Política de Seguridad de la Información

ÍNDICE

1. Contexto

El Consejo de Administración de Cellnex Telecom, S.A. (en adelante, "Cellnex Telecom", la "Compañía" o la "Organización") tiene, entre sus funciones como máximo órgano de gobierno, la de determinar las políticas generales de la Compañía. En el ejercicio de esta función, ha establecido la presente Política Global de Seguridad de la Información para todas las sociedades del Grupo Cellnex.

Esta política se implementa a través de un Sistema de Gestión de Seguridad de la Información (en adelante, "SGSI"), diseñado para garantizar la gestión sistemática de los riesgos de seguridad de la información, la protección de los activos y la mejora continua de los controles de seguridad de manera unificada y estructurada.

2. Marco de referencia

Esta política establece directrices y principios para garantizar la correcta implantación y gestión de la seguridad en el marco del Sistema de Gestión de Seguridad de la Información y de los requisitos de las normas ISO bajo las cuales la Compañía está certificada en materia de seguridad de la información.

La Política está alineada con estándares internacionales de referencia e iniciativas voluntarias a las que se adhiere Cellnex Telecom, incluyendo las siguientes:

- Norma ISO 27001.
- Norma ISO 22301.
- Esquema Nacional de Seguridad (ENS).
- NIST (Instituto Nacional de Estándares y Tecnología).

La Política respalda y debe interpretarse conjuntamente con, entre otras, las siguientes políticas corporativas:

- Política de Sostenibilidad
- Política de Seguridad y Salud en el Trabajo
- Política de Medioambiente y Cambio Climático
- Política Energética
- Política de Calidad y Sistema Integrado de Gestión
- Política Antisoborno, Regalos y Hospitalidad
- Política Global de Gestión de Riesgos
- Política de Relación con Grupos de Interés
- Política de Compras
- Política de Derechos Humanos

3. Propósito y alcance

Propósito:
Esta política establece las directrices y líneas de actuación en materia de Seguridad de la Información que regirán la forma en que **Cellnex Telecom** gestionará y protegerá su información y sus servicios, así como su comunicación a las partes interesadas y su implantación en todas las sociedades y áreas funcionales del Grupo Cellnex.

Alcance:
Esta política aplica a todas las sociedades que forman parte del Grupo **Cellnex Telecom** y es

responsabilidad de todo su equipo. Asimismo, aplica a todas las personas, independientemente de su vinculación con la Compañía, que utilicen recursos corporativos para llevar a cabo actividades de negocio o interactúen con redes internas y sistemas empresariales, ya sean propiedad de la Compañía o estén arrendados por la misma o por el empleado. Cada país dentro del Grupo Cellnex Telecom es responsable de garantizar el cumplimiento de esta política y de implantarla de acuerdo con la legislación y normativa local aplicable.

Esta política está alineada con y es complementaria al resto de políticas corporativas y normativa interna de **Cellnex Telecom.**

4. Principios básicos

La información es un activo crítico para **Cellnex Telecom**, y es necesario garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la misma, de acuerdo con los estándares reconocidos de gestión de la Seguridad de la Información en la prestación de servicios como operador de infraestructuras de telecomunicaciones para operadores, radiodifusores, Administraciones Públicas y corporaciones.

Cellnex Telecom se compromete a proteger a las personas, las instalaciones, los negocios y la marca mediante los siguientes principios:

Protección de los Activos de Información:

Se adoptan medidas para identificar y prevenir el acceso no autorizado, la modificación, divulgación o destrucción de los activos de información, garantizando que solo se utilicen para los fines aprobados por la Dirección.

Asignación de Recursos:

El equipo de **Cellnex Telecom** dispone de los recursos materiales, formación continua en tecnologías y competencias, así como de procesos de desarrollo para detectar necesidades individuales de acuerdo con esta política y alcanzar los objetivos de negocio.

Responsabilidad del Equipo:

La implicación en la protección de estos activos y en la implantación y mantenimiento de controles de seguridad adecuados es responsabilidad tanto de la Dirección como de todo el equipo de **Cellnex Telecom**.

Mejora Continua:

Operar dentro de un Sistema de Gestión basado en los estándares ISO 27001, centrado en la gestión de personas, la gestión de procesos y la mejora continua para garantizar la eficacia y la eficiencia.

5. Compromisos y líneas estratégicas

Compromiso con la Seguridad de la Información

La información es uno de los activos más valiosos para Cellnex, y su protección es crucial. La protección de la información sigue los principios de **confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad**, garantizando que la información solo sea accesible para personas autorizadas, esté protegida frente a modificaciones no autorizadas y esté disponible cuando se necesite. La organización se compromete a implementar medidas de seguridad de la información.

Todo el modelo de seguridad está centralizado en el área de **Seguridad Corporativa**, responsable de

definir las directrices generales para su cumplimiento local en cada país. Cada país cuenta con un representante de Seguridad de la Información, siendo el **SOC Global** en España, con capacidades CSIRT, el encargado de dar soporte a todas las unidades de negocio.

Gestión de Riesgos y Seguridad desde el Diseño

La organización está comprometida con la gestión de los **riesgos de seguridad de la información** mediante un **enfoque basado en riesgos**. Estos riesgos se identifican, evalúan y tratan mediante la implementación de controles adecuados. Además, se aplica **seguridad desde el diseño y por defecto** en todos los procesos de negocio, servicios y tecnologías, asegurando que la seguridad sea una parte integral de cada desarrollo desde su concepción.

Seguridad de los Recursos Humanos y Formación

Reconociendo que los recursos humanos son clave para la seguridad de la información:

Concienciación:

Proporcionar formación continua a empleados y colaboradores para proteger la información de forma eficaz.

Formación de Empleados:

Asegurar que los empleados conozcan las expectativas de seguridad desde su incorporación y reciban formación continua para detectar y responder a posibles amenazas.

Promoción del Comportamiento Ético:

Integrar la seguridad de la información en las actividades diarias y fomentar que el personal actúe de manera ética y responsable en materia de seguridad.

Gestión de Activos y Control de Accesos

La gestión de activos es una prioridad, con Cellnex Telecom implementando:

Clasificación e Inventario de Activos:

Garantizar que todos los activos de información estén clasificados y protegidos adecuadamente según su sensibilidad e importancia, siguiendo las directrices internas de clasificación y las normativas de protección de datos.

Mecanismos de Control de Acceso:

El acceso a estos activos se controla mediante **estrictos mecanismos** que solo permiten a personal autorizado interactuar con información sensible.

Protección Criptográfica:

Se utilizan técnicas criptográficas cuando es necesario para proteger la integridad y confidencialidad de los datos críticos.

Auditorías de Seguridad:

Auditorías periódicas para evaluar el cumplimiento e identificar áreas de mejora.

Gestión de vulnerabilidades y Pruebas de Penetración:

Escaneos y pruebas periódicas para detectar y corregir vulnerabilidades de seguridad.

Notificación y Gestión de Incidentes:

Las normas y estándares internos de **Cellnex Telecom**, junto con los procesos formales de notificación y gestión de incidentes, garantizan la identificación, notificación y resolución oportuna de incidentes de seguridad y cualquier irregularidad en el cumplimiento de las políticas. Todas las excepciones a esta Política deben estar debidamente documentadas, seguir los procedimientos establecidos y contar con la aprobación explícita del Consejo de Administración de Cellnex Telecom, S.A.

Métricas e Informes:

Monitorización continua de sistemas e indicadores clave (KPIs) relacionados con el Control de Riesgo Operacional (ORC).

Relación con Proveedores y Seguridad de Terceros

La gestión de la seguridad de la información en colaboración con terceros es esencial. La organización implementa prácticas de gestión de riesgos de terceros para asegurar que colaboradores externos y proveedores cumplan con los mismos estándares de seguridad.

Análisis e Identificación de Riesgos:

Identificar y analizar los riesgos de seguridad asociados a terceros a lo largo de todo el ciclo de vida de la relación con proveedores.

Implementación de Controles:

Aplicar controles de seguridad y realizar evaluaciones periódicas para garantizar que los terceros cumplen con los requisitos de seguridad de **Cellnex Telecom.**

Obligaciones Contractuales:

Asegurar que los requisitos de seguridad, incluidos acuerdos específicos de nivel de servicio (SLAs) en materia de seguridad de la información, estén claramente definidos e incorporados en los contratos con terceros.

Cumplimiento de la Normativa Legal y Regulatoria

El cumplimiento de **requisitos legales, regulatorios y contractuales** es fundamental. La organización se compromete a cumplir las leyes y normativas aplicables dentro de su ámbito, incluyendo, entre otras, el cumplimiento del RGPD. Esto garantiza que las prácticas de seguridad de la información estén alineadas con los requisitos legales actuales y futuros. El equipo de DPO colabora estrechamente con Global Security para asegurar el cumplimiento del RGPD. Se realizan auditorías y evaluaciones periódicas para garantizar el cumplimiento continuo.

Gestión de Incidentes y Continuidad de Negocio

Cellnex Telecom mantiene procesos sólidos para gestionar incidentes y garantizar la continuidad del negocio:

Gestión de Incidentes:

Implementación de un proceso bien definido para identificar, notificar y gestionar incidentes de seguridad de la información de forma rápida. Esto incluye el uso de un equipo CSIRT que opera 24/7 y el uso de capacidades DFIR para mejorar la detección y respuesta ante incidentes.

Planificación de Continuidad de Negocio:

Mantenimiento de planes integrales de continuidad de negocio que describen los procedimientos para mantener las operaciones críticas durante y después de incidentes significativos. Esto incluye planes de recuperación ante desastres (DRP) adaptados a los escenarios de contingencia identificados.

Seguridad Física y Ambiental

Proteger los activos físicos de Cellnex Telecom y la información sensible que gestionan, evitando accesos no autorizados mediante perímetros de seguridad establecidos y la implantación de sistemas de seguridad como alarmas de intrusión y controles de acceso cuando sea necesario.

Adquisición, Desarrollo y Mantenimiento de los Sistemas

Garantizar la seguridad por defecto, desde el diseño, en las aplicaciones desarrolladas internamente

por Cellnex Telecom durante las fases de desarrollo o implantación del software.

6. Responsabilidades

Consejo de Administración de Cellnex Telecom S.A. y CEO:

Garantizan la provisión de los recursos necesarios para la ejecución de los procesos de seguridad e integran la seguridad de la información en la toma de decisiones organizativas. Este compromiso de liderazgo asegura que la seguridad de la información sea una prioridad en toda la organización y que todos los empleados comprendan sus roles y responsabilidades en el mantenimiento de los estándares de seguridad.

Director de Seguridad de la Información (CISO):

Responsable de la gestión operativa de la seguridad de la información, incluyendo la elaboración y el mantenimiento de los estándares de seguridad incluidos en el Marco de Seguridad de la Información como parte del Sistema de Gestión de Seguridad de la Información, los controles para hacer cumplir dichos estándares y la provisión de asesoramiento y orientación sobre su implementación y mantenimiento.

Equipo de CSIRT:

Gestiona todos los incidentes de seguridad de la información (noc.security@cellnextelecom.com) y todos los incidentes que involucren datos personales con el equipo de privacidad de datos RGPD (personaldata@cellnextelecom.com).

Empleados, Contratistas, Consultores y Personal Temporal

Son plenamente responsables de cumplir con esta política y de proteger los activos de información en todas las etapas del tratamiento de la información.

Directores Generales de País y Representantes de Seguridad de País:

Implementan la política dentro de sus áreas de responsabilidad y garantizan que su personal cumpla con la misma.

Oficina de Seguridad de la Información:

Gestiona las operaciones diarias de seguridad de la información, incluyendo la monitorización, la respuesta a incidentes y las actividades de cumplimiento.

7. Desarrollo normativo interno

El Departamento de Global Security a nivel de Grupo y, cuando proceda, las áreas locales correspondientes, serán responsables de desarrollar los principios contenidos en esta política mediante la elaboración y aprobación de la normativa interna necesaria, de acuerdo con los procedimientos establecidos a tal efecto.

8. Aprobación, revisión, control y comunicación de la Política

Aprobación	Tras la recomendación previa del Comité de Auditoría y Gestión de Riesgos, el Consejo de Administración de Cellnex Telecom, S.A. aprobó la actualización de esta Política Global de Seguridad de la Información el 25/03/2026.
Revisión	El Departamento de Global Security revisará y propondrá actualizaciones de esta Política siempre que lo considere necesario o cuando se produzcan cambios significativos que puedan afectar a su contenido o aplicación. Estas revisiones garantizan que Cellnex se mantenga en cumplimiento con la legislación y normativa vigentes.
Control	El Departamento de Global Security es responsable de garantizar el cumplimiento de esta Política, en colaboración con todas las unidades corporativas y de negocio de la compañía. Cada área contribuye activamente a la aplicación de los principios y compromisos establecidos, asegurando que las prácticas operativas y estratégicas estén alineadas con los objetivos de seguridad de Cellnex Telecom.
Comunicación	El Departamento de Global Security se compromete a comunicar periódicamente sus avances en el cumplimiento de esta política a todas las partes interesadas internas y externas, en línea con este principio de transparencia. Asimismo, promoverá la concienciación y el cumplimiento de esta Política, que estará permanentemente disponible en el sitio web de la compañía.

9. Control de cambios

Versión	Elaborado por	Validez
1	Global Security	05/04/2019
2	Global Security + Revisado por Compliance	25/03/2026