Política sobre seguridad y ciberseguridad de los sistemas de información

Políticas corporativas 2025

Índice

01

Finalidad

El objetivo de la presente Política sobre Seguridad y Ciberseguridad de los Sistemas de Información (en adelante, la “Política”), que forma parte de la Política marco de Cumplimiento, es fijar y difundir las normas básicas y generales de Konecta, grupo multinacional de sociedades especializadas en la prestación de servicios y soluciones digitales de *customer management* (en adelante, Konecta, la Empresa, la Sociedad o la Compañía), para garantizar la integridad, privacidad y confidencialidad de la información, de conformidad a la legislación vigente en la materia, ponderando los riesgos y realizando un uso eficiente de los recursos, todo ello, en base a criterios de proporcionalidad en la gestión.

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se pueden producir conflictos y agresiones, y existen ciber amenazas que atentarán contra Konecta y sus diferentes compañías.

La presente Política establece un marco de referencia que sienta los principios para asegurar la protección de los sistemas de información de Konecta frente accesos no autorizados, pérdida o daños durante el procesamiento de la información u otro tipo de ciber amenazas, garantizando la disponibilidad, integridad y confidencialidad de la información de los datos gestionados por Konecta.

Esta Política se diseña para establecer el marco de referencia para los grupos de interés de Konecta internos (empleados, accionistas, inversores, directivos) y externos (clientes, proveedores, auditores gobiernos, entes reguladores, medios de comunicación, competidores y entidades financieras), potenciando la confianza en los sistemas de información de la compañía, velando por el escrupuloso cumplimiento de la normativa vigente en la materia en cada país, requerimientos propios, y estándares internacionales.

Esta Política estará disponible en la web corporativa (konecta.com) para garantizar que pueda ser consultada por todas las partes interesadas.

02

Ámbito de aplicación

La presente Política se encuentra incluida en el ámbito de aplicación de la Política marco de Cumplimiento y se extiende a todas las entidades de Konecta, respaldada por la dirección general de la compañía.

En consecuencia, su contenido se constituye de necesaria observancia para todas las personas trabajadoras de Konecta, independientemente del cargo o función que ocupen dentro de la organización o su ubicación geográfica.

Sin perjuicio de lo anterior, su ámbito de aplicación podrá extenderse, cuando sea necesario y posible por la naturaleza de la relación, a todas aquellas personas físicas y/o jurídicas vinculadas empresarial o profesionalmente con Konecta, por una relación distinta de la laboral: proveedores, contratistas y trabajadores de la cadena de suministro, y socios comerciales.

Dado que muchas de las sociedades de Konecta tienen su domicilio social fuera de la Unión Europea, se adaptará la regulación interna a la normativa propia de cada Estado en caso necesario, respetando y velando por los principios básicos aquí recogidos.

03

Principios generales de actuación

La Política sobre Seguridad y Ciberseguridad de los Sistemas de Información refleja el compromiso expreso de la Empresa para determinar y establecer las directrices y el soporte adecuado para la administración de la seguridad de la información que maneja, de acuerdo con los requerimientos propios y con las leyes y regulaciones vigentes.

Konecta vela por garantizar “un uso seguro de las redes y los sistemas de información a través del fortalecimiento de nuestras capacidades de prevención, defensa, detección, análisis, investigación, recuperación y respuesta frente a los ciberataques” que pudieran ocurrir.

Konecta aboga por potenciar un uso seguro de los sistemas de información y las telecomunicaciones, siempre manteniéndose alineado con la estrategia y objetivos del negocio y, en esta línea, se ha fijado entre sus objetivos específicos, los siguientes, siendo estos coherentes con el contexto donde se desarrollan las actividades de la compañía:

- Impulso de la seguridad y resiliencia de las redes y sistemas de información usados.
- Sensibilización a todo el personal de la compañía de los riesgos derivados del ciberespacio.
- Capacitar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas para sustentar los objetivos de Konecta en materia de ciberseguridad.

En este sentido, Konecta se compromete a lograr los siguientes objetivos:

- Considerar la información y los sistemas que la soportan como activos estratégicos. Así pues, Konecta manifiesta su determinación de alcanzar los niveles de seguridad necesarios que garanticen los requisitos de confidencialidad, integridad y disponibilidad de la información procesada en la organización y de los recursos de los sistemas de información que la procesan, almacenan o distribuyen.
- Garantizar la difusión de la normativa definida como soporte de esta Política, con el objetivo de conseguir infundir al personal trabajador de Konecta un nivel de concienciación y formación, en materia de seguridad de la información, que garantice la aplicación de prácticas adecuadas en esta materia, como elemento inherente al desarrollo de sus funciones.
- Promover que la consecución de los niveles de seguridad de la información requeridos se desarrolle, como un proceso continuo de mejora y progreso constante, sustentado en la definición de los objetivos y requisitos a cumplir, la implantación de los procesos y medidas oportunos, la comprobación de su efectividad, eficacia y eficiencia, y la adopción de las correcciones y modificaciones que resulten adecuadas.
- La presente Política debe ser la principal herramienta para garantizar adecuadamente la Seguridad de la Información, promoviendo y asegurando su cumplimiento dentro de los diferentes servicios.
- Velar por la existencia de los mecanismos necesarios que aseguren la continuidad de las actividades críticas de la empresa que estén sustentadas en los sistemas de información, permitiendo la recuperación de los mismos en un periodo de tiempo aceptable.

- Maximizar la calidad de los servicios prestados.
- Reducir o eliminar en la medida de lo posible, los peligros y riesgos en los activos, procesos y servicios que Konecta proporciona.
- Determinar medidas esenciales de seguridad de la información que Konecta debe adoptar para protegerse apropiadamente contra amenazas que podrían afectar en alguna medida la confidencialidad, integridad y disponibilidad de la información.

Los objetivos de la presente Política se implantarán basándose en una estrategia a largo plazo. Las actividades para alcanzar los objetivos deben ser mantenidas durante el tiempo.

Siguiendo con los riesgos de seguridad, los planes de acción deben ser definidos y ajustados cada año (controles de seguridad, definición de proyectos de seguridad, monitorización continua, etc.).

Se establecerán los planes de transición necesarios que reducir cualquier impacto en las actividades y/o los recursos de Konecta e igualmente esta velará para que las personas trabajadoras:

- ... conozcan y apliquen los procedimientos internos y protocolos en materia de seguridad de la información de Konecta.
- …dispongan de herramientas con las que puedan tener acceso sencillo a los procedimientos internos operativos (Intranet), adicionalmente se utilizarán canales de comunicación alternativos para la comunicación de ciertos procesos, medidas especiales o actualización de procedimientos.
- …sean conscientes de que deben procesar únicamente la información a la que han sido autorizados y usar los activos de Konecta únicamente para el desempeño de sus funciones profesionales. Las personas trabajadoras deberán cumplir con las normas básicas de acceso a aplicaciones y/o equipos con acceso a datos de carácter personal.
- …conozcan los procedimientos existentes en la compañía para saber cómo actuar ante cualquier actividad o amenaza que pueda afectar a la seguridad de la información, debiendo informar al Departamento de Tecnología y al Director de Seguridad (CISO).

Conscientes de que cada uno de los países en los que la compañía opera cuenta con un contexto social y con unas necesidades diferentes, la presente Política se articula a través de planes y acciones relacionados con los principios contemplados en la misma, adaptados a la realidad de cada una de sus operaciones locales.

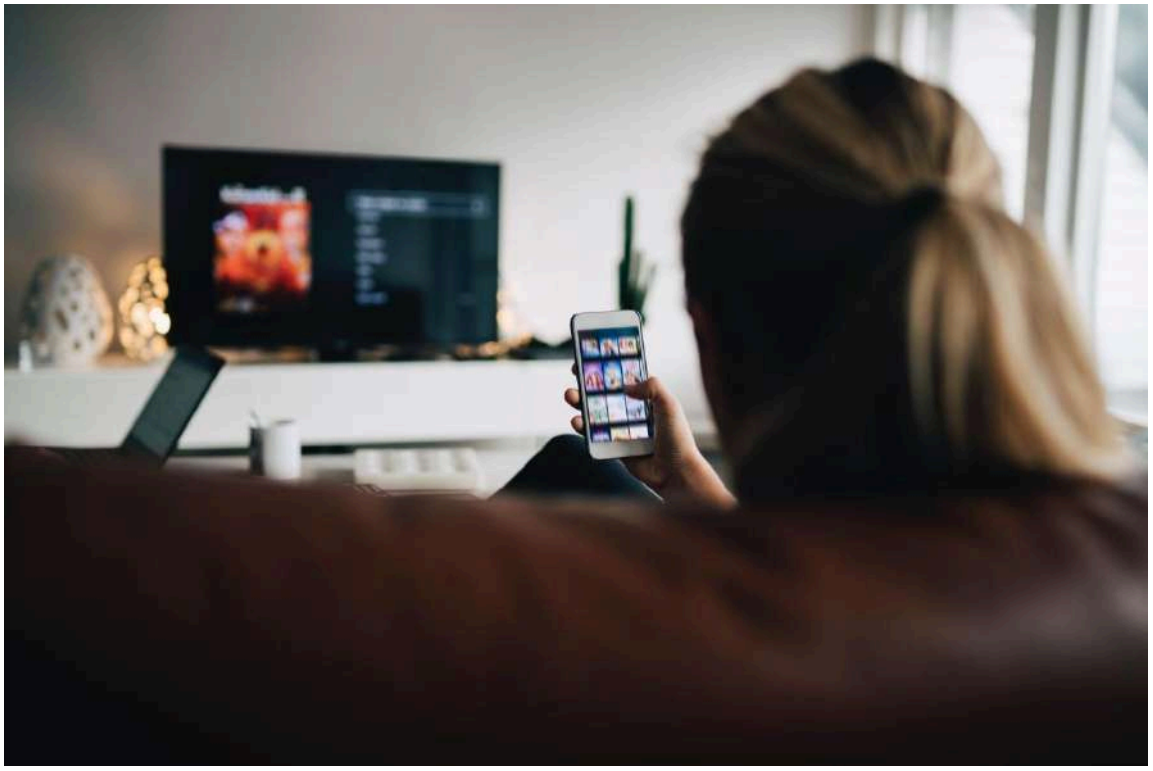
Estos principios de actuación dan respuesta a los impactos, riesgos y oportunidades (IROs) derivados de los temas materiales aplicables: seguridad de la información, transformación digital, cumplimiento y ética corporativa, y gestión de proveedores.

Tanto las personas trabajadoras como cualquier tercero que presuman la existencia de cualquier potencial incumplimiento vinculado a la presente Política o al Código Ético, podrán transmitir sus informaciones, dudas o inquietudes en esta materia, de manera confidencial y sin temor a represalias, a través de los Canales de Información disponibles en la web corporativa de Konecta (https://konecta.integrityline.com), según la naturaleza de la situación, de conformidad con el procedimiento PG COR 26 Canales de Información, disponible en el mismo espacio, en el cual se especifican los

diferentes canales disponibles y la naturaleza de la comunicación que se puede realizar a través de los mismos.

Este canal se encuentra disponible las 24 horas del día, los 7 días de la semana. No se tolerará ninguna represalia contra quien, de buena fe, comunique hechos que pudieran constituir un incumplimiento de esta política y aplicará a los comunicantes las garantías y protecciones establecidas por la normativa y legislación aplicable.

El incumplimiento de la presente política estará sujeto a las medidas disciplinarias correspondientes acorde con las normas y procedimiento internos, sin perjuicio de las sanciones administrativas o penales que, en su caso, puedan también resultar de ello y que sean impuestas por la autoridad competente.



04

Actualización y revisión

La presente Política sienta las bases del cumplimiento de las siguientes normativas:

- ISO/IEC 27001:*2022 Information technology -Security techniques-Information security management systems - Requirements*.
- ISO/IEC 27701- Extensión de la ISO 27001 para la gestión de la privacidad.
- ISO/IEC 27002:2022 *Information technology - Security techniques - Code of practice for information security controls.*
- 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) (Texto pertinente a efectos del EEE).
- Leyes en materia de Protección de Datos Personales que sean de aplicación en cada país.

La Política sobre Seguridad y Ciberseguridad de los Sistemas de Información se revisará periódicamente o cuando sea necesario, para ajustarla a los cambios en el modelo de negocio, a la aprobación de nueva normativa o a las mejores prácticas internacionales, garantizando su efectividad y cumplimiento continuo.

NOTA: La presente Política ha sido revisada y aprobada el 16 de diciembre de 2025 por el máximo órgano de gobierno y sustituye a cualquier versión anterior del mismo, siendo válido solo este documento a partir de la fecha.

Control de ediciones

Edición	Fecha de revisión	Revisado	Validado	Aprobado	Motivo del cambio
2	22/06/2021	TI_Seguridad de la Información Organización y Procedimientos	Asesoría Jurídica	Consejo de Administración	Revisión general de la política
3	19/12/2022	TI_Seguridad de la Información Organización y Procedimientos	Asesoría Jurídica	Consejo de Administración	Revisión general de la política
4	16/12/2025	TI_Seguridad de la Información Organización y Procedimientos	Asesoría Jurídica	Consejo de Administración	Adaptación requisitos legales Adecuación al nuevo formato y a la marca