DIRECTRIZ ESTRATEGICA
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Control del documento

Versión	Fecha	Cambio	Aprobado
1.0	15/06/2018	Versión inicial	Director de Riesgos no Financieros
1.1	15/03/2019	Revisión y actualización. Acta Comité de Auditoría No. 53. Acta JD Marzo 15/2019	Director de Riesgos no Financieros
1.2	21/05/2021	Revisión Comité de Auditoría No. 68. Mayo 21/2021	Junta Directiva
2.0	29/08/2025	Revisión y actualización de Comité de Auditoría (12/08/2025) y Junta Directiva (29/08/2025)	Junta Directiva

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

La Cámara de Riesgo Central de Contraparte de Colombia S.A. (CRCC) como proveedora de infraestructura y entidad de contrapartida central del mercado de valores y divisas, está comprometida en establecer, implementar, mantener y mejorar de forma continua el Sistema de Gestión de Seguridad de la Información y Ciberseguridad, el cual está alineado con la misión, visión y plan estratégico de la organización.

Este Sistema tiene como propósito gestionar los riesgos asociados a los activos de información, para preservar la confidencialidad, integridad y disponibilidad de dichos activos y gestionar los incidentes de seguridad; asegurando el cumplimiento de los requisitos legales y contractuales aplicables en materia de seguridad de la información, así como las expectativas y necesidades de las partes interesadas.

Así mismo, esta Política busca mejorar la resiliencia operativa digital, al reconocer la interdependencia sistémica de la organización con las demás entidades del sector financiero colombiano y la amenaza que representan los incidentes de seguridad generalizados para la confianza y funcionamiento del mercado.

Los objetivos generales para la gestión de la seguridad de la información y ciberseguridad son:

- Promover la cultura en seguridad de la información y ciberseguridad para los colaboradores y terceros, entrenando y capacitando a las partes interesadas.
- Establecer y asignar una estructura de gobierno donde se definan de forma clara los roles, responsabilidades y autoridades frente a la seguridad de la información y ciberseguridad.
- Asignar el personal, los recursos físicos, económicos y tecnológicos para la gestión de la seguridad de la información y ciberseguridad.
- Identificar, medir, controlar y monitorear los riesgos de seguridad de la información y ciberseguridad.
- Prevenir, resistir, responder y recuperarse de incidentes que afecten la confidencialidad, integridad y disponibilidad de la información.

- Proteger los activos de información críticos de la organización, de las amenazas, ya sean internas y/o externas, deliberadas o accidentales.

- Asegurar la continuidad de los servicios ante la materialización de un incidente de seguridad de la información.

- Cuando se generen nuevos proyectos, procesos o servicios se debe evaluar su impacto en la gestión de seguridad de la información y ciberseguridad y la necesidad de incluir nuevos procesos críticos o de ajustar los requerimientos mínimos tecnológicos y operativos.

La CRCC designa a la Dirección de Riesgos no Financieros como la encargada de establecer los lineamientos y las estrategias de seguridad de la información y ciberseguridad, para lo cual se toma como referencia los estándares NIST, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 27031, ISO/IEC 27032, ISO/IEC 27035 y CIS Critical Security Controls y se obliga como entidad vigilada por la Superintendencia Financiera de Colombia a atender las disposiciones contenidas en la Circular Básica Jurídica en la Parte I, Título IV, Capítulo V (requerimientos mínimos para la gestión de la seguridad de la información y ciberseguridad) y en la Parte I, Título II, Capítulo I (canales, medios, seguridad y calidad en el manejo de información en la prestación de servicios financieros).

La Política Seguridad de la Información y Ciberseguridad debe ser revisada al menos una vez cada año por el Comité de Auditoría y en caso de presentarse cambios, por la Junta Directiva.