POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN ESQUEMA NACIONAL DE SEGURIDAD

1. OBJETO

El presente documento responde a la necesidad de ENWESA de cumplir con los requisitos expresados en la legislación de seguridad de la información en servicios por medios electrónicos: el Real decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad – ENS, así como con la normativa y principios de seguridad de la información aplicadas en la compañía, para que repercuta, en última instancia, en la mejora de la seguridad de los servicios que la compañía ofrece a sus clientes y en la mejora de los propios procese internos de la organización.

La empresa se compromete a cumplir con el Artículo 1 del Esquema Nacional de Seguridad, establecida en el artículo 39 RD 311/2022, de 3 de mayo del ENS, desarrollando una política de seguridad que se ha de aplicar en la utilización de los medios electrónicos a los que se refiere la citada ley, y entiende que el Esquema Nacional de Seguridad está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información. Será aplicado para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.

Siguiendo las recomendaciones de la GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-801), y en función de nuestro alcance, los comités del Sistema ENS y el de seguridad y servicios se podrán realizar en un mismo acto.

A su vez la empresa también se compromete al cumplimiento de las Norma UNE-EN ISO/IEC 27001:2023, utilizando la estructura de gestión de la norma (políticas, procedimientos, análisis de riesgos, auditorías internas, revisión por la dirección, mejora continua) para organizar y gobernar las medidas exigidas por el Esquema Nacional de Seguridad mediante la implantación de un Sistema de Gestión de Seguridad de la Información.

Esta Política de Seguridad de la Información es efectiva desde la fecha de su aprobación y hasta que sea reemplazada por una nueva Política.

2. ALCANCE

Esta política se aplica sobre el personal y los sistemas TIC (infraestructuras, software, comunicaciones…) que dan soporte a los servicios dentro del ámbito de aplicación del Esquema Nacional de Seguridad en ENWESA.

Asimismo, dicha Política de Seguridad de la Información está alineada con la Política Corporativa de Seguridad de la Información y las directrices marcadas por la Normativa Corporativa de Seguridad de la Información del Grupo ENSA en su última versión.

3. DEFINICIONES

Información: Todo documento que puede ser comunicado, presentado o almacenado en cualquier forma.

Análisis de riesgos: Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.

Datos personales: Cualquier información concerniente a personas físicas identificadas o identificables.

Gestión de incidentes: Plan de acción para atender las incidencias que se den. Además de resolverlas debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización en lo que respecta a los riesgos.

Incidente de seguridad: Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información.

Política de seguridad: Conjunto de directrices, que rigen la forma en que una organización gestiona y protege la información y los servicios que considera críticos.

Principios básicos de seguridad: Fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.

Responsable de la información: Persona que tiene la potestad de establecer los requisitos de una información en materia de seguridad.

Responsable de la seguridad: El responsable de seguridad debe determinar las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Responsable del servicio: Persona que tiene la potestad de establecer los requisitos de un servicio en materia de seguridad.

Responsable del sistema: Persona que se encarga de la explotación del sistema de información.

Servicio: Función o prestación ejercida por alguna entidad oficial destinado a cuidar intereses o satisfacer necesidades de los ciudadanos.

Sistema de información: Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, utilizar, compartir, distribuir, poner a disposición, presentar o transmitir.

4. MARCO NORMATIVO

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

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas
- RD 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad.
- La Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantías de los Derechos Digitales (LOPDGDD).
- El 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 (RGPD).

- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, relativo a la regulación de las telecomunicaciones.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.
- Ley 59/2003, de 19 de diciembre, de firma electrónica. Tiene como objetivo fomentar la rápida incorporación de las nuevas tecnologías de seguridad de las comunicaciones electrónicas en la actividad de las empresas, los ciudadanos y las Administraciones públicas.

5. MISIÓN

En base a lo establecido en la Guía de Seguridad de las TIC CCN-STIC 805 se describen a continuación los objetivos de servicio de ENWESA (funciones que desarrolla, servicios que presta) en materia de seguridad que la pretende garantizar con la presente Política y que son:

- Garantizar la confidencialidad, integridad, autenticidad de la información y la continuidad en la prestación de los servicios.
- Implementar medidas de seguridad en función del riesgo.
- Formar y concienciar a los integrantes de la respecto a la seguridad de la información. Implementar medidas de seguridad que permitan la trazabilidad de los accesos y respetar, entre otros, el principio de mínimo privilegio, reforzando también el deber de confidencialidad de las personas usuarias en relación con la información que conocen en el desempeño de sus funciones.
- Desplegar y controlar la seguridad física haciendo que los activos de información se encuentren en áreas seguras, protegidos por controles de acceso, atendiendo a los riesgos detectados.
- Establecer la seguridad en la gestión de comunicaciones mediante los procedimientos necesarios, logrando que la información que sea transmita a través de redes de comunicaciones sea adecuadamente protegida.
- Controlar la adquisición, desarrollo y mantenimiento de los sistemas de información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.
- Controlar el cumplimiento de las medidas de seguridad en la prestación de los servicios, manteniendo el control en la adquisición e incorporación de nuevos componentes del sistema.
- Gestionar los incidentes de seguridad para la correcta detección, contención, mitigación y resolución de estos, adoptando las medidas necesarias para que los mismos no vuelvan a reproducirse.
- Proteger la información personal, adoptando las medidas técnicas y organizativas en atención a los riesgos derivados del tratamiento conforme a la legislación en materia de protección de datos.
- Supervisar de forma continuada el sistema de gestión de la seguridad, mejorando y corrigiendo las ineficiencias detectadas.

6. LOS PRINCIPIOS BÁSICOS DE ESTA POLÍTICA

Los principios que deben contemplarse a la hora de garantizar la seguridad de la información son los marcados en el artículo 5 del RD 311/2022, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, de manera que las amenazas existentes no se

materialicen o en caso de materializarse no afecten gravemente a la información que maneja, o los servicios que se prestan.

1. Seguridad integral. La seguridad de la información en la organización es integral.
2. Gestión de riesgos. Gestión de la seguridad está basada en riesgos.
3. Prevención, reacción y recuperación.
4. Existencia de líneas de defensa.
5. Vigilancia continua
6. La reevaluación periódica.
7. Diferenciación de responsabilidades: Se diferencian a los diferentes responsables de gestión del sistema y de la seguridad del mismo, especialmente entre el responsable del sistema y el responsable de la seguridad.

OTROS PRINCIPIOS GENERALES

- El análisis y gestión de riesgos es parte esencial del proceso de seguridad y se mantiene permanentemente actualizado.
- La información es protegida contra accesos y alteraciones no autorizadas, manteniéndola confidencial e íntegra.
- La información está disponible, y se permite su acceso autorizado, siempre que es necesario.
- La Seguridad de la Información es responsabilidad de todos. Todas las personas que tiene acceso a la información de la Organización deben protegerla, por lo que están adecuadamente formadas y concienciadas.
- La Seguridad de la Información no es algo estático, está constantemente controlada y periódicamente revisada. Las medidas de seguridad se reevaluarán y revisarán periódicamente una vez al año.
- Todos aquellos activos (infraestructura, soportes, sistemas, comunicaciones, etc.) donde reside la información, es transportada o es procesada, están adecuadamente protegidos.
- Las medidas de seguridad que se implanten deben estar en proporción a la criticidad de la información que protejan y a los daños o pérdidas que se pueden producir en ella. En todo momento se seguirá como mínimo las medidas de seguridad impuestas por el Esquema Nacional de Seguridad, las guías CCN-STIC elaboradas por el Centro Criptológico Nacional del Centro Nacional de Inteligencia.
- El tratamiento de datos de carácter personal debe estar siempre de acuerdo con las leyes aplicables en cada momento, siendo especialmente importantes la Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 y la Ley Orgánica 3/2018 de Protección de Datos de Carácter Personal y Garantía de Derechos Digitales.

7. ORGANIZACIÓN DE LA SEGURIDAD

Enwesa dispone de un Comité de Seguridad y Servicios para la gestión del Sistema y velar por el correcto cumplimiento de las políticas y normas implantadas en la organización.

Para asegurar la incompatibilidad de roles se han definido estos asignándolos a distintas personas en la organización, según las actas del comité de seguridad.

El comité lo forman:

Responsable de Servicios: Director General.

Responsable de Información: Director General.

Responsable de Seguridad: Controlador de Costes.

Responsable del Sistema: Responsable de Sistemas.

Administrador del Sistema: Administrador de Sistemas.

La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios. A esto se le llama, función diferenciada.

Para la designación de estos puestos Enwesa dispone de un procedimiento de designación y renovación de los roles o funciones de seguridad (IT de Designación y Renovación del Comité de Seguridad), en el que se establece que en el caso en que una persona del comité o responsables deba o quiera ser sustituida, abandone la empresa, o por cualquier otro motivo haya que añadir a alguna persona, los miembros restantes propondrán sustitutos dentro de la organización.

El comité elegirá la nueva composición en el plazo máximo de tres meses.

FUNCIONES DEL COMITÉ

Las funciones del comité serán las siguientes:

- Atender las inquietudes de la Dirección de la entidad y de los diferentes departamentos.
- Informar regularmente del estado de la seguridad de la información a la Dirección.
- Promover la mejora continua del sistema de gestión de la seguridad de la información
- 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.
- Elaborar (y revisar regularmente) la Política de Seguridad de la Información para su aprobación por la Dirección.
- Aprobar la Normativa de Seguridad de la Información.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios, desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la organización y recomendar posibles actuaciones.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de tales incidentes.
- 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 TIC desde su especificación inicial hasta su puesta en operación. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir

El responsable de la información: El responsable de la Información es el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad. El responsable de la información determinará los requisitos de confidencialidad, integridad, trazabilidad, disponibilidad y autenticidad de la información tratada.

Será la persona responsable de definir y firmar la política y la categorización del sistema.

Sus responsabilidades son:

- Determina los requisitos (de seguridad) de la información tratada, según los parámetros del Anexo I del ENS.
- La aprobación de los niveles de seguridad de la información
- La valoración de las consecuencias de un impacto negativo sobre la seguridad de la información.

El responsable del servicio: tiene la potestad de establecer los requisitos del servicio en materia de seguridad, y/o la potestad de determinar los niveles de seguridad de los servicios. El responsable del servicio determinará los requisitos de los servicios prestados.

- Será la persona responsable de definir y firmar la categorización del sistema.
- Determina los requisitos (de seguridad) de los servicios prestados, según los parámetros del Anexo I del ENS.
- Debe incluir las especificaciones de seguridad en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.
- Debe valorar las consecuencias de un impacto negativo sobre la seguridad de los servicios según la 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, el respeto de la legalidad y los derechos de los ciudadanos

Responsable de Seguridad de la Información:

Determina las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los responsables de la información y de los servicios. Será profesional cualificado y con niveles idóneos de gestión y madurez en los servicios prestados.

Será la persona responsable de firmar, para formalizar la Declaración de Aplicabilidad.

La persona responsable de la Seguridad (del ENS) será secretaria del Comité de Seguridad de la Información, y como tal:

- Convocará las reuniones del Comité de Seguridad de la Información.
- Preparará los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elaborará el acta de las reuniones.
- Será responsable de la ejecución directa o delegada de las decisiones del Comité

El responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios. La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios. La política de seguridad de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos.

El responsable del Sistema:

- Se encarga de la operación del sistema de información, atendiendo a las medidas de seguridad determinadas por el responsable de la Seguridad.
- En el caso de los sistemas de categoría ALTA, visto el dictamen de auditoría, el responsable del sistema podrá acordar la retirada de operación de alguna información, de algún servicio o del sistema en su totalidad, durante el tiempo que estime prudente y hasta la satisfacción de las modificaciones prescritas.

Con respecto a los informes de autoevaluación y/o los informes de auditoría, estos serán analizados por el responsable de la Seguridad competente, que elevará las conclusiones al Responsable del Sistema para que adopte las medidas correctoras adecuadas.

La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios.

- 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.

Administrador del sistema de seguridad de la información:

Tiene las siguientes responsabilidades:

- Monitorización del estado de seguridad del sistema, analizando la información proporcionada por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica instalados en el sistema
- Supervisión de que todo el equipamiento se ajusta a lo autorizado
- Supervisión de las actividades de los administradores del sistema: actuaciones y aplicación de los procedimientos de seguridad establecidos
- Supervisión de que las actividades de los usuarios del sistema están conformes a lo que cada uno está autorizado
- Cuando existe un sistema separado de gestión de privilegios, el ASS puede encargarse de las actuaciones relativas a la implantación y mantenimiento de las autorizaciones concedidas a los usuarios del sistema

8. GESTIÓN DE INCIDENTES DE SEGURIDAD

PREVENCION DE INCIDENTES

Se deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. El ENS a través de su artículo 19 establece la que los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto. De igual forma, el artículo 25 del citado ENS define que los sistemas de instalarán en áreas separadas, dotadas de un procedimiento de control de acceso.

Para ello se debe implementar 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.

Para garantizar el cumplimiento de la política se debe:

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

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 deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS. La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales. Los sistemas de detección de intrusos cumplen fundamentalmente con una labor de supervisión y auditoría sobre los recursos de la organización, verificando que la política de seguridad no es violada e intentando identificar cualquier tipo de actividad maliciosa de una forma temprana y eficaz. Se deberán establecer, en función de las necesidades, las siguientes clasificaciones:

- Sistemas de detección de intrusos a nivel de red.
- Sistemas de detección de intrusos a nivel sistema. Por su parte, el Reglamento General de Protección de Datos en sus artículos 33 y 34, respectivamente, obliga a notificar las violaciones de seguridad de datos personales a la Agencia Española de Protección de Datos cuando existe riesgo para los interesados y a los propios interesados cuando la violación suponga un alto riesgo para ellos. Por ello se deberán establecer controles internos para identificar y catalogar este tipo de incidencias relacionadas con datos personales y comunicarlas al Responsable de Seguridad.

Respuesta ante incidentes

Se debe:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Este apartado incluye las comunicaciones.

DATOS DE CARÁCTER PERSONAL

Para la prestación de los servicios previstos deben ser tratados datos de carácter personal. Enwesa dispone de un análisis de riesgos de seguridad con controles y medidas que reducen o eliminan los riesgos detectados y para determinados tratamientos de alto riesgo, se ha elaborado una Evaluación de impacto en protección de datos, que, entre otros aspectos, identifica los riesgos en materia de seguridad y recoge medidas y controles para que el riesgo residual sea aceptable.

FORMACIÓN Y CONCIENCIACIÓN

Las acciones específicas de concienciación y formación relativas al ENS se gestionan, sin distinción con las del Sistema de Gestión de Seguridad de la Información, por el departamento de desarrollo de RRHH. Dentro del marco del Sistema de gestión, desarrolla su metodología en el procedimiento PG-CF Competencia, formación y toma de conciencia.

COORDINACIÓN Y RESOLUCIÓN DE CONFLICTOS:

Coordinación, nombramiento y resolución de conflictos La coordinación se lleva a cabo en el seno del Comité de Dirección que podrá delegar en el Comité del SGI. Los nombramientos los establece la Dirección de la organización y se revisan cuando un puesto queda vacante. Las

diferencias de criterios que pudiesen derivar en un conflicto se tratarán en el seno del Comité del SGI y prevalecerá en todo caso el criterio de la Dirección ejecutiva.

9. TERCERAS PARTES

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 de la Información 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 quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de 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 y deberán formalizar su relación como encargados de tratamientos.

10. DOCUMENTACIÓN DE SEGURIDAD

La documentación relativa a la Seguridad de la Información estará clasificada en tres niveles, de manera que cada documento de un nivel se fundamenta en los de nivel superior:

- Primer nivel: Política de seguridad de la Información
- Segundo nivel: Normativas y procedimientos de seguridad.
- Tercer nivel: Informes, registros y evidencias electrónicas.

Primer nivel: Política de seguridad Documento de obligado cumplimiento por todo el personal, interno y externo, de la Organización, recogido en el presente documento.

Segundo nivel: Normativas y procedimientos de seguridad De obligado cumplimiento de acuerdo con el ámbito organizativo, técnico o legal correspondiente, desarrollados por Enwesa en el marco de su Sistema de Gestión en los que se han incluido los aspectos específicos del ENS para cumplir con los requisitos mínimos de seguridad que marca su artículo 12, tal y como indica la guía CCN-STIC 825 ENS, apartado 5.2. CUADRO RESUMEN. Para facilitar la trazabilidad entre las medidas de seguridad requeridas por el ENS y su implantación en Enwesa en el marco del SGSI, en la Declaración de Aplicabilidad del ENS se ha procedido a mapear las medidas de seguridad aplicables del Anexo II con los controles del Anexo A de ISO 27001. Realizado de acuerdo con la guía CCN-STIC 825 ENS – ESQUEMA NACIONAL DE SEGURIDAD CERTIFICATIONES 27001. La responsabilidad de aprobación de los documentos redactados en este nivel será competencia del Comité del SGI.

Tercer nivel: Informes, registros y evidencias electrónicas Documentos de carácter técnico que recogen evidencias generadas durante todas las fases del ciclo de vida del sistema de información, así como amenazas y vulnerabilidades de los sistemas de información.

Otra documentación: Se podrá seguir en todo momento los procedimientos, normas e instrucciones técnicas STIC, así como las guías CCN-STIC que publique el Centro Criptológico Nacional (CCN).

Según el artículo 11, la organización deberá disponer formalmente de una política de seguridad que articule la gestión continuada de la seguridad, que será aprobada por el titular del órgano superior correspondiente. Esta política de seguridad se establecerá de acuerdo con los principios básicos indicados y se desarrollará aplicando los siguientes requisitos mínimos:

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

En Enwesa se etiqueta la información almacenada, a través de calificación por permisos a los usuarios en el gestor documental. Además, la información se etiqueta a nivel de metadatos

Las personas tienen acceso según su calificación dentro de la organización.

DOCUMENTACIÓN

La información asociada a la seguridad y ENS se organiza, codifica y aprueba de acuerdo con los requisitos generales del Sistema de Gestión que se recogen en el procedimiento interno de Gestión de la Documentación

REVISIÓN Y APROBACIÓN DE LA POLÍTICA DE SEGURIDAD

La Política de Seguridad de la Información será revisada por el Comité de Seguridad de la Información y la Privacidad a intervalos planificados, que no podrán exceder el año de duración o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia. Los cambios sobre la Política de Seguridad de la Información deberán ser aprobados por el órgano superior competente que corresponda, de acuerdo con el artículo 12 del ENS. Cualquier cambio sobre la misma deberá ser difundido a todas las partes afectadas.

11. HISTÓRICO DE REVISIONES

Revisión	Fecha	Motivo
00	26/06/2024	Edición inicial
01	24/09/2024	Actualización Director General
02	19/11/2025	Inclusión apartado 5.- Misión

72133040A CARLOS ITURREGUI (R: A81619066)

Firmado digitalmente por: 72133040A CARLOS ITURREGUI (R: A81619066)
ND: CN = 72133040A CARLOS ITURREGUI (R: A81619066) C = ES O = ENWESA OPERACIONES SA S.M.E.
Fecha: 2025.11.19 13:37:07 +01'00'

19 de Noviembre de 2025

D. Carlos Iturregui Obregón
Director General