

ÍNDICE

1.	INTRODUCCIÓN	3
1.1.	Prevenición	3
1.2.	Detección	4
1.3.	Respuesta	4
1.4.	Recuperación	4
2.	OBJETIVOS	4
3.	ALCANCE	5
4.	MISIÓN	5
5.	MARCO NORMATIVO	5
5.1.	Normativa europea.....	5
5.2.	Normativa estatal	6
5.3.	Estándares internacionales.....	6
6.	POLÍTICA DE GESTIÓN.....	6
7.	LIDERAZGO Y COMPROMISO.....	7
8.	ORGANIZACIÓN DE LA SEGURIDAD.....	8
8.1.	Órganos	8
8.1.1.	Comité de Calidad y Seguridad	8
8.2.	Roles	8
8.2.1.	Responsable de Seguridad (Esquema Nacional de Seguridad).....	9
8.2.2.	Responsable de la Información (Esquema Nacional de Seguridad).....	10
8.2.3.	Responsable del Sistema (Esquema Nacional de Seguridad)	10
8.2.4.	Responsable del Servicio (Esquema Nacional de Seguridad).....	11
8.2.5.	Responsable del SGSI.....	11
8.3.	Procedimiento de Designación y Renovación.....	12
8.4.	Resolución de conflictos	12
8.5.	Política de seguridad integral.....	13
9.	FORMACIÓN Y CONCIENCIACIÓN	13
10.	DATOS DE CARÁCTER PERSONAL	13
11.	GESTIÓN DE RIESGOS.....	14
12.	DESARROLLO DE LA POLÍTICA DE SEGURIDAD INTEGRAL	15
13.	OBLIGACIONES DEL PERSONAL	15
14.	TERCERAS PARTES	15
15.	CONTROL DE ACCESO	16

16.	PROTECCIÓN DE LAS INSTALACIONES.....	16
17.	ADQUISICIÓN DE PRODUCTOS	16
18.	SEGURIDAD POR DEFECTO	16
19.	INTEGRIDAD Y ACTUALIZACIÓN DEL SISTEMA	17
20.	PROTECCIÓN DE LA INFORMACIÓN ALMACENADA Y EN TRÁNSITO	17
21.	PREVENCIÓN ANTE OTROS SISTEMAS DE INFORMACIÓN INTERCONECTADOS.....	18
22.	PROCESO DE AUTORIZACIONES	18
23.	REGISTRO DE ACTIVIDAD	19
24.	INCIDENTES DE SEGURIDAD	19
25.	CONTINUIDAD DE LA ACTIVIDAD.....	20
26.	MEJORA CONTINUA DEL PROCESO DE SEGURIDAD	20
27.	ESTRUCTURACIÓN DE LA DOCUMENTACIÓN DE SEGURIDAD DEL SISTEMA	20
28.	APROBACIÓN Y ENTRADA EN VIGOR.....	20
29.	PROCEDIMIENTO DE REVISIÓN.....	20

Rev.	Fecha	Modificaciones efectuadas
1	19.09.24	Primera elaboración.

1. INTRODUCCIÓN

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

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

Los sistemas TIC están protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso imprevisto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto se logra aplicando las medidas de seguridad exigidas por el R.D. 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad y sus guías de desarrollo CCN-STIC, así como otros estándares de carácter internacional (ISO 27001) y demás normativa aplicable, además de realizando un seguimiento continuo de los niveles de prestación de servicios, siguiendo y analizando las vulnerabilidades reportadas, y preparando una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Ecna se cerciora de que la seguridad TIC es una parte íntegra 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 son identificados e incluidos en la planificación, en la solicitud de ofertas y en los contratos para proyectos TIC.

Ecna está preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al art. 8 del ENS, y al Anexo A de la ISO 27001.

1.1. Prevención

Ecna vela activamente por 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 la organización implementa las medidas de seguridad determinadas por el ENS y la ISO 27001, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal están claramente definidos y documentados.

Para garantizar el cumplimiento de la política, **Ecna** lleva a cabo las siguientes acciones:

- ▶ 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.

1.2. Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, se monitoriza 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 art. 9 del ENS y Anexo A de la ISO 27001.

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

1.3. Respuesta

Ecna lleva a cabo las siguientes medidas:

- ▶ Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- ▶ Designar un punto de contacto (POC) para las comunicaciones con respecto a incidentes detectados.
- ▶ Establecer protocolos para el intercambio de información relacionada con el incidente.

1.4. Recuperación

Para garantizar la disponibilidad de los servicios críticos, **Ecna** desarrolla planes de continuidad de los sistemas TIC como parte de su plan general de continuidad del negocio y actividades de recuperación.

2. OBJETIVOS

Ecna ha establecido un marco de gestión de la seguridad de la información según lo establecido por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS), reconociendo así como activos estratégicos la información y los sistemas que la soportan.

Uno de los objetivos fundamentales de la implantación de este marco de referencia es el asentar las bases sobre las cuales los trabajadores de **Ecna** y sus clientes puedan acceder a los servicios en un entorno de gestión seguro, anticipándonos a sus necesidades, y preservando sus derechos.

La **POLÍTICA DE SEGURIDAD INTEGRAL** es el instrumento en que se apoyan los recursos de **Ecna** para alcanzar sus objetivos utilizando de forma segura los sistemas de información y las comunicaciones.

La **POLÍTICA DE SEGURIDAD INTEGRAL** identifica responsabilidades y establece principios y directrices para una protección apropiada y consistente de los servicios y activos de información gestionados por medio de las Tecnologías de la Información y de

las Comunicaciones (TIC).

El objetivo es lograr una protección, proporcional al riesgo, de la información tratada por **Ecna**, y de los sistemas, dispositivos y elementos que soportan los servicios y procesos de tratamiento, mediante la preservación de las dimensiones de seguridad de la información, es decir, su autenticidad, confidencialidad, integridad, disponibilidad, trazabilidad y conservación.

3. ALCANCE

Esta Política será de aplicación y de obligado cumplimiento para todos los empleados de **Ecna**; así como a sus recursos y procesos afectados por el ENS y la ISO 27001, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

4. MISIÓN

Ecna da servicio a sus clientes asegurando la efectividad de sus derechos y la continua mejora de los procedimientos, servicios y prestaciones de acuerdo con las políticas fijadas por la organización. Asimismo, en **Ecna** se tienen en cuenta los recursos disponibles, determinando de esta manera las prestaciones que proporcionan los servicios ofrecidos, sus contenidos y los correspondientes estándares de calidad.

Ecna se organiza y actúa con pleno respeto al principio de legalidad y de acuerdo con los principios de jerarquía, descentralización funcional, coordinación, eficacia en el cumplimiento de los objetivos fijados, eficiencia en la asignación y utilización de los recursos disponibles, transparencia, responsabilidad por la gestión y servicio efectivo a sus clientes.

La organización viene a ejercer sus competencias propias bajo su propia responsabilidad, debiendo atender siempre a la más eficaz coordinación con sus clientes. Para ejercer sus competencias, **Ecna** hace uso de sistemas de información que son protegidos de una forma efectiva y eficiente.

5. MARCO NORMATIVO

5.1. Normativa europea

- ▶ Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).
- ▶ 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 (Reglamento general de protección de datos).

5.2. Normativa estatal

- ▶ Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- ▶ Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- ▶ Ley 11/2022, de 28 de junio, General de Telecomunicaciones.
- ▶ Ley 5/2014, de 4 de abril, de Seguridad Privada.
- ▶ Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- ▶ Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.
- ▶ Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.
- ▶ 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.
- ▶ Real Decreto 951/2015, de 23 de octubre, de modificación del 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.
- ▶ Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil.

5.3. Estándares internacionales

- ▶ ISO/IEC 27000 – Tecnologías de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Visión de conjunto y vocabulario.
- ▶ ISO/IEC 27001– Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos.
- ▶ ISO/IEC 27002:2022 – Seguridad de la información, ciberseguridad y protección de la privacidad. Control de la seguridad de la información

6. POLÍTICA DE GESTIÓN

La Dirección de **Ecna** acuerda que el desarrollo de las actividades de la compañía y la consecución de los objetivos estratégicos requiere garantizar, en todo momento, el cumplimiento de los niveles establecidos de **confidencialidad, disponibilidad, integridad, autenticación y trazabilidad** para sus activos de información. Al mismo tiempo, requiere demostrar también su capacidad para proporcionar las soluciones y servicios propios de forma coherente, así como para gestionar eficientemente los servicios de seguridad de la información y ciberseguridad que ofrece a sus clientes.

Con esta finalidad, se ha desarrollado e implantado el SG que establece el marco de referencia para tratar de forma segura los activos de la compañía, y que garantiza la

confianza y satisfacción de los clientes mediante la integración de una metodología de prestación de servicios eficiente.

El compromiso de **Ecna** en cuanto a la gestión de la seguridad de la información es el siguiente:

- ▶ Hacer patente el **compromiso de la Dirección** con el SG, con la gestión de la seguridad de la información, tanto propia como la de sus clientes, reflejado en la firma y difusión de la presente política.
- ▶ Garantizar que se integran los requisitos del SG en los procesos de negocio de la compañía.
- ▶ Asegurar que se establecen los **objetivos** de la seguridad de la información, y que éstos son compatibles con el contexto y la dirección estratégica de la compañía.
- ▶ Definir, desarrollar y poner en funcionamiento los controles necesarios promoviendo el uso del enfoque a procesos y el **pensamiento basado en riesgos** para garantizar el cumplimiento, en todo momento, de los niveles de riesgo aprobados por la compañía.
- ▶ **Cumplir** en todo momento la **legislación** vigente, además de las normas y especificaciones particulares aplicables a los servicios prestados por la compañía y orientadas a la satisfacción del cliente.
- ▶ Crear una **cultura de gestión integrada** de los sistemas de información, tanto internamente, a todo el personal, como externamente a los clientes y proveedores.
- ▶ **Comprometer, dirigir y apoyar al personal** con el fin de contribuir a la eficacia del SG, **asegurar la disponibilidad de los recursos** necesarios para el mismo, así como **apoyar a otros roles** pertinentes de la dirección en la forma en la que aplique el sistema de gestión en sus áreas de responsabilidad.
- ▶ Tratar la gestión de la seguridad de la información como un proceso de **mejora continua**.
- ▶ Mantener la **confianza y satisfacción de los clientes**.
- ▶ Garantizar la **resiliencia** de la organización y sus sistemas de información **frente al cambio climático o desastres naturales**.

7. LIDERAZGO Y COMPROMISO

La dirección de **Ecna** demuestra su liderazgo y compromiso respecto al Sistema de Gestión (SG):

- ▶ Garantizando que la **POLÍTICA DE SEGURIDAD INTEGRAL** y **NORMATIVA DE SEGURIDAD** de **Ecna**, así como los objetivos de ésta se han establecido y son compatibles con la dirección estratégica de la compañía;
- ▶ Velando por que los recursos necesarios para el SG estén disponibles;
- ▶ Comunicando la importancia de una gestión eficaz del sistema y de satisfacer

los requisitos del sistema;

- ▶ Asegurando que el SG alcanza sus resultados previstos;
- ▶ Dirigiendo y apoyando a las personas a contribuir a la eficacia del SG;
- ▶ Promoviendo la mejora continua; y
- ▶ Apoyando otras funciones de gestión pertinentes para demostrar su liderazgo aplicable a sus áreas de responsabilidad.

8. ORGANIZACIÓN DE LA SEGURIDAD

La organización de la seguridad de **Ecna** queda establecida mediante la identificación y definición de las diferentes actividades y responsabilidades en la materia, y la implantación de la infraestructura que las soporte.

Con carácter general, todos y cada uno de los usuarios de los sistemas de información de **Ecna** son responsables de la seguridad de los activos de información mediante un uso adecuado de los mismos, siempre de acuerdo con sus atribuciones profesionales y académicas.

El documento **ORGANIZACIÓN DE LA SEGURIDAD** describe las funciones y responsabilidades de los roles implantados en **Ecna**.

8.1. Órganos

8.1.1. Comité de Calidad y Seguridad

El Comité de Calidad y Seguridad tiene como finalidad asumir la responsabilidad y la autoridad de tratar los temas concernientes al negocio, así como velar por la seguridad de la servicios y activos de información en **Ecna**, asegurando y facilitando la correcta coordinación e integración de todas las actuaciones en esta materia.

La estructura del Comité, así como los miembros que lo constituyen y la relación con otros elementos de la organización, está reflejada en la correspondiente acta.

La responsabilidad del Comité de Calidad y Seguridad está descrita en el documento **ORGANIZACIÓN DE LA SEGURIDAD**.

Los integrantes del Comité de Calidad y Seguridad son:

- ▶ Responsable del Servicio
- ▶ Responsable de la Información
- ▶ Responsable de Seguridad
- ▶ Responsable del Sistema
- ▶ Responsable del SGSI

8.2. Roles

Este apartado tiene por objetivo establecer los roles y responsabilidades relativas al

Sistema de Gestión (SG) implantado en **Ecna**.

8.2.1. Responsable de Seguridad (Esquema Nacional de Seguridad)

El ENS señala que el Responsable de la Seguridad determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Las dos funciones esenciales del Responsable de la Seguridad son:

- ▶ Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo con lo establecido en la **POLÍTICA DE SEGURIDAD INTEGRAL** de la organización.
- ▶ Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.

Además de ello, de acuerdo con el ENS y las guías CCN-STIC aplicables, tendrá las siguientes funciones:

- ▶ Elaborar las políticas de seguridad, en colaboración con el RSGSI.
- ▶ Desarrollar las políticas de seguridad, normativas y procedimientos derivados, y supervisar su efectividad, en colaboración con el RSGSI.
- ▶ Elaborar y aprobar el documento de Declaración de Aplicabilidad del Anexo II del R.D. 311/2022.
- ▶ Garantizar el cumplimiento normativo y evaluar los incumplimientos, en colaboración con el RSGSI.
- ▶ Decidir las medidas de seguridad que se aplican en la organización, en colaboración con el RSGSI.
- ▶ Realizar o promover auditorías periódicas para garantizar la correcta aplicación de las medidas de seguridad, en colaboración con el RSGSI.
- ▶ Determinar la metodología y herramientas para la evaluación de riesgos, en colaboración con el RSGSI.
- ▶ Elaborar la evaluación de riesgos y el plan de tratamiento resultante, así como aceptar el último, en colaboración con el RSGSI.
- ▶ Actuar como capacitador de buenas prácticas, en colaboración con el RSGSI.
- ▶ Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución, en colaboración con el RSGSI.
- ▶ Constituirse como punto de contacto con la autoridad competente.
- ▶ Constituir el punto de contacto especializado para la coordinación con el CSIRT de referencia.
- ▶ Notificar a la autoridad competente los incidentes de seguridad.
- ▶ Supervisar la subsanación de las deficiencias observadas en las auditorías, en colaboración con el RSGSI.
- ▶ Recopilar, preparar y suministrar información o documentación a la autoridad competente o el CSIRT de referencia, a su solicitud o por propia iniciativa.

8.2.2. Responsable de la Información (Esquema Nacional de Seguridad)

La Responsable de la Información tiene competencia suficiente para decidir sobre la finalidad, contenido y uso de la información y determinar los requisitos de seguridad de la información tratada.

Las funciones del Responsable de la Información son las siguientes:

- ▶ Determinar los niveles de seguridad de la información tratada, valorando los impactos de los incidentes que afecten a la seguridad de la información.
- ▶ Realizar, junto a los Responsables de Servicio y el Responsable de Seguridad, los preceptivos análisis de riesgos, y seleccionar las salvaguardas que se han de implantar.
- ▶ Aceptar los riesgos residuales respecto a los servicios calculados en el análisis de riesgos.
- ▶ Realizar, junto con el Responsable de Seguridad, el seguimiento y control de los riesgos.

8.2.3. Responsable del Sistema (Esquema Nacional de Seguridad)

Es un puesto operativo encargado de la explotación del sistema, dentro del ámbito del Esquema Nacional de Seguridad.

Las funciones del Responsable del Sistema son las siguientes:

- ▶ Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- ▶ Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- ▶ Decidir las medidas de seguridad que aplicarán los suministradores de componentes del Sistema durante las etapas de desarrollo, instalación y prueba del mismo, cerciorándose de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- ▶ El Responsable del Sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio, si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el Responsable de Seguridad antes de ser ejecutada.
- ▶ Realizar, junto con el Responsable de Seguridad, el seguimiento y control de los riesgos, incluyendo los relativos al incumplimiento de los acuerdos de niveles de servicio con terceros que provean servicios de tecnologías de la información bajo su responsabilidad.

8.2.4. Responsable del Servicio (Esquema Nacional de Seguridad)

El Responsable del Servicio posee competencia suficiente para decidir sobre la finalidad y prestación del servicio y determinar los requisitos de seguridad de los servicios prestados.

Las funciones del Responsable del Servicio son las siguientes:

- ▶ Determinar los niveles de seguridad del servicio tratado y mantener estos niveles actualizados, valorando los impactos de los incidentes que afecten a la seguridad de la información, conforme con lo establecido en el artículo 40 del ENS.
- ▶ Realizar, junto a los Responsables de la Información y el Responsable de Seguridad, los preceptivos análisis de riesgos, y seleccionar las salvaguardas que se han de implantar.
- ▶ Aceptar los riesgos residuales respecto a los servicios calculados en el análisis de riesgos.
- ▶ Notificar al Responsable de Seguridad cualquier incumplimiento de los acuerdos de nivel de servicio relativos a la seguridad de la información por parte de terceros que provean servicios bajo su responsabilidad.
- ▶ Realizar, junto con el Responsable de Seguridad, el seguimiento y control de los riesgos, incluyendo los relativos al incumplimiento de los acuerdos de niveles de servicio con terceros.
- ▶ Suspender, de acuerdo con el Responsable de la Información y el Responsable de Seguridad, la prestación de un servicio electrónico o el manejo de una determinada información, si es informado de deficiencias graves de seguridad.

8.2.5. Responsable del SGSI

Las funciones del Responsable del Sistema de Gestión de Seguridad de la Información (RSGSI) son:

- ▶ Elaborar y dar a conocer la **POLÍTICA DE SEGURIDAD INTEGRAL**, en colaboración con el Responsable de Seguridad.
- ▶ Desarrollar las políticas de seguridad, normativas y procedimientos derivados, y supervisar su efectividad, en colaboración con el Responsable de Seguridad.
- ▶ Asignar responsabilidades en seguridad de la información.
- ▶ Elaborar y aprobar el documento de Declaración de Aplicabilidad del Anexo A de la ISO 27001.
- ▶ Garantizar el cumplimiento normativo y evaluar los incumplimientos, en colaboración con el Responsable de Seguridad.
- ▶ Decidir las medidas de seguridad que se aplican en la organización, en colaboración con el Responsable de Seguridad.
- ▶ Realizar o promover auditorías periódicas para garantizar la correcta aplicación de las medidas de seguridad, en colaboración con el Responsable de Seguridad.
- ▶ Determinar la metodología y herramientas para la evaluación de riesgos, en

- colaboración con el Responsable de Seguridad.
- ▶ Elaborar la evaluación de riesgos y el plan de tratamiento resultante, así como aceptar el último, en colaboración con el Responsable de Seguridad.
 - ▶ Actuar como capacitador de buenas prácticas, en colaboración con el Responsable de Seguridad.
 - ▶ Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución, en colaboración con el Responsable de Seguridad.
 - ▶ Garantizar que las políticas, normativas y procedimientos que componen el SG es accesible por el personal de **Ecna**.
 - ▶ Garantizar que el SG se ajusta a los requerimientos normativos.
 - ▶ Reportar los resultados y el desempeño del SG a Dirección.
 - ▶ Establecer las medidas preventivas y/o correctoras ante desviaciones detectadas en las revisiones periódicas de los elementos que componen el SG.
 - ▶ Planificar, diseñar e implantar las acciones de formación y concienciación específicas en materia del SG.
 - ▶ Validar los resultados derivados de las revisiones periódicas del cumplimiento de las políticas, procesos y procedimientos que componen el SG.
 - ▶ Identificar y alimentar los objetivos del SG dentro de los objetivos de la organización.
 - ▶ Supervisar y controlar los cambios significativos en el contexto que puedan afectar al SG.
 - ▶ Acordar y establecer metodologías y métricas estándares para el SG.

8.3. Procedimiento de Designación y Renovación

Una vez aprobada la **POLÍTICA DE SEGURIDAD INTEGRAL** de **Ecna**, se asignarán los roles y componentes del Comité de Calidad y Seguridad, para el ejercicio de las competencias definidas en la Política. De igual forma Dirección nombrará el Responsable de Seguridad.

Los nombramientos del Comité y del Responsable de Seguridad serán revisados cada 5 años, o cuando haya algún cambio en la Organización o algún puesto quede vacante.

Asimismo, Dirección designará al Responsable del Servicio, Responsable de la Información, Responsable del Sistema y al Responsable del SGSI, así como sus funciones y responsabilidades dentro del marco establecido por la **POLÍTICA DE SEGURIDAD INTEGRAL**.

8.4. Resolución de conflictos

En caso de conflicto entre los diferentes responsables, éste será resuelto por el superior jerárquico de los mismos y, en su defecto, prevalecerá la decisión adoptada por el

Comité de Calidad y Seguridad.

8.5. Política de seguridad integral

Es misión del Comité de Calidad y Seguridad la revisión anual de esta **POLÍTICA DE SEGURIDAD INTEGRAL** y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por Dirección y difundida para que la conozcan todas las partes afectadas.

9. FORMACIÓN Y CONCIENCIACIÓN

Ecna lleva a cabo actividades de formación y concienciación para que el personal sea plenamente consciente de su responsabilidad con la seguridad de la información que afecta a todas las actividades y miembros de la organización, así como tengan una sensibilidad hacia los riesgos que se corren.

Con el objetivo de lograr la plena conciencia respecto a que la seguridad de la información afecta a todos los miembros de **Ecna**, y a todas las actividades, de acuerdo con el principio de Seguridad Integral recogido en el Artículo 5 del ENS, así como la articulación de los medios necesarios para que todas las personas que intervienen en el proceso y sus responsables tengan una sensibilidad hacia los riesgos que se corren.

10. DATOS DE CARÁCTER PERSONAL

Ecna, en el desarrollo de sus funciones, requiere hacer uso de datos de carácter personal. Por ello, se garantizarán los derechos y libertades de los interesados, así como la seguridad de la información, de las comunicaciones y de los sistemas de información que soportan los tratamientos de acuerdo con las medidas previstas en la legislación vigente.

Para lograr las necesarias garantías se realizarán todas las acciones pertinentes de las siguientes:

- ▶ La realización de análisis de riesgos sobre los tratamientos, y evaluaciones del impacto en la privacidad cuando sea probable que los tratamientos entrañen un alto riesgo para los derechos y libertades de los afectados.
- ▶ El diseño e implantación de medidas técnicas y organizativas para mitigar los riesgos relativos a los tratamientos de datos de carácter personal por defecto y desde el diseño.
- ▶ El rediseño de los procesos para mitigar los riesgos que no puedan mitigarse y asumirse.
- ▶ La elaboración de toda la documentación necesaria para soportar los procesos y garantizar los derechos y libertades de los afectados, cumpliendo con los principios establecidos por la normativa vigente.
- ▶ El traslado de las obligaciones a todo el personal que tenga acceso a los datos de carácter personal.

- ▶ La gestión de las relaciones con encargados de tratamiento con base en unos criterios establecidos, incluyendo la regulación a través de contratos que formalicen las obligaciones y los requisitos de seguridad.
- ▶ El mantenimiento de un registro de actividades de tratamiento.
- ▶ La información en los plazos requeridos, en base a las disposiciones de las leyes aplicables, a la correspondiente autoridad competente de protección de datos de lo siguiente:
 - Los tratamientos en uso.
 - Los resultados de las evaluaciones de impacto realizadas.
 - Las transferencias internacionales fuera de la Unión Europea (UE) que se vayan a llevar a cabo.
 - Las violaciones de seguridad que conlleven una probabilidad de riesgo contra los derechos y libertades de los interesados, dentro de las 72h siguientes a su detección.
 - Cualquier otra información que sea requerida por una ley o por indicaciones de la citada autoridad competente de protección de datos.
- ▶ La información por capas sobre los tratamientos a los afectados por los mismos, de forma concisa, transparente, inteligible y de fácil acceso.
- ▶ La recogida del consentimiento de los afectados de forma expresa e inequívoca, y previamente al inicio de los tratamientos y/o establecimiento de cesiones.
- ▶ La notificación a los afectados de violaciones de seguridad que supongan un alto riesgo contra sus derechos y libertades, dentro de las 72h siguientes a su detección

11. GESTIÓN DE RIESGOS

Se realiza un análisis de riesgos sobre todos los sistemas sujetos a esta Política, evaluando las amenazas y los riesgos a los que están expuestos. Se sigue la metodología MAGERIT (metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica que estima que la gestión de los riesgos es una piedra angular en las guías de buen gobierno):

- ▶ *MAGERIT- Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método.*
- ▶ *MAGERIT- Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos.*
- ▶ *MAGERIT- Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III – Guía de Técnicas.*

Para mayor detalle, consúltese el siguiente enlace:

https://administracionelectronica.gob.es/pae/Home/pae_Documentacion/pae_Metodologia/pae_Magerit.html

Este análisis se repetirá:

- ▶ Regularmente, al menos una vez al año.
- ▶ Cuando cambie la información manejada.
- ▶ Cuando cambien los servicios prestados.
- ▶ Cuando ocurra un incidente grave de seguridad.
- ▶ Cuando se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el Comité de Calidad y Seguridad establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Calidad y Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

12. DESARROLLO DE LA POLÍTICA DE SEGURIDAD INTEGRAL

Esta **POLÍTICA DE SEGURIDAD INTEGRAL** se desarrolla por medio de una **NORMATIVA DE SEGURIDAD** que afronte aspectos específicos de **Ecna**. Dicha Normativa está disponible para todos los miembros de la organización que necesitan conocerla, en particular para aquellos que utilizan, operan o administran los sistemas de información y comunicaciones de la organización.

13. OBLIGACIONES DEL PERSONAL

Todos los empleados de **Ecna** tienen la obligación de conocer y cumplir esta **POLÍTICA DE SEGURIDAD INTEGRAL** y la **NORMATIVA DE SEGURIDAD**, siendo responsabilidad del Comité de Calidad y Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Todos los empleados de **Ecna** atienden a una sesión de concienciación en materia de seguridad al menos una vez al año. Se establece un programa de concienciación continua para atender a todos ellos, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC reciben formación para el manejo seguro de los sistemas en la medida en que la necesitan 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.

14. TERCERAS PARTES

Cuando **Ecna** preste servicios a otros organismos o maneje información de éstos, se les hace partícipes de esta **POLÍTICA DE SEGURIDAD INTEGRAL**, se establecen canales para reporte y coordinación de los respectivos Comités de Seguridad y se establecen procedimientos de actuación para la reacción ante incidentes de seguridad.

Asimismo, en estos casos, se les hace partícipes de esta **POLÍTICA DE SEGURIDAD**

INTEGRAL y de la **NORMATIVA DE SEGURIDAD** que atañe 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 establecen procedimientos específicos de reporte y resolución de incidencias. Se garantiza 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 puede ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requiere un informe del Responsable de Seguridad que precisa los riesgos en que se incurre y la forma de tratarlos. Se requiere la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

15. CONTROL DE ACCESO

El acceso al sistema de información de **Ecna** está controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, tal y como se detalla en la **NORMATIVA DE SEGURIDAD** en el apartado de 'Control de acceso'. Estos accesos están debidamente autorizados, restringiendo el acceso a las funciones permitidas.

16. PROTECCIÓN DE LAS INSTALACIONES

Los sistemas de **Ecna** se instalan en áreas separadas, dotadas de un procedimiento de control de acceso, tal y como se detalla en la **NORMATIVA DE SEGURIDAD** en el apartado de 'Seguridad física y ambiental'. La oficina está siempre cerrada y se dispone de un control de llaves y gestión de claves para el acceso a la misma.

17. ADQUISICIÓN DE PRODUCTOS

Ecna utiliza productos de seguridad de las tecnologías de la información y comunicaciones que tengan certificada la funcionalidad de seguridad relacionada con el objeto de la adquisición. Esta certificación estará de acuerdo con las normas y estándares de mayor reconocimiento internacional en el ámbito de la seguridad funcional.

Esta exigencia se realiza de forma proporcionada a la categoría del sistema y nivel de seguridad de **Ecna**. Existirá una excepción en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del Responsable de Seguridad.

18. SEGURIDAD POR DEFECTO

Los sistemas de **Ecna** se diseñan y configuran de forma que garanticen la seguridad por defecto:

- a) Se retiren cuentas y contraseñas estándar.
- b) Se aplica la regla de «mínima funcionalidad»:

1. El sistema debe proporcionar la funcionalidad requerida para que la organización alcance sus objetivos y ninguna otra funcionalidad,
 2. No proporciona funciones gratuitas, ni de operación, ni de administración, ni de auditoría, reduciendo de esta forma su perímetro al mínimo imprescindible.
 3. Se elimina o desactiva mediante el control de la configuración, aquellas funciones que no sean de interés no sean necesarias, e incluso, aquellas que sean inadecuadas al fin que se persigue.
- c) Se aplica la regla de «seguridad por defecto»:
1. Las medidas de seguridad son respetuosas con el usuario y protegen a éste, salvo que se exponga conscientemente a un riesgo.
 2. Para reducir la seguridad, el usuario tiene que realizar acciones conscientes.
 3. El uso natural, en los casos que el usuario no ha consultado el manual, será un uso seguro.

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.

19. INTEGRIDAD Y ACTUALIZACIÓN DEL SISTEMA

En **Ecna** todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema, tal y como se detalla en la **NORMATIVA DE SEGURIDAD**. Asimismo, el estado de seguridad de los sistemas de **Ecna**, en relación con las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, es monitorizado y conocido en todo momento, reaccionando con diligencia a la hora de gestionar el riesgo según el estado de seguridad de los mismos.

20. PROTECCIÓN DE LA INFORMACIÓN ALMACENADA Y EN TRÁNSITO

En **Ecna** se aplican procedimientos para la gestión segura de soportes de almacenamiento de acuerdo con la presente política.

Se aplicará la debida diligencia y control a los soportes de información que permanecen bajo la responsabilidad de la organización, mediante las siguientes actuaciones:

- ▶ Garantizando el control de acceso con medidas físicas, lógicas o ambas.
- ▶ Garantizando que se respetan las exigencias de mantenimiento del fabricante, en especial, en lo referente a temperatura, humedad y otros agresores medioambientales, además:
 - Se aplican mecanismos criptográficos que garanticen la confidencialidad y la integridad de la información contenida.
 - Se emplean algoritmos acreditados por el Centro Criptológico Nacional.
 - Se emplean, preferentemente, productos certificados.

- Solo se utilizan unidades y medios extraíbles en caso de existir una necesidad de negocio para hacerlo.
- Se prohíbe el almacenamiento de Datos de Carácter Personal en soportes y dispositivos ópticos (CD, DVD, etc.) y flash USB (discos duros externos, pen drives, etc.) no autorizados.
- El contenido de los medios reutilizables es borrado de manera segura, de manera que no permite su recuperación, previamente a ser reutilizados.
- Borrado seguro mediante software.
- Cuando sea necesario podrá requerirse la autorización para la extracción de soportes fuera de las instalaciones de **Ecna**.
- Los soportes son almacenados en un ambiente seguro de acuerdo con las especificaciones del fabricante.
- Con objeto de mitigar el riesgo de pérdida de datos, se respetan los plazos de vida de los medios de almacenamiento, mediante la transferencia de los datos a un soporte nuevo que permita garantizar los periodos de retención.

Se presta especial atención a la información almacenada o en tránsito a través de entornos inseguros, tales como equipos portátiles, dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil.

Ecna evita de manera proactiva, mediante la realización de copias de seguridad, la pérdida de información, tal y como se detalla en la **NORMATIVA DE SEGURIDAD**.

Por otro lado, toda información sensible en soporte no electrónico está protegida bajo llave con el mismo grado de seguridad que en soporte electrónico.

21. PREVENCIÓN ANTE OTROS SISTEMAS DE INFORMACIÓN INTERCONECTADOS

Ecna analiza los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y lo controla y monitoriza a través de su punto de unión, tal y como se indica en la **NORMATIVA DE SEGURIDAD**.

22. PROCESO DE AUTORIZACIONES

Las responsabilidades relativas a la seguridad de la información se encuentran descritas documentalmente y son asignadas a personas específicas por parte de la Dirección, que disponen de la capacitación que permite que desarrollen su función eficazmente y de un proceso formal para autorizaciones respecto a los sistemas de información.

Se requerirá, en función del tipo de componente o actuación, la autorización de los siguientes roles:

Tipo de cambio	Autorizador
----------------	-------------

Actividad de negocio	Dirección
Proyecto / Servicio	Responsable del Servicio
Elemento tecnológico	Responsable de Seguridad

Los elementos sujetos al proceso de autorización serán como mínimo:

- ▶ Instalaciones habituales y alternativas.
- ▶ Entrada de equipos en producción.
- ▶ Entrada de aplicaciones en producción.
- ▶ Establecimiento de enlaces de comunicación.
- ▶ Utilización de medios telemáticos de comunicación.
- ▶ Utilización de soportes.
- ▶ Utilización de equipos móviles.
- ▶ Utilización de servicios de terceros, bajo contrato o convenio.
- ▶ Todos aquellos cambios que puedan suponer riesgo a la seguridad de la información de **Ecna** o de sus clientes.

23. REGISTRO DE ACTIVIDAD

Ecna registra las actividades de los usuarios, así como de los administradores del sistema, 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.

Asimismo, se protegen los sistemas de registro y los registros en sí de manipulaciones indebidas y accesos no autorizados.

Todo ello se recoge con detalle en la **NORMATIVA DE SEGURIDAD** en el apartado 'Registro de Actividad y Supervisión'.

24. INCIDENTES DE SEGURIDAD

Ecna dispone de un sistema de detección y reacción frente a código dañino, garantizando un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluidos los de comunicación de eventos, vulnerabilidades y debilidades de seguridad. Se dispone de procedimientos de gestión de incidentes de seguridad y de debilidades detectadas en los elementos del sistema de información de la organización.

Estos procedimientos cubren los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las

partes interesadas, el registro de las actuaciones y el aprendizaje resultante, con el fin de emplearlo para la mejora continua de la seguridad del sistema.

25. CONTINUIDAD DE LA ACTIVIDAD

Ecna evita de manera proactiva, mediante la realización de copias de seguridad, la pérdida de información. Asimismo, dispone de los mecanismos necesarios que garantizan la continuidad de las operaciones en caso de pérdida de los medios habituales de trabajo a través de los procesos de continuidad de negocio de la organización.

26. MEJORA CONTINUA DEL PROCESO DE SEGURIDAD

El proceso integral de seguridad implantado en **Ecna** será actualizado y mejorado de forma continua. Los procesos de ingeniería se actualizan frecuentemente para garantizar la mejora continua de los procesos de seguridad aplicados y adecuarse a nuevas amenazas potenciales.

27. ESTRUCTURACIÓN DE LA DOCUMENTACIÓN DE SEGURIDAD DEL SISTEMA

Ecna dispone de un proceso de gestión de documentación y registros que permite establecer el control documental del SG implantado. En él se especifica la estructura del SG, se describe los apartados de éste y la nomenclatura empleada para codificarlos. Asimismo, se cuenta con un procedimiento de gestión de cambios.

28. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 19 de septiembre de 2024 por Dirección.

Esta **POLÍTICA DE SEGURIDAD INTEGRAL** es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

29. PROCEDIMIENTO DE REVISIÓN

Será misión del Comité de Calidad y Seguridad la revisión anual de esta **POLÍTICA DE SEGURIDAD INTEGRAL** y la propuesta de revisión o mantenimiento de la misma.

Si procediera la elaboración y propuesta de una modificación y/o actualización, la Política será aprobada y difundida por el Comité de Calidad y Seguridad para que la conozcan todas las partes afectadas.

Nombre:

Fecha y firma: