CIRSA

Extracto de la Política de Seguridad de la información

Noviembre/2025

Índice

1. Objetivo

En Grupo CIRSA, la Seguridad de la Información no es solo una obligación normativa, sino un pilar estratégico que sustenta nuestra continuidad operativa, resiliencia tecnológica y protección de datos. Su gestión eficaz refuerza la confianza de nuestros clientes, empleados y socios, protege nuestra reputación corporativa y reduce significativamente los riesgos asociados a incidentes y/o ciberamenazas.

Esta visión trasciende el cumplimiento: implica una cultura de responsabilidad compartida, integrada en cada proceso, sistema y relación con terceros. La seguridad es, por tanto, un compromiso colectivo que involucra a todas las personas que forman parte del Grupo.

El equipo directivo de Grupo CIRSA, en línea con todo lo anterior y siendo consciente del valor que tiene su información y la necesidad de garantizar su disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad, considera fundamental establecer una Política de Seguridad de la Información con el fin de garantizar las operaciones de negocio.

Todo ello, además, con el objeto de cumplir con todas las obligaciones legales, reglamentarias y contractuales que sean necesarias en cada momento de aplicación en materia de seguridad de la información.

Así, procede a la elaboración e implementación de una Política de Seguridad de la Información que regule el marco de Gestión de la Seguridad y las actividades derivadas del mismo.

2. Ámbito de aplicación

Esta Política es aplicable para todo el Grupo CIRSA y/o cualquiera de sus empresas, filiales o sociedades del Grupo con independencia de su ubicación geográfica y de las funciones que le hayan sido encomendadas.

Asimismo, también tiene aplicabilidad sobre todos los empleados, servicios y/o colaboradores externos que tienen acceso y/o utilizan información del Grupo CIRSA. Por lo tanto, esta Política deberá ser accesible para todos ellos.

Los contenidos de esta política traen causa en las directrices definidas en el ordenamiento jurídico vigente, en el estándar de seguridad ISO/IEC 27001:2022, así como en el conjunto de normas de seguridad de Grupo CIRSA.

Lo establecido en el presente documento es de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en la Organización, incluyendo el personal de proveedores externos cuando proceda y sean usuarios de los Sistemas de Información de la Organización.

3. Descripción del contenido de la política

3.1. Principios de la Seguridad de la Información

Dada la importancia que tienen los sistemas de información, la Dirección de Grupo CIRSA establece los siguientes principios fundamentales de seguridad de la información:

Principio de cumplimiento normativo

Todos los sistemas de información se ajustarán a la normativa de aplicación legal regulatoria y sectorial que afecte a la seguridad de la información, en especial aquellas relacionadas con la protección de datos de carácter personal, seguridad de los sistemas, datos, comunicaciones y servicios electrónicos.

Principio de gestión del riesgo

Se deben minimizar los riesgos hasta niveles aceptables y buscar el equilibrio entre los controles de seguridad y la naturaleza de la información. Los objetivos de seguridad deben ser establecidos, revisados y coherentes con los aspectos de seguridad de la información.

Principios de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad

- Se debe garantizar **la confidencialidad** de la información, de tal manera que solo tengan acceso a la misma las personas autorizadas.
- Deberá asegurarse **la integridad** de la información con la que se trabaja, de modo que sea concisa y precisa, incidiéndose en la exactitud, tanto de su contenido como de los procesos involucrados.
- Se debe garantizar **la disponibilidad** de la información, asegurándose la continuidad del negocio soportado por los servicios de la información mediante planes de contingencias.
- Se debe garantizar **la autenticidad** de la información y la legitimidad del origen de su transmisión.
- Se debe garantizar **la trazabilidad** de las acciones, poniéndose la Organización frente al conocimiento de las operaciones, consultas o modificaciones de la información.

Principio de proporcionalidad

La implantación de controles que mitiguen los riesgos de seguridad de los activos debe hacerse buscando el equilibrio entre las medidas de seguridad, la naturaleza de la información y el riesgo.

Principio de responsabilidad

Todos los miembros del Grupo CIRSA deben ser responsables en su conducta en cuanto a la seguridad de la información, cumpliendo con las normas y controles establecidos.

Principio de mejora continua

Se revisará de manera recurrente el grado de eficacia de los controles de seguridad implantados en la Organización para aumentar la capacidad de adaptación a la constante evolución del riesgo y del entorno tecnológico.

Principio de permanente disposición y colaboración

Con las autoridades y organismos regulatorios en caso de necesidad, como parte de la vocación de servicio y de la responsabilidad de Grupo CIRSA con la sociedad en la que desarrolla su actividad.

3.2. Roles y responsabilidades

La Seguridad de la Información en Grupo CIRSA se gestiona a través de una estructura organizativa definida, que garantiza una adecuada toma de decisiones, una ejecución eficaz y un cumplimiento riguroso de las obligaciones legales y regulatorias. Esta estructura se basa en la colaboración coordinada de los siguientes actores clave:

1. El Comité de Seguridad de la Información, responsable de definir la estrategia, establecer los objetivos y priorizar los recursos necesarios para garantizar un nivel adecuado de seguridad en toda la Organización.
2. El Responsable de Seguridad de la Información, encargado de dirigir la implementación operativa de la estrategia definida, así como de coordinar y supervisar la ejecución del Plan de Seguridad.

3. El Comité Delegado de Protección de Datos, cuya función es asesorar y supervisar el cumplimiento de la normativa en materia de protección de datos personales y privacidad, colaborando estrechamente con el Responsable de Seguridad de la Información.

4. El Comité de Crisis, órgano de activación puntual que se constituye únicamente en situaciones excepcionales, con el objetivo de coordinar la respuesta ante incidentes críticos que puedan afectar a la continuidad del negocio o a la reputación del Grupo.

Además de los anteriores, existen dos actores fundamentales que complementan esta estructura:

- El Comité de Dirección, que proporciona el soporte institucional necesario para la aplicación de esta Política, asigna los recursos estratégicos y vela por el cumplimiento de los compromisos adquiridos con terceros.

- Todo el personal del Grupo CIRSA, que tiene la responsabilidad de conocer y aplicar esta Política en su actividad diaria, participar en las formaciones correspondientes y reportar cualquier incidente de seguridad detectado.

Esta estructura permite una gestión integral, eficiente y alineada con los principios de responsabilidad, prevención y mejora continua, asegurando que la Seguridad de la Información sea un componente transversal y estratégico en todas las actividades del Grupo.

3.3. Objetivos de la gestión de la seguridad

Mitigar los riesgos en materia de seguridad de la información

- Disponer de una gestión del riesgo con una metodología clara.
- Identificar las amenazas que puedan poner en riesgos a la Organización.
- Realizar análisis de riesgos periódicamente.
- Crear un parámetro de riesgo aceptable, por encima del cual la Organización deberá aprobar un Plan de Tratamiento. Este plan de tratamiento identificará contramedidas que deberán implementarse dentro de una planificación aprobada por el Comité de Seguridad y establecerá controles para medir su eficacia.
- Reconocer de forma expresa la aceptación de riesgos no tratados o gestionados, para que todas las partes implicadas conozcan los riesgos en materia de seguridad no gestionados.
- Disponer de un marco de referencia y actuación para la protección de los activos de los sistemas de información frente a amenazas, internas o externas, deliberadas o involuntarias, con la finalidad de garantizar la seguridad de la información y su disponibilidad.

Mantener la confidencialidad, integridad y disponibilidad de los activos de información

- Las dimensiones de seguridad (Confidencialidad, integridad y disponibilidad) de cada activo de la información se deben mantener en niveles aceptables para no afectar a sus propiedades ni al correcto desarrollo de la Organización.

Mejorar la cultura de ciberseguridad dentro de la Organización

- Fomentar la concienciación y formación del personal, tanto interno como externo, mediante la realización de acciones formativas, campañas de divulgación, etc. en materia de seguridad de la información.
- Con el fin de hacer frente a las continuas amenazas en ciberseguridad, se debe proporcionar recursos que permitan a los empleados de Grupo CIRSA detectar amenazas, identificarlas de forma eficiente y notificarlas a los equipos de gestión de incidentes.

- Además, estos recursos deberán ser válidos para reducir y bloquear estas amenazas cuando sea necesario.

3.4. Sanciones disciplinarias

Cualquier violación de la presente Política de Seguridad de la Información puede resultar en la toma de las acciones disciplinarias correspondientes de acuerdo con las disposiciones legales y contractuales vigentes en la compañía.

Asimismo, es responsabilidad de todos los empleados, servicios y/o colaboradores externos del Grupo CIRSA notificar de forma inmediata a la Dirección de ciberseguridad cuando se tenga conocimiento de cualquier desviación de la Normativa vigente y/o cualquier incidente de seguridad mediante la dirección: ciberseguridad@cirsa.com y, en cualquier caso, en el plazo máximo de doce (12) horas de su detección por parte del empleado, servicio y/o colaborador externo.

3.5. Revisión

Esta Política deberá ser revisada de forma periódica por el Comité de Seguridad, no siendo el período superior a un año y sin perjuicio de las modificaciones que pudieran ser necesarias por la producción de cambios significativos en la Organización.

De añadido, podrá ser revisada a propuesta de:

- Comité de Dirección.
- Cualquier miembro del Comité de Seguridad.
- Responsable de Seguridad.

4. Aprobación, vigencia y difusión

Esta política ha sido aprobada por el Consejo de Administración de CIRSA Enterprises, S.A. en su reunión de 20 de noviembre de 2025.

La presente política entra en vigor en la fecha de su aprobación. Su contenido será objeto de revisión periódica cuando proceda con el fin de adaptarla a cambios normativos o incorporar mejores prácticas en la materia. El citado Consejo de Administración será el órgano competente para su modificación, previa supervisión por parte de la Comisión del Consejo competente.

CIRSA
Ctra. de Castellar, 298
08226 Terrassa. Barcelona. Spain
T. 34 93 728 33 18
info@cirsa.com
www.cirsa.com