relleuTelecom
INTERNET | FIJO | MÓVIL

Política de Seguridad

EDICIÓN	CAMBIO	FECHA
00	Edición inicial	12/02/2024
01	Actualización de legislación	12/02/2026
02	Adaptación a requisitos de la guía 805 de junio 2025	11/06/2026

ELABORADO	REVISADO Y APROBADO
Comité de Seguridad de Seguridad	CEO
Fecha: 10/06/2026	Nombre: Mariano Rico Fecha: 11/06/2026

ÍNDICE

1. APROBACIÓN Y ENTRADA EN VIGOR

El presente texto constituye la Política de Seguridad de **RELLEU TELECOM S.L.U**. (en adelante **RELLEU TELECOM**) y se hace efectivo desde la fecha de su aprobación por parte de la Dirección. Esta política anula cualquier versión anterior y será revisada con carácter anual, documentándose en el informe de Revisión por la Dirección.

2. INTRODUCCIÓN

Empresa operadora de telecomunicaciones nacional autorizada para proveer servicios de telecomunicaciones tales como conexión a internet, telefonía fija y móvil y televisión por internet en cualquiera de las tecnologías disponibles. Para ello, asume valores que considera esenciales para la consecución de sus objetivos como es la preservación de la Información y los datos personales, tanto propios como del resto de partes interesadas y el desarrollo profesional y personal de todos los componentes de su equipo de trabajo.

Debido a nuestra actividad, en **RELLEU TELECOM** somos conscientes de que la información es un activo con un elevado valor para nuestra organización y requiere una protección y gestión adecuadas para dar continuidad a nuestra línea de negocio y minimizar posibles daños. El objetivo último de esta política es garantizar que **RELLEU TELECOM** pueda cumplir con sus objetivos, prestando servicios ininterrumpidos y preservando la calidad de la información mediante la prevención, detección, respuesta y recuperación ante incidentes.

3. ALCANCE

Esta política se aplica a todos los sistemas de información de **RELLEU TELECOM**, a todas las personas que conforman la organización, sin excepciones, y a los prestadores de servicios o proveedores de soluciones.

La Política de Seguridad proporciona las bases para definir y delimitar los objetivos y responsabilidades para las diversas actuaciones técnicas, legales y organizativas que se requieran para garantizar la seguridad de la información y la privacidad, cumpliendo el marco legal de aplicación y las políticas globales y específicas de firma, así como los procedimientos definidos

4. PRINCIPIOS RECTORES DE LA POLÍTICA

La gestión de la seguridad en **RELLEU TELECOM** se asienta en los siguientes principios:

- **Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad:** Garantizando que el acceso y las actuaciones sean de entidades autorizadas, exactas y registradas.
- **Prevención:** Implementando las medidas mínimas del ENS y evaluando rutinariamente la seguridad antes y durante la operación de los sistemas.
- **Detección:** Monitorizando de manera continua para detectar anomalías en la prestación de los servicios.
- **Respuesta y Recuperación:** Estableciendo protocolos eficaces y planes de continuidad de los sistemas frente a incidentes de seguridad.
- **Segregación de funciones:** El Responsable de la Seguridad será una figura diferenciada del Responsable del Sistema.

El propósito del Sistema de Seguridad de la Información es garantizar que los riesgos de la seguridad de la información y privacidad sean conocidos, asumidos, gestionados y minimizados de una forma documentada, sistemática, estructurada, repetible, asumible y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

Para ello, la dirección declara el compromiso de **RELLEU TELECOM** para:

- Establecer como objetivo primordial los sistemas de seguridad de la información que dan soporte a **la implantación y mantenimiento de equipos y aplicaciones informáticas**, con absoluto respeto a los estándares de calidad, preservando la información, con especial atención a la sensibilidad de los datos personales tratados, con todas las medidas necesarias a su alcance.
- Aplicar el principio de mejora continua a todos los procesos de la organización, con el objetivo adicional de conseguir el mayor grado de satisfacción de los clientes.
- Asegurar el cumplimiento de los requisitos legales y reglamentarios que sean de aplicación (en particular la relativa a la protección de los datos personales), así como los que la organización haya asumido de manera voluntaria en el desarrollo de la Responsabilidad Social Corporativa y en el Código de Conducta.
- Potenciar la participación, la comunicación, la información y la formación del equipo profesional con el objetivo de que se sienta partícipe del trabajo de la organización en su conjunto.
- Promover el compromiso de responsabilidad entre los componentes del equipo de acuerdo con los requisitos de calidad, así como los relativos a la privacidad y seguridad de la información acordados tanto internamente como con los clientes, mediante acciones de formación y concienciación adecuadas y regulares.
- Asegurar la continuidad del negocio desarrollando planes de continuidad conformes a metodologías reconocidas.
- Realizar y revisar periódicamente un análisis de riesgos basados en métodos reconocidos que nos permitan establecer el nivel tanto de privacidad de los datos

personales como de seguridad de la información a nivel general y de los proyectos y servicios en marcha y minimizar los riesgos mediante el desarrollo de políticas específicas, soluciones técnicas y acuerdos contractuales con organizaciones especializadas.

- Compromiso de información a partes interesadas.
- Selección de proveedores y subcontratistas en base a criterios relacionados con la privacidad y seguridad de la información.
- Establecer y cumplir los requisitos contractuales con las partes interesadas.
- Promover una cultura de mejora continua en la gestión de la seguridad de la información e implementar mejoras basadas en el análisis de incidentes, auditorías y revisiones periódicas
- Gestionar adecuadamente el ciclo de vida de la información, de manera que se puedan evitar usos incorrectos durante cualquiera de las fases.
- Asegurar la protección de los derechos de propiedad intelectual
- Establecer periódicamente un conjunto de objetivos e indicadores, que permitan a la dirección llevar a cabo un adecuado seguimiento de los niveles de servicio ofrecidos y las actividades de gestión.

La dirección de **RELLEU TELECOM** se compromete a apoyar y promover los principios establecidos en esta Política, para lo que pide al personal de **RELLEU TELECOM** que asuma y se atenga a las previsiones del sistema de gestión documentado para el ENS.

5. MARCO NORMATIVO

Las principales normativas que rigen esta Política son el Real Decreto 311/2022 (ENS), el RGPD y la LOPDGDD.

Ley / Regulación	**Responsabilidad**
Ley 40/2015, de 1 de octubre, establece y regula las bases del régimen jurídico de las Administraciones Públicas, los principios del sistema de responsabilidad de las Administraciones Públicas y de la potestad sancionadora, así como la organización y funcionamiento de la Administración General del Estado y de su sector público institucional para el desarrollo de sus actividades	Responsable de Seguridad
Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.	Responsable de Seguridad
Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal	Responsable de Seguridad

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos	Responsable de Seguridad
Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales	Responsable de Seguridad
Ley 34/2002 de Servicios de la Sociedad de la Información (LSSI)	Responsable de Seguridad
REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE	Responsable de Seguridad
Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.	Responsable de Seguridad

Además del marco legislativo general, **RELLEU TELECOM** ha desarrollado el proceso DG24_ Cumplimiento legal y normativo_Rev.0 y el registro DG24.R01_Listado de requisitos legales y otros requisitos. A través de estos, **RELLEU TELECOM** actualiza la legislación aplicable y verifica su cumplimiento

6. ORGANIZACIÓN DE LA SEGURIDAD

El modelo organizativo de seguridad se estructura de la siguiente manera:

7.1 Comité de Seguridad

El Comité reporta directamente al CEO. Entre sus funciones destacan: elaborar y revisar la Política de Seguridad, velar por el cumplimiento del marco legal, coordinar los Planes de Continuidad, dirimir posibles conflictos de responsabilidad y promover la mejora continua y formación.

El Comité de Seguridad tendrá las siguientes funciones:

- Atender las inquietudes de la Alta Dirección y de los diferentes departamentos.
- Informar regularmente del estado de la seguridad de la información a la Alta Dirección.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Elaborar la estrategia de evolución de la Organización en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.

- Elaborar (y revisar regularmente) la Política de Seguridad para que sea aprobada por la Dirección.
- Aprobar la normativa de seguridad de la información.
- Coordinar todas las funciones de seguridad de la organización.
- Velar por el cumplimiento de la normativa legal y sectorial de aplicación.
- Velar por el alineamiento de las actividades de seguridad a los objetivos de la organización.
- Coordinar los Planes de Continuidad de las diferentes áreas, para asegurar una actuación sin fisuras en caso de que deban ser activados.
- Coordinar y aprobar, en su caso, las propuestas de proyectos recibidas de los diferentes ámbitos de seguridad, encargándose gestionar un control y presentación regular del progreso de los proyectos y anuncio de las posibles desviaciones.
- Recibir las inquietudes en materia de seguridad de la Dirección de la entidad y transmitirlas a los responsables departamentales pertinentes, recabando de ellos las correspondientes respuestas y soluciones que, una vez coordinadas, habrán de ser comunicadas a la Dirección.
- Recabar de los responsables de seguridad departamentales informes regulares del estado de la seguridad de la organización y de los posibles incidentes. Estos informes, se consolidan y resumen para su comunicación a la Dirección de la entidad.
- Coordinar y dar respuesta a las inquietudes transmitidas a través de los responsables de seguridad departamentales.
- Definir, dentro de la Política de Seguridad Corporativa, la asignación de roles y los criterios para alcanzar las garantías pertinentes en lo relativo a segregación de funciones
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la Organización y recomendar posibles actuaciones respecto de ellos.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.
- Promover la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de la Organización. En particular velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
- Cuando existan discrepancias técnicas u operativas entre los distintos roles de responsabilidad del sistema, el Comité de Seguridad de la Información será el encargado de dirimir y resolver dichos conflictos mediante un análisis del impacto y del riesgo residual. Se contemplarán procedimientos específicos de resolución adaptados a

las singularidades normativas de cada área de actividad, garantizando siempre que ninguna decisión ejecutiva vulnere los requisitos mínimos de seguridad exigidos por el nivel MEDIO del ENS.

- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.

Los integrantes del Comité de Seguridad serán designados en un acta fundacional, donde se indicará la persona designada y el cargo que deberá ostentar.

El Secretario del Comité de Seguridad será el RESPONSABLE DE SEGURIDAD y tendrá como funciones

- Convoca las reuniones del Comité de Seguridad.
- 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.
- El Comité de Seguridad reportará al CEO.

Responsable de la Información

- Responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.
- Responsable último de cualquier error o negligencia que conlleve un incidente de confidencialidad o de integridad (en materia de protección de datos) y de disponibilidad (en materia de seguridad de la información).
- Establecer los requisitos de la información en materia de seguridad.
- Determinar y aprobar los niveles de seguridad de la información.
- Aprobar la categorización del sistema con respecto a la información.
- Los que se vayan indicando en los documentos dentro del alcance del ENS.
- Validar los requisitos de seguridad en sus respectivas dimensiones (Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad)
-

Responsable del Servicio

- Establecer los requisitos del servicio en materia de seguridad.
- Determinar los niveles de seguridad de los servicios.
- Aprobar la categorización del sistema con respecto a los servicios.
- Los que se vayan indicando en los documentos dentro del alcance del ENS.
- Validar los requisitos de seguridad en sus respectivas dimensiones (Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad)

Responsable de la Seguridad

Sus funciones serán las siguientes

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a 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.
- Aprobar la declaración de aplicabilidad.
- Canalizar y supervisar, tanto el cumplimiento de los requisitos de seguridad del servicio que se presta o solución que provee, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio (POC).
- Los que se vayan indicando en los documentos dentro del alcance del ENS.

El Responsable de la Seguridad será el secretario del Comité de Seguridad con las funciones indicadas en el apartado 3.5.1 de la presente política.

De conformidad con el principio de “segregación de funciones y tareas” recogido en el art. 10 del ENS, el Responsable de la Seguridad será una figura diferenciada del Responsable del Sistema.

Responsable del Sistema

Sus funciones serán las siguientes:

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.
- Potestad para proponer la suspensión del tratamiento de una cierta información o la prestación de un determinado servicio si aprecia deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.
- Los que se vayan indicando en los documentos dentro del alcance del ENS.

Responsable de Privacidad

Sus funciones serán las siguientes:

- Coordinar todos los aspectos relacionados con la adecuación de las actuaciones de **RELLEU TELECOM** en materia de protección de datos de carácter personal.

- Coordinar, junto con el Responsable de Seguridad, el cumplimiento del ENS con respecto a la protección de datos de carácter personal.

7.2 Procedimientos de designación

La designación del Responsable de Seguridad y de todos estos cargos compete exclusivamente al Comité de Seguridad. Dicho nombramiento se revisará cada dos años, o bien cuando se requiera la sustitución de los encargados por ausencias de larga duración o bajas que puedan comprometer la operatividad del sistema.

7.3 Revisión de la Política de Seguridad

Será misión del Comité de Seguridad la revisión anual de esta Política de Seguridad y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por la Alta Dirección y difundida para que la conozcan todas las partes afectadas.

7. TRATAMIENTO DE DATOS PERSONALES

RELLEU TELECOM trata datos de carácter personal especialmente sensibles. La entidad se rige estrictamente por los principios de: licitud, transparencia y lealtad; limitación de la finalidad; minimización de datos; exactitud; limitación del plazo de conservación; seguridad; y responsabilidad activa o demostrada

8. GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año
- Cuando cambie la información manejada
- Cuando cambien los servicios prestados
- Cuando ocurra un incidente grave de seguridad
- Cuando se reporten vulnerabilidades graves
- Cuando ocurran cambios significativos en la tecnología subyacente o en el entorno de amenazas.

Para la armonización de los análisis de riesgos, el Comité de Seguridad establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

La presente política determina las estrategias de tratamiento de riesgos y formaliza el protocolo de aceptación del riesgo residual, exigiendo una autorización explícita y motivada de la dirección para todo riesgo que supere el umbral de tolerancia institucional.

9. DESARROLLO DE LA POLÍTICA DOCUMENTAL

La documentación de seguridad está estructurada en tres niveles:

- Primer nivel (Política): Aprobada por la Alta Dirección (CEO) y revisada anualmente.
- Segundo nivel (Normativas y Procedimientos): Deben ser aprobados formalmente por el Comité de Seguridad.
- Tercer nivel (Registros y Evidencias): Gestionados por el Responsable del Sistema y el de Seguridad

La Política de Seguridad define la asignación de responsabilidades para cada activo de información gestionado por el sistema. Dicha relación se encuentra formalizada en el registro DG08.R01_Inventario SI, donde se identifica al Responsable de la Información basándose en la categorización y sensibilidad de los datos para los servicios incluidos en el alcance del sistema.
El personal tendrá acceso a la información relevante en el siguiente repositorio:

https://drive.google.com/drive/folders/1tjWV8QjjrZxIf06_3r7L1AnhzqDmqgaw

10. OBLIGACIONES DEL PERSONAL

Es obligación de todos los miembros de **RELLEU TELECOM** conocer y cumplir esta Política y sus normativas. La empresa garantiza programas de formación para todo el personal y, obligatoriamente, asistencia a una sesión de concienciación sobre seguridad de la información al menos una vez al año.
Las personas con responsabilidad en el uso, operación o administración de sistemas 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 se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

11. TERCERAS PARTES, PROVEEDORES Y CLIENTES

Cuando se presten servicios a terceros o se contraten proveedores, se les hará partícipes de esta Política, garantizando que su personal disponga del mismo nivel de concienciación y exigiendo procedimientos conjuntos de reporte de incidentes. Las terceras partes asumirán de forma contractual las obligaciones de esta normativa, pudiendo implantar sus propios procedimientos para satisfacerlas. Para garantizar la coordinación, se definirán protocolos específicos de reporte y resolución de incidencias.
En la adquisición de derechos de uso de activos y servicios en la nube, se garantizará el cumplimiento de los requisitos establecidos en las medidas de seguridad del Anexo II del ENS

para el nivel MEDIO, así como las directrices específicas de la Guía CCN-STIC correspondiente y las normativas internas de desarrollo seguro

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. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

12. GESTIÓN DE INCIDENTES DE SEGURIDAD

Los departamentos dispondrán de mecanismos para prevenir, detectar, reaccionar y recuperarse de incidentes. Esto incluye la designación de un punto de contacto (POC) y la colaboración para el intercambio de información con Equipos de Respuesta a Emergencias (CERT) Y de acuerdo al Artículo 8 del ENS.
Dentro del amparo de lo anterior, se encuentra embebida la protección de la privacidad. Nuestros sistemas tratan datos personales y por ello, la protección de la privacidad se erige como un pilar esencial en el marco de SGSI y se constituye como una necesidad social que las empresas deben respetar y proteger, así como objeto de legislación y/o regulación específica en todo el mundo.

12.1 Prevención

Los departamentos deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello los departamentos deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos deben:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

12.2 Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de

manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

12.3 Respuesta

Los departamentos deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

12.4 Recuperación

Para garantizar la disponibilidad de los servicios críticos, los departamentos deben desarrollar planes de continuidad de los sistemas como parte de su plan general de continuidad de negocio y actividades de recuperación.

RELLEU TELECOM está convencida de que una gestión eficaz de la Seguridad de la Información y de la Privacidad es un elemento habilitador para que la organización comprenda completamente y actúe de modo adecuado a los riesgos a los que la información es expuesta, así como para poder responder y adaptarse de manera eficiente a los crecientes requerimientos de organismos reguladores, leyes, y por supuesto sus clientes

.