República Argentina - Poder Ejecutivo Nacional
AÑO DE LA DEFENSA DE LA VIDA, LA LIBERTAD Y LA PROPIEDAD

Resolución

Número: RESOL-2024-431-APN-SSN#MEC

CIUDAD DE BUENOS AIRES
Lunes 2 de Septiembre de 2024

Referencia: EX-2024-85930360-APN-GA#SSN - POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

VISTO el Expediente EX-2024-85930360-APN-GA#SSN, la Ley N° 20.091, la Decisión Administrativa N° 641 de fecha 25 de junio de 2021, la Disposición de la DIRECCIÓN NACIONAL DE CIBERSEGURIDAD N° 1 de fecha 14 de febrero de 2022, las Resoluciones RESOL-2022-677-APN-SSN#MEC de fecha 27 de septiembre y RESOL-2023-31-APN-SSN#MEC de fecha 17 de enero, y

CONSIDERANDO:

Que la Decisión Administrativa N° 641 de fecha 25 de junio de 2021 aprobó los “Requisitos Mínimos de Seguridad de la Información para los Organismos del Sector Público Nacional", aplicables a todas las entidades y jurisdicciones comprendidas en el inciso a) del artículo 8° de la Ley N° 24.156.

Que la aprobación de una Política de Seguridad de la Información por la máxima autoridad del Organismo o por el funcionario a quien se le haya delegado la función, así como su revisión anual y eventual actualización, forman parte de los requisitos mínimos que debe cumplir el Organismo en virtud de la norma citada en el párrafo anterior (Anexo I, Directriz N° 1).

Que por Disposición de la DIRECCIÓN NACIONAL DE CIBERSEGURIDAD N° 1 de fecha 14 de febrero de 2022 se aprobó el “Modelo Referencial de Política de Seguridad de la Información”.

Que por Resolución RESOL-2022-677-APN-SSN#MEC de fecha 27 de septiembre se creó el Comité de Seguridad de la Información, al que se le asignó, entre otras funciones, la de proponer a la máxima autoridad del Organismo para su aprobación la Política de Seguridad de la Información, sus modificatorias y documentos derivados.

Que por Resolución RESOL-2023-31-APN-SSN#MEC de fecha 17 de enero se aprobó la Política de Seguridad de la Información del Organismo.

Que en cumplimiento del deber de revisión anual de dicha política, se advirtió la necesidad de su actualización y ampliación.

Que el 8 de agosto de 2024 el Comité de Seguridad de la Información acordó poner a disposición para su aprobación el documento actualizado y consolidado de Políticas de Seguridad de la Información.

Que la Gerencia de Asuntos Jurídicos ha dictaminado en el marco de su competencia.

Que la presente se dicta en uso de las facultades previstas en el artículo 67 de la Ley N° 20.091.

Por ello,

EL SUPERINTENDENTE DE SEGUROS DE LA NACIÓN

RESUELVE:

ARTÍCULO 1º.- Apruébase la “Política de Seguridad de la Información” que como Anexo IF-2024-87142162-APN-GCG#SSN integra la presente medida.

ARTÍCULO 2º.- Deróguese la Resolución RESOL-2023-31-APN-SSN#MEC de fecha 17 de enero.

ARTÍCULO 3°.- Notifíquese a la DIRECCIÓN NACIONAL DE CIBERSEGURIDAD dependiente de la SUBSECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES de la SECRETARÍA DE INNOVACIÓN, CIENCIA Y TECNOLOGÍA de la JEFATURA DE GABINETE, publíquese, dese a la DIRECCIÓN NACIONAL DEL REGISTRO OFICIAL y archívese.

Digitally signed by PLATE Guillermo Pedro
Date: 2024.09.02 16:44:29 ART
Location: Ciudad Autónoma de Buenos Aires

Guillermo Plate
Superintendente
Superintendencia de Seguros de la Nación

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2024.09.02 16:44:31 -03:00

Ministerio de Economía
República Argentina

SSN | SUPERINTENDENCIA DE SEGUROS DE LA NACIÓN

Política de seguridad de la Información

IF-2024-87142162-APN-GCG#SSN

ÍNDICE

INTRODUCCIÓN

La SUPERINTENDENCIA DE SEGUROS DE LA NACIÓN (SSN) reconoce que la información es un activo fundamental para el cumplimiento de sus objetivos. Por lo tanto, debe resguardarse adecuadamente, al igual que otros bienes y servicios necesarios para sus actividades. Esta protección abarca todo el ciclo de vida de la información, todos los formatos en los que se presente y cualquier soporte utilizado, con el fin de preservar la confidencialidad, integridad y disponibilidad de la misma.

La protección de la información requiere el establecimiento, implementación, monitoreo, revisión y mejora continua de un conjunto de mecanismos de seguridad o controles. Estos incluyen políticas, procesos, procedimientos, estructuras organizacionales, software y hardware. El objeto de estos mecanismos y controles es el de minimizar los riesgos a los que se encuentra expuesta la información, así como asegurar la continuidad de las operaciones del organismo.

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

CONSIDERACIONES GENERALES

1. OBJETIVOS

La presente Política de Seguridad de la Información (PSI) establece los lineamientos y las políticas específicas orientadas a resguardar la confidencialidad, integridad y disponibilidad de la información, protección de los recursos tecnológicos y continuidad de las operaciones de la SSN.

Los objetivos de la PSI son:

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

El presente documento se emite en cumplimiento de la normativa legal vigente. Esto incluye a aquella externa al organismo, como leyes nacionales, decretos, resoluciones y disposiciones que sean aplicables a los datos, a los sistemas informáticos y al ambiente tecnológico que utiliza, así como internas de la propia entidad, como ser políticas, procedimientos, cláusulas contractuales y acuerdos con empleados y terceros.

2. ALCANCE

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

Su cumplimiento es obligatorio para la totalidad de las autoridades y del personal que integra el organismo, cualquiera sea su modalidad de contratación y las fuentes de financiamiento correspondientes.

Asimismo, la PSI debe ser conocida y cumplida por toda persona, ya sea interna o externa, vinculada a la entidad a través de contratos, convenios, acuerdos o algún otro instrumento válido para establecer la relación con terceros, en la medida en que le sea aplicable.

3. MARCO NORMATIVO

La presente Política de Seguridad de la Información se encuentra alineada con la legislación vigente que regula aspectos que hacen a la seguridad de la información y con los estándares internacionales en la materia, en especial:

Leyes y decretos

- Ley 11.723 – Régimen legal de la propiedad intelectual.
- Ley 17.622 – Estadística y censos.
- Ley 19.549 – Ley de procedimiento administrativo.
- Ley 25.188 – Ética en el ejercicio de la función pública.
- Ley 25.326 – Protección de Datos Personales.
- Ley 25.506 – Firma Digital
- Ley 26.388 – Delitos informáticos.
- Decreto 577/2017 – Creación del Comité de Ciberseguridad.

Decisiones administrativas y Resoluciones

- Decisión Administrativa 641/2021 – Requisitos mínimos de seguridad de la información para organismos.
- Resolución JGM 580/2011 – Creación del Programa Nacional de Protección de Infraestructuras Críticas de Información y Ciberseguridad.
- Resolución JGM 1523/2019 – Definición de Infraestructuras Críticas.
- Resolución SIP 44/2023 – Segunda Estrategia Nacional de Ciberseguridad.
- Resolución SICYT 15/2024 – Lineamientos para el uso de herramientas digitales.

Disposiciones

- Disposición DNCIB 1/2021 – Centro Nacional de Respuestas a Incidentes Informáticos (CERT.ar).
- Disposición DNCIB 7/2021 – Registro de Puntos Focales en Ciberseguridad del Sector Público Nacional.
- Disposición DNCIB 8/2021 – Guía Introductoria a la Seguridad para el Desarrollo de Aplicaciones WEB.
- Disposición DNCIB 1/2022 – Modelo Referencial de Política de Seguridad de la Información.

- Disposición SSTI 3/2023 – Guía de notificación y gestión de incidentes de ciberseguridad.

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

- Norma ISO/IEC 27000 – Sistemas de gestión de la seguridad de la información. Visión de conjunto y vocabulario.
- Norma ISO/IEC 27001 – Sistemas de gestión de la seguridad de la información. Requisitos.
- Norma ISO/IEC 27002 – Código de prácticas para los controles de seguridad de la información.

4. PRINCIPIOS BÁSICOS

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

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

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

La SSN declara su compromiso y apoyo a la gestión de la seguridad de la información como parte integrante de la gestión del resto de los procesos establecidos en su ámbito. En este sentido, sus autoridades se comprometen a liderar la mejora continua de los procesos de gestión de seguridad de la información, asegurando su eficacia y eficiencia.

5. NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN

La SSN se compromete a establecer la normativa técnica de seguridad de la información necesaria para el cumplimiento de los lineamientos y de las políticas específicas que integran la PSI.

Los estándares, procedimientos y guías que se establezcan deben ser acordes a lo dispuesto en esta PSI y describir cómo se deben llevar a cabo las acciones comprendidas en este documento.

6. INCUMPLIMIENTO

El incumplimiento de la PSI y/o de la normativa técnica de seguridad de la información tendrá como resultado la aplicación de sanciones disciplinarias, conforme a la magnitud y característica del aspecto no cumplido, de acuerdo con la normativa aplicable.

Al respecto y de acuerdo a la legislación vigente, se establece como falta el incumplimiento de los lineamientos y políticas de esta PSI por parte de agentes y funcionarios, de acuerdo al régimen sancionatorio establecido en la Ley Marco de Regulación de Empleo Público Nacional N° 25.164, su Decreto Reglamentario N° 1421/02 y sus normas modificatorias y complementarias.

No constituirán incumplimiento las excepciones a la observancia de pautas o reglas específicas que fije la PSI y/o la normativa técnica de seguridad de la información cuando el responsable del área interesada requiera su autorización con anterioridad al hecho, conforme al procedimiento aplicable. Las autorizaciones son de carácter excepcional y se otorgan de forma temporaria. Su requerimiento y respuesta deben ser formalmente documentados, registrados y revisados.

7. APROBACIÓN

La normativa de seguridad de la información de la SSN, que comprende tanto la PSI como la normativa técnica que a partir de ella se elabore, requiere la aprobación de la máxima autoridad del organismo o autoridad competente.

8. VIGENCIA

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

9. REVISIÓN Y ACTUALIZACIÓN

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

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

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

10. COMUNICACIÓN

Esta Política debe ser comunicada al personal del organismo y a las partes externas relevantes de manera pertinente, accesible y comprensible. Además de su publicación en el Boletín Oficial, el texto íntegro y actualizado se mantendrá a disposición de los interesados en la Intranet del organismo y en el sistema KRONOS.

LINEAMIENTOS

1. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La SSN asigna al Comité de Seguridad de la Información (CSI) las funciones de planificación en materia de seguridad de la información y de supervisión de la investigación y monitoreo de los incidentes relativos a la seguridad de la información. La planificación comprende la propuesta de programas, proyectos y metodologías, su monitoreo y evaluación, así como la promoción de la difusión y apoyo a la seguridad de la información dentro del organismo.

El CSI es la principal instancia responsable de la planificación de la seguridad de los sistemas de información del organismo, sin perjuicio de las responsabilidades propias que asigna la estructura orgánico-funcional. El CSI puede ser asistido en sus actividades por Comisiones o Comités creados a estos efectos.

Son funciones propias del CSI elaborar la PSI, revisarla y proponer modificaciones, así como aprobar anualmente el Plan de Seguridad de la Información.

La organización de las actividades tendientes a la implementación de la presente PSI recae sobre el área del organismo responsable de las tecnologías de la información y comunicación. Esta área tiene a su cargo proponer y elevar al Comité la PSI y sus actualizaciones y el Plan de Seguridad de la Información. Asimismo, su titular o quien éste proponga es, a su vez, el punto focal designado ante la Dirección Nacional de Ciberseguridad (DNCIB), conforme lo requiere la Disposición DNCIB 7/21.

2. SEGURIDAD INFORMÁTICA DE LOS RECURSOS HUMANOS

La SSN procura que su personal esté debidamente informado respecto a la importancia de la seguridad de la información a través de programas específicos de concientización. En lo que hace al personal técnico, el organismo favorece el acceso a capacitación adecuada a sus funciones.

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

Los funcionarios titulares de las diversas dependencias de la SSN son los encargados de velar por el cumplimiento de la normativa vigente por parte del personal a su cargo.

Las acciones que se adopten en materia de seguridad de la información no podrán afectar los derechos individuales de los empleados, especialmente aquellos relacionados con la privacidad.

3. GESTIÓN DE ACTIVOS

El organismo adopta las medidas necesarias para contar con los activos de información inventariados, de forma tal que permita su clasificación en función de la criticidad. Se registra al responsable de cada activo, así como su ubicación, permitiendo de esta manera una adecuada gestión y protección de los activos de información. El concepto de activos abarca tanto al hardware como al software y a los dispositivos de comunicación, los elementos de apoyo, la información y los datos en sí mismos, cualquiera sea el soporte y formato en el que se encuentren.

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

4. AUTENTICACIÓN, AUTORIZACIÓN Y CONTROL DE ACCESO

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

Los privilegios se otorgan en forma expresa, son autorizados por los niveles competentes y se gestionan adecuadamente las altas y bajas de las cuentas y permisos de acceso, fijándose revisiones periódicas.

Los empleados, funcionarios y terceros destinatarios de esta Política son responsables del uso adecuado de los dispositivos y credenciales otorgadas por el organismo para el cumplimiento de sus funciones.

El organismo adopta acciones específicas, entre las cuáles se encuentra la comunicación de la PSI, para procurar que el personal incorpore las medidas de cuidado necesarias, tanto dentro como fuera del organismo.

Se monitorea, inspecciona y controla el tráfico de datos en las redes del organismo, así como toda comunicación externa entrante hacia las redes de la SSN y toda comunicación saliente hacia internet, enlaces punto a punto entre organismos y VPNs, con el objeto de verificar que no se violen las políticas de seguridad establecidas.

5. USO DE HERRAMIENTAS CRIPTOGRÁFICAS

El organismo establece el uso de herramientas criptográficas para asegurar la información y las comunicaciones, como ser contraseñas, servicios expuestos a internet y transmisión de datos, dentro y fuera del ámbito de la SSN. A su vez, para la transmisión de datos fuera del organismo se cumplirá con las medidas y canales que establece la normativa vigente como de cumplimiento obligatorio para los organismos de la Administración Pública Nacional.

6. SEGURIDAD FÍSICA Y AMBIENTAL

El organismo define perímetros de seguridad y controles para proteger las áreas consideradas críticas, considerando que su mal funcionamiento o puesta fuera de servicio puede entorpecer el normal desempeño de los sistemas de información de la SSN y/o exponer información que administra el organismo. Además, se controlan y monitorean los accesos físicos para permitir solo el ingreso y egreso de personal y equipamiento informático debidamente autorizados.

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.

Se realiza el mantenimiento periódico del equipamiento informático y se adopta la política de pantallas limpias, a fin de reducir los riesgos de acceso no autorizado a un equipo informático desatendido.

7. SEGURIDAD OPERATIVA

El organismo adopta medidas para minimizar los riesgos de acceso y cambios no autorizados o pérdida de información y para proteger las instalaciones y plataformas tecnológicas contra infecciones de código malicioso. Para ello, se compromete a desarrollar e implementar procedimientos acordes que permitan el desarrollo seguro de las operaciones del organismo, así como el control de la actividad de administradores y operadores.

En los procesos de desarrollo de software se definen entornos separados entre sí para el desarrollo, la realización de pruebas funcionales y no funcionales (testing) y producción, con el objeto de generar sistemas seguros. Asimismo, se definen entornos separados para pruebas que requieran simular el ambiente de producción y emplear muestras de datos productivos (pre-producción) y para la explotación de datos.

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

Se monitorean, registran y auditan eventos 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.

8. SEGURIDAD DE LAS 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 de la SSN.

Se considera al 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 afecte el rendimiento de la infraestructura de comunicaciones o ponga en riesgo la seguridad de la misma.

9. ADQUISICIÓN DE SISTEMAS, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

El organismo se compromete a adoptar medidas de seguridad para proteger por defecto y desde el diseño todas las aplicaciones que se desarrollen con medios propios o a través de terceros. En toda adquisición de sistemas informáticos, como también en todos los proyectos de desarrollo de software, 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 usan datos de prueba de manera segura y siguiendo requisitos de seguridad estipulados en los entornos de desarrollo y prueba.

10. RELACIÓN CON PROVEEDORES

Se establecen requisitos de seguridad para proteger los activos de información de la SSN a los que tienen acceso los proveedores, como también los riesgos asociados a los servicios provistos por parte de terceros. El organismo incluye en los pliegos de bases y condiciones particulares cláusulas vinculadas a la seguridad de la información, de cumplimiento efectivo y obligatorio por parte los contratantes.

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 en el marco de la presente.

11. GESTIÓN DE INCIDENTES DE SEGURIDAD

Todo el personal de la SSN es responsable de informar los eventos sospechosos de seguridad o incidentes que se detecten, como también de comunicar las fallas o debilidades que adviertan en el uso regular de los sistemas tecnológicos.

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.

De producirse el incidente, y que éste hubiera afectado información o datos personales de terceros, el organismo informará tal ocurrencia, de acuerdo a lo dispuesto por la normativa vigente.

Se podrán iniciar los procedimientos sumariales contemplados en la normativa vigente de la Administración Publica Nacional a los empleados que violen la Política de Seguridad de la Información y la normativa técnica de seguridad de la información.

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

12. ASPECTOS DE SEGURIDAD PARA LA CONTINUIDAD DE LA GESTIÓN

El organismo se compromete a desarrollar e implementar planes de contingencia para asegurar la continuidad de los procesos de la SSN, para que las operaciones se puedan restaurar en los plazos requeridos y manteniendo los requerimientos de seguridad. Se identificarán las ventanas de recuperación requeridas en los procesos críticos.

13. CUMPLIMIENTO

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

POLÍTICAS ESPECÍFICAS

1. POLÍTICA ORGANIZATIVA

Objetivo

- Establecer un marco gerencial para la implementación y control de la seguridad de la información dentro de la SSN.

1.1. Organización interna

1.1.1. *Comité de Seguridad de la Información*

El Comité de Seguridad de la Información (CSI) es la principal instancia responsable de la planificación de la seguridad de la información de la SSN. La planificación comprende la propuesta de programas, proyectos y metodologías, su monitoreo y evaluación, así como la promoción de la difusión y apoyo a la seguridad de la información dentro del organismo.

Conformación

El CSI está conformado por los titulares de la totalidad de las Gerencias que componen la estructura del organismo y del área responsable de las tecnologías de la información y comunicación.

El responsable del área de seguridad de la información o persona que el titular del área a cargo de las tecnologías de la información y comunicación designe para el seguimiento de la implementación de las medidas de seguridad de la información estará presente en las reuniones con voz, pero sin voto.

Asimismo, el Comité convocará a sus reuniones ordinarias al titular de la Unidad de Auditoría Interna, quien podrá participar en calidad de observador, y al personal de las áreas que resulte necesaria para el tratamiento y resolución de temas específicos.

Cada miembro del Comité debe designar por nota GDE un representante que lo reemplace en caso de ausencia, el que no podrá poseer cargo menor al de Coordinador.

La coordinación del CSI está a cargo del titular del área responsable de las tecnologías de la información y comunicación.

El CSI puede ser asistido en sus actividades por Comisiones creadas a estos efectos, conforme a la reglamentación que el Comité establezca en la materia.

Funciones

Son funciones del CSI:

- Proponer a la máxima autoridad del Organismo para su aprobación la Política de Seguridad de la Información, sus modificatorias y documentos derivados.
- Planificar, monitorear y evaluar las medidas relativas a la seguridad de los sistemas de información del Organismo.
- Aprobar anualmente el Plan de Seguridad de la Información.
- Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad de la información.
- Acordar y proponer programas, proyectos y metodologías relativas a la seguridad de la información.
- Promover la difusión y apoyo a la seguridad de la información dentro del Organismo.

Reuniones

El CSI se reunirá de forma ordinaria como mínimo una vez cada cuatro meses, pudiendo hacerlo de forma extraordinaria cuando las circunstancias así lo exigieran. Las reuniones se podrán realizar de forma presencial o virtual.

Lo tratado en reuniones del Comité quedará incorporado en actas firmadas por la totalidad de los miembros presentes. Las actas serán formalizadas mediante documento GDE, siendo responsabilidad de cada miembro la firma dentro de las 24 horas posteriores a su recepción.

Convocatoria, quórum y decisiones

La convocatoria a reuniones del CSI será llevada a cabo por su coordinador mediante correo electrónico. La convocatoria incluirá el temario e información y documentación correspondiente al orden del día. Los documentos cuya aprobación se ponga a

consideración del Comité se enviarán por correo electrónico en forma previa con al menos CINCO (5) días de anticipación.

Para sesionar será necesaria la presencia de la mayoría absoluta de sus miembros, entendiéndose como tal cuando los miembros presentes superen a los miembros ausentes. Si no se pudiera sesionar por falta de quórum, se fijará nueva sesión dentro de los DIEZ (10) días corridos de la fecha de la primera convocatoria.

Las decisiones del Comité se tomarán por simple mayoría de sus miembros presentes.

Deber de colaboración con el Comité

El CSI dispone de las facultades necesarias para solicitar a las distintas áreas involucradas la información que considere relevante y la participación en sus reuniones del personal que se estime necesario.

1.1.2. ***Responsable de Seguridad de la Información***

El área responsable de las tecnologías de la información y de las comunicaciones tiene a su cargo las funciones relativas a la seguridad de los sistemas informáticos de la SSN y procesos asociados. Así también, se le asigna la función de Responsable de Seguridad de la Información (RSI) del organismo. Como tal, tiene a su cargo la coordinación y supervisión de todos los aspectos inherentes a la seguridad tratados en la presente política.

Funciones

Son funciones del RSI:

- Elaborar y elevar al CSI para su consideración la Política de Seguridad de la Información y sus actualizaciones.
- Elaborar anualmente el Plan de Seguridad de la Información, presentarlo para su aprobación al CSI y monitorear su cumplimiento.
- Ejercer la Coordinación del CSI.
- Generar estándares, procedimientos y guías para la seguridad de la información.
- Promover la capacitación y concientización de la seguridad de la información en los agentes del organismo.

- Analizar la actividad en redes, servidores, puntos finales, bases de datos, aplicaciones, sitios web y otros sistemas, buscando actividades anómalas que puedan ser indicativas de un incidente o compromiso de seguridad.
- 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.
- Controlar el acceso a los recursos tecnológicos.
- Representar a la SSN como punto focal designado ante la Dirección Nacional de Ciberseguridad (DNCIB).

1.1.3. *Asignación de responsabilidades de la seguridad de la información*

Proceso de seguridad	Responsable según área de competencia
Apoyo e impulso de la implementación de la Política de Seguridad de la Información	Comité de Seguridad de la Información Área a cargo de las tecnologías de la información y de las comunicaciones
Planificación de las actividades de fortalecimiento del Sistema de Gestión de Seguridad de la Información	Comité de Seguridad de la Información Área a cargo de las tecnologías de la información y de las comunicaciones
Concientización en seguridad de la información	Área a cargo de las tecnologías de la información y de las comunicaciones Área a cargo de asuntos institucionales
Capacitación en seguridad de la información	Área a cargo de las tecnologías de la información y de las comunicaciones Área a cargo de recursos humanos
Gestión de activos	Área a cargo de las tecnologías de la información y de las comunicaciones Área a cargo de patrimonio Área a cargo de recursos humanos Área a cargo de soporte técnico
Control de accesos	Área a cargo de las tecnologías de la información y de las comunicaciones Área a cargo de recursos humanos

Seguridad física y ambiental	Área a cargo de seguridad física. Área a cargo de recursos humanos.
Seguridad operativa	Área a cargo de las tecnologías de la información y de las comunicaciones
Seguridad en las comunicaciones	Área a cargo de las tecnologías de la información y de las comunicaciones
Seguridad en el desarrollo de software	Área a cargo de las tecnologías de la información y de las comunicaciones
Seguridad en la relación con proveedores	Área a cargo de las tecnologías de la información y de las comunicaciones Área a cargo de la administración y gestión operativa.
Gestión de incidentes de seguridad	Área a cargo de las tecnologías de la información y de las comunicaciones
Planificación de la continuidad operativa	Comité de Seguridad de la Información
Cumplimiento normativo	Área a cargo de las tecnologías de la información y de las comunicaciones Área a cargo de los asuntos jurídicos

1.2. Segregación de tareas

Se deberá diseñar un 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.

1.3. Propietarios de la información

Se designarán como propietarios de la información que se procesa y almacena en la SSN a los responsables de las Gerencias, Subgerencias o Coordinaciones que por sus funciones tengan responsabilidad legal sobre el tratamiento de la misma, generen o utilicen 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 al Responsable de la Seguridad de la Información, debiendo

registrarse descripción de la información, propietario, procesos involucrados, área, recursos asociados, responsable técnico y cualquier otra información que sea relevante.

1.4. 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.

De requerirse el intercambio de información confidencial para fines de asesoramiento o de transmisión de experiencias y no mediare una obligación legal o contractual que asegure el deber de confidencialidad, sólo se permitirá el intercambio cuando se haya firmado previamente un acuerdo de confidencialidad.

1.5. Contacto con grupos de interés especial

El Responsable de la Seguridad de la Información 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. Asimismo, fomentará el intercambio con otros organismos de alertas tempranas, avisos y recomendaciones ante la aparición de nuevas vulnerabilidades o formas de violar la seguridad implementada.

1.6. Seguridad de la información en la gestión de proyectos

Se procurará contemplar al Responsable de la Seguridad de la Información en la gestión de proyectos a efectos de garantizar que se refleje adecuadamente la normativa en seguridad de la información.

2. POLÍTICA DE RECURSOS HUMANOS

Objetivo

- Procurar que los agentes, funcionarios y proveedores de la SSN conozcan, comprendan y cumplan con sus responsabilidades en seguridad de la información.

2.1.Antes del empleo

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

2.1.2. ***Revisión de antecedentes***

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

2.2. Inicio del empleo

2.2.1. ***Términos y condiciones del empleo***

Se deberá definir el modelo de acuerdo de confidencialidad, aplicable a los agentes, y de cláusula de confidencialidad, aplicable a contratos con proveedores, cuya firma será requerida cuando el organismo lo considere necesario, al inicio de la contratación. Su definición, revisión y las pautas para su implementación serán tarea del CSI.

Estos acuerdos, cuando así se lo requiera, deberán ser firmados por el personal de la SSN, cualquiera sea su situación de revista, como también así por terceros que tengan relaciones contractuales con el organismo.

Las copias quedarán a resguardo en el área a cargo de recursos humanos (agentes y funcionarios) y en el área a cargo de administración y gestión operativa (proveedores).

2.3. Durante el empleo

2.3.1. ***Responsabilidad de las Gerencias***

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

2.3.2. ***Programa de concientización en seguridad de la información***

Se deberán realizar tareas de capacitación y concientización de las políticas, procedimientos, guías y buenas prácticas dirigidas a todos los agentes que se desempeñen en el ámbito de la SSN. La capacitación y concientización comprenderán requerimientos de seguridad, responsabilidades legales, uso correcto de los dispositivos tecnológicos asignados y el uso correcto de los recursos en general.

2.3.3. *Procedimiento disciplinario*

La SSN podrá iniciar un procedimiento administrativo disciplinario con el objeto de sancionar administrativamente, según la normativa vigente, a todos aquellos agentes, sea cual fuere su situación de revista, que violen la normativa de seguridad de la información.

Los agentes que desempeñan sus tareas en el ámbito de la SSN, sea cual fuere su nivel escalafonario y su situación de revista incurrirán también, en su caso, en responsabilidad civil o patrimonial si ocasionan daños sobre los bienes y/o recursos aquí contemplados.

Podrán, asimismo, incurrir 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.

2.4. Cese del empleo

2.4.1. *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 de la SSN.

2.4.2. *Transferencia de conocimientos*

Los agentes que prestan servicios en la SSN 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 a la SSN antes de proceder a su desvinculación.

3. POLÍTICA DE DISPOSITIVOS MÓVILES Y TRABAJO REMOTO

Objetivo

- Proteger la información que es accedida, tratada o almacenada de manera remota y a través del uso de dispositivos móviles.

3.1. Dispositivos móviles de la SSN

Todo dispositivo móvil perteneciente a la SSN (notebooks, tabletas, teléfonos celulares, etc.), que pudiera contener información del organismo deberá cumplir con medidas de seguridad adecuadas para proteger el dispositivo móvil y la información que contiene.

En este sentido, se deberán desarrollar procedimientos para asegurar al dispositivo móvil y la información contenida, debiendo tener en cuenta los siguientes aspectos:

- Protección contra software malicioso del dispositivo móvil.
- Mecanismos de borrado seguro de la información en caso de robo o pérdida.
- Cifrado de las comunicaciones.
- Control de acceso a los recursos a los que accede el 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 exponiendo a la SSN ante la ocurrencia del incidente, los que incluirán:

- Revocación de las credenciales afectadas.
- Notificación al Responsable de la Seguridad de la Información.

3.2. Trabajo remoto

En aquellos casos en que por circunstancias excepcionales, por las características de las tareas u otro motivo justificado se requiera que personal tenga acceso remoto a recursos del organismo, el titular del área a la que pertenece, no inferior a Subgerente, solicitará de manera documentada la autorización al Responsable de Seguridad de la Información.

Los controles y disposiciones del trabajo remoto comprenden:

- Asegurar el cifrado de las comunicaciones
- 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.

- Definir el trabajo permitido, la franja horaria de trabajo asignada y los sistemas internos y servicio a los cuales el trabajador remoto solo estará autorizado a acceder.
- Definir reglas y orientación respecto del acceso de terceros al equipamiento e información.
- Proveer el hardware y el soporte y mantenimiento del software, cuando sea necesario.
- Efectuar auditorías y monitoreo de las actividades efectuadas remotamente.
- Realizar la anulación de las autorizaciones, derechos de acceso y devolución del equipo cuando finalicen las actividades remotas.
- 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.
- Se deberán implementar regularmente procesos de auditoría específicos para los casos de accesos remotos.

4. POLÍTICA DE GESTIÓN DE ACTIVOS

Objetivo

- Facilitar el control de los activos de información, su adecuada protección y un uso responsable.

4.1. Inventariado de activos

Se deberá mantener un inventario de activos preciso y actualizado. Cada activo deberá poseer un propietario asignado, estar claramente identificado y tipificado según sea:

- Información: bases de datos, archivos de datos, documentación.
- Activos de software: software de aplicaciones, software de sistemas, herramientas de desarrollo, y utilitarios.
- Activos físicos: equipamiento de computación, equipamiento de

comunicaciones, medios removibles y otros equipamientos.

- Instalaciones: tendido eléctrico, red de agua y gas, etc.
- Servicios: servicios de cómputo y de comunicaciones, servicios generales, por ejemplo: calefacción, iluminación, energía, y aire acondicionado.
- Personas, y sus calificaciones, habilidades y experiencia.

4.2. Responsables de activos

Deberá designarse responsables de los activos registrados, quienes deberán:

- Informar sobre cualquier cambio que afecte al activo del cual son responsables.
- Clasificar los activos en función a su sensibilidad y criticidad.
- Velar por la implementación de controles de seguridad requeridos para proteger los activos.

La implementación de los controles de seguridad podrá ser delegada a personal especializado, como también la gestión técnica u operativa.

4.3. Uso aceptable de activos de tecnología

Todos los agentes, sin importar su situación de revista, contratistas y usuarios de terceras partes deberán seguir las reglas que se establezcan 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.

4.4. 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. El organismo definirá el procedimiento aplicable para dicha devolución.

4.5. Clasificación de la información, etiquetado y manipulado de activos de información

Se deberán definir procedimientos de clasificación y etiquetado para determinar la criticidad de la información que se administra en la SSN, sobre la base de las tres características centrales de seguridad de la información: confidencialidad, integridad y disponibilidad.

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

La documentación administrativa que se genere en el marco del cumplimiento de la normativa de seguridad de la información tiene carácter reservado y, en consecuencia, su conocimiento y uso está restringido a quién está dirigida la actuación, o a la persona expresamente autorizada.

4.6.Gestión de soportes de almacenamiento

Se deben implementar procedimientos para la gestión de los soportes informáticos extraíbles, contemplando aspectos como la autorización y registro del retiro de estos dispositivos fuera de los edificios de la SSN.

Los soportes de medio extraíbles, como cintas magnéticas y discos externos, deben ser almacenados en un ambiente seguro y protegido, considerando la criticidad de la información contenida y las especificaciones de los fabricantes o proveedores del soporte de almacenamiento. Para esto, se podrá utilizar una caja de seguridad como opción para resguardar estos elementos.

Se deberán establecer procedimientos para el borrado seguro de la información al declararse la baja del soporte de almacenamiento que la contiene, así como para las operaciones de reciclado de los dispositivos de almacenamiento.

Los medios de almacenamiento que no puedan ser reutilizables deben ser destruidos físicamente de manera apropiada para impedir la recuperación de la información mediante técnicas forenses.

Además, se debe proteger la información y los soportes de almacenamiento en tránsito. Por lo tanto, es fundamental definir procedimientos para el transporte de soportes de almacenamiento que incluyan el cifrado de la información contenida, la utilización de servicios de mensajería confiables, la adopción de embalajes sellados, la entrega en mano u otros mecanismos que garanticen la seguridad del soporte durante su transporte.

5. POLÍTICA DE CONTROL DE ACCESOS

Objetivo

- Asegurar que los recursos del organismo sean accedidos únicamente por los usuarios autorizados y evitar el acceso no autorizado a los mismos.

5.1. Requisitos de negocio para el control de acceso

5.1.1. *Control de acceso*

Se controlará el acceso a la información y a los recursos tecnológicos de la SSN en función de los requisitos de negocio y siguiendo el principio de mínimo privilegio. Se otorgará acceso únicamente al conjunto mínimo de permisos que se requiera para realizar el trabajo.

Se definirán procedimientos que tengan en cuenta aspectos tales como:

- Segregación de las funciones referidas a quien solicita, quien autoriza y quien concede operativamente el acceso.
- Identificación del propietario de la información, del usuario que requiere el acceso y de la aplicación a la cual se desea acceder.
- Identificación de los requerimientos de seguridad de las aplicaciones y toda información relevante de seguridad relacionada a las mismas.
- Definición de perfiles de acceso de usuarios a las aplicaciones.
- Tipos de accesos, informando si son internos o externos, públicos o privados.
- Requerimientos de revisión periódica de los accesos concedidos.
- Revocación de los derechos de acceso.
- Administración de cuentas de usuarios y permisos de acceso de los mismos a los sistemas y dispositivos de red de la SSN.

5.1.2. *Acceso a las redes y a los servicios de red*

Los usuarios tendrán acceso solo a la red y a los servicios de red que hubieran sido específicamente autorizados, para cuyo acceso deberán emplear las credenciales asignadas que permitan su debida identificación.

El organismo establecerá los requisitos de autorización del equipamiento a emplear y los controles de dichos accesos.

5.2. Gestión de acceso de usuarios

5.2.1. *Creación e inhabilitación de cuentas de usuario*

Se deberán definir procedimientos que permitan crear e inhabilitar 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 contemplar los siguientes aspectos:

- Utilizar nombres de cuentas de usuario identificables que permitan determinar inequívocamente las actividades realizadas por dichas cuentas, ya sean cuentas de usuario o cuentas de servicio.
- Evitar que existan múltiples cuentas de usuario asociadas solo a un individuo, salvo excepciones por cuestiones de seguridad.
- Evitar la creación y uso de cuentas de usuario genéricas, compartidas para un grupo de usuarios o una tarea específica. Esto es permitido únicamente por razones operativas, previo análisis y autorización por parte del Responsable de Seguridad de la Información antes de su creación.
- Los nombres de las cuentas de usuario no deberán dar indicios del nivel de privilegios de la misma.
- Garantizar que no se otorgue acceso hasta que se hayan completado los procedimientos de autorización.
- Mantener un registro formal de todas las personas autorizadas para utilizar el servicio.
- Inhabilitar inmediatamente los derechos de acceso de los usuarios que cambian de funciones, de área de pertenencia o se desvinculan de la SSN.
- Establecer que los agentes de la SSN que intenten accesos no autorizados serán pasibles del inicio de procesos sancionatorios.
- Efectuar revisiones periódicas con el objeto de:
    - Inhabilitar cuentas de usuarios inactivas por más de tres meses.

- Inhabilitar cuentas de usuarios desvinculados de la SSN.
- Inhabilitar las cuentas de usuarios redundantes o no identificables previo análisis de sus actividades.

En el caso de existir excepciones para evitar inhabilitar cuentas de usuario, estas deberán ser debidamente justificadas y aprobadas por el Responsable de la Seguridad de la Información.

5.2.2. ***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 la información (Gerentes, Subgerentes y Coordinadores) serán los encargados de aprobar la asignación de los permisos de acceso y solicitar su implementación con la autorización también del Responsable de la Seguridad de la Información.

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

- El principio guía en materia de gestión de accesos es el mínimo privilegio.
- Identificar los niveles de acceso existentes en los sistemas, bases de datos y aplicaciones.
- Verificar que el nivel de acceso a otorgar sea adecuado al rol del usuario y que no comprometa la segregación de funciones.
- Establecer un proceso de autorización que registre todos los derechos de acceso asignados.
- Priorizar que los permisos de acceso se apliquen a roles o grupos, antes de aplicarlos directamente a los usuarios.

5.2.3. ***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 deberán considerar los siguientes aspectos:

- Evitar el uso de cuentas de usuarios con derechos de acceso privilegiados para

realizar actividades regulares.

- Los usuarios con privilegios especiales deben poseer dos cuentas de usuario, una que utilizará para sus tareas habituales y otra para realizar estrictamente actividades que requieran permisos especiales.
- Solo deberán asignarse privilegios especiales en caso de necesidad de uso, basado en los requisitos mínimos necesario para realizar las tareas y estar debidamente documentada
- Se deberá revisar periódicamente la actividad de los usuarios con derechos de accesos privilegiados para verificar que sólo sean utilizados para las actividades que dieron motivo a su asignación y, de no ser necesarios los privilegios, proceder a su restricción o baja de la cuenta.

5.2.4. 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.

5.2.5. Revisión de derechos de acceso de los usuarios

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

Se deberán revisar periódicamente, como mínimo anualmente, los derechos de acceso y privilegios asignados a los usuarios.

5.2.6. Revocación y cambios de derechos de acceso

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

Tras la desvinculación del usuario, se deberán inhabilitar los derechos de acceso a todos los sistemas y servicios de información utilizados por el individuo.

Ante un cambio de función de un usuario, 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 pudiera conocer el agente, contratista o usuario de tercera parte, tras la finalización de vínculo o ante un cambio de función, cuando dicha contraseña forme parte de una credencial de acceso de administración aún activa.

5.3.Responsabilidades del usuario

5.3.1. *Responsabilidad en el uso de contraseñas*

Los usuarios deberán seguir las buenas prácticas de seguridad referidas al uso de contraseñas debiendo cumplir con las siguientes premisas:

- Cambiar las contraseñas recibidas inicialmente por parte de los administradores por contraseñas seguras que cumplan los requisitos mínimos que se indiquen.
- 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 o fechas de cumpleaños.
- No reutilizar o reciclar viejas contraseñas.
- Mantener las contraseñas en secreto, no debiendo ser compartidas ni aún con su personal jerárquico.
- Cuando existiera indicio de que la confidencialidad de la contraseña hubiera sido comprometida deberá informarlo y solicitar inmediatamente el cambio de la misma.
- Evitar incluir contraseñas en los procesos automatizados de inicio de sesión.
- Evitar almacenar contraseñas en papel, archivos de texto, planillas de cálculo o cualquier aplicación cuya función no sea expresamente el almacenamiento seguro de contraseñas.

5.4. Control de acceso a servicios, sistemas y aplicaciones

5.4.1. *Política de utilización de los servicios de red*

Se restringirá y controlará el acceso a los servicios de red para garantizar que los usuarios que accedan a las redes y a sus servicios no comprometan la seguridad de los mismos.

El acceso a los servicios de red se realizará a través del empleo de las credenciales únicas otorgadas a estos efectos que permitan la debida identificación del usuario.

El Responsable de la Seguridad de la Información autorizará el acceso a los recursos de red, servicios e información únicamente mediante un pedido formal del propietario 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.

5.4.2. *Proceso de inicio de sesión segura*

El acceso a los servicios de información deberá ser posible solo a través de un proceso de inicio de sesión segura, el que deberá:

- Desplegar un aviso informativo, advirtiendo que sólo los usuarios autorizados pueden iniciar sesión en el equipo informático.
- 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.
- 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.
- Evitar configurar el equipo informático con credenciales almacenadas que provoquen el inicio de sesión de forma automática.
- Registrar todas las conexiones exitosas y los intentos de conexión fallidas.
- Evitar implementaciones que transmitan las contraseñas en texto plano sobre la red de datos.
- 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.
- Desbloqueo automático de la cuenta luego de cierto tiempo de haberse bloqueado.

5.4.3. ***Autenticación de usuarios para conexiones externas***

El acceso de usuarios remotos está estrictamente limitado y sujeto al cumplimiento de procesos de aprobación, los cuales deberán requerir de la expresa autorización del titular del área de pertenencia y del Responsable de Seguridad de la Información.

Toda conexión remota requerirá la implementación de un factor adicional de autenticación a la credencial de acceso (usuario y contraseña), pudiendo emplearse tokens físicos, tokens por email o app u otro método seguro que a tal efecto se determine. Se evitará el empleo de token SMS.

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

5.4.4. ***Gestión de contraseñas de usuarios***

Se deberán implementar sistemas gestores de contraseñas que garanticen la confidencialidad y eficiencia en la administración de las mismas.

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

- Generar mecanismos que permitan a los usuarios cambiar las contraseñas asignadas inicialmente la primera vez que ingresan al sistema.
- Establecer requisitos mínimos de complejidad en la generación de contraseñas.
- Establecer políticas para evitar la reutilización de contraseñas.
- No se deberán distribuir ni almacenar las contraseñas en texto plano.
- Se deberán cambiar las contraseñas por defecto de los sistemas y dispositivos luego que hubiera finalizado su instalación inicial.

- Se deberán cambiar las contraseñas de las cuentas utilizadas por los servicios de soporte externos a la SSN luego de que la tarea de los mismos hubiera finalizado.
- Se deberá implementar el cifrado mediante contraseña en operaciones de copias de resguardo y restauración de información crítica.
- Para asegurar el adecuado uso las contraseñas se deberán registrar y auditar las actividades relativas a la gestión de las mismas.

5.4.5. *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 sólo serán utilizadas ante necesidades específicas para realizar tareas de contingencia, recupero o reconfiguración que lo requieran.

Se definirá el procedimiento para la administración de contraseñas críticas, el que podrá tener en cuenta los siguientes aspectos:

- La conformación de la contraseña crítica deberá poseer un mayor nivel de complejidad que la requerida para cuentas regulares.
- La definición de la misma será efectuada como mínimo por dos personas, de tal manera que ninguna de ellas conozca la contraseña completa.
- Las partes de las contraseñas serán resguardadas de manera segura y separada.
- 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.
- Las contraseñas críticas se renovarán una vez utilizada, procediendo luego a su resguardo nuevamente.

5.4.6. *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 de la SSN sin haber sido debidamente autorizadas.

5.4.7. ***Acceso a Internet***

El acceso a internet deberá ser utilizado para propósitos laborales.

Se habilitará el acceso básico a Internet a equipos debidamente autorizados.

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.

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

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:

- Queda prohibido acceder a material pornográfico, actividades de apuestas, lúdicas, entretenimiento o pasatiempos de similar tenor.
- Queda prohibido atentar contra los sistemas informáticos y redes de comunicación de la SSN.
- Queda prohibido hacer uso de repositorios de internet no autorizados para almacenar información o documentación de la SSN.
- Queda prohibido hacer uso de servicios de transferencia de archivos no autorizados para el envío de información o documentación de la SSN.
- Queda prohibido el uso de servicios no autorizados que permitan el acceso a internet de manera anónima y eludan las restricciones o limitaciones que el organismo establezca.
- Todos los archivos descargados de internet deberán ser analizados con herramientas antimalware.
- Queda prohibido el uso de programas de mensajería, web chat o redes sociales con otro fin que no sea el laboral.
- Toda excepción a las enumeradas previamente debe contar la explicita

autorización del responsable del área a cargo del personal que lo requiera y deberá ser registrada formalmente.

- Las violaciones o intentos de violación a las pautas que aquí se fijan podrán ser informadas al titular del área de revista del agente, sin perjuicio de otras medidas que por la gravedad del hecho se puedan adoptar.

5.4.8. ***Control de acceso al código fuente***

Se deberá restringir y controlar el acceso al código fuente de las aplicaciones de software desarrolladas en o para la SSN.

Se deberá definir un responsable de la función de "Administrador de código fuente", 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.

Se deberá establecer que todo programa objeto o ejecutable en producción tenga un único programa fuente asociado de forma tal 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 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.

5.4.9. ***Identificación automática de estaciones de trabajo***

Se deberá tener en cuenta la identificación automática de las estaciones de trabajo conectadas a la red interna de la SSN 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.

5.4.10. ***Identificación y autenticación de los usuarios de red***

Todos los usuarios de red (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.

En circunstancias excepcionales, cuando exista un claro beneficio para la SSN, podrá utilizarse un identificador compartido para un grupo de usuarios o una tarea específica. En tal caso, se justificará y documentará debidamente.

6. POLÍTICA DE CRIPTOGRAFÍA

Objetivo

- Proteger la confidencialidad, autenticidad e integridad de la información a través del uso de herramientas criptográficas.

6.1.Cumplimiento de requisitos

6.1.1. ***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. 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.
- Transmisión de información, dentro y fuera del ámbito de la SSN.
- O bien, producto de la evaluación de riesgo sobre el activo de información que se desea asegurar su confidencialidad.

6.1.2. ***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.

6.1.3. ***Servicios de no repudio***

Se utilizarán servicios de "no repudio" cuando se determine 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.

6.1.4. ***Procedimientos para la gestión de claves criptográficas***

Se deberán redactar procedimientos que estipulen operaciones de:

- Almacenamiento de claves secretas y privadas, incluyendo la forma de acceso a las mismas por parte de los usuarios autorizados.
- Renovación y actualización de claves, incluyendo reglas sobre cuándo y cómo deben cambiarse las claves.
- Eliminación de claves, incluyendo cómo deben retirarse o desactivarse las mismas, por ejemplo, cuando las claves hayan caducado.
- Utilización de claves como parte de la administración de la continuidad de las operaciones, por ejemplo, para la recuperación de la información cifrada.
- Generación e implementación de claves en operaciones de copias de resguardo y restauración.

7. POLÍTICA DE SEGURIDAD FÍSICA Y AMBIENTAL

Objetivo

- Prevenir acciones que atenten contra la seguridad de los espacios físicos y equipamiento que puedan comprometer los activos, interferir o interrumpir las operaciones del organismo.

7.1. Áreas seguras

7.1.1. *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 de la SSN.

7.1.2. *Controles físicos de entrada*

Todas las instalaciones edilicias de la SSN 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 y horario de la visita al ingresar a las áreas protegidas, ya que sólo se permitirá el acceso por motivos específicos y autorizados. Asimismo, se deberá registrar fecha y horario al egresar de dichas áreas.

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

Se revisarán y actualizarán los derechos de acceso a las áreas protegidas. Dichos procesos serán documentados y firmados por el responsable del área de la que dependa.

7.1.3. *Seguridad de oficinas, despachos e instalaciones*

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

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

- Oficinas usadas por el titular de la SSN.
- Oficinas usadas por Gerentes y Subgerentes.
- Centro de datos.
- Oficinas de tecnología y sistemas.
- Oficinas de RRHH.

7.1.4. *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 de las áreas protegidas.

7.1.5. *Trabajo en áreas críticas*

Para incrementar la seguridad de las áreas críticas se deberán establecer controles y lineamientos adicionales, tanto para el personal de la SSN como para terceros que deban trabajar en dichas áreas, como ser:

- Implementar controles extras como ser el monitoreo mediante cámaras de seguridad.
- Evitar la ejecución de trabajos por parte de terceros sin supervisión de personal de la SSN.
- Limitar el acceso a las áreas protegidas sólo al personal perteneciente a dichas áreas o cuando sean autorizados por personal responsable de las misma.
- Restringir el ingreso de dispositivos de almacenamiento portable a menos que sea necesario para el desempeño de sus funciones.

7.1.6. *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 de la SSN.

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:

- Limitar el acceso a las áreas de depósito sólo al personal previamente identificado y autorizado.
- 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.
- Verificar y registrar el material entrante al ingresar a las instalaciones edilicias de la SSN.
- Inspeccionar el material entrante para descartar peligros potenciales antes de ser trasladado desde el área de depósito hasta el lugar de uso.

7.2. Seguridad en los equipos

7.2.1. *Emplazamiento y protección de equipos*

El equipamiento deberá ser ubicado y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas, peligros ambientales y acceso a personas no autorizadas. Para su emplazamiento y protección se tendrán en cuenta los siguientes puntos:

- Ubicar el equipamiento en un sitio en donde se minimice el acceso innecesario y se provea un control de acceso adecuado.
- Ubicar las instalaciones de procesamiento y almacenamiento de información en un sitio que permita la supervisión constante.
- Adoptar controles adecuados para minimizar el riesgo de amenazas potenciales por robo, hurto, incendio, polvo, calor y radiaciones electromagnéticas.
- No se debe comer, beber o fumar en proximidad de los equipos de procesamiento de la información, como ser el centro de cómputos o la sala de comunicaciones.

7.2.2. *Seguridad en el suministro eléctrico*

El equipamiento de procesamiento de datos debe 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 Sistema de Alimentación Ininterrumpida (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 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.

7.2.3. *Seguridad del cableado*

El cableado de comunicaciones que transporta datos y brinda apoyo a los servicios de información debe protegerse contra intercepción o daño. Por ello, se procurará que:

- Se adecue a los requisitos técnicos de acuerdo a la normativa vigente.
- Separar los cables de energía de los cables de comunicaciones de datos para evitar interferencias.
- Proteger el tendido del cableado de red troncal entre los pisos mediante la utilización de ductos blindados y/o con controles de acceso físicos.
- Utilizar piso técnico y/o cableado embutido en la pared, siempre que sea posible.
- Utilizar medios de transmisión alternativos seguros cuando no sea posible asegurar la seguridad en el cableado.

7.2.4. *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.

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

7.2.5. ***Seguridad de los equipos fuera de las instalaciones***

El uso de equipamiento destinado al procesamiento de información fuera del ámbito de la SSN deberá ser autorizado por el responsable patrimonial. En caso de que el mismo 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 de la SSN, 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, cuando el activo lo amerite y el organismo lo considere conveniente, mantendrá una adecuada cobertura de seguro para proteger el equipamiento fuera del ámbito de la SSN.

7.2.6. ***Reutilización o baja de equipamiento informático***

Se deberán aplicar operaciones de borrado seguro a todo equipamiento informático antes de su normalización para reutilización. Previo al borrado, se resguardará la información útil y licencias alojadas en dicho equipamiento.

7.2.7. ***Retiro de activos de propiedad de la SSN***

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

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

7.2.8. ***Pantallas limpias***

Los usuarios deben cerrar las sesiones de las aplicaciones, sistemas y servicios de red cuando no estén siendo usadas. Al ausentarse momentáneamente de su puesto de trabajo, deben 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.

De requerirse por motivos excepcionales derivados de la operatoria diaria una extensión del plazo para el bloqueo automático del equipo, el responsable del área en la que revista el usuario lo solicitará al Responsable de Seguridad de la Información. Los titulares de área asumen la responsabilidad por las consecuencias derivadas de dichas solicitudes excepcionales.

En ningún caso se podrá desactivar de manera permanente la política de bloqueo automático de equipos.

Al finalizar su jornada laboral, los usuarios deben cerrar las sesiones activas y apagar el equipo informático. Cuando sea requerido por el Responsable de Seguridad de la Información realizar tareas de mantenimiento sobre el equipo fuera del horario laboral, el usuario deberá cerrar las sesiones de servicios abiertos y activar el bloqueo.

7.2.9. *Escritorios Limpios*

Los usuarios deben proteger la información no pública que utilizan en sus tareas, no dejando documentación en papel u otro medio de almacenamiento 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.

8. POLÍTICA DE SEGURIDAD EN LAS OPERACIONES

Objetivo

- Asegurar que las actividades de tratamiento de información se realicen de manera adecuada y que los recursos de tratamiento y soporte de información estén debidamente protegidos.

8.1.Procedimientos y responsabilidades operativas

8.1.1. *Documentación de los procedimientos operativos*

Los procedimientos operativos deben 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:

- Información que se gestiona.
- Requerimientos o interdependencias con otros sistemas.
- Instrucciones para el manejo de errores u otras condiciones excepcionales que puedan surgir durante la ejecución de tareas.
- Personas de soporte a quien contactar en caso de dificultades operativas o técnicas imprevistas.

8.1.2. *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 de la SSN.

Se deberá 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.

Los procedimientos de control de cambios contemplarán los siguientes puntos:

- Identificación y registro de cambios significativos.
- Evaluación del posible impacto de dichos cambios.
- Aprobación formal de los cambios propuestos.
- Planificación del proceso de cambio.
- Prueba del nuevo escenario.
- Comunicación de detalles de cambios a todas las personas pertinentes.
- Identificación de las responsabilidades por la cancelación de los cambios

fallidos y la recuperación respecto de los mismos.

8.1.3. ***Planificación de la capacidad***

Se deberán 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.

8.1.4. ***Separación de entornos***

Para el proceso de desarrollo de software y con el objeto de generar sistemas seguros deben existir, al menos, tres entornos separados e independientes para el desarrollo, la realización de pruebas funcionales y no funcionales (testing) y producción. Asimismo, se contará con entornos separados para pruebas que requieran simular el ambiente de producción y emplear muestras de datos productivos (pre-producción) y para la explotación de datos.

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.

Se deberán programar controles y revisiones que tengan en cuenta los siguientes aspectos:

- El personal de desarrollo no tendrá acceso al ambiente productivo, oficiando sólo como asesor del personal de producción cuando estos lo requieran.
- Definir propietarios de la información para cada uno de los ambientes de procesamiento existentes.
- 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.
- El ambiente de producción deberá contar solamente 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.
- Los usuarios no tendrán acceso al ambiente de desarrollo ni accederán de

manera directa a las bases de datos del ambiente productivo.

- Únicamente los usuarios autorizados accederán a los ambientes de testing y de explotación de datos.
- Las restricciones de acceso a los distintos ambientes se podrán realizar en función de la pertenencia del usuario a un grupo de seguridad y/o por equipo.

8.2. Protección contra código malicioso

8.2.1. *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 de la SSN.

Para evitar la ejecución de código malicioso se deberá controlar toda actividad de lectura y grabación de archivos, en estaciones de trabajo y servidores y todo tráfico de carga y descarga de archivos en los servidores de conexión a internet.

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

8.3.Copias de seguridad y restauración

Se definirán procedimientos para el resguardo de la información que consideren:

- Definir los roles y funciones para cada actividad definida.
- Definir las actividades y responsabilidades en la elaboración y aprobación del Plan de backup.
- Identificar los registros, notificaciones, alertas y comunicaciones que deban efectuarse.
- 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.

- 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.
- Almacenar en una ubicación distinta a la de procesamiento copias de resguardo.
- 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.
- Verificar periódicamente la efectividad de los procedimientos de copias y restauración.
- Cifrar las copia de resguardo de información crítica.

8.4. Registro de actividad y monitoreo

8.4.1. *Registro de eventos*

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

Se deben 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 deben registrar mínimamente los siguientes datos:

- Inicio y cierre de sesión.
- Identificación del usuario.
- Identificación del equipo.
- Direcciones de redes y protocolos.
- Fecha y hora del evento.
- Descripción del evento.
- Registros de intentos de acceso al sistema exitosos y fallidos.

- Registros de intentos de acceso a los datos u otro recurso, exitosos y rechazados.
- Cambios de configuración del sistema.
- Ejecución de aplicaciones de sistemas.
- Archivos accedidos y el tipo de acceso.
- Activación y desactivación de los sistemas de protección.

8.4.2. ***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.

8.4.3. ***Actividad de los administradores y operadores***

Se deberá controlar periódicamente la actividad de los usuarios administradores y operadores de sistemas.

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

8.4.4. ***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.

8.5.Control en la instalación de software

8.5.1. ***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.

Se debe 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 analistas de desarrollo del software que se desea poner en producción.

8.6. Gestión de vulnerabilidades técnicas

8.6.1. *Vulnerabilidades técnicas y remediación*

Se deben adoptar medidas para minimizar o eliminar riesgos ante vulnerabilidades técnicas.

Se debe implementar el control de cambios, imponiendo el cumplimiento de procedimientos formales que garanticen que se cumplan pautas de seguridad y control. En este sentido, se deberá verificar que los cambios cumplan con los requisitos solicitados y se cuente con las autorizaciones necesarias.

Asimismo, se deben 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.

8.6.2. *Restricciones en la instalación de software*

Se prohíbe la instalación de software que no cuente con la autorización del Responsable de Seguridad de la Información. 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 normas complementarias, como así también el tipo de licenciamiento designado por el autor del mismo.

8.7.Auditoría de los sistemas en producción

8.7.1. *Controles de auditoría en los sistemas de información*

Se deberán planificar y definir cuidadosamente las actividades de auditoría a realizar sobre los sistemas en producción, con el objeto de minimizar el impacto en la SSN. Para ello, se definirán los procedimientos formales aplicables.

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

Se protegerá el acceso a los elementos utilizados en las auditorías de sistemas 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.

9. POLÍTICA EN LA GESTIÓN DE COMUNICACIONES

Objetivo

- Procurar la protección de las comunicaciones en las redes del organismo y a través de los canales de intercambio de información que el organismo establezca para el cumplimiento de sus funciones.

9.1. Gestión en la seguridad en las redes de datos

9.1.1. *Controles en las redes de datos*

Se deberán restringir las conexiones a los puertos de los dispositivos de red, permitiendo 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 circulan en las redes 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 deberán controlar los equipos informáticos que se conecten hacia y desde internet. Tal control deberá ser efectuado a través de dispositivos de seguridad que inspeccionan el

tráfico saliente y entrante, con el objeto de evitar que la navegación transgreda las normas que se establezcan.

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

9.1.2. *Seguridad de los servicios activos*

El Responsable de la Seguridad de la Información definirá las pautas para garantizar la seguridad de los servicios de red de la SSN. Dichos servicios activos deberán ser revisados periódicamente, proponiendo recomendaciones cuando sea necesario.

Se deberán seguir expresamente las siguientes directivas:

- Mantener instalados y habilitados sólo aquellos servicios que sean utilizados.
- Controlar el acceso lógico a los servicios, tanto su uso como su administración.
- Configurar cada servicio de manera segura, siguiendo las recomendaciones de buenas prácticas de seguridad del servicio en cuestión.
- Instalar periódicamente las actualizaciones de seguridad.
- Evaluar periódicamente la seguridad de los servicios.

9.1.3. *Segregación de redes*

Con el fin de restringir el acceso indebido se deberá segregar el tráfico de datos que circulan por las redes de la SSN 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.

9.2. Intercambio de información con partes externas

9.2.1. ***Procedimientos y controles de intercambio de información***

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

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

Los servicios que se exponen hacia internet deben estar protegidos ante amenazas externas.

Se deberán implementar controles para la detección de código malicioso que puede ser transmitido desde internet hacia las redes de la SSN.

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.

9.2.2. ***Acuerdos en los intercambios de información con entidades externas***

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

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

10.POLÍTICA DE USO DE CORREO ELECTRÓNICO

Objetivo

- Reducir los riesgos en las comunicaciones oficiales enviadas por correo electrónico institucional mediante la implementación de medidas y controles de seguridad.

10.1. Tipos de cuentas de correo electrónico

10.1.1. ***Cuentas de correo personales***

Son las usadas por personas que revisten las siguientes categorías o pertenecen a alguno de los siguientes agrupamientos:

- Funcionarios públicos.
- Empleados.
- Otras personas que soliciten formalmente para uso justificado.

El responsable de una cuenta de correo personal es el titular (usuario) de la misma. Sólo se permite una cuenta de correo personal por persona.

10.1.2. ***Cuentas de correo no personales o de organismos***

Además de las cuentas de correo personales, los responsables de las distintas Gerencias o unidades del organismo podrán solicitar la creación de cuentas de correo no personales o de organismo, siempre que estén justificadas y sean necesarias para el normal funcionamiento de la misma.

Las cuentas de correo no personales estarán vinculadas a un área o dependencia del organismo, siendo la autoridad del área o dependencia el responsable de la cuenta.

Las cuentas de correo no personales serán dadas de alta como grupos y sus miembros serán los indicados por el área que requiera su creación. Esta última tiene la responsabilidad de solicitar las altas y bajas que se requieran de miembros y administradores.

Los miembros de las cuentas de correo no personales serán exclusivamente cuentas de correo personales del organismo. De manera excepcional, se podrá incluir a un tercero o proveedor, cuando las circunstancias así lo justifiquen, quedando expresamente prohibida la incorporación como miembro de cuentas de correo particulares de personal del organismo.

De manera excepcional, cuando las tareas operativas del área a cargo de las tecnologías de la información y de las comunicaciones así lo requieran y la cuenta de correo no personal no pueda ser generada como grupo, se podrán asignar cuentas de correo de servicios para el envío, entre otros, de notificaciones y alertas. En tales casos, se individualizará al responsable de la cuenta, quien será el único con acceso a la misma.

Las cuentas de correo no personales no pueden ser usadas bajo ningún concepto para otros fines que no sean los propios del área o dependencia a la que pertenece y que motivaron su creación.

10.2. Asignación de cuenta de correo electrónico

El área responsable de las tecnologías de la información y de las comunicaciones asignará una cuenta de correo electrónico a todo el personal dado de alta, conforme el área de recursos humanos lo informe. Asimismo, podrá asignar una cuenta de correo electrónico a las personas relacionadas con el organismo autorizadas a tener una cuenta de correo oficial por funcionario con jerarquía no menor a Subgerente.

10.3. Formato de las cuentas de correo electrónico

Las cuentas de correo electrónico tendrán un nombre (login) y un dominio de correo. El formato de las cuentas de correo electrónico personales será: napellido@ssn.gob.ar, donde "n" constituye la inicial del nombre seguido del apellido del usuario.

No se podrán asignar alias genéricos a las cuentas de correo personales.

10.4. Límites y parámetros de gestión de correo electrónico

Se aplicarán con carácter general los siguientes límites y parámetros al momento de gestionar el servicio de correo electrónico:

- Tamaño de la cuenta (incluye otros servicios vinculados): 50GB.
- Tiempo máximo de inactividad de una cuenta: 60 días.
- Antigüedad máxima de una dirección de correo bloqueada para cancelar: 30 días.
- Tamaño máximo de archivo adjunto saliente: 25 MB.

10.5. Estados de una cuenta de correo electrónico

Las referencias tendrán en cuenta los siguientes estados de una cuenta de correo:

- Activa: una cuenta de correo está activa cuando puede enviar y recibir mensajes con normalidad.
- Inactiva: una cuenta de correo se considera inactiva cuando no se registra actividad (ingreso a la cuenta, envío de correo, etc.) por parte de un usuario.
- Bloqueada o suspendida: una cuenta de correo está bloqueada o suspendida

cuando no puede recibir mensajes.

- Cancelada: una cuenta de correo cancelada es una cuenta eliminada. Los mensajes dirigidos a una cuenta cancelada son rechazados devolviendo un mensaje de "cuenta de correo desconocida o inexistente". Una cuenta puede eliminarse por haberse cumplido el plazo de antigüedad máxima de una cuenta bloqueada, por cese de actividad o bien por solicitud de baja de una cuenta de correo no personal.

10.6. Uso responsable del correo electrónico

El uso del servicio de correo electrónico laboral está sujeto a las pautas generales establecidas en este documento, así como a las pautas específicas que se dispongan para este propósito. El acceso a la cuenta de correo electrónica asignada presupone la aceptación de las pautas de uso obligatorias, comunicadas a través de las vías oficiales correspondientes.

El usuario de una cuenta de correo electrónico del organismo se compromete a aceptar y cumplir los siguientes términos y condiciones que con carácter general se aplican a todos los servicios:

- Los usuarios son completamente responsables de todas las actividades realizadas con sus cuentas de correo institucionales.
- No deberán facilitar u ofrecer la cuenta de correo personal (la clave de acceso al servicio) a terceras personas.
- El correo electrónico es una herramienta para el intercambio de información entre personas, y no, una herramienta de difusión masiva e indiscriminada de información. Para ello existen otros canales más adecuados y efectivos. No resulta correcto el envío de correo a personas que no desean recibirlo. Si las autoridades del organismo reciben quejas, denuncias o reclamaciones por estas prácticas se tomarán las medidas sancionatorias adecuadas a la falta descripta.
- Se encuentra expresamente prohibido:
    - utilizar el correo electrónico para cualquier propósito comercial o

financiero.

- participar en la propagación de correos encadenados o en esquemas piramidales o temas similares. O la distribución de forma masiva de grandes cantidades de mensajes con contenidos inapropiados para nuestra organización.
- La suscripción a foros de discusión y/o grupos de noticias utilizando la cuenta de correo institucional.

Para asegurar un normal funcionamiento del servicio y un uso eficiente de los recursos del sistema de correo el usuario se compromete a:

- Revisar periódicamente su correo.
- Comunicarse con los administradores de correo electrónico del organismo cuando prevea no poder revisar el correo durante un intervalo de tiempo largo.
- Avisar de cualquier incidencia que pueda surgir y que estime puede afectar al normal comportamiento del servicio.

Si, en el ejercicio de sus funciones, el personal informático detectara cualquier anomalía que muestre indicios de usos ilícitos o contrarios a esta reglamentación, lo pondrá en conocimiento de la autoridad competente del organismo para que se tomen las medidas necesarias.

10.7. Uso indebido del correo electrónico

Los usos indebidos (que pueden constituir también usos ilegales) del correo electrónico del organismo pueden acarrear sanciones institucionales. Estos usos incorrectos incluyen, pero no se limitan a los siguientes:

- Enviar mensajes o material no solicitados que sean fraudulentos, difamatorios, discriminatorios, ofensivos, intimidantes, o de naturaleza amenazante.
- Intentar o apoderarse de claves de acceso de otros usuarios.
- Intentar acceder y/o modificar mensajes de otros usuarios.
- Usar el servicio de correo electrónico del Ministerio para propósitos no laborales, fraudulentos, comerciales o publicitarios.

- Enviar mensajes destructivos, obscenos o que contengan opiniones que atenten contra la dignidad o el honor de terceros.
- Utilizar el correo electrónico en suscripciones a listas de correos electrónicos o foros externos que no tengan relación con sus funciones dentro del organismo.
- Utilizar algún mecanismo que intente ocultar la identidad del emisor de correo electrónico.
- Hacer uso del correo institucional para la divulgación de información confidencial en contravención a lo estipulado en la legislación vigente.

10.8. Seguridad del correo electrónico

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

Se implementarán políticas que añadan un factor adicional de autenticación a la credencial de acceso (usuario y contraseña) del correo electrónico, pudiendo emplearse tokens físicos, tokens por email o app u otro método seguro que a tal efecto se determine. Se evitará el empleo de token SMS.

Se prohíbe adjuntar en la cuenta de correo electrónico laboral binarios ejecutables.

10.9. Privacidad y confidencialidad de la información

La SSN no realizará inspecciones de cuentas de correo electrónico sin el consentimiento del usuario, salvo en las circunstancias que a continuación se detallan. En estos casos, expresamente consignados, la SSN puede, a través del procedimiento establecido, inspeccionar y cerrar una cuenta o copiar su información para prevenir la alteración, destrucción y pérdida de información, sin el consentimiento del usuario del correo electrónico, conforme a la ley aplicable. Los supuestos son:

- Requisitoria de autoridad competente por denuncia o requerimiento legal.
- Sospecha de violación de la política interna de la institución o de las leyes vigentes.
- Circunstancias de emergencia, donde no actuar pudiera repercutir gravemente

en el servicio del organismo.

No constituyen inspecciones en los términos de lo dispuesto en este punto y quedan exceptuados del consentimiento del usuario los controles de seguridad del correo electrónico, conforme lo establece el punto 10.3.

10.10. Acceso al correo desde teléfonos celulares

El acceso a la cuenta de correo laboral a través de teléfonos celulares no administrados por el organismo está destinada a funcionarios con cargo igual o superior a Coordinador. El acceso de otros agentes a la cuenta de correo desde sus teléfonos celulares requiere la autorización por parte del titular del área, con cargo igual o superior a Subgerente.

Conjuntamente con las revisiones de accesos que se fijen, se controlará la vigencia de los permisos referidos.

11.POLÍTICA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Objetivo

- Fomentar la integración de la seguridad de la información en todos los sistemas a lo largo de su ciclo de vida.

11.1. Responsabilidad

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 la SSN en donde residan los desarrollos mencionados.

El Responsable de Seguridad de la Información junto con el Propietario de la Información definirán los controles y requerimientos de protección a ser implementados en los sistemas desarrollados internamente o por terceros. Asimismo, asignará, según corresponda, las funciones de "implementador" y "administrador de programas fuentes" al personal de su área que considere idóneo.

El "implementador" tendrá como funciones principales: a) la coordinación de la implementación de modificaciones o nuevos programas en el ambiente de producción; b) 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; c) 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; y d) rechazar la implementación en caso de encontrar defectos y/o si faltara la documentación estándar establecida.

Por su parte, el administrador de programas fuentes tendrá las funciones que se establecen en el punto 5.4.8.

11.2. Requerimientos de seguridad de los sistemas

11.2.1. *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. Por este motivo, se fomentará que el Responsable de la Seguridad de la Información o quien éste designe forme 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.
- 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.
- 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.

11.2.2. *Seguridad en los servicios accedidos desde redes públicas*

Se deberán implementar controles de seguridad que den soporte a todos los sistemas de la SSN. A estos efectos se tomarán en consideración:

- Vulnerabilidades de la información en los sistemas de oficina. Por ejemplo, la grabación de llamadas telefónicas o teleconferencias.
- Procedimientos y controles apropiados para administrar la distribución de información, como ser el uso de boletines electrónicos institucionales.
- Exclusión de categorías de información sensible de la SSN 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 trabajan en proyectos sensibles.
- La aptitud del sistema para dar soporte a las aplicaciones de la SSN, 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 determinados recursos o servicios a categorías específicas de usuarios.
- Retención y resguardo de la información almacenada en el sistema.
- Requerimientos y disposiciones relativos a sistemas de soporte de reposición de información previa.

11.2.3. ***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 de la SSN.

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 referida a la 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.

11.3. Seguridad en procesos de desarrollo

11.3.1. *Desarrollo seguro de software*

Se deberán establecer pautas para el desarrollo seguro de software aplicables a todo desarrollo de aplicaciones y sistemas de información dentro de la SSN como así también el realizado por terceros.

Se procurará involucrar al Responsable de la Seguridad de la Información en el ciclo de vida de desarrollo de los sistemas de información desde el inicio con el objeto de validar la arquitectura de seguridad.

Algunos de los requisitos a 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.

11.3.2. ***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. Para ello se deberán tomar en cuenta las siguientes consideraciones:

- Efectuar las actividades relativas al cambio en el ambiente de desarrollo y en el ambiente de testing.
- Obtener la aprobación por parte del usuario autorizado y del área de pruebas mediante pruebas en el ambiente correspondiente.
- Solicitar la autorización del Propietario de la Información, en caso de tratarse de cambios a sistemas de procesamiento de la misma.
- 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.
- Verificar que los cambios sean propuestos por usuarios autorizados y respeten los términos y condiciones que surjan de la licencia de uso.

11.3.3. ***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.

11.3.4. ***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.

11.3.5. ***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.

11.3.6. ***Tercerización del desarrollo de software***

En aquellos casos en los que se tercerice el desarrollo de software, el proveedor velará por el cumplimiento de los estándares de seguridad de la industria, asegurando una adecuada revisión del código, como así también el cumplimiento de los requerimientos de desarrollo mencionados en la presente política.

Se elaborarán acuerdos de licencias, propiedad de código y derechos conferidos.

Se considerará 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.

11.3.7. ***Seguridad en los entornos de desarrollo***

Se deberán implementar controles para proteger adecuadamente los entornos en los que se efectúan 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:

- Separación de entornos, conforme a lo señalado en el punto correspondiente.
- Seguridad en los datos de prueba y datos en producción que el sistema procesará, almacenará y transmitirá.
- Control de acceso al código fuente.
- Monitoreo del cambio en el código y en el entorno que lo almacena.
- Procedimiento de control de cambios.
- Revisión después de cambios en los sistemas operativos.
- Restricción del cambio de paquetes de software.
- Cambio de Paquetes de Software.
- Control de los aspectos de seguridad en el desarrollo de sistemas, tanto realizado por personal propio como por terceros.
- Copias de respaldo.

11.3.8. ***Evaluación de requisitos funcionales***

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

11.3.9. ***Evaluación de vulnerabilidades de seguridad***

Se procurará la realización de evaluaciones de seguridad en búsqueda de vulnerabilidades sobre los nuevos sistemas a implementar, 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.

11.4. Datos de prueba y operativos

11.4.1. ***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 al finalizar las pruebas.

11.4.2. ***Cambios a datos operativos***

La modificación, actualización o eliminación de los datos operativos deberán ser realizadas solo a través de los sistemas que procesan dichos datos y de acuerdo con el esquema de control de accesos implementado en los mismos. 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 las excepciones señaladas, teniendo en cuenta las siguientes pautas:

- 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 o grupos de usuario de emergencia para ser utilizadas en la ejecución de excepciones. Las mismas serán protegidas mediante contraseñas 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.

12. POLÍTICA DE SEGURIDAD EN LA RELACIÓN CON LOS PROVEEDORES

Objetivo

- Promover la protección de los activos de la organización accesibles a los proveedores.

12.1. Seguridad en la relación con proveedores

12.1.1. ***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 de la SSN.

12.1.2. ***Seguridad dentro de los acuerdos de los proveedores***

Se deberán establecer y documentar los acuerdos para garantizar que no existen discrepancias entre la SSN 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 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 identifican algunos de los términos que se podrán incluir en los acuerdos con el fin de poder satisfacer los requisitos de seguridad de la información identificados:

- 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.
- Requisitos legales y normativos, en especial los aspectos sobre protección de datos personales y los derechos de propiedad intelectual.
- Obligación de cada parte de implementar un conjunto de controles acordados, incluido el control de acceso, la revisión de desempeño, el monitoreo, los informes y la auditoría.
- Reglas de uso aceptable de la información, pudiendo incluirse un listado de lo que se considera uso inaceptable, en caso de ser necesario.
- Una lista del personal autorizado para acceder a/o recibir la información o los procedimientos o condiciones de la SSN para su autorización, y el retiro de la autorización para el acceso a/o la recepción de la información de la SSN al personal del proveedor.
- Requisitos y procedimientos de la administración de incidentes (en especial la notificación y la colaboración durante la remediación de incidentes).
- Requisitos de capacitación y concientización para procedimientos específicos

y requisitos de seguridad de la información.

- Normativas pertinentes para la subcontratación, incluidos los controles que se deben implementar.
- Socios de acuerdos pertinentes, incluida una persona de contacto para los asuntos de seguridad de la información.
- 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 generan dudas o inquietudes.
- Derecho a auditar los procesos y los controles del proveedor relacionados con el acuerdo.
- Procesos de resolución de defectos y resolución de conflictos.
- Declaración por parte del proveedor de su obligación de cumplir con la Política de Seguridad de la Información y demás requisitos de seguridad de la SSN.

12.1.3. ***Cadena de suministro de la tecnología de información y comunicación***

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

- Definir los requisitos de seguridad de la información que se aplicarán en los procesos de adquisición de tecnologías, productos o servicios de información y comunicación.
- Implementación de un proceso de monitoreo y métodos aceptables para validar que los productos y servicios de tecnología de información y comunicación están de acuerdo con los requisitos de seguridad establecidos.
- 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 de la SSN.

- Obtención de una garantía de que los componentes críticos y su origen se pueden rastrear en toda la cadena de suministros.
- Obtener la garantía de que los productos de tecnología de información y comunicación entregados funcionan según lo esperado y no contienen ninguna función inesperada o no deseada.
- Definición de las reglas para compartir la información en cuanto a la cadena de suministro y cualquier posible problema y compromiso entre la SSN y los proveedores.
- 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.

12.2. Administración de la prestación de servicios de proveedores

12.2.1. *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 son manejados en forma apropiada.

Se procurará asegurar 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.

12.2.2. *Gestión de cambios en la prestación de servicios*

El proceso de gestión de servicios de terceros deberá tener en cuenta los siguientes cambios en la SSN:

- Actualización de las políticas y procedimientos de la SSN.
- Actualización de los servicios ofrecidos por la SSN.
- Actualización de aplicaciones o nuevos sistemas.
- Implementación de nuevos controles de 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.

13.POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD

Objetivo

- Identificar y gestionar de manera adecuada los eventos e incidentes de seguridad de la información.

13.1. Gestión de incidentes de seguridad y mejoras

13.1.1. ***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 de 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 Responsable de la Seguridad de la Información y a la Gerencia de Asuntos Jurídicos, de considerarlo necesario, y la notificación a la Dirección Nacional de Ciberseguridad, dentro del plazo y por la vía que la normativa vigente establece.

El personal abocado a tareas de ciberseguridad podrá 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 tecnológicos de la SSN.

13.1.2. ***Notificaciones de eventos, fallas o anomalías***

Los eventos 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 detecten un evento sospechoso de seguridad o incidente, fallas o debilidades en el uso regular de los sistemas tecnológicos o anomalías del software instalado, deberán comunicarlo inmediatamente al Responsable de la Seguridad de la Información a través de la vía establecida.

Todos los agentes, 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.

Está expresamente prohibido a usuarios no afectados a tareas de ciberseguridad expresamente autorizados por el área responsable de las tecnologías de la información y de las comunicaciones realizar pruebas para detectar y/o explotar supuestas debilidades o fallas de seguridad.

13.1.3. ***Valoración de los eventos de seguridad***

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

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

13.1.4. ***Respuesta a los incidentes de seguridad***

Todo incidente de seguridad deberá ser respondido siguiendo los procedimientos establecidos. El procedimiento de respuesta al incidente de seguridad podrá incluir:

- Recopilación de la evidencia, con la mayor inmediatez a la ocurrencia del incidente.
- Realizar análisis forenses.
- Asegurarse de que todas las actividades de respuesta se realicen correctamente para el posterior análisis.
- Comunicar de la existencia del incidente de seguridad de la información o cualquier detalle pertinente a todas las personas y áreas con incumbencia y necesidad de conocer tal circunstancia.
- Notificar al Responsable de la Seguridad de la Información ante el escalamiento del incidente de seguridad.
- 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 confirmar el origen del mismo.

13.1.5. ***Aprendizaje de los incidentes de seguridad de la información***

Se deberán documentar y monitorear los tipos y volúmenes de las anomalías e incidentes de seguridad. Esta información se utilizará para identificar y evaluar aquellos que sean recurrentes o de alto impacto.

13.1.6. ***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 judicial.

Para lograr la validez de la evidencia, la SSN 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 ello, se establecen los siguientes requisitos:

- Almacenar los documentos en forma segura y mantener registro 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.
- 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.

14.POLÍTICA DE GESTIÓN DE LA CONTINUIDAD

Objetivo

- Determinar las necesidades para garantizar el nivel requerido de continuidad de las operaciones durante una situación adversa.

14.1. Gestión de continuidad de las operaciones

Se deberá establecer un plan de contingencia para actuar ante incidentes que produzcan la interrupción de la continuidad de las operaciones en la SSN, a fin de garantizar que la restauración de las operaciones sea un proceso ordenado y consistente.

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

- Identificación y priorización de los procesos críticos de las actividades de la SSN.
- Identificación de las amenazas que pudieran 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 o atentados.
- Asignación de responsabilidades.
- Establecimiento de una estructura de gestión.
- Documentación de la estrategia de continuidad de las actividades consecuente

con los objetivos y prioridades acordados.

- Comunicación y capacitación del personal en materia de procedimientos y procesos de emergencia acordados a través de procedimientos de recuperación.

14.1.1. ***Procedimientos para la continuidad en situaciones de emergencia***

Se deberán mantener los requisitos de seguridad de la información en los planes de continuidad de las operaciones que dan respuesta a situaciones de emergencia.

Se deberán establecer procedimientos de recuperación de desastres para diferentes escenarios de contingencia.

Se deberá nominar al personal de respuesta ante incidentes con la responsabilidad, autoridad y la competencia en los distintos niveles técnicos, comunicaciones y jerárquicos, para ejecutar el procedimiento de recuperación de desastres.

Se deberá establecer una estructura de administración adecuada para prepararse a mitigar y responder ante un evento disruptivo, con personal técnico y la competencia necesaria.

Se deberá desarrollar un plan documentado, procedimientos de respuesta y recuperación, detallando como la SSN administrará un evento disruptivo y mantendrá la seguridad de su información a un nivel predeterminado.

14.1.2. ***Verificación, revisión y evaluación de la continuidad de la seguridad de la información***

Se deberán realizar revisiones periódicas de los planes de continuidad de las operaciones, implementado a través de la planificación de pruebas para evaluar la efectividad de la misma. Esta actividad será llevada a cabo con la activa participación de los Propietarios de la información y recursos de información de que se trate, el Responsable de Seguridad de la Información y el personal que el titular del área responsable de las tecnologías de la información y de las comunicaciones designe.

14.2. Redundancia en las instalaciones de procesamiento y transmisión de la información

Se deberán 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.

15.POLÍTICA DE CUMPLIMIENTO

Objetivo

- Prevenir incumplimientos a la normativa legal aplicable en el tratamiento de información.

15.1. Cumplimiento de requisitos legales

15.1.1. ***Identificación de la legislación aplicable***

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

15.1.2. ***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 agentes podrán utilizar únicamente material autorizado por la SSN. La SSN sólo 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.

Los usuarios solo podrán utilizar software autorizado por el organismo según las condiciones de instalación descripta en el punto pertinente.

15.1.3. ***Protección de los registros de la SSN***

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 eliminados cuando el propietario de dicha cuenta fuera desvinculado de la SSN. Los registros de las cuentas de correos electrónicos 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 judicial.

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.

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 violación a la Ley N°17.622 y concordantes.

15.1.4. ***Protección de datos personales***

Todos los empleados deben conocer y respetar las restricciones al tratamiento de los datos y de la información respecto a la cual tengan acceso con motivo del ejercicio de sus funciones. Para ello, cuando el organismo lo considere necesario, se requerirá a los agentes, funcionarios y a los terceros que interactúen con el organismo la firma de un acuerdo de confidencialidad.

15.1.5. ***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 agentes deben conocer el alcance preciso del uso adecuado de los recursos informáticos y deberán respetarlo. En particular, se deberá respetar lo dispuesto en la ley 25.188 de Ética en el ejercicio de la función pública, la que establece, entre otros aspectos, 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.

15.2. Revisiones de cumplimiento de seguridad

15.2.1. ***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 que deberá realizar el Responsable de la Seguridad de la Información y permitirá incluir oportunidades de mejora en los objetivos de control y cambios en el enfoque de seguridad existente.

15.2.2. ***Cumplimiento de la Política y Procedimientos de Seguridad***

Los responsables de cada área deberán velar por el correcto cumplimiento de las normas y procedimientos de seguridad establecidos y brindarán apoyo a las revisiones de cumplimiento, efectuadas por el Responsable de la Seguridad de la Información.

El Responsable de la Seguridad de la Información tendrá la autoridad de realizar revisiones periódicas en todas las áreas de la SSN a efectos de garantizar el cumplimiento de las políticas, normas y procedimientos de seguridad vigentes.

15.2.3. ***Verificación de cumplimiento en los sistemas de información***

Se verificará periódicamente que los sistemas de información cumplan con la normativa de seguridad de la información. Las verificaciones 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 supervisión.

Anexo. Glosario

Activos de información

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

Amenaza

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

Archivo, registro, base o banco de datos

Indistintamente, designan al conjunto organizado de datos que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.

Ataque

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

Ataque informático

Ciberataque.

Auditabilidad

Define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

Autenticación

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

Ciberataque

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

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.

Confidencialidad

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

Continuidad operacional

Refiere a la continuidad de los procesos de gestión y su recuperación ante la ocurrencia de un evento o incidencia.

Control

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

Control de acceso

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

Datos personales

Información de cualquier tipo referida a personas humanas o de existencia ideal determinadas o determinables.

Datos sensibles

Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

Disociación de datos

Todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable.

Disponibilidad

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

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.

Evento de seguridad de la información

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

Incidente de seguridad de la información

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

Información

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

Integridad

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

Mínimo privilegio

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

Recurso

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

Riesgo

Es la combinación de la probabilidad de ocurrencia de una amenaza y su impacto si la misma tuviera éxito. Efecto de la incertidumbre sobre los objetivos.

Sistema de información

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

Titular de los datos

Toda persona humana o jurídica cuyos datos sean objeto de tratamiento.

Tratamiento de riesgos

Se refiere al proceso de selección e implementación de controles para modificar el riesgo.

Vulnerabilidad

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

República Argentina - Poder Ejecutivo Nacional
AÑO DE LA DEFENSA DE LA VIDA, LA LIBERTAD Y LA PROPIEDAD

Hoja Adicional de Firmas
Informe gráfico

Número: IF-2024-87142162-APN-GCG#SSN

CIUDAD DE BUENOS AIRES
Jueves 15 de Agosto de 2024

Referencia: Política de Seguridad de la Información

El documento fue importado por el sistema GEDO con un total de 83 pagina/s.

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2024.08.15 17:16:05 -03:00

Pablo Andrés MUSTICCHIO
Subgerente
Gerencia de Coordinación General
Superintendencia de Seguros de la Nación

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2024.08.15 17:16:05 -03:00