POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

GFI Securities Colombia S.A.

Este segmento es extraído del Manual de Políticas de Seguridad de la Información y Ciberseguridad de la compañía, el cual aplica para proveedores, contratistas y público en general.

INTRODUCCIÓN

El presente documento consagra la Política de Seguridad de la Información y Ciberseguridad (PSIC) para la compañía GFI SECURITIES COLOMBIA S.A., como también sus directrices y generalidades para su debido cumplimiento.

La presente política está conformada por generalidades, estándares (técnicos y generales de seguridad de la información), arquitectura computacional, procesos y procedimientos, estructura organizacional y mecanismos de verificación y control; y tiene como propósito garantizar que los riesgos de seguridad de la información y los riesgos de ciberseguridad sean conocidos, asumidos, gestionados y mitigados de forma documentada, sistemática, estructurada, eficiente y adaptable a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

La Políticas de Seguridad de la Información y Ciberseguridad como sus generalidades son elementos fundamentales dentro del PSIC, puesto que contienen directrices que enmarcan la actuación de todos los empleados, afiliados, proveedores y/o contratistas de GFI SECURITIES COLOMBIA S.A.

ÁMBITO DE APLICACIÓN

Esta Política será aplicable a la protección de los datos y sistemas según los lineamientos del corporativo (BGC Partners Inc), para lograr un funcionamiento de manera efectiva, salvaguardando los activos y la información de la compañía.

OBJETO

La Política de Seguridad de la Información y Ciberseguridad tienen por objeto la protección de los activos estratégicos de la compañía que dependen o usan las tecnologías de la información y las comunicaciones. Los objetivos específicos de esta política son:

- Establecer directrices generales relacionadas con seguridad de la información y ciberseguridad;
- Ser un medio de divulgación para comunicar los lineamientos establecidos por la Administración de la Compañía respecto a la seguridad de la información y la ciberseguridad, generando cultura y compromiso en todos los niveles de la organización;
- Establecer y comunicar la responsabilidad y autoridad sobre el manejo de la seguridad de la información y la ciberseguridad de la Compañía;
- Orientar el debido cuidado y la debida diligencia en la gestión de la seguridad de la información y la ciberseguridad;
- Establecer un orden y marco de actuación en temas de seguridad de la información y ciberseguridad, para todas las personas que presten sus servicios a GFI Securities Colombia S.A.;
- Garantizar la confiabilidad, imagen y credibilidad de la compañía con sus empleados, afiliados y terceros en general;
- Definir un lenguaje común sobre la seguridad de la información y la ciberseguridad dentro de la organización.

DEFINICIONES

- ACTIVO DE INFORMACIÓN: Conocimiento o datos que tienen valor para la entidad o el individuo.
- CIBERAMENAZA O AMENAZA CIBERNÉTICA: Aparición de una situación potencial o actual que pudiera convertirse en un ciberataque.
- CIBERATAQUE O ATAQUE CIBERNÉTICO: Acción criminal organizada o premeditada de uno o más agentes que usan los servicios o aplicaciones del ciberespacio o son el objetivo de esta o donde el ciberespacio es fuente o herramienta de comisión de un crimen.
- CIBERESPACIO: Entorno complejo resultante de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos conectados a dicha red, el cual no existe en ninguna forma física.
- RIESGO CIBERNÉTICO: Posibles resultados negativos derivados de fallas en la seguridad de los sistemas tecnológicos o asociados a ataques cibernéticos.
- CIBERSEGURIDAD: Es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la entidad.
- CUSTODIO: Persona o el área responsable de proteger la información, de acuerdo con los lineamientos establecidos por el Generador (ver definición más adelante).
- ESTÁNDAR DE SEGURIDAD DE LA INFORMACIÓN: Conjunto de requisitos de obligatorio cumplimiento que especifica tecnologías, métodos y delimita las responsabilidades respecto de la seguridad de la información; así mismo establece pautas de acciones, según lo que les corresponda a las áreas en el ámbito de sus funciones.
- EVENTO DE CIBERSEGURIDAD: Ocurrencia de una situación que podría afectar la protección o el aseguramiento de los datos, sistemas y aplicaciones de la entidad que son esenciales para el negocio.
- EVIDENCIA DIGITAL: Información con valor probatorio generada, transmitida o almacenada en forma digital (generada por computador o generada por medio diferente y almacenado o transmitido por computador).
- GENERADOR O RESPONSABLE: Persona o área que crea la información.
- INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: Cualquier evento adverso que afecte o amenace los fundamentos de seguridad de la información (Confidencialidad, Integridad, Disponibilidad), de tal manera que genere un impacto negativo sobre la información o la Compañía.
- INCIDENTE DE CIBERSEGURIDAD: Es cualquier evento adverso, real o sospechoso, que afecte o amenace con afectar la protección o el aseguramiento de los datos, sistemas y aplicaciones de la entidad que son esenciales para el negocio.
- INFORMACIÓN CORPORATIVA: Aquella que cumple con al menos una de las siguientes características:
  (i) Se produce, envía o recibe en desarrollo de una función, actividad, servicio u operación, asignada a la Compañía.
  (ii) Sirve de sustento o prueba de derechos, obligaciones o responsabilidades a cargo de la Compañía o de terceros en relación con el mismo.
  (iii) Aquella en la que constan las decisiones, normas o políticas tomadas o establecidas por las instancias competentes de la Compañía.
  (iv) Se genera como resultado de la interacción entre la Compañía y sus clientes, contratistas, o usuarios, que puede ser de interés para éstos o puede generar efectos jurídicos.
  (v) Se requiere con el fin de dar cumplimiento a alguna norma o política, dejar evidencia y prueba de las actuaciones realizadas por los empleados de la Compañía o por terceros que le prestan servicios.
  (vi) Contribuye a la memoria institucional.
- ISO 27002 FRAMEWORK: Es un estándar de seguridad de la información que proporciona recomendaciones de mejores prácticas sobre controles de seguridad de la información

para uso de los responsables de iniciar, implementar o mantener sistemas de gestión de seguridad de la información (SGSI). Infraestructura Crítica: Activos y sistemas, físicos o virtuales, que son tan vitales para la nación que la obstrucción o destrucción de estos activos y sistemas, podría ocasionar impactos adversos en la ciberseguridad nacional, en la seguridad económica y social, en la salud pública, o en una combinación de estos asuntos.

- PERSONAS QUE PRESTAN SERVICIOS A LA COMPAÑÍA: Comprende funcionarios, empleados, contratistas, empleados temporales, estudiantes en práctica y otros terceros que prestan servicios a GFI SECURITIES Colombia S.A.
- LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (TIC): Son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios; que permiten la compilación, procesamiento, almacenamiento, transmisión de información como: voz, datos, texto, video e imágenes (Ley 1341 de 2009 Art. 6).
- NIST CYBERSECURITY FRAMEWORK: El Marco de Ciberseguridad de NIST proporciona un marco de políticas de orientación de seguridad informática sobre cómo las organizaciones del sector privado en los Estados Unidos pueden evaluar y mejorar su capacidad para prevenir, detectar y responder a los ataques cibernéticos. Este Marco voluntario consta de estándares, directrices y mejores prácticas para gestionar los riesgos relacionados con la seguridad cibernética.
- RECURSOS DE TECNOLOGÍA DE INFORMACIÓN: Recursos o apoyos tecnológicos ofrecidos por la Compañía a los empleados o a terceros para el normal desempeño de sus funciones (ej.: correo, Internet, teléfonos, computadores personales, servidores de archivo, cuentas de acceso, etc.).
- RESILIENCIA: Capacidad de continuar prestando sus funciones misionales ante la materialización de eventos adversos críticos contra sus activos de información y plataforma tecnológica.
- USUARIO: Es aquella persona o área que ha sido autorizada por el Generador para tener acceso a cierta información.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

GFI SECURITIES COLOMBIA S.A., es consiente que la seguridad de la información y ciberseguridad es un componente crítico que se requiere para asegurar la confidencialidad, integridad y disponibilidad de los datos, la red y recursos de procesamiento. En su Política de Seguridad de la Información y Ciberseguridad la compañía garantiza la adecuada protección de los datos y sistemas, logrando así que funcione de manera efectiva, salvaguardando los activos y la información de la compañía.

GFI SECURITIES COLOMBIA S.A., implementa un programa de seguridad de la información y ciberseguridad alineando con las políticas corporativas, que busca el mejoramiento continuo para vigilar y promover el buen uso de la información y de los recursos tecnológicos.

POLÍTICAS GENERALES

En virtud de lo anterior, GFI Securities Colombia S.A., desarrolla las siguientes Políticas Generales de Seguridad de la Información:

- La Compañía gestiona la Seguridad de la Información y Ciberseguridad basado en el Sistema de Administración de Riesgos Operativos. Dicha gestión soporta la debida protección de la información a partir de principios universalmente aceptados de seguridad de la información (Confidencialidad, Integridad, Disponibilidad);
- La Compañía valora la información desde el punto de vista de seguridad y acorde a ello determina los mecanismos de protección adecuados;
- La Compañía desde las etapas iniciales de los proyectos, incluye la evaluación de aspectos relacionados con la arquitectura de seguridad y sigue los lineamientos establecidos al respecto;
- La Compañía atiende los incidentes relacionados con la seguridad de la información y ciberseguridad;
- La Compañía implementa mecanismos para vigilar y promover el buen uso de los recursos tecnológicos;
- La Compañía implementa mecanismos para vigilar y promover el buen uso de la información;
- La Compañía implementa controles de acceso (físicos y lógicos) para que la información corporativa se encuentre debidamente protegida. Así mismo, tiene mecanismos para seguimiento de actividades no autorizadas sobre la información o recursos de tecnología;
- La Compañía implementa mecanismos y procedimientos para minimizar los riesgos asociados a la gestión de la información en los procesos que soportan la operación del negocio;
- La Compañía implementa mecanismos y procedimientos para minimizar los riesgos asociados a la administración de la plataforma tecnológica que soporta la operación del negocio;
- La Compañía implementa un programa de ciberseguridad alineado con mejores prácticas y la Política Nacional de Ciberseguridad. Dicho programa busca el mejoramiento continuo de su postura de seguridad y aumentar su resiliencia.

RESPONSABILIDADES

PROVEEDORES

EL PROVEEDOR se compromete a cumplir con las siguientes obligaciones de la Política de Seguridad de la Información y Ciberseguridad:

- Todos los proveedores tienen la responsabilidad de proteger la información que está bajo su cuidado;
- Los proveedores que tengan acceso a información de la compañía deben reportar de inmediato los incidentes de seguridad en los cuales se pueda afectar la confidencialidad, integridad o disponibilidad de esta;
- Todo proveedor y/o tercero que tenga acceso a los activos de información y preste servicios a GFI Securities Colombia S.A., debe contar con políticas, normas y estándares de Seguridad de la Información al interior de su organización; las cuales deben desarrollarse y mantenerse actualizadas acorde con los riesgos a los que se ve enfrentada su organización;
- Todo Proveedor que preste el servicio de desarrollo de Software a GFI Securities Colombia S.A., debe implementar normas o las mejores prácticas de la industria en el desarrollo de las aplicaciones para garantizar la seguridad de los sistemas;
- Todo Proveedor y/o tercero que preste el servicio de desarrollo de Software a GFI Securities Colombia S.A., antes de enviar una aplicación a producción o ponerla a disposición de la compañía, debe realizar la revisión de los códigos fuente a través de un procedimiento manual o automático que permita identificar posibles vulnerabilidades en la codificación y su correspondiente solución. La no verificación de este procedimiento no exime a EL PROVEEDOR de su responsabilidad;
- Utilizar software legalmente adquirido, en cumplimiento de la Ley Colombiana. Para el efecto mantendrá indemne a GFI Securities Colombia S.A., de cualquier tipo de reclamación;
- Establecer con GFI Securities Colombia S.A., el procedimiento adecuado para el borrado seguro de la información propiedad de la compañía, sus clientes y/o terceros. Este procedimiento deberá ser desarrollado antes o durante el transcurso de la relación contractual;
- Todo proveedor y/o tercero que esté relacionado con los procesos y activos críticos para el negocio de GFI Securities Colombia S.A., debe contar con controles para evitar ataques contra la seguridad de la información y ciberseguridad, plan de contingencia y continuidad del negocio para los servicios prestados a la compañía;
- Todo proveedor y/o tercero que preste servicios a GFI Securities Colombia S.A., debe cumplir con las regulaciones locales y/o certificaciones de privacidad y seguridad de la información;

Para reportar cualquier evento sospechoso o un incidente de seguridad asociado a las actividades desarrolladas por GFI Securities Colombia S.A., sus clientes y/o sus terceros, por favor póngase en contacto con el Director de Tecnología e Información de la compañía a través de los siguientes canales de comunicación:

Teléfono: +57 (1) 7463600
Correo Electrónico: Wilson.Padilla@gfigroup.com

CONSUMIDORES FINANCIEROS

Estas son las medidas de seguridad y recomendaciones que deben adoptar nuestros clientes para su ciberseguridad:

- Los sistemas de GFI Securities Colombia S.A., se deben utilizar desde equipos y dispositivos confiables, preferiblemente que sean avalados por cada entidad. Los dispositivos de acceso público son manipulados por terceros y generan vulnerabilidades de acceso a la información.
- Las credenciales de usuario y contraseña no se deben compartir con terceros. Son personales e intransferibles y se deben mantener en reserva.
- El usuario debe bloquear y/o cerrar sesión cuando no esté utilizando los sistemas de GFI Securities Colombia S.A. Cuando el usuario no esté enfrente de las pantallas que dan acceso a los sistemas de GFI Securities Colombia S.A., estos se deben desconectar cerrando las sesiones.
- Aplique con periodicidad en los equipos y dispositivos las ultimas actualizaciones de parches y actualizaciones de los sistemas operativos y aplicaciones que se utilicen.
- Utilice en sus dispositivos programas de seguridad: Antivirus, Antimalware, Antispam, entre otros.
- Garantice la funcionabilidad de sus sistemas directamente con el área de Tecnología de su entidad. En caso necesario solicite apoyo para las aplicaciones y sistemas de GFI Securities Colombia S.A., a nuestra área de Tecnología e Información.

ESTRATEGIA DE COMUNICACIÓN

En caso de que dentro del análisis de los incidentes cibernéticos se identifique afectación significativa en la confidencialidad, integridad o disponibilidad de la información el Líder de la USIC y el Coordinador de Riesgos y Procesos procederán a:

- Reportar a la SFC el incidente que afecte de manera significativa la confidencialidad, integridad o disponibilidad de la información de GFI Securities Colombia S.A., haciendo una breve descripción del incidente, su impacto y las medidas adoptadas para gestionarlo;
- Reportar a las autoridades que hacen parte del modelo nacional de gestión de incidentes cibernéticos los incidentes cibernéticos;
- Informar a los clientes comprometidos vía correo electrónico y/o telefónicamente describiendo el incidente, su impacto y las medidas adoptadas para remediar la información.

LEGISLACIÓN NACIONAL VIGENTE Y JURISDICCIÓN APLICABLE

Esta política se rige por las leyes de la República de Colombia y por lo dispuesto en la Circular Externa 007 de 2018 y demás normas que las modifiquen, deroguen o sustituyan.

La actualización de este documento está basada en el Manual de Política de Seguridad de la Información y Ciberseguridad, el cual se presenta para su aprobación a la Junta Directiva de GFI Securities Colombia S.A., cada vez que sea necesario.