SENASA

Política de Seguridad de la Información

1.

1. ÍNDICE

1. ÍNDICE 2
2. OBJETO 3
3. ALCANCE 3
4. REFERENCIAS 4
5. DOCUMENTOS RELACIONADOS 4
6. RESPONSABILIDADES 4
7. MARCO ORGANIZATIVO, POLÍTICA DE SEGURIDAD 5
7.1. PRINCIPIOS BÁSICOS 5
7.1.1. Seguridad Integral 5
7.1.2. Gestión de Riesgos 5
7.1.3. Prevención 5
7.1.4. Detección 6
7.1.5. Respuesta 6
7.1.6. Recuperación 6
7.2. ESTRUCTURA ORGANIZATIVA Y DE SEGURIDAD 7
7.3. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 13
7.3.1. Declaración de la Política de Seguridad de la Información 13
7.3.2. Normativa de Seguridad 13
7.3.3. Procedimientos de Seguridad 14
7.3.4. Proceso de Autorización 14
7.4. MARCO LEGAL Y REGULATORIO 14
7.5. ESTRUCTURACIÓN DE SEGURIDAD DEL SISTEMA 15
7.6. OBLIGACIONES DE LOS USUARIOS 16
7.7. TERCERAS PARTES 16

2. OBJETO

SENASA depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad, autenticidad o trazabilidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en las dimensiones indicadas de la información tratada y los servicios prestados. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que las empresas deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad (en adelante, ENS) y los de la Norma ISO27001, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Todas las áreas y departamentos que integran SENASA deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas y en los pliegos de licitación para proyectos relacionados con las TIC.

Todas las áreas y departamentos que integran SENASA deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes de seguridad.

3. ALCANCE

La Política de Seguridad de la Información y las directrices que en ella se describen se aplican a todos los servicios prestados por la Sociedad que se apoyen en las Tecnologías de la Información y las Comunicaciones, así como a todo el personal que directa o indirectamente preste algún servicio para la organización, incluidas las personas que forman parte de los órganos de dirección y administración.

4. REFERENCIAS

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad y Norma **UNE-EN ISO/IEC 27001:2022** Sistema de Gestión de Seguridad de la Información.

- **UNE-EN ISO 27001:2022**
  - Punto 5. Liderazgo
- **ENS**
  - Artículo 12
  - Org.1. Política de seguridad

5. DOCUMENTOS RELACIONADOS

- PR86-01-Roles y Responsabilidades del SGSI
- PR85-01-Manual de Seguridad del Usuario
- PR71-01-Control de la documentación

6. RESPONSABILIDADES

FUNCIÓN	RESPONSABLE
Elaborar, mantener y garantizar la difusión de la Política de Seguridad de la Información	Responsable de Seguridad de la Información
Revisar anualmente la Política de Seguridad de la Información	Comité de Seguridad de la Información
Aprobar la Política de Seguridad de la Información	Consejo de Administración

7. POLÍTICA DE SEGURIDAD

7.1. PRINCIPIOS BÁSICOS

La Organización debe cumplir con sus objetivos teniendo en cuenta los siguientes principios básicos en materia de Seguridad de la Información.

7.1.1. Seguridad Integral

La Seguridad es entendida como un proceso integral compuesto de elementos técnicos, humanos, materiales y organizativos. Las medidas de seguridad que se despliegan al efecto de lograr aumentar la madurez en Seguridad de la Información tienen un carácter integral, para minimizar las fuentes de riesgo para la Información, prestando especial atención a la formación de las personas trabajadoras y sus responsables jerárquicos.

7.1.2. Gestión de Riesgos

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando cambie la información manejada.
- Cuando cambien los servicios prestados o la infraestructura que lo soporta
- Cuando ocurra un incidente grave de seguridad.

Para la armonización de los análisis de riesgos, el Comité de Seguridad de la Información (en adelante, CSI) establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. En este sentido, el CSI dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal

7.1.3. Prevención

Todas las áreas y departamentos que integran SENASA deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello, deben implementar las medidas mínimas de seguridad determinadas por el ENS y la ISO 27001, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todos los usuarios, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, todas las áreas y departamentos que integran la empresa deben:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

7.1.4.Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia.

La monitorización es especialmente relevante cuando se establecen líneas de defensa. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

7.1.5.Respuesta

Todas las áreas y departamentos que integran SENASA deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

7.1.6.Recuperación

Para garantizar la disponibilidad de los servicios críticos, todas las áreas y departamentos que integran SENASA deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

7.2. ESTRUCTURA ORGANIZATIVA Y DE SEGURIDAD

La organización del sistema de gestión de la seguridad de la información se desarrollará conforme a lo establecido en el Real Decreto 311/2022 y resto de normativa aplicable, así como en las guías técnicas publicadas por los organismos competentes, fundamentalmente el Centro Criptológico Nacional (CCN), adscrito al Centro Nacional de Inteligencia (CNI).

El documento **PR86-01-Roles y Responsabilidades del SGSI** establece la organización de seguridad de la SENASA. En dicho documento, se nombran todos los roles relativos al SGSI de la Organización

Será responsable de la coordinación de la seguridad de la información y único punto de contacto para todas las áreas y departamentos que integran SENASA en esta materia. Además del anterior, SENASA dispone de los siguientes roles, responsabilidades y autoridades relativas al SGSI:

- **Comité de seguridad de la información:** Es el órgano que coordina la Seguridad de la Información a nivel de organización. Estará constituido por la Alta Dirección, una representación designada por el Comité de Ética y Cumplimiento (CEC), el Responsable de Seguridad de la Información, el Responsable del Sistema, el Delegado de Protección de Datos (DPO) y el Responsable de los Servicios Jurídicos.

  A requerimiento del CSI se convocará cualesquiera otros Jefes de Departamento y responsables, cuya intervención sea precisa por ser afectados por el Esquema Nacional de Seguridad, ISO 27001 y por la legislación vigente en materia de protección de datos.

  Corresponde al CSI:

  - Convocar las reuniones del CSI.
  - Preparar los temas a tratar en las reuniones del CSI, aportando información puntual para la toma de decisiones.
  - Elaborar el acta de las reuniones.
  - La responsabilidad de la ejecución directa o delegada de las decisiones del CSI.

  Las funciones del CSI son las siguientes:

  - Atender las inquietudes de la Dirección de SENASA y de los diferentes departamentos.
  - Informar regularmente del estado de la seguridad de la información al Comité de Dirección de SENASA.
  - Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.
  - Elaborar la estrategia de evolución de SENASA en lo que respecta a la seguridad de la información.
  - Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.

- Elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada por la Dirección.
- Aprobar la normativa de seguridad de la información.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por SENASA y recomendar posibles actuaciones respecto de ellos.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de SENASA. En particular, velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
- Velar por que la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la Organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Recabará regularmente del personal técnico propio o externo, la información pertinente para tomar decisiones.
- Solicitar asesoramiento en los temas en que tenga que decidir o emitir una opinión. Este asesoramiento se determinará en cada caso, pudiendo materializarse de diferentes formas y maneras:
- Crear temporalmente grupos de trabajo especializados internos, externos o mixtos.
- Asistir a cursos u otro tipo de entornos formativos o de intercambio de experiencias.
- Reunirse de forma, al menos, semestral para dar seguimiento las tareas relativas al Sistema de Gestión de Seguridad de Información.

- **Comité de crisis:** El Comité de Crisis será convocado una vez se tenga la sospecha de que se superará el doble del tiempo establecido de recuperación en el establecido en el Plan de Continuidad de Negocio, establecido como objetivo en la recuperación ante un escenario de contingencia.

  El objetivo del Comité de Crisis será el establecimiento de decisiones estratégicas a tomar ante una situación de desastre.

- **Responsable de seguridad de la información:** Con el Departamento de Sistemas, el Responsable de Seguridad de la información velará por el cumplimiento de la Política de Seguridad de la Información, normas, procedimientos, registros, instrucciones técnicas, y demás documentos relacionados con la operación del Sistema de Gestión (nivel ejecutivo).

Se debe nombrar formalmente a una única persona, no pudiendo ser desarrollado por un órgano colegiado, aunque pueda delegar parte de sus funciones en otras personas.

Al Responsable de Seguridad de la Información le corresponden las siguientes funciones:

- Reportará directamente al Comité de Seguridad de la Información.
- Actuará como Secretario del Comité de Seguridad de la Información.
- Convocará al Comité de Seguridad de la Información, recopilando la información pertinente.
- Mantendrá la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo con lo establecido en la Política de Seguridad de la Información.
- Promoverá la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
- Recopilará los requisitos de seguridad de los Responsables de Información y del Servicio y determinará la categoría del Sistema.
- Realizará el Análisis de Riesgos de Tecnologías de la Información.
- Elaborará una Declaración de Aplicabilidad, a partir de las medidas de seguridad requeridas conforme al Anexo II del ENS y del resultado del Análisis de Riesgos.
- Facilitará al Responsable de la Información y al Responsable de Servicio información sobre el nivel de riesgo residual esperado tras implementar las opciones de tratamiento seleccionadas en el análisis de riesgos y las medidas de seguridad requeridas por el ENS.
- Coordinará la elaboración de la Documentación de Seguridad del Sistema.
- Participará en la elaboración, en el marco del Comité de Seguridad de la Información, de la Política de Seguridad de la Información.
- Aprobará los procedimientos técnicos y normativas internas relativos a la seguridad de la información, cuya aprobación no corresponda a un nivel superior.
- Facilitará periódicamente al Comité de Seguridad de la Información un resumen de actuaciones en materia de seguridad, de incidentes relativos a seguridad de la información y del estado de la seguridad del sistema (en particular del nivel de riesgo al que está expuesto el sistema).
- Elaborará, junto al Responsable del Sistema, Planes de Mejora de la Seguridad, para su aprobación por el Comité de Seguridad de la Información.
- Elaborará los Planes de Formación y Concienciación del personal en Seguridad de la Información, que deberán ser aprobados por el Comité de Seguridad de la Información.
- Validará los Planes de Continuidad y Planes de Contingencias, que deberán ser aprobados por el Comité de Seguridad de la Información y probados periódicamente por el Responsable del Sistema.
- Aprobará las directrices propuestas por el Responsable del Sistema para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos: especificación, arquitectura, desarrollo, operación y cambios.

- **Responsable de la información:** Corresponde al nivel de Alta Dirección, que entiende la misión de la organización, determina la estrategia y los objetivos que se propone alcanzar y responde de su cumplimiento. El Responsable de la Información puede ser una persona

concreta que ocupa un alto cargo en la dirección de la organización, o un órgano corporativo, que revestirá la forma de órgano colegiado (nivel gobierno). En SENASA, esta función corresponde al Comité de Seguridad de la Información. Al responsable de la Información le corresponden las siguientes funciones:

- Adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
- Tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.
- Responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
- Establece los requisitos de la información en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información.
- Determinará los niveles de seguridad en cada dimensión dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad.
- Aunque la aprobación formal de los niveles corresponda al Responsable de la Información, podrá recabar una propuesta del Responsable de la Seguridad y conviene que escuche la opinión del Responsable del Sistema.

- **Responsable de servicio:** Puede corresponder al nivel de Alta Dirección, que entiende la misión de la organización, determina la estrategia y los objetivos que se propone alcanzar y responde de su cumplimiento (nivel gobierno) o a una Dirección Ejecutiva, que entiende qué hace cada departamento y cómo estos se coordinan entre sí para alcanzar los objetivos marcados de la Organización (nivel ejecutivo). El Responsable del Servicio puede ser una persona concreta que ocupa un alto cargo en la dirección de la organización, o un órgano corporativo, que revestirá la forma de órgano colegiado. En SENASA, esta función corresponde al Comité de Seguridad de la Información. Las funciones del Responsable de Servicio son las siguientes:

  - Apoyo al DPO en materia de protección de datos en relación con servicios prestados. por los diferentes departamentos de SENASA.
  - Establece los requisitos de los servicios en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información para sus servicios dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad.
  - Tiene la responsabilidad última del uso que se haga de determinados servicios y, por tanto, de su protección.
  - Responsable último de cualquier error o negligencia que lleve a un incidente de disponibilidad de los servicios.
  - Aunque la aprobación formal de los niveles corresponda al Responsable del Servicio, podrá recabar una propuesta al Responsable de la Seguridad y conviene que escuche la opinión del Responsable del Sistema.

- La prestación de un servicio siempre debe atender a los requisitos de seguridad de la información que maneja, de forma que pueden heredarse los requisitos de seguridad de esta, añadiendo requisitos de disponibilidad, así como otros como accesibilidad, interoperabilidad, etc.

- **Responsable del sistema:** El Responsable del Sistema es la persona que se encarga de la explotación del sistema de información (nivel operaciones). Se debe nombrar formalmente a una única persona. El rol no podrá ser desarrollado por un órgano colegiado, aunque pueda delegar parte de sus funciones en otras personas.

  Al Responsable del Sistema le corresponden las siguientes funciones:

  - Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
  - Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
  - Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
  - El Responsable del Sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los Responsables de la Información afectada, del Servicio afectado y con el Responsable de la Seguridad antes de ser ejecutada.
  - Aplicar los procedimientos operativos y las normativas de seguridad.
  - Monitorizar el estado de la seguridad del Sistema de Información y reportarlo periódicamente o ante incidentes de seguridad relevantes al Responsable de Seguridad de la Información.
  - Elaborar los Planes de Continuidad y Planes de Contingencias para que sean validados por el Responsable de Seguridad de la Información, y coordinados y aprobados por el Comité de Seguridad de la Información.
  - Realizar ejercicios y pruebas periódicas de los Planes de Continuidad del Sistema para mantenerlos actualizados y verificar que son efectivos.
  - Elaborará las directrices para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos (especificación, arquitectura, desarrollo, operación y cambios) y las facilitará al Responsable de Seguridad de la Información para su aprobación.

- **Delegado de protección de datos:** El Delegado de Protección de Datos (DPO) es la persona responsable en el seno de una organización de realizar la supervisión y monitorización, de forma independiente y confidencial, del adecuado cumplimiento de la normativa en materia de protección de datos personales. El DPO desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

  Las funciones del Delegado de Protección de Datos están reguladas el artículo 39 RGPD, siendo las siguientes:

- Informar y asesorar a la entidad y al personal que se ocupe del tratamiento de datos personales de las obligaciones que les incumben en virtud del RGPD y de otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros.
- Supervisar el cumplimiento de lo dispuesto en el RGPD, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas de la entidad en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a protección de datos y supervisar su aplicación.
- Cooperar con la autoridad de control (la Agencia Española de Protección de Datos en España). Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a la autoridad de control cuando una evaluación muestre que el tratamiento entrañaría un alto riesgo.
- Realizar consultas, en su caso, sobre cualquier otro asunto y notificar las brechas de seguridad que se produzcan.

- **Propietarios del riesgo:** El propietario del riesgo es aquella persona o departamento de SENASA, conocedor en profundidad de los procesos del área que gobierna y responsable de la definición de los niveles de seguridad de cada dimensión (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad).

  En SENASA esta función corresponde al máximo responsable de cada área de gestión (alta dirección).

  Las funciones del propietario del riesgo incluyen:

  - Participar en la valoración de los activos de sus procesos, identificación de los riesgos asociados a la gestión del proceso, definir la necesidad de seguridad requerida para su área.
  - Es responsable de hacer cumplir las políticas de seguridad relacionadas con su área corporativa.
  - Es responsable de cualquier error o negligencia que lleve a un incidente de seguridad.
  - Define el acceso que se haga de los activos del personal bajo su supervisión.
  - Aprueba el plan de tratamiento de riesgos bajo su responsabilidad.
  - Aprueba el riesgo residual de su correspondiente área.
  - Debe conocer y hacer cumplir las medidas de seguridad implantadas tanto a nivel general como las específicas de su área.
  - Está representado en el Comité de Seguridad de la Información.
  - Debe revisar las medidas de seguridad implantadas en su área y sugerir mejoras cuando sean pertinentes.

- **Coordinador del PCN:** Las funciones del coordinador del Plan de Continuidad de Negocio (PCN) son las siguientes:

  - Analiza todos los aspectos relacionados con el potencial desastre y decide sobre la activación del PCN.

- Coordinará todas las actividades necesarias a llevará a cabo en el PCN, ya sea de mantenimiento, pruebas o mejoras durante un desastre.
- Verificará que todas las actividades se realizan en el orden previsto y por las personas adecuadas.

7.3. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

7.3.1. Declaración de la Política de Seguridad de la Información

SENASA ha establecido las directrices básicas para garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información en su Política de Seguridad de la información, la cual ha puesto a disposición de todas las partes interesadas en su página web corporativa.

Así mismo se desarrollará aplicando los siguientes requisitos mínimos:

- Organización e implantación del proceso de seguridad.
- Análisis y gestión de los riesgos.
- Gestión de personal.
- Profesionalidad.
- Autorización y control de los accesos.
- Protección de las instalaciones.
- Adquisición de productos de seguridad y contratación de servicios de seguridad.
- Mínimo privilegio.
- Integridad y actualización del sistema.
- Protección de la información almacenada y en tránsito.
- Prevención ante otros sistemas de información interconectados.
- Registro de la actividad y detección de código dañino.
- Incidentes de seguridad.
- Continuidad de la actividad.
- Mejora continua del proceso de seguridad.

7.3.2. Normativa de Seguridad

Esta Política se desarrollará por medio de normativas de seguridad que aborden aspectos específicos.

El **PR85-01-Manual de Seguridad del Usuario** estará a disposición de todas las personas que necesiten conocerlo, en particular para aquellas que utilicen, operen o administren los sistemas de información y comunicaciones. Dicho documento se encontrará disponible para todo el personal en la intranet corporativa y será facilitado al personal externo cuando sea necesario.

7.3.3. Procedimientos de Seguridad

SENASA dispone de documentación que detalla de forma clara y precisa cómo operar los elementos del sistema de información, que engloban los siguientes aspectos:

- Cómo llevar a cabo las tareas habituales.
- Quién debe hacer cada tarea.
- Cómo identificar y reportar comportamientos anómalos.
- La forma en que se ha de tratar la información en consideración al nivel de seguridad que requiere, precisando cómo efectuar:
    - Su control de acceso.
    - Su almacenamiento.
    - La realización de copias.
    - El etiquetado de soportes.
    - Su transmisión telemática.
    - Cualquier otra actividad relacionada con dicha información.

7.3.4. Proceso de Autorización

La Organización ha establecido un proceso formal por el cual se asignarán las autorizaciones y privilegios en función de las necesidades del puesto de trabajo y bajo la premisa de asignación de mínimos privilegios, que abarcarán los siguientes aspectos:

- Utilización de instalaciones, habituales y alternativas.
- Entrada de equipos en producción, en particular, equipos que involucren criptografía.
- Entrada de aplicaciones en producción.
- Establecimiento de enlaces de comunicaciones con otros sistemas.
- Utilización de medios de comunicación, habituales y alternativos.
- Utilización de soportes de información.
- Utilización de equipos móviles. Se entenderá por equipos móviles ordenadores portátiles, tabletas, teléfonos móviles u otros de naturaleza análoga.
- Utilización de servicios de terceros, bajo contrato o convenio, encargo, concesión, etc.

Dicho proceso queda reflejado en el procedimiento **PR86-01-Roles y Responsabilidades del SGSI**.

7.4. MARCO LEGAL Y REGULATORIO

SENASA trata datos de carácter personal. Los procesos de gestión de este tipo de datos, en el marco del Comité de Seguridad de la Información, recogen los tratamientos afectados y los responsables correspondientes.

Todos los sistemas de información de SENASA se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en los mencionados procesos de gestión de este tipo de datos.

Asimismo, el marco legal y regulatorio en el que se desarrollan las actividades queda identificado en el **RG818-01 Registro Legislación Aplicable**. De dicho registro se identifica y destaca la siguiente legislación:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.
- Ley Orgánica 3/2018 de 5 de diciembre de Protección de Datos de Carácter Personal y garantía de los derechos digitales.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

7.5. ESTRUCTURACIÓN DE SEGURIDAD DEL SISTEMA

De acuerdo con la clasificación de activos adoptada por la Organización, la documentación de procedimientos y registros del Sistema General de Gestión de la Información (SGSI) es gestionada de acuerdo con el nivel de seguridad determinado por el aprobador del documento, a saber:

- **Secreta**: Información de carácter restringido (primera categoría 1) que, por su contenido, tratamiento y/o ciclo de vida, deba almacenarse de forma cifrada para garantizar su integridad y confidencialidad.
- **Confidencial**: Información que contiene datos de carácter personal, datos de clientes de conocimiento no público, proyectos y actividades desarrollados por SENASA o documentación a la que únicamente tiene acceso la Dirección de la Organización o ciertos miembros (claves, etc.). En caso de divulgación puede causar perjuicio a la Organización.
- **Uso Interno**: Aquella información disponible al personal de la Organización, proveedores o terceros que precisen de información de la empresa para el desempeño de sus funciones (procedimientos, manuales, instrucciones del sistema de gestión, etc.), y que no ha sido clasificada como secreta, confidencial o pública.
- **Pública:** Información de la página web, folletos publicitarios, presentaciones divulgativas de productos y servicios, etc.

Las responsabilidades de la gestión y aprobación de la documentación se recogen en el procedimiento técnico **PR71-01-Control de la documentación.**

7.6. OBLIGACIONES DE LOS USUARIOS

Todos los miembros de SENASA tienen la obligación de conocer y cumplir la Política de Seguridad de la Información y las diferentes normativas en materia de seguridad de la información, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de SENASA con responsabilidad sobre la información atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año, a cuyo efecto se establecerá un programa de concienciación continua.

Los usuarios con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

7.7. TERCERAS PARTES

Cuando SENASA preste servicios a otros organismos o maneje información de estos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad creados y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando SENASA utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad de la Información y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de esta Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad de la Información que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

Aprobado por el Consejo de Administración de SENASA en la reunión celebrada con fecha 28 de noviembre de 2024.