1. OBJETIVO

Establecer el marco general para la Ciberseguridad y Seguridad de la Información, preservando su confidencialidad, integridad y disponibilidad, la continuidad al negocio, gestionar los riesgos asociados y cumplir con la misión, los objetivos estratégicos de la Organización y sus normas aplicables.

1.1. Objetivos específicos

- Establecer un marco y orden de actuación frente a la Ciberseguridad y Seguridad de la información.
- Establecer roles y responsabilidades en la gestión de Ciberseguridad y Seguridad de la información.
- Definir un lenguaje común en temas de Ciberseguridad y Seguridad de la información.
- Definir, implementar y mejorar de forma continua la gestión de Ciberseguridad y Seguridad de la información, alineada con las necesidades del negocio y con los requerimientos regulatorios internos y externos.

2. ALCANCE

Esta Política es aplicable y de obligatorio cumplimiento para todas sus dependencias y procesos de la FNC, en concordancia con los roles y responsabilidades definidos en este documento, que debe estar a disposición para conocimiento de terceros y usuarios externos.

3. CONDICIONES GENERALES

- Esta Política es un elemento fundamental del Buen Gobierno y Transparencia en la organización.
- Este documento está alineado con regulaciones de orden legal aplicables asociadas a la ciberseguridad y seguridad de la información, con los Estatutos de la FNC, el Código de Ética y Buen Gobierno Corporativo y se desarrolla a través de manuales, procedimientos y controles.
- La identificación y clasificación de los Activos de Información es la base para la gestión de riesgos de ciberseguridad y seguridad de la información, con el fin de determinar los niveles de protección adecuados.

4. GLOSARIO

Activo: Cualquier elemento valioso para una organización que debe ser protegido del acceso no autorizado, uso, divulgación, modificación, destrucción o compromiso.

Activo de Información: Es la información, los sistemas de información y plataformas tecnológicas relacionados con el tratamiento de la información en forma física o digital.

Amenaza: Causa potencial de un incidente de seguridad de la información no deseado, que puede resultar en daño a un sistema, persona u organización. (Adaptado ISO/IEC 27032:2020).

Ciberespacio: Entorno resultante de la interacción de personas, software y servicios en Internet, por medio de dispositivos tecnológicos y redes conectadas a él, que no existe en ninguna forma física. (Adaptado ISO/IEC 27032:2020).

Ciberseguridad: Preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio. (ISO/IEC 27032:2020).

Clasificación de los activos de información: Permite a la FNC asignar un valor a los activos de información en función de proteger el acceso no autorizado, modificación, divulgación o destrucción; y otras variables como las necesidades del negocio, cumplimiento regulatorio, requisitos legales, etc.

Confidencialidad de la información: Propiedad que se refiere a que la información no esté disponible ni sea revelada a individuos, organizaciones o procesos no autorizados. (MinTIC).

Dato: Unidad mínima de información que por sí misma no tiene sentido para quien la posee; sin embargo, adquiere mayor relevancia cuando conforma un conjunto coherente para el que la interpreta. (Glosario Isolución).

Disponibilidad de la información: Propiedad de la información que se refiere a que ésta debe de ser accesible y utilizable por solicitud de una persona, entidad o proceso autorizada cuando así lo requiera. (MinTIC).

Información: Conjunto organizado de datos, contenido en cualquier documento que se genere, obtenga, adquiera, transforme o controle. (Adaptado Ley 1712 de 2014 - Transparencia).

Integridad de la información: Se refiere a la exactitud y completitud de la información, esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción.(MinTIC)

Plataforma tecnológica: Se refiere a un conjunto de herramientas, componentes y servicios que proporcionan una base para el desarrollo y la implementación de aplicaciones y sistemas de software. Puede incluir hardware, software, redes, sistemas operativos y otros componentes necesarios para ejecutar aplicaciones. Estas plataformas suelen estar diseñadas para admitir diferentes tipos de aplicaciones y permitir la integración de diversas tecnologías.

Riesgo de Seguridad de la Información: Es la afectación negativa a un activo de información, generado por una amenaza que se aprovecha de una vulnerabilidad para causar el daño, afectando la Confidencialidad, Integridad y Disponibilidad.

Sistemas de Información: Conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes que manejan o tratan la información.(ISO/IEC 27000:2014).

Terceros y usuarios externos: Personas naturales o jurídicas que no son parte de la organización, que aportan valor a la misma y que por su labor desarrollan actividades en el cual deben acceder y obtener información de la empresa. (BASC).

Tratamiento: Cualquier operación o conjunto de operaciones sobre la información, tales como recolección, almacenamiento, uso, circulación o disposición final. (SIC)

Vulnerabilidad: Debilidad de un activo o control que puede ser aprovechado por una amenaza. (ISO/IEC 27032:2020).

5. CONTENIDO

5.1. MARCO LEGAL

La FNC protege la integridad, la disponibilidad y la confidencialidad de la información propia y de terceros a la que tiene acceso.

La FNC protege el centro de cómputo principal, el centro de cómputo alterno, los centros de cableado, los servicios en nubes públicas o privadas y demás infraestructura tecnológica que soporta sus procesos, ya sea por sus propios medios o gestionando lo que corresponda con los respectivos proveedores.

La FNC controla la operación de sus procesos de negocio preservando la confidencialidad, integridad y disponibilidad de la información en los sistemas de información y/o plataformas tecnológicas.

La FNC implementa controles de acceso a la información, en los sistemas de información y plataformas tecnológicas.

La FNC vela por el cumplimiento de metodologías y procedimientos del ciclo de vida de desarrollo de software incluyendo requerimientos de seguridad de la información en cada una de sus etapas.

La FNC busca mejorar el modelo de seguridad de la Información a través de una adecuada gestión de eventos de riesgo, incidentes y vulnerabilidades asociadas a los activos de información.

La FNC vela por la disponibilidad de la información en los sistemas de información y/o plataformas tecnológicas de sus procesos de negocio.

La FNC cumple con las obligaciones legales / regulatorias aplicables y contractuales relacionadas con ciberseguridad y seguridad de la información.

La FNC identifica, clasifica y protege sus activos de información, con el fin de preservar la confidencialidad, integridad y disponibilidad; así como los datos personales que sean tratados por éstas.

La FNC protege la información creada y transmitida por los procesos de negocio, con el fin de minimizar impactos financieros, reputacionales, operativos o legales debido a un uso inadecuado de ésta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o bajo su custodia.

La FNC cuenta con responsables para la implementación de la Política y Lineamientos de Ciberseguridad y Seguridad de la Información, buscando:

- Cumplir con lo indicado en el Manual de Ciberseguridad y Seguridad de la Información.
- Mantener la confianza sobre el manejo de la información bajo custodia de la FNC; tanto de las personas que le prestan servicio, como de terceros y usuarios externos.
- Proponer y apoyar las acciones de mejora en tecnología para la ciberseguridad y seguridad de la información.
- Establecer los lineamientos, procedimientos, metodologías e instructivos en materia de ciberseguridad y seguridad de la información.
- Promover la cultura de ciberseguridad y seguridad de la información, para fortalecer el Buen Gobierno y la Transparencia.
- Garantizar la continuidad del negocio frente a incidentes de Seguridad de la Información.

5.2 ROLES Y RESPONSABILIDADES

Los roles y responsabilidades definidas para la Ciberseguridad y Seguridad de la información son:

ROL	RESPONSABILIDADES
Comité Directivo y Gerente General	• Revisar y aprobar la Política Ciberseguridad y Seguridad de la Información. • Revisar la eficacia de la implementación de la Política y del Manual de lineamientos de Ciberseguridad y Seguridad de la Información. • Proporcionar y avalar los recursos necesarios para el desarrollo, la implementación y el mantenimiento de proyectos de Seguridad de la Información. • Promover el cumplimiento de las políticas y manuales definidos para Gestionar la Ciberseguridad y Seguridad de la Información • Mantener la confidencialidad, integridad y disponibilidad de los activos de información de la FNC.
Gestionar Tecnología de la Información y Comunicaciones	• Cumplir con la política y los lineamientos de ciberseguridad y seguridad de la información establecidos para la FNC. • Establecer e implementar controles a nivel de seguridad de la información con el fin de mitigar los riesgos que puedan afectar los activos de información en cuanto a la confidencialidad, disponibilidad e integridad de la información.
Gestionar Seguridad de la información	• Acompañar a los procesos en la identificación de necesidades de ciberseguridad y seguridad de la Información desde el punto de vista del negocio y cumplimiento, así como liderar los esfuerzos para su implementación. • Planear las actividades encaminadas a la administración de la ciberseguridad y seguridad de la información de la información, teniendo en cuenta procedimientos y requisitos legales. • Elaborar, proponer y comunicar políticas, lineamientos, metodologías, estándares, procedimientos, prácticas y guías para la gestión de la ciberseguridad y seguridad de la información. • Gestionar el desarrollo y la aplicación de la política de ciberseguridad y seguridad de la información; así como, de las normas, directrices y procedimientos, para el mejoramiento continuo. • Elaborar y presentar informes para las instancias pertinentes, con la periodicidad que corresponda y según la normatividad vigente. • Gestionar y apoyar el desarrollo de las actividades del Sistema de Administración de Riesgos de la FNC. • Proponer, implementar y gestionar acciones de mejoramiento que propicien el logro de los objetivos, el cumplimiento de los requisitos legales y otros requisitos, la atención de las partes interesadas y el aumento de la satisfacción de los clientes. • Dar a conocer a los procesos las irregularidades, incidentes o prácticas que atenten contra la ciberseguridad y seguridad de la información. • Planear y realizar pruebas de ciberseguridad y seguimiento a las acciones resultantes de dicha actividad.
Gestionar Asuntos Jurídicos	• Asesorar a los procesos en temas jurídicos y legales que involucren acciones ante las autoridades competentes relacionados con ciberseguridad y seguridad de la información.
Auditoría Interna Al Sistema De Control Interno	• En su función de aseguramiento, evaluar la eficacia de la gestión de riesgos; evaluar los reportes sobre riesgos; mantener informada a la alta dirección y proponer sus planes de auditoría basados en la evaluación de riesgos de la Organización. • Coordinar actividades para hacking ético y realizar seguimientos a las acciones resultantes de dicha actividad.
Gestionar Comunicaciones	• Apoyar en las labores de comunicación y sensibilización en temas de ciberseguridad y seguridad de la información.
Colaboradores	• Dar cumplimiento a las políticas, manuales y procedimientos de Gestionar Ciberseguridad y Seguridad de la información. • Reportar incidentes de seguridad que atenten contra la confidencialidad, integridad o disponibilidad de la información o evidencian un incumplimiento de las políticas de seguridad. • Participar activamente de las capacitaciones y campañas de sensibilización que se realicen desde Seguridad de la Información. • Participar de las actividades para la identificación de activos y riesgos de seguridad de la información de sus respectivas dependencias/ procesos /centros logísticos.
Terceros y usuarios externos	• Conocer la política de Ciberseguridad y seguridad de la información

5.3 SANCIONES

El incumplimiento de esta política de Ciberseguridad y Seguridad de la información, de los manuales y procedimientos que la desarrollen, por parte de los colaboradores, se considera como falta grave al Reglamento Interno de Trabajo de la Organización, a los contratos de vinculación como tal justa causa de terminación de la relación contractual, sin perjuicio de las demás acciones legales a que haya lugar.

5.4 ACTUALIZACIÓN O CONTROL DE CAMBIOS DEL DOCUMENTO

El presente documento se revisará al menos una vez al año y se actualizará cuando se presenten cambios significativos, cambios en el contexto interno o externo, o cambios en las regulaciones aplicables para la FNC.

6. REFERENCIAS

FE-RC-M-0005 MANUAL DE LINEAMIENTOS DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN

FE-GH-F-0089 CÓDIGO DE ÉTICA Y BUEN GOBIERNO

7. ANEXOS

RESOLUCIÓN 02 DE 2024 24 DE SEPTIEMBRE DE 2024

LISTA DE VERSIONES

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
1	11/Dic/2024	Por requerimientos de BASC y mejores prácticas: • Ajustes en redacción en todo el documento. • El término "Privacidad" ese incluye en el criterio de CONFIDENCIALIDAD • Se incluyen Condiciones Generales • Se complementa el Glosario • Se modifica el Marco General • Se extienden los roles y responsabilices • Se incluyen sanciones en caso de incumplimiento Este documento reemplaza al FE-RC-N-0003 de v1, de 14 de Agosto de 2019 "Poliíica de seguridad y privacidad de la información"

ELABORÓ	REVISÓ	APROBÓ
Nombre: Lina Gabriela Ojeda Vargas **Cargo:** Analista Seguridad de Informacion **Fecha:** 29/Oct/2024	**Nombre:** Johanna María Becerra Cobos **Cargo:** Especialista Desarrollo Organizacional **Fecha:** 31/Oct/2024 **Nombre:** Lina Maria Tamayo Berrio **Cargo:** COORDINADOR GOBIERNO INSTITUCIONAL **Fecha:** 26/Nov/2024 **Nombre:** Carlos Andres Osorio Arboleda **Cargo:** Especialista Desarrollo Organizacional **Fecha:** 10/Dic/2024 **Nombre:** Katherine Fernanda Bulla Valencia **Cargo:** Coordinador Seguridad de la Información **Fecha:** 10/Dic/2024	**Nombre:** Yesid Sanchez Veloza **Cargo:** Director Riesgo Corporativo **Fecha:** 11/Dic/2024