ANEXO

POLÍTICA
DE SEGURIDAD DE LA INFORMACIÓN MODELO

SENASA

I. INTRODUCCIÓN

La información es un recurso que, como otros activos importantes, es esencial y en consecuencia necesita ser protegido adecuadamente.

Todo Organismo se encuentra expuesto a riesgos en materia de seguridad de la información. No existe la seguridad completa, por lo que es necesario conocer cuál es el mapa de riesgos al cual se enfrenta el Organismo y tomar acciones tendientes a minimizar los posibles efectos negativos de la materialización de dichos riesgos.

La información puede existir en muchas formas. Puede estar impresa o escrita en un papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, mostrada en películas o hablada en una conversación. Cualquiera que sea la forma que tome la información o medio por el cual sea almacenada o compartida, siempre debiera estar apropiadamente protegida.

La seguridad de la información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo de las actividades y la operación normal del Organismo.

La seguridad de la información se logra implementando un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware.

Se necesitan establecer, implementar, monitorizar, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad específicos. Esto se debiera realizar en conjunción con otros procesos de gestión del Organismo.

El presente modelo podrá sufrir modificaciones futuras, de acuerdo a las novedades que se registren en la materia que trata, las cuales serán debidamente aprobadas y comunicadas.

La información y los procesos, sistemas y redes de apoyo son activos importantes. Definir, lograr, mantener y mejorar la seguridad de la información puede ser esencial para mantener una eficacia en la operación de las actividades del Organismo, observancia legal e imagen.

Las organizaciones, sus sistemas y redes de información enfrentan amenazas de seguridad de un amplio rango de fuentes; incluyendo fraude por computadora, espionaje, sabotaje, vandalismo, fuego o inundación. Las causas de daño como código malicioso, pirateo

computarizado o denegación de servicio se hacen cada vez más comunes, más ambiciosas y cada vez más sofisticadas.

La seguridad de la información es importante tanto para negocios del sector público como privado, y para proteger las infraestructuras críticas. En ambos sectores, la seguridad de la información funcionará como un facilitador; por ejemplo, para lograr e-gobierno o e-negocio, para evitar o reducir los riesgos relevantes.

La interconexión de redes públicas y privadas y el intercambio de fuentes de información incrementan la dificultad de lograr un control del acceso. La tendencia a la computación distribuida también ha debilitado la efectividad de un control central y especializado.

Muchos sistemas de información no han sido diseñados para ser seguros. La seguridad que se puede lograr a través de medios técnicos es limitada y debiera ser apoyada por la gestión y los procedimientos adecuados. Identificar qué controles establecer requiere de un planeamiento cuidadoso y prestar atención a los detalles.

La gestión de la seguridad de la información pretende, como mínimo, la participación de los diferentes grupos de interés, proveedores, terceros, clientes u otros grupos externos. También se puede requerir asesoría especializada de organizaciones externas.

Para lograr el éxito de la Política, han de establecerse factores críticos de éxito.

La experiencia ha demostrado que los siguientes factores con frecuencia son críticos para una exitosa implementación de la seguridad de la información dentro de una organización:

a) Política, objetivos y actividades de seguridad de información que reflejan los objetivos del Organismo.

b) Un enfoque y marco referencial para implementar, mantener, monitorizar y mejorar la seguridad de la información que sea consistente con la cultura organizacional.

c) Soporte visible y compromiso de todos los niveles de gestión.

d) Un buen entendimiento de los requerimientos de seguridad de la información, evaluación y gestión del riesgo.

e) Comunicación efectiva de la seguridad de la información con todos los directores, empleados y otras partes para lograr conciencia sobre el tema.

f) Distribución de lineamientos sobre la política y los estándares de seguridad de la información para todos los directores, empleados y otras partes involucradas.

g) Provisión para el financiamiento de las actividades de gestión de la seguridad de la información.

h) Provisión del conocimiento, capacitación y educación apropiados.

i) Establecimiento de un proceso de gestión de incidentes de seguridad de la información.

j) Implementación de un sistema de medición: que se utiliza para evaluar el desempeño en la gestión de la seguridad de la información y retroalimentación de sugerencias para el mejoramiento.

II. OBJETIVO

El objetivo de la presente Política de Seguridad de la Información o Política Modelo es el de crear un conjunto de reglas básicas que cumplan el personal del Organismo en el uso de la información para el desarrollo de sus tareas.

Mantener la Política de Seguridad del Organismo actualizada a efectos de asegurar su vigencia y nivel de eficacia.

III. RESPONSABLES DEL CUMPLIMIENTO

Todos los Directores Nacionales o Generales, Gerentes o equivalentes, titulares de Unidades Organizativas, tanto se trate de autoridades políticas o personal técnico y sea cual fuere su nivel jerárquico, son responsables de la implementación de esta Política de Seguridad de la Información dentro de sus áreas de responsabilidad, así como del cumplimiento de dicha Política por parte de su equipo de trabajo.

Las máximas autoridades del Organismo aprueban esta Política y son responsables de la autorización de sus modificaciones.

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

Todo el personal del Organismo y los terceros que interactúan de manera habitual u ocasional, que accedan a información sensible y/o a los recursos informáticos en el desarrollo de sus tareas habituales.

IV. INCUMPLIMIENTOS

Las medidas disciplinarias forman parte del conjunto de medidas disciplinarias del Organismo.

V. ESTÁNDARES Y MARCO LEGAL

Alineación con Normas Nacionales e Internacionales.

Todas las definiciones de la presente Política de Seguridad de la Información están alineadas con los estándares nacionales e internacionales vigentes para la práctica de seguridad de la información.

La presente Política Modelo reemplaza a los mismos fines a la aprobada por Disposición ONTI Nº 6/2005 y se dicta en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico del Organismo.

Debe ser conocida y cumplida por todo personal del Organismo, tanto se trate de funcionarios políticos como técnicos, y sea cual fuere su nivel jerárquico y su situación de revista.

VI. TÉRMINOS Y DEFINICIONES

A los efectos de la presente Política, se aplican las siguientes definiciones:

Comité de Seguridad: es un cuerpo integrado por representantes de todas las áreas sustantivas del Organismo, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

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

Información: se refiere a toda comunicación o representación de conocimiento inherente a las misiones y funciones del SERVICIO NACIONAL DE SANIDAD Y CALIDAD AGROALIMENTARIA, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Sistema de Información: se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

Tecnología de Información: se refiere al hardware y software operados por el Organismo o por un tercero que preste servicios al Organismo, sin tener en cuenta la tecnología utilizada, ya sea de computación de datos, telecomunicaciones u otro tipo.

Propietario de la Información: se vincula con la generación y/o administración; o disposición, de la información, entendiéndose por "propietario" a cualquier área del Organismo que posea la responsabilidad respecto de su manejo y preservación, conforme a sus funciones y competencias.

Compromiso de Confidencialidad: instrumento por el cual la persona física o jurídica declara conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitorización. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad de las personas físicas o jurídicas.

PUA o Política de Uso Aceptable de correo electrónico, Internet, Intranet y red de datos: define los derechos y las prohibiciones a que se deben atener los usuarios del Organismo, ya sea personal interno o externo. Esta política es una Resolución del SENASA y forma parte de la Cláusula: Gestión de Comunicaciones y Operaciones.

La PUA podrá ser modificada a distintos intervalos de tiempo y solo se anexará en este punto, ya que es más factible que se actualice gran parte de la PUA y en menor medida la presente Política Modelo.

Seguridad de la información: se entiende como la preservación de las siguientes características:

- Confidencialidad: la información será accesible solo a aquellas personas autorizadas a tener acceso a la misma.
- Integridad: consiste en salvaguardar la exactitud y totalidad de la información y los métodos de procesamiento.
- Disponibilidad: acceder a la información y a los recursos relacionados con la misma.

Adicionalmente, deben considerarse los conceptos de:

Autenticidad: busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando al emisor para evitar suplantación de identidades.

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

Protección a la duplicación: consiste en asegurar que una transacción solo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

No repudio: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.

Confiabilidad de la Información: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Riesgo: es la combinación de la probabilidad de ocurrencia de un evento y sus consecuencias o impacto.

Amenaza: una causa potencial de un incidente no deseado, el cual puede ocasionar daños a un sistema u organización.

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

Control: medio para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras organizacionales, las cuales pueden ser de naturaleza administrativa, técnica, de gestión o legal. Control es también utilizado como sinónimo de salvaguarda o de contramedida.

Evaluación de Riesgos: evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria del Organismo.

Tratamiento de Riesgos: es el proceso de selección e implementación de medidas para modificar el riesgo.

Gestión de Riesgos: son las actividades coordinadas para dirigir y controlar una organización en lo que concierne al riesgo.

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

VII. POLÍTICAS DEL ORGANISMO

ASPECTOS GENERALES

La Política Modelo está formada por ONCE (11) cláusulas o capítulos que abarcan las diferentes cláusulas, aspectos o dominios de la seguridad de la información. Se presentan de manera sistemática y consistente.

Ellas son:

• Política de seguridad
• Organización
• Gestión de Activos
• Recursos Humanos
• Física y Ambiental
• Gestión de Comunicaciones y Operaciones
• Gestión de Accesos
• Adquisición, Desarrollo y Mantenimiento de Sistemas
• Gestión de Incidentes de Seguridad
• Gestión de Continuidad
• Cumplimento

DESARROLLO DE LAS CLÁUSULAS O CAPÍTULOS:

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Generalidades

La información es un recurso que, como el resto de los activos, tiene valor para el Organismo y por consiguiente debe ser debidamente protegida.

Las Políticas de Seguridad de la Información protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información y de la operación

del Organismo, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos del Organismo.

Es importante que los principios de la Política de Seguridad sean parte de la cultura organizacional.

Para esto, se debe asegurar un compromiso manifiesto de las máximas Autoridades del Organismo y de los titulares de las Unidades Organizativas para la difusión, consolidación y cumplimiento de la presente Política.

Objetivo

Proteger los recursos de información del Organismo y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Asegurar la implementación de las medidas de seguridad comprendidas en esta Política, identificando los recursos y las partidas presupuestarias correspondientes, sin que ello implique necesariamente la asignación de partidas adicionales.

Mantener la Política de Seguridad del Organismo actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

Alcance

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

ORGANIZACIÓN DE LA SEGURIDAD

Generalidades

La presente Política de Seguridad establece la administración de la seguridad de la información, como parte fundamental de los objetivos y actividades del Organismo.

Por ello, se definirá formalmente un ámbito de gestión para efectuar tareas tales como la aprobación de la Política, la coordinación de su implementación y la asignación de funciones y responsabilidades.

Asimismo, se contemplará la necesidad de disponer de fuentes con conocimiento y experimentadas para el asesoramiento, cooperación y colaboración en materia de seguridad de la información.

Por otro lado, debe tenerse en cuenta que ciertas actividades del Organismo pueden requerir que terceros accedan a información interna, o bien puede ser necesaria la tercerización de ciertas funciones relacionadas con el procesamiento de la información. En estos casos, se considerará que la información puede ponerse en riesgo si el acceso de dichos terceros se produce en el marco de una inadecuada administración de la seguridad, por lo que se establecerán las medidas apropiadas para la protección de la información.

Objetivo

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

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

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

Alcance

Esta Política se aplica a todos los recursos del Organismo y a todas sus relaciones con terceros que impliquen el acceso a sus datos, recursos y/o a la administración y control de sus sistemas de información.

GESTIÓN DE ACTIVOS

Generalidades

El Organismo debe tener un conocimiento preciso sobre los activos que posee como parte importante de la administración de riesgos. Algunos ejemplos de activos son:

• Recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad y contingencia, información archivada, etc.

• Recursos de software: software de aplicaciones, sistemas operativos, herramientas de desarrollo y publicación de contenidos, utilitarios, etc.

• Activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, PABX, máquinas de fax, contestadores automáticos, switches de datos, etc.), medios magnéticos (cintas, discos, dispositivos móviles de almacenamiento de datos - pendrives, discos externos, etc.), otros equipos técnicos (relacionados con el suministro eléctrico, unidades de aire acondicionado, controles automatizados de acceso, etc.), mobiliario, lugares de emplazamiento, etc.

• Servicios: servicios informáticos y de comunicaciones, utilitarios generales (calefacción, iluminación, energía eléctrica, etc.).

Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información.

Generalmente, la información deja de ser sensible o crítica después de un cierto período de tiempo, por ejemplo, cuando la información se ha hecho pública. Estos aspectos deben tenerse en cuenta, puesto que la clasificación por exceso puede traducirse en gastos adicionales innecesarios para el Organismo.

Las pautas de clasificación deben prever y contemplar el hecho de que la clasificación de un ítem de información determinado no necesariamente debe mantenerse invariable por siempre, y que esta puede cambiar de acuerdo con una política predeterminada. Se debe considerar la cantidad de categorías a definir para la clasificación, dado que los esquemas demasiado complejos pueden tornarse engorrosos y antieconómicos o resultar poco prácticos.

La información adopta muchas formas, tanto en los sistemas informáticos como fuera de ellos. Puede ser almacenada (en dichos sistemas o en medios portátiles), transmitida (a través de redes o entre sistemas) e impresa o escrita en papel. Cada una de estas formas debe

contemplar todas las medidas necesarias para asegurar la confidencialidad, integridad y disponibilidad de la información.

Por último, la información puede pasar a ser obsoleta y, por lo tanto, ser necesario eliminarla. La destrucción de la información es un proceso que debe asegurar la confidencialidad de la misma hasta el momento de su eliminación.

Objetivo

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

Clasificar la información para señalar su sensibilidad y criticidad.

Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación (garantizar que los activos de información reciban un apropiado nivel de protección).

Alcance

Esta Política se aplica a toda la información administrada en el Organismo, cualquiera sea el soporte en que se encuentre.

RECURSOS HUMANOS

Generalidades

La seguridad de la información se basa en la capacidad para preservar su integridad, confidencialidad y disponibilidad, por parte de los elementos involucrados en su tratamiento: equipamiento, software, procedimientos, así como de los recursos humanos que utilizan dichos componentes.

En este sentido, es fundamental educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación de revista, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad. De la misma forma, es necesario definir las sanciones que se aplicarán en caso de incumplimiento.

La implementación de la Política de Seguridad de la Información tiene como meta minimizar la probabilidad de ocurrencia de incidentes. Es por ello que resulta necesario implementar un mecanismo que permita reportar las debilidades y los incidentes tan pronto como sea posible,

a fin de subsanarlos y evitar eventuales replicaciones. Por lo tanto, es importante analizar las causas del incidente producido y aprender del mismo, a fin de corregir las prácticas existentes, que no pudieron prevenirlo y evitarlo en el futuro.

Objetivo

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

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

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

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

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

Alcance

Esta Política se aplica a todo el personal del Organismo, cualquiera sea su situación de revista, y al personal externo que efectúe tareas dentro del ámbito del Organismo.

SEGURIDAD FÍSICA Y AMBIENTAL

Generalidades

La seguridad física y ambiental brinda el marco para minimizar los riesgos de daños e interferencias a la información y a las operaciones del Organismo. Asimismo, pretende evitar al máximo el riesgo de accesos físicos no autorizados, mediante el establecimiento de perímetros de seguridad.

Se distinguen TRES (3) conceptos a tener en cuenta: la protección física de accesos, la protección ambiental y el transporte, protección y mantenimiento de equipamiento y documentación.

El establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles tendientes a proteger las instalaciones de procesamiento de información crítica o sensible del Organismo, de accesos físicos no autorizados.

El control de los factores ambientales permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio. Deben contemplarse tanto los riesgos en las instalaciones del Organismo como en instalaciones próximas a la sede del mismo que puedan interferir con las actividades.

El equipamiento donde se almacena información es susceptible de mantenimiento periódico, lo cual implica en ocasiones su traslado y permanencia fuera de las áreas protegidas del Organismo. Dichos procesos deben ser ejecutados bajo estrictas normas de seguridad y de preservación de la información almacenada en los mismos. Así también se tendrá en cuenta la aplicación de dichas normas en equipamiento perteneciente al Organismo pero situado físicamente fuera de este ("housing") así como en equipamiento ajeno que albergue sistemas y/o preste servicios de procesamiento de información al Organismo ("hosting").

La información almacenada en los sistemas de procesamiento y la documentación contenida en diferentes medios de almacenamiento, son susceptibles de ser recuperadas mientras no están siendo utilizadas. Es por ello que el transporte y la disposición final presentan riesgos que deben ser evaluados.

Gran cantidad de información manejada en las oficinas se encuentra almacenada en papel, por lo que es necesario establecer pautas de seguridad para la conservación de dicha documentación; y para su destrucción cuando así lo amerite.

Objetivo

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

Proteger el equipamiento de procesamiento de información crítica del Organismo ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de

seguridad y controles de acceso apropiados. Asimismo, contemplar la protección del mismo en su traslado y permanencia fuera de las áreas protegidas, por motivos de mantenimiento u otros.

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

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

Proporcionar protección proporcional a los riesgos identificados.

Alcance

Esta Política se aplica a todos los recursos físicos relativos a los sistemas de información del Organismo: instalaciones, equipamiento, cableado, expedientes, medios de almacenamiento, etc.

GESTIÓN DE COMUNICACIONES Y OPERACIONES

Generalidades

La proliferación de software malicioso, como virus, troyanos, etc., hace necesario que se adopten medidas de prevención, a efectos de evitar la ocurrencia de tales amenazas.

Es conveniente separar los ambientes de desarrollo, prueba y operaciones de los sistemas del Organismo, estableciendo procedimientos que aseguren la calidad de los procesos que se implementen en el ámbito operativo, a fin de minimizar los riesgos de incidentes producidos por la manipulación de información operativa.

Los sistemas de información están comunicados entre sí, tanto dentro del Organismo como con terceros fuera de él. Por lo tanto, es necesario establecer criterios de seguridad en las comunicaciones que se establezcan.

Dichas comunicaciones permiten el intercambio de información, que debe estar regulado para garantizar las condiciones de confidencialidad, integridad y disponibilidad de la información que se emite o recibe por los distintos canales.

Objetivo

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

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

Alcance

Todas las instalaciones de procesamiento y transmisión de información del Organismo.

GESTIÓN DE ACCESOS

Generalidades

El acceso por medio de un sistema de restricciones y excepciones a la información es la base de todo sistema de seguridad informática. Para impedir el acceso no autorizado a los sistemas de información, se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso.

La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto, es necesario concientizarlos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular, aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

Objetivo

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

Controlar la seguridad en la conexión entre la red del Organismo y otras redes públicas o privadas. Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.

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

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

Alcance

La Política definida en este documento se aplica a todas las formas de acceso de aquellos a quienes se les haya otorgado permisos sobre los sistemas de información, bases de datos o servicios de información del Organismo, cualquiera sea la función que desempeñe.

Asimismo, se aplica al personal técnico que define, instala, administra y mantiene los permisos de acceso y las conexiones de red y a los que administran su seguridad.

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Generalidades

El desarrollo y mantenimiento de las aplicaciones es un punto crítico de la seguridad.

Durante el análisis y diseño de los procesos que soportan estas aplicaciones se deben identificar, documentar y aprobar los requerimientos de seguridad a incorporar durante las etapas de desarrollo e implementación. Adicionalmente, se deben diseñar controles de validación de datos de entrada, procesamiento interno y salida de datos.

Dado que los analistas y programadores tienen el conocimiento total de la lógica de los procesos en los sistemas, se deben implementar controles que eviten maniobras dolosas por parte de estas personas u otras que puedan operar sobre los sistemas, bases de datos y plataformas de software de base (por ejemplo, operadores que puedan manipular los datos y/o atacantes que puedan comprometer/alterar la integridad de las bases de datos) y en el caso de que se lleven a cabo, identificar rápidamente al responsable.

Asimismo, es necesaria una adecuada administración de la infraestructura de base, sistemas operativos y software de base, en las distintas plataformas, para asegurar una correcta

implementación de la seguridad, ya que en general los aplicativos se asientan sobre este tipo de software.

Objetivo

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

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

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

Alcance

Esta Política se aplica a todos los sistemas informáticos, tanto desarrollos propios o de terceros, y a todos los sistemas operativos y/o software de base que integren cualquiera de los ambientes administrados por el Organismo en donde residan los desarrollos mencionados.

GESTIÓN DE INCIDENTES DE SEGURIDAD

Generalidades

Existen numerosas amenazas que atentan contra la seguridad de la información, representando riesgos latentes que de materializarse pueden ocasionar incidentes de seguridad.

Los Organismos cuentan con innumerables activos de información, cada uno de los cuales puede encontrarse expuesto a sufrir incidentes de seguridad. Es por ello que resulta sumamente necesario contar con una capacidad de gestión de dichos incidentes que permita comenzar por su detección, llevar a cabo su tratamiento y colaborar en la prevención de futuros incidentes similares.

Objetivo

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

Alcance

La Política definida en este documento se aplica a todo incidente que pueda afectar la seguridad de la información del Organismo.

GESTIÓN DE LA CONTINUIDAD

Generalidades

La administración de la continuidad de las actividades es un proceso crítico que debe involucrar a todos los niveles del Organismo.

El desarrollo e implementación de planes de contingencia es una herramienta básica para garantizar que las actividades del Organismo puedan restablecerse dentro de los plazos requeridos.

Dichos planes deben mantenerse actualizados y transformarse en una parte integral del resto de los procesos de administración y gestión, debiendo incluir necesariamente controles destinados a identificar y reducir riesgos, atenuar las consecuencias de eventuales interrupciones de las actividades del Organismo y asegurar la reanudación oportuna de las operaciones indispensables.

Objetivo

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

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

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

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

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

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

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

Alcance

Esta Política se aplica a todos los procesos críticos identificados del Organismo.

CUMPLIMIENTO

Generalidades

El diseño, operación, uso y administración de los sistemas de información están regulados por disposiciones legales y contractuales.

Los requisitos normativos y contractuales pertinentes a cada sistema de información deben estar debidamente definidos y documentados.

La Dirección de Asuntos Jurídicos de este Servicio Nacional será responsable de encuadrar jurídicamente la formulación e implementación de la política.

Objetivos

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

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

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

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

Garantizar la existencia de controles que protejan los sistemas en producción y las herramientas de auditoría en el transcurso de las auditorías de sistemas.
Determinar los plazos para el mantenimiento de información y para la recolección de evidencia del Organismo.

Alcance
Esta Política se aplica a todo el personal del Organismo, cualquiera sea su situación de revista.
Asimismo, se aplica a los sistemas de información, normas, procedimientos, documentación y plataformas técnicas del Organismo y a las auditorías efectuadas sobre estos.

República Argentina - Poder Ejecutivo Nacional
2018 - Año del Centenario de la Reforma Universitaria

Hoja Adicional de Firmas
Anexo

Número: IF-2018-34059353-APN-DTINF#SENASA

CIUDAD DE BUENOS AIRES
Martes 17 de Julio de 2018

Referencia: E 8422/2017 ANEXO POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El documento fue importado por el sistema GEDO con un total de 21 pagina/s.

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
DN: cn=GESTION DOCUMENTAL ELECTRONICA - GDE, c=AR, o=MINISTERIO DE MODERNIZACION, ou=SECRETARIA DE MODERNIZACION ADMINISTRATIVA, serialNumber=CUIT 30715117564
Date: 2018.07.17 16:19:50 -03'00'

E/E María Claudia López
Líder de Proyecto
Dirección de Tecnología de la Información
Servicio Nacional de Sanidad y Calidad Agroalimentaria

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
DN: cn=GESTION DOCUMENTAL ELECTRONICA - GDE, c=AR, o=MINISTERIO DE MODERNIZACION, ou=SECRETARIA DE MODERNIZACION ADMINISTRATIVA, serialNumber=CUIT 30715117564
Date: 2018.07.17 16:19:51 -03'00'