

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

BDO Interaméricas

25 de Mayo del 2026

1. OBJETIVO

Establecer las directrices y lineamientos requeridos para proteger la información y los sistemas de información donde se administra, produce, procesa, almacena o transforma, los datos de BDO Interaméricas y de sus clientes; ante cualquier amenaza que pueda comprometer la Confidencialidad, Integridad, Disponibilidad y Trazabilidad de esta.

1.1. OBJETIVOS ESPECÍFICOS

1.1.1. Gestión de activos de información

Orientar a los colaboradores de BDO Interaméricas en el levantamiento, identificación, clasificación y manejo de los activos de información que producen, almacenan, recolectan o custodian, atendiendo las disposiciones normativas vigentes.

1.1.2. Gestión de riesgos de seguridad de la información

Gestionar los riesgos de seguridad de la información de forma oportuna por medio de controles, ayudando a reducir los impactos negativos de su materialización.

1.1.3. Gestión de incidentes de seguridad de la información

Gestionar los Incidentes de Seguridad de la Información que afecten la confidencialidad, Integridad o disponibilidad de los activos de información de BDO Interaméricas.

1.1.4. Fomentar cultura y apropiación

Fomentar una cultura y apropiación de seguridad y privacidad de la información en los colaboradores de BDO Interaméricas, con el fin de generar conciencia de sus deberes y responsabilidades al proteger los activos de información, controlar los riesgos y reducir el impacto que pueda generar su materialización.

2. ALCANCE

La Política de Seguridad de la Información aplica a todos los procesos, sedes, colaboradores, contratistas y partes interesadas que accedan, procesen, almacenen o administren información de BDO Interaméricas y de sus clientes. BDO Interaméricas está conformado por las oficinas de Colombia, Guatemala, El Salvador, Venezuela, Panamá, Nicaragua, Honduras y Ecuador, las cuales operan bajo un modelo de servicios compartidos (MTS), con una administración centralizada de los entornos tecnológicos a cargo de la oficina de Colombia. En consecuencia, es responsabilidad de todas las partes involucradas cumplir con los lineamientos del Sistema de Gestión de Seguridad de la Información - SGSI.

3. POLÍTICA

BDO Interaméricas, se compromete a establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información, que proteja la Confidencialidad, Integridad y Disponibilidad de la información, mediante controles de gobierno, técnicos y obligatorios, asegurando un enfoque de cultura y apropiación en la gestión de activos de información, la identificación de sus riesgos y la gestión de incidentes de seguridad, en cumplimiento con los requisitos legales, regulatorios y las políticas globales de BDO, apoyando el propósito y la misión de la firma.

3.1. ESTRUCTURA

La Política de Seguridad de la Información de BDO Interaméricas está diseñada para estar en línea con los requisitos y controles de seguridad de la información de BDO Global e ISO 27001:2022. Esta política describe 'QUÉ' aspectos deben protegerse y establece los dominios de control que deben implementarse.

En el “MAN-GSI(ITR)-01 Manual de Políticas Específicas de Seguridad de la Información BDO Interaméricas” se encuentra una descripción más detallada del enfoque y las medidas de seguridad de BDO Interaméricas, se definen para cada requisito o control el 'CÓMO' se implementan los lineamientos.

3.2. DECLARACIONES GENERALES DE GESTIÓN

Con esta Política, BDO Interaméricas Aceptará formalmente la propiedad y la responsabilidad de implementar y mantener la seguridad de la información, la gestión de los activos y riesgos para todos los servicios prestados, así como para todos los datos creados, procesados, recibidos en los procesos internos y de los clientes.

BDO Interaméricas:

- a) Acepta la responsabilidad formal sobre el Sistema de Gestión de Seguridad de la Información (SGSI), en coherencia con la visión ASG (ambientales, sociales y de gobernanza) de la firma.
- b) Asigna el rol de socio líder del Comité de Seguridad de la Información como representante de la alta dirección, y designa un Oficial de Seguridad de la Información con facultades para reportar directamente al Comité.
- c) Realiza evaluaciones periódicas, tanto internas como externas, sobre la eficacia de los controles establecidos.
- d) Se compromete con la mejora continua, gestionando los resultados de auditorías, riesgos, vulnerabilidades, amenazas y cambios tecnológicos o normativos.
- e) Implementa planes de cultura y apropiación del SGSI, con métricas de seguimiento trimestrales.
- f) Garantiza la inclusión de cláusulas contractuales específicas de seguridad de la información en los acuerdos con proveedores y aliados estratégicos.

- g) Administra de forma centralizada las herramientas tecnológicas y el control de accesos en entornos de nube, trabajo remoto y dispositivos móviles.

3.3. DOMINIOS DE CONTROL

Los siguientes son los dominios de control alineados a las prácticas líderes del mercado y los requerimientos de la Oficina Global de BDO, que permiten mediante su implementación, seguimiento y monitoreo, establecer niveles adecuados para proteger la Confidencialidad, Integridad y Disponibilidad de la información de BDO Interaméricas y sus clientes.

3.3.1. CONTROLES DE GOBIERNO

- a) Gestión de la Seguridad.
- b) Gestión de Riesgos de Seguridad de la información.
- c) Gestión de Personas.
- d) Continuidad de Negocio / Gestión de Crisis.
- e) Gestión de Servicios de TI.
- f) Gestión de Proveedores.
- g) Seguridad Física.

3.3.2. CONTROLES TÉCNICOS

- a) Sistemas Informáticos.
- b) Cifrado.
- c) Anti-Malware.
- d) Red.
- e) Gestión de Dispositivos Móviles.
- f) Gestión de Vulnerabilidades.
- g) Gestión de Identidad y Acceso.
- h) Filtrado de Contenido.
- i) Registro y Control.
- j) Desarrollo Seguro.

3.3.3. CONTROLES OBLIGATORIOS

- a) Disposición Segura o Reutilización de Equipos.
- b) Escritorio Limpio.
- c) Tecnologías de Reproducción.
- d) Uso del Correo Electrónico.
- e) Gestión de Medios Removibles.
- f) Clasificación y Etiquetado de la Información.
- g) Prevención de fuga de datos.
- h) Propiedad de la Información.
- i) Organización de la Seguridad.
- j) Gestión del Uso Seguro de Inteligencia Artificial (IA)
- k) Trabajo Remoto.
- l) Marco Normativo Aplicable.

4. CUMPLIMIENTO Y EXCEPCIONES

4.1. CUMPLIMIENTO

- a) La evidencia será entregada a BDO Global en la Herramienta de supervisión del cumplimiento continuo.
- b) Los manuales, procedimientos y demás lineamientos documentados se almacenarán, custodiarán y actualizarán en repositorios accesibles a las partes interesadas.
- c) BDO Interaméricas realiza auditorías internas y revisiones periódicas sobre la eficacia de los controles.

4.2. INCUMPLIMIENTO

- a) Se considera una falta grave la violación de cualquiera de las políticas establecidas en el presente documento o los derivados de este.
- b) Los colaboradores que infrinjan los lineamientos serán responsables de las sanciones disciplinarias a que haya lugar, de acuerdo con:
 - I. Reglamentos Internos de Trabajo de BDO Interaméricas.
 - II. Leyes y normatividad vigente.
 - III. Autoridades competentes.

4.3. EXCEPCIONES

Deben ser evaluadas y aprobadas por el comité de seguridad de la información o a quien el comité ejecutivo delegue, se debe documentar y mantener el registro de las excepciones a esta política y los lineamientos que de esta se desprenden.

5. PROPIEDADES DEL DOCUMENTO

Elaborado por:	Elias Alejandro López - Oficial de Seguridad de la Información
Revisado por:	Comité SGSI
Aprobado por:	Jaime Rios Barrero - Socio Champions de Seguridad de la Información/Líder Comité SGSI