ÍNDICE

1. INTRODUCCIÓN **2**
2. ALCANCE **4**
3. MISIÓN **5**
4. MARCO NORMATIVO **5**
5. ROLES: FUNCIONES Y RESPONSABILIDADES **6**
5.1. RESPONSABLE DE INFORMACIÓN 6
5.2. RESPONSABLE DEL SERVICIO 7
5.3. RESPONSABLE DE SEGURIDAD 7
5.4. RESPONSABLE DEL SISTEMA 8
6. DATOS DE CARACTER PERSONAL **9**
7. OBLIGACIONES DEL PERSONAL **10**
8. TERCERAS PARTES **10**
9. HISTORIAL DE REVISIONES **10**

		Firma:	Fecha:
EDITADO:	Responsable De Sistema		
SUPERVISADO:	Responsable De Seguridad		
APROBADO:	Dirección/Resp. Información Y Servicio		

1. INTRODUCCIÓN

La Dirección de aplicaciones tecnológicas **IDRUS,** entiende que el sistema de información que da soporte para la prestación de sus actividades es un activo fundamental, no sólo para garantizar la continuidad de las operaciones, sino también para asegurar la protección adecuada de la información.
Este sistema da soporte a actividades como:

Los sistemas de información que dan soporte a los servicios de soluciones de software, así como atención telefónica avanzada mediante la herramienta ROVOZIA con inteligencia artificial.

Dado su impacto en el desarrollo y la prestación de estos servicios, **IDRUS** mantiene un compromiso firme con la protección de sus activos más significativos. Este compromiso forma parte esencial de una estrategia orientada a la continuidad del negocio, la gestión de riesgos y el fortalecimiento de una cultura sólida de seguridad de la información. Este enfoque se alinea tanto con el Esquema Nacional de Seguridad (ENS), según el RD 311/2022, como con la norma ISO 27001:2022, que proporciona un marco internacionalmente reconocido para la implementación de sistemas de gestión de la seguridad de la información (SGSI).

Desde su constitución, el objetivo de **IDRUS** es prestar un servicio de alta calidad a sus clientes, asegurando el cumplimiento de todos los requisitos establecidos y garantizando la máxima satisfacción de los clientes mediante la protección continua de la información crítica de la organización y sus clientes. Este enfoque está centrado en la seguridad de la información, la protección de datos personales y la mejora continua de los procesos dentro de un marco que incluye tanto los estándares nacionales como internacionales.

Este compromiso de satisfacción y confidencialidad de la información forma la piedra angular de nuestra política, entendiendo la satisfacción no solo como el cumplimiento de los compromisos contractuales, sino también como la capacidad de adaptarse a las expectativas no contractuales derivadas de las necesidades descubiertas en la ejecución del servicio, y que el propio cliente nos comunica.

En este contexto, un aspecto fundamental de nuestra política es la implantación, operación y mantenimiento de un SGSI basado en la normativa del **Esquema Nacional de Seguridad (ENS)** conforme al RD 311/2022 y los requisitos de la **ISO 27001:2022**. A través de la aplicación de un SGSI conforme a estas normativas, buscamos la mejora continua en la calidad y la disponibilidad de los servicios prestados, así como la continuidad de las operaciones y la gestión eficaz de riesgos en todas las áreas de la organización.

La dirección de **IDRUS** ha establecido los siguientes pilares fundamentales para la mejora continua de la eficacia del SGSI, los cuales están alineados tanto con los requisitos del **ENS** como con los de la **ISO 27001:2022**, y servirán como base para la definición de nuestros objetivos anuales:

- **Preservación de la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información**:
  - Preservando la confidencialidad de la información y evitando su divulgación y el acceso por personas no autorizadas.
  - Manteniendo la integridad de la información procurando su exactitud y evitando su deterioro
  - Asegurando la disponibilidad de la información en todos los soportes y siempre que sea necesaria.
- **Cumplimiento de requisitos legales y reglamentarios**:
  - Cumplir con todos los requisitos legales, reglamentarios y contractuales aplicables, así como con cualquier otro requisito que la organización suscriba, realizando evaluaciones continuas del cumplimiento en todas las áreas de actividad.
- **Planificación de la continuidad del negocio**:
  - Tener implementado un plan de continuidad que permita recuperar rápidamente las operaciones tras cualquier incidente, garantizando la menor interrupción posible de los servicios.
- **Formación y concienciación en seguridad de la información**:
  - Fomentar la formación continua de todo el personal en materia de seguridad de la información, asegurando que nuestros recursos

humanos estén siempre actualizados frente a las necesidades tecnológicas emergentes y las amenazas cambiantes, conforme con los requisitos de la **ISO 27001:2022** y el **ENS**.

- **Compromiso con la mejora continua**:
  - Garantizar la mejora continua mediante la evaluación periódica del desempeño del SGSI, tomando decisiones informadas para ajustar procesos y controles, siempre con la intención de mantener la eficacia y eficiencia del sistema de gestión.
- **Gestión de incidencias y riesgos**:
  - Gestionar de manera adecuada todas las incidencias relacionadas con la seguridad de la información y evaluar los riesgos asociados a la organización. Esto incluye la identificación y mitigación de riesgos en todos los procesos y activos de información, para prevenir incumplimientos y asegurar el cumplimiento de los objetivos estratégicos.
- **Comunicación y cumplimiento de la política**:
  - Comunicar a todo el personal, contratistas, proveedores y otros terceros, el cumplimiento obligatorio de esta política, incluyendo medidas de seguridad en las instalaciones y procesos, y garantizando que todos los miembros de la organización comprendan sus responsabilidades en cuanto a la protección de la información.
- **Gestión de la satisfacción de los clientes y grupos de interés**:
  - Asegurar la satisfacción de nuestros clientes basándonos en un trato correcto y en un esfuerzo continuo en la prestación del servicio, cumpliendo con los requisitos y compromisos de seguridad y mejoras acordadas.
- **Evaluación de objetivos y fortalecimiento del compromiso**:
  - Establecer y revisar regularmente los objetivos del SGSI, alineándose con los compromisos adquiridos en esta política y fomentando la participación activa de todo el personal en el proceso de mejora continua.

IDRUS, a través de la implementación del SGSI conforme tanto a la **ISO 27001:2022** como los distintos Responsables dentro del **Esquema Nacional de Seguridad (ENS)**, valora la disponibilidad, confidencialidad, integridad, trazabilidad y autenticidad de la información como aspectos cruciales para la estimación de los riesgos y la protección de la información tanto propia como de nuestros clientes, a fin de garantizar la continuidad de nuestras operaciones y la confianza de nuestros clientes en nuestros servicios.

- Tener un plan de continuidad que permita recuperarse de un desastre en el menor tiempo posible.
- Velar por una **continua y permanente actualización de nuestros recursos**, tanto **tecnológicos** como, sobre todo, de nuestro **personal**, fomentando políticas de información y formación continua profesional que les permitan avanzar en sus conocimientos al ritmo que lo hace nuestro sector, fomentando la conciencia de la seguridad de la información, a fin de incrementar la competencia de los empleados

  Todos los empleados son informados de sus funciones y obligaciones de seguridad y son responsables de cumplirlas.
- Garantizar la **mejora continua**, manteniendo el Sistema de forma eficaz y efectiva para constatar el compromiso con los clientes, buscando para ello una mejor organización interna del trabajo y en la forma en que tratamos la información de nuestros clientes. Hay un responsable de seguridad encargado del SGSI de la organización.
- Gestionar adecuadamente todas las incidencias ocurridas, evaluando de forma concienzuda los **riesgos de la organización**, analizando los posibles riesgos de todos y cada uno de los procesos de la organización y de los activos de información, previendo y evitando de esta manera desviaciones, tomando las oportunas decisiones para minimizar posibles no conformidades.
- Comunicar a todo el personal y todo aquel que trabaje en su nombre, el obligado cumplimiento de esta Política, incluyendo contratistas y visitantes a nuestras instalaciones.
- Asegurar la **satisfacción de sus clientes** basándose en un trato siempre correcto y en un esfuerzo continuo en la prestación del servicio en base a sus requisitos y a nuestros compromisos de actualizaciones y mejoras.

- Cumplir con los **requisitos de los clientes y de sus grupos de interés**, así como con los requisitos legales y reglamentarios que afecten a la realización y prestación de los servicios prestados.
- **Establecer procesos operacionales** que salvaguarden a las personas, la propiedad, la información, los datos y las aplicaciones o sistemas de uso para las instancias establecidas por la organización.
- Establecer y revisar regularmente los Objetivos, acordes con los compromisos que se asumen en esta declaración, fortaleciendo el **compromiso y participación de todo el personal** en el desarrollo y consecución de los Objetivos.
- La Dirección, por su parte, valora especialmente y establece como criterio principal para la estimación de sus riesgos la valoración de la disponibilidad, confidencialidad e integridad de su información y aún más la de sus clientes.

2. ALCANCE

La organización establece esta política de seguridad de la información de acuerdo con el Esquema Nacional de Seguridad (ENS), conforme al Real Decreto 311/2022, y la norma ISO 27001:2022. Esta política se aplica a los sistemas de información que dan soporte a los siguientes servicios:

Los sistemas de información que dan soporte a los servicios de soluciones de software, así como atención telefónica avanzada mediante la herramienta ROVOZIA con inteligencia artificial.

La política de seguridad de la información implementada abarca todos los procesos, activos y servicios mencionados, y está alineada con los principios y requisitos tanto del Esquema Nacional de Seguridad (ENS) como de la norma ISO 27001:2022.

Esto incluye:

1. **Sistemas de Información y Procesos Relacionados**: Todos los sistemas de información que se utilizan para soportar los servicios mencionados estarán cubiertos por las medidas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información, conforme a los requisitos

establecidos tanto en el **RD 311/2022** (Esquema Nacional de Seguridad) como en la **ISO 27001:2022** (Sistema de Gestión de la Seguridad de la Información).

2. **Actividades de Soporte**: Además de los servicios que directamente involucran sistemas de información, la política también incluye las actividades de apoyo relacionadas con estos servicios, tales como la gestión de incidentes, mantenimiento, actualización y protección de los activos tecnológicos y la gestión de proveedores.
3. **Identificación de Activos y Procesos Críticos**: En el marco de la **ISO 27001:2022**, se identifican y gestionan los activos de información críticos asociados a cada uno de los servicios que forman parte del alcance. Este proceso incluye la evaluación y tratamiento de los riesgos asociados a la seguridad de la información, de acuerdo con lo especificado en la **ISO 27001:2022** y el **ENS**.
4. **Cumplimiento de Requisitos Legales y Normativos**: El alcance de esta política también cubre el cumplimiento de los requisitos legales, reglamentarios y contractuales aplicables en materia de seguridad de la información, conforme a la legislación española y a los requisitos de las normativas internacionales en seguridad de la información, incluyendo la **ISO 27001:2022** y el **Esquema Nacional de Seguridad**.
5. **Implementación y Mantenimiento del SGSI**: Esta política está alineada con la implementación y mantenimiento de un **Sistema de Gestión de la Seguridad de la Información (SGSI)**, conforme a la **ISO 27001:2022**, lo que incluye la mejora continua de los controles y procedimientos de seguridad, la revisión periódica de los riesgos asociados, la gestión de incidentes de seguridad y el establecimiento de planes de contingencia para garantizar la continuidad de las operaciones.
6. **Declaración de Aplicabilidad**: De acuerdo con los principios de la **ISO 27001:2022**, se establecerá y mantendrá una declaración de aplicabilidad vigente, que define los controles específicos aplicables para los sistemas de información cubiertos por esta política. Esto también estará alineado con los requisitos del **Esquema Nacional de Seguridad (ENS)** para garantizar que se apliquen las medidas de seguridad adecuadas a cada servicio y sistema crítico.

El alcance de esta política es de aplicación a todos los sistemas de información, procesos y actividades de **IDRUS**, que den soporte a los servicios anteriormente mencionados, sin limitación alguna, y abarca todos los niveles operativos, desde la gestión estratégica hasta las operaciones diarias. Además, se asegura de que todos los empleados y partes interesadas cumplan con los principios de seguridad de la información establecidos en la política, los procedimientos operacionales y los requisitos legales y normativos que afectan a los servicios prestados.

3. MISIÓN

En IDRUS, nuestra misión es revolucionar la comunicación telefónica para empresas y administraciones públicas mediante soluciones innovadoras basadas en inteligencia artificial. Nos comprometemos a crear sistemas inteligentes, eficientes y accesibles que optimicen recursos, reduzcan costes y garanticen que ninguna llamada quede sin atender.

Nuestra prioridad es la satisfacción de nuestros clientes y del usuario final, ofreciendo una experiencia fluida, eficaz y personalizada. Para lograrlo, integramos tecnologías avanzadas, desde infraestructura de comunicaciones hasta herramientas informáticas seguras y cifradas, asegurando un servicio de la máxima calidad.

Contamos con un equipo humano competente, ético y comprometido, que impulsa nuestro crecimiento y asegura el éxito de cada interacción.

Además, cumplimos con los REQUISITOS APLICABLES, tanto legales, con especial atención a la protección de datos personales, como aquellos que la organización suscribe, relativos a los plazos, la fiabilidad y la calidad de la imagen, aspectos fundamentales para mantener un elevado nivel de calidad asistencial.

Para cumplir con esta misión, **IDRUS** se compromete a:

- **Garantizar la seguridad de la información**: Adoptar un enfoque integral en la gestión de la seguridad de la información, basado en los principios establecidos por el Esquema Nacional de Seguridad (ENS) (RD 311/2022) y la ISO 27001:2022, para proteger tanto la información de los clientes como los propios

datos internos de la organización frente a posibles amenazas y vulnerabilidades.

- **Implementar un Sistema de Gestión de la Seguridad de la Información (SGSI)**: Asegurar que todas las actividades de IDRUS se desarrollen dentro de un marco de cumplimiento continuo con la ISO 27001:2022, con el fin de gestionar de manera eficaz los riesgos de seguridad de la información, mediante la aplicación de controles adecuados y la mejora continua del SGSI.
- **Proteger la información crítica**: Asegurar que toda la información crítica para la organización y para nuestros clientes se maneje con los niveles más altos de seguridad, respetando todos los requisitos legales, normativos y contractuales aplicables, y asegurando el cumplimiento de los principios del ENS y la ISO 27001:2022.
- **Fomentar la mejora continua**: A través de la implementación de medidas de seguridad alineadas con el Esquema Nacional de Seguridad (ENS) y la ISO 27001:2022, IDRUS se compromete a mejorar continuamente sus procesos, recursos y capacidades para abordar los riesgos emergentes en la seguridad de la información, adaptándose siempre a las nuevas necesidades tecnológicas y a los requisitos cambiantes de los clientes.
- **Concienciar y capacitar al personal**: Desarrollar programas continuos de formación y sensibilización sobre seguridad de la información para todo el personal de la organización, con el fin de fomentar una cultura de seguridad en todos los niveles y garantizar el cumplimiento de las directrices establecidas por el ENS y la ISO 27001:2022.
- **Cumplir con los requisitos legales y reglamentarios**: Asegurar que todas las actividades y servicios prestados se lleven a cabo en cumplimiento de los requisitos legales, regulatorios y contractuales, no solo a nivel nacional (de acuerdo con el Esquema Nacional de Seguridad), sino también conforme a las normativas internacionales aplicables en el ámbito de la seguridad de la información, tales como la ISO 27001:2022.
- **Proteger la continuidad del negocio**: Asegurar que los sistemas de información y los servicios que proporcionamos a nuestros clientes sean siempre accesibles y funcionen de manera continua, incluso ante situaciones adversas, mediante el establecimiento de planes de continuidad de negocio y recuperación ante desastres, conforme a lo establecido en la ISO 27001:2022.

En resumen, **IDRUS** se dedica a ofrecer soluciones innovadoras y de valor a nuestros clientes, garantizando la seguridad y la protección de la información a través de un enfoque integral y alineado con los estándares del Esquema Nacional de Seguridad (ENS) y la ISO 27001:2022. Esto nos permite ser un socio confiable, capaz de brindar soluciones que no solo optimizan los procesos de nuestros clientes, sino que también los protegen frente a los riesgos inherentes al tratamiento de la información

4. MARCO NORMATIVO

IDRUS se esfuerza en cumplir con toda la legislación aplicable a su actividad, ya sea de carácter general (Código Civil, Código de comercio, etc.) o específico, como por ejemplo la siguiente:

- **Real Decreto 311/2022, de 3 de mayo:** Regula el Esquema Nacional de Seguridad (ENS) y establece principios y requisitos de ciberseguridad en el sector público.
- **Ley 40/2015, de 1 de octubre:** Establece el Régimen Jurídico del Sector Público y regula la organización y funcionamiento de las administraciones públicas.
- **Guías de la serie 800 CCN-STIC:** Serie de guías del Centro Criptológico Nacional que orientan sobre seguridad y estructuración documental en el cumplimiento del ENS.
- **Ley Orgánica 3/2018, de 5 de diciembre:** Relativa a la Protección de Datos Personales y garantía de los derechos digitales, complementa y desarrolla el Reglamento General de Protección de Datos (RGPD).
- **Reglamento (UE) 2016/679 del Parlamento Europeo (RGPD):** Relativo a la protección de datos personales de las personas físicas en la UE y su libre circulación.
- **Reglamento (UE) nº 910/2014 (eIDAS):** Regula la identificación electrónica y los servicios de confianza en el mercado interior, derogando la Directiva 1999/93/CE.
- **Reglamento (UE) 2019/881 (Reglamento de Ciberseguridad):** Relativo a la ciberseguridad y certificación de tecnologías de la información, regula la

Agencia de la UE para la Ciberseguridad (ENISA) y sustituye al Reglamento (UE) n.o 526/2013.

- **Real Decreto Legislativo 1/1996, de 12 de abril:** Aprueba el texto refundido de la Ley de Propiedad Intelectual, armonizando las disposiciones legales sobre la materia. Actualizada por Ley 23/2006.

Además, **IDRUS** implementa y adapta sus políticas de seguridad de la información a los controles y principios de la ISO/IEC 27001:2022, como marco internacional de referencia para la protección de la información. Esta normativa se integra con el ENS para la mejora continua de la gestión de riesgos, la protección de activos y el establecimiento de un Sistema de Gestión de Seguridad de la Información (SGSI).

5. ROLES: FUNCIONES Y RESPONSABILIDADES

5.1. RESPONSABLE DE INFORMACIÓN

- Determina los requisitos (de seguridad) de la información tratada, según los parámetros del Anexo I del ENS.
- Formar parte y tomar decisiones en el Comité de Seguridad de la Información, con el objetivo de garantizar que los servicios prestados cumplen con los controles de seguridad de la información establecidos tanto en el **ENS** como en la **ISO 27001:2022**.
- Aprobación de los niveles de seguridad de la información, teniendo en cuenta tanto el **ENS** como los controles de la **ISO 27001:2022** para gestionar los riesgos asociados a la seguridad de la información.
- Proteger los activos, de acuerdo con las políticas y procedimientos establecidos en el Sistema de Gestión de la Seguridad de la Información (SGSI) según **ISO 27001:2022**
- Cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos, de acuerdo con la legislación aplicable y la política de seguridad de la información establecida

5.2. RESPONSABLE DEL SERVICIO

- Determina los requisitos (de seguridad) de los servicios prestados, · conforme a los parámetros del **Anexo I del ENS** y los requisitos de la **ISO/IEC 27001:2022**, asegurando que los servicios cumplan con los principios de seguridad de la información y se gestionen adecuadamente los riesgos asociados.
- Formar parte y tomar decisiones en el Comité de Seguridad de la Información, · de la Información, con el objetivo de garantizar que los servicios prestados cumplen con los controles de seguridad de la información establecidos tanto en el **ENS** como en la **ISO 27001:2022**.
- Aprobación de los niveles de seguridad de los servicios, asegurando que se implementen las medidas adecuadas para proteger la seguridad de los mismos.
- Proteger los activos, activos, aplicando las medidas y controles adecuados según lo especificado en el SGSI de acuerdo con los requisitos de la **ISO 27001:2022**..
- Cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos

5.3. RESPONSABLE DE SEGURIDAD / RESPONSABLE SGSI

- Determina las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los responsables de la información y de los servicios.
- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo con lo establecido en la Política de Seguridad de la Información de la organización.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
- Convoca las reuniones del Comité de Seguridad de la Información.

- Junto con el Responsable de Sistema, vela por el cumplimiento del ENS, especialmente en términos de actualización de controles y categorización de activo.
- Prepara los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elabora el acta de las reuniones.
- Es responsable de la ejecución directa o delegada de las decisiones del Comité.
- Elaborar y proponer para aprobación por la organización las políticas de seguridad, que incluirán las medidas técnicas y organizativas, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados y para prevenir y reducir al mínimo los efectos de los ciberincidentes que afecten a la organización y los servicios.
- Desarrollar las políticas de seguridad, normativas y procedimientos derivados de la organización, supervisar su efectividad y llevar a cabo auditorías periódicas de seguridad.
- Elaborar el documento de Declaración de Aplicabilidad.
- Actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos.
- Constituirse como punto de contacto con la autoridad competente en materia de seguridad de las redes y sistemas de información y responsable ante aquella del cumplimiento de las obligaciones que se derivan del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información y de su Reglamento de Desarrollo.
- Constituir el punto de contacto especializado para la coordinación con el CSIRT (Computer Security Incident Response Team – Equipo de Respuesta ante Emergencias Informáticas) de referencia (CCN-Cert, INCIBE..).

- Notificar a la autoridad competente, a través del CSIRT de referencia y sin dilación indebida, los incidentes que tengan efectos perturbadores en la prestación de los servicios.

- Recibir, interpretar y aplicar las instrucciones y guías emanadas de la Autoridad Competente, tanto para la operativa habitual como para la subsanación de las deficiencias observadas
- Recopilar, preparar y suministrar información o documentación a la autoridad competente o el CSIRT de referencia, a su solicitud o por propia iniciativa
- Determina las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los responsables de la información y de los servicios, garantizando que se apliquen los controles y medidas establecidos en la **ISO 27001:2022** para gestionar los riesgos relacionados con la seguridad de la información.
- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo con lo establecido en la Política de Seguridad de la Información de la organización y los controles de **ISO 27001:2022**.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad, como parte del plan de formación y sensibilización previsto en la ISO 27001:2022.
- Convoca las reuniones del Comité de Seguridad de la Información, garantizando que se traten los temas relacionados con los controles de seguridad establecidos en el **ENS** y la **ISO 27001:2022**.
- Junto con el Responsable de Sistema, vela por el cumplimiento del **ENS** y la **ISO 27001:2022**, especialmente en términos de actualización de controles y categorización de activos.
- Prepara los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones conforme a los principios de la **ISO 27001:2022**.
- Elabora el acta de las reuniones, registrando las decisiones y acciones a tomar de acuerdo con los requisitos de seguridad establecidos en el **SGSI**.
- Es responsable de la ejecución directa o delegada de las decisiones del Comité de Seguridad, incluyendo las relacionadas con el cumplimiento de la **ISO 27001:2022** y la protección de la información.

- Elaborar y proponer para aprobación por la organización las políticas de seguridad, que incluirán las medidas técnicas y organizativas adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados y para prevenir y reducir al mínimo los efectos de los ciberincidentes que afecten a la organización y los servicios, en conformidad con la **ISO 27001:2022**.
- Desarrollar las políticas de seguridad, normativas y procedimientos derivados de la organización, supervisar su efectividad y llevar a cabo auditorías periódicas de seguridad, de acuerdo con los requisitos de la **ISO 27001:2022**.
- Elaborar el documento de **Declaración de Aplicabilidad**, asegurando que los controles de seguridad propuestos sean aplicables y adecuados según los requisitos de la **ISO 27001:2022**.
- Actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos, alineándose con las directrices de la **ISO 27001:2022**.
- Constituirse como punto de contacto con la autoridad competente en materia de seguridad de las redes y sistemas de información y responsable ante aquella del cumplimiento de las obligaciones que se derivan del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información y de su Reglamento de Desarrollo, y garantizar la conformidad con los requisitos de **ISO 27001:2022**.
- Constituir el punto de contacto especializado para la coordinación con el **CSIRT** (Computer Security Incident Response Team – Equipo de Respuesta ante Emergencias Informáticas) de referencia (CCN-Cert, INCIBE, etc.), cumpliendo con los procedimientos de gestión de incidentes de seguridad de la **ISO 27001:2022**.
- Notificar a la autoridad competente, a través del CSIRT de referencia y sin dilación indebida, los incidentes que tengan efectos perturbadores en la prestación de los servicios, conforme a los procedimientos establecidos en la **ISO 27001:2022** para la gestión de incidentes.

- Recibir, interpretar y aplicar las instrucciones y guías emanadas de la Autoridad Competente, tanto para la operativa habitual como para la subsanación de las deficiencias observadas, garantizando el cumplimiento de las normas y controles de seguridad de **ISO 27001:2022**.
- Recopilar, preparar y suministrar información o documentación a la autoridad competente o el CSIRT de referencia, a su solicitud o por propia iniciativa, en cumplimiento con los requisitos de **ISO 27001:2022**.

5.4. RESPONSABLE DEL SISTEMA

- Formar parte y tomar decisiones en el Comité de Seguridad de la Información.
- Desarrollar, operar y mantener del Sistema durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y política de gestión del Sistema estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema.
- Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
- Junto con el Responsable de Seguridad, vela por el cumplimiento del ENS, especialmente en términos de actualización de controles y categorización de activos.
- Decidir las medidas de seguridad que aplicarán los suministradores de componentes del Sistema durante las etapas de desarrollo, instalación y prueba de este.
- Implantar y controlar las medidas específicas de seguridad del Sistema y cerciorarse de que éstas se integren adecuadamente dentro del marco general de seguridad.
- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del Sistema.

- Llevar a cabo el preceptivo proceso de análisis y gestión de riesgos en el Sistema.
- Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y determinar las medidas de seguridad que deben aplicarse según se describe en el Anexo II del ENS.
- Elaborar y aprobar la documentación de seguridad del Sistema.
- Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del Sistema.
- Investigar los incidentes de seguridad que afecten al Sistema, y en su caso, comunicación al Responsable de Seguridad o a quién éste determine.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- Puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el responsable de seguridad, antes de ser ejecutada.

6. DATOS DE CARACTER PERSONAL

IDRUS, trata los datos de carácter personal, por lo que mantiene un “registro de actividades de tratamiento”, al que tendrán acceso sólo las personas autorizadas, en el que se recogen los datos afectados y los responsables del tratamiento. Todos los sistemas de información de IDRUS se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado registro.

7. OBLIGACIONES DEL PERSONAL

Todos los trabajadores de IDRUS, tienen la obligación de conocer esta Política de Seguridad de la Información, que es de obligado cumplimiento dentro del alcance identificado, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Se establecerá un programa de concienciación continua para atender a todos los miembros de IDRUS, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC dentro del alcance recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o, si, por el contrario se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

8. TERCERAS PARTES

Las terceras partes relacionadas con **IDRUS**, dentro del alcance, firman con la **IDRUS** un acuerdo que protege la información intercambiada.

Cuando **IDRUS**, utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad. Dicha tercera parte, quedará sujeta a las obligaciones establecidas en dicha Política, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos.

9. HISTORIAL DE REVISIONES

Esta Política será revisada para su continua adecuación anualmente por la Dirección, así como los objetivos y metas de la **IDRUS**, y comunicada a todo el personal de la organización encontrándose a disposición del público bajo solicitud de cualquier parte interesada.

Revisión	Fecha	Razón Modificación
1.0	11/04/2025	Creación del Documento
1.1	17/06/2025	Edición de Documento
1.2	19/03/2026	Cambio de responsable de seguridad

La Gerencia se asegura que la Política de Seguridad de la Información es entendida, implantada y mantenida al día en todos los niveles de la Organización.

En Santander, a ……..…de …….. de 2026

Fdo.: *Carlos Recio Calzada*
Director/Gerente