1. Objetivo y ámbito de aplicación

1.1 Objetivo. Este documento establece los principios y directrices de seguridad de la información del Grupo Abertis y proporciona el marco de referencia por el que Abertis define las directrices de seguridad de la información y las normas por las que se regirán todas las actividades relacionadas con el tratamiento de la información dentro del Grupo.

El objetivo de la Política de Seguridad de la Información, en lo sucesivo denominada "la Política", es:

- Garantizar la protección de la información del Grupo de acuerdo con los criterios de confidencialidad, integridad, disponibilidad, responsabilidad y resiliencia de los datos.
- Establecer los principios generales que el Grupo aplicará para la protección de su información y los activos asociados.
- Proporcionar directrices para el cumplimiento de las leyes y normativas asociadas a la seguridad de la información y el cumplimiento normativo obligatorio.
- Referenciar las directrices de seguridad de la información y los documentos asociados para el tratamiento seguro de la información.

1.2 Ámbito de aplicación. Esta política es de aplicación a todas las empresas controladas[1] por el Grupo Abertis y a todos los terceros colaboradores que mantengan relaciones con el Grupo cuando tengan acceso directo y/o indirecto a información no pública del Grupo Abertis y/o información no pública gestionada por el Grupo Abertis

El Director General de cada empresa velará por que las normas y estándares internos se desarrollen y adapten a esta política y a la legislación aplicable.

2. Principios básicos

La información es uno de los activos que más valor añade al Grupo Abertis y requiere protección contra su uso ilícito, difusión, alteración, destrucción, robo u otros usos indebidos o prácticas ilegítimas. La gestión eficaz de la seguridad de la información permite tratar y reducir los riesgos causados por posibles amenazas y vulnerabilidades a lo largo del ciclo de vida de la información.

El Grupo Abertis está comprometido con la protección de nuestras personas, nuestras instalaciones, los negocios y la marca Abertis a través de los siguientes principios:

- Incluir la seguridad de la información en todos los procesos, servicios y tecnologías siguiendo el principio de "seguridad por diseño y por defecto".

[1] **Empresas controladas:** empresas en las cuales Abertis posee una participación superior al 50 % o, en caso contrario, en cuyos acuerdos con los accionistas consta que Abertis ostenta una posición de control.

- Sensibilizar y formar a todos los empleados sobre los riesgos para la seguridad de la información, proporcionando mecanismos para detectar, informar y reaccionar ante amenazas que puedan poner en peligro la seguridad de la información.
- Gestionar los riesgos de seguridad de la información basándose en una metodología de gestión de riesgos acorde con las normas del Grupo y las mejores prácticas del sector.
- Cumplir todas las obligaciones legales, normativas, industriales y contractuales que afectan a la seguridad de la información en las jurisdicciones en las que opera el Grupo.
- Establecer las medidas organizativas, técnicas y de control necesarias para garantizar la seguridad de la información y la resiliencia de la empresa en cada etapa de la gestión de amenazas e incidentes: identificación, detección, prevención, respuesta y recuperación.
- Garantizar la seguridad de la información en colaboración con terceros identificando, analizando, mitigando y supervisando los riesgos y controles de seguridad de la información en la cadena de suministro antes, durante y al final de la relación contractual.

Esta política, cuando procede, está en consonancia con las normas de mejores prácticas, como ISO/IEC 27002 "Código de buenas prácticas para la gestión de la seguridad de la información", ISO/IEC 27701 "Gestión de la información sobre privacidad", ISO/IEC 22301 "Gestión de continuidad del negocio", ISO 31000 "Gestión de riesgos", normas NIST como 800-14 "Principios y prácticas generalmente aceptados para la seguridad de los sistemas de tecnología de la información", NIST 800-53 "Controles de seguridad y privacidad para sistemas de información y organizaciones" o NIST 800-30 "Guía para la realización de evaluaciones de riesgos", controles de seguridad críticos del CIS para una ciberdefensa eficaz (comúnmente conocidos como "Controles CIS") e ISO/IEC 62443 "Seguridad de redes y sistemas industriales".

Es esencial que los profesionales del Grupo sean conscientes de la importancia de la seguridad de la información como parte de su actividad diaria. Por ello, se les anima a participar activamente en su desarrollo y mejora continua para proporcionar un entorno más seguro para todos.

3. Directrices específicas

3.1 Responsabilidades. La seguridad de la información y de los activos que la respaldan es responsabilidad de cada colaborador y de los Terceros que colaboran con el Grupo Abertis, quienes participarán activamente en esta responsabilidad actuando éticamente en relación con la protección de la información, cumpliendo con las obligaciones contractuales en materia de seguridad de la información y garantizando que solo utilizarán la información y los sistemas de información para la finalidad establecida por el Grupo Abertis.

Abertis establecerá, redactará y mantendrá la Política de Seguridad de la Información del Grupo para reflejar las normas internacionales de seguridad vigentes, los requisitos generales del negocio y los requisitos legales y normativos. Además, Abertis es responsable del desarrollo del marco para la gobernanza de la seguridad de la información en todo el Grupo, teniendo en cuenta los requisitos de negocio, los riesgos identificados, el estado de la tecnología, los controles y las medidas de seguridad aplicables.

3.2 Marco de seguridad de la información. En línea con la normativa del Grupo, cada Unidad de Negocio deberá desarrollar su propio órgano interno de política de seguridad de la información, que establecerá como mínimo:

- Compromiso de gestión.
- Enfoque de la empresa para gestionar la seguridad de la información.
- La definición y asignación de responsabilidades genéricas y específicas en materia de gestión y control de la seguridad de la información.

En relación con la protección de la información, el organismo de seguridad de la información debe regular y orientar sobre las siguientes áreas:

- Gobernanza de la seguridad de la información: incluye no solo los comités de gobernanza, sino también la revisión y actualización periódica de normas, guías y procedimientos para adaptarlos a los cambios y necesidades del negocio, así como a la evolución de los riesgos y los sistemas de protección.
- Gestión de riesgos de seguridad de la información: aplicar una metodología de riesgos y gestionar en consecuencia los riesgos y controles de seguridad de la información.
- Organización de la seguridad de la información: asignación de responsabilidades, separación de funciones, contacto con autoridades y grupos de interés especiales, así como seguridad en la gestión de proyectos.
- Seguridad de recursos humanos: aspectos relacionados con los permisos y funciones de los usuarios y que deben tenerse en cuenta antes, durante y para el cese o cambio de empleo.
- Gestión de activos: responsabilidades de los activos, clasificación de la información y gestión de los activos que contienen información.
- Control de acceso: requisitos de acceso, responsabilidades de los usuarios y acceso a los activos de información.
- Controles criptográficos.
- Seguridad física y medioambiental: garantizar la protección de las zonas y equipos que almacenan información sensible.
- Seguridad de las operaciones: procedimientos y responsabilidades, gestión de vulnerabilidades, protección frente a amenazas, gestión de copias de seguridad, registro de actividades, supervisión y auditoría de sistemas.
- Seguridad de las comunicaciones y las redes, incluida la transferencia de información.
- Seguridad de la Tecnología de Operaciones (OT), incluyendo todas las particularidades para la gestión de la seguridad de la información en los sistemas industriales.

- Adquisición, desarrollo y mantenimiento de sistemas: aplicar la seguridad a lo largo del ciclo de vida del software (SSDLC).
- Uso seguro de las soluciones de inteligencia artificial.
- Relación con los proveedores: evaluar el riesgo para la seguridad de la información de los proveedores y aplicar los controles adecuados antes, durante y después de la relación contractual.
- La gestión de incidentes de seguridad de la información tiene en cuenta todas las fases de un incidente: detección, análisis, respuesta, recuperación, comunicación a las partes interesadas y lecciones aprendidas.
- Gestión de la continuidad del negocio, incluida la gestión del Plan de Continuidad del Negocio ("BCP") y del Plan de Recuperación de Desastres ("DRP").
- Cumplimiento: aplicación de los requisitos legales, reglamentarios y contractuales, así como la revisión del cumplimiento de la Política.

Las políticas, directrices, normas y procedimientos de seguridad de la información deben revisarse y actualizarse periódicamente para adaptarlos a los cambios y necesidades de la empresa, así como a la evolución de los riesgos y los sistemas de protección.

4. Seguimiento y control

- Las reglas y normas internas de cada empresa deben establecer los mecanismos de seguimiento y control utilizados para identificar y notificar cualquier irregularidad en el cumplimiento de la política del Grupo.
- Abertis se reserva el derecho de solicitar a cada empresa la aplicación de los controles internos que considere necesarios.
- Abertis también medirá periódicamente el nivel de cumplimiento en todas las Unidades de Negocio mediante un proceso de evaluación formal.
- Todas las excepciones a esta Política deben hacerse por escrito, seguir procedimientos formales y ser aprobadas formalmente por la dirección del Grupo Abertis.
- El responsable de esta política debe revisarla al menos una vez al año para garantizar que su contenido se ajusta a las necesidades de la empresa, a la situación de riesgo y a los requisitos de seguridad de la información.

Política de Seguridad de la Información_v2
Fecha de publicación: 11/12/2024
Aprobada por: Consejero Delegado