# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

| **Edición** | **Modificaciones respecto a la edición anterior** |
|---|---|
| Primera edición | Creación del documento |

| **ELABORADO** | **APROBADO** |
|---|---|
| Responsable de seguridad<br>31.03.25 | Dirección<br>22.09.25 |

# ÍNDICE

# 1. Introducción

## 1.1. Misión y valores de la organización

- **Misión**. Es misión de la "Asociación para el Desarrollo de la Ingeniería de Mantenimiento" (en adelante INGEMAN) la promoción y difusión de la ingeniería del mantenimiento, facilitando el intercambio de opiniones y experiencias entre las personas involucradas en la función mantenimiento, contribuyendo a propagar una cultura de mantenimiento empresarial como medio para la calidad y la competitividad. Contribuyendo, al mismo tiempo, a la valoración del papel del mantenimiento y de las personas y entidades afectadas y a la mejora continua de la prestación de estos servicios.
- **Valores.** INGEMAN, presta sus servicios basándose en los valores que la organización considera adecuados en materia de seguridad. Estos valores implantados en la organización son:

  1.- Profesionalidad.
  2.- Protección de las Instalaciones.
  3.- Seguridad por defecto.
  4.- Protección de la información.
  5.- Prevención.
  6.- Mejora continua.
  7.- Confidencialidad.
  8.- Concienciación y formación.
  9.- Integridad y calidad de la información.
  10.- Disponibilidad de los sistemas de Información y continuidad de los servicios ante contingencias.
  11.- Gestión del riesgo.
  12.- Proporcionalidad en coste.

## 1.2. Servicios prestados

Desde INGEMAN se prestan los siguientes servicios:

- **Cooperación.** Establecer relaciones de cooperación con entidades pública o privadas, o con personas físicas, para la prestación de servicios, para promover la realización de estudios, trabajos e investigaciones técnicas sobre la ingeniería de mantenimiento y la gestión de activos y para la realización de ensayos de interés para la industria en general y en particular para sus asociados
- **Investigación.** Promover la realización de estudios, trabajos e investigaciones científicas sobre ingeniería del mantenimiento, para su implantación y mejora en el ámbito académico y empresarial.
- **Publicación.** Promover la publicación de trabajos y artículos sobre aspectos que se estimen de interés para la formación de los profesionales del mantenimiento o los fines sociales, en general.

- **Intercambio.** Establecer contactos con entidades o personas del resto de la industria española e internacional, para el intercambio de ideas y experiencias en los temas antes indicados.
- **Difusión.** Divulgar la importancia de la mejora de la mantenibilidad desde la fase de diseño de los sistemas, entre los diseñadores y fabricantes, como medio para reducir los costos en que incurrirán, más tarde, los usuarios de los mismos, al emplearlos como activos empresariales.
- **Normalización.** Participar y difundir las actividades de normalización del mantenimiento velando por el cumplimiento de las normas.
- **Organización.** Realizar actos para la difusión y formación en la ingeniería del mantenimiento tales como, cursos, seminarios, conferencias, congresos, jornadas técnicas, etc.
- **Certificación.** Llegar a acuerdos con entidades de normalización y certificación para poder certificar el cumplimiento de normas en el ámbito del mantenimiento.
- **Premios**. Constituir y fallar premios y becas para los trabajos de investigación y divulgación en relación con la ingeniería del mantenimiento.
- **Mejora de la competitividad**. Contribuir a la mejora de la competitividad de las empresas mediante la innovación y el desarrollo tecnológico.

## 2. Justificación de la política de seguridad de la información

### 2.1. Necesidad de seguridad en los sistemas

Para el cumplimiento de su misión, la prestación de los servicios identificados y el cumplimiento de sus objetivos, INGEMAN depende de los Sistemas TIC (Tecnologías de la Información y Comunicaciones).

Estos sistemas son administrados con diligencia, adoptando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información tratada o de los servicios prestados.

El objetivo de la seguridad de la información es garantizar la disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando ante posibles incidentes.

Los sistemas TIC están protegidos contra amenazas de rápida evolución con potencial para incidir en las dimensiones de seguridad anteriormente descritas, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se implementan estrategias que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios.

### 2.2. Requisitos de seguridad

INGEMAN aplica las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad (ENS), así como realiza un seguimiento continuo de los niveles de prestación de servicios, sigue y analiza los riesgos y vulnerabilidades a los que están expuestos los servicios y la información, y prepara una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Toda la organización debe 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 pliegos de licitación para proyectos de TIC.

INGEMAN en su compromiso por la seguridad integral está preparado para prevenir, detectar, reaccionar y recuperarse de incidentes.

## 3. Marco normativo

El marco legal en materia de seguridad de la información viene establecido por la siguiente legislación:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, fija los principios básicos y requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la Administración.
- 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 (RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos de carácter personal y garantía de derechos digitales.
- Ley Orgánica 1/2002, de 22 de marzo, que regula el Derecho de Asociación. Esta ley establece los principios básicos para la creación, funcionamiento y disolución de asociaciones, garantizando el derecho fundamental de asociación reconocido en el artículo 22 de la Constitución Española.

Las normas jurídicas que constituyen el marco legal de INGEMAN, así como la documentación normativa y legal que pudiera ser de aplicación se identifica en un registro disponible en los recursos habilitados por INGEMAN, el cual es revisado y actualizado periódicamente.

## 4. Principios de protección

Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información. Se establecen los siguientes:

A. **Seguridad integral:** La seguridad se entenderá como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos,

relacionados con el sistema, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas de información.

Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y la de los responsables jerárquicos, para evitar que, la ignorancia, la falta de organización y de coordinación o de instrucciones adecuadas, constituyan fuentes de riesgo para la seguridad

B. **Gestión de Riesgos**: El análisis y gestión de riesgos será parte esencial del proceso de seguridad, constituyendo una actividad continua y permanentemente actualizada. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.

C. **Prevención, detección, respuesta y conservación**: La seguridad del sistema debe contemplar las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta.

   Las medidas de prevención, que podrán incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, deben eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse.

   Las medidas de detección irán dirigidas a descubrir la presencia de un incidente de seguridad y ciberincidente.

   Las medidas de respuesta, que se gestionan en tiempo oportuno, están orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.

   Sin merma de los restantes principios básicos y requisitos mínimos establecidos, el sistema de información garantizará la conservación de los datos e información en soporte electrónico.

   De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

D. **Existencia de líneas de defensa**: El sistema de información ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuesta de forma que, cuando una de las capas sea comprometida, permita:

   - Desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto.

- Minimizar el impacto final sobre el mismo.

Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

E. **Vigilancia continua y Reevaluación periódica (Mejora continua)**: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado.

F. **Responsabilidad diferenciada**: En los sistemas de información se diferenciará el responsable de la información, que determina los requisitos de seguridad de la información tratada; el responsable del servicio, que determina los requisitos de seguridad de los servicios prestados; el responsable de seguridad, que determina las decisiones para satisfacer los requisitos de seguridad y el responsable del sistema, que se encarga de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo.

Las directrices fundamentales de seguridad se concretan en un conjunto de principios particulares y responsabilidades específicas, que se configuran como objetivos instrumentales que garantizan el cumplimiento de los principios básicos de la Política de Seguridad. Se establecen los siguientes:

a. Organización e implantación del proceso de seguridad.
b. Análisis y gestión de los riesgos.
c. Gestión de personal.
d. Profesionalidad.
e. Autorización y control de los accesos.
f. Protección de las instalaciones.
g. Adquisición de productos de seguridad y contratación de servicios de seguridad.
h. Mínimo privilegio.
i. Integridad y actualización del sistema.
j. Protección de la información almacenada y en tránsito.
k. Prevención ante otros sistemas de información interconectados.
l. Registro de la actividad y detección de código dañino.
m. Incidentes de seguridad.
n. Continuidad de la actividad.
o. Mejora continua del proceso de seguridad.

## 5. Roles del sistema de seguridad de la información de INGEMAN

La seguridad debe comprometer a todos los miembros de la Organización.

La Política de Seguridad de INGEMAN identifica a los responsables para velar por su cumplimiento y ser conocida por todos los miembros de la organización.

La responsabilidad de INGEMAN recae, en última instancia, en su Dirección. La Dirección es responsable de organizar las funciones y responsabilidades, la política de seguridad y de facilitar los recursos adecuados para alcanzar los objetivos propuestos.

La estructura organizativa de seguridad, y jerarquía en el proceso de decisiones la componen:

| Rol | Funciones |
|---|---|
| **Dirección** | Máxima representación de Ingeman que decide la misión y los objetivos de la organización en materia de seguridad de la información.<br>Es el máximo responsable de la implantación del ENS. |
| **Comité de Seguridad** | Órgano que toma decisiones que concretan cómo alcanzar los objetivos de en seguridad de la información y protección de la privacidad.<br>Es el principal responsable de establecer los recursos y medidas de seguridad necesarias para el tratamiento de los riesgos en materia de seguridad de la información. |
| **Responsable de la Información** | Tiene la responsabilidad última sobre qué seguridad requiere una cierta información manejada por Ingeman.<br>Determina los niveles de impacto (alto, medio o bajo) de las dimensiones de seguridad de la información.<br>Realiza la valoración de las consecuencias de un impacto negativo sobre la seguridad de la información atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio y el respeto de la legalidad. |
| **Responsable del Servicio** | A nivel de gobierno o nivel ejecutivo.<br>Determina los niveles de impacto (alto, medio o bajo) de las dimensiones de seguridad de los servicios.<br>Determina los requisitos (de seguridad) de los servicios prestados.<br>Tiene la responsabilidad última de determinar los niveles de servicio aceptables por la Organización como una actividad indelegable. |
| **Responsable de la Seguridad** | A nivel ejecutivo.<br>Funciona como supervisor del sistema de información y vehículo de reporte al Comité de Seguridad.<br>Determina las decisiones de seguridad pertinentes para satisfacer los requisitos de seguridad de la información y de los servicios, de acuerdo a lo establecido en la Política de Seguridad de la Información.<br>Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.<br>Deberá ser una persona física, jerárquicamente independiente. |

| Rol | Funciones |
|---|---|
| **Responsable del Sistema** | A nivel operacional.<br>Se encarga de la operación del sistema de información, atendiendo a las medidas de seguridad determinadas por el Responsable de la Seguridad.<br>Toma decisiones operativas: arquitectura del sistema, adquisiciones, instalaciones y operación del día a día.<br>Funciones:<br>a. Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información. |
| **Administrador de seguridad** | A nivel operacional<br>Encargado de ejecutar las acciones diarias de operación del sistema según las indicaciones recibidas. Depende del Responsable del Sistema.<br>Funciones:<br>a. La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.<br>b. La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información.<br>c. La gestión de las autorizaciones y privilegios concedidos a los usuarios del sistema, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.<br>d. La aplicación de los procedimientos operativos de seguridad.<br>e. Asegurar que los controles de seguridad establecidos son adecuadamente ejecutados.<br>f. Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.<br>g. Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.<br>h. Informar al Responsable de la Seguridad y al Responsable del Sistema de cualquier de anomalía, compromiso o vulnerabilidad relacionada con la seguridad.<br>i. Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución. |
| **Responsable de Protección de Datos** | Figura obligatoria para administraciones públicas, es el encargado de asesorar y supervisar todos los aspectos relacionados con el tratamiento de datos de carácter personal, incluidos los aspectos de seguridad (integridad, confidencialidad y disponibilidad) y violación de datos personales. Su nombramiento se produce por otra vía ya que sus cometidos no se ciñen únicamente a aspectos de seguridad.<br>INGEMAN cuenta con un Responsable de Protección de Datos para el |

| Rol | Funciones |
|---|---|
| | cumplimiento en la legislación en materia de protección de datos. |

### 5.1. Responsable de la Información

Al Responsable de la información corresponden las siguientes funciones:

| Función | Detalle |
|---|---|
| Responsabilidad | Tiene la responsabilidad última del tratamiento que se haga de una cierta información y, por tanto, de su protección. |
| Establecer requisitos de seguridad sobre la información | Establece los requisitos de la información en materia de seguridad y determina los niveles de seguridad de la información. |
| Determinar niveles de seguridad en cada dimensión | Determinar los niveles de seguridad en cada dimensión (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad). Aunque la aprobación formal de los niveles corresponda al Responsable de la Información, recabará una propuesta del Responsable de la seguridad y del Responsable del Sistema. |
| Adoptar medidas sobre los datos personales | 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. |

### 5.2. Responsable del Servicio

Al Responsable del Servicio corresponden las siguientes funciones:

| Función | Detalle |
|---|---|
| Responsabilidad | Tiene la responsabilidad última del uso que se haga de determinados servicios y, por tanto, de su protección. |
| Establecer los requisitos de seguridad del servicio | Tiene la potestad de establecer los requisitos del servicio en materia de seguridad y de determinar los niveles de seguridad de los servicios.<br>Aunque la aprobación formal de los niveles corresponda al Responsable del servicio, recabara una propuesta al Responsable de la seguridad y conviene que se escuche la opinión del Responsable del sistema. |
| Riesgos | Aprobar el riesgo residual (el resultante, una vez aplicados los controles de seguridad). |

### 5.3. Responsable de Seguridad

El Responsable de Seguridad es una figura clave, ya que a él le corresponde dinamizar y gestionar el día a día de todo el proceso de seguridad de la información.

Las funciones del Responsable de seguridad son las siguientes:

| Función | Detalle |
|---|---|
| Política Normativa y Procedimientos | Participa en la elaboración, en el marco del Comité de Seguridad, de la política y normativa de seguridad de la Información, para su aprobación por Dirección.<br>Elabora y aprueba los procedimientos operativos de seguridad de la Información. |
| Formación y concienciación | Promueve la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.<br>Elabora los Planes de formación y concienciación del personal en seguridad de la información, que serán aprobados por el Comité de seguridad. |
| Gestión de la Seguridad | Mantiene 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 presente política.<br>Recopila los requisitos de seguridad de los Responsables de información y servicio y determina la categoría del sistema.<br>Realizará el análisis de riesgos.<br>Facilita al Comité de Seguridad y a los Responsables 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.<br>Elabora la Declaración de Aplicabilidad a partir de las medidas de seguridad requeridas conforme al Anexo II del ENS y del resultado del análisis de riesgos.<br>Elabora, junto a al Responsable de Sistemas, planes de mejora de la seguridad, para su aprobación por el Comité de seguridad.<br>Valida los planes de continuidad de sistemas que elaborados por el Responsable de sistemas, que deben ser aprobados por el Comité de seguridad y probados periódicamente por el Responsable de sistemas.<br>Aprueba las directrices propuestas por el Responsable de sistemas para considerar la seguridad de la información durante todo el ciclo de vida de los activos y procesos: especificación, arquitectura, desarrollo, operación y cambios.<br>Elabora el informe anual sobre el estado de la seguridad de la información, con el progreso de los proyectos de los planes de mejora, resumen de las actuaciones en materia de seguridad, de los incidentes relativos a seguridad de la información, del estado de la seguridad del sistema, y en particular del nivel de riesgo residual al que está expuesto el sistema. |
| Monitorizar | Monitoriza los principales riesgos residuales asumidos por la Organización y recomienda posibles actuaciones respecto de ellos.<br>Monitoriza el desempeño de los procesos de gestión de incidentes de seguridad y recomienda posibles actuaciones respecto de ellos. En particular, vela por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información. |
| Asesoramiento | Asesora a otros responsables en la determinación de las medidas de seguridad necesarias a partir de los requisitos de seguridad establecidos |

| Función | Detalle |
|---|---|
| | por el contexto interno y externo del ámbito de la empresa |
| Comité de Seguridad | Facilita periódicamente al Comité de Seguridad 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 residual al que está expuesto el sistema). |

### 5.4. Responsable del Sistema

El Responsable del sistema es la persona que toma las decisiones operativas: arquitectura del sistema, adquisiciones, instalaciones y operación del día a día.

Las funciones del Responsable del sistema son las siguientes:

| Función | Detalle |
|---|---|
| Gestionar el Sistema | Desarrollar, operar y mantener los sistemas de información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.<br>Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.<br>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 el Responsable de la seguridad antes de ser ejecutada. |
| Establecer directrices y medidas | Definir la topología y sistema de gestión del sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.<br>Definir la política de conexión o desconexión de equipos y usuarios nuevos en el sistema.<br>Decidir las medidas de seguridad que aplican a los suministradores de componentes del sistema durante las etapas de desarrollo, instalación y prueba de este.<br>Determinar la configuración autorizada de hardware y software a utilizar en el sistema.<br>Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del sistema.<br>Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos. |
| Elaborar | Elaborar procedimientos operativos de seguridad. |
| Aprobar | Aprobar los cambios que afecten a la seguridad del modo de operación del sistema.<br>Aprobar los cambios en la configuración del sistema de información.<br>Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema. |
| Monitorizar | 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. |

### 5.5. Administrador de la Seguridad

El Administrador de seguridad es la persona encargada de ejecutar las acciones diarias de operación del sistema según las indicaciones recibidas de sus superiores jerárquicos.

Las funciones del Administrador de la Seguridad del Sistema son las siguientes:

| Función | Detalle |
|---|---|
| Implementar, gestionar y mantener la seguridad | La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.<br>Asegurar el estricto cumplimiento de los controles de seguridad establecidos.<br>Informar a los responsables de la seguridad y del Sistema sobre cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.<br>Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución. |
| Gestión, configuración y actualización | La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información.<br>Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes. |
| Gestión de las autorizaciones | La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado. |
| Aplicar los procedimientos | La aplicación de los procedimientos operativos de seguridad.<br>Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información. |
| Monitorizar la seguridad | Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema. |

### 5.6. Responsable de Protección de Datos

Las funciones del Responsable de Protección de Datos son las siguientes:

| Función | Detalle |
|---|---|
| Protección de Datos | Revisar, aprobar y gestionar la documentación derivada del cumplimiento de la protección de datos. |
| Protección de | Velar por el cumplimiento de las medidas necesarias en materia de |

| | |
|---|---|
| Datos | protección de datos. |

### 5.7. Comité de Seguridad

INGEMAN ha creado el Comité de Seguridad que estará compuesto por los siguientes puestos:

- Presidente de INGEMAN.
- Responsable de la Información.
- Responsable del Servicio.
- Responsable de la Seguridad.
- Responsable del sistema.
- Administrador de Seguridad.
- Responsable de Protección de Datos.

Funciones del secretario. Corresponde al secretario/a del Comité de Seguridad:

- Convocar las reuniones del Comité de Seguridad
- Preparar los temas a tratar en las reuniones del Comité, 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 Comité.

Funciones de los Vocales. Corresponde a los vocales del Comité de Seguridad:

- Participar en las reuniones.
- Contribuir con ideas y sugerencias para el buen desarrollo de las reuniones.

Los vocales pueden ser otras personas ajenas a la organización invitadas por el Comité de seguridad.

Todos miembros del Comité actuarán con voz y voto y sus acuerdos requerirán, como mínimo, el voto de la mayoría simple de sus miembros.

Funciones del Comité: Corresponde al Comité de Seguridad:

| Función | Detalle |
|---|---|
| Informar | Las inquietudes de la Dirección y de los diferentes departamentos/áreas en materia de seguridad de la información.<br>Del estado de la seguridad de la información a la Dirección. |
| Promover | La mejora continua.<br>La realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de INGEMAN en materia de seguridad. |

| Función | Detalle |
|---|---|
| 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. |
| Resolver | Los conflictos de responsabilidad que puedan aparecer entre los diferentes roles, responsables y/o entre diferentes áreas, elevando aquellos casos en los que no tenga suficiente autoridad para decidir. |
| Elaborar | La estrategia de evolución de INGEMAN en lo que respecta a la seguridad de la información. |
| Supervisar | La Política de seguridad de la Información.<br>Las auditorías internas de seguridad antes de cada certificación ENS. |
| Aprobar | La Política de Seguridad de la Información.<br>La normativa de seguridad de la información.<br>Los requisitos de formación y cualificación los puestos relacionados con la seguridad de la información.<br>Planes de mejora de la seguridad de la información.<br>La categorización del sistema de información de la organización en base al impacto (alto, medio o bajo) de las dimensiones de seguridad (confidencialidad, integridad, autenticidad, trazabilidad y disponibilidad) de los servicios y la información. |
| Velar | Por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.<br>Por qué la seguridad de la información se tenga en cuenta en todos los proyectos de la organización, desde su especificación inicial hasta su puesta en operación, por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas de la tecnología de la información.<br>Por la coordinación la respuesta ante incidentes, con roles y tiempos de respuesta bien definidos. |
| Monitorizar | El desempeño del sistema de información, asegurando la monitorización continua, estableciendo indicadores clave de rendimiento (KPIs) de seguridad. |

A requerimiento del Comité se convocará cualesquiera otras personas, cuya intervención sea precisa por ser afectados por el Esquema Nacional de Seguridad.

### 5.8. Responsable de Gestión del Personal

Al Responsable de Gestión del Personal le corresponde implantar las medidas de seguridad que le competan dentro del ámbito laboral de las personas y los recursos humanos de INGEMAN, incluyendo aspectos de seguridad de la información (ej. firma de normativa de uso de sistemas de información), e informará al Responsable de Seguridad de su grado de implantación, eficacia e incidentes.

### 5.9. Procedimientos de designación de personas del Comité

La Dirección de INGEMAN nombra formalmente mediante un acta de constitución a los integrantes del Comité, realizando así la designación a los distintos responsables del sistema de seguridad de la información en el ámbito del Esquena Nacional de Seguridad.

El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

## 5.10. Delegación de funciones

En caso de que, por su complejidad, distribución, separación física de sus elementos o número de usuarios se necesite de personal adicional para llevar a cabo las funciones de Responsable de la Seguridad, se podrá designar cuantos Responsables de Seguridad Delegados considere necesarios.

La designación corresponde al responsable de la Seguridad. Por medio de la designación de delegados, se delegan funciones. La responsabilidad final sigue recayendo sobre el Responsable de la Seguridad.

Los delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el responsable de la Seguridad. Es habitual que se encarguen de la seguridad de sistemas de información concretos o de sistemas de información horizontales.

Cada delegado tendrá una dependencia funcional directa del responsable de la Seguridad, que es a quien reportan.

## 5.11. Jerarquía en el proceso de decisiones y mecanismos de coordinación

Los diferentes roles de seguridad de la información (autoridad principal y posibles delegadas) se limitan a una jerarquía simple: el Comité de seguridad da instrucciones al Responsable de seguridad que se encarga de establecer las medidas de seguridad y supervisar que el Responsable del sistema las implementa según lo establecido en la política de seguridad aprobada para la INGEMAN.

El Responsable de Seguridad:

- Informa al Responsable del Sistema de las decisiones e incidentes en materia de seguridad que afecten a la información que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.
- Informa al Responsable del servicio de las decisiones e incidentes en materia de seguridad que afecten al servicio que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.
- Da cuenta al Comité de Seguridad:
    - Resumen consolidado de actuaciones en materia de seguridad.
    - Resumen consolidado de incidentes relativos a la seguridad de la información.

- Estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto.

El Responsable del Sistema

- Informa al Responsable de la Información de las incidencias y/o incidentes relativas a la información que le compete.
- Informa al Responsable del Servicio de las incidencias y/o incidentes relativas al servicio que le compete.
- Da cuenta al Responsable de la Seguridad:
  - Actuaciones en materia de seguridad, en particular en lo relativo a decisiones de arquitectura del sistema.
  - Resumen consolidado de los incidentes de seguridad.
  - Medidas de la eficacia de las medidas de protección que se deben implantar.

## 6. Estructura normativa y desarrollo de la Política de Seguridad

La estructura jerárquica de la documentación de seguridad es la siguiente:

| Documento | Detalle |
|---|---|
| Política | Define las metas y expectativas de seguridad.<br>Describe qué tipo de gestión de la seguridad se pretende lograr y cuáles son los objetivos perseguidos.<br>Debe ser elaborada por el Comité de seguridad y ser aprobada por la Dirección. |
| Normativa | Establece lo que se debe hacer y uniformiza el uso de aspectos concretos del sistema.<br>Es de carácter obligatorio.<br>Debe ser escrita por personas expertas en la materia o por el Responsable de seguridad y aprobada por el Comité de seguridad. |
| Procedimiento | Determina las acciones o tareas a realizar en el desempeño de un proceso relacionado con la seguridad y las personas o grupos responsables de su ejecución.<br>Un procedimiento debe ser claro, sencillo de interpretar y no ambiguo en su ejecución. No tiene por qué ser extenso, dado que la intención del documento es indicar las acciones a desarrollar.<br>Un procedimiento puede apoyarse en otros documentos para especificar, con el nivel de detalle que se desee, las diferentes tareas. Para ello, puede relacionarse con otros procedimientos o con instrucciones técnicas de seguridad.<br>Debe ser elaborado por el Responsable del sistema y aprobado por el Responsable de Seguridad. |
| Instrucciones técnicas | Determina las acciones o tareas necesarias para completar una actividad o proceso de un procedimiento concreto sobre una parte concreta del sistema de información (hardware, sistema operativo, aplicación, datos, |

| Documento | Detalle |
|---|---|
| | usuario, etc.).<br>Al igual que un procedimiento, son la especificación pormenorizada de los pasos a ejecutar.<br>Una instrucción técnica debe ser clara y sencilla de interpretar.<br>Debe documentar los aspectos técnicos necesarios para que la persona que ejecute la instrucción técnica no tenga que tomar decisiones respecto a la ejecución de esta. A mayor nivel de detalle, mayor precisión y garantía de su correcta ejecución.<br>Pueden ser elaborados por el Responsable del sistema o Administrador del sistema y deben ser aprobados por el Responsable de seguridad. |
| Guías | Tienen un carácter formativo y buscan ayudar a los usuarios a aplicar correctamente las medidas de seguridad proporcionando razonamientos donde no existen procedimientos precisos. Por ejemplo, suele haber una guía sobre cómo escribir procedimientos de seguridad.<br>Las guías ayudan a prevenir que se pasen por alto aspectos importantes de seguridad que pueden materializarse de varias formas.<br>Deben ser aprobadas por el Responsable de seguridad. |

La gestión de la documentación competé al Responsable de Seguridad y la gestión del acceso a la misma al Responsable del Sistema. Toda la documentación se encuentra disponible para todo el personal a través de los medios electrónicos oficiales de la organización.

Todo el personal de INGEMAN, ya sea interno y externo debe cumplir con las políticas, procedimiento e instrucciones técnicas de la organización.

## 7. Gestión de riesgos

Todos los sistemas sujetos a esta política deben contar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos.

El análisis de riesgos será la base para determinar las medidas de seguridad que se deben adoptar además de los mínimos establecidos por el Esquema Nacional de Seguridad.

El proceso de análisis, gestión de los riesgos y selección de medidas de seguridad a aplicar, (proporcionales a los riesgos y debidamente justificadas), es revisado y aprobado cada año por INGEMAN.

El análisis de los riesgos y su tratamiento deben ser una actividad repetida regularmente. Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando se produzcan cambios significativos en el sistema de información, servicios o información.
- Cuando ocurra un incidente de seguridad o se reporten vulnerabilidades graves o relevantes, según se considere.

### 7.1. Criterios de evaluación de riesgos

Para la armonización de los análisis de riesgos, el Comité de seguridad establece una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

Los criterios de evaluación de riesgos detallados se especifican en la metodología de evaluación de riesgos que ha elaborado INGEMAN, basándose en estándares y buenas prácticas reconocidas.

El Comité de Seguridad dinamiza la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

### 7.2. Riesgos que se derivan del tratamiento de los datos personales

Los riesgos derivados del tratamiento de datos personales se evalúan y tratan en base a la legislación vigente en materia de protección de datos.

## 8. Gestión de incidentes de seguridad

### 8.1. Prevención de incidentes

Todo INGEMAN, debe 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 INGEMAN implementa las medidas mínimas de seguridad determinadas por el ENS, 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 todo el personal, deben estar claramente definidos y documentados.

### 8.2. Monitorización y detección de incidentes

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios son monitorizados 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.

La gestión de incidentes se desarrolla en los procedimientos documentados y formales establecidos en INGEMAN.

# 9. Responsabilidades

## 9.1. Personal de INGEMAN

El personal de INGEMAN tiene la obligación de conocer y cumplir esta Política de seguridad de la información, así como el marco normativo de seguridad, siendo responsabilidad del Comité de seguridad disponer los medios necesarios para que la información llegue a los afectados.

El personal de INGEMAN atenderá a una sesión de concienciación en materia de seguridad TIC al menos una vez cada dos años. Se establece un programa de concienciación continua para atender al personal de INGEMAN, en particular al personal de nueva incorporación.

Las personas 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 es 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.

El cumplimiento de la presente Política de seguridad es obligatorio por parte de todo el personal interno o externo que intervenga en los procesos de INGEMAN, constituyendo su incumplimiento infracción grave a efectos laborales.

## 9.2. Terceras partes

INGEMAN da a conocer esta Política de Seguridad a través de su página web y hace participe de la misma a terceras partes pertinentes para su sistema de seguridad de la información. Así mismo, asegura que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política:

- Cuando se presten servicios o se gestione información de otras organizaciones, se les hará partícipe de esta Política de seguridad de la información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.
- Cuando se utilicen servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de seguridad y de la Normativa de seguridad que ataña a dichos servicios o información. Dicha tercera parte queda 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.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad 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.

Las terceras partes involucradas en tratamientos de datos de carácter personal deberán satisfacer los requisitos establecidos en la legislación en materia de protección de datos.

## 10. Revisión y aprobación de la política de seguridad

La Política de Seguridad de la Información es revisada por el Comité de Seguridad al menos anualmente, o siempre que se produzcan cambios ya sean menores o significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

Los cambios sobre la Política de Seguridad de la Información deben aprobarse por la Dirección de INGEMAN.

Cualquier cambio sobre la misma debe difundirse a todas las partes afectadas.