1. Objetivo y alcance del documento

La presente política establece los **principios, compromisos y lineamientos estratégicos** para la protección de la información en todos los procesos, servicios y activos tecnológicos de la organización. **Aplica** a todas las personas, recursos y sistemas que participan en la operación, gestión y soporte de la información corporativa, y constituye la base del Sistema de Gestión de Seguridad de la Información (SGSI), de acuerdo con los lineamientos de la norma ISO/IEC 27001.

2. Declaración de la Política

En BPM Consulting S.A.S., la Alta Dirección establece su compromiso de implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI), reconociendo la protección de los activos de información como un elemento estratégico para la continuidad del negocio, la confianza de los clientes y el cumplimiento de los requisitos aplicables.

Para la gestión efectiva de la seguridad de la información, la organización se compromete a:

- El cumplimiento de los requisitos legales, regulatorios, contractuales y de las partes interesadas pertinentes.
- La alineación con la estrategia organizacional y los objetivos del negocio.
- La gestión sistemática de los riesgos de seguridad de la información.
- Fortalecimiento de las capacidades organizacionales en seguridad de la información

3. Principios de Seguridad de la Información

La gestión de la seguridad de la información se basa en los siguientes principios:

- **Confidencialidad:** la información es accesible únicamente por personas autorizadas.
- **Integridad:** la información es exacta, completa y confiable.
- **Disponibilidad:** la información está disponible cuando se requiere.

4. Objetivos de Seguridad de la Información

1. Proteger los activos críticos de información la organización.
2. Velar por la disponibilidad y continuidad de la seguridad de la información
3. Mantener el cumplimiento de los requisitos legales, regulatorios y contractuales aplicables.
4. Alcanzar la conformidad del SGSI según los requisitos de la ISO 27001
5. Incluir tecnología que provea apoyo a la gestión del sistema de seguridad de la información.

Los objetivos serán definidos, medidos y monitoreados mediante indicadores establecidos en el SGSI

5. Enfoque de gestión del riesgo

La organización adopta un enfoque basado en riesgos para la gestión de la seguridad de la información, el cual permite:

- Identificar, analizar y tratar riesgos de manera sistemática.
- Priorizar la implementación de controles según el nivel de exposición.
- Mantener el riesgo dentro de los niveles aceptables definidos por la organización.

6. Articulación del SGSI

El SGSI se soporta en un conjunto de lineamientos que permiten su operación, incluyendo:

- POLITICA DE DISPOSITIVOS MOVILES
- POLITICA DE CONTROL DE ACCESO LOGICO
- POLITICA DE CLASIFICACION ETIQUETADO Y MANEJO DE INFORMACION
- POLITICA DE CONTROLES CRIPTOGRÁFICOS Y GESTION DE LLAVES
- POLITICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA
- POLITICA DE SEGURIDAD EN LAS RELACIONES CON PROVEEDORES
- POLITICA DE DESARROLLO SEGURO
- LINEAMIENTOS DE SEGURIDAD DE LA INFORMACION PARA EL DESARROLLO DE SOFTWARE
- LINEAMIENTOS PARA LE GESTION DE CONTRASEÑAS
- POLÍTICA DE CALIDAD OPERATIVA
- POLITICA DE CONTROL DE ACCESO FISICO
- POLITICA DE USO ACEPTABLE DE ACTIVOS
- POLITICA DE BACK UP DE LA INFORMACION
- POLITICA DE TELETRABAJO
- IMPLEMENTACION Y OPERACION DE SERVICIOS BPO
- POLITICA DEL SISTEMA INTEGRADO DE GESTIÓN
- POLITICA DE TRANSFERENCIA DE INFORMACION
- POLITICA PARA EL TRATAMIENTO DE DATOS PERSONALES
- LINEAMIENTOS PARA LA GOBERNANZA, SEGURIDAD Y USO CONFIABLE DE LA INTELIGENCIA ARTIFICIAL
- POLITICA DE SEGURIDAD PARA EL USO DE SERVICIOS EN LA NUBE

Estos lineamientos se desarrollan en documentos específicos que complementan la presente política.

7. Roles y Responsabilidades en Seguridad de la Información

Gerencia General

La Gerencia General lidera estratégicamente el Sistema de Gestión de Seguridad de la Información (SGSI), asegurando su alineación con los objetivos institucionales. Sus principales responsabilidades son:

- Definir y aprobar los objetivos estratégicos en materia de seguridad de la información.
- Asignar los recursos necesarios para el funcionamiento y mejora del SGSI.

- Aprobar las políticas y lineamientos clave del sistema.
- Impulsar la implementación y la cultura de seguridad de la información en toda la organización.
- Supervisar el cumplimiento de las obligaciones regulatorias.
- Evaluar y aprobar proyectos estratégicos asociados a la seguridad de la información.

Comité Directivo

El Comité Directivo opera como una instancia de decisión táctica y estratégica que apoya la gestión del SGSI, asegurando su alineación con los objetivos organizacionales y facilitando la implementación efectiva de los lineamientos institucionales en materia de seguridad de la información.

Sus principales responsabilidades son:

- Revisar periódicamente el estado del SGSI y proponer acciones para su mejora continua.
- Analizar los riesgos relevantes y las recomendaciones derivadas de los análisis de impacto (BIA) y evaluación de vulnerabilidades.
- Validar la pertinencia de controles y medidas implementadas, y proponer ajustes cuando sea necesario.
- Supervisar el cumplimiento de los planes y proyectos de seguridad de la información aprobados por la Gerencia General.
- Apoyar la integración de la seguridad de la información en todos los procesos organizacionales.
- Coordinar acciones con las diferentes áreas para asegurar el cumplimiento normativo y contractual en materia de seguridad.
- Facilitar la toma de decisiones cuando se presenten incidentes de seguridad de alto impacto.

Gerentes de Area

Son responsables de asegurar que las actividades bajo su gestión se desarrollen conforme a los lineamientos establecidos por el SGSI, actuando como puente entre la política de seguridad de la información y su aplicación práctica en el entorno operativo.

Sus responsabilidades incluyen:

- Implementar y mantener los controles de seguridad definidos para su proceso.
- Asegurar la correcta clasificación, uso y protección de la información que gestionan.
- Identificar y reportar riesgos o incidentes relacionados con la seguridad de la información.
- Promover la cultura de seguridad dentro de sus equipos de trabajo.
- Participar activamente en actividades de sensibilización, formación y auditorías internas.
- Colaborar con el Comité Directivo y el Oficial de Seguridad de la Información en la actualización de políticas, procedimientos o controles cuando se identifiquen brechas o cambios relevantes.

Oficial de Seguridad de la Información

El Oficial de Seguridad de la Información (OSI) es el responsable designado para coordinar, asesorar y monitorear la implementación del SGSI. Actúa como punto focal entre la estrategia organizacional y la aplicación de las medidas de seguridad, asegurando el cumplimiento de los requisitos normativos, contractuales y técnicos.

Sus responsabilidades incluyen:

- Coordinar la implementación y mantenimiento del SGSI.
- Gestionar la documentación del sistema y asegurar su actualización.
- Coordinar la identificación, análisis y tratamiento de riesgos de seguridad de la información.
- Hacer seguimiento a los controles establecidos y proponer ajustes cuando sea necesario.
- Consolidar información para la revisión por la dirección y auditorías internas o externas.
- Promover acciones de sensibilización, formación y cultura de seguridad.
- Actuar como enlace con entes de control, autoridades competentes y grupos de interés cuando se presenten incidentes relevantes.

Colaboradores

Todos los colaboradores de la organización tienen la responsabilidad de **cumplir y aplicar los lineamientos establecidos en el Sistema de Gestión de Seguridad de la Información (SGSI)**, actuando de forma consciente, ética y diligente frente al uso, manejo y protección de los activos de información.

Sus responsabilidades incluyen:

- Respetar las políticas, procedimientos e instructivos relacionados con la seguridad de la información.
- Garantizar la confidencialidad, integridad y disponibilidad de la información que manipulan o gestionan.
- Reportar de manera oportuna cualquier incidente, vulnerabilidad o anomalía que pueda afectar la seguridad de la información.
- Participar activamente en los procesos de capacitación y sensibilización en materia de seguridad.
- Utilizar los recursos tecnológicos de acuerdo con los lineamientos establecidos por la organización.

Contratistas y Terceros

Los contratistas, proveedores y terceros que acceden a la infraestructura tecnológica, sistemas o información de la organización están sujetos al cumplimiento de los lineamientos del SGSI, los acuerdos de confidencialidad y los compromisos establecidos en los contratos o convenios correspondientes.

Sus responsabilidades incluyen:

- Cumplir con los acuerdos de confidencialidad y niveles de acceso autorizados.
- Asegurar el tratamiento adecuado de la información a la que tengan acceso en el marco de sus funciones o servicios.
- Atender las instrucciones de la organización respecto al uso de los recursos tecnológicos y procedimientos de seguridad.
- Reportar de inmediato cualquier incidente, filtración o situación anómala que afecte los activos o la información.
- Participar, cuando se requiera, en actividades de inducción o formación relacionadas con la seguridad de la información.

8. GLOSARIO

Activo
Cualquier recurso que tiene valor para la organización, como hardware, software, documentos, infraestructura, servicios o información.

Amenaza
Evento o condición que podría causar daño a los activos de información o afectar su seguridad.

Confidencialidad
Propiedad de la información que asegura que solo las personas autorizadas pueden acceder a ella.

Disponibilidad
Capacidad de la información o los sistemas para estar accesibles y utilizables cuando se requieran.

Incidente de seguridad de la información
Evento inesperado que puede comprometer la confidencialidad, integridad o disponibilidad de la información.

Integridad
Propiedad que asegura que la información es exacta, completa y no ha sido modificada de forma no autorizada.

Política
Declaración, intenciones y directrices de la compañía, expresadas por la dirección general.

Riesgo
Posibilidad de que una amenaza explote una vulnerabilidad, causando un impacto negativo en la organización.

Seguridad de la información
Protección de la confidencialidad, integridad y disponibilidad de la información, así como de otros aspectos como la autenticidad y la trazabilidad.

Sistema de gestión de seguridad de la información (SGSI)
Conjunto de políticas, procesos y recursos utilizados para gestionar la seguridad de la información en la organización y mejorarla continuamente.

CONTROL DE CAMBIOS		
VERSIÓN	**FECHA DE APROBACIÓN**	**DESCRIPCION**
01	16-02-2022	Creación del documento.
02	17-05-2022	Se adiciona listado de partes interesadas. Se describe brevemente la intensión de cada política que hace parte del sistema.
03	27-06-2023	Se ajustó la declaración de la política, se adicionan los objetivos y el responsable, se actualizan los ítems de las políticas que hay de seguridad.
04	02/01/2024	Cambio de la clasificación del documento, de Privado a Público.
05	06/03/2024	Actualización de los siguientes elementos: • Objetivo de la política general • Objetivos de Seguridad de la Información conforme revisión por la Dirección. • Exclusión de los textos detallados para cada política indicada en el documento. • Inclusión del listado de las políticas que aplican para el Sistema de Seguridad de la Información
06	07/05/2024	Actualización del capítulo Políticas complementarias Seguridad de la Información: • Exclusión de las políticas relacionadas con medio ambiente, seguridad y salud en el trabajo, diversidad, equidad e inclusión y desconexión laboral, dado que sus alcances no incluyen la seguridad de la información. • Inclusión del documento Lineamientos de seguridad de la información para el desarrollo de software
07	06/12/2024	Inclusión de: ***"Lineamientos para la gestión de contraseñas",*** en el capítulo "Políticas complementarias Seguridad de la Información".
08	16/04/2025	• Actualización del nombre del documento teniendo en cuenta su contenido. • Actualización de la estructura del documento por capítulos, para un mejor entendimiento. • Ajuste en las responsabilidades de los roles, para alinearlos con el SGSI. • Actualización de los contactos de las autoridades y grupos de interés especial • Ajustes de redacción en todo el documento para aportar información de fácil entendimiento para las partes interesadas.
09	20/06/2025	Actualización del capítulo 5. Políticas complementarias de Seguridad de la Información, para incluir la Política de Seguridad para el uso de servicios en la nube.

CONTROL DE CAMBIOS		
VERSIÓN	**FECHA DE APROBACIÓN**	**DESCRIPCION**
10	23/02/2026	Actualización de la imagen corporativa mediante el ajuste del nuevo logo, la adecuación de colores en tablas y textos, alineados con la nueva paleta institucional
11	27-03-2026	Se actualiza el documento en los capítulos 2, 3 y 4, con el fin de optimizar su redacción, mejorar su claridad y fortalecer su alineación con la estrategia organizacional y los requisitos de la norma ISO/IEC 27001:2022, para facilitar su comprensión y apropiación por parte de las partes interesadas El ajuste incluye la simplificación del contenido, la organización de los principios de seguridad de la información y la consolidación de los compromisos relacionados con la gestión de riesgos, protección de activos de información, cumplimiento legal y mejora continua, sin modificar su alcance ni intención.