POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN ENS

Destrupaper SL - Sistema de Información ENS de categoría media

Documento	Política de Seguridad de la Información ENS	Edición	02
Fecha	21/05/2026	**Clasificación**	Uso público
Propietario	Dirección de Destrupaper	**Ámbito**	ENS - Nivel medio
Aprobación	Dirección / Comité de Seguridad	**Revisión**	Anual o por cambio relevante
Custodia	Repositorio corporativo autorizado	**Estado**	Vigente

Compromiso de Dirección

La Dirección de Destrupaper asume la seguridad de la información como una condición necesaria para la prestación de sus servicios, para la protección de la información de clientes y para el cumplimiento del Esquema Nacional de Seguridad.

Control de revisiones y aprobación

Versión	Cambios realizados	Fecha	Redactor / Revisor	Aprobador
01	Registro inicial de la política ENS	30/01/2024	Responsable del Sistema	Dirección
02	Actualización completa conforme al RD 311/2022, refuerzo de roles, alcance, gobierno, gestión de riesgos, proveedores, incidentes, continuidad, métricas y auditoría. Eliminación de referencias ajenas a Destrupaper.	21/05/2026	Responsable de Seguridad / Comité de Seguridad	Dirección

Índice orientativo

1. Objeto

La presente Política de Seguridad de la Información establece el marco general de gobierno, gestión y protección de la información de Destrupaper SL, en coherencia con el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, y con el resto de normativa aplicable a la organización.

La política define los principios, responsabilidades, órganos de gobierno, requisitos mínimos, estructura documental y mecanismos de revisión que deben aplicarse al sistema de información incluido en el alcance ENS. Su finalidad es asegurar que la información y los servicios se gestionan con niveles adecuados de confidencialidad, integridad, trazabilidad, autenticidad y disponibilidad.

2. Alcance

El alcance de esta política comprende los activos, servicios, personas, proveedores, instalaciones, sistemas, comunicaciones y repositorios de información que participan en la prestación de los servicios de Destrupaper sujetos al Esquema Nacional de Seguridad en categoría media.

- Puestos de trabajo, equipos portátiles o de sobremesa y dispositivos auxiliares empleados por la organización.
- Repositorios corporativos, carpetas compartidas y servicios en la nube utilizados para el almacenamiento y tratamiento de información.
- Servicios de comunicaciones, seguridad endpoint, hosting web y otros proveedores que soporten servicios dentro del alcance.
- Documentación, registros, evidencias y procedimientos que componen el sistema documental ENS.
- Información de clientes, proveedores, empleados y terceros tratada durante la prestación del servicio.

Criterio de alcance

Cualquier nuevo servicio, sistema, proveedor o tratamiento de información que pueda afectar al alcance ENS se evaluará antes de su puesta en servicio y se incorporará al análisis de riesgos, inventario, categorización y Declaración de Aplicabilidad cuando corresponda.

3. Compromiso de Dirección y objetivos

Destrupaper, como empresa dedicada a la destrucción de documentación confidencial, asume el compromiso de proteger la información que trata y de prestar sus servicios con garantías adecuadas de seguridad. La Dirección proporciona los recursos necesarios, impulsa la mejora continua y exige el cumplimiento de esta política a empleados, colaboradores y proveedores que participen en el sistema.

3.1. Objetivos de seguridad

- Garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información y de los servicios soportados por el sistema.
- Prevenir incidentes de seguridad en la medida que resulte técnica, organizativa y económicamente viable.
- Detectar, gestionar y comunicar los incidentes de seguridad de forma eficaz y proporcional al impacto.
- Asegurar la recuperación de la información y la continuidad de los servicios ante contingencias, errores operativos o indisponibilidades.
- Mantener un sistema documental ordenado, actualizado y trazable, que permita demostrar el cumplimiento del ENS.

- Mejorar de forma continua la seguridad mediante análisis de riesgos, auditorías, indicadores, acciones correctivas y revisiones periódicas.
- Cumplir la legislación aplicable, los requisitos contractuales y los compromisos asumidos con clientes, administraciones públicas y otras partes interesadas.

4. Principios básicos del ENS

La seguridad de la información en Destrupaper se rige por los principios básicos del Esquema Nacional de Seguridad. Estos principios son de aplicación a las decisiones técnicas, organizativas y documentales adoptadas sobre el sistema.

Principio	Aplicación en Destrupaper
Seguridad integral	La seguridad se considera de forma global, incluyendo personas, procesos, tecnología, instalaciones, proveedores y documentación.
Gestión de riesgos	Las medidas de seguridad se seleccionan y mantienen en función de los riesgos identificados y de la categoría del sistema.
Prevención, detección, respuesta y conservación	El sistema incorpora medidas para prevenir incidentes, detectar eventos, responder de forma ordenada y conservar evidencias.
Líneas de defensa	La protección se estructura en medidas organizativas, operacionales y técnicas que actúan de forma complementaria.
Vigilancia continua	La organización revisa eventos, indicadores, vulnerabilidades, cambios y evidencias de seguridad.
Reevaluación periódica	La política, los riesgos, la Declaración de Aplicabilidad y las evidencias se revisan periódicamente y ante cambios relevantes.
Diferenciación de responsabilidades	Los roles de seguridad están definidos, documentados y coordinados mediante el Comité de Seguridad.
Proporcionalidad	Las medidas se aplican de forma proporcionada al nivel de riesgo, categoría del sistema, impacto en los servicios y naturaleza de la información tratada.

5. Requisitos mínimos de seguridad

La organización aplica los requisitos mínimos del ENS como marco de referencia para establecer, mantener y evidenciar sus medidas de seguridad. Estos requisitos se desarrollan mediante políticas, procedimientos, registros, evidencias técnicas y controles operativos.

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

6. Marco legal y regulatorio

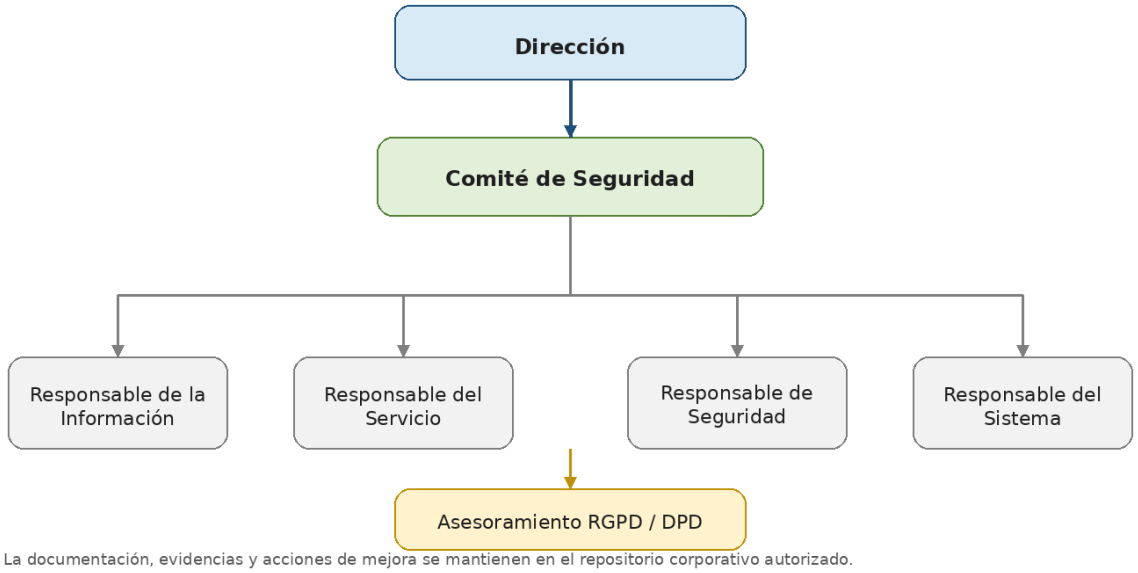
El sistema de seguridad de la información se mantiene conforme al marco legal y regulatorio aplicable a la actividad de Destrupaper. La relación de normativa aplicable se conserva en el sistema documental y se revisa cuando se produzcan cambios legales, contractuales o de alcance.

- Reglamento (UE) 2016/679, General de Protección de Datos (RGPD).

- Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Instrucciones Técnicas de Seguridad aplicables al ENS, incluyendo conformidad, auditoría, informe del estado de la seguridad y notificación de incidentes.
- Guías CCN-STIC aplicables al alcance del sistema, especialmente las relativas a categorización, análisis de riesgos, Declaración de Aplicabilidad, criptografía, incidentes, continuidad, interconexiones y medidas de protección.
- Reglamento (UE) 910/2014 eIDAS y Ley 6/2020, cuando se utilicen certificados electrónicos o servicios de confianza.
- Ley 34/2002, de servicios de la sociedad de la información y comercio electrónico, cuando resulte aplicable.
- Normativa de propiedad intelectual, prevención de riesgos laborales, contratación, confidencialidad y obligaciones contractuales asumidas con clientes y proveedores.

7. Gobierno de la seguridad y roles ENS

Mapa de gobierno de seguridad ENS



La documentación, evidencias y acciones de mejora se mantienen en el repositorio corporativo autorizado.

Rol / función	Responsabilidades
Dirección	Aprueba la política, proporciona recursos, lidera el sistema de seguridad, valida las decisiones estratégicas y promueve la mejora continua.
Responsable de la Información	Determina los requisitos de seguridad de la información tratada, participa en la valoración de las dimensiones CITAD y autoriza criterios de uso, clasificación y protección.
Responsable del Servicio	Determina los requisitos de seguridad de los servicios prestados, participa en la valoración del impacto y coordina la continuidad y calidad del servicio.
Responsable de Seguridad	Supervisa el cumplimiento de esta política, propone medidas de seguridad, coordina la gestión de riesgos, impulsa auditorías, revisa evidencias y valida la Declaración de Aplicabilidad.
Responsable del Sistema	Implanta, opera y mantiene las medidas técnicas y organizativas sobre los sistemas, redes, equipos, copias, accesos, registros y servicios tecnológicos.

Rol / función	Responsabilidades
Delegado o asesor de protección de datos	Asesora en los aspectos relacionados con datos personales, RAT, ejercicio de derechos, brechas de seguridad y coordinación con la normativa de protección de datos.
Usuarios y colaboradores	Cumplen las normas de uso, protegen las credenciales, notifican incidentes, usan los recursos autorizados y tratan la información conforme a su clasificación y necesidad de acceso.
Proveedores	Cumplen las condiciones contractuales, medidas de seguridad, confidencialidad, niveles de servicio y procedimientos de coordinación establecidos por Destrupaper.

8. Comité de Seguridad

El Comité de Seguridad es el órgano de coordinación y seguimiento de la seguridad de la información. Está integrado, al menos, por Dirección, Responsable de la Información, Responsable del Servicio, Responsable de Seguridad y Responsable del Sistema. El Delegado o asesor de protección de datos participa cuando los asuntos tratados afecten a datos personales.

8.1. Funciones del Comité

- Aprobar y revisar la Política de Seguridad de la Información y su desarrollo documental.
- Ratificar la designación, renovación o cese de los roles ENS.
- Revisar la categorización del sistema y la valoración de las dimensiones CITAD.
- Aprobar criterios de tratamiento de riesgos, medidas compensatorias o medidas complementarias de vigilancia.
- Supervisar la Declaración de Aplicabilidad y el estado de implantación de las medidas ENS.
- Revisar incidentes significativos, resultados de auditoría, acciones correctivas e indicadores de seguridad.
- Impulsar la formación, concienciación y mejora continua del sistema.

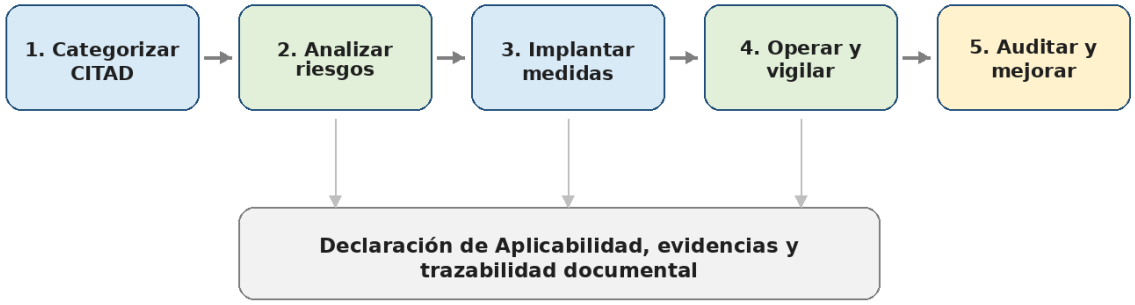
El Comité se reunirá con periodicidad mínima anual y siempre que se produzcan cambios relevantes en el alcance, riesgos, servicios, proveedores, incidentes de impacto o resultados de auditoría que lo aconsejen. Las decisiones se documentarán mediante actas, registros o evidencias equivalentes conservadas en el repositorio corporativo autorizado.

9. Gestión de riesgos, categorización y Declaración de Aplicabilidad

Destrupaper mantiene un proceso de análisis y gestión de riesgos que permite identificar amenazas, vulnerabilidades, impactos, riesgos inherentes y riesgos residuales sobre la información y servicios incluidos en el alcance. Las decisiones de tratamiento se documentan, revisan y se vinculan con las medidas de seguridad implantadas.

- La categorización del sistema se realiza conforme al Anexo I del ENS, valorando confidencialidad, integridad, trazabilidad, autenticidad y disponibilidad.
- La categoría resultante condiciona la selección de medidas del Anexo II del ENS y sus refuerzos aplicables.
- La Declaración de Aplicabilidad identifica para cada medida su aplicabilidad, justificación, evidencias asociadas y estado de implantación.
- Las medidas no aplicables se justifican de forma expresa en función del alcance, arquitectura, servicios o ausencia de determinada funcionalidad.
- El análisis de riesgos se revisa, como mínimo, anualmente y cuando se produzcan cambios relevantes en activos, proveedores, servicios, tecnología o amenazas.

Ciclo de gestión de la seguridad ENS



La política se revisa periódicamente y ante cambios relevantes en alcance, riesgos, servicios, proveedores, evidencias o normativa.

10. Organización documental del sistema

El sistema documental de seguridad de la información se estructura en políticas, normas, procedimientos, instrucciones técnicas, registros y evidencias. La documentación se conserva en repositorios corporativos autorizados, con control de acceso según perfiles, trazabilidad de cambios y revisión periódica.

La documentación disponible en el repositorio de Destrupaper incluye, entre otros, la Política de Seguridad de la Información ENS, acta de constitución del Comité de Seguridad y nombramiento de responsables, comunicación de política y normativa a empleados, Declaración de Aplicabilidad, normativa, procedimientos, evidencias ENS, métricas e indicadores, política de copias de seguridad, política de gestión de contraseñas, política de gestión de incidentes, política de encriptación, política de uso de correo electrónico e instrucciones técnicas de gestión de accesos, comunicaciones, incidentes y tratamiento de riesgos.

Tipo de documento	Contenido y finalidad
Políticas	Política de Seguridad de la Información ENS; políticas de copias de seguridad, contraseñas, incidentes, encriptación, correo electrónico, eliminación y destrucción.
Normativa e instrucciones	Normativa de seguridad e instrucciones técnicas de gestión de accesos, comunicaciones, incidentes, clasificación y tratamiento de riesgos.
Procedimientos	Procedimientos de control de acceso, gestión de cambios, gestión de incidentes, copias de seguridad, proveedores y continuidad.
Registros y evidencias	Inventario, matriz de accesos, actas, revisiones, métricas, auditorías, evidencias técnicas, registros de incidentes, copias y restauraciones.
Declaración de Aplicabilidad	Relación de medidas ENS, aplicabilidad, justificación, evidencias, medidas compensatorias y observaciones de seguimiento.

11. Control de acceso y uso de los sistemas

El acceso a la información y a los sistemas de Destrupaper se concede conforme al principio de necesidad de conocer, mínimo privilegio y segregación de funciones. Todo usuario debe estar identificado, autorizado y vinculado a un perfil de acceso coherente con sus responsabilidades.

- Las altas, modificaciones y bajas de usuarios se documentan y autorizan por el responsable correspondiente.

- Los accesos se revisan periódicamente y se ajustan cuando cambien las funciones, relación laboral, proveedor o necesidad de acceso.
- Los usuarios protegen sus credenciales y no las comparten con terceros.
- Los puestos de trabajo se bloquean tras un periodo de inactividad y requieren autenticación para reanudar la sesión.
- Las carpetas compartidas y SharePoint se configuran con permisos por usuario o grupo, evitando accesos innecesarios.
- Los accesos de terceros se limitan al servicio contratado, se documentan y se revocan cuando dejan de ser necesarios.

12. Protección de equipos, comunicaciones y servicios

Los equipos, comunicaciones y servicios incluidos en el alcance se protegen mediante medidas técnicas y organizativas proporcionadas al riesgo. La organización mantiene inventario de activos, control de configuración, protección endpoint, mecanismos de filtrado, control de dispositivos, actualización de sistemas y seguimiento de incidencias técnicas.

12.1. Equipos y dispositivos

- Los puestos de trabajo y dispositivos conectados se identifican en inventario y se asignan a un responsable.
- La protección endpoint se mantiene activa y actualizada en los equipos dentro del alcance.
- Las impresoras y dispositivos multifunción se configuran con criterios de seguridad, control de acceso e impresión protegida cuando traten información sensible.
- Los dispositivos con capacidad de almacenamiento permiten la eliminación de trabajos o información retenida cuando resulte necesario.
- Los equipos portátiles, si existen dentro del alcance, se protegen mediante cifrado, control de acceso, inventario y procedimiento de pérdida o robo.

12.2. Comunicaciones y perímetro

- Las comunicaciones externas se realizan mediante canales seguros, especialmente HTTPS/TLS para servicios cloud y SharePoint.
- Los controles de filtrado, router, firewall de sistema operativo y protección endpoint se documentan como mecanismos de protección del perímetro lógico.
- La separación de flujos se gestiona mediante permisos, carpetas compartidas, controles de acceso y mecanismos de red disponibles.
- Los servicios web y hosting se mantienen bajo condiciones de servicio, soporte, certificado TLS y controles de seguridad del proveedor.
- El proveedor de comunicaciones se considera relevante para la continuidad y disponibilidad del sistema y se gestiona mediante relación contractual, contacto de soporte y nivel de servicio aplicable.

13. Proveedores y servicios externos

Los proveedores que prestan servicios dentro del alcance ENS se identifican, clasifican y gestionan en función de la criticidad del servicio que soportan. La relación de proveedores incluye servicios de comunicaciones, hosting web, servicios cloud, seguridad endpoint, soporte tecnológico y otros servicios que puedan afectar a la seguridad del sistema.

- Los proveedores críticos disponen de responsable interno, punto de contacto, condiciones de servicio y mecanismo de seguimiento.
- Los contratos, condiciones o acuerdos deben contemplar confidencialidad, disponibilidad, soporte, gestión de incidencias y responsabilidades de seguridad.

- Los proveedores cloud o de seguridad aportan, cuando corresponda, certificaciones, documentación de cumplimiento o garantías equivalentes.
- Las incidencias de proveedores se registran y se siguen hasta su cierre.
- El uso de servicios externos se revisa cuando cambien proveedor, alcance, ubicación de datos, nivel de servicio o medidas de seguridad.

14. Protección de datos personales

Cuando el sistema trate datos personales, Destrupaper aplicará los requisitos del RGPD, la LOPDGDD y la normativa ENS. El Responsable de Seguridad coordinará con el Delegado o asesor de protección de datos la identificación de requisitos, análisis de riesgos, medidas de seguridad, gestión de brechas y evidencias de cumplimiento.

- Se mantiene un Registro de Actividades de Tratamiento acorde con los tratamientos reales.
- Los tratamientos se evalúan en función de su finalidad, base jurídica, categorías de datos, destinatarios, plazos de conservación y medidas de seguridad.
- Las brechas de seguridad que afecten a datos personales se evalúan y comunican conforme al procedimiento aplicable.
- Se informa a los interesados y se atienden los derechos de protección de datos por los cauces establecidos.
- Los contratos con encargados del tratamiento incluyen obligaciones de seguridad, confidencialidad y colaboración.

15. Continuidad, copias de seguridad y recuperación

Destrupaper mantiene medidas de continuidad y recuperación para asegurar la disponibilidad de la información y de los servicios relevantes. Las copias de seguridad se realizan conforme al procedimiento establecido y se orientan a recuperar información ante pérdida accidental, error operativo, indisponibilidad del equipo origen o incidente de seguridad.

- El procedimiento de copias identifica información respaldada, origen, destino, frecuencia, responsable, retención y controles de acceso.
- Cuando se utilicen repositorios corporativos en la nube, se aplican permisos de acceso y controles de trazabilidad sobre las carpetas compartidas.
- Las restauraciones se prueban periódicamente y se documenta el resultado para acreditar la recuperabilidad de la información.
- Los medios de respaldo eléctrico, como SAI, se identifican y se documentan para facilitar la continuidad básica y la parada ordenada de equipos.
- El BIA y los objetivos de recuperación, cuando estén definidos, se revisan para mantener coherencia con el modelo de copias y continuidad.

16. Gestión de incidentes, vulnerabilidades y cambios

La organización mantiene procedimientos para registrar, clasificar, analizar, comunicar y resolver incidentes de seguridad. Los incidentes se documentan con su impacto, acciones realizadas, responsables, tiempos de resolución y lecciones aprendidas.

- Los usuarios comunican incidentes, sospechas, pérdidas, accesos no autorizados o comportamientos anómalos por los canales establecidos.
- El Responsable de Seguridad evalúa los incidentes y coordina su tratamiento con el Responsable del Sistema y, cuando proceda, con proveedores o asesor de protección de datos.

- Los cambios en sistemas, proveedores, configuraciones, servicios, equipos o repositorios se registran, evalúan y aprueban antes de su implantación.
- La organización conserva evidencias de parches, actualizaciones, mantenimiento, cambios y validaciones realizadas.
- Los resultados de incidentes, auditorías, vulnerabilidades o pruebas generan acciones de mejora cuando sea necesario.

17. Monitorización, métricas e indicadores

Destrupaper mantiene mecanismos de vigilancia y revisión de eventos de seguridad basados en las herramientas disponibles, registros de sistemas, protección endpoint, servicios cloud y revisión periódica por los responsables. Las métricas e indicadores permiten evaluar el estado de implantación, eficacia y evolución del sistema de seguridad.

Indicador	Contenido mínimo
Incidentes	Número de incidentes, tipología, severidad, tiempo de resolución y acciones correctivas.
Accesos	Altas, bajas, cambios de permisos, revisiones periódicas y accesos de terceros.
Equipos	Equipos protegidos, estado de antivirus/endpoint, actualizaciones, incidencias y dispositivos conectados.
Copias	Ejecución de copias, pruebas de restauración, errores y tiempo de recuperación.
Proveedores	Servicios críticos, incidencias, SLA, revisiones y certificaciones disponibles.
Formación	Acciones de concienciación, asistencia, contenidos y eficacia.
Auditoría	Observaciones, no conformidades, acciones correctivas y grado de cierre.

18. Formación, concienciación y deberes del personal

La seguridad de la información requiere la participación activa de todas las personas que trabajan con el sistema. Destrupaper promueve acciones de formación y concienciación para asegurar que el personal conoce sus obligaciones, los riesgos más habituales y los procedimientos de actuación.

- El personal debe conocer y aceptar las normas de uso de sistemas, correo electrónico, navegación web, contraseñas, soportes, puestos de trabajo y tratamiento de información.
- Las acciones de concienciación recordarán periódicamente buenas prácticas, ingeniería social, identificación de incidentes y canales de comunicación.
- El personal técnico y los responsables de seguridad reciben formación específica acorde con sus funciones.
- Los acuerdos de confidencialidad se aplican a empleados, colaboradores y proveedores que accedan a información de Destrupaper o de sus clientes.

19. Auditoría, revisión y mejora continua

La política y el sistema de seguridad se revisan mediante auditorías internas, auditorías externas, revisiones del Comité de Seguridad, indicadores, análisis de riesgos, resultados de incidentes y seguimiento de acciones correctivas. Las conclusiones de estas revisiones se documentan y se incorporan al ciclo de mejora continua.

- La política se revisará al menos anualmente y ante cambios relevantes en alcance, riesgos, servicios, proveedores, tecnologías o normativa.

- Las auditorías evaluarán el cumplimiento de la política, la Declaración de Aplicabilidad, las medidas ENS y la suficiencia de evidencias.
- Las no conformidades y observaciones se gestionarán mediante acciones correctivas con responsable, plazo, evidencia de cierre y validación de eficacia.
- Los documentos obsoletos se retirarán del uso ordinario y se conservarán conforme a los criterios de control documental.

20. Aprobación, publicación y entrada en vigor

La presente Política de Seguridad de la Información ENS entra en vigor desde su aprobación por la Dirección de Destrupaper. Su contenido será comunicado al personal y a los colaboradores que deban conocerla, y se mantendrá disponible en el repositorio corporativo autorizado.

Esta política se complementa con el resto de políticas, normas, procedimientos, instrucciones técnicas, registros y evidencias que desarrollan el sistema de seguridad de la información de Destrupaper.

Aprobación

Rol	Nombre y cargo	Firma / fecha 21/05/2026
Dirección	CEO / Socio administrador	
Responsable de Seguridad	Designado por Comité de Seguridad	
Responsable del Sistema	Designado por Comité de Seguridad	