ANEXO I

LINEAMIENTOS GENERALES DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. INTRODUCCIÓN

La seguridad de la información implica la protección de la información ante un rango amplio de amenazas, con el objeto de minimizar los riesgos a los que se encuentra expuesta y asegurar la continuidad de la operación normal del organismo. Tiene por objetivo principal la preservación de la confidencialidad, integridad y disponibilidad de la información.

Dentro del Sector Público Nacional (S.P.N.), la seguridad de la información es importante para el desarrollo de sus actividades y la protección de las infraestructuras críticas de información que proveen servicios esenciales a la sociedad. En este aspecto, el S.P.N. ejerce un rol regulatorio que lo obliga a velar por la seguridad de los datos tratados y servicios brindados.

En el ámbito de esta Superintendencia de Riesgos del Trabajo (S.R.T.) y en el marco de las funciones otorgadas por la Ley N° 24.557, ésta genera y brinda información a la ciudadanía que es considerada un factor clave para la toma de decisiones, y constituye el eje sobre el cual gravitan los procesos y sistemas de gestión desarrollados en el organismo.

Es decir, la información es un activo que, como otros bienes y servicios requeridos para el cumplimiento de los objetivos del organismo, resulta esencial para el desarrollo de las actividades de su competencia. Asimismo, la S.R.T. trata con datos catalogados como sensibles por la Ley N° 25.326 de Protección de Datos Personales. En consecuencia, la información que gestiona, de acuerdo a su criticidad, necesita ser protegida adecuadamente en todo el ámbito de la S.R.T., ya que, como cualquier organización en la actualidad, enfrenta amenazas de seguridad en sus sistemas y redes de información, cada vez más frecuentes y sofisticadas.

Dicha información puede presentarse en diversos formatos (almacenada electrónicamente; transmitida por correo o utilizando otros medios electrónicos; como contenido multimedial; impresa o escrita en papel, entre otros). Pero sin perjuicio del formato en que se encuentre y del soporte que se utilice, debe estar apropiadamente protegida durante todo su ciclo de vida: desde su creación hasta su eventual destrucción, desuso o archivo definitivo.

Por su parte, dada su importancia y carácter, dicha información debe ser administrada al mismo nivel que los recursos económicos, materiales y humanos con los que cuenta el organismo, debiendo éste ajustarse y cumplir con los requisitos necesarios para recibir, resguardar, administrar y suministrar correctamente la información del Sistema de Riesgos del Trabajo.

En dicho contexto, una adecuada gestión de la seguridad de la información permite proteger los recursos de ésta y la tecnología utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar la confidencialidad, integridad, disponibilidad de la información, así como el cumplimiento de las normas aplicables.

En esa línea, la Política de Seguridad de la Información de la S.R.T. (PSI) se desarrolla en pos de los Requisitos Mínimos de Seguridad de la Información para los Organismos del Sector Público Nacional, establecidos por la Decisión Administrativa de Jefatura de Gabinete de Ministros N° 641/2021, en función de sus competencias, los riesgos a los que se expone y a los recursos disponibles.

Para lograr un estado de protección adecuado resulta necesario implementar un conjunto de mecanismos de seguridad o controles que incluyen, entre otros, procesos, políticas, procedimientos, definición de responsabilidades, software y hardware. Asimismo, se necesita definir, establecer, implementar, monitorear, revisar y mejorar estos mecanismos para fortalecer el cumplimiento de los objetivos de seguridad específicos. Esto se debe realizar en forma coordinada con otros procesos de gestión de la S.R.T..

Del mismo modo, los procesos, sistemas y redes de apoyo son también activos importantes. Definir, lograr, mantener y mejorar la seguridad de la información es esencial para preservarlos, mantener la eficacia en la operación, cumplir con el marco legal y las normas internas, y proteger la información de las y los trabajadores.

En consecuencia, es preciso establecer una PSI que defina las directivas necesarias para lograr la protección de dicha información de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información y de la operación de la S.R.T., minimizar los riesgos del daño y asegurar el efectivo cumplimiento de sus objetivos.

En tal orden, resulta importante que los principios de la PSI sean parte de la cultura organizacional. Establece el compromiso por parte de las máximas autoridades del organismo y de los titulares de Unidades Organizativas para su difusión, consolidación y cumplimiento, tanto por parte del personal como de terceros que puedan tener acceso a datos, recursos y/o sistemas de información.

2. OBJETIVO

La presente PSI establece las directrices y líneas de acción en materia de seguridad de la información para que la S.R.T. gestione de manera segura y proteja la información a la que da tratamiento, incluyendo los recursos tecnológicos que utiliza y los servicios que brinda. Son sus objetivos:

- Definir el propósito, la dirección, los principios, las reglas básicas y los mecanismos de comunicación para la protección de la información del organismo y de los recursos utilizados en su tratamiento; asegurar su uso como base para establecer un conjunto de normas, procedimientos, lineamientos y guías acordes a los procesos que se llevan adelante en la S.R.T., su plataforma tecnológica y demás recursos de los que dispone.

- Proteger los derechos de los titulares de los datos personales procesados, así como de la información propia de la S.R.T..

- Fomentar la inclusión de aspectos de seguridad de la información en la cultura organizacional de la S.R.T..

3. ALCANCE

A partir de la entrada en vigencia de la presente política de seguridad, será de aplicación obligatoria en todo el ámbito de la S.R.T., a su personal -cualquiera sea su modalidad contractual- y a la totalidad de sus procesos, así como a todas las relaciones con terceros -cualquiera fuere la vinculación directa, indirecta o por interpósita persona con el organismo- siempre que impliquen el acceso de estos a datos, recursos y/o sistemas de información propios de esta Superintendencia.

4. PRINCIPIOS BÁSICOS

Los principios de la seguridad de la información adoptados por la S.R.T. son la confidencialidad, la integridad y la disponibilidad de la información a la que le da tratamiento y de los activos de información utilizados para su gestión.

Uno de los pilares en la gestión actual del organismo es lograr una mejora continua de los procesos de gestión de seguridad de la información, asegurando su eficacia y eficiencia. En consecuencia, incorpora la gestión de la seguridad de la información como parte integrante de la gestión del resto de los procesos establecidos en su ámbito.

La S.R.T. establece sus requisitos de seguridad de la información en base a un análisis y evaluación de riesgos sobre sus activos de la información.

El presente documento se dicta en cumplimiento de las disposiciones legales vigentes tanto generales como las particulares dictadas por el organismo.

Se establece como falta el incumplimiento de los lineamientos y disposiciones de esta PSI, por parte de los agentes y funcionarios, en función de lo dispuesto por el régimen sancionatorio establecido en la S.R.T.. Respecto de terceros vinculados al organismo, se aplicarán penalidades de acuerdo a lo establecido en las cláusulas estipuladas en los contratos, convenios, acuerdos o demás instrumentos que celebre el organismo con terceros.

Atento su obligatoriedad, la presente Política deberá ser comunicada fehacientemente, puesta a disposición a todos aquellos comprendidos dentro de sus alcances, a saber: funcionarios y agentes que integran la S.R.T., bajo cualquier tipo de modalidad de contratación, y todas aquellas personas vinculadas a la entidad a través de contratos, convenios, acuerdos o algún otro instrumento válido para establecer la relación con terceros, en la medida en que les sea aplicable y en las secciones que le correspondan.

Asimismo, será acompañada de acciones de capacitación y concientización a fin de poner en conocimiento su entrada en vigencia.

5. DEFINICIONES

ACTIVO DE INFORMACIÓN: Es cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para el organismo. Pueden ser sistemas de información, bases de datos, servicios de información, procesos de negocio, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones.

AMENAZA: Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, ser accidental o intencionada

ANÁLISIS 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 de la S.R.T..

COMITÉ DE SEGURIDAD DE LA INFORMACIÓN: Es el cuerpo integrado en la S.R.T. conforme a los términos del artículo 2 de la Resolución S.R.T. N° 77/20, destinado al tratamiento de temas relacionados a la Seguridad de la Información y a garantizar el apoyo manifiesto de las autoridades a las iniciativas en la materia.

EVALUACIÓN DE RIESGOS: Se refiere al proceso de comparación de los resultados del análisis del riesgo con los criterios de riesgo para determinar si el riesgo y/o magnitud son aceptables o tolerables. Ayuda a la toma de decisiones sobre el tratamiento del riesgo.

GESTIÓN DE RIESGOS: Se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

INCIDENTE DE SEGURIDAD: Refiere a cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información del organismo. Puede ser causado

mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

INFORMACIÓN: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, óptico, en papel, en pantallas de computadoras, audiovisual u otro.

MÁXIMAS AUTORIDADES: Este concepto comprende al Superintendente y Gerente General de la S.R.T..

SEGURIDAD DE LA INFORMACIÓN: Se entiende como la preservación de las siguientes características:

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

Adicionalmente, deberán considerarse los conceptos de:

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

SISTEMA DE INFORMACIÓN: Referido también como sistema o aplicativo, es un conjunto de componentes interrelacionados que trabajan juntos para recopilar, procesar, almacenar y difundir información. Apoyo automatizado a las funciones de una organización (coordinación, control, análisis y visualización de una organización).

TECNOLOGÍA DE LA INFORMACIÓN: Se refiere al hardware y software operados por el organismo o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la S.R.T., sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

TITULARES DE LAS UNIDADES ORGANIZATIVAS: Dentro de este concepto quedan incluidos los Gerentes y Subgerentes, como también en los casos que correspondan, los Jefes de Departamento de la S.R.T..

6. REVISIÓN Y ACTUALIZACIÓN

La presente PSI deberá ser revisada, a partir de su entrada en vigencia con una periodicidad no superior a los doce (12) meses, ello con el objeto de poder adaptarla a nuevas exigencias organizativas o del entorno que pudieran presentarse.

En caso de futuras actualizaciones deberán ser comunicadas a todo el personal y terceros involucrados con el organismo. Asimismo, se deberán disponer las medidas necesarias para que esté a disposición de los mencionados.

Asimismo, será motivo suficiente para su revisión y eventual actualización cualquier modificación de la normativa vigente aplicable, así como un cambio en los objetivos estratégicos del organismo o cualquier otro evento interno o externo a esta S.R.T. que pueda generar impacto en la misma.

7. RESPONSABILIDADES

A continuación, se detallarán las responsabilidades generales sobre la PSI que tendrán las diferentes áreas intervinientes de la S.R.T. en su promoción, elaboración, implementación operativa, difusión y control sobre los aspectos de seguridad plasmados en la presente, en línea con sus funciones establecidas.

Las responsabilidades específicas de las áreas, dentro del marco de sus competencias, se detallarán en los anexos, lineamientos y procedimientos que se desprendan de la presente PSI. Cabe destacar que los titulares directos de las unidades organizativas cuentan con la facultad de delegar sus funciones a las distintas áreas que se encuentren bajo su dependencia.

MÁXIMAS AUTORIDADES

- Aprobar la PSI, así como las funciones generales en materia de seguridad de la información;
- Promover dentro de la S.R.T. la gestión de la seguridad de la información como parte integral de los procesos del organismo;
- Impulsar las iniciativas que el/las áreas/s competente/s proponga/n con el objetivo de preservar la confidencialidad, integridad y disponibilidad de la información que gestiona.

COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

- Revisar y proponer a la máxima autoridad de la S.R.T. para su aprobación la PSI, así como las funciones generales en materia de seguridad de la información;
- Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área;
- Realizar el seguimiento sobre las principales iniciativas aprobadas y sobre decisiones particulares tomadas en el Comité;
- Tomar conocimiento del resultado de las evaluaciones de riesgos de Seguridad de la Información y realizar un seguimiento de los cambios significativos que afectan a los recursos de información frente a las amenazas más importantes;
- Acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la Información;
- Tomar conocimiento y realizar un seguimiento que considere pertinente de las acciones preventivas, correctivas y de mitigación ejecutadas ante la ocurrencia de incidentes de ciberseguridad;
- Garantizar que la seguridad sea parte del proceso de planificación informática del organismo;
- Promover la difusión y apoyo a la seguridad de la información dentro de la S.R.T..

RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN

- Confeccionar la Política de Seguridad de la Información;
- Desempeñarse como el punto focal ante la Dirección Nacional de Ciberseguridad;
- Revisar y actualizar la presente Política en forma anual;
- Gestionar el cumplimiento de la normativa en la materia de seguridad de la información;

- Promover la difusión de la presente Política e impulsar un programa de concientización sobre la misma para todo el personal de la S.R.T.;
- Monitorear el cumplimiento de las disposiciones de esta PSI y de las normas que se desprendan de ella;
- Presentar el Plan de Seguridad de la Información anual que contemple objetivos y actividades para llevar adelante la gestión de la seguridad de la información;
- Establecer un marco de trabajo para el análisis y evaluación de riesgos de SI;
- Gestionar el análisis y evaluación de riesgos de seguridad, acompañando las necesidades del organismo;
- Elaborar e implementar lineamientos, procedimientos y guías relacionados al establecimiento de un marco de seguridad de la información;
- Establecer y velar por la inclusión de medidas que garanticen un adecuado marco de seguridad para los procesos y activos de información.

SUBGERENCIA DE SISTEMAS

- Colaborar en el establecimiento y definición de medidas de seguridad a implementar sobre los procesos y activos de información;
- Elaborar e implementar, conjuntamente con el RSI, proyectos informáticos que puedan surgir a partir del cumplimiento de esta PSI;
- Velar por un abordaje de la seguridad de la información en todos los proyectos informáticos que se desarrollen dentro de su dependencia;
- Colaborar en el análisis y gestión de riesgos de seguridad de la información.

TITULARES DE LAS UNIDADES ORGANIZATIVAS

- Llevar a cabo las acciones necesarias para el cumplimiento de la PSI de acuerdo a las responsabilidades establecidas;
- Implementar la presente PSI en el ámbito de su competencia, y promover el cumplimiento de la misma por parte de sus equipos de trabajo y de terceros involucrados;
- Velar por un abordaje de la seguridad de la información en todos los proyectos que se desarrollen dentro de su dependencia;
- Definir la criticidad de la información de su unidad organizativa y determinar el impacto que pudiera tener la interrupción de las actividades y procesos críticos. Los titulares de las unidades organizativas serán responsables de la información y de su gestión en el ámbito de sus respectivas áreas o departamentos, elaborando el análisis de criticidad de las mismas, en pos de garantizar la confidencialidad, integridad y disponibilidad de ésta;
- Evaluar los riesgos a los que se encuentra expuesta la información que gestionan, en el marco de los criterios establecidos por el RSI;
- Gestionar, en los casos que se mantengan relaciones con terceros con acceso a datos, recursos y/o a la administración y control de la información, vinculados a través de contratos, convenios, acuerdos o demás instrumentos para establecer dicha relación, acerca de la inclusión de cláusulas respecto a sus obligaciones y responsabilidades en cuanto al cumplimiento de la Política de Seguridad de la Información y el deber de confidencialidad.

UNIDAD AUDITORÍA INTERNA

- Colaborar, en el ámbito de su competencia, en la revisión y actualización de la PSI;

- Verificar, a través de las auditorías que correspondan, el cumplimiento de la presente PSI, dentro de las distintas unidades organizativas;
- Colaborar en el control y efectuar recomendaciones sobre modificaciones en los aspectos de seguridad.

PERSONAL DE LA S.R.T.

- Conocer y cumplir con lo estipulado en la presente PSI, así como con las normas, lineamientos, procedimientos y metodologías que se desprendan de la misma;
- Actuar conforme a los requisitos de seguridad establecidos, en cumplimiento de sus funciones;
- Tratar y gestionar de manera adecuada y responsable la información, sistemas informáticos, dispositivos y ambiente tecnológico de la S.R.T. a los cuales se brinde acceso.

8. LINEAMIENTOS ESPECÍFICOS

ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

Se desarrollará e implementará un marco organizativo que habilite una efectiva gestión y operación de la seguridad de la información en la S.R.T., teniendo en cuenta la segregación de las funciones, en la medida de lo posible, y la asignación de áreas de responsabilidad que no entren en conflicto, ello en miras de incrementar los niveles de seguridad de la información. Asimismo, las autoridades impulsarán las iniciativas de seguridad de la información que el área competente proponga con el objetivo de preservar la confidencialidad, integridad y disponibilidad de la información que gestiona.

Se establecerán lineamientos de seguridad para todas las relaciones con terceros que impliquen el acceso a datos, recursos y/o sistemas de información. Se instrumentará la inclusión de cláusulas a través de contratos, convenios, acuerdos o demás instrumentos para establecer dicha relación, y se suscribirán convenios de confidencialidad en función de las responsabilidades que correspondan, en caso de ser necesario.

Se abordarán los aspectos referidos a la seguridad de la información en el diseño y gestión de los proyectos que lleve adelante el organismo, y en el establecimiento de medidas de seguridad para la modalidad de trabajo remoto y el uso de dispositivos móviles.

SEGURIDAD INFORMÁTICA DE LOS RECURSOS HUMANOS

El personal que se desempaña en el organismo es considerado un recurso central para la protección de la información. Es por ello que deben ser concientizados y capacitados para desarrollar habilidades y conocimientos en seguridad de la información, y hacer un uso responsable de la misma y de los recursos utilizados en su gestión con el fin de prevenir eventos de seguridad y mitigar riesgos. En el caso del personal técnico, asimismo, deberá ser adecuadamente entrenado, a través de programas de capacitación específicos.

Por su parte se establecerá la adopción de los principios de seguridad de la información y el conocimiento de la PSI. en los procesos de contratación de personal. Asimismo, se establecerá la obligatoriedad de la suscripción de convenios de confidencialidad y aceptación de la Política de Seguridad, teniendo en cuenta que las responsabilidades correspondientes pueden exceder la vigencia de la relación laboral.

Los permisos de acceso a diversos entornos, aplicativos y ambientes de trabajo deberán ser otorgados de acuerdo a cada perfil del usuario y mantenerse actualizados a fin de resguardar el acceso a la información que estrictamente resulte necesaria para el ejercicio de sus funciones.

GESTIÓN DE ACTIVOS

La gestión y protección efectiva de los activos de información en función de su clasificación de acuerdo a su criticidad es importante para la adecuada gestión de la S.R.T.. Se establecerán lineamientos para poder clasificar cada activo de información, teniendo en cuenta la confidencialidad, integridad y disponibilidad de los datos, así como las funciones que soporta el activo y la normativa aplicable.

Se deberán llevar adelante inventarios actualizados sobre los activos de información, y exigir a todos los agentes y funcionarios que se desvinculan de la S.R.T. la devolución del equipamiento y/o dispositivos informáticos en su poder. En el mismo sentido, se deberá proceder a una destrucción segura de los equipamientos y dispositivos informáticos que puedan contener información crítica o datos personales, una vez catalogados como defectuosos o de rezago.

AUTENTICACIÓN, AUTORIZACIÓN Y CONTROL DE ACCESOS

La S.R.T. adoptará los mecanismos necesarios para que solo el personal autorizado acceda a los activos de información considerados críticos. El acceso a la información se establecerá en base a la “necesidad de saber”, es decir que quienes accedan deben tener un motivo válido para hacerlo en razón de su rol y/o funciones y usando una política de “Mínimo Privilegio”. Estos privilegios se otorgarán en forma expresa, serán autorizados por los niveles competentes y se gestionarán adecuadamente las altas y bajas de las cuentas y permisos de acceso, con revisiones periódicas.

Se requerirá al personal y terceros, sea cual fuese su modalidad de contratación, el uso responsable de los dispositivos y datos de autenticación otorgados por el organismo para el cumplimiento de sus funciones y/o servicios, y se comprometerá sobre la obligatoriedad de no compartirlos y mantenerlos siempre seguros, tanto dentro como fuera de las premisas de la S.R.T..

USO DE HERRAMIENTAS CRIPTOGRÁFICAS

Se utilizarán sistemas y técnicas criptográficas para la protección de la información del organismo, de acuerdo a su nivel de criticidad, con el fin de preservar su confidencialidad, integridad, autenticidad y no repudio, tanto para su almacenamiento como para su transmisión.

Asimismo, se protegerán las claves criptográficas durante todo su ciclo de vida y se utilizarán certificados digitales válidos en los sitios web institucionales.

SEGURIDAD FÍSICA Y AMBIENTAL

La S.R.T. protegerá sus instalaciones y sus activos físicos de procesamiento e intercambio de información, incluyendo sus puestos de trabajo, en función de la criticidad de la información que éstos gestionan, mediante el establecimiento de perímetros de seguridad, áreas protegidas y controles ambientales, en la medida en que se considere necesario.

Además, se monitorearán los accesos físicos para permitir sólo ingresos y egresos debidamente autorizados y se mantendrá un registro actualizado de los activos físicos que procesan información. Se implementarán y harán cumplir medidas de seguridad para los activos físicos que deban llevarse fuera del organismo, manteniéndose el registro correspondiente.

SEGURIDAD OPERATIVA

Dentro de la S.R.T. se llevarán a cabo las acciones necesarias para que las operaciones se desarrollen en forma segura, en todas las instalaciones de procesamiento de información, asignándose las debidas responsabilidades y desarrollando procedimientos acordes. Se adoptarán 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.

Se deberá realizar el debido resguardo de la información acorde con la criticidad de los datos y con los procesos de este organismo, llevando a cabo las pruebas de restauración.

SEGURIDAD DE LAS COMUNICACIONES

La S.R.T. adoptará las medidas necesarias para proteger adecuadamente la información que se comunica por sus redes informáticas y para minimizar los riesgos que pudieran afectar la infraestructura de soporte. Toda información que se transfiera fuera del organismo, incluyendo la que se transmite a través de los servicios de correo electrónico, será protegida de acuerdo a su nivel de criticidad.

Se asignarán cuentas de correo electrónico institucionales a todo el personal, quienes están obligados a utilizarlas para toda comunicación vinculada a sus funciones.

Se exigirá la firma de acuerdos de confidencialidad y no divulgación relacionados a la transferencia de información, en los casos en los que se considere necesario, y cuando el organismo entienda resulte conveniente para el tipo de información que se trate.

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

La S.R.T. adoptará las medidas de seguridad necesarias para proteger por defecto y desde el diseño todas las aplicaciones que se desarrollen internamente, utilizando una metodología de desarrollo seguro. Asimismo, incorporará requerimientos y lineamientos de seguridad en el proceso de contratación de aplicaciones o desarrollos de terceros.

En tal sentido, se promoverá la capacitación relacionada a una metodología de desarrollo seguro.

RELACIÓN CON PROVEEDORES

Se considerarán los aspectos vinculados con la identificación, análisis y gestión de riesgo desde el estudio de factibilidad de las decisiones de contratación de bienes y servicios, bienes y servicios tecnológicos, y/o que pudieran tener impacto en la seguridad de la información.

La S.R.T. incluirá en los pliegos de bases y condiciones particulares cláusulas vinculadas a la seguridad de la información, así como cláusulas para el mantenimiento del nivel de servicio, de cumplimiento efectivo y obligatorio por parte de los cocontratantes. Estas disposiciones considerarán los aspectos pertinentes a la protección de la información y los servicios que se brinden, desde el inicio del proceso contractual hasta su finalización, extendiéndose el deber de confidencialidad aun extinguido el vínculo que los una. Los requisitos a incluir serán acordes a la criticidad de la información y los servicios a brindar, al análisis de riesgos y el cumplimiento de todas las normas legales y contractuales aplicables.

GESTIÓN DE INCIDENTES DE SEGURIDAD

La S.R.T. adoptará las medidas necesarias para prevenir, detectar, gestionar, resolver y reportar los incidentes de seguridad que puedan afectar sus activos de información. Las debilidades detectadas en los procesos serán debidamente comunicadas, identificadas y minimizadas de forma tal que se apliquen las acciones correctivas en el menor tiempo posible.

Cuando el personal del organismo detecte un evento que podría constituir un incidente de seguridad, deberá comunicarlo al área competente a través de los canales de comunicación establecidos. Se deberá realizar un análisis de severidad de los incidentes para evaluar la estrategia de escalamiento para la gestión y comunicación del mismo.

ASPECTOS DE SEGURIDAD PARA LA CONTINUIDAD DE LA GESTIÓN

Se contemplarán todos los aspectos de seguridad requeridos en los procedimientos de continuidad de la gestión del organismo que se desarrollan, especialmente cuando se trate de información, servicios o sistemas críticos.

Se realizarán análisis de impacto y se identificarán las ventanas de recuperación requeridas en los procesos críticos. Asimismo, se documentarán los procesos, procedimientos y controles necesarios para llevar a cabo dicho plan.

CUMPLIMIENTO

La S.R.T. cumplirá las disposiciones legales, normativas y contractuales que le son aplicables y promoverá el acatamiento de las políticas y normas de seguridad que se aprueban en su ámbito.

En el mismo sentido, atenderá y dará cumplimiento a las recomendaciones correspondientes a los hallazgos de las auditorías internas y externas que se realicen, adoptando las medidas correctivas que correspondan.

9. NORMATIVA DE APLICACIÓN

A continuación, se detalla la normativa de aplicación de carácter general y particular. Asimismo, se deberán contemplar sus modificatorias, complementarias y reglamentarias y/o en las que en el futuro las sustituyan:

NORMAS DE APLICACIÓN

A. Ley N° 20.744 “Contrato de Trabajo”
B. Ley Nº 24.156 “Administración Financiera y de los Sistemas de Control del Sector Público Nacional”
C. Ley N° 24.557 “Riesgos del Trabajo”
D. Ley Nº 24.766 “Confidencialidad sobre Información y Productos que estén legítimamente bajo control de una persona y se divulgue indebidamente de manera contraria a los Usos Comerciales Honestos”.
E. Ley N° 25.188 “Ética en el ejercicio de la Función Pública”
F. Ley Nº 25.326 “Protección de los Datos Personales”
G. Ley Nº 25.506 “Firma Digital”
H. Ley Nº 26.388 “Modificación del Código Penal – Incorporación de Delitos Informáticos”
I. Decreto Nº 41/99 “Código de Ética de la Función Pública”
J. Decreto N° 214/06 “Convenio Colectivo de Trabajo General para la Administración Pública Nacional”
K. Decisión Administrativa Jefatura de Gabinete de Ministros N° 641/2021 “Requisitos Mínimos de Seguridad de la Información para los Organismos del Sector Público Nacional”
L. Disposición N° 1/2022 Dirección Nacional de Ciberseguridad “Modelo Referencial de Política de Seguridad de la Información”
M. Resolución S.R.T. N° 4/2019 “Estructura Organizativa de la S.R.T.”
N. Resolución S.R.T. N° 77/2020 “Creación del Comité de Seguridad de la Información”

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

Hoja Adicional de Firmas
Anexo firma conjunta

Número: IF-2023-66574133-APN-GT#SRT

CIUDAD DE BUENOS AIRES
Viernes 9 de Junio de 2023

Referencia: ANEXO I Lineamientos Generales de la Política de Seguridad de la Información-EX-2023-56789749-APN-GT#SRT

El documento fue importado por el sistema GEDO con un total de 11 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2023.06.09 09:33:01 -03:00

Diego Maximiliano Segovia
Subgerente
Subgerencia de Sistemas
Superintendencia de Riesgos del Trabajo

Digitally signed by Gestion Documental Electronica
Date: 2023.06.09 12:42:46 -03:00

Marcelo Angel Cainzos
Gerente
Gerencia Técnica
Superintendencia de Riesgos del Trabajo

Digitally signed by Gestion Documental Electronica
Date: 2023.06.09 12:42:47 -03:00