

Política de Seguridad de la Información

OVERANT INTERNET, S.L. — CIF B54303169

Conforme al artículo 12 y a la medida org.1 del Real Decreto 311/2022 (Esquema Nacional de Seguridad)

Versión 2.1 — 19 de octubre de 2026 · sustituye a la versión 2.0, aprobada el 15 de octubre de 2026

1. Objeto

Esta política establece las directrices de seguridad de la información de OVERANT INTERNET, S.L. y constituye el documento de referencia del que derivan la normativa, los procedimientos y los registros de seguridad de la organización. Su cumplimiento es obligatorio para todo el personal, propio o contratado, que acceda a los sistemas de información de la organización.

2. Misión y objetivos

OVERANT INTERNET, S.L. presta a clientes privados y a entidades del sector público servicios de alojamiento web y de correo, desarrollo web, distribución de licencias de software, control horario y canal de denuncias (sistema interno de información de la Ley 2/2023). Su misión en materia de seguridad es garantizar la disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad de la información y de los servicios que presta.

Son objetivos de seguridad de la organización:

- Proteger la identidad de las personas informantes y el contenido de las comunicaciones que reciben los canales de denuncias, con el deber de confidencialidad que impone la Ley 2/2023.
- Mantener los servicios disponibles para los clientes y recuperarlos en plazo ante una incidencia.
- Cumplir el Esquema Nacional de Seguridad en la categoría que corresponda a cada sistema y mantener vigentes la certificación y la declaración de conformidad obtenidas.
- Mejorar de forma continua la seguridad a partir de los incidentes, las auditorías y la revisión periódica de los riesgos.

3. Alcance

Esta política se aplica a toda la organización y a todo el personal, propio o contratado, que acceda a sus sistemas de información. El Esquema Nacional de Seguridad se aplica sistema a sistema; a la fecha de esta versión, los sistemas sujetos y su forma de acreditación son los siguientes:

Servicios gestionados en OVH Public Cloud	Un único alcance formado por los sistemas de información que soportan dos servicios prestados a entidades públicas y privadas: el canal de denuncias (sistema interno de información de la Ley 2/2023: formulario público, panel de gestión de expedientes y avisos por correo) y el alojamiento web gestionado (sitios web y bases de datos de cada cliente en instancias propias), junto con el nodo de administración desde el que se gestionan y sus copias de seguridad. Todo se aloja en OVH Public Cloud, en Francia. Categoría MEDIA · certificación de conformidad por entidad acreditada (art. 38.1).
Plataforma de servicios	Los sistemas que soportan los servicios de hosting compartido en servidores dedicados, control horario, desarrollo web y distribución de licencias de software. No incluye el alojamiento web gestionado en OVH Public Cloud, que forma parte del alcance anterior. Categoría BÁSICA · declaración de conformidad por autoevaluación (art. 38.1).

La declaración de alcance de cada expediente de seguridad detalla los activos, los proveedores y las exclusiones. En todo caso quedan fuera el contenido y las aplicaciones que cada cliente gestiona por su cuenta sobre los servicios contratados. Cualquier ampliación del alcance se aprueba por el Comité de Seguridad y se incorpora en la siguiente revisión de esta política.

4. Marco legal y regulatorio

Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad, que conforme a su artículo 2.3 se aplica a la organización como proveedora de servicios a entidades del sector público · Reglamento (UE) 2016/679, General de Protección de Datos · Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales · Ley 2/2023, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción · Ley 34/2002, de servicios de la sociedad de la información y de comercio electrónico · Ley 9/2017, de Contratos del Sector Público · Real Decreto-ley 12/2018, de seguridad de las redes y sistemas de información.

5. Categoría de los sistemas

Cada sistema se categoriza conforme al Anexo I del Real Decreto 311/2022 valorando las cinco dimensiones de seguridad; su categoría es la del nivel más alto alcanzado en cualquiera de ellas. La valoración razonada consta en el expediente de cada sistema y la aprueba la Dirección.

Servicios gestionados en OVH Public Cloud	MEDIA Canal de denuncias: confidencialidad, integridad, autenticidad y trazabilidad en nivel MEDIO; disponibilidad en nivel BAJO. Alojamiento web gestionado: valoración propia en su expediente. La categoría del alcance es la del nivel más alto de los dos servicios.
Plataforma de servicios	BÁSICA Las cinco dimensiones en nivel BAJO.

6. Organización de la seguridad

Se diferencian, conforme a los artículos 11 y 13, el responsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema. Las personas designadas y sus funciones son las siguientes:

Responsable de la Información	Antonio Miguel Sivera Peris Determina los requisitos de la información tratada, en los términos del artículo 13 del Real Decreto 311/2022, y establece los niveles de seguridad de la información.
Responsable del Servicio	Antonio Miguel Sivera Peris Determina los requisitos de los servicios prestados y establece sus niveles de seguridad.
Responsable de la Seguridad	Antonio Olmos Determina las decisiones necesarias para satisfacer los requisitos de seguridad de la información y de los servicios; supervisa la implantación de las medidas, promueve la formación y concienciación, y verifica el cumplimiento. Reporta directamente a la administración de la sociedad.
Responsable del Sistema	Antonio Miguel Sivera Peris Desarrolla, opera y mantiene el sistema de información durante todo su ciclo de vida, define su arquitectura y aplica las medidas de seguridad aprobadas.

La designación se formaliza mediante acta firmada por la administración de la sociedad, que se revisa al menos anualmente y de forma inmediata ante cualquier cese o cambio de funciones.

Para tareas técnicas de administración la organización dispone además de un asistente técnico, que no es un rol de seguridad: opera con su propia cuenta en el nodo de administración, solo en sesiones que autoriza en cada caso el Responsable del Sistema, y todas sus acciones quedan registradas como las de cualquier administrador.

7. Diferenciación de responsabilidades y medidas compensatorias

El artículo 13.3 exige que el Responsable de la Seguridad y el Responsable del Sistema sean personas distintas y sin dependencia jerárquica. Son personas distintas (Antonio Olmos y Antonio Miguel Sivera Peris), pero el segundo es administrador de la sociedad y la plantilla es reducida. La organización se acoge a la excepción del propio artículo 13.3 por ausencia justificada de recursos y aplica estas medidas compensatorias:

- Cuentas de administración nominativas, con llave personal y código del móvil, en un nodo de administración único; sin cuentas compartidas.
- Registro de cada orden de administración en el nodo, revisado cada semana por el Responsable de la Seguridad. Si en ese periodo él mismo ha usado una cuenta de administración, la revisión de su actividad la hace la Dirección.
- Las sesiones del asistente técnico requieren la autorización del Responsable del Sistema en cada caso y quedan registradas.
- Revisión semestral de los derechos de acceso por el Comité de Seguridad, con acta.
- Auditoría de la seguridad por una entidad independiente conforme al artículo 31, y revisión anual del sistema de gestión por el Comité.
- El Responsable de la Seguridad reporta directamente a la administración de la sociedad y puede elevar cualquier discrepancia al Comité, que la resuelve por escrito.

8. Comité de Seguridad

Comité de Seguridad: Antonio Miguel Sivera Peris (dirección; Responsable de la Información, del Servicio y del Sistema) y Antonio Olmos (Responsable de la Seguridad). Reunión semestral y extraordinaria ante incidente relevante, con acta. El Comité revisa semestralmente los derechos de acceso y los registros de las cuentas de administración, como medida compensatoria de la segregación limitada (ver op.acc.3).

Corresponde al Comité aprobar y revisar esta política, resolver los conflictos de responsabilidad, aceptar por escrito el riesgo residual, revisar los derechos de acceso y hacer el seguimiento de los incidentes y de las acciones correctivas.

9. Gestión del riesgo

La organización realiza y mantiene actualizado un análisis de riesgos de los sistemas incluidos en el alcance, que se revisa al menos una vez al año y siempre que cambien los servicios prestados, la información tratada, la infraestructura o el escenario de amenazas. El riesgo residual lo acepta por escrito el Comité de Seguridad. La selección de medidas parte del Anexo II del Real Decreto 311/2022 y se documenta en la declaración de aplicabilidad, donde se justifica también toda medida que no resulte aplicable.

10. Datos de carácter personal

Los sistemas incluidos en el alcance tratan datos de carácter personal. La organización cumple el Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018, mantiene el registro de actividades de tratamiento, en el que analiza también si debe nombrar delegado de protección de datos, y suscribe los correspondientes contratos de encargo de tratamiento con clientes y proveedores. Las medidas de seguridad del ENS se aplican sin perjuicio de las que exija la normativa de protección de datos.

11. Servicios prestados por terceros

La infraestructura que soporta los servicios se aloja en proveedores externos de la Unión Europea. La organización exige y conserva la acreditación de conformidad con el ENS de dicho proveedor y su declaración de alcance, verifica que cubre los productos y los centros de datos utilizados, firma contratos de encargo de tratamiento con los proveedores que acceden a datos personales, y traslada a los contratos los requisitos de seguridad y de notificación de incidentes. Las medidas relativas a instalaciones e infraestructura física se consideran heredadas del proveedor y se acreditan mediante su certificación.

12. Estructura documental

La documentación de seguridad se estructura en cuatro niveles: política, normativa, procedimientos y registros. Se conserva en el expediente ENS, con control de versiones y acceso restringido a los roles designados.

13. Obligaciones del personal

Todo el personal conoce esta política y la normativa que de ella deriva, y está obligado a: utilizar los recursos exclusivamente para fines profesionales; proteger las credenciales, que son personales e intransferibles; no compartir cuentas; comunicar de inmediato cualquier incidente o sospecha de incidente de seguridad; y aplicar las medidas de seguridad establecidas para el puesto de trabajo, incluido el trabajo en remoto. El incumplimiento podrá dar lugar a las responsabilidades laborales que procedan.

14. Formación y concienciación

La organización mantiene un plan de formación y concienciación en seguridad, con acciones al menos anuales y en el momento de la incorporación de nuevo personal, y conserva registro de su realización.

15. Gestión de incidentes

Los incidentes de seguridad se registran, clasifican y tratan conforme al procedimiento de gestión de incidentes. Se notifican a las autoridades y a los clientes afectados cuando así lo exija la normativa aplicable, incluida la notificación al CCN-CERT o al INCIBE-CERT según corresponda.

16. Aprobación, vigencia y revisión

Esta política es aprobada por la administración de la sociedad, entra en vigor en la fecha de su aprobación y permanece vigente hasta su sustitución expresa. Se revisa al menos una vez al año y siempre que se produzcan cambios relevantes en la organización, los servicios, la normativa o los riesgos. Se comunica a todo el personal y se pone a disposición del auditor, de la entidad de certificación y de los clientes que la requieran.

Aprobada por la administración de la sociedad

Fecha

Antonio Miguel Sivera Peris — Administrador único

Hoja de firma

Política de Seguridad de la Información — OVERANT INTERNET, S.L. — NIF B54303169
Artículo 12 del Real Decreto 311/2022, de 3 de mayo (Esquema Nacional de Seguridad)

El artículo 12 del Real Decreto 311/2022 dispone que «todas las entidades del ámbito de aplicación dispondrán de una política de seguridad, aprobada por el **órgano competente** que corresponda». Esta hoja recoge ese acto y forma parte inseparable del documento que la precede.

Documento firmado

Documento	Política de Seguridad de la Información — medida org.1 del Anexo II
Versión	2.1
Huella SHA-256 (16)	0f4a7806c4b63782
Páginas firmadas	Las que preceden a esta hoja

Firmante

Nombre	Antonio Miguel Sivera Peris
Condición	Órgano competente de OVERANT INTERNET, S.L. (administrador único)
Firmado como	Antonio Miguel Sivera Peris
Fecha y hora	2026-10-19 19:49
Verificación de identidad	código enviado a antonio.sivera@ctmd.es
Traza técnica	La dirección IP y el agente desde los que se firmó constan en el expediente de la entidad y se facilitan al auditor o al órgano que los requiera.
Firma	

La firma se realizó de forma electrónica a través del expediente de seguridad de la organización, mediante un enlace personal y un código de un solo uso enviado al correo corporativo del firmante, y queda registrada con la huella del documento: si el texto de la política cambia, cambia su huella y hay que volver a aprobarla.