

	Información Documentada	Código	Fecha	Rev.	Aprobado
	POLÍTICA SEGURIDAD DE LA INFORMACIÓN ENS	DC-052	06/03/2026	01	Dirección
	Modificación: Creación del documento.	Clasificación: Uso interno			Pág.:1 de 22

CONTENIDO

1.	Objetivo	5
2.	Alcance	5
2.1.	Objetivos y misión de la organización	6
2.2.	Marco regulatorio	6
3.	Desarrollo de la Política de Seguridad de la información	6
4.	Categorización de los sistemas de información	7
5.	Principios básicos	8
5.1.	La seguridad como un proceso integral	8
5.2.	Gestión de la seguridad basada en la gestión de los riesgos	9
5.3.	Prevención	9
5.4.	Existencia de líneas de defensa	10
5.5.	Vigilancia continua y detección	10
5.6.	Respuesta	11
5.7.	Recuperación	11
5.8.	Conservación	12
5.9.	Reevaluación periódica	12
5.10.	Diferenciación de responsabilidades	12
6.	Marco regulatorio	12
7.	Organización de la Seguridad	13
7.1.	Roles: Funciones y Responsabilidades	14
7.2.	Comités: Funciones y Responsabilidades	15
7.3.	Procedimiento para la designación y renovación de roles	16
7.4.	Mecanismo de coordinación y resolución de conflictos	16
7.5.	Política de Seguridad de la Información	16
7.6.	Gestión de la documentación	16
8.	Requisitos de seguridad de la información	17
8.1.	Organización e implantación del proceso de seguridad	17
8.2.	Análisis y gestión de riesgos	17
8.3.	Gestión del personal	17
8.4.	Profesionalidad	18
8.5.	Terceras Partes	18
8.6.	Autorización y control de los accesos	19
8.7.	Protección de las instalaciones	20
8.8.	Adquisición de productos de seguridad y contratación de servicios de seguridad	20
8.9.	Mínimo privilegio	20
8.10.	Integridad y actualización del sistema.	21
8.11.	Protección de información almacenada y en tránsito	21
8.12.	Prevención ante otros sistemas de información interconectados	22
8.13.	Registro de actividad y detección de código dañino	22
8.14.	Incidentes de seguridad	23
8.15.	Continuidad de la actividad	23

	Información Documentada	Código	Fecha	Rev.	Aprobado
	POLÍTICA SEGURIDAD DE LA INFORMACIÓN ENS	DC-052	06/03/2026	01	Dirección
	Modificación: Creación del documento.	Clasificación: Uso interno			Pág.:2 de 22

8.16.	Protección de los datos de carácter personal	23
8.17.	Ciclo de vida de servicios y sistemas.	24
8.18.	Mejora continua del proceso de seguridad	24
9.	Cumplimiento de requisitos mínimos	24
10.	Auditoría de Seguridad	25
11.	Referencias	26
11.1.	Documentos internos	26
11.2.	Referencias externas	26

	Información Documentada	Código	Fecha	Rev.	Aprobado
	POLÍTICA SEGURIDAD DE LA INFORMACIÓN ENS	DC-052	06/03/2026	01	Dirección
	Modificación: Creación del documento.	Clasificación: Uso interno			Pág.:3 de 22

1. Objetivo

El presente documento establece la Política de Seguridad de la Información de Numintec , efectiva desde su fecha de aprobación y hasta ser reemplazada por nueva versión de Política.

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

En consonancia con el artículo 1 del *Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. (ENS)*, esta política establece los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información. Serán aplicados por Numintec para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que se gestionen para la prestación de los servicios contemplados en el alcance.

Esta política complementa y desarrolla la *Política del Sistema Integrado de Gestión* de Numintec, elaborada en el marco del SGSI de acuerdo con los requisitos de, entre otras, la norma ISO 27001.

2. Alcance

La presente política se refiere a los sistemas de información que dan soporte a los servicios prestados desde Numintec que consisten en la provisión de servicios de desarrollo, comercialización y servicio técnico de soluciones de comunicación en la nube propias, e infraestructura TIC de soporte de acuerdo con la declaración de aplicabilidad vigente.

Asimismo, la presente política aplica a todas las personas trabajadoras y colaboradoras de Numintec sin excepciones, así como a todas las terceras partes identificadas como prestadores de servicios en el ámbito de este alcance, incluidas a aquellas unidades de Numintec que dan soporte a la actividad de la empresa.

En concordancia con el artículo 13 del ENS, esta política establece que la seguridad de la información compromete a todos los miembros de la organización. Mediante esta política de seguridad se identifican unos claros responsables de velar por su cumplimiento y ser conocida por todos los miembros de la organización.

2.1. Distribución y revisión

Es tarea de la persona Responsable de Seguridad de la información asegurar la revisión, aprobación y distribución de este documento, así como el estado de actualización de todos los documentos a los que se hace referencia.

2.2. Objetivos y misión de la organización

Los objetivos y misión de la organización se han definido en *DC-005 Política del Sistemas Integrado de Gestión de Numintec*, publicada en la web y disponible para todo el personal y colaboradores de Numintec.

	Información Documentada	Código	Fecha	Rev.	Aprobado
	POLÍTICA SEGURIDAD DE LA INFORMACIÓN ENS	DC-052	06/03/2026	01	Dirección
	Modificación: Creación del documento.	Clasificación: Uso interno			Pág.:4 de 22

2.3. Marco regulatorio

El marco legal contemplado en el alcance de la Política de Seguridad de la Información de Numintec es el que está desarrollado en el apartado 6. *Marco normativo* de este documento.

3. Desarrollo de la Política de Seguridad de la información

Esta Política de Seguridad de la Información complementa las políticas de seguridad de Numintec, recogidas en el Sistema Integrado de Gestión y adecuadas a las medidas de seguridad que aplican según la *DC-053 Declaración de Aplicabilidad ENS*.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto 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 implica que Numintec ha puesto en marcha un Sistema de Gestión de la Seguridad de la Información, según el cual se aplican las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad (ENS), y se realiza un seguimiento continuo de los niveles de prestación de servicios, se siguen y analizan las vulnerabilidades reportadas, y se prepara una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

El conjunto de áreas de Numintec debe contemplar la seguridad TIC como 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.

Esta Política de Seguridad de la Información se ha desarrollado por medio de una normativa de seguridad que afronta aspectos específicos. La normativa de seguridad está a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La normativa de seguridad estará disponible en el repositorio de GDRIVE con la documentación del SIC para empleados, y forma parte del proceso de Onboarding para todas las personas trabajadoras de Numintec.

4. Categorización de los sistemas de información

En aplicación de los criterios establecidos en el artículo 40 del ENS, la categoría de los sistemas de información dentro del alcance de esta política, en materia de seguridad, modulará el equilibrio entre la importancia de la información que manejan, los servicios que prestan y el esfuerzo de seguridad requerido, en función de los riesgos a los que están expuestos, bajo el criterio del principio de proporcionalidad.

La determinación de la categoría indicada en el apartado anterior se efectuará en función de la valoración del impacto que tendría un incidente que pudiera afectar a la seguridad de la información o de los servicios con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad, como dimensiones de seguridad,

Atendiendo a lo establecido en el Anexo I del ENS, así como en la guía *CCN-STIC 803 ENS. Valoración de los sistemas*, los fundamentos para la valoración de las consecuencias de un impacto negativo sobre la seguridad de la información y de los servicios se efectuará atendiendo a su repercusión en la capacidad de la organización para:

	Información Documentada	Código	Fecha	Rev.	Aprobado
	POLÍTICA SEGURIDAD DE LA INFORMACIÓN ENS	DC-052	06/03/2026	01	Dirección
	Modificación: Creación del documento.	Clasificación: Uso interno			Pág.:5 de 22

- a) el logro de sus objetivos;
- b) la protección de sus activos;
- c) el cumplimiento de sus obligaciones de servicio y contractuales;
- d) el respeto de la legalidad vigente;
- e) el respeto a los derechos de las personas.

Esta valoración y los criterios aplicados se encuentran recogidos en la Categorización documentada en el *DC-053 Declaración de Aplicabilidad ENS*.

Para determinar el nivel requerido para cada dimensión de seguridad se toma como referencia la identificación y valoración detallada de los principales activos de servicios y de información determinada en el *IMP-040 Tabla de Valoración de Activos*.

Para realizar esta valoración de activos respecto a las diferentes dimensiones de seguridad se tienen en cuenta los criterios de clasificación de la información establecidos en el documento *DC-032 Política de Clasificación de Información*, y que serán acordes con los que se establecen en el Anexo I del ENS.

En atención a las facultades determinadas en el artículo 41 del ENS, corresponderá al responsable de cada activo efectuar las valoraciones aquí mencionadas, y al responsable de cada sistema la determinación de la categoría de este.

5. Principios básicos

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, autenticidad de la información, trazabilidad de los servicios y datos, uso previsto 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.

Tal como establece el artículo 5 del ENS, el objeto último de la seguridad de la información es asegurar que una organización administrativa pueda cumplir sus objetivos utilizando sistemas de información. En las decisiones en materia de seguridad deberán tenerse en cuenta los siguientes principios básicos:

- a) Seguridad como proceso integral.
- b) Gestión de la seguridad basada en riesgos.
- c) Prevención, detección, respuesta y conservación.
- d) Existencia de líneas de defensa.
- e) Reevaluación periódica.
- f) Diferenciación de responsabilidades.

Es importante remarcar que, tal como establece el artículo 8 del ENS, la seguridad del sistema debe contemplar las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta la organización.

5.1. La seguridad como un proceso integral

Tal como se refleja en el artículo 6 del ENS, la seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales, jurídicos y organizativos, relacionados con el sistema de información. La política de seguridad de la información estará regida por este principio, el cuál excluye cualquier actuación puntual o tratamiento coyuntural.

	Información Documentada	Código	Fecha	Rev.	Aprobado
	POLÍTICA SEGURIDAD DE LA INFORMACIÓN ENS	DC-052	06/03/2026	01	Dirección
	Modificación: Creación del documento.	Clasificación: Uso interno			Pág.:6 de 22

El conjunto de áreas y departamentos de Numintec debe contemplar la seguridad como una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción y diseño 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 las planificaciones.

5.2. Gestión de la seguridad basada en la gestión de los riesgos

En consonancia con los principios establecidos en los artículos 6 y 14 del ENS, la apreciación, análisis y tratamiento de los riesgos serán parte esencial de la gestión de la seguridad y deberán mantenerse permanentemente actualizados.

La gestión de los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables.

La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.

Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos apreciados.

El análisis de riesgos se realizará siguiendo el *DC-023 Metodología Evaluación de Riesgos de seguridad de la información* y se revisará regularmente (mínimo con regularidad anual), o cuando:

- cambie la información manejada;
- cambien los servicios prestados;
- ocurra un incidente grave de seguridad;
- se reporten vulnerabilidades graves.

5.3. Prevención

Las diferentes áreas y departamentos sujetos al alcance de esta política 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. Para ello se han implementado las medidas mínimas de seguridad determinadas por el ENS, así como los controles adicionales identificados a través de una evaluación de amenazas y riesgos.

Tal como se indica en el artículo 8 del ENS, las medidas de prevención deben eliminar o, al menos reducir, la posibilidad de que las amenazas lleguen a materializarse con perjuicio para el sistema. Estas medidas de prevención contemplarán, entre otras, la disuasión y la reducción de la exposición.

Para garantizar el cumplimiento de esta política, se han establecido los siguientes requisitos:

- 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 continua del desempeño de las medidas de seguridad y de la operación de los sistemas.

Estos controles, así como los roles y responsabilidades de seguridad de todo el personal, están claramente definidos y documentados.

	Información Documentada	Código	Fecha	Rev.	Aprobado
	POLÍTICA SEGURIDAD DE LA INFORMACIÓN ENS	DC-052	06/03/2026	01	Dirección
	Modificación: Creación del documento.	Clasificación: Uso interno		Pág.:7 de 22	

5.4. Existencia de líneas de defensa

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el artículo 9 del ENS que implementan una estrategia de protección constituida por múltiples capas de seguridad, dispuestas de forma que, cuando una de las capas falle, permita:

- Desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse.
- Reducir la probabilidad de que el sistema sea comprometido en su conjunto.
- Minimizar el impacto final sobre el mismo.

Estas líneas de defensa estarán constituidas por medidas de naturaleza organizativa, física y lógica.

5.5. Vigilancia continua y detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar el desempeño de las líneas de defensa y la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios o la presencia de ciber incidentes, y actuar en consecuencia según el principio de vigilancia continua establecido en el artículo 10 del ENS.

Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables de forma regular y también cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

5.6. Respuesta

Las medidas de detección estarán acompañadas de medidas de respuesta, de forma que los incidentes de seguridad se gestionen en tiempo oportuno.

Mediante los adecuados procedimientos operativos:

- Se han establecido mecanismos para responder eficazmente a los incidentes de seguridad.
- Se ha designado un punto de contacto para las comunicaciones con respecto a incidentes detectados en las diferentes áreas de Numintec o terceras partes involucradas.
- Se han establecido protocolos para el intercambio de información con las partes interesadas relacionadas con el incidente.

5.7. Recuperación

Las medidas de recuperación permitirán la restauración de la información y los servicios que pudieran haberse visto afectados por incidentes disruptivos, de forma que se pueda hacer frente a las situaciones en las que estos incidentes afecten a la disponibilidad de los activos habituales de tratamiento o a la integridad de la información.

Como parte del plan general de continuidad de negocio de Numintec, se desarrollarán planes de continuidad de los sistemas de información que contemplen el desarrollo de procedimientos de recuperación para cada uno de los riesgos de disrupción identificados que permita recuperar las actividades críticas de acuerdo con los objetivos tiempos de recuperación (RTO) y punto de recuperación de los datos (RPO) establecidos.

Con este propósito se ha elaborado el DC-015 *Plan de continuidad de la Seguridad de la Información* para garantizar la disponibilidad de los servicios críticos.

	Información Documentada	Código	Fecha	Rev.	Aprobado
	POLÍTICA SEGURIDAD DE LA INFORMACIÓN ENS	DC-052	06/03/2026	01	Dirección
	Modificación: Creación del documento.	Clasificación: Uso interno		Pág.:8 de 22	

Asimismo, se contempla la realización de pruebas y ensayos para verificar la viabilidad y adecuación de los procedimientos de recuperación mediante los planes de prueba documentados de acuerdo con los correspondientes planes de continuidad.

5.8. Conservación

El sistema de información garantizará la conservación de los datos e información en soporte electrónico.

Para ello, se identificarán los principales activos de información y se determinarán los requisitos de conservación y retención, que servirá como punto de partida para establecer las políticas de copias de seguridad necesarias.

La implementación de estas políticas de copias de seguridad debe permitir asegurar los supuestos de inalterabilidad de la información y limitación de acceso según el principio de mínimo privilegio.

5.9. Reevaluación periódica

La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

Las medidas de seguridad se revisarán, se reevaluarán y actualizarán periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, llegando incluso a un replanteamiento de la seguridad, si fuese necesario.

Esta revisión y reevaluación periódica se llevará a cabo dentro del marco de gestión de riesgos y mejora continua del Sistema de Gestión de la Seguridad de la Información.

5.10. Diferenciación de responsabilidades

De acuerdo con el principio de diferenciación de responsabilidades establecido en el artículo 11 del ENS, Numintec establece funciones y responsabilidades de forma que la seguridad de la información se gestione como función diferenciada

Las políticas que aplican para la definición de estas funciones y responsabilidades están cubiertas en el apartado 7. *Organización de la Seguridad* de este documento

6. Marco regulatorio

El marco legal en materia de seguridad de la información que aplica a Numintec en el desarrollo de su actividad está recogido en la intranet: *Listado legislación SIG* incluido en el registro *IMP-001 Lista de documentación*.

Cabe remarcar que en lo que hace referencia específicamente al Esquema Nacional de Seguridad, se contempla:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad
- Instrucciones técnicas de seguridad de obligado cumplimiento, según lo previsto en la Disposición adicional segunda del Real Decreto 311/2022.

	Información Documentada	Código	Fecha	Rev.	Aprobado
	POLÍTICA SEGURIDAD DE LA INFORMACIÓN ENS	DC-052	06/03/2026	01	Dirección
	Modificación: Creación del documento.	Clasificación: Uso interno			Pág.:9 de 22

- Informe del estado de la seguridad
- Conformidad con el Esquema Nacional de Seguridad
- Auditoría de la seguridad de los sistemas de información
- Notificación de incidentes de seguridad

El contenido de estas instrucciones técnicas será de obligado cumplimiento en cuanto sus disposiciones se apliquen a una entidad del sector privado no sujeta a las obligaciones establecidas por la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

- Para el mejor cumplimiento de lo establecido en el Esquema Nacional de Seguridad, se tendrán como referencia las correspondientes guías de seguridad de las tecnologías de la información y la comunicación (guías CCN-STIC), particularmente de la serie 800 que elabora y difunde el CCN.

Asimismo, se contempla dentro del marco normativo el cumplimiento voluntario de estándares en seguridad de la información tal como la ISO 27001, ISO 27017, ISO 27018, ISO 27701.

Así como cumplimiento de directrices de la UE como el Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) n° 168/2013 y el Reglamento (UE) 2019/1020 y la Directiva (UE) 2020/1828 (Reglamento de Ciberresiliencia) y Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 y (UE) 2016/1011.

7. Organización de la Seguridad

Tal como establece el artículo 11 del ENS, Numintec establece funciones y responsabilidades de forma que la seguridad de la información se gestione como función diferenciada.

En especial se debe atender los siguientes principios de diferenciación de responsabilidades:

- En los sistemas de información se diferenciarán el responsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema.
- La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la explotación de los sistemas de información concernidos.

7.1. Comités: Funciones y responsabilidades

Se ha constituido el Comité de Seguridad de la Información que se rige por el procedimiento *PR-049 Procedimiento del Comité de Seguridad de la información*, en el que se detallan su composición, sus funciones y responsabilidades.

El Comité de Seguridad de la Información es el órgano responsable de establecer la estrategia, impulsar, priorizar, y efectuar el seguimiento de los Proyectos, Planes y Programas de Seguridad de los Sistemas de Información, coordinando y asegurando su adecuado soporte por las distintas áreas responsables y adaptándose a las necesidades de las áreas de negocio para dar cumplimiento a los objetivos de seguridad establecidos por la Dirección e informar a ésta de su estado y evolución.

Las funciones que el comité de seguridad de la información desempeñará son las siguientes:

- Revisión y aprobación de la política de seguridad de la información.
- Supervisión y control de los cambios introducidos respecto al tratamiento de los activos de información.

	Información Documentada	Código	Fecha	Rev.	Aprobado
	POLÍTICA SEGURIDAD DE LA INFORMACIÓN ENS	DC-052	06/03/2026	01	Dirección
	Modificación: Creación del documento.	Clasificación: Uso interno			Pág.:10 de 22

- Revisión, seguimiento y coordinación de las incidencias producidas en la seguridad de la información.

7.2. Roles: Funciones y Responsabilidades

Dentro de la organización de Numintec, incluyendo Numintec, han determinado unas funciones y responsabilidades generales relativas a la seguridad de la información y la protección de datos personales.

Estas funciones y responsabilidades están determinadas en el organigrama de Numintec y detalladas en las respectivas descripciones de puesto de trabajo.

Por otro lado, el Esquema Nacional de Seguridad (ENS) establece que en los sistemas de información se diferenciará la persona responsable de la información, la persona responsable del servicio, la persona responsable de la seguridad y la persona responsable del sistema. Asimismo, establece que la responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la explotación de los sistemas de información concernidos

De acuerdo con estas premisas, y siguiendo lo establecido por la *Guía de Seguridad de las TIC CCN-STIC 801 ENS Responsabilidades y Funciones*, se establecen las siguientes atribuciones para cada uno de estos cargos:

Cargo	Atribuciones
Responsable de la Información	Determina los requisitos (de seguridad) de la información tratada, según los parámetros del Anexo I del ENS. Tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección. Es el responsable último de cualquier error o negligencia que conlleve un incidente de confidencialidad o de integridad y de disponibilidad Tiene la potestad de determinar los niveles de seguridad de la información. Está a cargo de valoración de las consecuencias de un impacto negativo sobre la seguridad de la información que efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos. Puede haber más de un Responsable de la Información, atendiendo a la existencia de diferentes sistemas (con su correspondiente Información) dentro del alcance.
Responsable del Servicio	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. Tiene la potestad de determinar los niveles de seguridad de los servicios. Está a cargo de valoración de las consecuencias de un impacto negativo sobre la seguridad de los servicios que efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de

	Información Documentada	Código	Fecha	Rev.	Aprobado
	POLÍTICA SEGURIDAD DE LA INFORMACIÓN ENS	DC-052	06/03/2026	01	Dirección
	Modificación: Creación del documento.	Clasificación: Uso interno			Pág.:11 de 22

	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. Puede haber más de una Persona Responsable del Servicio, atendiendo a la existencia de diferentes sistemas (que prestan servicios) dentro del alcance.
Responsable de la Seguridad	Determina las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por las personas responsables de la información y de los servicios. Supervisar la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones. Deberá ser una persona física, jerárquicamente independiente de la persona Responsable del Sistema. Debe 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 de la Información de la organización. Debe promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad, así como actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos. Debe elaborar y proponer para aprobación por la organización las políticas de seguridad, que incluirán las medidas técnicas y organizativas, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados y para prevenir y reducir al mínimo los efectos de los ciber incidentes que afecten a la organización y los servicios. Debe desarrollar las políticas de seguridad, normativas y procedimientos derivados de la organización, supervisar su efectividad y llevar a cabo auditorías periódicas de seguridad. Constituye el punto de contacto especializado para la coordinación con el CSIRT de referencia. Es el encargado de notificar al CSIRT de referencia y sin dilación indebida, los incidentes que tengan efectos perturbadores en la prestación de los servicios y la seguridad de la información tratada. Debe elaborar y firmar la Declaración de Aplicabilidad, que es el documento que formaliza la relación de medidas seleccionadas del Anexo II del ENS. Los informes de autoevaluación y/o los informes de auditoría serán analizados por la persona Responsable de la Seguridad, que elevará las conclusiones a la persona Responsable del Sistema para que adopte las medidas correctoras adecuadas.
Responsable del Sistema	Se encarga de la operación del sistema de información, atendiendo a las medidas de seguridad determinadas por la persona Responsable de la Seguridad.

	Información Documentada	Código	Fecha	Rev.	Aprobado
	POLÍTICA SEGURIDAD DE LA INFORMACIÓN ENS	DC-052	06/03/2026	01	Dirección
	Modificación: Creación del documento.	Clasificación: Uso interno		Pág.:12 de 22	

	Se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo Tiene las siguientes funciones: a) Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento. b) Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo. c) Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad. Puede proponer la suspensión del tratamiento de una cierta información o la prestación de un determinado servicio si aprecia deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.
--	--

En Numintec se han determinado los siguientes cargos, con referencia a los puestos de trabajo definidos en el organigrama de la organización:



La persona designada será aquella que en cada momento ocupe el puesto de trabajo referenciado.

7.3. Punto de Contacto para la seguridad de la información

En cumplimiento de lo establecido en el artículo 13 del ENS, Numintec designa a la persona Responsable de Seguridad como POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, a fin de que canalice y supervise, tanto el cumplimiento de los requisitos de seguridad del servicio que presta o solución que provea, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio.

	Información Documentada	Código	Fecha	Rev.	Aprobado
	POLÍTICA SEGURIDAD DE LA INFORMACIÓN ENS	DC-052	06/03/2026	01	Dirección
	Modificación: Creación del documento.	Clasificación: Uso interno			Pág.:13 de 22

7.4. Procedimiento para la designación y renovación de roles

Los roles y funciones de seguridad serán los determinados en esta Política, y su designación y renovación estará formalizada con la aprobación de esta política.

En caso de que exista alguna variación en las personas designadas para cada uno de los cargos relacionados, la persona sustituta automáticamente asumirá las funciones y responsabilidades inherentes a los roles de seguridad que le son propios, quedando dicha designación formalizada en una posterior reunión del Comité de Seguridad de la Información.

7.5. Mecanismo de coordinación y resolución de conflictos

Se establece el Comité de Seguridad de la Información como órgano para la coordinación y resolución colegiada de conflictos. Será indispensable su participación en aquellas situaciones en que se pueda dar un conflicto de intereses por parte de alguno de sus miembros a la hora de tomar alguna decisión relacionada o que afecte a la seguridad de la información.

En el caso de que no se alcance ningún acuerdo en el marco de este Comité, corresponderá a la Dirección General de Numintec ejercer la función de arbitraje y tomar las decisiones oportunas.

7.6. Política de Seguridad de la Información

Será misión del Comité de Seguridad la revisión anual de esta Política de Seguridad de la Información a propuesta de revisión o mantenimiento del RSI. Cualquier miembro del Comité de Seguridad podrá proponer al RSI la necesidad de revisión o mantenimiento de la Política de Seguridad.

La Política será revisada por los miembros del Comité de Seguridad, aprobada por la Dirección General y difundida para que la conozcan todas las partes afectadas.

7.7. Gestión de la documentación

Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso serán las establecidas en las políticas y procedimientos que apliquen al Sistema Integrado de Gestión de Numintec.

Asimismo, se dispone de *DC-032 Políticas de Clasificación de la Información* que define el criterio para la clasificación de la documentación, el procedimiento para su clasificación, quién debe generarla y aprobarla, qué personas pueden acceder a ella, con qué frecuencia o bajo qué circunstancias debe revisarse.

8. Requisitos de seguridad de la información

Esta Política de Seguridad contempla todos los requisitos mínimos de seguridad determinados en el artículo 12 del ENS.

	Información Documentada	Código	Fecha	Rev.	Aprobado
	POLÍTICA SEGURIDAD DE LA INFORMACIÓN ENS	DC-052	06/03/2026	01	Dirección
	Modificación: Creación del documento.	Clasificación: Uso interno			Pág.:14 de 22

8.1. Organización e implantación del proceso de seguridad

Tal como se establece en el apartado *Alcance* de esta política, la seguridad compromete a todos los miembros de Numintec.

Según se detalla en el apartado 7. *Organización de la Seguridad*, se identifican unos claros responsables de velar por el cumplimiento de esta Política de Seguridad de la Información, la cual deberá ser conocida por todos los miembros de Numintec.

8.2. Análisis y gestión de riesgos

Este análisis y gestión se llevará a cabo tal como se dispone en el apartado 5.2 *Gestión de la seguridad basada en los riesgos* de esta política.

8.3. Gestión del personal

Tal como establece en IMP-274 Normativa de Seguridad de la Información, la información sobre nuestra empresa, nuestros clientes, nuestro personal y nuestros proveedores es el activo más valioso de Numintec, por lo que se debe usar y proteger de manera apropiada. Los recursos informáticos que se proporcionan a todas las personas empleadas y colaboradoras de Numintec pertenecen a Numintec y deben estar protegidos de manera similar. Estos recursos incluyen sistemas de información, computadoras, redes, así como documentos físicos (por ejemplo, impresiones).

Por lo tanto, es crucial que todo el personal de Numintec accedan, usen y compartan toda la información y los activos de TI de la empresa de manera responsable y en total cumplimiento con las leyes y reglamentos de privacidad, protección y almacenamiento de datos. Esto no solo garantiza que el personal pueda acceder a la información y los recursos que necesita para hacer su trabajo cuando los requiera, sino también que esta información no caerá en las manos equivocadas y no terminemos con “intrusos” dentro de las paredes virtuales de nuestra empresa.

Todos los miembros de Numintec tienen la obligación de conocer y cumplir con esta IMP-274 Normativa de Seguridad de la Información, así como las normativas y procedimientos de seguridad que les apliquen en el ejercicio de sus funciones, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue a los afectados.

Como parte del proceso de incorporación de los nuevos miembros y mediante recordatorios anuales, se asegura que todo el personal conoce y se compromete al cumplimiento de estos principios y políticas.

Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuentes de riesgo para la seguridad.

Todos los miembros de Numintec atenderán a la formación obligatoria en materia de Seguridad de la Información, y participarán en programas de concienciación continua.

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 este.

El personal relacionado con la información y los sistemas ejercitará y aplicará los principios de seguridad en el desempeño de su cometido.

	Información Documentada	Código	Fecha	Rev.	Aprobado
	POLÍTICA SEGURIDAD DE LA INFORMACIÓN ENS	DC-052	06/03/2026	01	Dirección
	Modificación: Creación del documento.	Clasificación: Uso interno			Pág.:15 de 22

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

8.4. Profesionalidad

La seguridad de los sistemas de Numintec 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 operación.

La cualificación del personal se determina en los requisitos de cada puesto de trabajo según se especifica en las descripciones de puesto de trabajo correspondientes: *DPT-XX*.

El personal de Numintec está comprometido en cumplir y hacer cumplir las políticas de seguridad de la información. Esta obligación está contemplada en las descripciones de puesto de trabajo de todas las personas trabajadoras.

Numintec exigirá, de manera objetiva y no discriminatoria, que las terceras partes que les presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.

8.5. Terceras Partes

Cuando Numintec preste servicios a otras entidades o trate información de otras entidades, si así lo requieren, se les hará partícipes de esta Política de Seguridad de la Información.

Cuando Numintec utilice servicios de terceros o comparta información con terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que atañe 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 esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

En cualquier caso, los proveedores de servicios de terceros deberán proporcionar garantías de seguridad de la información suficientes y adecuadas a los servicios prestados, siguiendo la *DC-036 Política de seguridad de uso de los servicios en la nube*. En el caso particular de aquellos servicios que se presten dentro del marco del alcance de la certificación ENS, se exigirá que los proveedores presten sus servicios de conformidad con los requisitos del ENS que les apliquen.

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 de la persona 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.

8.6. Autorización y control de los accesos

El *Proceso de Autorizaciones sobre los sistemas de IT* se ha definido en el apartado 12. Proceso de Autorizaciones de la presente Política y cubre todos los elementos de los sistemas de información.

- Utilización de instalaciones, habituales y alternativas.
- Entrada de equipos en producción, en particular, equipos que involucren criptografía.
- Entrada de aplicaciones en producción.

	Información Documentada	Código	Fecha	Rev.	Aprobado
	POLÍTICA SEGURIDAD DE LA INFORMACIÓN ENS	DC-052	06/03/2026	01	Dirección
	Modificación: Creación del documento.	Clasificación: Uso interno			Pág.:16 de 22

- d) Establecimiento de enlaces de comunicaciones con otros sistemas.
- e) Utilización de medios de comunicación, habituales y alternativos.
- f) Utilización de soportes de información.
- g) Utilización de equipos móviles. Se entenderá por equipos móviles, ordenadores portátiles, tabletas, u otros de naturaleza análoga.
- h) Utilización de servicios de terceros, bajo contrato o convenio.

El acceso a los sistemas de información de Numintec está controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas.

La política de control de accesos a los sistemas de información está documentada en *DC-034 Políticas de Control de Acceso*. Adicionalmente, se han establecido procedimientos operativos (PR-XX) para gestionar los accesos a los sistemas de información.

8.7. Protección de las instalaciones

Las actividades de Numintec se llevan a cabo totalmente en modalidad de emplazamiento virtual, ya que estas actividades se llevan a cabo en un entorno on-line permitiendo que los miembros de diferentes ubicaciones físicas ejecuten procesos llevando a cabo su trabajo de forma remota, en entornos en la nube.

La infraestructura de IT se apoya en infraestructuras propias de terceros que proporcionan servicios en modalidad SaaS y PaaS. Estos terceros deben proporcionar garantías conformes se cumplen los requisitos de seguridad establecidos por las políticas de Numintec y ser conformes a los requisitos del ENS aplicables

8.8. Adquisición de productos de seguridad y contratación de servicios de seguridad

En la adquisición de productos de seguridad de las TIC que vayan a ser empleados por Numintec se utilizarán, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del Responsable de Seguridad.

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

Para la contratación de servicios de seguridad se estará a lo dispuesto en los apartados anteriores y en lo relativo a profesionalidad y cualificación del personal y niveles de gestión.

La adquisición de productos y contratación de servicios de seguridad se registrará por lo establecido en el proceso de compras y gestión de proveedores recogido en el Sistema de Gestión de Numintec.

8.9. Mínimo privilegio

Los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto y se apliquen políticas de mínimo privilegio basadas estrictamente en la "necesidad de conocer".

- a) Los sistemas proporcionarán la mínima funcionalidad requerida para que la organización alcance sus objetivos.

	Información Documentada	Código	Fecha	Rev.	Aprobado
	POLÍTICA SEGURIDAD DE LA INFORMACIÓN ENS	DC-052	06/03/2026	01	Dirección
	Modificación: Creación del documento.	Clasificación: Uso interno			Pág.:17 de 22

- b) 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.
- c) En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés, sean innecesarias e incluso aquellas que sean inadecuadas al fin que se persigue.
- d) 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.

8.10. Integridad y actualización del sistema.

Todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema, aplicándose el procedimiento de autorización determinado en esta misma política.

Se deberá conocer en todo momento el estado de seguridad de los sistemas, con relación a 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.

8.11. Protección de 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 equipos portátiles, tabletas, dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil.

A este respecto se deberán aplicar las medidas de protección acordes a la clasificación de la información contenidas en estos soportes según se define en el *DC-032 Política de Clasificación de Información*.

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 de seguridad que correspondan a la naturaleza del soporte en que se encuentren.

8.12. Prevención ante otros sistemas de información interconectados

El sistema debe 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 digitales.

Se analizarán los riesgos derivados de la interconexión de los sistemas, a través de redes, con otros sistemas, y se controlará su punto de unión, aplicándose mecanismos basados en controles criptográficos para asegurar la autenticidad de los extremos de la comunicación y la confidencialidad e integridad de la información según se define en la *DC-035 Políticas de Controles Criptográficos*.

8.13. Registro de actividad y detección de código dañino

Para aquellos sistemas y aplicaciones en los que sea necesario registrar la actividad de los usuarios, dicho registro se realizará con la finalidad exclusiva de cumplir los requisitos normativos que sean de aplicación o, si así lo determina la evaluación de riesgos, para garantizar la trazabilidad de los servicios.

	Información Documentada	Código	Fecha	Rev.	Aprobado
	POLÍTICA SEGURIDAD DE LA INFORMACIÓN ENS	DC-052	06/03/2026	01	Dirección
	Modificación: Creación del documento.	Clasificación: Uso interno			Pág.:18 de 22

El registro de actividad se realizará con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales.

Se registran 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.

Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

Al objeto de preservar la seguridad de los sistemas de información, y de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, Numintec podrá, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.

8.14. Incidentes de seguridad

Numintec debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes.

El procedimiento *PR-045 Gestión de Incidentes de Seguridad de la Información* establece el procedimiento de gestión de incidentes de seguridad y de debilidades detectadas en los elementos del sistema de información.

Este procedimiento cubre los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones.

El registro de incidentes se emplea para la mejora continua de la seguridad del sistema.

El proceso es acorde con lo que establece el Artículo 33 del ENS y la *Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad* a fin de que pueda gestionar la comunicación del incidente al CSIRT de referencia, que en este caso es el INCIBE-CERT. Este proceso se llevará a cabo de acuerdo con las indicaciones de la *Guía CCN-STIC-817 Gestión de Ciberincidentes*.

8.15. Continuidad de la actividad

Las medidas de recuperación permitirán la restauración de la información y los servicios que pudieran haberse visto afectados por incidentes disruptivos, de forma que se pueda hacer frente a las situaciones en las que estos incidentes afecten a los activos habituales de tratamiento o a la integridad de la información

Se ha elaborado el documento *DC-015 Plan de Continuidad de la Seguridad de la Información* que contemplan el desarrollo de estrategias de respuesta y recuperación para cada uno de los riesgos de interrupción identificados que permita recuperar las actividades críticas de acuerdo con los objetivos tiempos de recuperación (RTO) y punto de recuperación de los datos (RPO) establecidos según el *DC-049 BIA - Business Impact Analysis*.

	Información Documentada	Código	Fecha	Rev.	Aprobado
	POLÍTICA SEGURIDAD DE LA INFORMACIÓN ENS	DC-052	06/03/2026	01	Dirección
	Modificación: Creación del documento.	Clasificación: Uso interno			Pág.:19 de 22

Asimismo, se contempla la realización de pruebas y ensayos para verificar la viabilidad y adecuación de los procedimientos de recuperación mediante los planes de prueba documentados según los correspondientes planes de continuidad.

8.16. Protección de los datos de carácter personal

Numintec trata datos de carácter personal de acuerdo con los requisitos establecidos por el Reglamento Europeo de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD).

La documentación de los tratamientos y el análisis de los riesgos que se derivan del tratamiento de datos personales se contemplan en la documentación gestionada desde *el área de People and Compliance*.

Organizativamente se ha nominado un Responsable de Protección de Datos y se ha contratado como servicio externo un Delegado de Protección de Datos.

Ciclo de vida de servicios y sistemas.

Las especificaciones de seguridad se incluirán en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.

Asimismo, con el propósito de asegurar que cualquier cambio aplicado a un entorno productivo con un software nuevo o modificado que se instala, sigue un proceso definido, aportando evidencia de documentación, aprobaciones, pruebas, etc., asegurando así los requisitos de control, rentabilidad, calidad y seguridad, se debe aplicar el procedimiento PR-015 *Gestión de Cambios*.

8.17. Mejora continua del proceso de seguridad

El Sistema de Gestión de la Seguridad de la Información será actualizado y mejorado de forma continua, aplicando los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de las tecnologías de la información, por ejemplo, los de la norma ISO 27001:2022

Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a gestión de la seguridad recogidos en el *ID-007 Directrices de Seguridad de la Información*.

9. Cumplimiento de requisitos mínimos

En referencia al artículo 28 del ENS, para dar cumplimiento a los requisitos mínimos establecidos, se aplicarán las medidas de seguridad adecuadas teniendo en cuenta:

- La identificación y valoración de los activos que constituyen el sistema, recogido en el documento *IMP-040 Tabla de Valoración de Activos*.
- La categoría del sistema, determinada como **MEDIA** en el documento *DC-053 Clasificación y Declaración de Aplicabilidad ENS*.
- Las decisiones que se adopten para gestionar los riesgos identificados documentadas en el plan de tratamiento de riesgos.

	Información Documentada	Código	Fecha	Rev.	Aprobado
	POLÍTICA SEGURIDAD DE LA INFORMACIÓN ENS	DC-052	06/03/2026	01	Dirección
	Modificación: Creación del documento.	Clasificación: Uso interno			Pág.:20 de 22

- El tratamiento de datos personales de acuerdo con lo establecido por la legislación vigente en materia de protección de datos personales.
- La selección de las medidas de seguridad de acuerdo con la categoría del sistema y las dimensiones de seguridad relevantes y según se relacionan en el documento *DC-053 Clasificación y Declaración de Aplicabilidad ENS*.
- La aplicación de medidas compensatorias cuando se pueda justificar que protegen igual o mejor el riesgo sobre los activos y se satisfacen los principios básicos y los requisitos mínimos previstos en el ENS.
- Las instrucciones técnicas de seguridad y guías de seguridad publicadas por el Centro Criptológico Nacional en desarrollo de la disposición adicional del ENS.

10. Auditoría de Seguridad

Los sistemas de información dentro del alcance de esta política serán objeto de una auditoría interna regular ordinaria, al menos cada dos años, que verifique el cumplimiento de los requerimientos del ENS.

Con carácter extraordinario, deberá realizarse dicha auditoría siempre que se produzcan modificaciones sustanciales en el sistema de información, que puedan repercutir en las medidas de seguridad requeridas. La realización de la auditoría extraordinaria determinará la fecha de cómputo para el cálculo de los dos años, establecidos para la realización de la siguiente auditoría interna regular ordinaria, indicados en el párrafo anterior.

Esta auditoría se realizará en función de la categoría del sistema, determinada en el documento *DC-053 Declaración de Aplicabilidad ENS*.

El resultado de cada auditoría se recogerá en un informe que deberá ser analizado por el Responsable de Seguridad, quien presentará sus conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

Adicionalmente, dentro del marco de la mejora continua del proceso de seguridad se establece:

- Realización de auditorías internas de cumplimiento anuales, en base a los requisitos de la ENS.
- Realización de auditorías técnicas regulares para la identificación de posibles vulnerabilidades y la verificación de la eficacia de las medidas técnicas implementadas.

11. Sistema de Gestión de la Seguridad de la Información

El Sistema de Gestión de la Seguridad de la Información (SGSI) se implementa aplicando los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de las tecnologías de la información y el proceso de mejora continua, en un modelo PDCA (Plan-Do-Check-Act) Este SGSI se apoya en los aspectos fundamentales:

- Planificación de la seguridad de la información

Desarrollada a partir del Análisis de Riesgos de Seguridad de la Información según se establece en el P01 Procedimiento de Evaluación de Riesgos de Seguridad de la Información y a partir del cual se determinan los controles a implementar (basados en las medidas de seguridad establecidas para el ENS) y el plan de tratamiento de riesgos.

El plan de tratamiento de estos riesgos conlleva la definición de objetivos a fin de minimizar el riesgo residual hasta un valor aceptable.

	Información Documentada	Código	Fecha	Rev.	Aprobado
	POLÍTICA SEGURIDAD DE LA INFORMACIÓN ENS	DC-052	06/03/2026	01	Dirección
	Modificación: Creación del documento.	Clasificación: Uso interno			Pág.:21 de 22

- Implementación, ejecución y operación de los controles de seguridad de la información

Se aplican las medidas de seguridad establecidas por el ENS y documentadas en la Declaración de Aplicabilidad (DC-053 Declaración de Aplicabilidad ENS).

- Medición y supervisión del desempeño de la seguridad de la información

Esta supervisión se lleva a cabo mediante la medición de indicadores que deben aportar métricas que permitan analizar y evaluar el estado de los procesos y medir la efectividad de los controles implementados.

- Identificación de iniciativas de mejora continua

A partir de los resultados de la supervisión del desempeño y de los objetivos de mitigación de riesgos se deben identificar iniciativas de mejora continua (IMS) que permitan corregir las desviaciones detectadas, así como mejorar el desempeño de los controles de seguridad de la información.

Asimismo, contribuirán a estas IMC los resultados de las diferentes auditorías de seguridad, tanto las obligatorias de revisión del sistema (internas y externas) como aquellas auditorías técnicas que se lleven a cabo y que permitan identificar vulnerabilidades y puntos de mejora de las medidas implantadas.

Estas IMC quedarán registradas en el IMP-053 Registro de Iniciativas de Mejora Continua.

12. Proceso de Autorización

El objetivo de este proceso es definir el proceso formal de autorizaciones que cubre todos los elementos de los sistemas de información.

- Utilización de instalaciones, habituales y alternativas.
- Entrada de equipos en producción, en particular, equipos que involucren criptografía.
- Entrada de aplicaciones en producción.
- Establecimiento de enlaces de comunicaciones con otros sistemas.
- Utilización de medios de comunicación, habituales y alternativos.
- Utilización de soportes de información.
- Utilización de equipos móviles. Se entenderá por equipos móviles ordenadores portátiles, PDA, u otros de naturaleza análoga.
- Utilización de servicios de terceros, bajo contrato o Convenio.

La gestión de las autorizaciones se rige por la aplicación de las políticas y procedimientos definidos en cada uno de los ámbitos en los que se requiere su control.

En el caso de que existan políticas definidas, las autorizaciones se otorgarán de forma ordinaria sin que sea necesario un proceso de aprobación formal.

Tipo de Autorización	Proceso
Utilización de instalaciones, habituales y alternativas	Actualmente no se requiere, dado que las actividades se llevan a cabo en modalidad de emplazamiento virtual.
Entrada de equipos en producción, en particular, equipos que involucren criptografía.	De acuerdo con el <i>PR-015 Gestión de Cambios</i> En el caso de que los equipos involucren criptografía se deberá verificar el cumplimiento de <i>DC-035 Política de Controles Criptoográficos</i> .

	Información Documentada	Código	Fecha	Rev.	Aprobado
	POLÍTICA SEGURIDAD DE LA INFORMACIÓN ENS	DC-052	06/03/2026	01	Dirección
	Modificación: Creación del documento.	Clasificación: Uso interno			Pág.:22 de 22

Entrada de aplicaciones en producción.	De acuerdo con el <i>PR-015 Gestión de Cambios</i>
Establecimiento de enlaces de comunicaciones con otros sistemas.	De acuerdo con el <i>PR-015 Gestión de Cambios</i>
Utilización de medios de comunicación, habituales y alternativos	Se realiza una petición que gestionará el área TIC En el caso de que la petición suponga un riesgo para la seguridad de la información se requerirá la autorización del Responsable de Seguridad
Utilización de soportes de información.	En general el uso de soportes de información no está permitido. En caso de que sea necesario su uso se solicitará al área TIC
Utilización de equipos móviles.	El uso de equipos móviles es parte consustancial del desarrollo del trabajo de los empleados por lo que no se requiere ninguna autorización específica.
Utilización de servicios de terceros, bajo contrato o Convenio	Se aplica el <i>DC-036 Política de Seguridad del uso los servicios en la nube.</i>

13. Referencias

13.1. Documentos internos

- Documentación del Sistema de Gestión de Seguridad de la Información de Numintec

13.2. Referencias externas

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Instrucciones técnicas de seguridad y guías de seguridad publicadas por el Centro Criptológico Nacional.
- ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements.