POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Establece el conjunto de directrices conforme a las que Enresa debe gestionar y proteger la información que trata y los servicios que presta, a través de un sistema de gestión de la seguridad de la información (en adelante, SGSI), en el marco legal vigente, en particular el Real Decreto 311/2022, de 3 de mayo, que regula el Esquema Nacional de Seguridad (en adelante, ENS). Esta Política se aplicará a todos los procesos de negocio, a las personas que los gestionan ya sean personal de Enresa o de sus empresas contratistas, y a todas las fases del ciclo de vida de la información: generación, recepción, tratamiento, transmisión, almacenamiento y destrucción, así como a los sistemas que las soportan, en lo que respecta a su análisis, diseño, desarrollo, implantación, explotación y mantenimiento.

Todas las actuaciones de Enresa deben tener como referencia la cultura de seguridad y calidad, así como la innovación en tecnología y en sistemas de gestión.

Principios básicos de actuación

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

1. **Seguridad como proceso integral.** La seguridad de la información es un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con los sistemas de información.
2. **Gestión de la seguridad basada en riesgos:** el análisis y la gestión de los riesgos es parte esencial del proceso de seguridad, debiendo constituir una actividad continua y actualizada. La reducción de estos se realizará mediante la aplicación de medidas proporcionales tanto a los potenciales riesgos como a la criticidad y al valor de la información y de los servicios afectados.
3. **Prevención, detección, respuesta y conservación:** la seguridad del sistema debe contemplar acciones relativas a la prevención, detección, respuesta, recuperación y conservación de la información, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta. Además, el sistema de información garantizará la conservación de los datos e información en soporte electrónico.
4. **Existencia de líneas de defensa:** los sistemas de información han de disponer de una estrategia de protección constituida por varias líneas de defensa, que podrá incluir medidas de naturaleza organizativa, física y técnica.
5. **Vigilancia continua y reevaluación periódica:** la vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la evolución tanto de los riesgos como de los sistemas de protección.

6. **Diferenciación de responsabilidades:** en el sistema de información se diferenciarán los roles del responsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema.

Acciones de mejora de la Seguridad de la Información

1. **Análisis y gestión de los riesgos.** El análisis y gestión de riesgos será parte esencial del proceso de seguridad con objeto de permitir 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 adecuadas a la naturaleza de la información y los tratamientos, que guarden un equilibrio entre los riesgos detectados y el coste para minimizarlos. La gestión de riesgos debe realizarse de manera continua sobre los sistemas de información y se someterá a reevaluación periódica. Para la realización de los análisis de riesgos se tendrán en cuenta las recomendaciones de las guías elaboradas por el Centro Criptológico Nacional.
2. **Gestión de personal.** Enresa desarrollará actividades específicas orientadas a la formación y concienciación de su personal en materia de seguridad de la información, así como a la difusión de la Política de Seguridad de la Información y su desarrollo, en particular entre el personal de nueva incorporación.
3. **Autorización, control de los accesos y mínimo privilegio.** El acceso a los sistemas y servicios de información de Enresa estará limitado a los usuarios, procesos, dispositivos u otros sistemas de información, debidamente autorizados y exclusivamente a las funciones autorizadas. Los sistemas de información se diseñarán y configurarán otorgando los mínimos privilegios necesarios para el correcto desempeño de las tareas de sus usuarios.
4. **Protección de las instalaciones.** Los sistemas de información de Enresa y su infraestructura de comunicaciones asociadas deberán permanecer en áreas controladas y disponer de los mecanismos de acceso adecuados en función del análisis de riesgos.
5. **Adquisición de productos de seguridad y servicios de seguridad.** La adquisición de productos de seguridad y la contratación de servicios de seguridad de las tecnologías de la información y la comunicación que vayan a ser empleados en los sistemas de información de Enresa, se realizarán de forma proporcionada a la categoría del sistema y los niveles de seguridad determinados, certificando siempre que sea posible la funcionalidad de seguridad a través del Catálogo de Productos y Servicios STIC (CPSTIC) del Centro Criptológico Nacional.
6. **Integridad y actualización del sistema.** La inclusión de cualquier elemento físico o lógico en el inventario de activos del sistema de información de Enresa o su modificación, requerirá autorización formal conforme el procedimiento de autorización establecido.
7. **Protección de información almacenada y en tránsito.** Se prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros, mediante la inclusión de medidas de protección adecuadas y proporcionales. Son entornos inseguros los equipos portátiles, dispositivos móviles, dispositivos

periféricos, soportes de información removibles y comunicaciones sobre redes abiertas o con cifrado débil.

8. **Prevención ante otros sistemas de información interconectados.** Se protegerá el perímetro de los sistemas de información de Enresa, especialmente, si se conectan a redes públicas, constituyéndose una arquitectura de protección perimetral, utilizando para ellos dispositivos que permitan proteger los flujos de información.
9. **Registros de actividad y detección de código dañino.** Enresa podrá disponer de herramientas para registrar las actividades de los usuarios en las redes y sistemas de información, 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. Estos datos no permiten realizar el perfilado de usuarios. Para reforzar la seguridad de los sistemas de información, se analizarán las comunicaciones entrantes o salientes de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio y evitar la distribución malintencionada de código dañino.
10. **Incidencias de seguridad.** Enresa dispondrá de un procedimiento de gestión de incidentes de seguridad que describa el protocolo a seguir para la comunicación y el registro de actuaciones a realizar.
11. **Continuidad de la actividad.** Los sistemas de información de Enresa dispondrán de copias de seguridad y se establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales. Se elaborarán e implantarán planes de contingencia para asegurar que los procesos de negocio pueden restablecerse en el tiempo requerido.
12. **Mejora continua.** El proceso de seguridad de los sistemas de Enresa, deberá ser actualizado y mejorado de forma continua, aplicándose las mejores prácticas y estándares reconocidos de mercado.

Esta Política de Seguridad deberá mantenerse actualizada permanentemente para adecuarla al progreso de los servicios de Enresa, a la evolución tecnológica y al desarrollo de la sociedad de la información, así como a los estándares nacionales e internacionales de seguridad.

Esta política fue aprobada por el Consejo de Administración de Enresa en su sesión del 26 de junio de 2023