Política de Seguridad de la Información

Versión	Fecha	Redactado por	Control de cambios
1.0	mar23	Matías Roma	Documento inicial.
1.1	oct23	Matías Roma	Simplificación y corrección del documento.
1.2	dic23	Matías Roma	Corrección del alcance y referenciación al ENS.
1.3	nov24	Matías Roma	Simplificación del documento.
2.0	abr26	Iago Docando	Adaptación plantilla política. Ampliación roles. Ampliación principios básicos de seguridad. Renombrar documento, antes: política de seguridad.
2.1	jun26	Verónica Gutiérrez	Ampliación de roles y responsabilidades en aspectos de IA. Ampliación Información relacionada. Ampliación Medidas Compensatorias.
2.2	ago26	Verónica Gutiérrez	Se amplía el apartado 6 para incorporar los principios básicos del ENS y los requisitos mínimos del artículo 12.6 del RD 311/2022

1 Objetivo 2
2 Vigencia y revisión 3
3 Alcance y excepciones 3
4 Marco normativo y metodológico 3
5 Roles y responsabilidades 4
5.1 Medidas compensatorias en la diferenciación de responsabilidades 5
6 Principios generales de seguridad de la información 5
6.1 Principios básicos y requisitos mínimos del ENS 6
6.1.1 Principios básicos ENS 6
6.1.2 Requisitos mínimos ENS 6
7 Compromiso de la Dirección 6
8 Designación de roles 7
9 Resolución de conflictos 7
10 Gestión de riesgos 7
11 Uso de Inteligencia Artificial (IA) 7
12 Documentación relacionada 8

1 Objetivo

La presente Política de Seguridad de la Información establece los principios, directrices, responsabilidades y criterios generales para proteger la información y los servicios gestionados por Landra Sistemas, asegurando su confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

Esta política tiene como finalidad garantizar una gestión adecuada de la seguridad de la información, conforme a las obligaciones legales, contractuales y normativas, en particular las derivadas de la ISO/IEC 27001:2022, el Esquema Nacional de Seguridad (RD 311/2022) y el resto de los requisitos aplicables, proporcionando un marco común de actuación para todo el personal y terceros relacionados.

2 Vigencia y revisión

Este documento estará vigente desde la fecha de su aprobación y hasta que sea sustituido por una nueva versión debidamente autorizada. La aprobación debe quedar reflejada mediante firma visible en el cajetín de versiones de la portada.

La política será revisada al menos una vez al año, y adicionalmente cuando se produzcan:

- Cambios significativos en el contexto interno o externo de la organización.
- Cambios relevantes en los sistemas de información o en los servicios prestados.
- Modificaciones en la normativa aplicable.
- Incidentes graves de seguridad de la información.

3 Alcance y excepciones

Esta política se aplica a:

- Todo el personal de Landra Sistemas.
- Los sistemas de información, activos, datos y servicios incluidos en el alcance del SGSI.
- Los proveedores y terceros que accedan, gestionen o traten información o sistemas de la organización.

Los sistemas incluidos en el alcance del ENS dispondrán de una categorización formal conforme a la normativa vigente, que determinará los requisitos de seguridad aplicables.

Las excepciones a esta política deberán ser justificadas, documentadas, evaluadas desde el punto de vista del riesgo y aprobadas explícitamente por el Resp. de Seguridad.

4 Marco normativo y metodológico

La gestión de la seguridad de la información se realiza conforme a:

- ISO/IEC 27001:2022, Sistemas de Gestión de la Seguridad de la Información.
- Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad.
- Guías de Seguridad CCN-STIC aplicables, incluyendo CCN-STIC-801 sobre Inteligencia Artificial.

- Legislación vigente sobre de protección de datos personales y seguridad de la información.
- Políticas, procedimientos e instrucciones internas aprobadas por la organización.

5 Roles y responsabilidades

Comité de Seguridad *(en conjunto)*	Órgano encargado de coordinar, supervisar y controlar la gestión de la seguridad de la información en la organización. Con separación de tareas para cada rol.
Resp del Sistema	**Aprobar esta política y sus revisiones.** Garantizar que los sistemas de información disponen de los recursos necesarios para cumplir los requisitos de seguridad. Resolver conflictos necesidades de negocio / requisitos de seguridad. Responsabilidad última sobre la seguridad del sistema de información. Impulsar la mejora continua del sistema de gestión de seguridad.
Resp de Seguridad	Proponer, mantener y actualizar esta política. Mantener la Declaración de Aplicabilidad del ENS. Coordinar la implantación del ENS y del SGSI. Supervisar el proceso de gestión de riesgos y validar sus resultados. Coordinar la gestión de incidentes de seguridad y elevar los más graves al Comité / Dirección. Promover acciones de formación y concienciación en seguridad. Analizar los resultados de auditorías internas y externas y proponer acciones correctivas. Definir y supervisar criterios de uso seguro de herramientas de Inteligencia Artificial en el marco del SGSI. En particular: ▫ Identificar, analizar y gestionar los riesgos específicos derivados del uso de sistemas de Inteligencia Artificial. ▫ Supervisar el uso de herramientas de IA, garantizando la protección de la información y el cumplimiento de la normativa aplicable. ▫ Evaluar los riesgos asociados al uso de datos en sistemas de IA, incluyendo posibles fugas de información o uso indebido. ▫ Garantizar la alineación con las guías CCN-STIC aplicables.
Resp del Servicio	Determinar los requisitos de seguridad de los servicios prestados. Asegurar que los servicios cumplen los niveles de seguridad exigidos. Valorar el impacto de incidentes de seguridad sobre la prestación del servicio. Coordinar necesidades de continuidad del servicio. Participar en el análisis de riesgos desde la perspectiva del servicio.
Resp de la Información	Determinar los requisitos de seguridad de la información. Clasificar la información conforme a criterios establecidos. Autorizar el acceso a la información y revisar permisos periódicamente. Valorar el impacto de incidentes de seguridad de la información. Participar en el análisis y tratamiento de riesgos de la información.
Técnicos Sistemas **	Implantar y operar las medidas de seguridad aprobadas. Garantizar el correcto funcionamiento de los controles de seguridad. Gestionar los cambios en los sistemas de información conforme a los procedimientos establecidos.

	Detectar y notificar incidentes de seguridad. Mantener la trazabilidad y los registros de actividad requeridos.
Dpto Calidad y/o de Cumplimiento **	Asegurar la coherencia documental del SGSI. Coordinar auditorías internas y dar soporte a auditorías externas. Verificar el cumplimiento de los requisitos normativos y contractuales. Control de versiones, revisiones y aprobaciones de la documentación. Soporte al Comité en el seguimiento de acciones correctivas / mejoras.
Resto de personal	Cumplir la política, aplicar las medidas de seguridad establecidas y comunicar cualquier incidente o vulnerabilidad detectada.

** En ausencia de estos roles estas responsabilidades serán cubiertas por el Resp del Sistema (técnicos sistemas) y por los Resp del Servicio y de la Información (calidad/cumplimiento).

5.1 Medidas compensatorias en la diferenciación de responsabilidades

En cumplimiento del principio de diferenciación de responsabilidades establecido en el artículo 11 del ENS, se establece la separación entre el Responsable de Seguridad y el Responsable del Sistema.

Dado que, dentro de la estructura organizativa, puede existir una relación jerárquica entre estos roles, la organización establece medidas compensatorias para garantizar su independencia funcional, conforme a lo requerido por el ENS.

En el seno del Comité de Seguridad, las decisiones se adoptan de manera conjunta, sin jerarquías operativas entre los miembros, valorando cada uno su ámbito de responsabilidad. Este comité actúa como órgano de supervisión y validación de las decisiones relevantes en materia de seguridad de la información.

Las decisiones adoptadas quedarán registradas, garantizando su trazabilidad y revisión posterior en el marco de las revisiones por la Dirección. Ninguno de los roles podrá validar unilateralmente decisiones que afecten directamente a sus propias funciones de control o supervisión, requiriéndose su revisión y conformidad por el Comité de Seguridad.

6 Principios generales de seguridad de la información

La seguridad de la información en Landra Sistemas se basa en los siguientes principios generales:

- **Cumplimiento normativo.** Asegurando el respeto a la legislación y normas aplicables.
- **Personas en el centro.** Priorizar incidentes con impacto personal sobre los que no los tengan.
- **Enfoque holístico** considerando las dimensiones de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.
- **Uso responsable de Inteligencia Artificial.** El uso de sistemas de IA deberá realizarse garantizando la seguridad de la información, evitando riesgos asociados a sesgos, fugas de información, uso indebido de datos y falta de control sobre los resultados generados. Todas estas consideraciones se recogerán en una política específica, sobre el uso permitido de IA en la organización.
- **Responsabilidad compartida.** Cada persona es responsable de la seguridad en su ámbito de actuación, sea este mayor o menor, y de notificar desviaciones que pueda detectar.

- **Seguridad en terceros.** Los proveedores y terceros con acceso a información o sistemas estarán sujetos a requisitos de seguridad proporcionales al riesgo de los servicios prestados.
- **Formación / Concienciación.** Periódicamente en función de requisitos de cada rol.

6.1 Principios básicos y requisitos mínimos del ENS

Asimismo, la seguridad de la información se fundamenta en los principios básicos establecidos en el Capítulo II del Real Decreto 311/2022 y se desarrolla mediante la aplicación de los requisitos mínimos de seguridad definidos en su artículo 12.

6.1.1 Principios básicos ENS

- **Seguridad como proceso integral**, entendiendo la seguridad como un proceso permanente que integra elementos humanos, técnicos, jurídicos y organizativos relacionados con los sistemas de información.
- **Gestión de la seguridad basada en los riesgos,** aplicando medidas proporcionadas a la naturaleza de la información tratada, los servicios prestados y los riesgos identificados.
- **Prevención, detección, respuesta y conservación**, estableciendo medidas orientadas a evitar incidentes, detectarlos, responder ante ellos y preservar la información y los servicios.
- **Existencia de líneas de defensa**, mediante medidas organizativas, físicas y lógicas que permitan reducir la probabilidad de compromiso del sistema y minimizar su impacto.
- **Vigilancia continua**, orientada a detectar actividades o comportamientos anómalos y facilitar una respuesta oportuna.
- **Reevaluación periódica**, revisando y actualizando las medidas de seguridad conforme evolucionen los riesgos, los sistemas y las amenazas.
- **Diferenciación de responsabilidades**, separando las funciones de responsabilidad sobre la información, los servicios, la seguridad y los sistemas, conforme a lo establecido en el ENS.

6.1.2 Requisitos mínimos ENS

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

La organización desarrollará estos requisitos mínimos mediante políticas, normas, procedimientos, controles, registros y evidencias que formarán parte del SGSI y del sistema de gestión ENS, garantizando su aplicación efectiva y verificable.

7 Compromiso de la Dirección

La Dirección de Landra Sistemas manifiesta su compromiso expreso con la seguridad de la información, apoyando la implantación, mantenimiento y mejora continua del SGSI, y promoviendo una cultura de seguridad alineada con los objetivos estratégicos de la organización.

Este compromiso incluye la asignación de recursos adecuados, la formación y concienciación del personal y el respaldo a las decisiones necesarias para proteger la información y los servicios.

8 Designación de roles

- Todos los roles son nombrados por la Dirección.
- El Responsable de Seguridad es nombrado por la Dirección a propuesta del resto de roles del Comité.
- Todos los roles reportan al Comité de Seguridad, y éste a Dirección.
- Habrá evidencia registrada de aceptación del nombramiento.
- Los nombramientos se revisarán anualmente (revisión de la dirección) o cuando haya algún cambio que lo justifique.

9 Resolución de conflictos

En caso de conflictos / dudas sobre a quién le corresponde una responsabilidad específica, hasta dónde llega el alcance de una determinada responsabilidad, detalles sobre en qué consiste una tarea, etc. se trasladarán al comité para su análisis.

El Comité escuchará a todas las partes interesadas por separado, buscará a mayores evidencias neutrales y objetivas, y dictaminará una resolución que será comunicada a dichas partes.

10 Gestión de riesgos

Todos los sistemas de información regulados por esta política deberán contar con un análisis de riesgos específico y documentado, siempre ajustado a la complejidad y criticidad de cada sistema.

Cuanto mayor sea la complejidad o el impacto crítico del sistema, mayor debe ser el nivel de formalidad, exhaustividad y trazabilidad en el análisis realizado.

Una Política de Gestión de Riesgos de Seguridad de la Información establecerá los detalles de la gestión. En ausencia de dicha política, como mínimo se deberán observar los principios de la metodología Magerit.

11 Uso de Inteligencia Artificial (IA)

La organización regula el uso de sistemas de Inteligencia Artificial en el marco del SGSI, con el objetivo de garantizar la seguridad de la información, la protección de datos y el cumplimiento normativo.

Se establecen los siguientes principios:

- El uso de herramientas de IA deberá evaluarse previamente desde el punto de vista del riesgo.
- No está permitido introducir información sensible en sistemas de IA externos sin autorización.
- Se garantizará la supervisión humana en los procesos donde la IA tenga impacto relevante.
- Se identificarán y gestionarán los riesgos derivados del uso de IA, incluyendo posibles fugas de información o resultados no confiables.
- El Responsable de Seguridad supervisará la adopción y uso de la IA conforme a las guías CCN-STIC aplicables.

12 Documentación relacionada

La presente política establece el marco general de actuación en materia de seguridad y se desarrolla mediante un conjunto de políticas, normas, procedimientos e instrucciones que conforman el Sistema de Gestión de la Seguridad de la Información (SGSI) de la organización.

En cumplimiento de lo establecido en el Esquema Nacional de Seguridad (RD 311/2022), esta política se complementa con la normativa interna que desarrolla los requisitos mínimos de seguridad, incluyendo entre otros:

- Política de Gestión de Riesgos de Seguridad de la Información.
- Declaración de Aplicabilidad (SoA).
- Procedimientos de gestión de incidentes de seguridad.
- Procedimientos de control de accesos e identidades.
- Normativa y criterios de clasificación de la información.
- Normativa de uso aceptable de los sistemas de información.
- Procedimientos de gestión de cambios.
- Planes de continuidad de negocio y recuperación ante desastres.
- Normativa de seguridad aplicable a proveedores y terceros.
- Procedimientos de auditoría interna y seguimiento del SGSI.

Esta documentación será gestionada de forma controlada, garantizando su coherencia con la presente política, su actualización periódica y su disponibilidad para el personal autorizado.