

POLÍTICA

SEGURIDAD DE LA INFORMACIÓN

ENS

USO PÚBLICO

INDICE

1. OBJETO 3

2. REFERENCIAS 3

3. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 3

3.1. la organización 3

3.2. misión de la organización 3

3.3. El marco regulatorio en el que se desarrollamos nuestras las actividades. 4

3.4. Los roles o funciones de seguridad. 4

3.4.1. Punto único de contacto 5

3.5. La estructura y composición del comité para la gestión y coordinación de la seguridad. 6

3.6. Las directrices para la estructuración de la documentación de seguridad 6

3.7. Los riesgos que se derivan del tratamiento de los datos personales. 6

4. control de ediciones 6

Aprobado por:

Comité de Seguridad

Firmado:

Wenceslao Sánchez de la Peña

Director General

1. OBJETO

Este documento establece la Política de Seguridad de la Información de TELECOM CLM, alineada con el Esquema Nacional de Seguridad (ENS), para proteger la información tratada en el marco de sus actividades.

Aplica a los sistemas, servicios, procesos, personal y terceros que gestionen información o activos asociados a servicios de telecomunicaciones y tecnologías de la información de TELECOM CLM.

2. REFERENCIAS

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

3. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

3.1. LA ORGANIZACIÓN

TELECOM CLM tiene por objeto la prestación de servicios relacionados con telecomunicaciones y tecnologías de la información, con el objetivo estratégico de ofrecer productos y servicios competitivos y adecuados a las necesidades del mercado.

La apertura a redes públicas y nuevas tecnologías incrementa la exposición y los riesgos asociados a la información y comunicaciones, por lo que esta Política define las directrices para gestionarlos.

3.2. MISIÓN DE LA ORGANIZACIÓN

Telecom Castilla-La Mancha (Telecom CLM) es la operadora nacional de telecomunicaciones que garantiza el acceso y la difusión de las nuevas tecnologías a ciudadanos y empresas en Castilla-La Mancha. Ofrecemos una amplia gama de servicios de telecomunicaciones, incluyendo:

- **Operador neutro**. Proporcionamos infraestructuras compartidas para operadores locales, autonómicos y nacionales, facilitando la expansión de sus servicios en la región.
- **Televisión y radio**. Nos encargamos de la transmisión y mantenimiento de señales de televisión digital terrestre y radio FM, asegurando una cobertura óptima en toda Castilla-La Mancha.
- **Banda ancha e internet rural**. Ofrecemos soluciones de conectividad de alta velocidad tanto para zonas urbanas como rurales, reduciendo la brecha digital y promoviendo el desarrollo tecnológico en áreas menos accesibles.
- **Red de emergencias y servicios críticos**. Implementamos y gestionamos redes de comunicación esenciales para servicios de emergencia, garantizando una respuesta rápida y eficiente en situaciones críticas.
- **Ingeniería y consultoría en telecomunicaciones**. Brindamos asesoramiento experto y desarrollamos proyectos a medida para empresas y administraciones públicas, optimizando sus infraestructuras de comunicación.
- **Servicios IoT y soluciones personalizadas**. Facilitamos la implementación de tecnologías de Internet de las Cosas, permitiendo a las empresas mejorar su eficiencia operativa y ofrecer nuevos servicios a sus clientes.

Esta Política establece un marco preventivo, reactivo y de mejora para asegurar confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.

3.3. EL MARCO REGULATORIO EN EL QUE SE DESARROLLAMOS NUESTRAS LAS ACTIVIDADES.

TELECOM CLM se compromete a cumplir los requisitos legales y normativos aplicables, y los requisitos suscritos con clientes y partes interesadas en materia de seguridad de la información.

En el desarrollo de nuestras actividades, estamos comprometidos con el cumplimiento de los requisitos legales establecidos en:

- 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 (vigente en aquellos artículos que no contradigan el RGPD)
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.
- Ley 2/2019, de 1 de marzo, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, y la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017.
- DIRECTIVA 2014/26/UE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 26 de febrero de 2014 relativa a la gestión colectiva de los derechos de autor y derechos afines y a la concesión de licencias multiterritoriales de derechos sobre obras musicales para su utilización en línea en mercado interior
- Ley 1/2019, de 20 de febrero, de Secretos Empresariales.
- Ley 10/2021, de 9 de julio, de trabajo a distancia.
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

3.4. LOS ROLES O FUNCIONES DE SEGURIDAD.

TELECOM CLM se compromete a:

- Integrar la seguridad en la operativa habitual y desde el diseño de procesos y sistemas (seguridad “desde el diseño”).
- Mantener inventarios actualizados de activos/servicios y gestionar riesgos y cambios de forma continua.
- Clasificar la información según su importancia y aplicar controles de tratamiento, almacenamiento, transmisión y destrucción acordes.

Por este motivo, se han establecido los siguientes roles de seguridad:

Responsable de la información. Esta figura recae en el Comité de Seguridad de la Información. Es el órgano encargado de determinar los requisitos de seguridad de la información tratada, aprobando los niveles de seguridad de la información. Entre sus funciones se incluye la aprobación de esta política de seguridad.

Responsable del servicio. Valora impactos sobre los servicios y asegura la continuidad y calidad del servicio.

Responsable de seguridad. Determina las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los responsables de la información y de los servicios.

Participa en la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones seleccionando, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a su juicio.

Las medidas del Anexo II del ENS, así como aquellas otras necesarias para garantizar el adecuado tratamiento de datos personales podrán ser ampliadas por causa de la concurrencia indicada o del prudente arbitrio del responsable de la Seguridad del sistema, habida cuenta del estado de la tecnología, la naturaleza de los servicios prestados y la información manejada, y los riesgos a que están expuestos.

Es el responsable de aprobar la declaración de aplicabilidad que incluya las medidas del Anexo II del Esquema Nacional de Seguridad.

Es el responsable de analizar y determinar las medidas compensatorias de forma justificada mediante su aprobación formal.

Analizar y supervisar los supuestos concretos de utilización de las infraestructuras y servicios comunes de la organización.

Analizar los informes de auditoría, y encargarse de que se adopten las medidas correctivas adecuadas.

Responsable del sistema de información. Se encarga de la operación del sistema de información, atendiendo a las medidas de seguridad determinadas por el responsable de la Seguridad.

Delegado de protección de datos. Es la persona encargada de determinar los fines y los medios del tratamiento de la información que contenga datos de carácter personal, y se asegura de que se cumplen los requisitos establecidos en el reglamento general de protección de datos y la ley orgánica de protección de datos y garantía de los derechos digitales.

Estos roles son desempeñados por los miembros de la organización designados por el Comité de Seguridad sin una duración determinada hasta que decida su renovación.

En el caso de que durante la realización de alguna actividad se requiriese su coordinación o mediación en la resolución de un conflicto, éste será elevado al Comité de Seguridad para su resolución.

Para los demás puestos de trabajo se han establecido sus funciones y responsabilidades en sus perfiles de puesto de trabajo.

3.4.1. Punto único de contacto

Se ha establecido como punto de contacto (POC) para notificar cualquier asunto relativo a la seguridad de la información la dirección de correo electrónica: **it@telecomclm.es**

3.5. LA ESTRUCTURA Y COMPOSICIÓN DEL COMITÉ PARA LA GESTIÓN Y COORDINACIÓN DE LA SEGURIDAD.

El Comité de Seguridad de la Información se encuentra compuesto por:

- Dirección General.
- Responsable de seguridad.
- Responsable del sistema.
- Responsable de los servicios.
- Delegado de protección de datos.

El Comité de Seguridad realiza las funciones de responsable de la información, coordinación de las actividades desarrolladas por los cargos nombrados para garantizar la seguridad y actúa como máximo órgano de decisión con los otros miembros de la organización.

3.6. LAS DIRECTRICES PARA LA ESTRUCTURACIÓN DE LA DOCUMENTACIÓN DE SEGURIDAD

La documentación de seguridad se estructura de forma jerárquica: Política → Manual/Normativa → Procedimientos/Instrucciones → Registros de evidencia.

El acceso se limita por control de accesos y principio de mínimo privilegio, garantizando trazabilidad y custodia de evidencias del Sistema de Gestión.

3.7. LOS RIESGOS QUE SE DERIVAN DEL TRATAMIENTO DE LOS DATOS PERSONALES.

Cuando TELECOM CLM trate datos personales propios o de clientes, aplicará controles adecuados conforme a la normativa aplicable y evaluará riesgos y medidas en función del tipo de tratamiento y su criticidad.

En caso de encargos de tratamiento con terceros, se formalizarán acuerdos y requisitos de seguridad proporcionales al riesgo.

4. CONTROL DE EDICIONES

EDICION	MOTIVO DEL CAMBIO	FECHA
1	Primera elaboración de la política	17/1/2026