BDO Chile

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Documentos con Validez Legal **Ley Nº 19.799**. Certificado por **E-Sign S.A.**

CONTROL DOCUMENTAL	IDENTIFICADOR	FECHA
VERSIÓN	4	Septiembre 2025
AUTOR	CISO	
APROBADOR	Comité de Seguridad	Septiembre 2025
DISTRIBUCIÓN	Todas las partes interesadas	
CLASIFICACIÓN	Pública	
ULTIMOS CAMBIOS REALIZADOS	Actualización 2026	01/09/2026

1. CONTENIDO

1. CONTENIDO 1
2. INTRODUCCIÓN 2
3. OBJETIVO 2
4. ALCANCE 3
5. REFERENCIAS NORMATIVAS 3
6. REVISIÓN, VALIDACIÓN Y DIFUSIÓN 4
7. RESPONSABILIDADES 4
8. DEFINICIONES 5
9. COMPROMISO 6
10. DISPOSICIÓN 7
11. USO DE INTELIGENCIA ARTIFICIAL (IA) 8
12. REVISIÓN Y ACTUALIZACIÓN DEL DOCUMENTO 9
13. COMUNICACIÓN Y DISTRIBUCIÓN 9

Documentos con Validez Legal **Ley Nº 19.799**. Certificado por **E-Sign S.A.**

2. INTRODUCCIÓN

La información constituye uno de los activos más valiosos para BDO Chile, siendo esencial para el desarrollo de sus operaciones, la prestación de servicios profesionales y el cumplimiento de sus obligaciones legales, contractuales y regulatorias.

En un entorno cada vez más digitalizado y expuesto a amenazas de diversa índole, la protección de la información requiere un enfoque estructurado, proactivo y basado en la gestión de los riesgos. Por esta razón la presente política establece los lineamientos generales para preservar la confidencialidad, integridad y disponibilidad de la información, promoviendo una cultura de seguridad en todos los niveles de la organización.

Esta política forma parte del marco normativo del Sistema de Gestión de Seguridad de la Información (SGSI) que esta alineado con los requisitos de la norma ISO/IEC 27001:2022, y es de aplicación obligatoria para todo el personal, colaboradores, contratistas y terceros que accedan o gestionen información de la organización

3. OBJETIVO

Definir los criterios y lineamientos esenciales para la administración, uso y protección de la información, así como de los recursos informáticos asociados a su tratamiento. Esta política se basa en normas y regulaciones nacionales e internacionales, así como en los lineamientos estratégicos de la organización.

La dirección de la firma, su cuerpo ejecutivo y todo el personal comprenden que la información, tanto propia como de clientes, es un recurso fundamental para la organización y, por tanto, asumen la responsabilidad que les corresponde en su adecuada protección.

Esta política tiene como objetivo:

- Proteger los activos de información: Garantizando la seguridad de la información gestionada en los procesos corporativos.
- Prevenir y gestionar riesgos de seguridad: Manteniendo una gestión eficaz sobre los riesgos que puedan afectar a los activos de la organización.
- Cumplir con requisitos legales y regulatorios: Asegurando el cumplimiento de normativas nacionales e internacionales y otras regulaciones aplicables.
- Establecer una cultura organizacional de seguridad: Fomentar la concienciación y responsabilidad de todo el personal sobre buenas prácticas y deberes en materia de seguridad de la información.
- Garantizar la continuidad del negocio: Diseñar y mantener planes que aseguren la resiliencia operativa frente a incidentes que puedan afectar a los procesos clave.
- Establecer y comunicar las directrices generales de seguridad de la información, ciberseguridad y privacidad que rigen en BDO Chile.

Documentos con Validez Legal **Ley Nº 19.799**. Certificado por **E-Sign S.A.**

- Establecer un marco de trabajo para la implementación de controles adecuados y efectivos para proteger los activos de información durante su uso cotidiano.
- Establecer la directriz de gestionar los riesgos a un nivel aceptable mediante el diseño, implementación y mantenimiento de un Sistema de Gestión de la Seguridad de la Información (SGSI).

4. ALCANCE

Esta política es aplicable a todo el personal interno o externo que realice actividades para la firma e incluye:

- Los activos de información propiedad de la firma o de sus clientes que se encuentren bajo la custodia o administración de esta.
- La infraestructura tecnológica que permite la generación, procesamiento, transmisión y almacenamiento de información.
- Las instalaciones físicas donde residen los activos de información.
- Las personas que hacen uso de los activos de información, ya sea personal de la firma, de los clientes o de empresas prestadoras de servicios.

Esta política aplica a todas las unidades organizativas, procesos, sistemas y personas que forman parte de BDO Chile., así como a terceros que acceden o gestionan información en nombre de la organización.

- Se encuentra bajo el alcance de esta política:
- Toda la información tratada por la organización, independientemente de su formato (digital, físico o verbal) y ubicación.
- Todos los activos de información utilizados para soportar los procesos de negocio.
- Los sistemas de información, redes, infraestructuras tecnológicas y servicios en la nube utilizados por BDO Chile.
- El personal interno y externo, incluyendo empleados, contratistas, socios de negocio y proveedores que tengan acceso a información o recursos tecnológicos de la organización.
- El cumplimiento de esta política es obligatorio y constituye la base para la implementación y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), conforme a los lineamientos de la norma ISO/IEC 27001:2022.

5. REFERENCIAS NORMATIVAS

Esta política se basa en las siguientes normas y regulaciones:

- ISO/IEC 27001:2022 - Tecnología de la Información - Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la Información - Requisitos.
- ISO/IEC 27002:2022 - Código de práctica para controles de seguridad de la información.
- Ley 21663 - Ley Marco de Ciberseguridad.
- Ley de Protección de Datos Personales y regulaciones nacionales aplicables.
- Regulaciones y estándares específicos del sector de operación de la organización.

Documentos con Validez Legal **Ley Nº 19.799**. Certificado por **E-Sign S.A.**

6. REVISIÓN, VALIDACIÓN Y DIFUSIÓN

La presente política es revisada anualmente y actualizada cuando es necesario. Será aprobada por el Comité de Seguridad. Si no hay modificaciones, deberá indicarse la justificación correspondiente en el registro de cambios.

Una copia de este documento quedará disponible para el personal interno y para terceros que presten servicios dentro del alcance del SGSI.

7. RESPONSABILIDADES

Para garantizar la adecuada implementación, operación y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), la organización ha definido y documentado los roles, funciones y responsabilidades relacionados con la seguridad de la información.

Dichos roles y responsabilidades específicos vinculados a la gestión de la seguridad de la información se encuentran establecidos y documentados en el "SGSI-DOC-05.2 Roles, responsabilidades y autoridades", el cual forma parte integral del marco normativo del Sistema de Gestión de Seguridad de la Información (SGSI).

Dicho manual define:

Los perfiles y niveles de responsabilidad involucrados en la gestión de la seguridad de la información.

Las funciones específicas de cada rol, incluyendo obligaciones, dependencias jerárquicas, y autoridades asignadas.

Las responsabilidades individuales y colectivas frente al cumplimiento de controles, reporte de incidentes, tratamiento de riesgos y uso adecuado de los activos de información.

El presente documento reconoce la obligatoriedad de dicho manual y establece que toda persona que actúe en nombre de la organización o acceda a su información deberá cumplir con las funciones y responsabilidades allí establecidas.

Documentos con Validez Legal **Ley Nº 19.799**. Certificado por **E-Sign S.A.**

8. DEFINICIONES

Término	Abreviatura	Descripción
Seguridad de la Información	SI	Preservación de la confidencialidad, integridad y disponibilidad de la información. Además, puede incluir otras propiedades como la autenticidad, la trazabilidad (responsabilidad), la no repudio y la confiabilidad.
Activo de información	AI	Cualquier dato, sistema, dispositivo, servicio, proceso o conocimiento que tenga valor para la organización y deba ser protegido frente a accesos no autorizados, pérdidas, alteraciones o divulgaciones indebidas.
Confidencialidad	C	Propiedad de la información que garantiza que solo está disponible para personas autorizadas a acceder a ella.
Integridad	I	Propiedad de la información que asegura que los datos son exactos, completos y no han sido modificados sin autorización
Disponibilidad	D	Garantía de que la información y los sistemas estén accesibles y utilizables por los usuarios autorizados cuando sea necesario.
Sistema de Gestión de Seguridad de la Información (SGSI)	SGSI	Conjunto de políticas, procedimientos, directrices, recursos y actividades asociadas que se utilizan para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información dentro de la organización.
Incidente de seguridad de la información	IA	Evento o conjunto de eventos no deseados o inesperados relacionados con la seguridad de la información que tienen una alta probabilidad de comprometer la operación del negocio y la protección de los activos de información.

Documentos con Validez Legal **Ley Nº 19.799**. Certificado por **E-Sign S.A.**

	Riesgo de seguridad de la información	R	Posible impacto negativo sobre los activos de información, derivado de la explotación de vulnerabilidades por parte de amenazas, que puede afectar los objetivos del negocio.
	Amenaza	A	Causa potencial de un incidente no deseado que puede causar daño a los activos de información o a la organización.
	Vulnerabilidad	V	Debilidad o fallo en un activo o grupo de activos que puede ser explotado por una o más amenazas.
	Parte interesada	PI	Persona u organización que puede afectar, verse afectada o percibirse como afectada por una decisión o actividad relacionada con la seguridad de la información.
	Usuario	U	Toda persona que accede a los sistemas de información o recursos tecnológicos de la organización ya sea de forma directa o mediante autorización, incluyendo personal interno, contratistas, proveedores y terceros.

9. COMPROMISO

- La Dirección de BDO Chile reafirma su compromiso con diseñar, implementar, operar, monitorear y mejorar continuamente los procesos y herramientas tecnológicas necesarias para asegurar que los riesgos de seguridad, ciberseguridad y privacidad de la información sean gestionados apropiadamente.
- La Dirección de BDO Chile asegurará la existencia de recursos para la operación y mejora continua de un Sistema de Gestión de Seguridad de la Información basado en ISO/IEC 27001:2022.
- La Dirección de BDO Chile asegura el cumplimiento de la normativa vigente en temas de Seguridad de la Información, ciberseguridad y privacidad, y los requerimientos contractuales establecidos por los clientes.
- La Dirección de BDO Chile reafirma su compromiso con la existencia de planes de contingencia, elaborados y mantenidos metodológicamente, para garantizar la continuidad de los servicios prestados.
- Todo colaborador, permanente o temporal, tiene la obligación de proteger los activos de información, los sistemas y la infraestructura tecnológica de la firma, actuando siempre de forma responsable y profesional, y conforme a lo establecido por esta política y otras complementarias.

Documentos con Validez Legal **Ley Nº 19.799**. Certificado por **E-Sign S.A.**

- Todo proyecto que involucre activos de información deberá incorporar los requerimientos de seguridad y ciberseguridad desde su concepción.
- Todo colaborador tiene la responsabilidad de notificar incidentes de seguridad y ciberseguridad, así como potenciales debilidades detectadas.

10. DISPOSICIÓN

Aplicación de la política:

BDO Chile, reafirma su compromiso de adoptar un enfoque estructurado y transversal que permita a todas las áreas y partes interesadas gestionar eficazmente la seguridad de la información. Este enfoque busca garantizar la confidencialidad, integridad y disponibilidad de los activos de información mediante la aplicación de controles adecuados, la asignación de responsabilidades claras y la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), en alineación con los principios de la norma ISO/IEC 27001 y el cumplimiento de las obligaciones legales, contractuales y regulatorias vigentes.

Gestión del Riesgo:

BDO Chile reconoce que una gestión eficaz de los riesgos asociados a la seguridad de la información es esencial para la protección de sus activos y la continuidad del negocio. Por ello, se compromete a identificar, evaluar y tratar de forma proactiva los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información, mediante un enfoque estructurado, definido y alineado con los principios de la norma ISO/IEC 27001:2022 como se indica en el documento "SGSI-DOC-06.2 Plan de tratamiento de riesgos - V2.0".

La organización revisará periódicamente su contexto interno y externo, así como los riesgos emergentes, asegurando la implementación de controles proporcionales al nivel de riesgo identificado. Este proceso será parte integral de la toma de decisiones estratégicas y operativas.

Notificación y respuesta ante incidentes:

Se establece un procedimiento formal para la detección, análisis, notificación y respuesta ante incidentes de seguridad de la información. Los incidentes graves serán reportados ante la autoridad competente y en los tiempos establecidos según el documento "SGSI-POL-A5.24 Política de Gestión de Incidentes y Eventos". Todo el personal tiene la obligación de reportar eventos sospechosos mediante los canales establecidos.

Conservación de la Información:

- BDO Chile asegura una gestión adecuada del ciclo de vida de la información, desde su creación o recepción hasta su eliminación o archivo definitivo, con el objetivo de preservar su valor, cumplir con las obligaciones legales y contractuales, y mitigar los riesgos asociados a su uso indebido o retención innecesaria.

Documentos con Validez Legal **Ley Nº 19.799**. Certificado por **E-Sign S.A.**

- La conservación de la información será realizada conforme a criterios establecidos de:
- Pertinencia temporal, según los plazos mínimos y máximos definidos por la legislación vigente, normas profesionales aplicables y necesidades del negocio.
- Clasificación y sensibilidad, de modo que se apliquen medidas de seguridad proporcionales al nivel de criticidad de la información.
- Soporte y formato, considerando tanto documentos físicos como digitales, con controles de acceso, respaldo, trazabilidad y protección contra alteraciones.

La disposición final de la información ya sea su eliminación segura o archivo histórico, se realizará bajo lo establecido en el documento "SGSI-PRO-A8.10 Procedimiento de Retención y Eliminación de Datos", para garantizar su trazabilidad, asegurando la confidencialidad y cumplimiento normativo durante todo el proceso.

La responsabilidad sobre la conservación y resguardo de la información recae en cada unidad de negocio, bajo la supervisión de las áreas de Seguridad de la Información, Legal y Gestión Documental.

11. USO DE INTELIGENCIA ARTIFICIAL (IA)

BDO promoverá el uso responsable, ético y seguro de la Inteligencia Artificial en todas las áreas de negocio, alineado con la normativa aplicable y con los principios de Privacidad y Ética desde el Diseño.

Cualquier sistema, herramienta o servicio que utilice IA (incluyendo modelos generativos, SaaS, APIs o desarrollos internos) deberá:

- Ser evaluado previamente por el Comité de Inteligencia Artificial junto con el área de TI y Ciberseguridad para identificar riesgos, impactos y medidas de mitigación.
- Garantizar la confidencialidad, integridad y disponibilidad de la información procesada, evitando usos indebidos, sesgos o resultados discriminatorios.
- No utilizar datos confidenciales, sensibles o propiedad de la organización en sistemas de IA generativa que no cuenten con aprobación expresa de la Dirección y medidas de protección adecuadas.
- Informar claramente a usuarios y clientes cuando interactúen con un sistema de IA, detallando su finalidad y el uso de los datos personales.
- Mantener un inventario actualizado de las soluciones de IA utilizadas, su propósito y responsables.
- Implementar controles de trazabilidad y registro de las decisiones automatizadas que puedan tener impacto significativo en personas o procesos.
- Está prohibido el uso de IA para fines ilegales, discriminatorios, de suplantación de identidad, manipulación de información, desinformación o cualquier otro que contravenga los principios y políticas de la firma.

Documentos con Validez Legal **Ley Nº 19.799**. Certificado por **E-Sign S.A.**

Formación y Concienciación:

Se debe garantizar que todo el personal involucrado en el SGSI conoce esta política, sus objetivos y procesos, a través de su divulgación, acciones formativas y acciones de concienciación.

También se debe garantizar la distribución de los documentos que aplican a cada nivel, de acuerdo con los diferentes roles definidos en la firma.

Auditoria y Mejora Continúa:

La Alta Dirección de BDO Chile debe garantizar y verificar, mediante auditorías internas y externas, el grado de cumplimiento de las directrices de esta Política y que éstas son operadas e implementadas correctamente, responsabilizándose del cumplimiento de las medidas correctivas que hayan podido determinarse con el fin de mantener la mejora continua.

La organización establece su compromiso permanente con la mejora continua del sistema de Gestión de la Información. En este marco, se implementarán mecanismos sistemáticos para revisar, evaluar y perfeccionar los controles, políticas, normas, procedimientos y medidas de seguridad adoptadas, con el objetivo de asegurar su eficacia frente a la evolución de las amenazas, los riesgos, los avances tecnológicos y los requisitos normativos y contractuales aplicables.

La mejora continua se fundamenta en un enfoque basado en evidencia, que incluye la realización periódica de auditorías internas, revisiones por la dirección, análisis de resultados de desempeño, tratamiento de no conformidades, lecciones aprendidas de incidentes y la identificación de oportunidades de mejora en todos los niveles de la organización.

12. REVISIÓN Y ACTUALIZACIÓN DEL DOCUMENTO

El presente documento permanecerá vigente desde el momento de su aprobación y publicación. Esta rige hasta la publicación de su próxima revisión. El intervalo de revisión estimado es de 12 meses.

Toda versión revisada será registrada con su correspondiente número de versión y fecha de aprobación, y será comunicada adecuadamente a los usuarios afectados para garantizar su conocimiento y correcta aplicación.

13. COMUNICACIÓN Y DISTRIBUCIÓN

BDO Chile, garantiza que la presente Política de Seguridad de la Información sea comunicada, distribuida y comprendida por todos los colaboradores, contratistas y partes pertinentes que intervienen en el tratamiento, uso o resguardo de información dentro del ámbito de la organización.

Documentos con Validez Legal **Ley Nº 19.799**. Certificado por **E-Sign S.A.**

La política será:

- Aprobada por la Alta Dirección y registrada formalmente dentro del Sistema de Gestión de Seguridad de la Información (SGSI).
- Comunicada a todo el personal mediante canales oficiales, incluyendo inducciones, capacitaciones periódicas, la intranet corporativa y comunicaciones internas.
- Distribuida en su versión vigente a las partes internas y externas relevantes, asegurando su disponibilidad y acceso en todo momento para su consulta.
- Comprendida y asumida como obligatoria por todos los destinatarios, quienes deberán actuar conforme a sus lineamientos y podrán ser requeridos a firmar acuse de recibo o constancia de lectura según el caso.

Marcelo Emilio
Donatucci Téllez
7045080-1
mdonatucci@bdo.cl

Firmado electrónicamente según Ley 19799
el 22-10-2026 a las 17:31:04 con Firma Electrónica Avanzada
Código de Validación: 1792701064255
Validar en https://www5.esigner.cl/esignercryptofront/documento/verificar/

Heraldo Germán
Hetz Vorpahl
5535725-0
heraldo.hetz@bdo.cl

Firmado electrónicamente según Ley 19799
el 22-10-2026 a las 17:00:14 con Firma Electrónica Avanzada
Código de Validación: 1792699214435
Validar en https://www5.esigner.cl/esignercryptofront/documento/verificar/

Documentos con Validez Legal Ley Nº 19.799. Certificado por E-Sign S.A.