FONDECUN
FONDO DE DESARROLLO DE PROYECTOS DE CUNDINAMARCA

CUNDINAMARCA ¡REGIÓN Que Progresa!

RESOLUCIÓN No. 045 de 2020
(30 de diciembre de 2020)

POR LA CUAL SE ADOPTA LA POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL FONDO DE DESARROLLO DE PROYECTOS DE CUNDINAMARCA – FONDECÚN.

EL GERENTE GENERAL DEL FONDO DE DESARROLLO DE PROYECTOS DE CUNDINAMARCA - FONDECÚN – FONDECÚN

En uso de sus atribuciones legales y estatutarias, en especial las conferidas en el artículo 18, numeral 18 y el articulo 19 del Decreto Ordenanzal No. 431 de 2020 y

CONSIDERANDO

Que en el artículo 15 de la Constitución Política, consagra el derecho fundamental de las personas a conservar su intimidad personal y familiar, al buen nombre y a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellos en bancos de datos y en archivos de las entidades públicas y privadas.

Que la Ley 1273 de 2009 '*por medio del cual se modifica el Código Penal, crea un nuevo bien jurídico tutelado denominado "De la Protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones "TIC", entre otras disposiciones'* estableció como conductas punibles agresiones contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, atentados informáticos y otras infracciones.

Que el Decreto 1499 de 2011, el cual modifico el Decreto 1083 de 2015 (Decreto Único Reglamentarlo del Sector de Función Pública), adoptó el Modelo Integrado de Planeación y Gestión MIPG, definiendo en su artículo 2.2.22.3.2 como *"... un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atienden los planes de desarrollo y resuelvan necesidades y problemas de los ciudadanos, con integridad, y calidad de servicio".*

Que la ley Estatutaria 1581 de 2012 "*Por la cual se dictan disposiciones generales para la protección de datos personales"*, la cual constituye el marco general de la Protección de Datos Personales en Colombia reglamentando el ejercicio del derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías fundamentales plasmados en los artículos 17, 15 y 20 de la Constitución Política.

Que con el fin de facilitar la implementación y cumplimiento de la Ley 1581 de 2012 en la entidad se deben reglamentar aspectos relacionados con la autorización del Titular de información para el tratamiento de sus datos personales, las políticas de Tratamiento de los Responsables y Encargados,

el ejercicio de los derechos de los Titulares de información, las transferencias de datos personales y la responsabilidad demostrada frente al Tratamiento de datos personales.

Que la ley 1712 de 2014 *"Por medio de la cual se cree la Ley de Transparencia y del Derecho de Acceso a la Internación Púbica nacional y se dictan otras disposiciones"*, tiene como objetivo principal regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información.

Que el Decreto 1078 de 2015, modificado por decreto 1008 de 2018 *"Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de tecnologías de la información y las Comunicaciones*", en el artículo 2.2.9.1.1.3., incluye la seguridad de la información entre los principios de la Política de Gobierno Digital que debe ser aplicado por todas las entidades públicas; de igual manera, en el artículo 2.2.9.1.2.1. se establece que la Política de Gobierno Digital se desarrollara a través de componentes y habilitadores transversales, y respecto de estos últimos indica que son los elementos fundamentales de: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales los que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la política de Gobierno Digital.

Que las entidades que conforman la Administración Pública en los términos del artículo 39 de la Ley 489 de 1998, como el caso del Fondo de Desarrollo de Proyectos de Cundinamarca - Fondecún - Fondecún, están obligados a adoptar la Política de Gobierno Digital, siguiendo los lineamientos del Manual dé Gobierno digital, que define procedimientos, estándares y acciones a ejecutar por parte de las entidades.

Que la adopción de un Sistema de Gestión de Seguridad de la Información es una decisión estratégica para una organización. El establecimiento e implementación del sistema de gestión de la seguridad de la infamación de una entidad pública como es el Fondo de Desarrollo de Proyectos de Cundinamarca - Fondecún, está determinado por las necesidades y objetivos de la entidad, los requisitos de seguridad, los procesos organizaciones empleados, el tamaño y estructura de la organización.

Que conforme a la normatividad citada surge la necesidad de adoptar una política institucional de seguridad y privacidad de la información considerando el papel estratégico de las tecnologías de información y comunicaciones - TIC; así como las herramientas para respaldar las actividades ejecutadas en el Fondo de Desarrollo de Proyectos de Cundinamarca - Fondecún, incentivando la cultura de seguridad de la información a los usuarios, previniendo o solucionando posibles ataques informáticos, virus, robos, uso indebido de software o pérdidas de información.

Que, dado lo anterior se hace necesario adoptar mediante el presente acto administrativo, la Política General de Seguridad y Privacidad de la Información, implementación del Modelo de Seguridad y Privacidad de la Información (MSP), así como definir los lineamientos frente al uso y manejo de la información del Fondo de Desarrollo de Proyectos de Cundinamarca - Fondecún.

En mérito de lo anteriormente expuesto,

RESUELVE:

ARTÍCULO PRIMERO: ADOPTAR la Política General de Seguridad y Privacidad de la Información y la Política de Tratamiento de datos personales, del Fondo de Desarrollo de Proyectos de Cundinamarca - Fondecún, que hacen parte integral de la presente resolución, y las cuales fueron aprobadas por el comité Institucional de Gestión y Desempeño según acta nro. 4 de fecha 26 de octubre de 2020.

ARTÍCULO SEGUNDO: ORDENAR la divulgación de esta política a todas las dependencias del Fondo de Desarrollo de Proyectos de Cundinamarca y publicación en todos los medios de la entidad.

ARTÍCULO TERCERO. ORDENAR a la Subgerencia Administrativa y Financiera realizar el seguimiento anual al cumplimiento de la política.

ARTÍCULO CUARTO. La presente Resolución rige a partir de la fecha de su expedición, es de obligatorio conocimiento, aplicación y acato por parte de todos los servidores públicos y contratistas de la entidad y deroga todas las disposiciones que le sean contrarias. Contra la misma no procede recurso alguno.

Dado en Bogotá, D.C., a los treinta (30) días del mes de diciembre de 2020.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE

FRANCISCO JAVIER SALCEDO CAYCEDO
Gerente General

V°B°. German Medina Franco – Jefe de Oficina Asesora Jurídica
Revisó: Ángela Andrea Forero Mojica – Subgerente Administrativa y financiera
Zayra Daniela casas Lozano – Profesional Jurídico
Elaboro: Nelson Andrés Reina Cruz – Contratista

POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

FONDECUN
FONDO DE DESARROLLO DE PROYECTOS DE CUNDINAMARCA

POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

CONTENIDO

POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

INTRODUCCION

Las políticas y estándares de seguridad informática establecidas en el presente documento son la base fundamental para la protección de los activos informáticos y de toda la información de las Tecnologías de Información y Comunicaciones (TIC´s) en Fondecún.

Según el decreto 1078 de 2015, decreto único reglamentario del sector de tecnologías de la información y las comunicaciones, en la estrategia de gobierno en línea Artículo 2.2.9.1.2,1. Numeral 4, componente de seguridad y privacidad de la información comprende las acciones transversales a los demás componentes, tendientes a proteger la información y los sistemas de información, del acceso, uso, divulgación, interrupción o destrucción no autorizada, y el decreto 1499 decreto único reglamentario del sector Función Pública, en lo relacionado con el Sistema de Gestión el cual se articula con el sistema de seguridad de la información y más aún la seguridad digital, el Fondo de Desarrollo de Proyectos de Cundinamarca – Fondecún, de acuerdo con el Modelo de Seguridad y Protección de la Información, desarrolla e implementa la política general de seguridad de la información, adoptando las políticas necesarias para la protección de la información preservando con calidad, confiabilidad, privacidad, integridad, disponibilidad, y confidencialidad, buscando concientizar a todos los funcionarios y contratistas de la entidad de la importancia del cumplimiento de las normas establecidas y que se aplica a todos los recursos y servicios informáticos existentes en Fondecún.

Este documento describe los principios de seguridad que se deben tener en cuenta para el manejo de la información y de recursos tecnológicos de la entidad, es así como complemento a esta política encontraremos los lineamientos de seguridad donde se encontrara la gestión para usuario final, manejo de contraseñas, políticas de uso de equipos, políticas del uso de red, políticas de uso de cuentas de correo y protección contra virus informáticos.

Ya que para Fondecún, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática 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 de los diferentes grupos de interés identificados.

1. OBJETIVOS

1.1 Objetivo General

Crear directrices que orienten a los usuarios empleados y contratistas de Fondecún, para un uso responsable de los diferentes recursos y servicios informáticos y de telecomunicaciones, asegurando la información de Fondecún en la integridad, no repudio, disponibilidad, legalidad, y confidencialidad de la información.

1.2 OBJETIVOS ESPECIFICOS

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de Fondecún.
- Garantizar la continuidad del negocio frente a incidentes.
- Definir lineamientos para el desarrollo de trabajo remoto.
- Fondecún ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

2. ALCANCE

Aplica a todos los usuarios que hagan uso de recursos y servicios informáticos y de telecomunicaciones de la infraestructura de Fondecún**.** De acuerdo con lo anterior, esta política aplica a funcionarios, contratistas, terceros, aprendices, practicantes, proveedores y la ciudadanía en general.

3. Definiciones

- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

- **Autorización:** Consentimiento previo, expreso e informado para llevar a cabo el acceso, manipulación, divulgación o destrucción de la información.

- **Base de Datos:** Conjunto organizado de Datos que sea objeto de tratamiento.

- **Confidencial:** significa que la información no esté disponible o revelada a individuos, entidades o procesos no autorizados.

- **Confidencialidad:** Garantizar que la información es accesible sólo para aquellos autorizados a tener acceso.

- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- **Hardware:** Conjunto de los componentes físicos que componen la estructura de una computadora.

- **Información pública:** Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.

- **Internet:** Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación.

- **Password:** Una contraseña o password es una serie secreta de caracteres que permite a un usuario tener acceso a un archivo, a un ordenador, o a un programa.

- **Riesgo** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- **SGSI:** Sistema de Gestión de Seguridad de la Información

- **Seguridad de la información:** es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información y de los sistemas de información, busca la protección de acceso, de utilización, divulgación o destrucción no autorizada, manteniendo la confidencialidad, la disponibilidad e integridad de datos y de la misma.

- **Trazabilidad** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

- **Vulnerabilidad** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

4. Política General De Seguridad De La Información

EL Fondo de Desarrollo de Proyectos de Cundinamarca -Fondecún, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema

de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para Fondecún, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática 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 de los diferentes grupos de interés identificados.

Teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Establecer las políticas y procedimientos para la realización de trabajo remoto por parte de los funcionarios y contratistas.
- Fortalecer la cultura de seguridad de la información en los funcionarios, contratistas y clientes de Fondecún.
- Garantizar la continuidad del negocio frente a incidentes.

A continuación se establecen las 13 políticas de seguridad que soportan el SGSI de Fondecún:

1. El Fondo de Desarrollo de Proyectos de Cundinamarca ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.

2. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.

3. El Fondo de Desarrollo de Proyectos de Cundinamarca protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.

4. El Fondo de Desarrollo de Proyectos de Cundinamarca protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es

fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

5. El Fondo de Desarrollo de Proyectos de Cundinamarca protegerá la información de las amenazas originadas por parte del personal.

6. El Fondo de Desarrollo de Proyectos de Cundinamarca protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

7. El Fondo de Desarrollo de Proyectos de Cundinamarca controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

8. El Fondo de Desarrollo de Proyectos de Cundinamarca implementará control de acceso a la información, sistemas y recursos de red.

9. El Fondo de Desarrollo de Proyectos de Cundinamarca garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

10. El Fondo de Desarrollo de Proyectos de Cundinamarca garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

11. El Fondo de Desarrollo de Proyectos de Cundinamarca garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

12. El Fondo de Desarrollo de Proyectos de Cundinamarca dispondrá de los procesos adecuados para la realización de trabajo remoto Home Office.

13. El Fondo de Desarrollo de Proyectos de Cundinamarca garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

Las responsabilidades frente a la seguridad de la información del Fondecún son definidas, compartidas, publicadas y deberán ser aceptadas por cada uno de los funcionarios, contratistas o practicantes de Fondecún.

5. RESPONSABILIDADES

La definición de roles y responsabilidades definirá las tareas y procesos a cargo de cada uno de los miembros que conforman dentro de la entidad el modelo de seguridad, permitiendo el desarrollo adopción e implementación del modelo en la entidad. El organigrama y la definición de roles y responsabilidades se encuentran adicionalmente en el anexo 1 Organigrama.

5.1. Responsabilidades Directivos y Alta Gerencia

Liderar la implementación del modelo de seguridad de la información.
Definir el grupo responsable que implementara el modelo de seguridad de la información.

5.2. Responsabilidades Equipo De Gestión

- El equipo de gestión será el encargado de implementar el modelo de seguridad de la información, definiendo e implementando la política.

- Generar el cronograma de la implementación del Modelo de Seguridad y privacidad de la información.

- El equipo de gestión liderara y realizara seguimiento a todas las actividades necesarias para adoptar el Modelo de Seguridad de la Información.

- Planear las actividades necesarias para una adecuada administración y sostenibilidad del mismo.

- Establecer los requerimientos mínimos de seguridad que deberán cumplir los sistemas de información a desarrollar, actualizar o adquirir dentro de la entidad.

- Planear, implementar y hacer seguimiento a las tareas, fechas, costos y plan de trabajo de los objetivos específicos del cronograma definido.

- Realizar un seguimiento permanente a la ejecución de los planes de trabajo, monitoreando los riesgos del proyecto para darle solución oportuna y escalar al Comité de seguridad en caso de ser necesario.

- Monitorear el estado del proyecto en términos de calidad de los productos, tiempo y los costos.

- Liderar la programación de reuniones de seguimiento y velar por la actualización de los indicadores de gestión del proyecto.

5.3. Responsabilidades área de tecnologías de la información

- Instaurar, configurar y publicar la política de seguridad de la información y de todos los servicios tecnológicos a todos los usuarios en la entidad.

- Revisar el cumplimiento de la política de seguridad de la información.

- Salvaguardar la información que reposa en los diferentes sistemas de información, bases de datos y aplicativos de la entidad.

- Evaluar todos los servicios tecnológicos en busca de posibles vulnerabilidades de seguridad de la información.

- Evaluar y realizar junto con el equipo de gestión las correcciones de la política de seguridad Continuamente.

- Proporcionar medidas de seguridad físicas, lógicas y procedimentales para la protección de la información digital de la entidad.

- Analizar, aplicar y mantener los controles de seguridad implementados para asegurar los datos e información gestionados en la Institución.

6. Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

7. ENTRADA EN VIGENCIA

La presente Política de Seguridad Informática entra en vigencia a partir de la fecha de aprobación por parte del comité de gestión de Fondecún.

8. REVISIÓN O ACTUALIZACIÓN DE LA POLÍTICA

La presente política deberá ser revisada con el fin de mantenerla actualizada con los requerimientos de la entidad y de ley una vez cada doce meses como mínimo.

LINEAMIENTOS DE SEGURIDAD INFORMÁTICA
FONDO DE DESARROLLO DE PROYECTOS DE CUNDINAMARCA

FONDECUN
FONDO DE DESARROLLO DE PROYECTOS DE CUNDINAMARCA

CONTENIDO

Contenido

LINEAMIENTOS POLÍTICA DE SEGURIDAD INFORMÁTICA

INTRODUCCIÓN

El Fondo de Desarrollo de Proyectos de Cundinamarca – Fondecún en el presente documento "Lineamientos políticas de seguridad informática" describe las reglas a desarrollar por cada funcionario y contratista en aras de gestionar toda información de la entidad, de acuerdo a la política general de seguridad y privacidad de la información.

Permitiendo la confidencialidad, integridad, disponibilidad de la misma, y dando cumplimiento a las buenas prácticas de seguridad de la información enunciadas en la norma técnica ISO 27001 del 2013 y el modelo de seguridad y privacidad de la información de la estrategia de Gobierno En Línea.

1. OBJETIVO

Definir las prácticas de seguridad que permitan el adecuado manejo de la información dentro del Fondo de Desarrollo de Proyectos de Cundinamarca – Fondecún, cumpliendo con el modelo de seguridad y privacidad de la información.

2. ALCANCE

Las siguientes políticas de seguridad deberá ser aplica por todos los usuarios que hagan uso de recursos y servicios informáticos y de telecomunicaciones de la infraestructura de Fondecún**.** De acuerdo con lo anterior, esta política aplica a funcionarios, contratistas, terceros, aprendices, practicantes, proveedores y la ciudadanía en general.

3. Definiciones

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC
27000).

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Autorización: Consentimiento previo, expreso e informado para llevar a cabo el acceso, manipulación, divulgación o destrucción de la información.

Base de Datos: Conjunto organizado de Datos que sea objeto de tratamiento.

ERP(Sistema de Planificación de Recursos Empresariales): es un sistema el cual permite automatizar y administrar los distintos procesos empresariales de distintas áreas: finanzas, recursos humanos, operaciones, entre otras.

Confidencial: significa que la información no esté disponible o revelada a individuos, entidades o procesos no autorizados.

Confidencialidad: Garantizar que la información es accesible sólo para aquellos autorizados a tener acceso.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Hardware: Conjunto de los componentes físicos que componen la estructura de una computadora.

Información pública: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.

Internet: Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación.

Password: Una contraseña o password es una serie secreta de caracteres que permite a un usuario tener acceso a un archivo, a un ordenador, o a un programa.

Riesgo Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

SGSI: Sistema de Gestión de Seguridad de la Información

Seguridad de la información: es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información y de los sistemas de información, busca la protección de acceso, de utilización, divulgación o destrucción no autorizada, manteniendo la confidencialidad, la disponibilidad e integridad de datos y de la misma.

Trazabilidad Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

Vulnerabilidad Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

4. PRINCIPIOS GENERALES

- Las políticas de seguridad de la información se basan en proteger y resguardar los activos y toda la información generada por Fondecún como los recursos y servicios.
- El personal que tenga un vínculo laboral o contractual con Fondecún debe recibir en su proceso de inducción y reinducción la política de seguridad de la información con las directrices a seguir con el fin de que se cumplan a cabalidad para garantizar la confidencialidad, integridad y disponibilidad de la información.
- Concientizar a todos los funcionarios, contratistas o practicantes sobre los riesgos asociados con el uso de los recursos tecnológicos de Fondecún y en especial del trato de la información.
- El personal que tenga un vínculo laboral o contractual con Fondecún debe aceptar las condiciones de confidencialidad y de uso adecuado de los activos informáticos y de la información.
- Se consideran violaciones graves el robo, daño, divulgación de información reservada o confidencial de la entidad, o el que se le declare culpable de un delito informático.
- Los usuarios deben hacer buen uso a los recursos compartidos como teléfonos, impresoras, Scanner y se debe realizar ahorro de insumos como papel, tintas y consumos telefónicos.
- Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir las Políticas y Estándares de Seguridad Informática planteados en este documento.
- El área de tecnología deberá realizar y presentar un análisis del estado de los equipos y dispositivos de computo de la entidad con el fin de identificar equipos y dispositivos de comunicación que deban ser actualizados o en su defecto ser remplazados por equipos de última generación, con el fin de prestar a cada funcionario y servidor de Fondecún las mejores herramientas computacionales para el desarrollo de su labor.

5. DEFINICIÓN DE LAS POLÍTICAS DE SEGURIDAD

Es fundamental para el modelo de seguridad y protección de la información y para el correcto desarrollo de las actividades de Fondecún, que se cumpla con las siguientes normas.

5.1. POLÍTICAS DE USUARIO

5.1.1. Para todo nuevo funcionario se deberá realizar la verificación de:

- Los antecedentes de acuerdo con las leyes y normas existentes.
- Verificar la información de las hojas de vida como referencias personales, referencias laborales, información de estudios.

5.1.2. Todo funcionario que ingrese a la entidad deberá firmar en calidad de aceptación un acuerdo de seguridad y confidencialidad.

5.1.3. Todo nuevo usuario que ingrese a la entidad debe ser reportado por la oficina de recursos humanos, jurídica o por el jefe inmediato al área de informática y comunicaciones para la creación del correspondiente usuario de red, creación cuenta de correo institucional, asignación de permisos informáticos, espacio de almacenamiento en red y asignación de equipo de cómputo del cual se hará responsable sobre su uso y cuidado.

5.1.4. Se debe solicitar la creación de credenciales (usuario y contraseña) para el acceso tanto a recursos tecnológicos, como a los sistemas de información, por medio del formato de solicitud "GI-F-06 Solicitud para el registro de usuarios", indicando la vigencia y el área de Funcionamiento, el cual deberá ser diligenciado por el jefe inmediato, el área de recursos humanos o gestión contractual y ser entregado al área de tecnología debidamente firmado, este procedimiento aplica para adiciones y/o prorrogas.

5.1.5. Las credenciales de acceso son responsabilidad exclusiva del funcionario o contratista, de uso personal e intransferible y es el único responsable por las actividades quesean realizadas con dicho identificador.

5.1.6. Los perfiles de usuario, credenciales de acceso se deben configurar de acuerdo al tiempo de duración del contrato en caso de los contratistas y para los funcionarios de planta se deben configurar para que nunca expire.

5.1.7. 6.1.4. El equipo de cómputo asignado a cada usuario, deberá ser para uso exclusivo de las funciones de los funcionarios o servidores la entidad.

5.1.8. Todo funcionario de la entidad debe tener activo el usuario con su correspondiente Password (ver políticas de usuario y contraseña) y el correo institucional por parte del área de informática y comunicaciones.

5.1.9. Toda vez que un funcionario se ausente de su puesto debe dejar la estación de trabajo bloqueada para evitar daño, manejo inadecuado del equipo o pérdida de la información.

5.1.10. Todo funcionario o contratista será responsable del manejo de la información y su adecuado almacenamiento, para lo cual debe de guardar toda información en la unidad de red creada y asignada para este proceso. Estará prohibido que se guarde información en los escritorios de trabajo del computador o en cualquier otra ubicación de los equipo de cómputo, al igual que tampoco se debe almacenar o guardar información personal en esta unidades de red, esto con el fin de realizar un adecuado proceso de respaldo o backups de la información.

5.1.11. En cualquier caso el usuario a cargo del equipo informático y/o de telecomunicaciones se hará responsable por las medidas disciplinarias y legales que conlleve el no cumplimiento de las Políticas establecidas en este documento.

5.1.12. Los usuarios que no tengan contrato vigente, automáticamente se restringirá el ingreso al sistema, en el caso que se le renueve el contrato, el área Jurídica o el supervisor; Subgerente Técnico y/o Subgerente Administrativo, enviara un correo al personal encargado del área tecnológica para habilitar nuevamente el usuario en la red.

5.1.13. Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.

5.1.14. Los usuarios deberán usar el sistema de mesa de ayuda en la medida que requieran soporte técnico o asesoría en uso de herramientas tecnológicas o fallas en el sistema tanto de Hardware como de Software.

5.1.15. Todos los funcionarios y contratistas deberán asegurarse de dejar cerrada totalmente su sesión de trabajo para evitar el uso de su identidad, cuando se retire del equipo en que se encuentre laborando.

5.1.16. El encargado del área de tecnología será el único responsable de ejecutar los movimientos de altas, bajas o cambios de perfil de los usuarios.

5.1.17. Cuando un funcionario o contratista se retire de la entidad esto deberá ser informado por el jefe inmediato, el área de recursos humanos o el área gestión contractual al área de sistemas mediante el sistema de mesa de ayuda o por correo electrónico el formato “GI - F- 07 Solicitud para el retiro de usuarios” con el fin de eliminar las respectivas credenciales de acceso a los recursos tecnológicos y los sistemas de información. Así mismo el funcionario o contratista en proceso de retiro debe entregar el correspondiente equipo de cómputo asignado en correcto estado y funcionamiento lo cual deberá ser verificado por el área de tecnología.

5.2. POLÍTICAS DE DEFINICIÓN DE USUARIO Y CONTRASEÑA

Con el fin de que cada funcionario pueda hacer uso de los recursos tecnológicos y a la información de la entidad se les asignara un usuario y contraseña, garantizando seguridad de acceso tanto a equipos como a información con las siguientes características.

5.2.1. Todo usuario debe poseer un identificador con password único para tener acceso y poder usar los recursos informáticos.

5.2.2. La asignación de identificadores a los diferentes funcionarios, contratistas, así como su desactivación de los sistemas se harán de acuerdo a los procedimientos establecidos y según sea solicitado por los directores, jefes de oficina o por los grupos de Talento Humano y Gestión Contractual.

5.2.3. Las cuentas de usuarios deben ser configuradas para que exijan cambio de clave cada 30 días, con el objetivo de garantizar mayor seguridad en el uso de los recursos y acceso a información con diferentes niveles de confidencialidad.

5.2.4. Toda nueva contraseña establecida por los usuarios debe tener una longitud mínima de 10 dígitos y cumplir con las características de complejidad las cuales son:

- Debe tener un longitud de mínimo 10 caracteres
- Caracteres en mayúsculas
- Caracteres en minúsculas
- Números (0,1,2,3,4,5,6,7,8,9)
- Caracteres especiales (*,%,$,&,!,+,/, etc).

5.2.5. En el caso de que a un usuario se le olvide el password o que se le bloquee la cuenta de red, el funcionario podrá solicitar al área tecnología el restablecimiento de la misma por mesa de ayuda https://newaccount1615568022446.freshdesk.com/support/home y por correo electrónico a soporte.sistemas@fondecun.gov.co.

5.2.6. El usuario y contraseña para acceso a los sistemas de información ERP de la entidad, se deben solicitar por medio del formato de solicitud de creación de usuarios para el sistema indicando los módulos a los que tendrá acceso y el tipo de permiso para cada módulo, indicando vigencia, el cual deberá ser diligenciado por el jefe inmediato, el área de recursos humanos o gestión contractual.

5.2.7. Está prohibido que las contraseñas se dejen de forma legible en cualquier medio impreso dejándolas en un lugar público donde personas no autorizadas puedan hacer uso de ellas.

5.2.8. Las contraseñas de ninguna manera podrán ser transmitidas mediante servicios de mensajería electrónica instantánea ni vía telefónica, igualmente se debe evitar utilizar la misma contraseña para el acceso a equipos, sistemas de información y correos.

5.2.9. El usuario podrá realizar el cambio de clave del correo institucional desde el portal web de la entidad ingresando al servicio de correo electrónico institucional, en caso que se le olvide la contraseña podrá solicitar al área de tecnología el restablecimiento de la misma mediante el aplicativo de mesa de ayuda o por correo electrónico personal.

5.2.10. Está prohibido intentar acceder de forma no autorizada con otro usuario y clave diferente a la personal en cualquier sistema de información o plataforma tecnológica.

5.2.12. Está prohibido para los usuarios proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica de Fondecún, a acepción que se tenga el visto y/o la autorización del Gerente General.

5.3. POLÍTICAS SOBRE EL MANEJO DE LA INFORMACIÓN

Con el fin de garantizar el adecuado manejo de la información por cada uno de los funcionarios y colaboradores de Fondecún se define.

5.3.1. El Fondo de Desarrollo de Proyectos de Cundinamarca, es el dueño de los activos de información y los funcionarios, contratistas y terceros que estén autorizados son los encargados administradores de estos activos.

5.3.2. Cada director de área o jefe de oficina será el responsable de la información que genere o manipule el área a su cargo y como tal será el encargado de aprobar o denegar los permisos de quienes pueden tener acceso a su información.

5.3.3. Cada responsable de los activos de información generara un inventario de dichos activos, asumiendo las indicaciones de las guías para tal fin.

5.3.4. Toda información digital que se genere o que se manipule dentro de Fondecún y que tenga relación con la entidad debe ser resguardada en los servidores destinados para el almacenamiento de la información.

5.3.5. Es obligatorio el uso de las carpetas de red, evitando lo máximo posible el uso de almacenamiento en unidades locales del sistema para almacenar la información crítica del negocio, para lo cual cada usuario debe tener configurado en su equipo el acceso a la red, que le direccione a la carpeta de red Fondecún en el servidor de almacenamiento, en la cual deberá guardar toda la información y sobre la que se realizara copias de respaldo.

5.3.6. La información digital que se genere por los usuarios de la entidad debe cumplir con los principios fundamentales de Privacidad, Integridad, Disponibilidad, Control de Acceso y Auditabilidad.

5.3.7. La información digital debe contar con niveles de protección adecuada según su nivel de sensibilidad de tal manera que permita el acceso y uso únicamente a los usuarios autorizados.

5.3.8. El material impreso o digitalizado que sea procesado en Fondecún no podrá ser retirado de la entidad, sin previa autorización de Gerente General, Subgerente Administrativo, Gerente de convenio o supervisor del contrato.

5.3.9. Es obligación la revisión de información en las unidades de red con el fin de auditar a los usuarios que almacenan información no permitida o redundante en la red. El uso de unidades de red se encuentra limitado exclusivamente a información corporativa.

5.3.10. En caso de pérdida, daño, accesos no autorizados, o mal uso de la información confidencial de la compañía (digital o impresa) el responsable del proceso debe informar inmediatamente a la Subgerencia Administrativa, detallando lo ocurrido y las implicaciones que esto puede tener sobre la operación del negocio.

5.3.11. Se deberá realizar el backup a la información de los usuarios que se retiren de la entidad, incluyendo correos electrónicos. Los usuarios que requieran estos Backup deberán solicitar al Subgerente Administrativo y/o Subgerente Técnico autorización quien por medio de correo electrónico al área de tecnología autorizara el acceso al Backup a consultar, especificando o estableciendo el tiempo de consulta de la información solicitada, en cualquier caso los permisos otorgados sobre la información a consultar serán exclusivamente de lectura.

5.3.12. Se debe realizar copias de seguridad del correo electrónico de cada usuario al retirarse de la entidad, para lo cual si es necesario cada usuario informara la clave de la cuenta de correo y si utiliza equipo personal debe permitir el acceso al mismo para realizar el backup del correo.

5.3.13. La entidad deberá contar adicionalmente con un respaldo de la información en un sitio externo a las oficinas de la entidad, en caso de desastres naturales como terremotos, incendios, inundaciones que involucren el daño total o parcial de las instalaciones de Fondecún. Para tal caso se deberá garantizar el correcto almacenamiento con confiabilidad, integridad, disponibilidad, y confidencialidad, en cualquier momento. Ver también políticas de back up.

5.3.14. Está prohibido el uso de memorias USB y unidades de CD's, solo personal autorizado podrá tener acceso a estos dispositivos con el fin de cumplir procesos netamente del área, evitar las infecciones por virus informáticos y el robo de información. Para lo cual cada jefe de dependencia debe reportar al área de tecnología el listado de funcionarios a su cargo que manejaran estos tipos de dispositivos, indicando el tiempo de uso, tipo de dispositivo al que tiene acceso (USB, CD-ROM), el tipo de acceso (lectura, escritura).

5.3.15. El funcionario que tenga autorización para utilizar dispositivos externos (USB, CD- ROM) será el responsable de la información que en este se maneje y del buen uso de estos.

5.3.16. Cada funcionario o contratista autorizara, restringirá y delimitara a los demás usuarios de la entidad el acceso a la información, de acuerdo a los roles y responsabilidades de los diferentes funcionarios, contratistas o practicantes que por sus actividades requieran acceder a consultar, crear o modificar parte o la totalidad de la información.

5.3.17. Cada funcionario, contratista debe asegurarse que la papelería destinada a reciclaje bien sea para ser reutilizada o para ser retirada de la entidad, no contenga información sensible para el bienestar de la entidad o de cualquier funcionario o contratista, información como números de cedula, números de nit, información bancaria, datos de localización (direcciones), correos personales, para lo cual cualquier documento que tenga este tipo información debe ser destruido y no llevado a reutilizar, evitando la fuga de información.

5.4. POLÍTICAS PARA LA SEGURIDAD FÍSICA

Se pretende enfocar las medidas mínimas para fortalecer adecuadamente el acceso físico a los dispositivos informáticos e infraestructura de red y servicios de comunicaciones de la entidad.

5.4.1. Los equipos de cómputo (computadores de escritorio y portátiles) deben ser asegurados con guaya para evitar hurtos, las claves o llaves de las mismas deben ser manejadas exclusivamente por el área de tecnología.

5.4.2. Todo usuario deberá reportar de forma inmediata al área de tecnología cuando se presenten riesgos sobre la infraestructura tecnológica de Fondecún, como choques eléctricos, caídas de líquidos sobre cualquier dispositivo, golpes, etc.

5.4.3. Los servidores y dispositivos de conexión de red y comunicaciones se deben alojar en un cuarto de datos aislado a los usuarios con puerta, en el que se pueda restringir y controlar el ingreso de

personal, este cuarto debe contar condiciones ambientales adecuadas para evitar daño a los equipos y poseer un nivel de seguridad física mínimo.

5.4.4. Solo el personal del área de Tecnología podrá manipular e instalar equipos de comunicaciones, estaciones, laptops, periféricos y servidores; Los usuarios no deben mover o reubicar, instalar o desinstalar dispositivos, en caso de ser necesario se debe solicitar al área de tecnología. Equipos diferentes a los de Fondecún, como tabletas, celulares, portátiles, etc, no deben ser conectados a la red local de la entidad.

5.4.5. Si los funcionarios o contratistas necesitan utilizar equipos propios diferentes a los proporcionados por la institución, deben solicitar la autorización, verificación y registro de la Oficina de Sistemas y cumplir con los controles mínimos de seguridad establecidos como tener instalado antivirus licenciado y actualizaciones parches de seguridad para poder conectarse a la red.

5.4.6. El cableado estructurado o cualquier elemento físico de red solo puede ser manipulado por personal del área de Tecnología o un tercero que sea autorizado únicamente por esta misma área.

5.4.7. Está prohibido el acceso a usuarios de Fondecún o cualquier otra persona sin previa autorización del Ingeniero del área de Tecnología a centros de cómputo y Servidores, solo está autorizado el acceso a personal del área de Tecnología. Cualquier persona que ingrese a centros de cómputo deberá tener acompañamiento por personal del área de tecnología y así proteger la información y los bienes informáticos.

5.4.8. Todo personal sin excepción que ingrese al centro de cómputo de la entidad debe registrarse en el formato diseñado para tal caso, en el que se dejara fecha, hora ingreso, nombre, motivo, autorizado por, fecha de salida y firma.

5.4.9. Los equipos de cómputo que funcionan como servidores deben estar bajo la responsabilidad de personal con habilidad y experiencia para realizar las tareas de administración.

5.4.10. La administración de los servidores podrá realizarse por parte del personal interno o a través de la contratación con terceros.

5.4.11. Es responsabilidad del usuario o funcionario evitar en todo momento la fuga de información, que se encuentre almacenada en los equipos de cómputo que tenga asignados.

5.4.12. El usuario que tenga a su cargo un equipo de cómputo, periférico, cámara, video proyector, etc, será el responsable directo de su uso y cuidado, respondiendo por este bien de acuerdo a lo estipulado para los casos de robo o pérdida del mismo. En caso de daño, desperfecto por maltrato, descuido o negligencia, se realizara reporte de incumplimiento de políticas de seguridad al usuario que tenga a cargo el dispositivo.

5.4.13. Los funcionarios o contratistas que necesiten retirar de las instalaciones de la entidad un dispositivo de cómputo propio de la misma requerirán contar con la autorización y formato de retiro de equipos de cómputo debidamente diligenciado y firmado por el jefe del área a la cual pertenece

(Subgerencia Administrativa y Financiera, Subgerencia Técnica, Oficina Asesora Jurídica o Gerencia General).

5.4.14. Se debe evitar colocar objetos como carpetas, folios, hojas y bebidas encima del equipo cómputo o tapar las salidas de ventilación del monitor, CPU y portatiles.

5.4.15. Mientras se opera el equipo de cómputo, no se debe consumir alimentos o ingerir líquidos.

5.4.16. El usuario debe asegurarse que los cables de conexión del equipo de cómputo, eléctrico y de datos no sean pisados al colocar otros objetos, en caso de que no se cumpla el usuario debe solicitar la reubicación de cables con el personal del área de tecnología.

5.4.17. Solo el personal del área de tecnología está autorizado para abrir o destapar los diferentes equipos de cómputo, realizar los mantenimientos correctivos o preventivos o por parte de un tercero con el que se suscriba contrato para tal fin.

5.4.18. En caso de robo o extravió de algún elemento de computo se debe notificar inmediatamente al área de inventarios y a la subgerencia administrativa, para tomar las medidas correspondientes.

5.4.19. Cuando se vaya a realizar un mantenimiento en algunos de los equipos del Centro de Cómputo restringido, se debe dar aviso con anticipación a los usuarios para evitar traumatismos.

5.4.20. Se debe garantizar los equipos de protección contra incendios, inundaciones y fluctuaciones eléctricas (UPS).

5.5. POLÍTICAS PARA EL USO DE SOFTWARE

Partiendo de la importancia de cumplir con las normas legales sobre los derechos de autor, derechos de uso y divulgación e instalación de software se presentan algunas normas prioritarias para el cumplimiento de estas.

5.5.1. En los equipos de cómputo que pertenezcan a Fondecún, solo se deberá instalar y usar software que tenga las respectivas licencias, acuerdos de uso o que sean en su totalidad software libre, evitando al máximo la instalación de software demo o de prueba.

5.5.2. Solo el personal del área de tecnología está autorizado para la instalación desinstalación, actualización y administración de software en los equipos que pertenecen a la entidad.

5.5.3. Todas las Licencias del software adquiridas por Fondecún a través de compra, donación o cesión son propiedad y de uso exclusivo de la entidad.

5.5.4. El software adquirido e instalado en los equipos de la entidad debe ser usado exclusivamente para uso relacionado con las actividades propias del ejercicio de Fondecún.

5.5.5. En el caso de hallar software ilegal instalado en los equipos de la entidad, se hará responsable al usuario que tenga el equipo a cargo para toda responsabilidad civil, económica y penal cuando se le haya comprobado su falta.

5.5.6. El control, manejo de las licencias y el inventario de los Medios, paquete de CD´s será responsabilidad del área de tecnología.

5.5.7. El área de tecnología se hará responsable del inventario físico de cada equipo con sus respectivas licencias del software instalado.

5.5.8. Si se requiere la instalación de algún software debe solicitarlo por escrito o por correo electrónico al área de tecnología, indicando la justificación, equipo donde se deberá realizar dicha instalación y contar con la autorización de la subgerencia administrativa o subgerencia técnica.

5.5.9. El software y aplicaciones que están permitidas varían de acuerdo al área y las necesidades de cada usuario, pero en general los únicos programas y aplicaciones permitidos según la cantidad de licencias adquiridas son: Microsoft Word, Excel, Power Point, Outlook, Adobe Pdf, Visores de Autocad, WinRAR, SI-APITAL.

5.5.10. El área de tecnología deberá llevar un inventario de las licencias de software de la entidad en la que se relacione como mínimo el tipo de software, la clave de licencia y el equipo en el que fue instalada.

5.6. POLÍTICAS PARA EL USO DE CORREOS ELECTRÓNICOS

Los correos electrónicos como uno de los servicios de comunicación más importantes y de mayor uso dentro de la entidad para el intercambio de información, es de vital importancia garantizar el funcionamiento y adecuado uso, por y para cada usuario.

5.6.1. Todo funcionario o contratista de Fondecún debe contar con un correo electrónico institucional, el cual debe ser asignado dentro de los primeros 3 días posteriores a la firma del contrato, para este proceso el jefe inmediato, el área de recursos humanos o de gestión contractual debe solicitar por medio del canal de mesa de ayuda o por correo electrónico al área de tecnología la apertura de la cuenta de correo electrónico, anexando el formato de solicitud especificando el tipo de vínculo con la entidad (funcionario-contratista) y la fecha de terminación del contrato, la asignación del correo electrónico esta sujeta a la disponibilidad de cuentas existentes.

5.6.2. El uso de las cuentas de correo electrónico institucionales asignadas a cada usuario es y deben ser de uso estrictamente laboral, no se debe utilizar para registrarse a páginas para uso personal como redes sociales, eventos, almacenes de cadena, etc, el usuario debe tomar responsabilidad y compromiso para su uso.

5.6.3. Todos los usuarios deben utilizar para el manejo de las cuentas de correo electrónico el cliente Microsoft Outlook, el cual esta licenciada por lo entidad, cuando se asigne la cuenta de correo se configurar en el equipo de cómputo asignado, igualmente todos los funcionarios y contratistas tendrán la posibilidad de tener acceso al correo electrónico institucional externamente a la entidad través del sitio www.fodecun.gov.co.

5.6.4. Se debe realizar back up del correo electrónico y crear un nuevo PST cuando este supere los dos (2) Gigas de tamaño con el fin de evitar pérdidas de correo y daños en los mismos.

5.6.5. Todos los usuarios deben manejar los mensajes de correo electrónico entrantes y salientes y archivos adjuntos como información propiedad de Fondecún y destinada exclusivamente al ejercicio estricto de sus funciones y responsabilidades.

5.6.6. Queda prohibido falsificar, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.

5.6.7. Los usuarios no deben utilizar cuentas de correos electrónicos asignadas a otros usuarios. En caso de ser necesario la utilización o lectura de correos de otra persona ya sea porque el propietario de la cuenta se encuentre de vacaciones, permisos, incapacitado o porque es un funcionario retirado de la entidad, se debe contar con autorización del funcionario ausente o con autorización del jefe de área por escrito o por correo al área de tecnología.

5.6.8. Para el re-direccionamiento de correos a otra cuenta se debe enviar autorización por el aplicativo de mesa de ayuda o por correo electrónico al área de tecnología, evitando el re direccionamiento a una cuenta de correo externa para efectos de resguardar la información de la entidad.

5.6.9. Fondecún podrá revisar los buzones de correo electrónico cuando lo estime conveniente para verificar el cumplimiento de la política o por otras razones acordes a los intereses legítimos de la institución enviando autorización por escrito o por correo al área de tecnología por parte de la gerencia general.

5.6.10. A todo correo electrónico entrante y saliente se realizara análisis para filtrar en la media de lo posible el tráfico de correo electrónico no deseable (SPAM).

5.6.11. Cuando un correo electrónico entrante sea sospechoso de spam, se enviara un mensaje de advertencia en el asunto del correo al destinatario avisándole, el usuario será quien identifique si proviene de una fuente segura para proceder a abrirlo, en caso contrario el usuario deberá borrar del buzón de correo el mensaje sin acceder al mismo.

5.6.12. Fondecún no se hace responsable del uso inapropiado que los usuarios hagan de sus cuentas de correo electrónico.

5.6.13. Los funcionarios y contratistas podrán únicamente hacer uso del correo institucional durante la vigencia del respectivo contrato.

5.6.14. El uso de listas de correos y reenvíos masivos serán únicamente para comunicaciones estrictamente laborales con información de interés general y formal.

5.6.15. Todo correo electrónico tiene la misma validez que un documento físico.

5.6.16. Toda cuenta de correo electrónico debe tener configurada la firma del funcionario o contratista dueño de cada cuenta, para que sea utilizada en todo correo electrónico enviado, en la que debe contener la siguiente información, es responsabilidad del usuario su configuración y/o inclusión:

- Nombre del funcionario o contratista
- Cargo y/o ocupación.
- Oficina o área a la que pertenece.
- Dirección y teléfono de la entidad
- Logo de la entidad.

5.6.17. Las cuentas de correo electrónico otorgadas a los funcionarios o contratistas serán desactivadas tan pronto su vinculación con la entidad se termine, para lo que los jefes de área, el jefe inmediato, el área de recursos humanos o de gestión contractual deberán informar al área de tecnología.

5.7. POLÍTICAS PARA LA GENERACIÓN DE BACKUPS

Como medidas de contingencia para aseguramiento y restablecimiento de la información es indispensable definir las políticas de generación de backups que permitan identificar el tipo de backup, procesos de restauración y los responsables de dicha actividad.

5.7.1. La creación de copias de respaldo es una herramienta muy útil como medida de seguridad informática en caso de daño, perdida, borrado de la información o de los dispositivos de almacenamiento, por lo cual se debe realizar copias de respaldo o Backups periódicamente de toda la información digital de la entidad el área de tecnología debe programar las tares necesarias.

5.7.2. El área de tecnología del Fondo de Desarrollo de Proyectos de Cundinamarca será responsable generar y desarrollar las tareas necesarias para realizar los backups internos de la información, para lo cual la entidad cuenta con dos NAS (Network access server), en los que se debe almacenar el backup, asegurándose de realizar este proceso por lo menos una vez por semana en horarios que no generen traumatismos a los usuarios.

5.7.3. Las copias de seguridad se deben realizar en las NAS dispositivo de almacenamiento externo de forma organizada para garantizar su pronta recuperación.

5.7.4. Las copias de seguridad o Backups se deben realizar al menos una vez a la semana y el último día hábil del mes, registrando el cumplimiento de esta actividad en un formato de bitácora adecuado.

5.7.5. El área de tecnología con supervisión de la gerencia general y la subgerencia administrativa y financiera deberá gestionar la contratación e implementación de los servicios y procedimientos necesarios para realizar backups de la información de la entidad en un data center externo o en la web, como medida de mitigación de riesgos en caso de desastres naturales como terremotos, incendios, inundaciones que involucren el daño total o parcial de los servidores internos o de las instalaciones de la entidad, "Fondecún".

5.7.6. Los servicios de backup en data center externos deben contratar con empresas que garanticen el correcto almacenamiento de la información, con la seguridad adecuada y la posibilidad de recuperación o tener acceso a este en cualquier momento.

5.8. POLÍTICA DE USO DE DISPOSITIVOS MÓVILES

Se define las directrices para el manejo de los dispositivos móviles suministrados por Fondecún y para los dispositivos personales de los funcionarios o contratistas que requieran conectarse a la red de datos de la entidad, partiendo de la premisa que estos dispositivos son herramienta de trabajo.

5.8.1. Todos los dispositivos móviles entregados por Fondecún solo deben tener instalado y configurado los aplicativos permitidos por el área de tecnología.

5.8.2. Todos los dispositivos móviles entregados por Fondecún solo deben tener configurado cuentas de correo electrónicos institucionales y asignada al usuario del dispositivo.

5.8.3. Los dispositivos móviles deben tener contraseña de ingreso y bloqueo del equipo de manera automática y manual.

5.8.4. Los dispositivos móviles institucionales deben tener únicamente la tarjeta sim asignada por la entidad, de igual forma la tarjeta sim únicamente debe instalarse en los equipos asignados por la entidad.

5.8.5. En caso de pérdida del dispositivo, ya sea por extravío o hurto, deberá informar de manera inmediata al área de tecnología y recursos físicos e inventarios, para poder realizar el procedimiento administrativo por perdida de elementos.

5.8.6. Es responsabilidad del encargado de los teléfonos móviles institucionales, mantenerlos encendidos y cargados durante las horas laborales de igual forma darles un adecuado uso.

5.8.7. Los usuarios que requieran conectar a la red de Fondecún los dispositivos móviles personales deberán realizar la solicitud al área de tecnología, quien estará encargada de realizar la configuración adecuada para que se cumplan los requerimientos de seguridad.

5.8.7. Para los equipos portátiles asignados por la entidad y que sean retirados de las instalaciones para trabajo remoto se debe mantener el control de acceso con usuario y contraseña, conservando la seguridad de la información.

5.8.7. Los usuarios que necesiten retirar los equipos de cómputo asignados por la entidad deben hacerlo mediante el formato de solicitud y autorización de salida de equipos, el cual debe estar firmado por el jefe de área subgerente o jefe OAJ, según corresponda, entregando dicho formato al área TIC e informar dejando copia en la recepción a la salida de la entidad.

5.8.7. El funcionario o contratista que retire de las instalación de la entidad cualquier equipo de cómputo se hace responsable de la seguridad del mismo y de la información en este almacenada.

5.9. POLÍTICAS DE SEGURIDAD, EL USO DE INTERNET Y DE RED

El área de tecnología como responsable de los recursos de red debe mantener su funcionamiento, y asegurar el adecuado uso por cada funcionario o contratista por medio de mecanismos de control de acceso, implementando medidas que permitan asegurar la disponibilidad de los recursos y servicios de red.

5.9.1. El área de tecnología es la encargada de gestionar y prestar todos los recursos necesarios para la implementación y prestación del servicio de internet, con los requerimientos de seguridad adecuados.

5.9.2. El acceso a internet con que cuenta la entidad es exclusivamente para las actividades relacionadas de acuerdo al cargo y funciones desempeñadas.

5.9.3. El acceso a internet (navegación web, FTP u otros servicios) es controlado y debe ser para uso corporativo durante la jornada laboral, solo se prestarán los servicios de red estrictamente necesarios para el desarrollo de las labores institucionales.

5.9.4. Los usuarios deben reportar al área de tecnología cualquier incidente que se presente en el servicio de internet.

5.9.5. El área de tecnología debe monitorear el uso del canal de acceso a internet para identificar que se esté realizando adecuado uso por los usuarios.

5.9.6. Está prohibido la descarga de software de internet sin la autorización de la gerencia o del área de tecnología

5.9.7. Se debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de internet en caso de contingencia interna.

5.9.8. Fondecún se reserva el derecho de realizar supervisión de los sitios de Internet visitados y del uso de los servicios habilitados.

5.9.9. Los funcionarios y contratistas no deben acceder a páginas que contengan información relacionada con pornografía, drogas, alcohol, webproxy, hacking y cualquier otra página que vaya en contra de la ética y moral, las leyes del país, o normas de la presente política.

5.9.10. Está prohibido el acceso a páginas de redes sociales, mensajería instantánea y otras similares.

5.9.11. Se prohíbe el uso de aplicativos (AnyDesk, Team Viewer, entre otros) que permitan la administración remota de equipos conectados a Internet, salvo que se cuente con autorización de la gerencia general y con un mecanismo de control de acceso seguro.

5.9.12. Los usuarios de los recursos de internet no deben descargar, usar o instalar juegos, música, películas, información que de alguna manera atenten contra la propiedad intelectual de sus autores.

5.9.13. La información que se proporcione por medio de la red Intranet debe ser de interés general e institucional.

5.9.14. El área de tecnología debe implementar las medias necesarias para minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos.

5.9.15. El área de tecnología debe identificar los mecanismos de seguridad y los niveles de servicio de red requeridos e incluirlos en los acuerdos de nivel de servicios de red.

5.9.16. El uso de la red inalámbrica de Fondecún es para uso exclusivo de usuarios que requieran su uso como parte de sus funciones o actividades propias del negocio.

5.9.17. El área de tecnología debe asegurar que las redes inalámbricas cuenten con mecanismos de autenticación que evite los accesos no autorizados.

5.9.18. El área de tecnología realizar la identificación, documentación de los servicios, protocolos, puertos y puntos de red.

5.9.19. El área de tecnología debe realiza los procesos necesarios para instalar seguridad física/lógica entre la red interna de la entidad y las redes públicas a la que se tenga conexión.

5.9.20. El uso de los recursos de las redes es utilizado como medio de comunicación para la conexión del total de equipos e impresora, por lo tanto debemos garantizar un uso considerable por parte de los usuarios para contar con el ancho de banda suficiente para las labores importantes que se realizan día a día.

5.9.21. Se debe establecer esquemas de identificación para los dispositivos conectados a la red de datos que faciliten su administración, mantenimiento y el acceso a los servicios disponibles

5.9.22. Los servicios de red deben utilizarse en forma responsable, apropiada y con los niveles de seguridad que se establezcan en las directrices técnicas para cada uno de ellos

5.9.23. Se prohíbe la conexión de cualquier equipo de cómputo externo de la entidad a la red de datos, ya sea por cable o por red inalámbrica sin la previa revisión y autorización del área de tecnología, esta autorización debe solicitarse mediante el formato de registro y conexión

5.9.24. Los usuarios que requieran conectar a la red de Fondecún los dispositivos personales deberán solicitar la conexión mediante el formato de solicitud de conexión equipos externos presentándolo al área TIC, dejando el registro del tipo de equipo, sistema operativo, tipo antivirus, dirección MAC, serial, enter otros, luego de su validación se procederá a realizar la configuración adecuada para que se cumplan los requerimientos de seguridad.

5.9.24. Los funcionarios o contratistas que deseen que los equipos de cómputo personales accedan a la red de datos de la entidad deben cumplir con todos los requisitos o controles de seguridad, como tener mínimo un software de seguridad antivirus licenciado y actualizado diferente a Microsoft Defender, tener actualizado el sistema operativo y únicamente podrán realizar las tareas para las que fueron autorizados.

5.10. POLÍTICAS SOBRE LA RED FÍSICA DE DATOS Y LA RED ELÉCTRICA

5.10.1. El sistema de cableado estructurado debe contar en todo su recorrido con la protección de ductería (canaletas, rieles, tubo) adecuada necesaria para evitar daños en su parte física, durante todo su recorrido.

5.10.2. Se debe contar con un sistema de cableado que cumpla las normas de cableado estructurado EIA/TIA 568, para este propósito se debe tener en la infraestructura de red cableado estandarizado en categoría 6ª.

5.10.3. El centro de cableado y de servidores de Fondecún debe contar con una seguridad minina de acceso físico, en la que se controle mediante puerta con seguro el ingreso al personal no autorizado y mediante formato de ingreso a centro de cómputo registrar los ingresos del personal de mantenimiento.

5.10.4. El sistema de cableado estructurado debe contar en todos sus elementos con el correspondiente maquillaje de identificación.

5.10.5. Cualquier cambio que se realice en el sistema de cableado estructurado y en el centro de cómputo deben ser bajo la supervisión del encargado del área de tecnología y debe quedar documentado.

5.10.6. Los usuarios de la entidad deben cuidar el sistema de cableado dando una correcta utilización.

5.10.7. A la red regulada de la entidad solo se debe conectar los equipos y dispositivos propios de Fondecún que pertenezcan al área de tecnología y que sean indispensables para el manejo de la información, como computadores, portátiles, servidores, unidades de almacenamiento, impresoras.

Dispositivos personales no se deben conectar a la red regulada ni equipos que representen riesgo al adecuado funcionamiento de la red regulado como cafeteras, ventiladores, aspiradoras, etc.

5.10.8. En el caso de interrupciones del servicio eléctrico, los usuarios deben guardar toda información digital que estén trabajando en un tiempo aproximado a 10 minutos, tiempo durante el cual la carga de las UPS de la entidad brindaran soporte a los equipos de cómputo, para evitar pérdidas de información.

5.11. POLÍTICAS PARA LA PROTECCIÓN CONTRA VIRUS INFORMÁTICOS

Con el ánimo proteger la ciber información y servicios de tecnología, previniendo amenazas informáticas como la ejecución de software malintencionado, spam, malware, entre otras, se define los siguientes lineamientos.

5.11.1. El área de tecnología será la responsable por mantener vigente las licencias y actualizado el software antivirus corporativo con que cuenta la entidad.

5.11.2. Todo equipo de cómputo perteneciente a la entidad debe tener instalado y actualizado el antivirus debidamente licenciado por la entidad para la protección de infecciones informáticas, a nivel de red y de estaciones de trabajo, contra virus y código malicioso.

5.11.3. Los usuarios deben seguir las recomendaciones y directrices establecidas con el fin de prevenir la infección con virus informáticos.

5.11.4. Todos los equipos de cómputo de la entidad deben tener configurado las actualizaciones automatizas para la instalación de parches de seguridad.

5.11.5. Todos los correos y archivos adjuntos deberán ser analizados por el antivirus con el fin de prevenir la infección y propagación de virus informático, así mismo los dispositivos externos de almacenamiento como memorias, unidades extraíbles.

5.11.6. Los equipos propios de funcionarios y contratistas que son autorizados para conectarse a la red de datos de la entidad deben tener antivirus licenciado y contar con las medidas de seguridad apropiadas.

5.11.7. Se prohíbe el acceso a las carpetas compartidas a funcionarios y contratistas desde equipos de cómputo que no cuenten con antivirus corporativo actualizado.

5.12. POLÍTICAS PARA LA CONEXIÓN REMOTA

Se definen las directrices para las distintas conexiones remotas, su uso y su correcto lineamiento de seguridad lo cual brinde resguardo a todos los sistemas e información de la entidad.

5.12.1. Realizar la solicitud de conexiones VPN por medio de la Mesa de Ayuda al área de tecnología utilizando el formato establecido para esto, indicando usuario, periodicidad, equipo con el que se realizara la conexión remota, servicio e información a la que tendrá acceso y tipo de acceso.

5.12.2. Contar con las aprobaciones requeridas para establecer conexión remota (VPN) a los dispositivos de la plataforma tecnológica de la entidad y acatar las instrucciones de acceso establecidas para las conexiones remotas.

5.12.3. Los funcionarios y contratistas que soliciten acceso por medio de una VPN son responsables del uso adecuado del acceso remoto.

5.12.4. Los equipos utilizados para el acceso remoto deben contar con protección ante software malicioso (Antivirus licenciado y con todas sus características) y configurado usuario y contraseña para el ingreso y en general los lineamientos de seguridad descritos en este documento.

5.12.5. Las credenciales de acceso de los usuarios deben contar con contraseñas robustas y debe ser cambiadas periódicamente, además de incluir el doble factor de autenticación

5.12.6. Los dispositivos utilizados por el usuario para el trabajo en acceso remoto deben ser configurados con el software de acceso VPN utilizado por la entidad y verificar el correcto funcionamiento de los demás aplicativos (sistema operativo, antivirus, control de actualizaciones, entre otros) tanto si son corporativos o aportados por el usuario.

5.12.7. El área de tecnología verificara que todas las especificaciones técnicas y de seguridad en los equipos de cómputo sean las exigidas y adecuadas para la conexión remota.

5.12.8. Se debe evitar conexión a redes wi-fi públicas ya que estas son propensas a ataques en los cuales pueden perjudicar la integridad de la información y de los sistemas conectados a la misma.

5.12.9. No instalar ni configurar en los servicios ni en la infraestructura tecnológica de la entidad (computadores de escritorio, portátiles, equipos móviles, servidores de cómputo físicos y virtuales, etc.) software para conexiones remotas gratis o de pago como: Gotomypc, Teamviewer, LogMeIn, AnyDesk, Etc., salvo que se cuente con autorización de la gerencia general y con un mecanismo de control de acceso seguro.

5.13. POLÍTICAS ESCRITORIO LIMPIO Y EQUIPOS DESATENDIDOS

5.13.1. Conservar su escritorio libre de información propia de la entidad (papeles o unidades de almacenamiento externo), los cuales podrían ser copiados, utilizados o estar al alcance de terceros o por personal que no tenga autorización para su uso o conocimiento.

5.13.2. No exponer, publicar, divulgar, o dejar a la vista información sensible que contenga datos de la Entidad o información de datos personales o cualquier información que se considere importante. Así mismo, éstos deben quedar fuera del alcance de terceros sin autorización y/o supervisión.

5.13.3. Al finalizar la jornada de trabajo, los funcionarios o contratistas deberán guardar en un lugar seguro los documentos y medios que contengan información pública de uso interno, pública clasificada o pública reservada.

5.13.4. Bloquear la pantalla de su equipo de cómputo cuando no esté haciendo uso de este, o cuando por algún motivo deba ausentarse de su puesto de trabajo, (por ejemplo, bloquear los equipos con sistema operativo Windows con las teclas Windows + L y no solo apagar el monitor).

5.13.5. La pantalla de computador (escritorio) debe estar libre de archivos o enlaces de acceso a archivos, estos deben ubicarse en las debidas carpetas de almacenamiento.

5.13.6. Salir de todas las aplicaciones y apagar los equipos de cómputo al finalizar sus actividades diarias.

5.13.7. Después de imprimir documentos de carácter CONFIDENCIAL, evitar reutilizar y antes de reciclar destruir papel que contenga información CONFIDENCIAL.

5.13.8. Proteger bajo llave la información CONFIDENCIAL (papeles o unidades de almacenamiento externo) en horario no hábil o cuando los puestos de trabajo se encuentren desatendidos.

5.13.9. El área de tecnología realizara inspecciones para revisar que los equipos de hardware no se encuentren encendidos, al finalizar la jornada laboral en dado caso se realizan los respectivos reportes y alertas.

6. ENTRADA EN VIGENCIA

La presente Política de Seguridad Informática entra en vigor a partir de la fecha de aprobación por parte del comité de gestión de Fondecún.

7. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS		
VERSIÓN	**FECHA**	**DESCRIPCIÓN DE LA MODIFICACION**
01	Diciembre 2020	Aprobación del documento
02	Enero 2022	Actualización del documento para la vigencia 2022.

03	Julio 2023	Actualización de lineamientos de seguridad – políticas de conexiones remontas, políticas uso de internet y de red, actualización formato.