PROCESO: SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

PL-SSI-01-V1

Bogotá, D. C. 30 de julio de 2019

CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN
0	17/12/2018	Creación del documento
1	30/07/2019	Ajustes por creación de la Dirección de Seguridad de la Información

TABLA DE CONTENIDO

1. INTRODUCCIÓN 4
2. OBJETIVO....4
3. ALCANCE 4
4. DESARROLLO DE LA POLITICA....4
5. ESTRATEGIA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD....5
5.1. PRINCIPIOS DE SEGURIDAD DE LA INFORMACION....5
5.2. ETAPAS DE SEGURIDAD DE LA INFORMACION Y CIBERSEGURIDAD 6
5.3. PILARES DE SEGURIDAD DE LA INFORMACION EN LA FDN 6
6. CULTURA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD 7
6.1. CAPACITACION 7

1. INTRODUCCIÓN

Dar a La Financiera de Desarrollo Nacional (en adelante la FDN) reconoce la importancia de identificar y proteger la información que recibe, produce, almacena, transmite y comparte por cualquier medio, incluyendo los medios digitales, para ello ha definido la siguiente Política de Seguridad de la Información y Ciberseguridad que se construye a través de los pilares de confidencialidad, integridad y disponibilidad de la información.

La tecnología, el uso de Internet y su continuo avance es de gran importancia para la evolución de la compañía y conseguir sus objetivos estratégicos, por lo que el correcto uso de la información y los recursos, así como la seguridad en internet y en el ciberespacio, deben ser gestionados, conocidos y cumplidos por todos sus colaboradores, proveedores, accionistas e interesados.

2. OBJETIVO

La Política de Seguridad de la Información y Ciberseguridad tienen como objetivo principal establecer lineamiento sobre el uso y protección de la información (en reposo o en tránsito), de los recursos de información, de la tecnología utilizada para su procesamiento y de los activos intangibles (como la reputación e imagen) por parte de los usuarios autorizados, administradores, proveedores, terceros e interesados, frente a amenazas internas o externas, deliberadas o accidentales, garantizando el cumplimiento de la confidencialidad, integridad y disponibilidad de la información de la FDN.

La FDN para el cumplimiento de dicho objetivo ha definido una estrategia de seguridad de la información y ciberseguridad compuesta por un modelo de gestión, los principios, las etapas y los pilares de Seguridad de la Información y Ciberseguridad.

3. ALCANCE

La Política de Seguridad de la Información y Ciberseguridad de la FDN aplica para todos los activos de información locales y en el ciberespacio, los colaboradores de la FDN, accionistas, colaboradores externos (proveedores y contratistas) e interesados que tengan acceso a la información y/o recursos de tecnología de la compañía.

4. DESARROLLO DE LA POLITICA

4.1. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDA

La FDN considera que la información es uno de sus activos más valiosos y entiende la importancia de un adecuado uso del mismo, por lo tanto se ha comprometido con la implementación, operación y mejora continua de un Sistema de Gestión de Seguridad de la Información y Ciberseguridad, buscando establecer un marco de confianza en el ejercicio de sus deberes con sus partes interesadas, enmarcado en el cumplimiento de las leyes y en concordancia con la misión, visión, estrategias y necesidades de la compañía.

Para la FDN la protección de la información es vital, por esta razón busca la disminución del impacto sobre sus activos generado por los riesgos identificados, con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades del negocio.

Todas las decisiones y acciones alrededor del Sistema de Gestión de Seguridad de la Información y Ciberseguridad están determinadas por las siguientes premisas:

1. Proteger los activos de Información.
2. Minimizar el riesgo en las funciones de la entidad.
3. Mantener la confianza de sus clientes, socios y empleados.
4. Cumplir las políticas específicas y sus procedimientos e instructivos.
5. Fortalecer la cultura en los funcionarios, terceros, aprendices, practicantes y clientes.
6. Garantizar la seguridad en la continuidad del negocio frente a incidentes.
7. Apoyar la innovación tecnológica.

Todo el personal, sea cual fuere su nivel jerárquico, son responsables de la implementación y cumplimiento de esta Políticas de Seguridad de la Información y Ciberseguridad dentro y fuera de sus dependencias, así como el cumplimiento por parte de su equipo de trabajo.

5. ESTRATEGIA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

La Política se desarrolla a través de una Estrategia de Seguridad de la Información y Ciberseguridad cuya base es el Modelo de Gestión de Seguridad de la Información (Norma ISO 27001/2013) y el desarrollo de tres elementos que se integran y relacionan entre sí, para lograr alcanzar dos objetivos: Consolidar la Cultura de seguridad de la Información y minimizar la exposición a pérdidas económicas y de daño reputacional en la FDN.

Estrategia de Seguridad de la Información

5.1. PRINCIPIOS DE SEGURIDAD DE LA INFORMACION

Confidencialidad: Es el término utilizado para asegurar que la información solo esta accesible para los funcionarios, entidades o procesos autorizados.

Integridad: Es el término utilizado para salvaguardar la exactitud y estado completo de los activos de información.

Disponibilidad: La información y los activos deben ser accesibles y utilizables por el personal autorizado cuando se requiera.

5.2. ETAPAS DE SEGURIDAD DE LA INFORMACION Y CIBERSEGURIDAD

La FDN, para garantizar una gestión efectiva en Seguridad de la Información y Ciberseguridad, ha definido implementar, ajustar, mantener y mejorar sus procesos con las siguientes etapas de gestión:

5.3. PILARES DE SEGURIDAD DE LA INFORMACION EN LA FDN

Los pilares de seguridad de la información son el tercer componente del Modelo de Seguridad de la Información y es la base que soporta el desarrollo de una estrategia, que conlleva a que el Sistema el Gestión de Seguridad de la Información de la FDN, permita la consolidación de una Cultura de Seguridad de la Información, minimice la exposición a pérdidas de dinero y de daño reputacional de la FDN, los pilares son:

La Gestión de Procesos: En este pilar se encuentra toda la gestión del sistema desde el proceso de Gestión de Seguridad de la información, compuesto por la Política de Seguridad de la Información, los manuales, procedimientos, lineamientos, instructivos, protocolos, formatos y en general toda la información que define y establece la administración de la seguridad de la información en la FDN.

Así mismo, se incluyen en este pilar el seguimiento y monitoreo de los riesgos de seguridad de la **información** y ciberseguridad, los indicadores de riesgo, los planes de mejoramiento a las diferentes auditorias que se realizan en la compañía, relacionadas con la seguridad de la Información y ciberseguridad.

La Gestión de Tecnología: Este pilar busca identificar las capacidades tecnológicas que en materia de seguridad de la información cuenta la FDN, determinar si son las adecuadas para la administración de los riesgos actuales o emergentes, así mismo, sugerir la adquisición de nuevos sistemas o herramientas de seguridad de la información y ciberseguridad, que permitan cerrar las brechas identificadas o que conlleven a mejorar las capacidades de la FDN, con base en los nuevos adelantos y tendencias tecnológicas disponibles en seguridad de la información y ciberseguridad.

La Gestión del Talento Humano: El talento humano es el principal activo de información, ya que bajo su responsabilidad están los demás activos de información de la FDN, es en este sentido que este pilar se desarrolla buscando llegar a las personas que integran la compañía, para lograr la consolidación de una cultura de seguridad de la información, por medio de actividades de capacitación, educación en buenas prácticas de seguridad, talleres de sensibilización, así mismo, busca medir el avance en el cumplimiento de los lineamiento de seguridad establecidos.

6. CULTURA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Todos los funcionarios de la entidad, sin importar el tipo de contrato, deben recibir formación y educación apropiada, actualizada y de manera periódica, alineada a su nivel de responsabilidad sobre las Políticas, proceso y controles de Seguridad de la Información y Ciberseguridad, además, deben participar activamente en todas las campañas de concientización sobre el tema que la entidad programe.

El responsable de la Seguridad de la Información y Ciberseguridad de la Entidad debe mantener contactos apropiados con las autoridades pertinentes y con grupos de interés especial externo a la entidad (CSIRT) y participar en los diferentes foros y conferencias profesionales de especialistas en el tema para mantenerse actualizado en el riesgo cibernético que pueda afectar a la entidad y en los controles efectivos para administrar dicho riesgo.

6.1. CAPACITACION

La conciencia y el entrenamiento en Seguridad de la Información y Ciberseguridad, incluyendo actualizaciones regulares son elementos importantes para contrarrestar ataques de ingeniería social.

El Responsable de Seguridad de la Información y Ciberseguridad elaborará y coordinará la ejecución los programas de capacitación y concientización para la FDN, con el fin de asegurar el desarrollo y ejecución del mismo. Estos planes serán específicos y deberán abarcar a la totalidad de los funcionarios de la compañía asegurando que se tengan entendidos los roles y responsabilidades de cada uno de ellos con la Seguridad, así como los controles que debe ser implementados y mantenidos.

El plan general de capacitación y concientización debe atender las necesidades de la compañía y dar solución a los riesgos detectados, para lo cual se deben realizar por lo menos una vez al año y siempre que se presenten alguno de los siguientes eventos:

1. Ingreso de empleados nuevos.
2. Cambios tecnológicos significativos
3. Desarrollo de nuevos productos o líneas de negocio

El contenido de las capacitaciones y la concientización del personal debe incluir:

1. Las últimas amenazas y formas de ataque, incluye ingeniería social
2. Como la información personal y corporativa puede ser robada y manipulada a través de ataques y cómo puede ser usada en contra de ellos
3. Qué información debe ser protegida y cómo protegerla de acuerdo con la Política de Seguridad de la Información y Ciberseguridad.
4. Cuándo y cómo reportar o escalar un evento sospechoso o aplicación maliciosos.
5. Las normas vigentes, así como las políticas y procedimientos adoptados por la Compañía y las mejores prácticas.

Toda campaña de concientización o programa de capacitación al personal de la compañía debe ser evaluado, para ello, todos los participantes deben suscribir un acta donde acepten y certifiquen su entendimiento del contenido, de las Políticas de Seguridad de la Información y Ciberseguridad, de su rol y responsabilidad con la misma y de los riesgos a las que está expuesto, El responsable de Seguridad debe realizar pruebas periódicas para determinar el nivel de conciencia y validar el entendimiento y cumplimiento de las mismas.