1. DECLARACIÓN DE LA DIRECCIÓN Y ALCANCE

Con el fin de asegurar dicha gestión, en IBERVÍAS INGENIEROS, S.L.U. hemos implantado un Sistema de Gestión de Seguridad de la Información de acuerdo a los requisitos de la norma ISO/IEC 27001:2022 y del Esquema Nacional de Seguridad (ENS - Real Decreto 311/2022).

El propósito de este marco es garantizar la continuidad de los sistemas de información, minimizar los riesgos operativos y asegurar el cumplimiento de los objetivos estratégicos y legales de la organización. Esta política se aplica a todos los activos de información, sistemas, procesos, personal y terceras partes que interactúen con la información gestionada por la compañía.

2. OBJETIVOS Y PRINCIPIOS BÁSICOS

El objetivo de esta Política de Seguridad es fijar el marco de actuación necesario para proteger los recursos de información frente a amenazas internas o externas, deliberadas o accidentales, garantizando las dimensiones de la seguridad exigidas por el ENS.

- **Confidencialidad:** garantizar que la información sólo sea accesible a personas, entidades o procesos autorizados.
- **Integridad**: asegurar la exactitud y completitud de la información y de sus métodos de procesamiento.
- **Disponibilidad:** garantizar que los usuarios autorizados tengan acceso a la información y activos asociados cuando lo requieran
- **Autenticidad:** asegurar que la información o el origen de los datos sea legítimo y verificable.
- **Trazabilidad:** posibilitar la identificación del origen y del historial de acciones realizadas sobre la información o el sistema.

3. COMPROMISOS DE LA ORGANIZACIÓN

Para garantizar el cumplimiento de esta Política, la Dirección de IBERVIAS INGENIEROS, S.L.U. asume y promueve los siguientes compromisos:

- **Cumplimiento legal y normativo:** cumplir con la legislación vigente en materia de seguridad de la información, protección de datos personales y los requisitos del Esquema Nacional de Seguridad (RD 311/2022)
- **Protección de la privacidad:** asegurar la privacidad de los datos personales gestionados por IBERVÍAS INGENIEROS, S.L.U. de clientes, empleados, proveedores y terceras partes.
- **Gestión formal del riesgo:** identificar, analizar y evaluar los riesgos de seguridad de la información mediante metodologías reconocidas (como MAGERIT), aplicando los controles adecuados para mitigarlos
- **Categorización de sistemas:** clasificar formalmente los sistemas de información según sus niveles de seguridad (Básica, Media o Alta) de acuerdo con los criterios del anexo I del RD 311/2022 y aplicar las medidas de seguridad correspondientes (Anexo II)
- **Continuidad y resiliencia:** asegurar la capacidad de respuesta y recuperación ante situaciones de emergencia, restableciendo los servicios críticos en el menor tiempo posible.

- **Protección proporcional:** proteger los activos de información conforme a su valor, importancia y nivel de criticidad para la organización.
- **Concienciación y capacitación:** promover la formación contínua y la concienciación en seguridad de la información para todo el personal.
- Mejora continua: establecer objetivos de seguridad anuales y mantener un proceso continuo de revisión e innovación en nuestras actividades y sistemas.

4. ESTRUCTURA ORGANIZATIVA Y ROLES DE SEGURIDAD

Para garantizar la eficacia y aplicación del SGSI, la gobernanza de la seguridad se articula de la siguiente manera:

- **Comité de Seguridad de la Información:** responsable de la aprobación, difusión y supervisión global del SGSI, así como del seguimiento de los objetivos e incidentes de seguridad.
- **Roles de Seguridad ENS:** en cumplimiento del art 12 del RD 311/2022, se definen y formalizan en la normativa interna las responsabilidades diferenciadas para los siguientes roles:
  - **Responsable de la Información:** determina los requisitos de seguridad de la información tratada.
  - **Responsable del servicio:** determina las decisiones para satisfacer los requisitos de seguridad y supervisa su implantación
  - **Responsable del sistema:** supervisa la explotación diaria y el correcto funcionamiento técnico de las instalaciones y sistemas.

5. MARCO DOCUMENTAL DE SEGURIDAD

Esta política de seguridad constituye el nivel superior del marco normativo de IBERVIAS INGENIEROS, S.L.U. se despliega y complementa a través de un cuerpo documental estructurado en:

- Normas de Seguridad: políticas específicas sobre aspectos concretos, control de accesos, uso aceptable, contraseña, teletrabajo, etc.
- Procedimientos de Seguridad: instrucciones operativas para ejecutar tareas seguras (gestión de incidentes, copias de seguridad, gestión de cambios)
- Guías e Instrucciones Técnicas: configuraciones seguras y requisitos técnicos para sistemas e infraestructura.

6. OBLIGATORIEDAD Y REVISIÓN

Toda persona (personal propio, contratistas o colaboradores externos) cuya actividad pueda, directa o indirectamente, verse afectada por los requisitos del Sistema de Gestión de la Seguridad de

la Información, está obligada al cumplimiento estricto de la Política de Seguridad y de su normativa de desarrollo. El incumplimiento no justificado podrá derivar en las medidas disciplinarias o contractuales oportunas.

Está Política de Seguridad será revisada formalmente por el Comité de Seguridad de la Información con carácter anual, o de forma extraordinaria siempre que se produzcan cambios significativos en la infraestructura, la legislación o el entorno de riesgos de la organización.

IBERVIAS INGENIEROS, S. L.

Firmado por la Dirección

Fecha de actualización: Agosto de 2026