Anexo.: Política de Seguridad de Información

INTRODUCCIÓN

Objetivo

Establecer la política que contemple las directivas y normas, para la protección de los activos de información, basada en la confidencialidad, integridad y disponibilidad que SENASA requiere.

Alcance

Esta Política abarca a todos los colaboradores, proveedores y clientes de SENASA con acceso a los activos de información.

Responsabilidades

Todo el personal de SENASA y terceros, que interactúan de una manera habitual u ocasional con los activos de información, son responsables de informarse del contenido de la Política de Seguridad de Información y cumplirlo en el desarrollo de sus tareas habituales.

El incumplimiento de la Política de Seguridad de Información de SENASA, tendrá como resultado la aplicación de la respectiva sanción, conforme a la magnitud y característica del aspecto incumplido.

Política de Seguridad de Información

El Servicio Nacional de Sanidad Agraria, tiene la necesidad de proteger los servicios y activos de la información en sus diferentes sedes del país, lo que implica que toda información obtenida, utilizada, procesada, almacenada y distribuida debe ser rigurosamente asegurada. Apoyándose en los principios fundamentales para preservar la información, como son la confidencialidad, integridad y disponibilidad de la información.

Objetivos Generales de la Política de Seguridad de la Información.

- Establecer los lineamientos para la gestión de la seguridad de la información, los cuales serán emitidos por el comité de seguridad de la información, el oficial de seguridad de la información y la coordinación técnica de la seguridad de la información del SENASA, en el marco de sus responsabilidades.
- Implementar el plan del sistema de gestión de la seguridad de la información (SGSI).
- Mantener el monitoreo continuo en prevención, ante amenazas al sistema de gestión de seguridad de la información.
- Determinar las oportunidades de mejora continua para el sistema de gestión de la seguridad de la información.

Protección de los Activos de la Información

Todos los colaboradores del SENASA tienen el compromiso de cumplir el alcance y la política determinada por la institución, con el objeto de salvaguardar la seguridad de la información. Protegiéndola contra violaciones de autenticidad, accesos no autorizados, pérdida de integridad y libre disponibilidad.

Asimismo, ante las amenazas y vulnerabilidades encontradas, se debe valorizar, identificar, evaluar y tratar los riesgos, a fin de mitigar los mismos. En caso estos riesgos se materialicen, se pondrá en práctica el plan de continuidad del negocio, registrando y analizando cualquier violación de las políticas y controles en el sistema de gestión de la seguridad de la información (SGSI) para su posterior mejora continua.

Creemos que la clave de éxito en la seguridad de la información está en la prevención sostenida mediante una cultura de preservación de la información, debiendo concientizar y comunicar adecuadamente a los colaboradores a nivel nacional.

1. POLÍTICAS DERIVADAS

1.1 Política de Activos TI (Tecnologías de Información)

1.1.1 PROPÓSITO

La sección de la Política de los activos de Tecnologías de la Información (TI), define los requisitos para el manejo adecuado y seguro de todos los Activos de Tecnologías de la Información en el SENASA.

1.1.2 ALCANCE

Aplica a todos los Activos TI asignados a los colaboradores, proveedores, prestadores de servicio y clientes de la Organización.

1.1.3 DEFINICIONES DE LA POLÍTICA

1. Todos los Activos TI a nivel nacional, deben ser registrados ~~patrimonialmente~~, clasificados, afectados o asignados para su uso aceptable en las actividades del proceso inmerso.
2. Cada usuario es responsable de la conservación y utilización de los Activos TIC que le han sido asignados
3. En el caso que SENASA brinde un activo a un tercero, el Jefe del área que recibe el servicio asume la responsabilidad del activo.
4. Todos los Activos TI deben mantenerse en lugares apropiados, con restricciones de acceso, condiciones ambientales y el diseño de acuerdo a la clasificación de seguridad y las especificaciones técnicas de los citados activos.
5. Los activos TI de escritorio y portables deben ser asegurados si se dejan desatendidos. Siempre que sea posible, esta política debe ser aplicada de forma automática.
6. El acceso a los Activos TI está prohibido para personas no autorizadas. Los préstamos y movilizaciones de un activo, debe hacerse a través de la gestión de solicitudes de servicio y procesos de gestión de accesos. Los espacios en donde se ubican los Activos TI, deben estar ordenados, limpios y libre de objetos que atente contra su funcionamiento. Los colaboradores deben apoyar a la cultura de buen uso y cuidado de los activos.
7. El Equipo de Soporte TI es el único responsable de mantener y actualizar las configuraciones. Ningún otro usuario está autorizado a cambiar o actualizar la configuración de los Activos de TIC. Eso incluye la modificación de hardware o software de instalación. Las configuraciones de red, dispositivos móviles, dispositivos de almacenamiento móviles, tarjetas de memoria, memoria flash, chips, entre otras deben ser registradas y autorizadas por las áreas de la UIE.
8. Los dispositivos de almacenamiento móviles (pendrive) se usan en forma restringida y temporalmente, deben ser declarados a través de documento, indicando el plazo y las razones de uso.
9. Está terminantemente prohibido la extracción de un Activo TI de las instalaciones de SENASA que no esté clasificado como un activo portable por el usuario. Es necesario, acreditar el registro de salida y retorno.
10. Todos los Activos TI que sean transportados al exterior de las instalaciones, deben permanecer en posesión del colaborador, evitando su exposición al público y con documento de patrimonio.
11. Cumplir los requisitos legales, estatutos, normas, reglamentos y contratos referidos a la seguridad de la información
12. Las pérdidas, robos, daños, manipulación u otro incidente relacionado con los Activos TI que compromete la seguridad, deben ser reportados a la brevedad posible al comité de gestión de la seguridad de la información a la UIE.
13. Se deben implementar controles en tecnologías de cifrado y borrado en Activos TI portables.

14. La eliminación y bajas de los Activos TIC debe hacerse de acuerdo con los procedimientos específicos para la protección de la información, actualizando el inventario de los activos. Si almacenan información confidencial deben ser destruidos físicamente en presencia de un miembro del comité de seguridad de la Información. En caso, almacenen información sensible deben ser borrados del medio de almacenamiento completamente y en presencia de un miembro del comité de gestión de la Seguridad de la Información antes de desecharlas. Para ello, son responsables los Directores Generales o Ejecutivos en publicar el registro del tipo de información (confidencial, reservado o secreto).
15. Los Activos de las TIC dañados que contienen información sensible deben pasar por una evaluación de riesgo para determinar si es que deben ser destruidos en lugar de ser reparados o descartados.
16. Todos los Activos TI deben pasar por el respectivo mantenimiento acorde a la programación anual de mantenimientos preventivos provista por la UIE.

1.2 Política de Control de Acceso

1.2.1 PROPÓSITO

Establecer los requisitos para el control adecuado de accesos a los Servicios de Tecnologías de la Información y la infraestructura del SENASA.

1.2.2 ALCANCE

Esta política se aplica a colaboradores, proveedores, prestadores de servicio y clientes de SENASA con acceso a los Servicios brindados por la UIE.

1.2.3 DEFINICIONES DE LA POLÍTICA

1. Cualquier sistema que maneja información valiosa y / o confidencial de la organización debe estar protegida con un sistema de control de acceso basado en contraseñas.
2. Las listas de control de accesos deben estar en el lugar para controlar el acceso a los recursos por los diferentes grupos de usuarios.
3. Los controles de acceso obligatorios deben estar en un lugar adecuado para regular el acceso de los procesos de operación en nombre de los usuarios
4. Acceso a los recursos debe concederse en función de cada grupo y no en función de cada usuario.
5. El acceso se concederá en virtud del principio de "privilegio", es decir, cada usuario debe recibir los derechos mínimos y el acceso a los recursos necesarios para que sean capaces de realizar sus funciones.
6. Siempre que sea posible, los accesos deben gestionarse de forma centralizada.
7. Los usuarios deben abstenerse de tratar de forzar o evadir los controles de acceso con el fin de obtener un mayor nivel de acceso.
8. Controles automáticos, tecnologías de análisis y procedimientos de revisión periódicas deben estar en el lugar adecuado para detectar cualquier intento para eludir los controles.
9. Todo personal externo (clientes, proveedores, visitas, etc.), que requiera conectar un equipo de trabajo a la red de la institución, deberá pasar por un control y análisis previo

del personal de Soporte Técnico, con el fin de detectar y eliminar posibles infecciones que representen un riesgo de seguridad.

1.3 Política de Control de Contraseñas

1.3.1 PROPÓSITO

La sección de la Política de Control de Contraseñas define los requisitos para el correcto y seguro manejo de contraseñas en la Organización.

1.3.2 ALCANCE

Esta política se aplica a colaboradores, proveedores, prestadores de servicio y clientes de SENASA con acceso a los Servicios brindados por la UIE.

1.3.3 DEFINICIONES DE LA POLÍTICA

1. Cualquier sistema que maneja información valiosa y / o confidencial debe estar protegido con un sistema de control de acceso basado en contraseñas.
2. Cada colaborador debe tener una identidad única y personal para el acceso a los servicios brindados por la UIE.
3. Las identidades deben ser creadas y gestionadas de forma centralizada. Se recomienda utilizar un único inicio de sesión para acceder a múltiples servicios.
4. Cada identidad debe tener una contraseña alfanumérica fuerte y privada para ser capaz de acceder a cualquier servicio. Deben ser lo menos ocho (8) caracteres de longitud.
5. Cada colaborador podrá utilizar la misma contraseña por un periodo no mayor a noventa (90) días. La misma contraseña no podrá ser utilizada de nuevo durante al menos un año.
6. La contraseña para algunas identidades especiales no expirará. En esos casos, la contraseña debe tener al menos quince (15) caracteres de longitud.
7. Compartir contraseñas está terminantemente prohibido. Las contraseñas no deben ser reveladas o expuestas a la vista del público.
8. Cada vez que una contraseña se considerare comprometida, por sospecha que alguien más la conozca, se debe cambiar inmediatamente.
9. Para las aplicaciones consideradas de alto nivel de importancia para el SENASA, se debe utilizar certificados digitales y la autenticación de factores múltiples que utilizan tarjetas inteligentes, siempre que sea posible.

1.4 Política de Correo Electrónico

1.4.1 PROPÓSITO

La sección de la Política de Correo Electrónico define los requisitos para el uso correcto y seguro del correo electrónico en la Organización.

1.4.2 ALCANCE

Esta política se aplica a colaboradores, proveedores, prestadores de servicio y clientes de SENASA con acceso a los Servicios brindados por la UIE.

1.4.3 DEFINICIONES DE LA POLÍTICA

1. Todas las direcciones de correo electrónico asignadas, almacenamiento de buzón de correo y enlaces de transferencia deben ser utilizados sólo para fines estrictamente laborales. El uso ocasional de la cuenta institucional de correo electrónico para fines personales puede ser permitido si, al hacerlo, no hay consumo perceptible en los recursos de la Organización y la productividad del trabajo no se ve afectada.
2. El uso de los recursos de la Institución para la publicidad no autorizada, correo no deseado, campañas políticas, y otros usos no relacionados con el negocio está estrictamente prohibidas.
3. De ninguna manera el correo electrónico se utilizará para revelar información confidencial o sensible de la Organización al margen de los receptores autorizados de la misma.
4. Uso del correo electrónico de la Organización para la difusión de mensajes que se consideran ofensivos, racistas, obscenos o de cualquier forma contraria a la ley y la ética están estrictamente prohibidos.
5. El uso del correo electrónico se mantiene sólo en la medida y por el tiempo que se necesita para realizar las tareas. Cuando un colaborador se desvincula de la empresa, la cuenta asociada debe desactivarse según los procedimientos establecidos para el ciclo de vida de las cuentas.
6. Los usuarios deben tener identidades privadas para acceder a sus mensajes de correo electrónico y recursos de almacenamiento, con excepción de los casos específicos en los que el uso común se puede considerar apropiado.
7. Las cuentas de acceso a correo electrónico corporativo deben ser protegidas por contraseñas seguras. La complejidad y el ciclo de vida de las contraseñas son administrados por los procedimientos de la empresa para la gestión de cuentas. No se recomienda compartir contraseñas. Los usuarios no deben suplantar a otros usuarios.
8. Los mensajes salientes de los usuarios corporativos deberían incluir la firma al pie del mensaje.
9. Los archivos adjuntos deben ser limitados en tamaño de acuerdo a los procedimientos indicados por la Organización. Siempre que sea posible, las restricciones deben ser aplicadas de forma automática.
10. Tecnologías de escaneo de virus y programas maliciosos deben estar en el ordenador del colaborador para garantizar la máxima protección en el correo electrónico entrante y saliente.
11. Los incidentes de seguridad deben ser reportados y tratados tan pronto como sea posible de acuerdo con la Gestión de Incidentes y los procesos de Seguridad de Información. Los usuarios no deben tratar de responder por sí mismos a los ataques de seguridad.
12. Contenido de los buzones debe almacenarse centralmente en lugares donde la información puede ser respaldada y manejada de acuerdo a los procedimientos de la empresa.

1.5 Política de Internet

1.5.1 PROPÓSITO

La sección Política de Internet define los requisitos para el acceso adecuado y seguro a Internet.

1.5.2 ALCANCE

Esta política se aplica a colaboradores, proveedores, prestadores de servicio y clientes de SENASA con acceso a los Servicios brindados por la UIE.

1.5.3 DEFINICIONES DE LA POLÍTICA

1. El acceso a Internet es limitado para todos los usuarios.
2. El uso del servicio de mensajería instantánea, de la marca establecida en la Institución, está permitido para fines del negocio en interés del SENASA.
3. El acceso a sitios pornográficos, sitios de hacking, y otros sitios de riesgo está estrictamente prohibido.
4. La descarga es un privilegio asignado a algunos usuarios, con la autorización previa del área correspondiente.
5. Acceso a Internet es principalmente para fines laborales. Un poco de navegación personal limitada se permite si al hacerlo no hay consumo perceptible de los recursos de los sistemas de TI y la productividad del trabajo no se ve afectada. La navegación personal no es recomendada durante las horas de trabajo.
6. El tráfico entrante y saliente es regulado, utilizando servidores de seguridad.
7. Los usuarios, al acceder a Internet deben comportarse de una manera compatible con el prestigio de la Organización. Los ataques como la denegación de servicio, el spam, la pesca (fishing), el fraude, la piratería, la distribución de material cuestionable, infracción de derechos de autor y otros están estrictamente prohibidos.
8. El tráfico de Internet se debe supervisar en los cortafuegos. Cualquier ataque o abuso debe ser reportado inmediatamente al responsable de Seguridad de la Información.
9. Los servidores, estaciones de trabajo y equipos deben contener mecanismos para la detección y prevención de ataques y abusos. Estos incluyen firewalls, detección de intrusos y otros.

1.6 Política de Antivirus

1.6.1 PROPÓSITO

La sección de Política Antivirus define los requisitos para la correcta ejecución del antivirus y otras formas de protección en la organización.

1.6.2 ALCANCE

Esta política se aplica a los servidores, estaciones de trabajo y equipos en la organización, incluyendo dispositivos portátiles que puedan viajar fuera de las instalaciones de la organización. Algunas directivas se aplican a equipos externos y dispositivos de acceso a los recursos de la organización.

1.6.3 DEFINICIONES DE LA POLÍTICA

1. Todos los equipos y dispositivos con acceso a la red de la organización deben tener instalado un cliente antivirus con protección en tiempo real.
2. Todos los servidores y estaciones de trabajo de propiedad de la Organización o permanentemente en uso en las instalaciones de la Organización deben tener un antivirus gestionado de forma centralizada. Eso también incluye dispositivos de viaje que se conecta regularmente a la red de la organización, o que se pueden gestionar a través de canales seguros a través de Internet.
3. Computadoras de la Organización que trabajan permanentemente en la red de otra organización pueden quedar exentos de la regla anterior si así lo requiere la política de seguridad de la otra organización, siempre y cuando dichos equipos estén protegidos.
4. Los equipos portátiles que rara vez se conectan a la red de la organización puede tener aprobado e instalado un antivirus de gestión independiente.
5. Todos los antivirus deben actualizar de forma automáticamente su definición de virus. Ello debe ser supervisado para asegurar que se la actualización se llevó a cabo con éxito.
6. Ordenadores visitantes y todos los equipos que se conectan a la red de la Organización están obligados a mantenerse "sanos", es decir, con un antivirus instalado y actualizado.

1.7 Política de Acceso Remoto

1.7.1 PROPÓSITO

La sección de la Política de Acceso Remoto define los requisitos para el acceso remoto seguro a recursos internos de la Organización.

1.7.2 ALCANCE

Esta política se aplica a los usuarios y dispositivos que necesitan acceder a recursos internos de la Organización desde ubicaciones remotas.

1.7.3 DEFINICIONES DE LA POLÍTICA

1. Para acceder a los recursos internos desde ubicaciones remotas, los usuarios deben tener la autorización necesaria del Administrador de la Seguridad de la Información.
2. Sólo los canales seguros con autenticación entre el servidor y cliente deben estar disponibles para el acceso remoto. Tanto el servidor y los clientes deben recibir certificados de confianza mutua.
3. El acceso remoto a la información confidencial no se debe permitir. La excepción a esta regla sólo podrá autorizarse en los casos estrictamente necesarios.
4. Los usuarios no deben conectarse desde ordenadores públicos, a menos que el acceso sea utiizado para ver contenido público.

1.8 Política de Subcontratación

1.8.1 PROPÓSITO

La sección de Política de Subcontratación define los requerimientos necesarios para minimizar los riesgos asociados con la externalización de un servicio, funciones y procesos.

1.8.2 ALCANCE

Esta política se aplica a la organización; los proveedores de servicios, funciones y procesos que están siendo subcontratados.

1.8.3 DEFINICIONES DE LA POLÍTICA

1. Antes del inicio de cualquier servicio externo, función o proceso, es necesario se evalúe los riesgos de seguridad y las consecuencias financieras.
2. La subcontratación de servicios se debe realizar conforme a la Ley de Contrataciones del Estado, la reglamentación concerniente y los procedimientos internos del SENASA.
3. Se debe realizar evaluaciones de desempeño del proveedor de servicios antes y durante la prestación del servicio externo. En caso que, el SENASA no cuente con un experto sobre el servicio efectuado, se deberá contratar a una persona natural o jurídica bajo la ley de Contrataciones del Estado.
4. El contrato de servicio y los niveles de servicio deben estar contemplados dentro de los Términos de Referencia origen de la sub-contratación.
5. El proveedor de servicios debe obtener la autorización del SENASA, si se propone contratar a un tercero para soportar el servicio subcontratado.

Glosario de Términos de la Política de Seguridad de la Información

Activo de la Información / Activos TI
Todo lo que la Institución considera importante o de lata validez para la misma, ya sea por contener información importante o ser un instrumento para el manejo de la información.

Activo desatendido
Refiere a un activo de TI que se está siendo utilizado en forma permanente.

Activo portable
Son los activos de TI que pueden ser trasladados en diferentes lugares, como por ejemplo: Computadora portátil, Tablet.

Administrador de la Seguridad de la Información
Responsable principal de la Seguridad de la Información dentro de la Unidad de Informática y Estadística.

Colaborador
Todo Colaborador que realiza labores en SENASA (Funcionario, Servidor)

Comité de Seguridad de la Información

Es el equipo integrado por representantes de diversas áreas de la Institución, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad para lograr un trabajo eficaz y seguro.

Control de acceso
Verificación de la identidad y derechos de una persona o computador que solicita acceso a un recurso.

Equipo de Soporte TI
Es el personal encargado de las funciones de realizar el soporte a los servicios tecnológicos en la Unidad de Informática y Estadística.

Gestión de Incidentes
Tratamiento que se da a los incidentes reportados a Informática.

Información confidencial
Información que tiene un nivel de importancia alta para la Institución y la cuál no puede ser de divulgación masiva.

Oficial de Seguridad de la Información
Responsable máximo en planificar, desarrollar y controlar las políticas, procedimientos y acciones con el fin de mejorar la Seguridad de la Información dentro de la Institución.

Plan de Continuidad del Negocio
Es un conjunto de medidas que debe realizar la Institución para recuperar y restaurar las funciones críticas parcialmente o totalmente interrumpidas.

Servicio de Tecnologías de la Información
Servicios tecnológicos que brinda la Unidad de Informática y Estadística

Sistema de Gestión de Seguridad de la Información (SGSI)
Es el diseño, implantación y mantenimiento de un conjunto de procesos y políticas con el fin de gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.