

GRUPO BOLSA MERCANTIL



GRUPO BOLSA
MERCANTIL

POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Septiembre 2026

TABLA DE CONTENIDO

1.	OBJETIVOS.....	3
2.	GENERALIDADES DE LA POLÍTICA	3
2.1.	Alcance y aplicabilidad	3
2.2.	Principios rectores.....	3
2.3.	Gobierno y responsabilidades.....	4
2.3.1.	Modelo de las tres líneas	4
2.3.2.	Roles y responsabilidades	5
2.3.3.	Delegación de gobierno:	6
2.4.	Lineamientos por dominio	6
2.4.1.	Lineamiento de adquisición, desarrollo y mantenimiento de software y sistemas de información.....	6
2.4.2.	Lineamiento de control de acceso	7
2.4.3.	Lineamiento de controles criptográficos	7
2.4.4.	Lineamiento de dispositivos móviles	7
2.4.5.	Lineamientos gestión de activos de información	7
2.4.6.	Lineamiento de las operaciones y comunicaciones.....	8
2.4.7.	Lineamiento interno de relación con terceros.....	8
2.4.8.	Lineamiento de seguridad del recurso humano	8
2.4.9.	Lineamiento interno de seguridad física y del entorno	9
2.4.10.	Lineamiento de gestión de incidentes de seguridad	9
2.4.11.	Lineamiento de monitoreo de alertas de seguridad.....	9
2.4.12.	Lineamiento de escritorio y pantalla limpia.....	10
2.5.	Marco normativo y control	10
2.5.1.	Normativa aplicable	10
2.6.	Estructura documental del SGSI.....	10
2.7.	Ciclo de revisión	10
2.8.	Disposición de acceso en caso de toma de posesión.....	10
3.	HISTORIAL DE CAMBIOS.....	11
Anexo 1.	glosario	12

1. OBJETIVOS

1.1. Objetivo principal

Proteger los activos de información del Grupo Bolsa Mercantil, en adelante el Grupo, frente a riesgos y amenazas internas o externas, deliberadas o accidentales. Esta protección busca preservar la confidencialidad, integridad, disponibilidad, legalidad, privacidad y confiabilidad de la información, contribuir al cumplimiento de la misión y los objetivos estratégicos de la organización, y brindar confianza a los grupos de interés.

1.2. Objetivos específicos

- Definir, implementar, operar y mejorar continuamente el sistema de gestión de seguridad de la información y ciberseguridad (SGSI), con base en los lineamientos internos, los estándares aplicables y la normativa vigente.
- Garantizar la implementación de controles de seguridad de la información y ciberseguridad mediante la asignación de los recursos necesarios para su ejecución y mantenimiento.
- Mantener actualizada esta política para garantizar su vigencia y efectividad frente a las necesidades del Grupo y los requerimientos de los organismos de control.

2. GENERALIDADES DE LA POLÍTICA

2.1. Alcance y aplicabilidad

La presente política aplica a todo el ámbito del Grupo, sus activos de información, sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la organización a través de cualquier tipo de relación.

La presente política debe ser cumplida por:

- La Junta Directiva y la Alta Gerencia.
- Todos los colaboradores, incluyendo pasantes y practicantes.
- Los colaboradores vinculados bajo esquemas de contratación externa.
- Los proveedores de bienes o servicios que puedan afectar los activos de información del Grupo.
- Las sociedades comisionistas miembros de la Bolsa y sus vinculados.
- Los participantes de los mercados y líneas del negocio del Grupo.
- Los organismos externos de supervisión y control, cuando corresponda.

El incumplimiento de la presente política puede generar consecuencias administrativas, disciplinarias, civiles y/o penales, de acuerdo con la normativa interna vigente del Grupo y la legislación colombiana aplicable.

2.2. Principios rectores



La seguridad de la información y ciberseguridad del Grupo se rige por los siguientes principios. Estos deben orientar las decisiones y actuaciones de las personas y entidades incluidas en el alcance de esta política.

PRINCIPIO	DESCRIPCIÓN
Confidencialidad	La información solo está disponible y es revelada a las personas, entidades o procesos autorizados.
Integridad	La información es precisa, coherente y completa durante todo su ciclo de vida.
Disponibilidad	La información y los recursos necesarios para su uso están accesibles cuando se requieran.
Legalidad	El Grupo cumple la normativa legal, reglamentaria y contractual aplicable en materia de seguridad de la información y ciberseguridad.
Confiabilidad	La información es la apropiada para la administración del Grupo y el cumplimiento de sus obligaciones.
Autenticidad	El Grupo garantiza la validez y la verificación del origen de la información, así como de las condiciones en las que se genera, transmite y distribuye.
Auditabilidad	Los eventos significativos se registran para facilitar su posterior verificación y control.
No repudio	Ninguna parte puede alegar que no envió o recibió información válidamente transmitida.
Protección a duplicación	Cada transacción se ejecuta una sola vez, salvo que se establezca lo contrario, con el fin de impedir su reproducción fraudulenta.
Gestión basada en riesgos	Las decisiones relacionadas con seguridad de la información y ciberseguridad se fundamentan en la identificación, análisis, evaluación y tratamiento de los riesgos.
Mejora continua	El Grupo revisa y fortalece permanentemente la gestión de la seguridad de la información y la ciberseguridad frente a los cambios tecnológicos, las amenazas emergentes y las necesidades del negocio.

2.3. Gobierno y responsabilidades

2.3.1. Modelo de las tres líneas

El marco de gestión de riesgos del Grupo se fundamenta en el modelo de las tres líneas, establecido por el Instituto de Auditores Internos (IIA, 2020 — actualizado 2024). Este modelo identifica las estructuras y los procesos que facilitan el logro de los objetivos organizacionales y promueve una estructura de gobierno sólida y una gestión efectiva de los riesgos. Para la gestión de los riesgos de seguridad de la información y ciberseguridad, el Grupo adopta los principios y roles de este modelo y garantiza su correcta implementación en todas las entidades que lo conforman.

A continuación, se describen las tres líneas y sus funciones dentro del SGSI:

LÍNEA	FUNCIÓN
Primera línea: operación	La Vicepresidencia de Tecnología, por medio de la Dirección de Aseguramiento y la Dirección de Producción e Infraestructura, opera los controles, implementa las arquitecturas de seguridad y ejecuta las acciones correctivas de la operación diaria.

	Líderes de proceso, en la gestión de activos de información y el proceso de gestión de riesgos.
Segunda línea: supervisión y control	La Vicepresidencia de Riesgos y Cumplimiento, por medio de la Dirección de Riesgos y del Oficial de Seguridad de la Información, define el modelo de seguridad, supervisa su cumplimiento, gestiona los riesgos de seguridad de la información y monitorea los eventos que puedan afectar los activos de información del Grupo. El Comité de Riesgos actúa como instancia de gobierno, consolida y evalúa los asuntos de seguridad que requieren una decisión estratégica y los presenta ante la Junta Directiva.
Tercera línea: aseguramiento independiente	Auditoría Interna proporciona a la Junta Directiva y al Comité de Auditoría aseguramiento independiente y objetivo sobre la eficacia del gobierno, la gestión de riesgos y el modelo de seguridad de la información y ciberseguridad.

2.3.2. Roles y responsabilidades

ROL	RESPONSABILIDAD PRINCIPAL
Junta Directiva	Aprueba la presente política y sus actualizaciones, hace seguimiento a la gestión del SGSI, garantiza la disponibilidad de los recursos necesarios para su implementación y mejora continua, toma decisiones estratégicas sobre los riesgos que superan el apetito de riesgo definido y promueve una cultura de seguridad de la información y ciberseguridad en todos los niveles del Grupo.
Presidencia	Promueve el compromiso de la alta dirección con la seguridad de la información y ciberseguridad, supervisa que la estrategia del SGSI esté alineada con los objetivos organizacionales y garantiza que los lineamientos del modelo de seguridad se implementen en todas las entidades que conforman el Grupo.
Vicepresidencia de Riesgos y Cumplimiento y Oficial de Seguridad de la Información	Define el modelo de seguridad de la información y ciberseguridad del Grupo, supervisa su cumplimiento, gestiona los riesgos asociados a los activos de información, monitorea los eventos de seguridad y propone al Comité de Riesgos los ajustes estratégicos que requiere el SGSI para su posterior presentación ante la Junta Directiva. Coordina el programa de protección y tratamiento de datos personales y lidera la mejora continua del sistema de gestión.
Vicepresidencia de Tecnología	Opera y administra los sistemas y recursos tecnológicos. Gestiona los riesgos de tecnología de la información, el Plan de Recuperación ante Desastres (DRP) y la continuidad tecnológica. Alinea la tecnología con los requerimientos de seguridad definidos por la Vicepresidencia de Riesgos y Cumplimiento.
Vicepresidencia Financiera	Garantiza la disponibilidad de los recursos presupuestales necesarios para implementar y operar los controles del SGSI.
Vicepresidencia de Talento Humano y Gestión Administrativa	Implementa los controles de seguridad en todas las etapas de la relación laboral, administra la seguridad física de las instalaciones y coordina los programas de formación y sensibilización en seguridad de la información.

Vicepresidencia Jurídica y Secretaría General	Identifica los requisitos legales, reglamentarios y contractuales en materia de seguridad. Verifica que los contratos con terceros incluyan las cláusulas de seguridad y cumplimiento aplicables.
Auditoría Interna	Planifica y ejecuta auditorías periódicas del SGSI con objetividad e imparcialidad. Presenta los resultados al Comité de Auditoría y propone planes de acción.
Propietarios de la información	Clasifican la información según su sensibilidad, documentan esa clasificación y definen qué usuarios pueden acceder a ella, de acuerdo con sus funciones y competencias.
Colaboradores y terceros	Conocen y cumplen esta política y los lineamientos del SGSI. Reportan oportunamente los eventos, incidentes o situaciones que puedan comprometer la seguridad de la información.

2.3.3. Delegación de gobierno:

La Junta Directiva delega en la Vicepresidencia de Riesgos y Cumplimiento la gestión, la actualización y la comunicación de los lineamientos técnicos que desarrollan esta política.

La actualización de estos lineamientos no requiere la aprobación de la Junta Directiva, salvo cuando implique modificaciones a este marco rector.

La Vicepresidencia de Riesgos y Cumplimiento garantiza que los lineamientos vigentes estén disponibles para los grupos de interés, sean revisados al menos una vez al año y respondan a los requisitos normativos aplicables y al perfil de riesgo del Grupo.

2.4. Lineamientos por dominio

Cada dominio desarrolla las disposiciones de esta política de acuerdo con su ámbito de aplicación. Los lineamientos relacionados contienen el detalle operativo, los estándares técnicos y los procedimientos aplicables. Estos documentos forman parte integral del SGSI y son de obligatorio cumplimiento.

2.4.1. Lineamiento de adquisición, desarrollo y mantenimiento de software y sistemas de información.

La operación del Grupo se apoya en plataformas tecnológicas que soportan procesos misionales críticos. Por tanto, una vulnerabilidad presente en cualquier etapa del ciclo de vida del software puede comprometer la confidencialidad, la integridad y la disponibilidad de la información del Grupo y sus clientes.

- La seguridad de la información es un requisito obligatorio durante todo el ciclo de vida del software y de los sistemas de información.
- El Grupo evalúa los requisitos de seguridad como criterio para adquirir sistemas y servicios tecnológicos.
- El Grupo incorpora medidas de seguridad desde las etapas de diseño y desarrollo y durante el mantenimiento de los sistemas.

Ver detalle: *Lineamiento de adquisición, desarrollo y mantenimiento de sistemas.*

2.4.2. Lineamiento de control de acceso

El acceso no autorizado a los sistemas y a la información del Grupo representa uno de los principales riesgos de seguridad en el sector financiero. Garantizar que solo las personas y los procesos autorizados accedan a la información es fundamental para proteger los activos del Grupo y cumplir sus obligaciones regulatorias.

- El acceso a la información y a los sistemas se otorga exclusivamente a las personas y los procesos autorizados, de acuerdo con el principio de mínimo privilegio.
- El Grupo revisa periódicamente los accesos y los revoca de manera inmediata cuando deja de existir la necesidad que justificó su asignación.
- El uso de dispositivos móviles y el trabajo remoto están sujetos a controles robustos de autenticación y autorización.

Ver detalle: *Lineamiento de control de acceso.*

2.4.3. Lineamiento de controles criptográficos

La transmisión y el almacenamiento de información confidencial en un entorno financiero requieren mecanismos que garanticen el acceso exclusivo de las partes autorizadas. El Grupo gestiona información sensible de clientes, operadores y colaboradores. Su divulgación o acceso no autorizado puede generar consecuencias regulatorias, reputacionales y operativas.

- El Grupo utiliza controles criptográficos para proteger la confidencialidad, la integridad y la autenticidad de los activos de información sensibles.
- Los mecanismos de cifrado y la gestión de las llaves criptográficas cumplen los estándares técnicos vigentes aprobados por la Vicepresidencia de Riesgos y Cumplimiento.

Ver detalle: *Lineamiento de controles criptográficos.*

2.4.4. Lineamiento de dispositivos móviles

La operación del Grupo requiere que sus colaboradores accedan a la información y a los sistemas desde distintas ubicaciones y dispositivos. El uso de dispositivos móviles extiende el perímetro de seguridad más allá de las instalaciones físicas del Grupo y aumenta la exposición a riesgos de pérdida, robo o acceso no autorizado a la información.

- El uso de dispositivos móviles para acceder a la información del Grupo está sujeto a las condiciones de seguridad definidas por la Vicepresidencia de Riesgos y Cumplimiento.
- Los colaboradores que utilicen dispositivos móviles para acceder a los sistemas del Grupo son responsables de usarlos adecuadamente y de cumplir los controles aplicables.

Ver detalle: *Lineamiento de dispositivos móviles.*

2.4.5. Lineamientos gestión de activos de información

Los activos de información del Grupo son fundamentales para la operación del negocio. Su identificación, clasificación y protección son necesarias para que los demás controles de seguridad sean eficaces. No es posible proteger lo que no se conoce ni clasificar lo que no tiene un propietario definido.

- Todo activo de información debe tener un propietario responsable de su clasificación, protección y disposición adecuada.
- La información se clasifica y se trata de acuerdo con sus niveles de confidencialidad, integridad y disponibilidad y con las directrices del Grupo.
- El ciclo de vida de los activos de información, incluida su disposición final segura, está sujeto a controles formales.

Ver detalle: *Lineamiento de activos de información.*

2.4.6. Lineamiento de las operaciones y comunicaciones

La disponibilidad y la seguridad de los sistemas de información del Grupo dependen de la adecuada ejecución de los procedimientos operativos y de la protección de las comunicaciones internas y externas. Un cambio no controlado o una comunicación desprotegida pueden afectar la continuidad de los procesos misionales y la integridad de la información.

- Las operaciones tecnológicas se ejecutan de acuerdo con procedimientos documentados y actualizados que incorporan los controles necesarios para proteger la información.
- Las comunicaciones internas y externas del Grupo se realizan por medio de canales autorizados, protegidos y monitoreados.

Ver detalle: *Lineamiento de las operaciones y comunicaciones.*

2.4.7. Lineamiento interno de relación con terceros

El Grupo trabaja con proveedores, contratistas y aliados estratégicos que, en el ejercicio de sus funciones, acceden a la información y a los sistemas del Grupo. El acceso de terceros representa un riesgo que debe gestionarse mediante controles contractuales y operativos, para asegurar que los requisitos de seguridad del Grupo también se apliquen fuera de la organización.

- Todo tercero con acceso a la información del Grupo debe asumir compromisos formales de seguridad y confidencialidad como condición para prestar sus servicios.
- Los contratistas, proveedores y demás terceros que accedan a información del Grupo deben suscribir los acuerdos de confidencialidad aplicables antes de recibir dicho acceso.
- Los contratos con terceros deben incluir cláusulas de seguridad proporcionales al nivel de riesgo. La Vicepresidencia Jurídica y Secretaría General verifica su inclusión.
- El Grupo evalúa periódicamente a los proveedores críticos en materia de seguridad de la información.

Ver detalle: *Lineamiento de relación con terceros.*

2.4.8. Lineamiento de seguridad del recurso humano

Las personas cumplen un papel fundamental en la protección de la información y también pueden generar riesgos de seguridad por acciones involuntarias o deliberadas. El Grupo reconoce que la seguridad de la información no depende exclusivamente de los controles técnicos. También requiere que cada colaborador conozca, comprenda y asuma sus responsabilidades durante toda su vinculación.

- La seguridad de la información debe gestionarse en todas las etapas de la relación laboral: vinculación, permanencia y desvinculación.
- Antes de acceder a los sistemas del Grupo, los colaboradores deben conocer y asumir sus responsabilidades en materia de seguridad de la información.
- La desvinculación debe incluir la revocación inmediata de los accesos y la devolución de los activos de información asignados.

Ver detalle: *Lineamiento de seguridad del recurso humano.*

2.4.9. Lineamiento interno de seguridad física y del entorno

La protección de la información no depende exclusivamente de controles lógicos o tecnológicos. Las instalaciones del Grupo albergan infraestructura crítica. El acceso no autorizado, el daño o la interrupción de esta infraestructura pueden comprometer la operación del negocio y generar efectos similares a los de un ataque cibernético.

- El Grupo protege sus instalaciones y activos tecnológicos contra accesos físicos no autorizados, daños e interferencias.
- El Grupo protege los equipos contra amenazas ambientales y fallas en los servicios de suministro que puedan afectar la operación.
- El Grupo controla y registra el acceso de visitantes a las áreas críticas o restringidas.

Ver detalle: *Lineamiento de seguridad física y del entorno.*

2.4.10. Lineamiento de gestión de incidentes de seguridad

Ningún sistema de seguridad elimina por completo la posibilidad de que ocurra un incidente. La capacidad del Grupo para detectar los eventos de seguridad, responder ante ellos y recuperarse oportunamente es tan importante como la prevención. Esta capacidad contribuye a reducir su impacto en la organización, sus clientes y su reputación.

- Todo evento o incidente de seguridad de la información debe reportarse oportunamente a la Vicepresidencia de Riesgos y Cumplimiento.
- El Grupo dispone de un proceso formal para gestionar los incidentes, responder ante ellos, recuperar la operación, documentar las lecciones aprendidas y fortalecer la mejora continua.
- La Vicepresidencia de Riesgos y Cumplimiento presenta los incidentes de alto impacto ante el Comité de Riesgos y la Junta Directiva, según corresponda.

Ver detalle: *Lineamiento de incidentes de seguridad de la información y ciberseguridad.*

2.4.11. Lineamiento de monitoreo de alertas de seguridad

El entorno de amenazas cibernéticas al que está expuesto el Grupo cambia continuamente. La detección temprana de eventos anómalos mediante el monitoreo continuo de los sistemas, las herramientas y los servicios de ciberseguridad es fundamental para responder ante posibles ataques que, si no se identifican oportunamente, pueden convertirse en incidentes de alto impacto.

- El Grupo mantiene capacidades de monitoreo continuo para detectar amenazas y ciberataques y responder oportunamente ante ellos.
- El Grupo registra, correlaciona y analiza los eventos de seguridad para fortalecer la mejora continua del SGSI.

Ver detalle: *Lineamiento de monitoreo de alertas de seguridad de la información y ciberseguridad.*

2.4.12. Lineamiento de escritorio y pantalla limpia

El puesto de trabajo es uno de los principales puntos de contacto entre los colaboradores y la información del Grupo. Un equipo desbloqueado, una pantalla visible o un documento físico desatendido pueden exponer información confidencial y generar consecuencias similares a las de una brecha de seguridad tecnológica.

- El Grupo establece directrices de escritorio y pantalla limpios para reducir los riesgos de pérdida, modificación o acceso no autorizado a la información durante la jornada laboral y fuera de ella.

Ver detalle: *Lineamiento de escritorio y pantalla limpia.*

2.5. Marco normativo y control

2.5.1. Normativa aplicable

- ISO/IEC 27001:2022. Sistema de Gestión de Seguridad de la Información.
- ISO/IEC 27002:2022. Controles de Seguridad de la Información.

El Normograma del Grupo contiene la normativa legal, regulatoria y sectorial aplicable al SGSI del Grupo. La Dirección de Regulación de la Vicepresidencia Jurídica y Secretaría General gestiona y actualiza el Normograma. La Dirección de Cumplimiento de la Vicepresidencia de Riesgos y Cumplimiento verifica la aplicación de la normativa, de acuerdo con los esquemas regulatorios de la Superintendencia Financiera de Colombia.

2.6. Estructura documental del SGSI

Esta política constituye el marco rector (nivel 1) del Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSI) del Grupo. Sus disposiciones se desarrollan mediante lineamientos específicos por dominio (nivel 2) y documentos operativos (nivel 3), de acuerdo con la naturaleza y la finalidad de cada control.

El Manual de Gobierno de Seguridad de la Información y Ciberseguridad define la arquitectura documental del SGSI, sus tipos documentales y las reglas de jerarquía, aprobación, administración, revisión y control. La Vicepresidencia de Riesgos y Cumplimiento administra este manual.

2.7. Ciclo de revisión

La Vicepresidencia de Riesgos y Cumplimiento revisa esta política al menos una vez al año y la actualiza cuando las condiciones del negocio, el entorno regulatorio o el perfil de riesgo del Grupo lo requieran. La Vicepresidencia de Riesgos y Cumplimiento presenta las modificaciones a la Junta Directiva, que debe aprobarlas antes de su entrada en vigor.

2.8. Disposición de acceso en caso de toma de posesión

La Vicepresidencia de Riesgos y Cumplimiento, en coordinación con la Vicepresidencia Jurídica y Secretaría General, establece el protocolo para garantizar que la Superintendencia Financiera de Colombia (SFC), Fogafín, Fogacoop o las personas que estas entidades designen puedan acceder a la información y a los sistemas que operan en la nube, en caso de toma de posesión de alguna de las entidades que conforman el Grupo.

3. HISTORIAL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO
0	21/11/2018	Versión inicial. Aprobada por la Junta Directiva en sesión 597 del 28 de noviembre de 2018.
1	16/07/2019	Modificación numeral 4. Aprobada por la Junta Directiva en sesión 607 del 26 de junio de 2019.
2	20/01/2022	Revisión y actualización integral con apoyo de Innovinc SAS. Actualización de cargos según nueva estructura organizacional. Aprobada en sesión ordinaria de Junta Directiva No. 652 del 20 de enero de 2022.
3	28/07/2023	Ajustes en objetivo, nombre (se retira 'privacidad'), inclusión de nuevos monitoreos y controles. Aprobada en sesión ordinaria de Junta Directiva No. 677 del 19 de julio de 2023.
4	16/08/2024	Ajustes por cambio de estructura organizacional. Creación de Anexo No. 1 (definiciones). Se crean tres nuevas Lineamientos: incidentes, monitoreo y escritorio/pantalla limpia. Aprobada en sesión ordinaria de Junta Directiva No. 693 del 15 de agosto de 2024.
5	28/09/2026	Reorganización integral de la Política bajo una arquitectura documental de tres niveles. Se mantiene la Política como Marco Rector, se trasladan los anexos a lineamientos específicos por dominio, se independiza el glosario y se reorganizan los contenidos operativos en manuales, procedimientos, instructivos, matrices, formatos y registros. Se ajustan la redacción, las responsabilidades y las referencias documentales. Aprobada en sesión ordinaria de Junta Directiva No. 722 del 20 de agosto del 2026.

ANEXO 1. GLOSARIO

Activo de información: Elemento que el Grupo valora y debe proteger, como datos en medios digitales o físicos, equipos, programas informáticos, servicios y personas con conocimientos críticos para la organización.

Activo tecnológico: Equipo, dispositivo, aplicación, plataforma, servicio, componente de infraestructura o recurso tecnológico utilizado para procesar, almacenar o transmitir información.

Amenaza: Causa potencial de un evento no deseado que puede afectar los activos de información o la operación del Grupo.

Apetito de riesgo: Nivel de riesgo que el Grupo está dispuesto a asumir para alcanzar sus objetivos estratégicos.

Auditabilidad: Propiedad que garantiza el registro de los eventos significativos para facilitar su posterior verificación y control.

Autenticidad: Propiedad que permite verificar la validez del origen de la información y las condiciones de su generación, transmisión y distribución.

Ciberseguridad: Conjunto de capacidades que permiten anticipar, prevenir y enfrentar amenazas cibernéticas para proteger los datos, sistemas y aplicaciones del Grupo.

Colaborador: Persona vinculada laboralmente con alguna de las entidades del Grupo, incluidos los empleados, pasantes y practicantes.

Confidencialidad: Propiedad que garantiza que la información solo esté disponible y se revele a las personas, entidades o procesos autorizados.

Confiabilidad: Propiedad que garantiza que la información sea adecuada para la administración del Grupo y el cumplimiento de sus obligaciones.

Controles criptográficos: Mecanismos que utilizan algoritmos y llaves criptográficas para transformar la información en un formato ininteligible para las personas o los procesos que no estén autorizados para acceder a ella.

Disponibilidad: Propiedad que garantiza que la información y los recursos necesarios para utilizarla estén accesibles cuando se requieran.

Dispositivo móvil: Equipo electrónico de fácil transporte que tiene capacidad para procesar datos y conectarse a redes. Incluye teléfonos inteligentes, tabletas, computadores portátiles y medios de almacenamiento portátiles.

Evento de seguridad: Ocurrencia identificada en un sistema, servicio o red que indica una posible violación de esta política o una situación desconocida que puede ser relevante para la seguridad de la información.

Externalización (outsourcing): Modalidad de contratación mediante la cual el Grupo encarga a un tercero la ejecución de procesos o funciones específicas que pueden implicar el acceso a activos de información.

Gestión basada en riesgos: Enfoque mediante el cual las decisiones relacionadas con la seguridad de la información y la ciberseguridad se fundamentan en la identificación, el análisis, la evaluación y el tratamiento de los riesgos sobre los activos de información.



Grupo Bolsa Mercantil (Grupo): Conjunto de entidades que integran el Grupo Bolsa Mercantil y se encuentran dentro del alcance de esta política.

Incidente de seguridad: Evento o conjunto de eventos que comprometen la confidencialidad, la integridad o la disponibilidad de la información del Grupo.

Integridad: Propiedad que garantiza que la información sea precisa, coherente y completa durante todo su ciclo de vida.

Legalidad: Propiedad que garantiza el cumplimiento de la normativa legal, reglamentaria y contractual aplicable en materia de seguridad de la información y ciberseguridad.

Lineamiento: Documento que desarrolla las disposiciones de esta política y establece directrices específicas para implementar controles dentro de un dominio de seguridad.

Llave criptográfica: Código generado mediante algoritmos que determina la transformación de un texto legible en un texto cifrado o viceversa. Las llaves criptográficas son información de alta sensibilidad y su acceso debe estar estrictamente limitado.

Marco rector: Documento de mayor nivel jerárquico dentro de la estructura documental del SGSI. Establece los principios, el gobierno y los lineamientos que rigen la seguridad de la información y la ciberseguridad en el Grupo.

Mejora continua: Actividad recurrente mediante la cual el Grupo mejora el desempeño del SGSI y revisa sus componentes frente a los cambios tecnológicos, las amenazas emergentes y las necesidades del negocio.

Mínimo privilegio: Principio según el cual cada usuario, proceso o sistema debe tener acceso únicamente a los recursos necesarios para cumplir sus funciones.

Modelo de las tres líneas: Marco de gobierno establecido por el Instituto de Auditores Internos que define tres niveles de responsabilidad: operación de los controles, supervisión y aseguramiento independiente.

Monitoreo: Proceso continuo de observación y análisis de los eventos registrados en los sistemas de información para detectar oportunamente amenazas, vulnerabilidades o incidentes de seguridad.

No repudio: Propiedad que garantiza que ninguna de las partes pueda negar el envío o la recepción de información transmitida válidamente.

Normograma: Compilación organizada de la normativa legal, regulatoria y sectorial aplicable al Grupo. La Dirección de Regulación de la Vicepresidencia Jurídica y Secretaría General gestiona y actualiza este documento.

Oficial de seguridad de la información: Rol responsable de definir y supervisar el modelo de seguridad de la información y ciberseguridad del Grupo.

Plan de recuperación ante desastres (DRP): Conjunto de estrategias, procedimientos y recursos destinados a restablecer los servicios tecnológicos y la infraestructura crítica después de una interrupción o un desastre.

Privacidad: Propiedad que garantiza que los datos personales se traten de manera legítima, segura y transparente, de acuerdo con las finalidades autorizadas, los derechos de sus titulares y la normativa aplicable.

Propietario de la información: Colaborador responsable de clasificar los activos de información según su sensibilidad, documentar esta clasificación y definir los usuarios que pueden acceder a ellos de acuerdo con sus funciones y competencias.

Protección contra la duplicación: Propiedad que garantiza que una transacción se ejecute una sola vez, salvo que se establezca lo contrario, para impedir su reproducción fraudulenta.

Proveedor crítico: Tercero cuya falla, indisponibilidad, incumplimiento o afectación de seguridad puede generar un impacto significativo en la operación, los activos de información o las obligaciones del Grupo.

Recurso tecnológico: Elemento de equipos, programas informáticos, telecomunicaciones, infraestructura, servicios en la nube o componentes tecnológicos utilizado por el Grupo.

Riesgo de seguridad de la información: Posibilidad de que una amenaza aproveche una vulnerabilidad y genere consecuencias negativas sobre los activos de información, los procesos o los objetivos del Grupo.

Seguridad de la información: Conjunto de políticas, procesos, controles y prácticas orientados a preservar la confidencialidad, la integridad, la disponibilidad, la autenticidad, la legalidad, la privacidad y la confiabilidad de la información.

Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSI): Conjunto de políticas, procesos, procedimientos, responsabilidades, recursos y controles mediante los cuales el Grupo dirige, implementa, opera, monitorea, revisa y mejora la seguridad de la información y la ciberseguridad.

Tercero: Persona natural o jurídica externa que mantiene una relación contractual, comercial, operativa o de prestación de servicios con el Grupo.

Toma de posesión: Medida de intervención adoptada por la autoridad competente que puede requerir el acceso a la información, los sistemas y los servicios de las entidades que conforman el Grupo.

Vulnerabilidad: Debilidad de un activo, sistema, proceso o control que puede ser aprovechada por una amenaza y ocasionar un incidente de seguridad.