comunicación de incidentes de seguridad y deben informar los mismos tan pronto hayan tomado conocimiento de su ocurrencia.

16.1.3 Notificación de puntos débiles de la seguridad

Todos los usuarios de los servicios de información del Organismo que detectasen fallas o debilidades de seguridad, o tomasen conocimiento indirectamente acerca de la existencia de ellas, serán responsables de comunicarlo formalmente a la Coordinación de Seguridad Informática.

Está expresamente prohibido que los usuarios ajenos a la Coordinación de Seguridad Informática realicen pruebas para detectar y/o explotar supuestas debilidades o fallas de seguridad.

16.1.4 Comunicación de Anomalías del Software Instalado

Todos los usuarios de los servicios de información del Organismo que detectasen anomalías del software en uso deberán comunicarlo formalmente a la Coordinación de Seguridad Informática, para determinar si la misma califica como un incidente de seguridad informática o no.

16.1.5 Valoración de los eventos de seguridad

Deberá existir un procedimiento de evaluación de los eventos de seguridad que permita decidir si el evento clasificará como incidente de seguridad de la información.

Se deberán registrar los resultados de la evaluación y la decisión en detalle con fines de referencia y verificación futuros.

16.1.6 Respuesta a los incidentes de seguridad

Todo incidente de seguridad deberá ser respondido siguiendo los procedimientos establecidos.

Dicho procedimiento de respuesta al incidente de seguridad debería incluir:

a) Recopilar la evidencia lo más pronto posible, posterior a la ocurrencia del incidente.

b) Realizar análisis forenses, en concordancia con el punto 16.1.8 Recopilación de evidencias.

c) Asegurarse de que todas las actividades de respuesta se realicen correctamente para el posterior análisis.

d) Comunicar de la existencia del incidente de seguridad de la información o cualquier detalle pertinente a todas las personas y áreas con un incumbencia y necesidad de saber.

e) Notificar al Comité de Seguridad ante el escalamiento del incidente de seguridad.

f) Cerrar y registrar formalmente el incidente, una vez gestionado correctamente el mismo.

Restablecido el normal funcionamiento y reanudado el nivel de seguridad normal se deberá realizar un análisis post-incidente, cuando sea necesario, para profundizar el análisis o confirmación del origen del mismo.

16.1.7 Aprendizaje de los incidentes de la seguridad

Se deberán documentar, cuantificar y monitorear los tipos, volúmenes y costos de las anomalías e incidentes de seguridad. Esta información se utilizará para identificar y evaluar aquellos que sean recurrentes o de alto impacto. A efectos de establecer la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de casos futuros similares.

16.1.8 Recopilación de evidencias

Se deberán definir procedimientos para la identificación, recopilación, adquisición y preservación de la información que pudiera servir como evidencia válida, ya sea para implementar una medida disciplinaria interna o iniciar una acción legal.

Para lograr la validez de la evidencia, el Organismo deberá garantizar que sus sistemas de información cumplen con la normativa y los estándares o códigos de práctica relativos a la producción de evidencia válida, como también se deberá asegurar la disponibilidad de los recursos tecnológicos necesarios para la recopilación, adquisición y preservación de evidencia forense.

Para lograr la calidad y totalidad de la evidencia es necesario la solidez de esta, por lo cual se establecerá los siguientes requisitos:

a) Almacenar los documentos en papel originales en forma segura y mantener registros acerca de quién lo halló, dónde se halló, cuándo se halló y quién presenció el hallazgo. Cualquier investigación debe garantizar que los originales no sean alterados.

b) Copiar la información para garantizar su disponibilidad. Se mantendrá un registro de todas las acciones realizadas durante el proceso de copia. Se almacenará en forma segura una copia de los medios y del registro.

Cuando se detecta un incidente, puede no resultar obvio si éste derivará en una demanda legal, por lo tanto, se deberán tomar todos los recaudos establecidos para la obtención y preservación de la evidencia.

Se debe tener presente lo dispuesto por el Reglamento de Investigaciones Administrativas, procedimiento administrativo especial, de naturaleza correctiva interna que constituye garantía suficiente para la protección de los derechos y correcto ejercicio de las responsabilidades impuestas a los agentes públicos. Este Decreto debe ser complementado por lo dispuesto en la Ley N° 19.549 (Ley de Procedimientos Administrativos) y por toda otra normativa aplicable, incluido el Código Penal, el que sanciona a quien sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público (Art. 255).

Av. Julio A. Roca 609, C1067ABB
Ciudad Autónoma de Buenos Aires, Argentina
Horario de atención de 9:30 a 16:00

ces@indec.gob.ar
Tel.: (54-11) 5031-4632

www indec.gob.ar

INDECArgentina

17 Política de Gestión de la Continuidad

Objetivo

Minimizar los efectos de las posibles interrupciones de las actividades normales del Organismo (sean éstas resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.

Analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro.

Maximizar la efectividad de las operaciones de contingencia del Organismo con el establecimiento de planes que incluyan al menos las siguientes etapas:

a) Notificación/Activación: Consistente en la detección y determinación del daño y la activación del plan.

b) Reanudación: Consistente en la restauración temporal de las operaciones y recuperación del daño producido al sistema original.

c) Recuperación: Consistente en la restauración de las capacidades de proceso del sistema a las condiciones de operación normales.

Asegurar la coordinación con el personal del Organismo y los contactos externos que participarán en las estrategias de planificación de contingencias. Asignar funciones para cada actividad definida.

17.1 Gestión de Continuidad de las Operaciones

17.1.1 Proceso de Administración de los Planes de Continuidad

Deberá existir un plan de contingencia, para actuar ante la interrupción de la continuidad de las operaciones en el Organismo, a fin de garantizar que los planes operativos de restauración de las operaciones sean ordenados y consistentes entre sí.

El proceso de administración de la continuidad de la operatoria deberá tener en cuenta:

a) Identificar y priorizar los procesos críticos de las actividades del Organismo.

b) Asegurar que todos los integrantes del Organismo comprendan los riesgos que la misma enfrenta, en términos de probabilidad de ocurrencia e impacto de posibles amenazas, así como los efectos que una interrupción puede tener en la actividad del Organismo.

c) Elaborar y documentar una estrategia de continuidad de las actividades del Organismo consecuente con los objetivos y prioridades acordados.

d) Proponer planes de continuidad de las actividades del Organismo de conformidad con la estrategia de continuidad acordada.

e) Establecer un cronograma de pruebas periódicas de cada uno de los planes de contingencia, proponiendo una asignación de funciones para su cumplimiento.

f) Coordinar actualizaciones periódicas de los planes y procesos implementados.

g) Considerar la contratación de seguros que podrían formar parte del proceso de continuidad de las actividades del Organismo.

h) Proponer las modificaciones a los planes de contingencia.

17.1.2 Continuidad de las Actividades y Análisis de los impactos

Al establecer un Plan de Continuidad de las Actividades del Organismo se deberán contemplar los siguientes puntos:

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

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

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

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

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

17.1.3 Elaboración e implementación de los planes de continuidad de las Actividades del Organismo

Los propietarios de procesos y recursos de información, con la asistencia del Responsable de Seguridad Informática, elaborarán los planes de contingencia necesarios para garantizar la continuidad de las actividades del Organismo.

El proceso de planificación de la continuidad de las actividades considerará los siguientes puntos:

a) Identificar y acordar respecto a todas las funciones y procedimientos de emergencia.

b) Analizar los posibles escenarios de contingencia y definir las acciones correctivas a implementar en cada caso.

c) Implementar procedimientos de emergencia para permitir la recuperación y restablecimiento en los plazos requeridos. Se debe dedicar especial atención a la evaluación de las dependencias de actividades externas y a los contratos vigentes.

d) Documentar los procedimientos y procesos acordados.

e) Instruir adecuadamente al personal, en materia de procedimientos y procesos de emergencia acordados, incluyendo el manejo de crisis.

f) Instruir al personal involucrado en los procedimientos de reanudación y recuperación en los siguientes temas:

- Objetivo del plan.
- Mecanismos de coordinación y comunicación entre equipos (personal involucrado).
- Procedimientos de divulgación.
- Requisitos de la seguridad.
- Procesos específicos para el personal involucrado.
- Responsabilidades individuales.

g) Probar y actualizar los planes, guardando evidencia formal de las pruebas y sus resultados.

Asimismo, el proceso de planificación debe concentrarse en los objetivos de las actividades requeridas del organismo, por ejemplo, restablecimiento de los servicios a los usuarios en un plazo aceptable. Deben considerarse los servicios y recursos que permitirán que esto ocurra, incluyendo, dotación de personal, recursos que no procesan información, así como acuerdos para reanudación de emergencia en sitios alternativos de procesamiento de la información.

17.1.4 Marco para la Planificación de la Continuidad de las Actividades del Organismo

Se mantendrá un solo marco para los planes de continuidad de las actividades del Organismo, a fin de garantizar que los mismos sean uniformes e identificar prioridades de prueba y mantenimiento.

Cada plan de continuidad especificará claramente las condiciones para su puesta en marcha, así como las personas a cargo de ejecutar cada componente del mismo. Cuando se identifiquen nuevos requerimientos, se modificarán los procedimientos de emergencia establecidos, por ejemplo, los planes de evacuación o los recursos de emergencia existentes.

El administrador de cada plan de continuidad será el encargado de coordinar las tareas definidas en el mismo.

Estas modificaciones deben ser propuestas por el Comité de Seguridad de la Información para su aprobación.

El marco para la planificación de la continuidad de las actividades del Organismo tendrá en cuenta los siguientes puntos:

Av. Julio A. Roca 609, C1067ABB
Ciudad Autónoma de Buenos Aires, Argentina
Horario de atención de 9:30 a 16:00
ces@indec.gob.ar
Tel.: (54-11) 5031-4632
www indec.gob.ar
INDECArgentina

a) Prever las condiciones de implementación de los planes que describan el proceso a seguir (cómo evaluar la situación, qué personas estarán involucradas, etc.) antes de poner en marcha los mismos.

b) Definir los procedimientos de emergencia que describan las acciones a emprender una vez ocurrido un incidente que ponga en peligro las operaciones del Organismo y/o la vida humana. Esto debe incluir disposiciones con respecto a la gestión de las relaciones públicas y a vínculos eficaces a establecer con las autoridades pertinentes, por ejemplo, la policía, bomberos y autoridades locales.

c) Realizar los procedimientos de emergencia que describan las acciones a emprender para el traslado de actividades esenciales del Organismo o de servicios de soporte a ubicaciones transitorias alternativas, y para el restablecimiento de los procesos en los plazos requeridos.

d) Redactar los procedimientos de recuperación que describan las acciones a emprender para restablecer las operaciones normales del Organismo.

e) Definir un cronograma de mantenimiento que especifique cómo y cuándo será probado el plan, y el proceso para el mantenimiento del mismo.

f) Efectuar actividades de concientización e instrucción al personal, diseñadas para propiciar la comprensión de los procesos de continuidad las actividades y garantizar que los procesos sigan siendo eficaces.

g) Documentar las responsabilidades y funciones de las personas, describiendo los responsables de la ejecución de cada uno de los componentes del plan y las vías de contacto posibles. Se deben mencionar alternativas cuando corresponda. Es de suma importancia definir a un responsable de declarar el estado de contingencia, lo cual dará inicio al plan.

Se deberán definir explícitamente los administradores de los planes de contingencia.

El cumplimiento de los procedimientos implementados para llevar a cabo las acciones contempladas en cada plan de continuidad, deben contarse entre las responsabilidades de los administradores de cada plan. Las disposiciones de emergencia para servicios técnicos alternativos, como instalaciones de comunicaciones o de procesamiento de información, normalmente se cuentan entre las responsabilidades de los proveedores de servicios.

17.1.5 Ensayo, Mantenimiento y Reevaluación de los Planes de continuidad del Organismo

Debido a que los planes de continuidad de las actividades del Organismo pueden fallar, por suposiciones incorrectas, errores o cambios en el equipamiento, se establecen las siguientes pautas de acción:

- El Comité de Seguridad de la Información establecerá un cronograma de pruebas periódicas de cada uno de los planes de contingencia.
- El cronograma indicará quienes son los responsables de llevar a cabo cada una de las pruebas y de elevar el resultado obtenido al citado Comité.

Av. Julio A. Roca 609, C1067ABB
Ciudad Autónoma de Buenos Aires, Argentina
Horario de atención de 9:30 a 16:00
ces@indec.gob.ar
Tel.: (54-11) 5031-4632
www indec.gob.ar
INDECArgentina

Se deben utilizar diversas técnicas para garantizar que los planes de contingencia funcionarán ante un hecho real, y éstas incluirán por lo menos:

a) Efectuar pruebas de discusión de diversos escenarios (discutiendo medidas para la recuperación las actividades utilizando ejemplos de interrupciones).

b) Realizar simulaciones (especialmente para entrenar al personal en el desempeño de sus roles de gestión posterior a incidentes o crisis).

c) Efectuar pruebas de recuperación técnica (garantizando que los sistemas de información puedan ser restablecidos con eficacia).

d) Realizar ensayos completos probando que el Organismo, el personal, el equipamiento, las instalaciones y los procesos pueden afrontar las interrupciones.

Para las operaciones críticas del Organismo se tomarán en cuenta, además, los siguientes mecanismos:

a) Efectuar pruebas de recuperación en un sitio alternativo (ejecutando los procesos de las actividades del Organismo en paralelo, con operaciones de recuperación fuera del sitio principal).

b) Realizar pruebas de instalaciones y servicios de proveedores (garantizando que los productos y servicios de proveedores externos cumplan con los compromisos contraídos).

Todas las pruebas efectuadas deben ser documentadas, resguardándose la evidencia formal de la ejecución y de los resultados obtenidos.

Los planes de continuidad de las actividades del Organismo serán revisados y actualizados periódicamente, para garantizar su eficacia permanente. Se incluirán procedimientos en el programa de administración de cambios del Organismo para garantizar que se aborden adecuadamente los tópicos de continuidad de las actividades.

Se deberá definir la periodicidad de revisión de los planes de contingencia es la siguiente, indicando el nombre del plan de contingencia, responsable y periodicidad de revisión.

Cada uno de los Responsables de Procesos es el responsable de las revisiones periódicas de cada uno de los planes de continuidad de su incumbencia, como así también de la identificación de cambios en las disposiciones relativas a las actividades del Organismo aún no reflejadas en dichos planes.

Debe prestarse atención, especialmente, a los cambios de:

- Personal.
- Direcciones o números telefónicos.
- Estrategia del Organismo.
- Ubicación, instalaciones y recursos.
- Legislación.
- Contratistas, proveedores y clientes críticos.
- Procesos, o procesos nuevos / eliminados.

- Tecnologías.
- Requisitos operacionales.
- Requisitos de seguridad.
- Hardware, software y otros equipos (tipos, especificaciones, y cantidad).
- Requerimientos de los sitios alternativos.
- Registros de datos vitales.

Todas las modificaciones efectuadas serán propuestas por el Comité de Seguridad de la Información para su aprobación por el superior jerárquico que corresponda.

Por otra parte, el resultado de este proceso será dado a conocer a fin de que todo el Personal involucrado tenga conocimiento de los cambios incorporados.

17.2 Redundancia

17.2.1 Redundancia en las Instalaciones de Procesamiento y Transmisión de la Información

Se deberá implementar en las instalaciones de procesamiento y transmisión de la información, componentes y/o arquitecturas redundantes, a efectos de cumplir con los requisitos de disponibilidad operativa.

Av. Julio A. Roca 609, C1067ABB
Ciudad Autónoma de Buenos Aires, Argentina
Horario de atención de 9:30 a 16:00
ces@indec.gob.ar
Tel.: (54-11) 5031-4632
www indec.gob.ar
INDECArgentina

18 Política de Cumplimiento

Objetivos

Cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas al Organismo y/o al empleado o que incurran en responsabilidad civil o penal como resultado de su incumplimiento.

Garantizar que los sistemas cumplan con la política, normas y procedimientos de seguridad del Organismo.

Revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información.

Optimizar la eficacia del proceso de auditoría de sistemas y minimizar los problemas que pudiera ocasionar el mismo, o los obstáculos que pudieran afectarlo.

Garantizar la existencia de controles que protejan los sistemas en producción y las herramientas de auditoría en el transcurso de las auditorías de sistemas.

Determinar los plazos para el mantenimiento de información y para la recolección de evidencia del Organismo.

18.1 Cumplimiento de Requisitos Legales

18.1.1 Identificación de la Legislación Aplicable

Se deberán identificar y documentar en los sistemas de información del Organismo los requisitos normativos, contractuales o legales. Del mismo modo se deberá definir y documentar los controles específicos, las responsabilidades y funciones individuales para cumplir con dichos requisitos.

18.1.2 Derechos de Propiedad Intelectual

Se deberá garantizar el cumplimiento de los requisitos legales y contractuales relacionados con la instalación y uso de software protegido por la legislación relativa a la propiedad intelectual.

Los empleados podrán utilizar únicamente material autorizado por el Organismo. El Organismo solo podrá autorizar el uso de material producido por el mismo, o material autorizado o suministrado por su titular, conforme los términos y condiciones acordadas y lo dispuesto por la normativa vigente.

La infracción a estos derechos puede tener como resultado acciones que podrían iniciar sumarios administrativos internos, hasta acciones legales que podrían derivar en demandas penales, por infracción a la Ley de Propiedad Intelectual N° 11.723, ya que el software es considerado una obra intelectual que goza de la protección de dicha ley.

Los usuarios solo podrán utilizar software autorizado por el Organismo según las condiciones de instalación descriptas en el punto 12.6.2 Restricciones en la Instalación de Software

18.1.3 Protección de los Registros del Organismo

Los registros de datos se deberán proteger contra pérdida, destrucción, acceso no autorizado, publicación no autorizada, degradación del medio de almacenamiento, obsolescencia del formato o medio de almacenamiento.

Los registros de datos, correspondientes a las cuentas de correos electrónicos no deberán ser eliminadas cuando el propietario de dicha cuenta fuera desvinculado del Organismo, sino que deberán ser almacenados por un período mínimo de diez años.

Los sistemas de almacenamiento de datos deberán ser seleccionados de modo tal que los datos requeridos puedan recuperarse de una manera aceptable ante requerimiento de un tribunal de justicia.

Se deberá clasificar y detallar los períodos de retención, medios de almacenamiento y responsables de su mantenimiento.

Los sistemas de almacenamiento y manipulación deberán garantizar una clara identificación de los registros y de su período de retención legal o normativa.

La protección de los datos deberá ser garantizada por el documento “Acuerdo de Confidencialidad”.

Asimismo, los funcionarios o empleados que revelen a terceros o utilicen en provecho propio cualquier información individual de carácter estadístico o censal, de la cual tengan conocimiento por sus funciones, o que incurran dolosamente en tergiversación, omisión o adulteración de datos de los censos o estadísticas, serán pasibles a acciones penales por infracción a la Ley 17.622.

18.1.4 Protección de Datos y Privacidad de la Información Personal

A través de la presente “Política de Seguridad de la Información” y la “Política de Uso Aceptable de los Recursos de Tecnología de la Información” se informarán y detallarán las actividades que serán objeto de control y monitoreo, a fin de no violar el derecho a la privacidad del empleado.

Todos los empleados deben conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan conocimiento con motivo del ejercicio de sus funciones. Por lo cual el Organismo poseerá un “Acuerdo de Confidencialidad”, el cual deberá ser suscrito por todos los funcionarios públicos y contratistas, en concordancia con el punto 6.1.6 Acuerdo de confidencialidad.

18.1.5 Prevención del Uso Inadecuado de los Recursos de Procesamiento de Información

Toda utilización de los recursos de procesamiento de información, con propósitos no autorizados o ajenos al destino por el cual fueron provistos se considerará como uso indebido.

Todos los empleados deberán conocer el alcance preciso del uso adecuado de los recursos informáticos y deberán respetarlo, según se declara en la Política de Uso Aceptable de los Recursos de Tecnología de la Información.

En particular, se deberá respetar lo dispuesto por las siguientes normas:

- Ética en el Ejercicio de la Función Pública. Ley 25.188: Establece que las personas que se desempeñen en la función pública deben proteger y conservar la propiedad del Estado y sólo emplear sus bienes con los fines autorizados.
- Código de Ética de la Función Pública: Dispone que el funcionario público debe proteger y conservar los bienes del Estado y utilizar los que le fueran asignados para el desempeño de sus funciones de manera racional, evitando su abuso, derroche o desaprovechamiento.
- Código Penal Art. 255: Sanciona a quien sustrajere, ocultare, destruyere o inutilizare objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario o de otra persona en el interés del servicio público. Si el culpable fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo.
- Ley N° 24.624. Artículo 30: Autoriza el archivo y la conservación en soporte electrónico u óptico indeleble de la documentación financiera, de personal y de control de la Administración Pública Nacional y otorga valor jurídico y probatorio a la documentación existente que se incorpore al Archivo General de la Administración, mediante la utilización de tecnología que garantice la estabilidad, perdurabilidad, inmutabilidad e inalterabilidad del soporte de guarda físico de la mencionada documentación.
- Decisión Administrativa 43/96: Reglamenta el Art. 30 de la Ley 24.624. Determina su ámbito de aplicación, define conceptos y precisa los requisitos de carácter general, los relacionados con los documentos en particular y con el soporte a utilizar en la redacción, producción o reproducción de aquellos.
- Ley de Propiedad Intelectual N° 11.723: Protege los derechos de autor de las obras científicas, literarias y artísticas, incluyendo las compilaciones de datos o de otros materiales.
- Ley N° 25.506: Establece que la exigencia legal de conservar documentos, registros o datos también queda satisfecha con la conservación de los correspondientes documentos digitales firmados digitalmente, según los procedimientos que determine la reglamentación, siempre que sean accesibles para su posterior consulta y permitan determinar fehacientemente el origen, destino, fecha y hora de su generación, envío y/o recepción.
- Código Penal: Sanciona a aquel que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos (Art. 183).

Av. Julio A. Roca 609, C1067ABB
Ciudad Autónoma de Buenos Aires, Argentina
Horario de atención de 9:30 a 16:00
ces@indec.gob.ar
Tel.: (54-11) 5031-4632
www indec.gob.ar
INDECArgentina

18.1.6 Delitos Informáticos

Todos los empleados deberán conocer la existencia de la Ley 26.388 de Delitos Informáticos, la cual, a partir de su promulgación, castiga penalmente ciertas conductas cometidas mediante medios informáticos.

Cabe señalar que la mayoría de las conductas descritas por dicha norma vinculada ya han sido señaladas en los apartados precedentes.

18.2 Revisiones de Cumplimiento de Seguridad

18.2.1 Revisión independiente de la Seguridad de la Información

Deberán efectuarse revisiones independientes de seguridad, para garantizar la eficacia de la implementación de seguridad existente. Esta revisión será independiente a la Coordinación de Seguridad Informática y permitirá incluir oportunidades de mejora en los objetivos de control y cambios en el enfoque de seguridad existente.

Dicha revisión deberá ser realizada por individuos independientes a la Coordinación de Seguridad Informática, por ejemplo, Auditoría Interna o Especialistas de Seguridad externos al Organismo.

18.2.2 Cumplimiento de la Política y Procedimientos de Seguridad

Los responsables de cada Dirección, dentro de su área de responsabilidad, deberán velar por el correcto cumplimiento de las normas y procedimientos de seguridad establecidos y brindarán apoyo a las revisiones de cumplimiento, efectuadas por la Coordinación de Seguridad Informática.

La Coordinación de Seguridad Informática, tendrá la autoridad de realizar revisiones periódicas en todas las áreas del Organismo a efectos de garantizar el cumplimiento de las políticas, normas y procedimientos de seguridad vigentes.

18.2.3 Verificación de Cumplimiento en los Sistemas de Información

Se verificará periódicamente que los sistemas de información cumplan con la política, normas y procedimientos de seguridad, las que incluirán la revisión de los sistemas en producción a fin de garantizar que los controles de hardware y software hayan sido correctamente implementados. En caso de ser necesario, estas revisiones contemplarán la asistencia técnica especializada.

El resultado de la evaluación se volcará en un informe técnico para su ulterior interpretación por parte de los especialistas. Para ello, la tarea podrá ser realizada por un profesional experimentado (en forma manual o con el apoyo de herramientas de software), o por un paquete de software automatizado que genere reportes que serán interpretados por un especialista técnico.

La verificación del cumplimiento comprenderá pruebas de penetración y tendrá como objetivo la detección de vulnerabilidades en el sistema y la verificación de la eficacia de los controles con relación a la prevención de accesos no autorizados. Se tomarán los recaudos necesarios en el caso de pruebas de penetración exitosas que comprometan la seguridad del sistema.

Las verificaciones de cumplimiento sólo serán realizadas por personas competentes, formalmente autorizadas y bajo la supervisión.

República Argentina - Poder Ejecutivo Nacional
2020 - Año del General Manuel Belgrano

Hoja Adicional de Firmas
Informe gráfico

Número: IF-2020-78943740-APN-DI#INDEC

CIUDAD DE BUENOS AIRES
Lunes 16 de Noviembre de 2020

Referencia: PSI - INDEC.-

El documento fue importado por el sistema GEDO con un total de 92 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2020.11.16 16:12:39 -03:00

Gabriel Alejandro Serralta
Director
Dirección de Informática
Instituto Nacional de Estadística y Censos

Digitally signed by Gestion Documental Electronica
Date: 2020.11.16 16:12:40 -03:00