POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Ineco, empresa de ingeniería y consultoría referente en movilidad sostenible y transformación digital, ratifica su firme compromiso para velar por la seguridad de la información en todos sus procesos, sirviendo el presente documento como marco de referencia de este **compromiso**, el cual es de aplicación en todas las fases del ciclo de vida de la información (generación, distribución, almacenamiento, procesamiento, transporte, consulta y destrucción), así como a los sistemas de información que la sustentan. Se incluye a todos los activos, procesos, servicios y tecnologías implicados en el tratamiento de la información, independientemente de su formato o ubicación, y abarca tanto al personal interno como a terceros que accedan o gestionen información en nombre de Ineco.

MISIÓN

Corresponden a Ineco las competencias y funciones establecidas por los estatutos del propio organismo, así como aquellas que deriven de su relación con el resto de las empresas, entidades jurídicas, Administraciones Públicas del Estado o personas físicas.

ALCANCE

Se establece el alcance de esta política de seguridad de la información en cumplimiento del ENS e ISO 27001, definido como:

"Los sistemas de información que soportan los servicios que conforman el catálogo de productos de Ineco:

- *Administración Inteligente*
- *Smart Products*
- *ERTMS*
- *Consultoría*
- *Proyectos*
- *Obras*
- *Operación*
- *Mantenimiento*
- *I+D+I*
- *ORAT*
- *Material Rodante*
- *BIM*
- *Project Management*

según la Declaración de Aplicabilidad vigente "

MARCO REGULATORIO

La presente política se desarrolla conforme al marco legal vigente en materia de seguridad de la información, incluyendo el Esquema Nacional de Seguridad (Real Decreto 311/2022 de 3 de mayo), en delante ENS, el Reglamento General de Protección de Datos (RGDP) y demás normativas aplicables establecidas en el documento integrado en nuestro sistema de gestión.

PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad de la Información aplica los principios básicos que se establecen en el ENS y la norma ISO 27001, de acuerdo con el interés general, naturaleza y complejidad de la materia regulada, permitiendo una protección adecuada de la información y los servicios.

Atendiendo al ENS y la norma ISO 27001, Ineco implementa diversas medidas de seguridad proporcionales a la naturaleza de la información y los servicios a proteger, teniendo en cuenta la categoría de los sistemas afectados, bajo los siguientes principios:

La seguridad como proceso integral

La seguridad de la información en Ineco debe contar con el compromiso y apoyo de todos los niveles directivos de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas de la organización para conformar un todo coherente y eficaz. La seguridad constituye un proceso integral compuesto por todos los elementos técnicos, humanos, materiales y organizativos relacionados con el sistema basado en la mejora continua de todos ellos y del proceso en sí mismo.

Se debe prestar la máxima atención a la formación y 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.

Prevención, detección, respuesta y conservación

Ineco implementa un proceso integral de prevención, detección, respuesta y conservación frente a incidentes de seguridad con procedimientos de detección, análisis, comunicación, resolución y registro de las actuaciones para la mejora continua de la seguridad de los sistemas, designando un punto de contacto para las comunicaciones con respecto a incidentes detectados y estableciendo protocolos para el intercambio de información relacionada con el incidente, incluyendo las comunicaciones con los Equipos de Respuesta a Emergencias (CERT).

Líneas de defensa

Ineco implementa una estrategia de protección basada en múltiples capas, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una de las capas falla, el sistema implementado permita:

- ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse;
- reducir la probabilidad de que el sistema sea comprometido en su conjunto y
- minimizar el impacto final sobre el mismo.

Vigilancia continua

La vigilancia continua exige la monitorización de los registros de actividad. Se registrará la información estrictamente necesaria para la investigación de actividades indebidas o no autorizadas que permitan identificar al responsable de la actividad.

Reevaluación periódica

Ineco implementa controles y evaluaciones regulares y periódicas de la seguridad, de forma interna o con la ayuda de terceros, para conocer en todo momento el estado de la seguridad de los sistemas y adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección.

Diferenciación de responsabilidades

Se organiza la seguridad comprometiendo a todos los miembros de Ineco mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas.

Se nombrarán, al menos, el responsable de la información, el responsable del servicio, el responsable de seguridad, y el responsable del sistema, quedando diferenciada la responsabilidad de la seguridad de la responsabilidad de explotación de los sistemas.

ROLES Y COMITÉS

En el contexto de la seguridad de la información, Ineco ha definido los siguientes roles y comités:

Comité de Seguridad y Riesgos de la Información

Para la gestión de la Seguridad de la Información, se crea el Comité de Seguridad y Riesgos de la Información formado por un equipo multidisciplinar que coordinará las actividades y controles de seguridad establecidos en Ineco y que velará por el cumplimiento de la normativa vigente, interna y externa, en materia de protección de datos de carácter personal y seguridad.

Las funciones del Comité de Seguridad y Riesgos de la Información son las siguientes:

- Elaborar y revisar regularmente la Política de Seguridad de la Información que deberá ser aprobada por la Dirección de Ineco.
- Definir, dentro de la Política de Seguridad de la Información, la asignación de roles y los criterios para alcanzar las garantías pertinentes en lo relativo a segregación de funciones.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización, elevándolo a la Dirección en aquellos casos en los que no tenga suficiente autoridad para decidir.
- Aprobar el marco normativo y medidas técnicas a implementar de acuerdo con el Plan Director de Seguridad de la Información (PDSI).
- Coordinar todas las funciones de seguridad de la organización.
- Velar por el cumplimiento de la normativa legal y sectorial de aplicación.
- Velar por el alineamiento de las actividades de seguridad con los objetivos de la organización.
- Coordinar los Planes de Continuidad de las diferentes áreas, para asegurar una actuación sin fisuras en caso de que deban ser activados.
- Recibir las inquietudes en materia de seguridad de la Dirección y transmitirlas a los responsables departamentales pertinentes, recabando de ellos las correspondientes respuestas y soluciones que, una vez coordinadas, habrán de ser comunicadas a la Dirección.
- Recabar, a través del Responsable de Seguridad, informes regulares del estado de la seguridad de la organización y de los posibles incidentes, para poder adoptar las decisiones oportunas.
- Promover la mejora continua del sistema de gestión de la seguridad de la información (SGSI).
- Elaborar la estrategia de evolución de la organización en lo que respecta a 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, que están alineados con la estrategia decidida en la materia, evitando duplicidades.
- Supervisar y aprobar la gestión de riesgos de seguridad de la información, el Plan de Tratamiento de Riesgos (PTR) y los principales riesgos residuales asumidos por la organización, recomendando a la Dirección posibles actuaciones.
- A través del Responsable de Seguridad, monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
- 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 la organización. En particular velará por la coordinación de distintos planes que puedan realizarse en diferentes áreas.

- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en operación.

Este Comité identifica objetivos y estrategias relacionados con la seguridad de la información y dirige y controla los procesos relacionados con la seguridad. Su composición estará formada por las personas que ostenten los siguientes cargos:

Secretario: Corresponde al Secretario/a del Comité de Seguridad y Riesgos de la Información

- Convocar las reuniones del Comité de Seguridad y Riesgos de la Información
- 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.
- Comunicar las decisiones tomadas en comité a los diversos responsables encargados de su ejecución.
- Firmar aquellos documentos del SGSI aprobados colegiadamente por el Comité, en representación de este.

Vocales: Corresponde a los vocales del Comité de Seguridad y Riesgos de la Información

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

Las decisiones del Comité serán consensuadas entre todos los participantes. Todos los integrantes del Comité actuarán de manera autónoma, no viéndose obligado en actuar ni votar condicionado por otros miembros del Comité.

El Comité se reunirá periódicamente, como mínimo, una vez al año para validar y revisar todos los puntos anteriores.

ROLES Y RESPONSABILIDADES

Anualmente, la Dirección designará los distintos cargos de seguridad, presentándolos en una reunión del Comité de Seguridad y Riesgos de la Información. En caso de no recogerse nuevas designaciones, se entenderán renovados los cargos actuales por un periodo de un año, sin periodicidad máxima, sujeto a la necesidad de la empresa.

El Comité de Seguridad y Riesgos de la Información nombrará formalmente mediante acta a los distintos roles responsables.

Las funciones de los diferentes roles de seguridad son las siguientes.

Responsable del Servicio

Tiene la potestad de establecer los requisitos del servicio en materia de seguridad o, en terminología del ENS, la potestad de determinar los niveles de seguridad de los servicios. Aunque la aprobación formal de los niveles corresponda al Responsable del Servicio, se puede recabar una propuesta al Responsable de Seguridad y conviene que se escuche la opinión del Responsable del Sistema.

El Responsable del Servicio deberá tener en cuenta que 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.

Aceptar el riesgo residual asociado a los servicios de los cuáles es responsable, obtenido tras llevarse a cabo el análisis de riesgos.

Gestionar los tratamientos que contengan datos personales y su tratamiento siguiendo las indicaciones del DPD.

Delegación de funciones

En caso de que, por su complejidad, distribución, separación física o número de usuarios se necesite personal adicional para llevar a cabo las funciones de Responsable del Servicio, se podrán designar cuantos Responsables del Servicio delegados se consideren necesarios.

La designación corresponde al Responsable del Servicio, por medio de la designación de delegados, se delegan funciones, la responsabilidad final sigue recayendo sobre el Responsable del Servicio.

Los delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable del Servicio relacionadas con su rol.

Responsable de la Información

Al Responsable de la Información le corresponde establecer los requisitos de la información en materia de seguridad. Igualmente es su competencia determinar los niveles de seguridad de la información en cada dimensión (confidencialidad, integridad, autenticidad, trazabilidad y disponibilidad) dentro del marco establecido en el Anexo I del ENS. Aunque la aprobación formal de los niveles corresponda al Responsable de la Información, podrá recabar una propuesta del Responsable de Seguridad y conviene que escuche la opinión del Responsable del Sistema.

Deberá adoptar o solicitar la adopción de 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, siguiendo siempre las indicaciones del DPD.

Tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.

Delegación de funciones

En caso de que, por su complejidad, distribución, separación física o número de usuarios se necesite personal adicional para llevar a cabo las funciones de Responsable de la Información, se podrán designar cuantos Responsables de la Información delegados se consideren necesarios.

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

Los delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable de la Información relacionadas con su rol.

Responsable de Seguridad

Será el responsable de tomar las decisiones apropiadas para satisfacer los requisitos de seguridad de la información y de los servicios, de mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad y de recopilar los requisitos de seguridad de los responsables de Información y Servicio y determinar la categoría del Sistema.

Igualmente es su responsabilidad realizar el Análisis de Riesgos de la información. Para ello:

- Facilitará a los responsables de Información y a los 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.
- Elaborará la Declaración de Aplicabilidad a partir de las medidas de seguridad requeridas conforme al Anexo II del ENS y los requisitos de los controles de la norma ISO 27001, así como del resultado del Análisis de Riesgos.
- Elaborará, junto al Responsable del Sistema, Planes de Mejora de la Seguridad, para su aprobación por el Comité de Seguridad y Riesgos de la Información.

- Monitorizará los principales riesgos residuales asumidos por la Organización y recomendará posibles actuaciones respecto de ellos.

Además, será responsable de:

- Validar los Planes de Continuidad de Sistemas que elabore el Responsable del Sistema, que deberán ser aprobados por el Comité de Seguridad y Riesgos de la Información y probada su idoneidad periódicamente.
- Promover la formación y concienciación en materia de Seguridad de la Información dentro de su ámbito de responsabilidad.
- Aprobar las directrices propuestas por el Responsable del 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.
- Elaborar la memoria 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 el desempeño de los procesos de gestión de incidentes de seguridad y recomendará posibles actuaciones respecto de ellos. En particular, velará por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de Seguridad de la Información.
- Asesorar a los responsables de áreas en la determinación de las medidas de seguridad necesarias a partir de los requisitos de seguridad establecidos por el contexto interno y externo de Ineco.
- Facilitar periódicamente al Comité de Seguridad y Riesgos 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.

Así mismo, actuará como secretario dentro del Comité de Seguridad y Riesgos de la Información.

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 del Responsable de Seguridad, se podrá designar cuantos Responsables de Seguridad Delegados considere necesarios.

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

Los delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable de 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 Seguridad, que es a quien reporta.

Responsable del Sistema

Es el responsable de la explotación del sistema de información.

Deberá responsabilizarse de gestionar el sistema de información de Ineco, incluyendo**:**

- Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

- 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 Seguridad antes de ser ejecutada.

Establecerá directrices y medidas de actuación responsabilizándose de:

- Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema.
- Decidir las medidas de seguridad que aplicarán los suministradores de componentes del Sistema durante las etapas de desarrollo, instalación y prueba del mismo.
- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema.
- Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del Sistema.
- Elaborar procedimientos de seguridad.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del Sistema.
- 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.

El Responsable del Sistema actuará de manera autónoma no viéndose obligado en actuar condicionado por el Responsable de Seguridad más allá de las funciones de supervisión de este, derivadas del rol que desempeña. Del mismo modo, tendrá independencia en sus decisiones y votación en el Comité de Seguridad, siendo independiente del Responsable de Seguridad.

Delegación de funciones

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

La designación corresponde al Responsable del Sistema, por medio de la designación de delegados, se delegan funciones, la responsabilidad final sigue recayendo sobre el Responsable del Sistema.

Los delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable del Sistema relacionadas con la operación, mantenimiento, instalación y verificación del correcto funcionamiento del Sistema de información.

Delegado de Protección de Datos

El Delegado de Protección de Datos tendrá, en lo que respecta a las responsabilidades del ENS, las siguientes funciones:

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del reglamento en vigor y de otras disposiciones de protección de datos de la Unión o de los Estados miembros.

- Supervisar el cumplimiento de lo dispuesto en el Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento 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 la protección de datos y supervisar su aplicación de conformidad con el ENS.
- Cooperar con la autoridad de control.
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

El Delegado de Protección de Datos 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.

Coordinación y resolución de conflictos

El Comité de Seguridad y Riesgos de la Información dará las instrucciones al Responsable de Seguridad, que se encargará de darles cumplimiento supervisando que administradores y operadores implementen las medidas de seguridad establecidas.

El Responsable del Sistema:

Informa al Responsable de la Información de las incidencias funcionales relativas a la información que le compete.

Informa al Responsable del Servicio de las incidencias funcionales relativas al servicio que le compete.

Da cuenta al Responsable de 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.

El Responsable de Seguridad:

Informa al Responsable de la Información 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 y Riesgos de la Información:

- 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.

Será el Comité de Seguridad y Riesgos de la Información el responsable de resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización, elevándolo a la Dirección en aquellos casos en los que no tenga suficiente autoridad para decidir.

Todas las decisiones del Responsable de Seguridad que afecten directamente al Responsable del Sistema se elevarán al Comité de Seguridad para realizar una evaluación previa a cualquier cambio o decisión.

REQUISITOS MÍNIMOS

Ineco depende de los sistemas de Tecnologías de Información y Comunicaciones, en adelante TIC, 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, trazabilidad y la autenticidad** de la información tratada o los servicios prestados.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en cualquiera de las cinco dimensiones de la seguridad de la información. 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. Es por ello por lo que el ENS, en su artículo 12 establece que "Todos los órganos superiores de las Administraciones Públicas deberán disponer formalmente de su Política de Seguridad, que será aprobada por el titular del órgano superior correspondiente".

Esto implica que Ineco debe aplicar las medidas mínimas de seguridad exigidas por el ENS, 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 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 pliegos de licitación para proyectos de TIC. Las áreas deben estar preparadas para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el Artículo 8 del ENS.

Ineco establece como **objetivos de seguridad de la información** los siguientes:

- Cumplir la legislación de seguridad y privacidad.
- Garantizar la calidad y protección de la información.
- Garantizar la prestación continuada de los servicios.
- Lograr la plena concienciación de los usuarios respecto a la seguridad de la información.

La Dirección de Ineco, comprometida con la implantación y el mantenimiento del Sistema de Gestión de la Seguridad de la Información, fijará y aprobará anualmente unos objetivos de nivel de riesgo aceptable en el Comité de Seguridad y Riesgos de la Información. Los objetivos deben ser vigentes y estar alineados con el propósito y la estrategia de la Organización, ser medibles o estimables y coherentes con las presentes directrices.

Datos de carácter personal

Ineco solo recogerá datos de carácter personal cuando sean adecuados, pertinentes, no excesivos y conforme al ámbito y a las finalidades para los que se hayan obtenido cumpliendo con las obligaciones y principios recogidos en la normativa de aplicación que esté vigente en cada momento en materia de protección de datos.

De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa vigente de protección de datos, todo ello, tal y como se establece en la normativa interna relacionada con la protección de datos personales.

Análisis y Gestión de los riesgos

Ineco asume el compromiso de controlar los riesgos de seguridad, así como dar cumplimiento a la legislación y normas internas vigentes bajo un proceso de mejora continua conforme a los marcos y metodologías existentes en la actualidad en análisis y gestión de riesgos.

Con el objetivo de conocer el nivel de exposición de los activos de información a los riesgos y amenazas en seguridad, el Responsable de Seguridad acordará la realización de un análisis de riesgos cuyas conclusiones se plasmarán en actuaciones para tratar y mitigar el riesgo, acciones que deberán ser justificadas y ser proporcionales al riesgo a mitigar, pudiendo incluso replantear la seguridad de los sistemas en caso necesario.

Se contemplará la realización adicional de un análisis de riesgos de los sistemas de información cuando:

- Se modifique de manera importante la infraestructura del sistema de información.
- Se modifiquen los servicios prestados.
- Ocurran incidentes graves de seguridad.
- Se reporten vulnerabilidades graves que afecten a los sistemas de la información de la organización.

Las conclusiones de los análisis de riesgos serán revisadas por el Responsable de Seguridad y éste las comunicará al Comité de Seguridad y Riesgos de la Información.

Criterios de evaluación de riesgos

Para la armonización de los análisis de riesgos, Ineco ha establecido una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. Los criterios de evaluación de riesgos detallados se especificarán en la metodología de evaluación de riesgos desarrollada internamente.

Deberán tratarse, como mínimo, todos los riesgos que puedan impedir la prestación de los servicios o el cumplimiento de la misión de la organización de forma grave. Se priorizarán especialmente los riesgos que impliquen un cese en la prestación de servicios.

Directrices de tratamiento de riesgos

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

Proceso de aceptación del riesgo residual

Los riesgos residuales serán determinados por el Responsable de Seguridad.

Los niveles de riesgo residual esperados sobre cada Información tras la implementación de las opciones de tratamiento previstas deberán ser aceptados previamente por el responsable de esa información.

Los niveles de riesgo residuales esperados sobre cada servicio tras la implementación de las opciones de tratamiento previstas deberán ser aceptados previamente por el responsable de ese servicio.

Los niveles de riesgo residuales serán presentados por el Responsable de Seguridad al Comité de Seguridad y Riesgos de la Información, para que éste proceda, en su caso, a evaluar, aprobar o rectificar las opciones de tratamiento propuestas.

Gestión de incidentes de seguridad

Monitorización y detección de incidentes

En Ineco existen sistemas de monitorización para la detección, análisis y reporte de incidentes. Estos se recogen en el procedimiento interno de control de sistemas en operación.

Respuesta ante incidentes

Para garantizar la disponibilidad de los servicios y garantizar la protección de la información, Ineco dispone de un procedimiento de gestión de incidentes. Asimismo, se dispone de un plan de contingencia.

Los planes de continuidad de los sistemas TIC se desarrollan por el Responsable del Sistema.

Se dispone de procedimientos específicos actualizados periódicamente de reporte y resolución de incidencias.

Gestión del personal

Obligaciones del personal

Todos los miembros de Ineco tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información, siendo responsabilidad del Comité de Seguridad y Riesgos de la Información disponer los medios necesarios para que la información llegue a los afectados. Para ello, la presente política está disponible en la Intranet. Asimismo, se establecerá un programa de concienciación continua para atender a todos los miembros de Ineco, en particular, a los de nueva incorporación.

Terceras partes

Cuando se realicen servicios o se gestione información de algún usuario externo, se les hará partícipe de la Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad y Riesgos de la Información.

Cuando se presente información a usuarios externos, se les hará partícipes de la presente Política 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 garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en este documento.

Cuando algún aspecto recogido en el presente documento 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.

Se requerirá una persona de contacto (POC) para la comunicación directa con terceras partes.

Concienciación y formación

Los miembros de la organización atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez cada año y se establecerá un programa de concienciación continua para atender a los miembros de la organización, en particular a los 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 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.

Profesionalidad

La seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidencias y desmantelamiento.

Se hace necesario que, de manera objetiva y no discriminatoria, las organizaciones que presten servicios de seguridad a Ineco cuenten con unos niveles idóneos de gestión y madurez en los servicios prestados.

Autorización y control de los accesos

El acceso a los sistemas de información deberá ser controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas. Dicha responsabilidad recaerá sobre el Responsable de Seguridad.

Los responsables internos deberán velar, en el ámbito de sus servicios y competencias, por el cumplimiento de las instrucciones de coordinación, medidas y estrategias que determine el Responsable de Seguridad.

Para corregir, o exigir responsabilidades, cada usuario que acceda a la información del sistema debe identificarse de forma única, de modo que sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son y quién ha realizado determinada actividad.

Protección de las instalaciones

Los sistemas se instalarán en áreas separadas, dotadas de un procedimiento de control de acceso. Por ello, en primer lugar, se ha de establecer un perímetro físico de seguridad que proteja la información de la organización para prevenir incidencias, y garantizar el funcionamiento del resto de medidas.

El acceso a los locales, mediante vías de acceso autorizadas y controladas, barreras arquitectónicas como paredes o ventanas, elementos adicionales como áreas de descarga controladas, debe ser gestionado para proteger las zonas que contienen instalaciones informáticas o permiten el acceso a las mismas.

Dentro del perímetro de seguridad, se deben identificar las ubicaciones que almacenan soportes que puedan contener datos confidenciales o especialmente protegidos, estas ubicaciones dispondrán de una identificación personal de los usuarios que permita validar si disponen de autorización para su acceso.

Se deben validar las medidas de seguridad físicas de acceso al perímetro de seguridad, compuestas por puertas, cerraduras, alarmas, vigilancia y formalizarlas en instrucciones de acceso a los locales, que deberán ser comunicadas a todo el personal.

Los responsables internos deberán velar, en el ámbito de sus servicios y competencias, por el cumplimiento de las instrucciones de coordinación, medidas y estrategias que determine el Responsable de Seguridad Física.

Adquisición de productos de seguridad

En la adquisición de productos de seguridad de las TIC, así como, de seguridad física, que vayan a ser utilizados por Ineco, se valorarán positivamente aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, y se velará por que se contemple en los pliegos contractuales.

La certificación indicada deberá estar de acuerdo con las normas y estándares de mayor reconocimiento internacional, en el ámbito de la seguridad funcional.

Se establece que todos los productos de software y hardware destinados a la seguridad deben cumplir con los requisitos mínimos definidos por el ENS. Estos productos deben estar certificados conforme a estándares reconocidos por el Centro Criptológico Nacional a través de la guía del CCN-STIC 105 o por otras normativas de seguridad internacionalmente aceptadas.

Los componentes críticos deberán ser certificados, y el cumplimiento de medidas organizativas y técnicas como el cifrado, control de accesos y protección contra código dañino será verificado antes de su implementación.

Seguridad por defecto

Los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto:

- El sistema proporcionará la mínima funcionalidad requerida para que la organización sólo alcance sus objetivos y no alcance ninguna otra funcionalidad adicional.
- Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.
- En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.
- El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

Integridad y actualización del sistema

Todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema.

Se deberá conocer en todo momento el estado de seguridad de los sistemas, en relación con las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de estos.

Protección de la información almacenada y en tránsito

En la estructura y organización de la seguridad del sistema, se prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros. Tendrán la consideración de entornos inseguros los siguientes dispositivos: equipos portátiles, dispositivos periféricos, soportes de información (pendrive, disco duro) y comunicaciones sobre redes abiertas o con cifrado débil.

Forman parte de la seguridad los procedimientos que aseguren la recuperación y conservación a largo plazo de los documentos electrónicos producidos por Ineco en el ámbito de sus competencias.

Toda información en soporte no electrónico, que haya sido causa o consecuencia directa de la información electrónica, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello se aplicarán las medidas que correspondan a la naturaleza del soporte en que se encuentren, de conformidad con las normas de aplicación a la seguridad de estos.

Prevención ante otros sistemas de información interconectados

El sistema ha de proteger el perímetro, en particular, si se conecta a redes públicas. Se entenderá por red pública de comunicaciones la red de comunicaciones electrónicas que se utiliza, en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público. En todo caso se analizarán los riesgos derivados de la interconexión del sistema, o a través de redes, con otros sistemas, y se controlará su punto de unión.

Registro de actividad

Con la finalidad exclusiva de lograr el cumplimiento del objeto de la normativa aplicable, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Continuidad de la actividad

Los sistemas dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

Mejora continua del proceso de seguridad

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a gestión de las tecnologías de la información.

ESTRUCTURACIÓN DE LA DOCUMENTACIÓN

La normativa de seguridad de Ineco se estructura en 6 niveles:

1. Políticas: Documento que recoge las intenciones y la dirección de la organización, tal como las expresa formalmente la alta dirección.
2. Manuales: Documento que recoge las especificaciones de todo o de una parte del sistema de gestión de la organización.

3. Procesos: Documento que relaciona esquemáticamente un conjunto de actividades que utilizan las entradas para proporcionar un resultado previsto.
4. Procedimientos: Documento en el que se especifica quién, qué, dónde, cuándo y por qué se lleva a cabo un proceso o actividad. El cómo, dependiendo de cada caso, podrá estar especificado en el propio procedimiento o en una instrucción de trabajo. Un procedimiento puede describir todo o parte de un proceso de la organización.
5. Instrucciones de trabajo: Documento en el que se especifica cómo se lleva a cabo un proceso o una actividad concreta.
6. Formatos, registros, otros: Documentos que contienen la forma y el medio establecidos por la organización para registrar determinadas actividades o procesos, que presentan resultados obtenidos o proporcionan evidencias de actividades realizadas, que ofrecen información de soporte, etc.

La descripción completa de la estructuración de la documentación se encuentra en el documento interno establecido para tal efecto.

Calificación de la información

Se seguirá lo definido en el documento interno de calificación de la información, en el que se recogen los siguientes casos:

- TLP en la mensajería (como el correo electrónico y el chat)
- TLP en los documentos

Siendo un esquema creado para fomentar un mejor intercambio de información sensible en el ámbito de la seguridad de la información.

CAMBIO CLIMÁTICO

Ineco ha realizado el análisis de los servicios prestados por la organización, así como su operativa habitual para la prestación de los mismos no encontrando aspectos que puedan influir en el cambio climático del planeta. El análisis establece el cumplimiento de los requisitos legales establecidos.

Se han analizado los requisitos de las partes interesadas sin hallar ninguno específicamente relacionado con el cambio climático.

Ineco ha establecido acciones para reducir la huella respecto al cambio climático, siendo las principales la verificación del cálculo de su huella según la norma ISO 14064, la certificación en la norma ISO 14001 y el facilitar al empleado la posibilidad de compartición de vehículo para el desplazamiento a oficinas mediante aplicación.

En base a ambos análisis se concluye la no necesidad de aplicar medidas más allá de los requisitos legales estándar establecidos.

Ineco se compromete a difundir esta política poniéndola a disposición de todos los grupos de interés, promoviendo y asegurando su cumplimiento.

26 de Febrero de 2026

Comité de Dirección de Ineco