PROCESO: CEO-SOP-SIS
AREA: Dirección General
NIVEL DE CONFIDENCIALIDAD: Pública
NATURALEZA: Soporte
OBJETIVO: Definir el objetivo, dirección, principios y reglas básicas para la gestión de la seguridad de la información.

FORMA: CEO-SOP-SIS-09 Política de Seguridad de la Información

VIGENCIA: 11 agosto 2025
USUARIOS:

- **Todos los colaboradores**
- **Terceros que tengan relación con Directum**

Contenido

INTRODUCCIÓN

En Directum la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad.

Consciente de sus necesidades Directum implementa un Sistema de Gestión Integral, como la herramienta que permite identificar y mitigar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad y contribuye al cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes. El proceso de análisis de riesgos de los activos de información es el soporte para el desarrollo de las Políticas de Seguridad de la Información y de los controles y objetivos de control seleccionados para obtener los niveles de protección esperados en Directum; este proceso será liderado de manera permanente por el Gerente de Calidad y Seguridad de la Información.

Esta política será revisada con regularidad como parte del proceso de revisión gerencial, o cuando se identifiquen cambios en el negocio, su estructura, sus objetivos o alguna condición que afecten la política, para asegurar que sigue siendo adecuada y ajustada a los requerimientos de negocio, operativos y regulatorios.

ALCANCE

Los usuarios de este documento son todos los empleados de Directum, como también terceros externos a la organización.

DOCUMENTOS DE REFERENCIA

- Norma ISO/IEC 27001, capítulos 5.2 y 5.3. A5.1
- Metodología de evaluación y tratamiento de riesgos ver QA-AD-SGI
- CEO-SOP-SIS 12 Política de Controles Criptográficos
- CEO-SOP-SIS 13 Política de Uso Aceptable
- CEO-SOSP-SIS 10 Política de Actualizaciones
- CEO-SOP-SIS 16 Política de Gestión de Incidentes en Seguridad de la Información

DEFINICIONES

Confidencialidad: característica de la información por la cual solo está disponible para personas o sistemas autorizados.

Integridad: característica de la información por la cual solo es modificada por personas o sistemas autorizados.

Disponibilidad: característica de la información por la cual solo la pueden acceder las personas autorizadas cuando sea requerido.

Seguridad de la información: es la preservación de la confidencialidad, integridad y disponibilidad de la información.

GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

OBJETIVOS Y MEDICIÓN

Los objetivos generales son los siguientes: cumplir con los requerimientos de seguridad que marca el mercado y que son requeridos por nuestros clientes, mantener una sólida imagen hacia el mercado, así como reducir a un nivel razonablemente aceptable el daño ocasionado por incidentes de seguridad adversos; las metas están en línea con los objetivos comerciales, con la estrategia y los planes de negocio de la organización. Dar testimonio del compromiso de la Dirección General con relación a la seguridad de la información.

Garantizar el cumplimiento de la legislación vigente en materia de protección de datos de carácter personal y seguridad de la información, así como de todos los requerimientos legales, reglamentarios y contractuales que resulten aplicables.

Los objetivos para controles individuales de seguridad o grupos de controles son propuestos por el Gerente de Calidad y Seguridad de la Información y son aprobados por el Comité de Seguridad (equipo guía)

Todos los objetivos deben ser revisados al menos una vez al año o cuando se realice un cambio organizacional, aplicativo, normativo o tecnológico que impacte la seguridad de la información.

REQUISITOS PARA LA SEGURIDAD DE LA INFORMACIÓN

Esta política debe cumplir los requisitos legales y normativos importantes para la organización en el ámbito de la seguridad de la información y la protección de datos personales en poder de particulares, como también con las obligaciones contractuales y regulatorias.

CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

El proceso de seleccionar los controles (protección) está definido en la metodología de evaluación y tratamiento de riesgos.

Los controles seleccionados y su estado de implementación se detallan en la Declaración de Aplicabilidad.

CONTINUIDAD DEL NEGOCIO

La Gestión de la continuidad del negocio está reglamentada en el Plan de Continuidad del Negocio.

RESPONSABILIDADES

Las responsabilidades para el SGI en materia de Seguridad de la Información son las siguientes:

- El Gerente de Calidad y Seguridad de la Información es el responsable de garantizar que el SGI sea implementado y mantenido de acuerdo con esta Política y de garantizar que todos los recursos necesarios estén disponibles.
- El Gerente de Calidad y Seguridad de la Información es el responsable de la coordinación operativa del SGI, como también de informar su desempeño.
- La Dirección General debe revisar el SGI al menos una vez por año o cada vez que se produzca una modificación significativa; y debe elaborar minutas de dichas reuniones. El objetivo de las verificaciones por parte de la dirección es establecer la conveniencia, adecuación y eficacia del SGI.
- El Gerente de Calidad y Seguridad de la Información implementará programas de capacitación y concientización a los empleados sobre seguridad de la información.
- La protección de la integridad, disponibilidad y confidencialidad de los activos es responsabilidad del propietario de cada activo.
- Todos los incidentes o debilidades de seguridad deben ser informados de acuerdo con el Procedimiento para la Gestión de Incidentes.
- El Gerente de Calidad y Seguridad de la Información definirá qué información relacionada con la seguridad de la información será comunicada a qué parte interesada (tanto interna como externa), por quién y cuándo.
- El Gerente de Calidad y Seguridad de la Información es el responsable de adoptar e implementar el Plan de capacitación y concientización, que corresponde a todas las personas que cumplen una función en la gestión de la seguridad de la información.
- Los activos de información de Directum, serán identificados y clasificados para establecer los mecanismos de protección necesarios.
- Directum definirá e implantará controles para proteger la información contra violaciones de autenticidad, accesos no autorizados, la perdida de integridad y que garanticen la disponibilidad requerida por los clientes y usuarios de los servicios ofrecidos por la entidad.
- Todos los empleados y/o contratistas serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.

- Se realizarán auditorías y controles periódicos sobre el Sistema de Gestión de Seguridad de la Información de Directum.
- Únicamente se permitirá el uso de software autorizado que haya sido adquirido legalmente por Directum.
- Es responsabilidad de todos los empleados de Directum reportar los Incidentes de Seguridad, eventos sospechosos y el mal uso de los recursos que identifique.
- Las violaciones a las Políticas y Controles de Seguridad de la Información serán reportadas, registradas y monitoreadas.
- Directum contará con un Plan de Continuidad del Negocio que asegure la continuidad de las operaciones, ante la ocurrencia de eventos no previstos o desastres naturales.
- Adicionalmente Directum cuenta con políticas específicas y un conjunto de estándares y procedimientos que soportan la política corporativa.
- El proveedor de TI que da soporte a Directum será el responsable de la ejecución de las políticas y procedimientos establecidos por Directum.
- Se contará con un consultor externo para todo lo referente a asesoría en la implementación y auditoría de dichos controles.

COMUNICACIÓN DE LA POLÍTICA

El Gerente de Calidad y Seguridad de la Información debe asegurarse de que todos los empleados de Directum, como también los participantes externos correspondientes, estén familiarizados con esta Política.

APOYO PARA LA IMPLEMENTACIÓN DEL SGI

A través del presente, el Gerente de Calidad y Seguridad de la Información y la Dirección General, declara que en la implementación y mejora continua del SGI se contará con el apoyo de los recursos adecuados para lograr todos los objetivos establecidos en esta Política, como también para cumplir con todos los requisitos identificados.

AUDITORIAS

Se deberán realizar auditorías anuales para la revisión y cumplimiento de todas las políticas y controles establecidas y derivadas de esta política. Dichas auditorias podrán ser realizadas por personal externo.