

	Política de Seguridad de la Información	Fecha	13/04/2026
		Versión	2.0

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

Responsable: Resp de Seguridad	Clasificación: Interno	Aprobado por: Resp del Sistema
--	----------------------------------	--

	Política de Seguridad de la Información	Fecha	13/04/2026
		Versión	2.0

1	Objetivo.....	2
2	Vigencia y revisión.....	3
3	Alcance y excepciones.....	3
4	Marco normativo y metodológico	3
5	Roles y responsabilidades	3
6	Principios generales de seguridad de la información	4
7	Compromiso de la Dirección	5
8	Designación de roles	5
9	Resolución de conflictos	5
10	Gestión de riesgos	5

Responsable: Resp de Seguridad	Clasificación: Interno	Aprobado por: Resp del Sistema
--	----------------------------------	--

	Política de Seguridad de la Información	Fecha	13/04/2026
		Versión	2.0

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

Responsable: Resp de Seguridad	Clasificación: Interno	Aprobado por: Resp del Sistema
--	----------------------------------	--

	Política de Seguridad de la Información	Fecha	13/04/2026
		Versión	2.0

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	<p>Aprobar esta política y sus revisiones.</p> <p>Garantizar que los sistemas de información disponen de los recursos necesarios para cumplir los requisitos de seguridad.</p> <p>Resolver conflictos necesidades de negocio / requisitos de seguridad.</p> <p>Responsabilidad última sobre la seguridad del sistema de información.</p> <p>Impulsar la mejora continua del sistema de gestión de seguridad.</p>
Resp de Seguridad	<p>Proponer, mantener y actualizar esta política</p> <p>Mantener la Declaración de Aplicabilidad del ENS.</p> <p>Coordinar la implantación del ENS y del SGSI.</p> <p>Supervisar el proceso de gestión de riesgos y validar sus resultados.</p> <p>Coordinar la gestión de incidentes de seguridad y elevar los más graves al Comité / Dirección.</p> <p>Promover acciones de formación y concienciación en seguridad.</p> <p>Analizar los resultados de auditorías internas y externas y proponer acciones correctivas.</p>
Resp del Servicio	<p>Determinar los requisitos de seguridad de los servicios prestados.</p> <p>Asegurar que los servicios cumplen los niveles de seguridad exigidos.</p> <p>Valorar el impacto de incidentes de seguridad sobre la prestación del servicio.</p> <p>Coordinar necesidades de continuidad del servicio</p> <p>Participar en el análisis de riesgos desde la perspectiva del servicio.</p>
Resp de la Información	<p>Determinar los requisitos de seguridad de la información</p> <p>Clasificar la información conforme a criterios establecidos.</p> <p>Autorizar el acceso a la información y revisar permisos periódicamente.</p> <p>Valorar el impacto de incidentes de seguridad de la información.</p> <p>Participar en el análisis y tratamiento de riesgos de la información.</p>
Técnicos Sistemas **	<p>Implantar y operar las medidas de seguridad aprobadas.</p> <p>Garantizar el correcto funcionamiento de los controles de seguridad.</p> <p>Gestionar los cambios en los sistemas de información conforme a los procedimientos establecidos.</p> <p>Detectar y notificar incidentes de seguridad.</p> <p>Mantener la trazabilidad y los registros de actividad requeridos.</p>
Dpto Calidad y/o de Cumplimiento **	<p>Asegurar la coherencia documental del SGSI.</p> <p>Coordinar auditorías internas y dar soporte a auditorías externas.</p> <p>Verificar el cumplimiento de los requisitos normativos y contractuales.</p> <p>Control de versiones, revisiones y aprobaciones de la documentación.</p> <p>Soporte al Comité en el seguimiento de acciones correctivas / mejoras.</p>
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)

Responsable: Resp de Seguridad	Clasificación: Interno	Aprobado por: Resp del Sistema
--	----------------------------------	--

	Política de Seguridad de la Información	Fecha	13/04/2026
		Versión	2.0

6 Principios generales de seguridad de la información

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

- **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** sobre las 5 dimensiones de la seguridad: Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad.
- **Gestión proporcional.** Medidas adecuadas al nivel de riesgo identificado.
- **Prevención.** Priorizar medidas que eviten incidentes en la medida de lo posible.
- **Mejora continua,** revisando y perfeccionando el SGSI de forma sistemática.
- **Definición clara de responsabilidades.**
- **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.
- **Formación / Concienciación.** Periódicamente en función de requisitos de cada rol.

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 resp 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.

Responsable: Resp de Seguridad	Clasificación: Interno	Aprobado por: Resp del Sistema
--	----------------------------------	--

	Política de Seguridad de la Información	Fecha	13/04/2026
		Versión	2.0

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.

Responsable: Resp de Seguridad	Clasificación: Interno	Aprobado por: Resp del Sistema
--	----------------------------------	--