Política General de Seguridad de la Información y Ciberseguridad

La Financiera de Desarrollo Territorial S.A. - FINDETER consciente de la importancia de proteger los activos de información que soportan la operación y continuidad del negocio frente a los riesgos que puedan afectar su seguridad, establece políticas, responsabilidades, procedimientos e instructivos, que representan la posición de la Junta Directiva y Equipo Directivo con respecto a la implementación, operación y sostenibilidad del Sistema de Gestión de Seguridad de la Información 'SGSI' y del Sistema de Administración de Riesgos de Seguridad de la Información y Ciberseguridad 'SARSICIB' de la entidad, en cumplimiento de la normatividad vigente.

FINDETER establece la Política General de Seguridad de la Información y Ciberseguridad, con el objetivo de:

- Cumplir con los principios de seguridad de la información y ciberseguridad.
- Minimizar los riesgos de seguridad de la información y ciberseguridad.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los trabajadores, contratistas, terceros y demás partes interesadas.
- Apoyar la innovación tecnológica.
- Implementar y mantener la sostenibilidad del sistema de administración de riesgos de seguridad de la información y ciberseguridad.
- Proteger los activos de información.
- Establecer las políticas específicas, procedimientos e instructivos en materia de seguridad de la información y ciberseguridad.
- Fortalecer la cultura de seguridad de la información y ciberseguridad en FINDETER.
- Gestionar la continuidad del negocio frente a incidentes de seguridad.
- Dar cumplimiento a las obligaciones legales vigentes relacionadas con seguridad de la información aplicables a FINDETER.

OBJETIVO

Asegurar que los servicios ofrecidos por FINDETER cumplan con los lineamientos de seguridad y que la gestión de los activos de información preserve la Calidad, Disponibilidad, Integridad y Confidencialidad de la misma. En relación con este último cuando a ello haya lugar de acuerdo con su naturaleza. Lo anterior a efectos de apoyar a la Alta Dirección en el cumplimiento de los objetivos estratégicos y misionales de la Entidad.

ALCANCE Y APLICABILIDAD

Esta política aplica a todos los trabajadores, proveedores, terceros y partes interesadas que tengan acceso o responsabilidad sobre la información objeto de tratamiento por parte de la entidad.

POLITICAS GENERALES DE SEGURIDAD Y CIBERSEGURIDAD DE LA INFORMACION

A continuación, se establecen las políticas generales que soportan el Sistema de Gestión de Seguridad de la Información de FINDETER:

1. Definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información alineado a las necesidades del negocio, a las directrices establecidas por la Junta Directiva y el Equipo Directivo, y a la metodología de gestión y tratamiento de riesgos de conformidad con la normatividad vigente y aplicable a FINDETER.
2. Las responsabilidades frente a la Seguridad de la Información y Ciberseguridad son definidas, compartidas, publicadas y aceptadas por cada uno de los trabajadores, proveedores o terceros.
3. Gestionar los riesgos que afectan la seguridad de la información y la ciberseguridad del negocio, adoptando los controles que resulten pertinentes para su tratamiento.
4. Proteger la información recolectada, generada, almacenada, procesada, resguardada o transmitida por los procesos del negocio, con el fin de minimizar impactos financieros, operativos y legales, causados por amenazadas que afecten su seguridad o por un uso incorrecto de esta, así como una potencial infracción al derecho al habeas data cuando se trate de datos de carácter personal.
5. Proteger las instalaciones físicas y la infraestructura tecnológica y de procesamiento de información que soporta la operación y continuidad del negocio.
6. FINDETER controla la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
7. Implementar mecanismos para el control de acceso a la información, a los sistemas de información y sus recursos de red de FINDETER, bajo los principios de mínimo privilegio y necesidades de acceso.
8. FINDETER establece que los mecanismos de autenticación (usuario y contraseña) a los recursos tecnológicos y sistemas de información de la entidad, son de uso obligatorio y de carácter personal e intransferible.

9. FINDETER aplica los procedimientos de administración de cuentas de usuarios en consideración al rol de cada usuario y su necesidad de acceso a la información para el desarrollo de sus funciones.
10. Propender que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
11. Establecer una mejora continua de su modelo de Seguridad de la Información y Ciberseguridad a través de una adecuada gestión de los eventos e incidentes de Seguridad de la Información y Ciberseguridad y las vulnerabilidades asociadas con la plataforma tecnológica.
12. Validar la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos o incidentes de Seguridad de la Información y Ciberseguridad.
13. Cumplir con las obligaciones legales, regulatorias y contractuales establecidas.
14. FINDETER exige a los trabajadores que sobre sus escritorios de trabajo no debe permanecer sin ningún tipo de protección información reservada o clasificada de la entidad, principalmente en caso de ausencia. Así como un adecuado manejo de dicha información.
15. FINDETER exige a sus trabajadores, proveedores y terceros autorizados bloquear sus estaciones de trabajo cada vez que se ausente de su puesto de trabajo.
16. FINDETER exige a los trabajadores, proveedores y terceros autorizados que brindan servicios a la entidad, firmar acuerdos de confidencialidad y aceptación de las políticas de seguridad.
17. Contar con políticas de seguridad específicas alineadas a la política General de Seguridad de la Información y Ciberseguridad.

El incumplimiento a la Política General de Seguridad de la Información y Ciberseguridad traerá consigo, las consecuencias legales que apliquen a la normativa de la entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad de la Información y Ciberseguridad se refiere.

La presente Política se entiende perfeccionada con la aprobación de la Junta Directiva de la entidad.

Aprobación inicial: Junta Directa 28 de mayo de 2019, Acta No. 351
Aprobación última modificación: Junta Directiva 30 de noviembre de 2021, Acta No. 390