



POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

V2 JULIO DE 2026 // CONDIS SUPERMERCATS, S.A.U.

ÍNDICE

- 1 Definición de la Seguridad Informática
- 2 Alcance de la Política Corporativa de Seguridad de los Sistemas de Información
- 3 Objetivos
- 4 Declaración de Principios sobre Seguridad de los Sistemas de Información
- 5 Requisitos de la Política Corporativa de Seguridad de los Sistemas de Información en Condis
- 6 Normativa y Procedimientos
- 7 Cumplimiento y Comunicación
- 8 Resultados esperados de esta Política

1. DEFINICIÓN DE SEGURIDAD INFORMÁTICA

Seguridad Informática son las medidas y controles que aseguran la confidencialidad, integridad y disponibilidad de los activos de los Sistemas de Información, incluyendo hardware, software, firmware y aquella información que procesan, almacenan y comunican.

Definiremos "La Información" como un conjunto organizado de datos, que constituyen un mensaje sobre determinado ente o fenómeno. En este caso este ente corresponde a Condis Supermercats S.A.U., en adelante CONDIS, y la información a cualquier mensaje emitido sobre este.

La Seguridad de la Información debe garantizar:

- *Confidencialidad*

"Confidencialidad" se refiere al hecho de que sólo tienen acceso a la información de la red o que circulan por ella las personas autorizadas. Nadie puede acceder a la información sin haber sido autorizado.

La identificación de los usuarios exige autenticación. Para mantener la información protegida de las personas ajenas a ella es necesaria la encriptación, que se lleva a cabo con medios técnicos.

- *Integridad*

"Integridad" se refiere al hecho de que los métodos que gestionan la información garantizan un tratamiento sin errores de la misma. La información no debe cambiar mientras se está transfiriendo o almacenando, y nadie, no autorizado, puede modificar el contenido de la información o los archivos y aún menos eliminarlos.

- *Disponibilidad*

"Disponibilidad" se refiere al hecho de que los usuarios que necesitan la información para llevar a cabo sus funciones y responsabilidades y a quienes va dirigida dicha información siempre tienen acceso a ella. Los métodos para garantizar la disponibilidad incluyen un control físico y técnico de las funciones de los sistemas de datos, así como la protección de los archivos, su correcto almacenamiento y la realización de copias de seguridad.

La información es para CONDIS y para las personas y Sociedades que dependen de sus servicios, uno de sus activos más valiosos y un bien crítico sin el cual no podría desarrollar su actividad. CONDIS basa en gran medida, la calidad de su gestión en la utilización de esta información de forma exacta, completa y obtenida a tiempo.

Por lo tanto, se reconoce la gran importancia de las medidas de seguridad para lograr que la información no esté afectada por amenazas tales como errores, fraudes, malversaciones, sabotajes, terrorismo, extorsiones, espionaje industrial, violaciones de intimidad, interrupciones de servicio y desastres naturales.

La Dirección de CONDIS reconoce su responsabilidad en desarrollar las directrices de seguridad que permitan minimizar los riesgos potenciales a los que se encuentra expuesta en la consecución de los objetivos estratégicos del negocio.

2. ALCANCE DE LA POLÍTICA CORPORATIVA DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

La Política Corporativa de Seguridad de los Sistemas de Información será aplicable a todos los colaboradores internos y externos que interaccionen con CONDIS que tengan acceso a la información gestionada o en propiedad de la misma, en adelante “Colaboradores de Condís”.

La Política también será aplicable a toda la información, independientemente del soporte, y a los Sistemas de Información propiedad de CONDIS o gestionados para CONDIS.

3. OBJETIVOS

El objetivo de esta Política de Seguridad de los Sistemas de Información es definir las principales pautas que conduzcan a la formulación de los procedimientos de Seguridad de los Sistemas de Información para salvaguardar la información, de acuerdo a lo expuesto en el primer punto del presente documento.

La formulación de la Política Corporativa de Seguridad de los Sistemas de Información se sustenta en los siguientes pilares claves para lograr la protección de la información de CONDIS:

- La información de CONDIS y sus Sistemas de Información son activos críticos que deben ser protegidos para asegurar su funcionamiento.
- La información de CONDIS debe ser protegida conforme a su susceptibilidad, valor y criticidad.
- Todos los colaboradores internos y externos de CONDIS tienen la responsabilidad de proteger la información que se les ha confiado.
- La protección de la información permite el desarrollo del negocio de CONDIS; las medidas de protección deben desarrollarse conforme a una evaluación del riesgo.
- Para determinar qué medidas de protección son necesarias, debe asegurarse la confidencialidad, integridad y disponibilidad de la información y clasificar la misma como Confidencial, Uso Interno o Pública.

4. DECLARACIÓN DE PRINCIPIOS SOBRE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

Los principios sobre seguridad de la información en torno a los cuales se construyen las medidas de Seguridad de los Sistemas de Información son los siguientes:

- La información debe ser protegida durante todo su ciclo de vida, desde su creación o recepción hasta su procesamiento, comunicación, transporte, almacenamiento, difusión a colaboradores externos y su eventual destrucción.
- CONDIS protegerá la información de la difusión o manipulación no autorizada o pérdida de la misma.
- Los terceros subcontratados (colaboradores externos) que puedan acceder a la información propiedad de CONDIS han de estar sometidos al control de los estándares del mismo en cuanto a la seguridad de la información.
- Cada colaborador interno tiene la obligación y el deber de proteger adecuadamente la información, conforme a las clasificaciones y estándares de CONDIS.

5. REQUISITOS DE LA POLÍTICA CORPORATIVA DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN EN CONDIS

- La Política Corporativa de Seguridad de los Sistemas de Información, ha sido aprobada por la Dirección de CONDIS.
- Su contenido es de obligado cumplimiento para todos los colaboradores internos y externos de CONDIS.
- El cumplimiento de la Política de Seguridad de la Información es necesario para la protección de los derechos legales de CONDIS. Los transgresores de la misma estarán sujetos a las medidas disciplinarias que considere la Dirección de CONDIS.
- La Política Corporativa de Seguridad de los Sistemas de Información es un documento vivo que se deberá actualizar y modificar por el procedimiento que en la misma se establecerá. Asimismo, la Política ha de conocerse por todos los miembros de la organización de CONDIS.

6. NORMATIVA Y PROCEDIMIENTOS

Para la consecución de los objetivos y principios incluidos en esta Política de Seguridad, se han desarrollado una serie de normas que articulan las reglas generales sobre áreas específicas relativas a seguridad en los sistemas de información.

Esta normativa se constituye como base para el desarrollo de un conjunto de medidas específicas que se concretan en los Manuales de Procedimientos.

Se han determinado los objetivos a cubrir por la normativa, alineados con los objetivos de control impuestos por la ISO/IEC 27001:2022, y que se agrupan en las categorías siguientes:

- Políticas de Seguridad.
- Organización de la Seguridad de la Información.
- Seguridad en los Recursos Humanos.
- Gestión de Activos.
- Control de Acceso.
- Criptografía.
- Seguridad física y Ambiental.
- Seguridad de las Operaciones.
- Seguridad de las Comunicaciones.
- Adquisición, desarrollo y mantenimiento de los sistemas de información.
- Relaciones con proveedores.
- Gestión de los incidentes de Seguridad.
- Aspectos de la Seguridad de la Información en la Gestión de la Continuidad de Negocios.
- Cumplimiento.

7. CUMPLIMIENTO Y COMUNICACIÓN

Esta Política de Seguridad junto con su Normativa y Procedimientos, son de obligado cumplimiento por todos los colaboradores internos y externos de CONDIS que tengan acceso mediante cualquier medio a la información, sistemas de información e instalaciones propiedad de CONDIS.

La Dirección de CONDIS promoverá las acciones necesarias para que los colaboradores internos y externos de CONDIS conozcan y apliquen todos los aspectos incluidos en la política de Seguridad.

8. RESULTADOS ESPERADOS DE ESTA POLÍTICA

De la correcta aplicación de la política de seguridad de la información debe resultar:

- Mejora de la gestión de la seguridad sobre una base continua: la organización debe disponer de más defensas en forma de conocimientos, procedimientos y herramientas para evitar, repeler o minimizar posibles ataques o incidencias.
- Incremento de la confianza con clientes, proveedores, socios de negocios, etc.
- Reducción del riesgo de pérdida, robo o corrupción de información.
- Establecimiento de un marco de comparación con indicadores y métricas que ayuden a gestionar la seguridad desde el punto de vista de la Dirección de Grupo Condis.

