Políticas y Generales:

Política Seguridad de la Información

1. Propósito

Garantizar un nivel adecuado de protección de los activos de información de la organización, frente a cualquier amenaza que pueda generar un impacto directo en GBM, sus clientes y socios comerciales. El Sistema de Gestión de Seguridad de la Información (SGSI) establece, implementa, opera, revisa, mantiene y mejora de forma continua los procesos y controles relacionados con la seguridad de la información, adoptando un enfoque integral de gestión de riesgos y alineado con los controles establecidos en la norma y los estándares seguridad utilizados.

2. Alcance

Esta política es aplicable a todas las actividades de la organización relacionadas con la gestión de la seguridad de la información.

3. Roles y responsabilidades

Con el fin de asegurar el cumplimiento efectivo de esta política de seguridad de la información. Estas responsabilidades están orientadas a implementar, operar, mantener, revisar y mejorar continuamente el SGSI para GBM.

3.1 Information Security Board

- Asegurar que la estrategia de Seguridad de la Información este alineada con los objetivos del negocio,
- Aprobar la política de seguridad de la información
- Aprobar y proveer los recursos necesarios para implementar y mantener los objetivos de seguridad.
- Definir la tolerancia y los criterios de aceptación del riesgo.
- Promover una cultura organizacional orientada a la gestión del riesgo y la protección de la información
- Velar por el cumplimiento de los requisitos legales, contractuales, regulatorios de seguridad y protección de datos.
- Monitorear el desempeño del Sistema de Gestión de Seguridad de la Información
- Aprobar iniciativas estratégicas relacionadas con seguridad.

3.2 Information Security Manager

- Diseñar e implementar la estrategia de Seguridad de la Información
- Diseñar y coordinar la implementación de controles técnicos y operativos de seguridad de la información
- Asegurar el cumplimiento de los requisitos del SGSI
- Medir y evaluar la eficacia de los controles implementados y proponer ajustes.
- Coordinar la gestión de incidentes de seguridad
- Evaluar e identificar acciones sobre los resultados de los análisis de riesgos.
- Elaborar reportes periódicos del estado de la seguridad de la información corporativo.
- Escalar riesgos o desviaciones relevantes al ISB.
- Aprobar nuevas políticas de seguridad de la información y aprobar cambios a las existentes.

3.3. Information Security Specialist / Gestores del SGSI

- Ejecutar los controles definidos en las políticas y procedimientos de seguridad de la información
- Implementar, configurar y mantener soluciones de seguridad.
- Asegurar el cumplimiento de estándares técnicos de seguridad.
- Identificar eventos de seguridad e investigar posibles incidentes.

- Ejecutar planes de respuesta y recuperación de incidentes.
- Administración de usuarios (bajo el alcance definido)
- Ejecutar el control de la gestión de vulnerabilidades y pruebas de seguridad
- Identificar riesgos emergentes y reportarlo al ISM.
- Coordinar el análisis y evaluación de riesgos de seguridad de la información.
- Desarrollar y actualizar los procedimientos, controles y documentación relacionada.
- Monitorear el desempeño del SGSI, identificando oportunidades de mejora.
- Capacitar y sensibilizar al personal en materia de seguridad de la información.

3.4 Business Processes Analyst

- Alinear los procesos organizacionales con los requisitos definidos en las políticas y procedimientos de seguridad de la información.
- Facilitar la integración de los controles de seguridad en los procesos organizacionales.
- Dar seguimiento al cumplimiento normativo y contractual derivado de las políticas y procedimientos de seguridad.
- Asegurar la gestión del cambio y mejora continua del SGSI.

3.5 Dueños/ responsables del proceso

- Identificar, analizar y evaluar riesgos de seguridad en conjunto con Seguridad de la Información
- Asegurar que los procesos cumplan con los requisitos de Seguridad de la Información
- Diseñar e implementar controles alineados a las políticas y procesos de seguridad.
- Proveer información y evidenciar sobre los controles implementados y su efectividad.

4. Políticas

GBM se compromete a garantizar la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), mediante el liderazgo activo de la Alta Dirección (Information Security Board - ISB), quien asegura la disponibilidad de recursos adecuados y promueve una cultura organizacional basada en la seguridad de la información. Este compromiso se sustenta en un enfoque de gestión de riesgos, respuesta a incidentes y cumplimiento normativo y contractual, mediante el diseño, implementación y control de medidas orientadas a proteger la confidencialidad, integridad, disponibilidad y no repudio de la información, en coherencia con los objetivos estratégicos de la organización.

5. Objetivos

5.1. Gobernanza de Seguridad de la Información: Fortalecer la gobernanza de la seguridad de la información, mediante la definición de lineamientos y directrices claras que deben ser aplicadas por todos los colaboradores y terceros con acceso a los sistemas e infraestructura de TI. Se busca reducir la exposición al riesgo operativo y asegurar el cumplimiento del marco normativo interno.

5.2. Compromiso y sensibilización: Consolidar el compromiso y la sensibilización organizacional, promoviendo la participación activa de la Alta Dirección (ISB) y la concientización continua del personal respecto a la protección de los activos de información.

5.3. Garantizar la Mejora Continua del SGSI: Mediante la implementación sistemática de acciones correctivas y preventivas orientadas a reducir riesgos significativos y a reforzar los controles establecidos.

5.4. Aseguramiento de la Confidencialidad, Integridad, Disponibilidad y No Repudio de la Información: Proteger los Principios Fundamentales de la seguridad de la información: Confidencialidad, Integridad, Disponibilidad y No Repudio, a través de la implementación y supervisión de controles técnicos y organizacionales adecuados.

5.5. Gestión Adecuada de los Riesgos de Seguridad de la Información: Gestionar eficazmente los riesgos de seguridad de la información, asegurando la identificación, evaluación, tratamiento y monitoreo continuo de riesgos que puedan afectar a la organización o a sus clientes.

6. Sanciones

6.1. En caso se identifique el incumpliendo a lo establecido en esta política, se tomarán acciones con base a lo establecido en la **PG-EDP-001 Política para el Proceso Disciplinario del Colaborador** y en caso de ser temas de criticidad alta se considerará lo que establezca el **PG-CCO-003 Código de Ética**.

Fin del Documento

Políticas y Generales

Política Seguridad de la Información

PG-SDI-001

Fecha de Publicación	**25/sep/2025 18:04**			Versión	**8**
Fecha de Elaboración	**24/sep/2025 10:34**	Frecuencia de Vigencia	**12 Meses**	Vigencia del Documento	**25/sep/2026 18:04**
Emisor	**MARIA JOSE TENORIO SIBAJA**				
Puesto	**BUSINESS PROCESSES ANALYST**				

Firmas

Paso	Participante	Puesto	Fecha
Aprobación Business Process	MARIA JOSE TENORIO SIBAJA	BUSINESS PROCESSES ANALYST	24/sep/2025 10:37
Aprobación Dueño de Proceso	MARIO ADOLFO RODRIGUEZ BARRAZA	INFORMATION SECURITY MANAGER	25/sep/2025 18:04