POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

BPO CONSULTORES S.A.S.

ABRIL DE 2026

CONTENIDO

1. Objetivo, alcance y usuarios

El propósito de esta Política de alto nivel es definir el objetivo, la dirección, los principios y las reglas básicas para la gestión de la seguridad de la información en BPO Consultores S.A.S., con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, apoyar los objetivos estratégicos del negocio y generar confianza en las partes interesadas.

Esta Política aplica a toda la organización BPO Consultores S.A.S., y es de obligatorio cumplimiento para todos los empleados, contratistas, proveedores y terceros que accedan, gestionen o utilicen activos de información de la empresa, independientemente de su rol, área, modalidad de vinculación o servicio prestado. La Política cubre todos los procesos, personas, tecnologías, sistemas y activos de información de la organización, incluidos aquellos gestionados dentro del alcance del Sistema de Gestión de Seguridad de la Información (SGSI).

Los usuarios de este documento son todas las personas que interactúan con los activos de información de BPO Consultores S.A.S., quienes deberán cumplir las disposiciones aquí establecidas como parte de sus responsabilidades laborales y contractuales.

2. Documentos de referencia

- Norma ISO/IEC 27001, puntos 5.2, 5.3, 6.2, 7.4 controles 6.3
- Documento sobre el alcance del SGSI D-GD-003
- Declaración de aplicabilidad D-GSC-001

3. Terminología básica sobre seguridad de la información

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

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

- Integridad: característica de la información por la cual solo que es modificada por personas o sistemas autorizados y de una forma permitida.

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

- Sistema de gestión de seguridad de la información: parte de los procesos generales de gestión que se encarga de planificar, implementar, mantener, revisar y mejorar la seguridad de la información.

- Privacidad de los datos: también llamado privacidad, es el aspecto de la información relacionado con la habilidad de una organización o individuo para determinar qué datos de un sistema de información pueden ser compartidos con terceras partes.

- Amenazas: es la potencial causa de un incidente que puede resultar en daños a los sistemas u organización, en otras palabras, las amenazas es cualquier actor capaz de actuar en contra de un activo de información, de manera que resulte comprometido.

- Incidentes de seguridad: es uno o más eventos inesperados e indeseados, que puedan posiblemente comprometer la seguridad de la información y debilitar o detener las operaciones del negocio.

- Ataque: es un intento no autorizado de acceso, uso, alteración, exposición, robo, des habilitación o destrucción de un activo de información.

- ISO/IEC 27001: es la especificación de un sistema de gestión de la seguridad de la información, es decir, son un conjunto de políticas y procedimientos que incluyen controles legales, físicos y técnicos involucrados en los procesos de gestión del riesgo de una organización.

4. Gestión de seguridad de la información

4.1. Objetivo General

El Sistema de Gestión de Seguridad de la Información (SGSI) de BPO Consultores S.A.S. tiene como objetivo establecer, implementar, mantener y mejorar

continuamente un marco de gestión para la protección de los activos de información de la organización, asegurando su confidencialidad, integridad y disponibilidad.

El SGSI apoya la protección de la información utilizada en todos los procesos y servicios de BPO Consultores S.A.S., incluyendo, pero no limitándose, al servicio de administración de infraestructura en la nube, generando confianza en las partes interesadas, reduciendo el impacto de incidentes de seguridad y respaldando el cumplimiento de los objetivos estratégicos del negocio.

4.2. Objetivos específicos

- Diseñar e implementar controles relacionados con la disponibilidad, confidencialidad e integridad en BPO Consultores S.A.S.
- Identificar, valorar y controlar los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información de BPO Consultores S.A.S
- Gestionar las solicitudes e incidentes de seguridad de la información promoviendo la mejora continua.
- Establecer mecanismos que fomenten la concienciación y cultura de seguridad de la información en todo el personal de BPO Consultores S.A.S.

4.3. Medición de los objetivos

BPO Consultores S.A.S. medirá el cumplimiento de todos los objetivos del SGSI al menos una vez al año. Cada objetivo contará con indicadores definidos y con un responsable asignado, quien será el encargado de aplicar el método de medición establecido, realizar el seguimiento, analizar y evaluar los resultados correspondientes.

Los resultados consolidados serán presentados a la Gerencia como insumo para la Revisión por la Dirección.

1. Cantidad de controles que fueron diseñados e implementados.

$$Eficiencia\ en\ implementación\ de\ controles\ (\%)$$

$$= \frac{Controles\ implementados}{Controles\ norma} \times 100$$

META		
ACEPTABLE: 60% - 75%	**SATISFACTORIA:** 76% - 90%	**SOBRESALIENTE:** 91% - 100%

2. De los riesgos identificados y valorados, cuántos de los riesgos que requieren tratamiento, fueron efectivamente tratados con un control.

$$Eficiencia\ en\ el\ tratamiento\ de\ los\ riesgos\ (\%) = \frac{Cantidad\ de\ riesgos\ tratados}{Cantidad\ de\ riesgos\ identificados} \times 100$$

META		
ACEPTABLE: 60% - 75%	**SATISFACTORIA:** 76% - 90%	**SOBRESALIENTE:** 91% - 100%

3. Durante la operación del servicio, se mide la cantidad de incidentes y solicitudes mensuales y el estado de las mismas.

$$\boldsymbol{Eficiencia\ en\ el\ tratamiento\ de\ los\ incidentes\ y\ solicitudes}\ (\%) = \frac{\boldsymbol{Cantidad\ de\ incidentes\ y\ solicitudes\ cerrados}}{\boldsymbol{Total\ de\ incidentes\ y\ solicitudes}} \times \mathbf{100}$$

META		
ACEPTABLE: 60% - 75%	**SATISFACTORIA:** 76% - 90%	**SOBRESALIENTE:** 91% - 100%

4. Medir la proporción entre la cantidad de empleados involucrados con el sistema de Gestión y los asistentes a las capacitaciones ejecutadas.

$$Eficiencia\ en\ la\ capacitación\ y\ entrenamiento\ (\%) = \frac{Cantidad\ de\ personas\ que\ asistieron}{Total\ de\ personas\ citadas} \times 100$$

META		
ACEPTABLE: 60% - 75%	**SATISFACTORIA:** 76% - 90%	**SOBRESALIENTE:** 91% - 100%

4.4. Compromiso de la Alta Dirección

La alta dirección de BPO Consultores S.A.S. se compromete con la seguridad de la información como un pilar estratégico de la organización, promoviendo una cultura de protección de los activos de información y cumplimiento de los requisitos aplicables. Este compromiso se extiende a todas las partes interesadas, incluyendo empleados, clientes, aliados y proveedores.
En este sentido, la organización adopta los siguientes compromisos:

- Establecer y revisar periódicamente los objetivos de seguridad de la información, alineándolos con los planes estratégicos del negocio.
- Cumplir con todos los requisitos legales, normativos, contractuales y otros compromisos suscritos que sean relevantes para la seguridad de la información.
- Promover y facilitar la mejora continua del SGSI mediante auditorías, revisiones de desempeño, retroalimentación del personal y evaluación de riesgos emergentes.
- Asegurar la disponibilidad de los recursos humanos, tecnológicos y financieros necesarios para la implementación, mantenimiento y mejora del SGSI.
- Garantizar la difusión y comprensión de esta política dentro de la organización y entre los terceros relevantes, como proveedores de servicios y aliados estratégicos.
- Fomentar un entorno seguro mediante programas de formación, concienciación y desarrollo de competencias en seguridad de la información para todo el personal involucrado.

Esta política aplica a todos los procesos, personas, tecnologías, sistemas y proveedores de BPO Consultores S.A.S., y constituye el marco corporativo para la protección de la información en la organización.

4.5. Revisión y comunicación de la política

La política será revisada al menos una vez al año por la Alta Dirección, Gerente del Proyecto, el Gerente de Tecnología y/o el Oficial de Seguridad de la Información, o cuando existan cambios significativos en el contexto interno o externo de la organización. Esta política se comunica a todas las partes interesadas internas y

externas pertinentes, y está disponible para consulta de empleados, clientes y proveedores.

El Gerente del Proyecto debe asegurar que todos los empleados de BPO Consultores S.A.S. conozcan, comprendan y cumplan esta Política. Asimismo, será responsable de coordinar las actividades de divulgación y concienciación interna necesarias para su adecuada aplicación.

El Director de Tecnología será responsable de comunicar esta Política a los clientes, proveedores y demás terceros relevantes, así como de velar por su cumplimiento en los casos en que dichos terceros tengan acceso a los activos de información de BPO Consultores S.A.S.

4.6. Controles de seguridad de la información

La selección de controles de seguridad se realiza con base en los resultados del proceso de evaluación y tratamiento de riesgos, conforme a la metodología definida por BPO Consultores S.A.S.

Los controles aplicables, su justificación y estado de implementación están documentados en la Declaración de Aplicabilidad, la cual constituye un elemento central para asegurar la protección de los activos de información, garantizando la confidencialidad, integridad y disponibilidad requeridas.

Los controles, en su selección se evaluará también el costo beneficio.

4.7. Continuidad del negocio

La gestión de la continuidad del negocio se rige por el Plan de Continuidad del Negocio de BPO Consultores S.A.S., el cual ha sido desarrollado para asegurar que la organización esté preparada para responder ante la materialización de riesgos o interrupciones no planeadas que afecten sus procesos, servicios y activos de información, incluidos aquellos gestionados dentro del alcance del SGSI.

4.8. Roles y responsabilidades

Algunas de las responsabilidades para el SGSI son las siguientes:

Promotor del Proyecto (CEO)

- Garantiza que el SGSI sea implementado, mantenido y alineado con esta política.
- Asegura que los recursos humanos, tecnológicos y financieros requeridos estén disponibles para la operación y mejora continua del SGSI.

Gerente del Proyecto del SGSI

- Lidera la planificación, ejecución y seguimiento del SGSI.
- Coordina el uso eficiente de los recursos destinados a la implementación y mantenimiento del sistema.
- Revisa el SGSI al menos una vez al año o cada vez que se produzcan cambios significativos, documentando formalmente los resultados de estas revisiones.
- Informa periódicamente a la Alta Dirección sobre el estado y desempeño del SGSI.
- Adopta, implementa y da seguimiento al plan de formación y concienciación en seguridad de la información, asegurando su alineación con el alcance del servicio de infraestructura en la nube.
- Es responsable del cumplimiento de la programación de capacitaciones para todos los colaboradores con funciones relevantes en el SGSI.

Director de Tecnología

- Proveer la disponibilidad y continuidad de la infraestructura tecnológica que soporta los servicios en la nube
- Liderar la ejecución de planes de continuidad y recuperación ante desastres relacionados con la infraestructura.
- Garantizar la efectividad de los respaldos y pruebas periódicas de restauración
- Implementar, mantener y supervisar controles técnicos de seguridad en los sistemas de información, en cumplimiento con la ISO/IEC 27001:2022
- Gestionar configuraciones seguras de sistemas, redes y plataformas en la nube.

- Asegurar el uso de herramientas de protección contra malware, filtrado de tráfico y seguridad perimetral
- Administrar el ciclo de vida de cuentas de usuario, incluidas cuentas privilegiadas, asegurando revisiones periódicas.
- Coordinará con el Oficial de Seguridad la respuesta y recuperación ante incidentes de seguridad.
- Apoyará la gestión de riesgos tecnológicos, evaluando amenazas y vulnerabilidades que puedan afectar la seguridad de la información.
- Asegurará que los proveedores tecnológicos cumplan con los requisitos de seguridad establecidos en el SGSI.
- Participar en auditorías internas y externas, proporcionando evidencias técnicas cuando sean requeridas.
- Mantener comunicación permanente con el Oficial de Seguridad de la Información y otras áreas involucradas.

Oficial de Seguridad de la Información (CISO)

- Coordina operativamente el SGSI y vela por el cumplimiento de los controles definidos.
- Gestiona la respuesta ante incidentes de seguridad de la información, evaluando su impacto y promoviendo acciones de mitigación.
- Define qué información relacionada con la seguridad debe ser comunicada, a quién, por quién y en qué momento, tanto a nivel interno como externo.
- Informa a la Alta Dirección sobre el desempeño del sistema y las oportunidades de mejora.
- Supervisa la implementación de controles técnicos y organizativos que garanticen la confidencialidad, integridad y disponibilidad de la información.

Propietarios de activos de información

- Son responsables de la protección y correcto uso de los activos de información bajo su custodia.
- Deben asegurar que los activos estén identificados, clasificados y protegidos conforme a los lineamientos del SGSI.

Nota:
Las responsabilidades relacionadas con la gestión de activos de información, la identificación, evaluación y tratamiento de riesgos asociados al alcance del SGSI en

la infraestructura en la nube, se encuentran definidas en el Procedimiento de Evaluación y Tratamiento de Riesgos (P-GSC-002). Las demás responsabilidades se complementan con el documento del alcance del SGSI

Todos los colaboradores

Todos los colaboradores de BPO Consultores S.A.S. son responsables de cumplir con las políticas, procedimientos y controles de seguridad de la información definidos por la organización, independientemente de si sus funciones se encuentran o no dentro del alcance del SGSI, y de reportar de manera inmediata cualquier incidente, evento o debilidad de seguridad al correo
📧 seguridad@bpoconsultores.com.co

5. Uso de información personal en medios corporativos

Todo empleado de BPO Consultores S.A.S. acepta que la información personal almacenada en los dispositivos, sistemas y medios proporcionados por la organización para el cumplimiento de sus funciones no le otorga derecho de propiedad sobre dichos contenidos.

Esto incluye, pero no se limita a, correos electrónicos, archivos electrónicos o físicos, registros de actividad, datos de navegación o cualquier otra información almacenada en medios corporativos.

Sin perjuicio de lo anterior, BPO Consultores S.A.S. actuará como responsable del tratamiento de los datos personales conforme a lo establecido por la Ley 1581 de 2012 y sus decretos reglamentarios, asegurando la protección, confidencialidad y tratamiento adecuado de los datos personales conforme al principio de finalidad y proporcionalidad.

6. Incumplimiento en seguridad de la información

Cualquier incumplimiento será sancionado por medio de los siguientes artículos del Reglamento Interno de Trabajo D-GT-001:

ARTÍCULO 66. SON OBLIGACIONES ESPECIALES DEL TRABAJADOR. Además de las obligaciones propias del cargo, las mencionadas en el artículo 58 del

Código Sustantivo del Trabajo, todos los trabajadores de la empresa BPO CONSULTORES S.A.S tienen las siguientes obligaciones:

57. Velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información de la organización, en cualquier formato, especialmente si dicha información está protegida por reserva legal, o ha sido clasificada como confidencial.

60. Acatar y cumplir a cabalidad el sistema de gestión de la seguridad información (SGSI) y política de protección de datos personales creados por la empresa para la custodia de estos. Permitir que las áreas de control en cualquier momento realicen auditorías, con el fin de verificar que se cumplan los procedimientos establecidos por la empresa y responder a cualquier inquietud de su equipo de trabajo.

ARTÍCULO 70. SE PROHÍBE A LOS TRABAJADORES.

67. Utilizar dispositivos personales como teléfonos móviles, computadores portátiles o memorias de almacenamiento de datos como discos duros externos o USB entre otros, así como sistemas digitales o electrónicos con el fin de almacenar o transferir información sensible de la Empresa sin autorización previa de esta.
68. Enviar información confidencial o sensible a través de canales no seguros, como correos electrónicos personales, aplicaciones de mensajería no aprobadas o redes públicas.
69. Dejar documentos físicos o digitales desatendidos o sin la custodia requerida, como carpetas, hojas de trabajo o pantallas abiertas, en áreas comunes o accesibles a terceros.
70. Modificar, alterar o eliminar información sin la debida autorización y sin seguir los procedimientos establecidos.
71. Introducir datos falsos o inexactos en los sistemas de la Empresa, ya que esto puede comprometer la calidad de la información y los procesos de toma de decisiones.
72. Manipular sistemas o bases de datos de manera no autorizada, incluyendo el uso de credenciales de otros empleados para acceder a información restringida.
73. Ignorar los procedimientos de respaldo y recuperación de datos, lo que podría poner en riesgo la integridad de la información en caso de incidentes.
74. Interrumpir intencionalmente el acceso a sistemas o servicios críticos, como servidores, redes o aplicaciones, sin una justificación válida y autorización previa.
75. Desconectar equipos o dispositivos que afectan la operación de los sistemas de información, como cámaras de seguridad, servidores o puntos de acceso.

76. No reportar fallos o incidentes que puedan comprometer la disponibilidad de la información, como caídas de sistemas, pérdida de conectividad o ataques cibernéticos.

7. Gestión de registros guardados con base a este documento

Nombre	Almacenamiento	Responsable Del Registro	Controles Para La Protección	Tiempo De Retención	Disposición
Objetivos del SGSI F-GSC-004	Carpeta Compartida SGSI	Gerente de Proyecto	Los registros sólo pueden editados y/o modificados Gerente de Proyecto	3 años.	Archivar

8. Gestión de cambios de los documentos

El propietario de este documento es el Gerente del Proyecto que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Fecha de Revisión	Descripción del Cambio	Nombre y Cargo de quien realiza	Nombre y Cargo del revisor	Nombre y Cargo del aprobador	Versión
05/05/2025	Elaboración del documento	Camila Arteaga Administradora Documental	Verónica Restrepo Gerente del Proyecto	Patricia Botero CEO – Promotor del Proyecto	01
06/02/2026	Se cambia la clasificación de la política a Público y se cambia el correo de comunicación de los incidentes. Se amplía el alcance del documento a todo BPO consultores	Verónica Restrepo Gerente del Proyecto	Verónica Restrepo Gerente del Proyecto	Patricia Botero CEO – Promotor del Proyecto	02

08/04/2026	Se actualiza nombre del numeral 5. Se elimina concepto Manual del artículo 66.	Camila Arteaga Administradora Documental	Verónica Restrepo Gerente del Proyecto	Patricia Botero CEO – Promotor del Proyecto	03

PATRICIA DEL PILAR BOTERO ÁNGEL
C.C. 42.897.830
CEO – Promotor del Proyecto
BPO CONSULTORES S.A.S
NIT 900.410.325-2