POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2022

FEDERACIÓN NACIONAL DE DEPARTAMENTOS

Dr. Didier Tavera Amado
DIRECTOR EJECUTIVO

Dra. Diana Carolina Villalba Erazo
SUBDIRECTORA ADMINISTRATIVA Y FINANCIERA

Felipe Mejía Maya
GERENTE DE TECNOLOGÍA

El día 21 de octubre de 2022 fue aprobada la versión dos (2) de la Política de Seguridad y Privacidad de la Información por el Comité de Gestión y Desempeño, Integrado por:

Dirección Ejecutiva
Secretaría General
Subdirectora Acuerdos y Convenios
Subdirectora Administrativa Y Financiera
Subdirectora de Gobierno y Regiones
Subdirector de Gestión Humana
Subdirector de Fortalecimiento Territorial
Jefa Control Interno
Jefa de Comunicaciones
Jefe de Planeación
Gerente Tecnología

Elaborado por:
Felipe Mejía Maya – Gerente de Tecnología
Iván Darío Tapia Morfil – Contratista profesional FND
Jorge Eliecer Perna Manrique - Contratista profesional FND

Revisado por:
Clara Consuelo Ovalle Jiménez – Jefe de Control Interno FND
Jorge Eliecer Perna Manrique - Contratista profesional FND

CONTENIDO

1. INTRODUCCIÓN 5
2. OBJETIVOS 5
3. DIRECTRICES 6
4. ALCANCE 6
5. REQUISITOS LEGALES Y/O REGLAMENTARIOS 7
6. TÉRMINOS Y DEFINICIONES 8
7. POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 13
8. POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 14
8.1. POLÍTICA DE ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACIÓN 14
8.1.1. Conformación del Comité de Seguridad de la Información 14
8.1.2. Funciones del comité de Seguridad de la Información 14
8.1.3. Responsabilidades del comité de Seguridad de la Información 15
8.2. POLITICA DE SEGURIDAD PARA LOS RECURSOS HUMANOS 15
8.2.1. Proceso Disciplinario 16
8.3. 8.3 GESTIÓN DE ACTIVOS DE INFORMACIÓN 19
8.3.1. Política de uso de los activos 20
8.3.2. Política de uso de estaciones cliente (Equipo de cómputo personales) 20
8.3.3. Política de uso de Internet 20
8.3.4. Política para uso de dispositivos móviles 21
8.3.5. Política de la clasificación de la información 22
8.4. CONTROL DE ACCESOS 22
8.4.1. Política de establecimiento, uso y protección de claves de acceso 23
8.4.2. Manejo de contraseñas para administradores de tecnología 24
8.4.3. Política de uso de puntos de red de datos (red de área local - LAN) 25
8.4.3.1. Segregación en redes 26
8.4.3.2. Control de Acceso Remoto 26
8.5. CIFRADO 26
8.5.1. Política de controles criptográficos 26
8.6. SEGURIDAD FÍSICA Y AMBIENTAL 27
8.6.1. Política de seguridad del centro de datos y centros de cableado 27
8.6.2. Política de seguridad de los Equipos 28
8.6.3. Política de escritorio y pantalla limpia 28
8.6.4. Política de manejo disposición de información, medios y equipos 28
8.7. SEGURIDAD DEL AREA Y DE LAS ACTIVIDADES DE OPERACIONES DE TIC 29
8.7.1. Política de respaldo y restauración de información sistemas de información 30

8.7.2. Política para realización de copias en estaciones de trabajo de usuario final 30
8.7.3. Política de registro y seguimiento de eventos de sistemas de información y comunicaciones 31
8.7.4. Política de control de software operacional de La FND. 32
8.7.5. Política de gestión de vulnerabilidades 32
8.8. SEGURIDAD DE LAS TELECOMUNICACIONES 33
8.8.1. Política para la transferencia de información. 33
8.8.2. Política Administradores de Sistemas de Información y de uso de correo electrónico 33
8.8.3. Política de uso de mensajería instantánea y redes sociales 34
8.9. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN 35
8.10. RELACIONES CON PROVEEDORESY TERCEROS 35
8.10.1. Política de Tercerización u Outsourcing 35
8.11. GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN 36
8.12. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO 36
8.13. CUMPLIMIENTO 37
8.13.1. Política de tratamiento de datos personales 37
8.13.2. Política de cumplimiento de requisitos legales y contractuales 38
8.13.3. Política de Revisiones de Seguridad de la Información 38
8.14. POLÍTICA ANTISOBORNO FND 39
8.14.1. Identificación de puntos críticos – Metodología Antisoborno FND 39
8.15. POLÍTICA DE SEGURIDAD POST PANDEMIA COVID 19 40
8.15.1. Teletrabajo 40
8.15.1.1. ..... Modalidades de Teletrabajo 40
8.15.1.2. ..... Pasos para implementar el Teletrabajo 41
8.15.2. Trabajo en Casa 41
8.15.3. Soluciones de trabajo en Casa 41
8.15.4. Protección perimetral externa 42
8.15.5. Servicios en la nube 43
8.15.6. Operaciones cibernéticas 43
8.15.7. Ciberataques 44

1. INTRODUCCIÓN

La Federación Nacional de Departamentos establece que la información, en sus diferentes formatos, es un activo fundamental para el desarrollo de las actividades, en razón a que es una herramienta útil para la toma de decisiones, motivo por el cual, está comprometida a proteger los diferentes activos de información de la entidad (Colaboradores, información, infraestructura tecnológica y entorno laboral, entre otros), orientando sus esfuerzos a la preservación de la confidencialidad, integridad, disponibilidad de la información, a la continuidad de las operaciones de gobernabilidad, la administración y/o gestión de riesgos, la creación de cultura y conciencia de seguridad en los trabajadores, contratistas, proveedores y personas que hagan uso de los activos de información de la entidad.

En el presente documento se definen las políticas que conforman el Sistema de Gestión de Seguridad de la Información SGSI al interior de la Federación Nacional de Departamentos, las cuales deben ser adoptadas por los funcionarios, contratistas, proveedores y visitantes. Estas políticas están orientadas a fortalecer la seguridad de la información bajo el cumplimiento de la normatividad colombiana vigente, apoyándose en el modelo de seguridad y privacidad de la información de MinTIC y en la norma ISO/IEC 27001:2013.

2. OBJETIVOS

las pautas, directrices y reglas para crear una adecuada cultura de seguridad y protección de la información a la que es susceptible de tratamiento dentro de los procesos implementados en La Federación Nacional de Departamentos, estableciendo dentro de las funciones de la Gerencia de Tecnología su liderazgo e implementación.

Informar al mayor nivel de detalle a los usuarios, directivos, trabajadores y contratistas las normas y mecanismos que deben cumplir en las interacciones con los activos de información de La Federación Nacional de Departamentos, y establecer el alcance de las responsabilidades que compromete en la gestión a cada uno de ellos.

3. DIRECTRICES

Se debe verificar que se definan, implementen, revisen y actualicen las políticas de seguridad de la información.

Se debe establecer un plan de socialización de las políticas de seguridad, que permita el fomento continuo de la creación de cultura y conciencia de seguridad en los trabajadores, contratistas, proveedores, personas, usuarios de las Tecnologías de la Información y las comunicaciones -TIC- implementadas en la Federación Nacional de Departamentos.

Todos los usuarios de las Tecnologías de la Información y las comunicaciones -TIC- implementadas en La Federación Nacional de Departamentos, tienen la responsabilidad y obligación de cumplir con las políticas, normas, procedimientos y buenas prácticas de seguridad de la información establecidas en el presente documento de políticas de seguridad y privacidad de la información.

El Director, los Subdirectores, Secretario General, Gerentes, jefes de oficina y/o área y/o dependencia, coordinadores, supervisores de contratos, deben asegurarse que todos los procedimientos de seguridad de la información dentro de su área y ámbito de responsabilidad, se realicen correctamente para lograr el cumplimiento de las políticas y estándares de seguridad de la información de La Federación Nacional de Departamentos.

4. ALCANCE

Las Políticas de seguridad de la Información cubren los aspectos de privacidad, acceso, autenticación, mantenimiento y divulgación relacionados con cualquier activo de información, que conllevan a disponer guías y controles que deben ser cumplidos por los directivos, trabajadores, contratistas y terceros, que laboren o tengan relación con La Federación Nacional de Departamentos, para alcanzar un adecuado nivel de protección en cuanto a confidencialidad, integridad y disponibilidad de la información.

Este documento debe ser de conocimiento de todos los colaboradores (trabajadores y contratistas) de La Federación Nacional de Departamentos. Así mismo, se exigirá su cumplimiento en los procesos de contratación de la entidad, y su lectura y conocimiento debe ser requisito necesario antes de realizar cualquier proceso de contratación.

5. REQUISITOS LEGALES Y/O REGLAMENTARIOS

Con el objeto de mitigar los riesgos relacionados con la autenticidad, la integridad, la disponibilidad, el no repudio, la confidencialidad y la trazabilidad de la información, se tiene que cualquier incidente que viole el marco normativo legal vigente en Colombia, en materia de políticas de seguridad de la Información estará sujeto, entre otras, a lo establecido en las siguientes disposiciones legales:

- Constitución Política de Colombia: artículo 15, reconoce como Derecho Fundamental el Habeas Data.
- Ley 527 de 1999: por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se dictan otras disposiciones.
- Ley 599 de 2000: Por la cual se expide el Código Penal.
- Ley 1221 de 2008: Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
- Ley 1266 de 2008: Por la cual se dictan las disposiciones generales del Habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- Ley 1273 de enero 5 de 2009: Por medio de la cual se modifica el Código Penal, se 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.
- Ley 1474 de 2011: Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública. Estatuto Anticorrupción.
- Ley 1581 de 2012 Por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 1712 de 2014 Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Ley 1952 de 2019: Por medio de la cual se expide el código general disciplinario.
- Ley 2088 de 2021: Por la cual se regula el trabajo en casa y se dictan otras disposiciones.
- Decreto 884 del 2012: Por medio del cual se reglamenta la Ley 1221 de 2008 y se dictan otras disposiciones.
- Decreto 1377 de 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Decreto 886 de 2014: Por el cual se reglamenta el Registro Nacional de Bases de Datos.

- Decreto 103 de 2015: Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- Ley 1778 de 2016: Por la cual se dictan normas sobre la responsabilidad de las personas jurídicas por actos de corrupción transnacional y se dictan otras disposiciones en materia de lucha contra la corrupción.
- CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016. Política Nacional de Seguridad digital.

6. TÉRMINOS Y DEFINICIONES

A continuación, se relacionan las siguientes definiciones para una comprensión adecuada de la presente política:

Activo: Según [ISO/IEC 13335-12004], cualquier cosa que tiene valor para la organización. También se entiende por cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización.

Es todo aquello que contiene información, la cual posee un valor y es necesaria para realizar los procesos misionales y operativos de la Federación Nacional de Departamentos. Se pueden clasificar de la siguiente manera:

- **Datos**: Son todos aquellos elementos básicos de la información (en cualquier formato) que se les da tratamiento en el FND.
- **Aplicaciones**: Es todo el software (Sistema de información, herramientas de ofimática, entre otros) que se utiliza para la gestión de la información.
- **Personal**: Son todos los colaboradores de la FND (Planta, contratistas, clientes, usuarios) en general, todos aquellos que tengan acceso de una manera u otra a los activos de información de la FND.
- **Servicios**: Son tanto los servicios internos, aquellos que una parte de la organización suministra a otra, como los externos, aquellos que la organización suministra a clientes y usuarios.
- **Tecnología**: Son todos los equipos utilizados para gestionar la información y las comunicaciones.
- **Instalaciones**: Son todos los lugares en los que se alojan otro tipo de activos.
- **Equipamiento auxiliar**: Son todos aquellos activos que dan soporte a otros activos y que no se hallan en ninguno de los tipos anteriormente definidos.

Activo de Información: Todo aquel elemento lógico o físico que conforme cualquiera de los sistemas de información de la institución; por ejemplo: Bases de datos, sistemas operacionales, redes, sistemas de información y comunicaciones, documentos digitales y/o impresos, fichas, formularios y recursos humanos.

Administrador del Sistema: Persona responsable de administrar, controlar, supervisar y garantizar la operatividad y funcionalidad de los sistemas. Dicha administración está dirigida y/o coordinada por la Gerencia de Tecnología y se realizará por conducto de la persona natural y/o jurídica a quien se le delegue.

Administrador de servicio de Correo electrónico: Persona responsable de gestionar el servicio de correo, dentro de sus tareas está: Configurar las cuentas de correo, solucionar problemas que se presente con el servicio de correo electrónico, apoyar y/o responder preguntas a los usuarios relacionadas con el servicio, entre otras.

Análisis de riesgos: Proceso sistemático que permite identificar y determinar el impacto o grado de vulnerabilidad de los activos de la organización.

Ataque Cibernético: Cualquier Intento de penetrar, alterar, robar, copiar, destruir, deshabilitar, entre otros, y/o toma de control de un activo de información por parte de un usuario no deseado ni autorizado, por lo general con intenciones de causar algún daño o de obtener beneficios.

Brecha de Seguridad: deficiencia de algún recurso, módulo o componente, relacionado con tecnologías de la información y las comunicaciones, que pone en riesgo los servicios de información o expone la información en sí misma, sea o no protegida por reserva legal.

Buzón de correo: También conocido como cuenta de correo, es un espacio exclusivo, asignado en el servidor de correo, para almacenar los mensajes de correo y archivos adjuntos enviados por otros usuarios internos o externos a La Federación Nacional de Departamentos.

Centro de Computo: También conocido como Centro de Procesamiento de Datos, o Data Center; es una edificación con infraestructura especialmente adecuada (muros, pisos, accesos, energía, aire acondicionado de precisión, ups, planta eléctrica, control de acceso, sistemas de extinción de fuego, detectores de humo y calor, entre otros) para el alojamiento, instalación, configuración y operación de la plataforma tecnológica (equipos servidores, sistemas de almacenamiento, sistemas operacionales, sistemas de información, bases de datos, telecomunicaciones), encargada del procesamiento de datos e información de manera automatizada. El procesamiento se lleva a cabo con la utilización de computadoras (Hardware) y programas (Software) necesarios para cumplir con dicha tarea.

Chat:Sistema de comunicación simultánea y sincronizada entre dos o más personas, haciendo uso de Internet.

Confidencialidad: Característica de la información por medio de la cual no se revela ni se encuentra a disposición de individuos, organizaciones o procesos no autorizados. La información debe ser vista o estar disponible solo a las personas autorizadas.

Control: Mecanismo para manejar el riesgo, incluyendo políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas, y que pueden ser de carácter administrativo, técnico o legal.

Correo Electrónico: También conocido como e-mail, es un servicio de red que permite a los usuarios registrados, enviar y recibir mensajes que incluyen textos, imágenes, videos, audio, programas, a través de internet.

Corrupción: de acuerdo con Transparencia por Colombia, la corrupción consiste en el *abuso de posiciones de poder o de confianza, para el beneficio particular en detrimento del interés colectivo, realizado a través de ofrecer o solicitar, entregar o recibir bienes o dinero en especie, en servicios o beneficios, a cambio de acciones, decisiones u omisiones.*

Cuentas de Correo: Son espacios de buzones para la recepción, envió y almacenamiento de mensajes de correo electrónico en internet.

Contraseña o Password: Es una forma de autenticación privada, que puede estar compuesta por la combinación de números, letras y caracteres especiales, que permiten a un usuario autenticarse ante un sistema y así tener acceso a un computador, a un archivo y/o a un programa.

Disponibilidad: Es la garantía de poder acceder a los activos de la información cuando sea necesario, por personal autorizado.

Evento de Seguridad de la información: Ocurrencia identificada de una situación de sistema, servicio o red que indica una posible violación de la política de seguridad de la información o falla de salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad de un activo de información.

Firma Digital: La firma digital hace referencia, en la transmisión de mensajes por medios electrónicos y en la gestión de documentos electrónicos, a un método criptográfico que asocia la identidad de una persona o de un equipo informático al mensaje o documento.

Fraude: Engaño económico con la intención de conseguir un beneficio, y con el cual alguien queda perjudicado.

Incidente de Seguridad de la información: Es la identificación de la ocurrencia de un hecho que está relacionado con los activos de información, que indica una posible brecha en las Políticas de Seguridad o falla en los controles y/o protecciones establecidas.

Infraestructura de Procesamiento de Información: Es cualquier sistema de procesamiento de información, servicio, plataforma tecnológica, o instalación física que los contenga.

ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.

ISO 17799: Código de buenas prácticas en gestión de la seguridad de la información adoptado por ISO transcribiendo la primera parte de BS7799. A su vez, da lugar a ISO 27002 por cambio de nomenclatura el 1 de Julio de 2007. No es certificable.

ISO/IEC 27001: Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 2005, segunda publicación en 2013.

ISO 27002: Código de buenas prácticas en gestión de la seguridad de la información (transcripción de ISO 17799). No es certificable. Cambio oficial de nomenclatura de ISO 17799:20005 a ISO 27002:20005 el 1 de Julio de 2007.

Firewall: Dispositivo que permite controlar, bloquear o filtrar el acceso en redes de comunicación.

Hacker: Persona dedicada a realizar entradas no autorizadas a los sistemas, por medio de redes de comunicación como Internet, con el objeto de encontrar vulnerabilidades en los sistemas.

No conformidad: Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.

No conformidad grave: Ausencia o fallo de uno o varios requerimientos de la ISO/IEC 27001 que, basada en evidencias objetivas, permita dudar seriamente de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo inaceptable.

No repudio: Los activos de información deben tener la capacidad para probar que una acción o un evento han tenido lugar, de modo que tal evento o acción no pueda ser negado posteriormente.

Partes interesadas: Persona u organización que puede afectar o ser afectada o percibirse a sí misma como afectada por una decisión o actividad.

Phishing: Delito enmarcado en la categoría de las estafas, que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta mediante una aparente comunicación oficial electrónica.

Política de Seguridad: Definición en la cual se establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información.

Privacidad de la información: Cuando una organización o individuo debe determinar qué datos en un sistema informático se pueden compartir con terceros.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Seguridad de la Información: es el conjunto de medidas preventivas y reactivas s que permiten resguardar y proteger la información.

Sistema de Información: se refiere a un conjunto ordenado de mecanismos que tienen como fin la administración de datos y de información, de manera que puedan ser recuperados y procesados fácil y rápidamente.

Soborno: el que entregue o prometa dinero u otra utilidad a un testigo para que falte a la verdad o la calle total o parcialmente en su testimonio (Estatuto Anticorrupción, 2011).

Teletrabajador: Persona que desempeña actividades laborales a través de tecnologías de la información y la comunicación por fuera de la empresa a la que presta sus servicios.

Trabajo en casa: es la habilitación al trabajador para que, en situaciones excepcionales, pueda desempeñar sus labores desde su casa, sin que haya cambios al contrato laboral.

Usuario: en este documento se emplea para referirse a funcionarios, contratistas, proveedores y visitantes, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la FND.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

7. POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Federación Nacional de Departamentos, entendiendo la importancia de una adecuada gestión de la información está comprometida con su protección, de tal forma que pueda responder por la integridad, confidencialidad y la disponibilidad de sus activos, enmarcado en el estricto cumplimiento de la normatividad aplicable, y en concordancia con la naturaleza de la entidad.

Aplica para todos los funcionarios, contratistas, proveedores y terceros, teniendo cada uno un papel fundamental en la administración de la seguridad de la información, así como la responsabilidad de mantener un ambiente seguro en la entidad que nos permita una mejora en el Sistema de Gestión de Seguridad de la Información.

La Federación Nacional de Departamentos, para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Minimizar el riesgo de los procesos misionales de la Federación Nacional de Departamentos.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información y garantizar el mejoramiento continuo del mismo.
- Proteger los activos de información.
- 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 la Federación Nacional de Departamentos.
- Garantizar la continuidad del negocio frente a incidentes.

Esta Política proporciona el marco de referencia para la mejora continua del Sistema de Gestión de Seguridad de la Información, así como para establecer y revisar los objetivos del Sistema de Gestión de Seguridad de la Información, siendo comunicada a toda la Organización a través del INTEDYA CLOUD instalado en la organización y su publicación en paneles informativos, siendo revisada anualmente para su adecuación y extraordinariamente cuando concurran situaciones.

8. POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

8.1. POLÍTICA DE ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACIÓN

Esta política se encarga de definir los roles y responsabilidades, los cuales implican actividades de administración, operación y gestión de la seguridad de la información, que se deben tener para la Seguridad de la Información, especialmente en lo que se refiere a la protección de los activos de información en la Federación Nacional de Departamentos.

El Comité de Seguridad de la Información será el encargado de monitorear el cumplimiento de las políticas de seguridad, así como de verificar que se realicen las actualizaciones que requieran.

8.1.1. Conformación del Comité de Seguridad de la Información

El Comité estará integrado así:

- El Gerente de Tecnología o su delegado.
- El Jefe de Planeación o su delegado.
- El Secretario(a) General o su delegado.
- El Jefe de Gestión Documental o su delegado.
- El Jefe de Control Interno o su delegado.

8.1.2. Funciones del comité de Seguridad de la Información

- Proponer y revisar el cumplimiento de normas y políticas de seguridad, que garanticen acciones preventivas y correctivas para la salvaguarda de equipos e instalaciones de cómputo, así como las bases de datos e información en general.
- Revisar el estado general de la seguridad de la información.
- Revisar y analizar los incidentes de seguridad de la información existentes.
- Revisar y aprobar los proyectos de seguridad de la información.
- Aprobar las modificaciones o nuevas políticas de seguridad de la información.
- Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.

- Identificar necesidades de evaluación de los procesos soportados por los recursos informáticos y su plataforma tecnológica.
- Realizar otras actividades inherentes a la naturaleza del comité relacionadas con la seguridad de la información.

8.1.3. Responsabilidades del comité de Seguridad de la Información

- Responsables del análisis, revisión y centralización de todas las acciones referidas a la gestión de Seguridad de la Información de la organización y de mantener la vigencia de las políticas de acuerdo con las necesidades y requerimientos del negocio.
- Asegurar que exista una dirección y apoyo de la alta dirección (comité directivo), o a quien se delegue, sobre los principios y las metas para soportar la administración y desarrollo de iniciativas sobre la gestión de la seguridad de los activos de información, a través de compromisos apropiados y de recursos adecuados, como la formulación y mantenimiento de las políticas de seguridad de la información a través de todos los trabajadores de la organización.
- Validar las políticas de seguridad de la información y procedimientos para el uso adecuado y administración de los recursos informáticos asignados a los trabajadores de la organización, asegurando que la información se encuentre protegida.

8.2. POLITICA DE SEGURIDAD PARA LOS RECURSOS HUMANOS

La Federación Nacional de Departamentos implementa acciones para asegurar que los trabajadores, contratistas, proveedores y demás colaboradores de la Entidad, entiendan sus responsabilidades del cumplimiento de las políticas como usuarios y la responsabilidad de los roles asignados.

La información almacenada en los equipos de cómputo de la FND o la información sujeta al tratamiento dentro de la relación contractual, independiente del sitio de almacenamiento, es propiedad de La Federación Nacional de Departamentos y cada usuario es responsable por proteger la integridad, confidencialidad y disponibilidad de la información.

Se debe capacitar y sensibilizar a los trabajadores sobre las políticas de seguridad de la información.

Se debe asegurar que los trabajadores, contratistas y demás colaboradores de La Federación Nacional de Departamentos, adopten sus responsabilidades en relación con las políticas de seguridad de la información y actúen de manera consistente frente a las mismas, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información o las tecnologías de la información y las comunicaciones empleadas para el tratamiento de la información.

En situaciones de incumplimiento y/o violaciones a las políticas de seguridad de la información se considerará falta grave y el incidente se reportará a Gestión Humana, Supervisor del contrato y Secretaria General, para dar inicio a las acciones pertinentes, de acuerdo con los procedimientos correspondientes, pudiendo ser, entre otros, suprimir el permiso de uso de los recursos asignados, terminación anticipada de contrato y/o proceso disciplinario.

8.2.1. Proceso Disciplinario

Dentro de la estrategia de seguridad de la información de La Federación Nacional de Departamentos, está establecido un proceso disciplinario formal para los trabajadores que hayan cometido alguna violación de la Política de Seguridad de la Información.

De llegar a realizarse procesos disciplinarios, se debería utilizar como enseñanzas y así prevenir y/o evitar que los trabajadores, contratistas y los otros colaboradores de La Federación Nacional de Departamentos violen las políticas y los procedimientos de seguridad de la información, así como para cualquier otra violación de la seguridad. Las investigaciones disciplinarias corresponden a actividades pertenecientes al proceso de gestión de la subdirección de Gestión Humana.

Actuaciones que conllevan a la violación de la seguridad de la información establecidas por La Federación Nacional de Departamentos, son entre otras:

- No firmar los acuerdos de confidencialidad o de entrega de información o de activos de información.
- No reportar los incidentes de seguridad o las violaciones a las políticas de seguridad, cuando se tenga conocimiento de ello.
- No actualizar la información de los activos de información a su cargo.
- Clasificar y registrar de manera inadecuada la información, desconociendo los estándares establecidos para este fin.
- Mantener la reserva de la información hasta dos años después de retirarse de la Federación.

- NO guardar de forma segura la información cuando se ausenta de su puesto de trabajo o al terminar la jornada laboral, "documentos impresos que contengan información pública reservada, información pública clasificada (privada o semiprivada)".
- NO guardar la información digital, producto del procesamiento de la información perteneciente a La Federación Nacional de Departamentos.
- Dejar o almacenar información reservada, en carpetas compartidas o en lugares distintos al equipo de cómputo que ha sido asignado para tal fin, obviando las medidas de seguridad.
- Dejar las gavetas abiertas o con las llaves puestas en los escritorios, dejar los computadores encendidos y sin bloquear la sesión en horas no laborables.
- Permitir que personas ajenas a La Federación Nacional de Departamentos, permanezcan sin acompañamiento al interior de las instalaciones donde se encuentren equipos de cómputo, en los cuales se almacena la información de la federación.
- Almacenar en los discos duros de los computadores personales de los usuarios, la información de la Entidad, en caso de que se haya autorizado el uso de algún equipo personal, la información de la entidad se debe almacenar en la nube (asociada a la cuenta de correo suministrada por la entidad).
- Solicitar cambio de contraseña de Otro usuario, sin la debida autorización del titular o su jefe inmediato.
- Hacer uso de la red de datos de la institución, para obtener, mantener o difundir en los equipos de sistemas, material pornográfico (penalizado por la ley) u ofensivo, cadenas de correos y correos masivos no autorizados.
- Utilización de software no relacionados con la actividad laboral y que pueda degradar el desempeño de la plataforma tecnológica institucional.
- Recibir o enviar información institucional a través de correos electrónicos personales, diferentes a los asignados por la institución, sin previa autorización del jefe inmediato o del supervisor del contrato.
- Enviar información reservada o información clasificada como privada o semiprivada por correo, copia impresa o electrónica sin la debida autorización y sin la utilización de los protocolos establecidos para la divulgación.
- Utilizar equipos electrónicos o tecnológicos desatendidos o a través de sistemas de interconexión inalámbrica, sirvan para transmitir, recibir y almacenar datos.
- Usar dispositivos de almacenamiento externo en los computadores, cuya autorización no haya sido otorgada por la Gerencia de Tecnología de La Federación Nacional de Departamentos
- Permitir el acceso de trabajadores a la red corporativa, sin la autorización de la Gerencia de Tecnología de La Federación Nacional de Departamentos.

- Utilización de servicios disponibles a través de internet, como FTP y Telnet, no permitidos o autorizados por la Gerencia de Tecnología de La Federación Nacional de Departamentos o de protocolos y servicios que no se requieran y que puedan generar riesgo para la seguridad.
- Negligencia en el cuidado de los equipos, dispositivos portátiles o móviles entregados para actividades propias de La Federación Nacional de Departamentos.
- No cumplir con las actividades designadas para la protección de los activos de información de La Federación Nacional de Departamentos.
- Destruir o desechar, de forma incorrecta, la documentación institucional.
- Descuidar documentación con información pública reservada o clasificada de la Entidad, sin las medidas apropiadas de seguridad que garanticen su protección.
- Registrar información reservada o clasificada, en notas pos-it, apuntes, agendas, libretas, y otros sin el debido cuidado.
- Almacenar información reservada o clasificada, en cualquier dispositivo de almacenamiento portátil o conectar computadores portátiles u otros sistemas eléctricos o electrónicos personales a la red de datos de La Federación Nacional de Departamentos, sin la debida autorización del jefe inmediato y/o supervisor y del trámite de registro de estos equipos ante la Gerencia de Tecnología utilizando los formatos que se definan para tal fin.
- Archivar información pública reservada o clasificada, sin claves de seguridad o cifrado de datos.
- Promoción o mantenimiento de negocios personales, o utilización de los recursos tecnológicos de La Federación Nacional de Departamentos para beneficio personal.
- El que sin autorización acceda en todo o parte del sistema informático o se mantenga dentro del mismo en contra de la voluntad de La Federación Nacional de Departamentos.
- El que impida u obstaculice el funcionamiento o el acceso normal al sistema informático, los datos informáticos o las redes de telecomunicaciones de La Federación Nacional de Departamentos, sin estar autorizado.
- El que destruya, dañe, borre, deteriore o suprima datos informáticos o un sistema de tratamiento de información de La Federación Nacional de Departamentos.
- El que distribuya, envíe, introduzca software malicioso u otros programas de computación de efectos dañinos en la plataforma tecnológica de La Federación Nacional de Departamentos.
- El que viole datos personales de las bases de datos (manuales y/o automatizadas) de La Federación Nacional de Departamentos.
- El que superando las medidas de seguridad informática suplante un usuario ante los sistemas de autenticación y autorización establecidos por La Federación Nacional de Departamentos.

- No mantener la confidencialidad de las contraseñas de acceso a la red de datos, los recursos tecnológicos o los sistemas de información de La Federación Nacional de Departamentos o permitir que otras personas accedan con el usuario y clave del titular a éstos.
- Permitir el acceso u otorgar privilegios de acceso a las redes de datos de La Federación Nacional de Departamentos a personas no autorizadas.
- Llevar a cabo actividades fraudulentas o ilegales, o intentar acceso no autorizado a cualquier computador de La Federación Nacional de Departamentos o de terceros.
- Ejecutar acciones tendientes a eludir o variar los controles establecidos por La Federación Nacional de Departamentos.
- Retirar de las instalaciones de la institución, estaciones de trabajo o computadores portátiles que contengan información institucional sin la autorización pertinente.
- Sustraer de las instalaciones de La Federación Nacional de Departamentos, documentos con información institucional calificada como información pública reservada o clasificada, o abandonarlos en lugares públicos o de fácil acceso.
- Entregar, enseñar y divulgar información institucional, calificada como información pública reservada y clasificada a personas o Entidades no autorizadas.
- No realizar el borrado seguro de la información en equipos o dispositivos de almacenamiento, de La Federación Nacional de Departamentos, para traslado, reasignación o para disposición final.
- Ejecución de cualquier acción que pretenda difamar, abusar, afectar la reputación o presentar una mala imagen de La Federación Nacional de Departamentos o de alguno de sus trabajadores.
- Realizar cambios no autorizados en la plataforma tecnológica de La Federación Nacional de Departamentos.
- Acceder, almacenar o distribuir pornografía infantil.
- Instalar programas o software no autorizados en las estaciones de trabajo o equipos portátiles institucionales, cuyo uso no sea autorizado por la Gerencia de Tecnología de La Federación Nacional de Departamentos.
- Copiar sin autorización los programas de La Federación Nacional de Departamentos, o violar los derechos de autor o acuerdos de licenciamiento.

8.3. 8.3 GESTIÓN DE ACTIVOS DE INFORMACIÓN

La Federación Nacional de Departamentos es el dueño de la propiedad intelectual de los avances tecnológicos e intelectuales desarrollados por los trabajadores y los contratistas, derivadas del

objeto del cumplimiento de funciones y/o tareas asignadas, como las necesarias para el cumplimiento del objeto del contrato.

La Federación Nacional de Departamentos es propietario de los activos de información y, los administradores de estos activos son los trabajadores, contratistas o demás colaboradores de La Federación Nacional de Departamentos (denominados "usuarios") que estén autorizados y sean responsables por la información de los procesos y de las tecnologías de la información y las comunicaciones (TICs) a su cargo.

La Federación Nacional de Departamentos mantendrá un inventario actualizado de sus activos de información, quedando bajo la responsabilidad de cada jefe de área y deberá ser reportado a la Gerencia de Tecnología, para su consolidación y centralización.

8.3.1. Política de uso de los activos

La Federación Nacional de Departamentos, implementa las directrices para lograr y mantener la protección adecuada y uso de los activos de información, mediante la asignación y entrega a los usuarios finales, quienes deben administrarlos de acuerdo a sus roles y funciones.

8.3.2. Política de uso de estaciones cliente (Equipo de cómputo personales)

- Los usuarios no podrán realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo.
- Los usuarios no deben mantener almacenados en los discos duros de las estaciones cliente o discos virtuales de red, archivos de vídeo, música, y fotos y cualquier tipo de archivo que no sean de carácter institucional.

8.3.3. Política de uso de Internet

La Federación Nacional de Departamentos, permite el acceso al servicio de internet, estableciendo lineamientos que garanticen la navegación segura y el uso adecuado de la red por parte de los

usuarios finales, evitando errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones WEB.

La Gerencia de Tecnología, implementa herramientas para evitar la descarga de software no autorizado y/o código malicioso en los equipos institucionales.

Los usuarios de los activos de información de La Federación Nacional de Departamentos tienen restringido el acceso a páginas relacionadas con pornografía, violencia, nueva era, juegos, sitios de apuestas en líneas, concursos, entre otros, porque su contenido no corresponde al cumplimiento de la misión de la FND.

Se prohíbe la descarga, uso, intercambio y/o instalación de programas, juegos, música, videos, películas, imágenes, protectores y fondos de pantalla, software de libre distribución.

8.3.4. Política para uso de dispositivos móviles

La Entidad establece las directrices de uso y manejo de dispositivos móviles (teléfonos móviles, teléfonos inteligentes "smart phones", tabletas, entre otros), suministrados por La Federación Nacional de Departamentos y que hagan uso de los servicios de información de la Entidad.

Los usuarios no están autorizados a cambiar la configuración, a desinstalar software, formatear o restaurar de fábrica los equipos móviles institucionales, cuando se encuentran a su cargo, únicamente se deben aceptar y aplicar las actualizaciones.

- Los dispositivos móviles empresariales deben tener únicamente la tarjeta sim asignada por la empresa, de igual forma la tarjeta sim únicamente debe instalarse en los equipos asignados por la empresa.

- Ante la pérdida (extravío o hurto) o daño del equipo, se deberá informar de manera inmediata a la Gerencia de Tecnología y continuar con el procedimiento administrativo por perdida o daño de elementos tecnológicos establecido por la empresa.

- Los dispositivos móviles empresariales, debe permanecer encendidos y cargados durante las horas laborales o de acuerdo con la responsabilidad y requerimientos propios del cargo.

- Es responsabilidad del colaborador hacer buen uso del dispositivo suministrado por la FND con el fin de realizar actividades propias de su cargo o funciones asignadas en la empresa.

8.3.5. Política de la clasificación de la información

La Federación Nacional de Departamentos consiente de la necesidad de asegurar que la información reciba el nivel de protección apropiado de acuerdo al tipo de clasificación establecido por la ley y por ella, define reglas de como clasificar la información:

- Se considera información toda forma de comunicación o representación de conocimiento o datos digitales, escritos en cualquier medio, ya sea magnético, papel, visual u otro que al que se le de tratamiento en La Federación Nacional de Departamentos.
- Los usuarios responsables de la información de La Federación Nacional de Departamentos, deben identificar los riesgos a los que está expuesta la información de sus áreas, consolidando dicha información en la matriz de riesgo de cada proceso, teniendo en cuenta que la información pueda ser copiada, divulgada, modificada o destruida física o digitalmente por personal interno o externo.

8.4. CONTROL DE ACCESOS

La Entidad define las reglas para asegurar un acceso controlado, físico o lógico, a la información y plataforma informática de La Federación Nacional de Departamentos.

La conexión remota a la red de área local de La Federación Nacional de Departamentos debe realizarse a través de una conexión VPN segura suministrada por la FND, la cual debe ser aprobada, registrada y auditada, por la Gerencia de Tecnología, previa autorización del comité de Seguridad de la Información, quien analizará la solicitud, la cual debe estar firmada por el jefe inmediato del usuario que solicita el acceso remoto.

El acceso a los activos de información de La Federación Nacional de Departamentos estará permitido únicamente a los usuarios autorizados, el cual deberá utilizar durante el proceso de autenticación.

El funcionario que disponga de usuario(s) de acceso a los activos de información, será responsable de su uso, el cual es personal e intransferible.

8.4.1. Política de establecimiento, uso y protección de claves de acceso

Ningún usuario deberá acceder a la red o a los servicios TIC de La Federación Nacional de Departamentos, utilizando una cuenta de usuario o clave de otro usuario.

La Federación Nacional de Departamentos, suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y a los sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible.

El cambio de contraseña solo podrá ser solicitado por el titular de la cuenta, en donde se llevará a cabo la validación de los datos personales; en caso de ser solicitado el cambio de contraseña para otra persona, debe ser realizada por su jefe inmediato (previa autorización por parte de la Gerencia de Tecnología).

Las claves o contraseñas deben ser fuertes, para lo cual se recomienda:

- Tener mínimo ocho (8) caracteres alfanuméricos.
    - utilizar al menos un carácter alfabético en mayúscula
    - utilizar caracteres en minúsculas
    - utilizar dígitos entre O y 9
    - utilizar caracteres especiales: ¡, $, %, &,)
- Cada vez que se cambie una clave, la nueva debe ser distinta de las tres últimas, anteriormente utilizadas.

Las cuentas de los usuarios que hagan más de 3 intentos fallidos de acceso quedarán deshabilitadas y los usuarios deberán solicitar su desbloqueo.

Las contraseñas de acceso **NO** deben ser reveladas a ninguna persona. Todas las contraseñas deben ser tratadas como información sensible y confidencial.

- No registrar las contraseñas en papel, archivos digitales o dispositivos manuales, a menos que se puedan almacenar de forma segura y el método de almacenamiento este aprobado. Las contraseñas no deben ser incluidas en mensajes de correo electrónico, ni ningún otro medio de comunicación electrónica. Tampoco deben ser comunicadas las contraseñas en conversaciones telefónicas.

Los sistemas estarán configurados para que: la contraseña no sea visible en la pantalla durante el inicio de sesión, se bloquee la cuenta de usuario si se ingresa una clave incorrecta de manera reiterada, y para que se bloqueen los equipos tras un periodo de inactividad, mediante protector de pantalla que requiera una nueva autenticación del usuario.

Los responsables de sistemas o de la configuración e instalación de los equipos, deberán asegurarse que las claves creadas por los fabricantes de software o hardware, serán cambiadas durante la instalación inicial.

En el caso de que sea necesario su almacenamiento, los responsables de sistemas de la organización garantizarán que estas se conservan cifradas, o de manera que no puedan ser conocidas o accedidas por nadie.

Ante una baja o ausencia y/o novedades temporales del usuario, el responsable del departamento podrá solicitar al responsable del sistema la cesión de clave o datos a la persona designada por él, para lo cual existirá autorización expresa, y deberán de quedar evidencias al respecto.

Se realizarán, por parte de la FND, revisiones periódicas y programadas de los derechos de acceso, privilegios o permisos de los usuarios verificando que estos disponen de acceso a las utilidades, recursos o sistemas que precisan para el desarrollo de sus funciones, y que se cumple el principio de “mínimo privilegio”.

8.4.2. Manejo de contraseñas para administradores de tecnología

Si la FND, tiene implementado el servicio de Directorio Activo, se debe garantizar en las plataformas de tecnología que el ingreso a la administración, en lo posible, se realice con la vinculación directamente de las credenciales de los usuarios de directorio activo.

Los usuarios súper-administradores y sus correspondientes contraseñas a las consolas administrables se dejan en custodia en sobre sellado en el área segura donde designe la Entidad, las credenciales allí contenidas deben ser modificadas de manera mensual o cuando amerite.

Las contraseñas referentes a las cuentas "predefinidas" incluidas en los sistemas o aplicaciones adquiridas deben ser desactivadas. De no ser posible su desactivación, las contraseñas deben ser cambiadas después de la instalación del producto.

El personal de la Gerencia de Tecnología no debe dar a conocer su clave de usuario a terceros de los sistemas de información, sin previa autorización del Gerente de Tecnología.

Los usuarios y claves de los administradores de sistemas y/o del personal de la Gerencia de Tecnología son de uso personal e intransferible.

El personal de la Gerencia de Tecnología debe emplear obligatoriamente las claves o contraseñas con un alto nivel de complejidad y utilizar los servicios de autenticación fuerte que posee la Entidad de acuerdo al rol asignado.

Los administradores de los sistemas de información deben seguir las políticas de cambio de clave y utilizar procedimiento de salvaguarda o custodia de las claves o contraseñas en un sitio seguro. A este lugar solo debe tener acceso Gerente de Tecnología o el Asesor o colaborador para la de Seguridad de la Información.

8.4.3. Política de uso de puntos de red de datos (red de área local - LAN)

Asegurar los puntos de red y validar su correcta operación.

Las direcciones internas, configuraciones e información relacionada con la topología y diseño de los sistemas de comunicación y redes de la entidad serán restringidas, de tal forma que no sean conocidas por usuarios internos, clientes o personas ajenas a la entidad sin la previa autorización de la Gerencia de Tecnología.

Todas las conexiones a redes externas que accedan a la red interna de la Entidad pasarán a través de un punto adicional de control como: UTM, firewall, Gateway, o servidor de acceso.

Los usuarios que tengan acceso a direcciones IP públicas no pueden establecer conexiones a redes de acceso a información privadas, a menos que hayan sido aprobadas por la Gerencia de Tecnología de la FND.

8.4.3.1. Segregación en redes

La infraestructura tecnológica de La Federación Nacional de Departamentos que soporta Sistemas de Información debe estar separada en segmentos de red físicos y lógicos e independientes de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio de acceso a Internet. La separación de estos segmentos debe ser realizada por medio de elementos de conectividad perimetrales e internos de enrutamiento y de seguridad. (se tienen segregadas las redes en dos: una red de invitados y otra red para colaboradores de la FND en cada una de las sedes y se tiene posibilidad de aplicar diferentes criterios de ancho de banda, control de accesos, administrar el uso de impresoras y equipos) – cuentan con el diagrama de redes (pendiente enviar el diagrama de redes).

8.4.3.2. Control de Acceso Remoto

La administración remota de equipos o de la infraestructura de computo debe dejar evidencia escrita de la justificación por las que se asigna, al igual que de la responsabilidad que tiene el funcionario a quien se otorga este permiso, la solicitud debe ser realizada por el Jefe del Área correspondiente y debe ser avalada por la Gerencia de Tecnología. El acceso remoto, será siempre a través de VPN.

8.5. CIFRADO

8.5.1. Política de controles criptográficos

Implementar actividades para proteger activos de información reservada, fortaleciendo la confidencialidad, mediante el uso de herramientas criptográficas.

Cualquier usuario interno o externo que requiera acceso remoto a la red y a la infraestructura de cómputo de La Federación Nacional de Departamentos, sea por cualquier medio tecnológico existente, siempre deberá estar autenticado y sus conexiones deberán estar cifradas.

Toda información que se extraiga de los sistemas de información misionales deberá estar cifrada para evitar que la misma pierda su confidencialidad.

8.6. SEGURIDAD FÍSICA Y AMBIENTAL

La FND, debe implementar los controles necesarios en los centros de datos y/o centros de cableado de La Federación Nacional de Departamentos, para evitar el acceso de personas no autorizadas.

Todas las áreas destinadas al procesamiento, almacenamiento de documentos o información, así como aquellas en las que se encuentren los equipos de cómputo y demás infraestructura de los sistemas de información y comunicaciones, se consideran áreas de acceso restringido.

8.6.1. Política de seguridad del centro de datos y centros de cableado

Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.

En las instalaciones del centro de datos o de los centros de cableado, No está permitido:

- Almacenar elementos diferentes a equipo de TICs.
- Fumar
- Introducir alimentos o bebidas
- El porte de armas de fuego, corto punzantes o similares.
- Mover, desconectar y/o conectar equipo de cómputo sin autorización.
- Modificar la configuración del equipo o intentarlo sin autorización.
- Alterar software instalado en los equipos sin autorización.
- Alterar o dañar las etiquetas de identificación de los sistemas de información o sus conexiones físicas.
- Extraer información de los equipos en dispositivos externos.
- Abuso y/o mal uso de los sistemas de información.
- Toda persona debe hacer uso únicamente de los equipos y accesorios que les sean asignados y para los fines que se les autorice.

Los centros de cómputo deben mantener las condiciones físicas y ambientales óptimas recomendadas, así como controles automáticos para incendio, temperatura y cuando sea posible, monitoreo por Circuito Cerrado de Televisión.

8.6.2. Política de seguridad de los Equipos

Asegurar la protección de la información en los equipos.

La Federación Nacional de Departamentos, debe poseer la infraestructura necesaria, con el fin de actuar contra eventos que pongan en riesgo la integridad y confidencialidad de la información, y es así, que los equipos de cómputo están conectados a las instalaciones eléctricas apropiadas.

8.6.3. Política de escritorio y pantalla limpia

Definir las pautas generales para reducir el riesgo de acceso no autorizado, pérdida y daño de la información durante y fuera del horario de trabajo normal de los usuarios.

- Los trabajadores, contratistas, personas en comisión, pasantes y terceros que tienen algún vínculo con La Federación Nacional de Departamentos, deben conservar su escritorio libre de información, propia de la Entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.
- Los usuarios de los sistemas de información y comunicaciones de La Federación Nacional de Departamentos, deben bloquear la pantalla de su computador con el protector de pantalla, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo.
- Los usuarios de los sistemas de información y comunicaciones de La Federación Nacional de Departamentos deben cerrar las aplicaciones y servicios de red cuando ya no los necesiten.
- Al imprimir documentos con información reservada y/o pública clasificada (semi-privada o privada), deben ser retirados de la impresora inmediatamente y no se deben dejar sobre el escritorio sin custodia.
- No se debe utilizar fotocopiadoras, escáneres, equipos de fax, cámaras digitales y en general equipos tecnológicos que se encuentren desatendidos.

8.6.4. Política de manejo disposición de información, medios y equipos

La FND establece actividades para evitar la divulgación, la modificación, el retiro o la destrucción no autorizada de información almacenada en los medios proporcionados por La Federación Nacional de Departamentos, velando por la disponibilidad y confidencialidad de la información.

Los medios y equipos donde se almacena, procesa o comunica la información, deben mantenerse con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto estado de funcionamiento, para ello se debe realizar los mantenimientos preventivos y correctivos que se requieran.

El servicio de acceso a Internet, Intranet, Sistemas de información, medio de almacenamiento, aplicaciones (Software), cuentas de red, navegadores y equipos de cómputo son propiedad de la FND y deben ser usados únicamente para el cumplimiento de su misión.

Se debe realizar la aplicación del procedimiento de borrado seguro en los equipos de cómputo y demás dispositivos, una vez el funcionario haya sido retirado de la Entidad, de acuerdo a lo definido por La Federación Nacional de Departamentos.

Está restringida la copia de archivos en medios removibles de almacenamiento, por lo cual se deshabilita la opción de escritura en dispositivos USB, unidades ópticas de grabación en todos los equipos de cómputo institucionales; la autorización de uso de los medios removibles debe ser tramitada a través de la Gerencia de Tecnología.

8.7. SEGURIDAD DEL AREA Y DE LAS ACTIVIDADES DE OPERACIONES DE TIC

Definir las reglas, si aplica, para asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de datos (área de operaciones) de La Federación Nacional de Departamentos, con el fin de robustecer la continuidad de los sistemas de TIC.

- Se definirán procedimientos, registros e instructivos de trabajo debidamente documentados, los cuales serán progresivamente implementados, con el fin de asegurar el mantenimiento y operación adecuada de la infraestructura tecnológica.
- Cada procedimiento tendrá un responsable para su definición, mantenimiento e implementación.
- Para la gestión de las operaciones de la infraestructura de procesamiento de información en La Federación Nacional de Departamentos, la Gerencia de Tecnología, con el apoyo de las demás áreas, establecerá mecanismos que permitan segregar las funciones de administración (sistemas operativos, bases de datos y aplicaciones), monitoreo y operación, separando entre estos los diferentes ambientes de desarrollo, pruebas y producción.

8.7.1. Política de respaldo y restauración de información sistemas de información

Proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y el software, se pueda recuperar después de una falla, garantizando que la información y la infraestructura de software crítica de la FND, sean respaldadas y puedan ser restauradas en caso de una falla y/o desastre.

La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información y solicitadas a través de la herramienta de gestión de Solicitudes de Soporte Técnico establecida por la FND

Semanalmente, el personal encargado de realizar las copias de seguridad de la información de los sistemas de Información de La Federación Nacional de Departamentos, verificarán la correcta ejecución de los procesos de backups, suministrarán los medios de almacenamiento requeridas para cada trabajo y controlarán la vida útil de cada medio empleado.

Los medios que vayan a ser eliminados o que cumplan el periodo de retención deben surtir un proceso de borrado seguro y posteriormente serán eliminados o destruidos de forma adecuada.

El personal encargado de realizar las copias de seguridad de la información de los sistemas de Información, deberían generar y realizar tareas de restauración aleatorias de la información y deben ser documentadas.

La información previamente definida y contenida en los servidores de La Federación Nacional de Departamentos, se respaldará de forma periódica, determinada según el procedimiento definido para tal fin. Adicionalmente, se realizarán pruebas periódicas de recuperación y verificación de la información almacenada en los medios con el fin de verificar su integridad y disponibilidad.

8.7.2. Política para realización de copias en estaciones de trabajo de usuario final

Facilitar y asegurar la realización de copias de información en estaciones de trabajo de usuario final.

Todos los usuarios son responsables de realizar una copia de respaldo del original de la información de valor, confidencial o crítica a su cargo. Estas copias separadas deben ser efectuadas con la periodicidad requerida de acuerdo con los cambios que se presenten en la información.

El uso de dispositivos de almacenamiento externo (dispositivos móviles, DVD, CD, memorias USB, agendas electrónicas, celulares, etc.), pueden ocasionalmente generar riesgos para la FND al ser conectados a los computadores, ya que son susceptibles de transmisión de virus informáticos o pueden ser utilizados para la extracción de información no autorizada. Para utilizar dispositivos de almacenamiento externo se debe obtener aprobación formal.

Ningún usuario final debe realizar copias de la información contenida en la estación de trabajo a medios extraíbles de información, excepto aquellos que se encuentren autorizados y habilitados los privilegios de escritura por puertos USB.

La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario o área propietaria de la información y solicitadas a través de la herramienta de gestión de Solicitudes de Soporte Técnico establecida por la FND.

Los medios que vayan a ser eliminados o que cumplan el periodo de retención deben surtir un proceso de borrado seguro y posteriormente serán eliminados o destruidos de forma adecuada.

Todos los mensajes son sujetos a análisis frente a amenazas y ataques dirigidos, y pueden ser conservados, puestos en cuarentena y/o eliminados permanentemente por parte de la FND.

8.7.3. Política de registro y seguimiento de eventos de sistemas de información y comunicaciones

Preservar la integridad, confidencialidad y disponibilidad de los registros de eventos (logs) generados por los sistemas de información y comunicaciones de La Federación Nacional de Departamentos.

Los trabajadores y contratistas de La Federación Nacional de Departamentos, deberán informar inmediatamente al Comité de Seguridad de la Información, jefe inmediato, supervisor de contrato o al personal de la gerencia de tecnología cualquier situación sospechosa, o incidente de seguridad que comprometa la confidencialidad, integridad y disponibilidad de la información.

El Comité de Seguridad de la Información será el encargado de realizar la investigación y seguimiento a los eventos e incidentes de seguridad reportados.

8.7.4. Política de control de software operacional de La FND.

Generar acciones que permitan preservar la integridad de los sistemas operativos pertenecientes a La Federación Nacional de Departamentos.

Los responsables de la administración de las plataformas de producción estarán obligados a controlar el acceso y uso de los programas fuente, el acceso a los archivos de los sistemas y/o a las aplicaciones que operan en ellas, así como a la programación de las actualizaciones necesarias a realizar.

No se permitirá la instalación de herramientas de desarrollo ni programas fuente en los sistemas de producción, a menos que sea autorizado por el Comité de Seguridad de la información y la Gerencia de Tecnología.

No se permitirá el uso de versiones de software en los sistemas de información misionales en el ambiente de producción que no sean soportadas por los fabricantes, ni versiones de prueba que no hayan sido liberadas al mercado (Beta), a menos que sea autorizado por el Comité de Seguridad de la Información y/o la Gerencia de Tecnología.

8.7.5. Política de gestión de vulnerabilidades

La Federación Nacional de Departamentos, deberá implementar los lineamientos para gestión de vulnerabilidades.

Una vez identificadas las vulnerabilidades técnicas potenciales, La Federación Nacional de Departamentos, identificará los riesgos asociados y los controles de seguridad a ser tenidos en cuenta (esta acción puede implicar la actualización de sistemas vulnerables y/o aplicación de las medidas de acción necesarias).

El Comité de Seguridad de la información realizará el seguimiento y verificación de que se hayan corregido las vulnerabilidades identificadas.

8.8. SEGURIDAD DE LAS TELECOMUNICACIONES

Implementar mecanismos de control que permitan mantener la disponibilidad de las redes de datos, sistemas de comunicaciones e instalaciones de procesamiento (área de operaciones) de La Federación Nacional de Departamentos.

La Federación Nacional de Departamentos a través del Comité de Seguridad de la información, identificará los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión sobre los servicios de red, incluyendo los mismos en los contratos establecidos con sus contratistas.

8.8.1. Política para la transferencia de información.

Proteger la información transferida al interior y exterior de La Federación Nacional de Departamentos.

La Gerencia de Tecnología, cuando se utilice el servicio de trasferencia de archivos, realizará el control del uso de sistemas de transferencia de archivos vía sFTP a terceros.

8.8.2. Política Administradores de Sistemas de Información y de uso de correo electrónico

Definir las pautas generales para asegurar una adecuada protección de la información de La Federación Nacional de Departamentos, en el uso del servicio de correo electrónico por parte de los usuarios autorizados.

El personal de la Gerencia de Tecnología, no debe dar a conocer a terceros, los usuarios y claves que por sus labores le han sido suministradas, e los sistemas de información, plataformas de gestión y monitoreo, sin previa autorización del Gerente de Tecnología.

Los usuarios y claves de los administradores de sistemas y del personal de la Gerencia de Tecnología son de uso personal e intransferible.

El personal de la Gerencia de Tecnología debe emplear obligatoriamente las claves o contraseñas con un alto nivel de complejidad y utilizar los servicios de autenticación fuerte que posee la FND de acuerdo al rol asignado.

Los administradores de los sistemas de información deben seguir las políticas de cambio de clave y utilizar procedimientos de salvaguarda o custodia de las claves o contraseñas en un sitio seguro. A este lugar solo debe tener acceso el Gerente de Tecnología, el Asesor o colaborador para la de Seguridad de la Información.

Se prohíbe enviar o reenviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad de las personas, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral, las buenas costumbres y/o que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluido el lavado de activos.

La cuenta de correo electrónico deberá ser usada para el desempeño de las funciones asignadas dentro de La Federación Nacional de Departamentos.

Los mensajes y la información contenida en los buzones de correo son de propiedad de La Federación Nacional de Departamentos. El usuario podrá crear un histórico de su correo siempre y cuando sea almacenado en el disco duro del usuario y bajo su propia responsabilidad.

8.8.3. Política de uso de mensajería instantánea y redes sociales

La Federación Nacional de Departamentos define las pautas generales para asegurar una adecuada protección de la información, en el uso del servicio de mensajería instantánea y de las redes sociales, por parte de los usuarios autorizados.

La información que se publique o divulgue por cualquier medio de Internet, de cualquier funcionario, contratista o colaborador de La Federación Nacional de Departamentos, que sea creado a nombre personal en redes sociales como: twitter®, facebook®, youtube®, likedink®, blogs, instagram, etc, se considera fuera del alcance de las políticas establecidas y por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado.

Toda información distribuida en las redes sociales que sea originada por la Entidad, debe ser autorizada por los jefes de área para ser socializadas, utilizando un vocabulario institucional.

8.9. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Garantizar que la seguridad es parte integral de los sistemas de información.

El Desarrollo de tecnologías informáticas se debe orientar sobre herramientas basadas en tecnologías de última generación, que permitan la portabilidad y escalabilidad de las aplicaciones.

La supervisión y seguimiento a proyectos de infraestructura informática, deben incorporar como un elemento básico de la supervisión, el cumplimiento de la aplicación de políticas de seguridad tanto en el desarrollo de la solución como en el producto final que será entregado a la Entidad.

Todos los desarrollos de software deben surtir una fase de pruebas de funcionalidad en la cual se evidencien los controles establecidos en relación con la integridad de la información que será ingresada una vez se lleve a cabo su implementación.

Los desarrollos de software deben involucrar la correspondiente documentación interna y externa que permitan identificar su seguimiento hasta el nivel de rutinas y procedimientos.

8.10. RELACIONES CON PROVEEDORESY TERCEROS

8.10.1. Política de Tercerización u Outsourcing

Se deben establecer mecanismos de control en las relaciones contractuales, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por los proveedores o contratistas, cumplan con las políticas de seguridad de la información de La Federación Nacional de Departamentos, las cuales deben se divulgadas por los trabajadores responsables de la realización y/o firma de contratos o convenios.

En los contratos o acuerdos con los proveedores y/o contratistas se debe incluir una causal de terminación del acuerdo o contrato de servicios, por el no cumplimiento de las políticas de seguridad de la información.

Los contratistas, oferentes y/o proveedores deben aceptar y firmar el acuerdo de confidencialidad establecido por La Federación Nacional de Departamentos.

Se deben identificar los riesgos para la información y los servicios de procesamiento de información (operaciones) que involucren partes externas a La Federación Nacional de Departamentos.

El resultado del análisis de riesgos será la base para el establecimiento de los controles y debe ser presentado al Comité de seguridad de la Información antes iniciar el estudio de mercado e invitación o publicación del proyecto de pliegos del contrato de outsourcing en el portal de contratación.

Los trabajadores de La Federación Nacional de Departamentos que fungen como supervisores de contratos relacionados con sistemas de información deberán realizar seguimiento, control y revisión de los servicios suministrados por los proveedores y/o contratistas.

8.11. GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN

Asegurar que los eventos e incidentes de seguridad que se presenten con los activos de información, sean comunicados y atendidos oportunamente, empleando los procedimientos definidos, con el fin de ejecutar oportunamente las acciones correctivas.

- Los trabajadores y contratistas de La Federación Nacional de Departamentos, deberán informar inmediatamente al Comité de Seguridad de la Información cualquier situación sospechosa, o incidente de seguridad que comprometa la confidencialidad, integridad y disponibilidad de la información.
- El Comité de Seguridad de la Información será el encargado de realizar la investigación y seguimiento a los eventos e incidentes de seguridad reportados.
- Todos los incidentes de seguridad reportados serán investigados y se les hará seguimiento por parte del Comité de Seguridad de la Información. Los resultados de las investigaciones serán informados a Dirección/ Comité directivo/, especificando las causas, consecuencias, responsabilidades, solución y acciones para evitar que se presenten nuevamente.

8.12. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Es el conjunto de procedimientos y estrategias definidos para contrarrestar las interrupciones en las actividades misionales de la FND, para proteger sus procesos críticos contra fallas mayores en los sistemas de información, principalmente, misionales o contra desastres y asegurar que las operaciones se recuperen oportuna y ordenadamente, generando un impacto mínimo o nulo ante una contingencia. Prevenir interrupciones en las actividades de la plataforma Tecnológica de La Federación Nacional de Departamentos que van en detrimento de los procesos críticos de Tecnología de la Información afectados por situaciones no previstas o desastres.

- Si la alta dirección lo considera necesario, se debe desarrollar e implantar un Plan de Continuidad para asegurar que los procesos misionales apoyados en las Tecnologías de la Información y las comunicaciones de La Federación Nacional de Departamentos podrán ser restaurados dentro de escalas de tiempo razonables.
- Federación Nacional de Departamentos, si la alta dirección lo considera necesario, deberá tener definido un plan de acción que permita mantener la continuidad del negocio teniendo en cuenta los siguientes aspectos:
- La Identificación y asignación de prioridades a los procesos críticos apoyados en las Tecnologías de la Información y las comunicaciones de La Federación Nacional de Departamentos de acuerdo con su impacto en el cumplimiento de la misión de la Entidad.
- Documentación de la estrategia de continuidad del negocio.
- Documentación del plan de recuperación del negocio de acuerdo con la estrategia definida anteriormente.
- Plan de pruebas de la estrategia de continuidad del negocio.

La alta dirección de La Federación Nacional de Departamentos, si lo considera necesario, se encargará de la definición y actualización de las normas, políticas, procedimientos y estándares relacionados con la continuidad del negocio, igualmente velará por la implantación y cumplimiento de las mismas.

8.13. CUMPLIMIENTO

Los diferentes aspectos contemplados en este documento son de obligatorio cumplimiento para todos los trabajadores, personal en comisión permanente, contratistas y otros colaboradores de La Federación Nacional de Departamentos. En caso de que se violen las políticas de seguridad ya sea de forma intencional o por negligencia, La Federación Nacional de Departamentos tomará las acciones disciplinarias y legales correspondientes.

8.13.1. Política de tratamiento de datos personales

La Federación Nacional de Departamentos, en cumplimiento de la Ley 1581 de 2012 y sus decretos reglamentarios, es el responsable del tratamiento de los datos y serán utilizados para el desarrollo directo de su objeto social. Si requiere mayor información puede consultar en nuestra página www.fnd.org.co, en la opción del menú “Transparencia”: Protección de Datos Personales.

8.13.2. Política de cumplimiento de requisitos legales y contractuales

La Federación Nacional de Departamentos respeta y acata las normas legales existentes relacionadas con seguridad de la información, para lo cual realizará una continua revisión, identificación, documentación y cumplimiento de la legislación y requisitos contractuales aplicables para la Entidad, relacionada con la seguridad de la información.

La Gerencia de Tecnología deberá garantizar que todo el software que se utilice y los activos de información de La Federación Nacional de Departamentos que estén protegidos por derechos de autor y requiera licencia de uso o sea software de libre distribución en cualquiera de los casos, se tenga la respectiva licencia o servicio por su uso.

- La Gerencia de Tecnología realizará el procedimiento de copias de respaldo (backups) de los registros y/o información alojados en los sistemas de información misionales o cuando los servicios sean tercerizados se deberá verificar que se realice los respectivos respaldos. .
- Las Dependencias de La Federación Nacional de Departamentos que tratan con datos personales de trabajadores, proveedores, contratistas, u otras personas deben obtener la autorización para el tratamiento de datos personales que permita recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de la Entidad, así mismo los Jefes de las dependencias deben asegurar que tendrán acceso a los datos personales únicamente los trabajadores que tengan una necesidad laboral legitima.

8.13.3. Política de Revisiones de Seguridad de la Información

Garantizar la aplicabilidad de las políticas y procedimientos implementados en La Federación Nacional de Departamentos.

Los Altos Directivos, Directores, subdirectores, Secretarios, Jefes de oficina y/o áreas, gerente, coordinadores, deben verificar y supervisar el cumplimiento de las políticas de seguridad de la información en su área de responsabilidad.

8.14. POLÍTICA ANTISOBORNO FND

La Federación Nacional de Departamentos, considera fundamental la identificación de los diferentes riesgos de soborno, corrupción y fraude que se puedan presentar al interior de la entidad, de manera que se puedan adelantar las acciones de control requeridas para impedir que se lleven a cabo por parte de sus directivos, empleados, contratistas, proveedores o por cualquier tercero con el que se tenga algún tipo de relación.

8.14.1. Identificación de puntos críticos – Metodología Antisoborno FND

La Federación Nacional de Departamentos realizará el análisis de los principales puntos críticos asociados a cada uno de sus procesos, especialmente aquellos que son más vulnerables a la corrupción como el área jurídica y contractual, talento humano, atención a la ciudadanía, presupuesto y financiera y control interno.

Para la identificación de estos puntos críticos, las áreas deben tener en cuenta fuentes de información como los informes de los entes de control, los resultados del Índice de Transparencia (ITA), resultados del FURAG y autoevaluación de los procesos. Lo anterior, con el fin de identificar las zonas de opacidad o vacíos institucionales que aumentan el riesgo de materialización de prácticas como el soborno, el fraude, etc.

La Federación Nacional de Departamentos implementa medidas de control para prevenir o mitigar la materialización de riesgos de corrupción asociados con el soborno y fraude, entre estos están los siguientes:

- Revisión de los flujos de caja y transacciones financieras realizadas por la entidad.
- Evaluar la respuesta de la entidad desde su institucionalidad ante posibles escenarios de soborno.
- Evaluar las medidas anticorrupción implementadas, y su cumplimiento y conformidad con el Estatuto Anticorrupción (Ley 1474 de 2011) y la legislación aplicable en cada proceso.
- Auditar el área específica bajo riesgo de soborno de manera individualizada.

8.15. POLÍTICA DE SEGURIDAD POST PANDEMIA COVID 19

La Federación Nacional de Departamentos entiende que la seguridad cibernética post pandemia es una realidad con la cual debemos vivir, por lo que considera necesario implementar medidas acordes con lo acontecido, como adoptar una infraestructura tecnológica robusta que contenga medidas más exigentes de ciberseguridad.

La FND ha ido asumiendo rápidos cambios que ha traído la pandemia, por ello ha venido y continua en el proceso de adaptarse a las nuevas necesidades, incluido el movimiento de una gran parte de la fuerza laboral hacia el trabajo en casa.

8.15.1. Teletrabajo

El artículo 2 de la Ley 1221 de 2008 lo define de la siguiente manera: Es una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y la comunicación – TIC para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo.

8.15.1.1. Modalidades de Teletrabajo

- Autónomos: son aquellos que utilizan su propio domicilio o un lugar escogido para desarrollar su actividad profesional, puede ser una pequeña oficina, un local comercial. En este tipo se encuentran las personas que trabajan siempre fuera de la empresa y sólo acuden a la oficina en algunas ocasiones.
- Móviles: son aquellos teletrabajadores que no tienen un lugar de trabajo establecido y cuyas herramientas primordiales para desarrollar sus actividades profesionales son las Tecnologías de la Información y la comunicación, en dispositivos móviles.
- Suplementarios: son aquellos teletrabajadores que laboran dos o tres días a la semana en su casa y el resto del tiempo lo hacen en una oficina.

8.15.1.2. Pasos para implementar el Teletrabajo

Se debe solicitar a MinTIC una asesoría de implementación. La metodología de implementación se hace en los siguientes pasos fundamentales:

- Compromiso institucional (querer hacerlo)
- Planeación (organizar el proceso - cronograma)
- Autoevaluación (revisión interna frente a los recursos humanos, técnicos, jurídicos y tecnológicos con los que cuenta la organización)
- Adopción e implementación

8.15.2. Trabajo en Casa

De acuerdo al artículo 2 de la Ley 2028 de 2021: Se entiende como trabajo en casa la habilitación al servidor público o trabajador del sector privado para desempeñar transitoriamente sus funciones o actividades laborales por fuera del sitio donde habitualmente las realiza, sin modificar la naturaleza del contrato o relación laboral, o legal y reglamentaria respectiva, ni tampoco desmejorar las condiciones del contrato laboral, cuando se presenten circunstancias ocasionales, excepcionales o especiales que impidan que el trabajador pueda realizar sus funciones en su lugar de trabajo, privilegiando el uso de las tecnologías de la información y las comunicaciones.

Este no se limita al trabajo que puede ser realizado mediante tecnologías de la información y las comunicaciones, medios informáticos o análogos, sino que se extiende a cualquier tipo de trabajo o labor que no requiera la presencia física del trabajador o funcionario en las instalaciones de la empresa o entidad.

8.15.3. Soluciones de trabajo en Casa

Anticipando un aumento permanente en el trabajo en casa, la FND debe considerar:

- Procurar suficiente ancho de banda bajo demanda para mover contenido, especialmente videoconferencia, a través y entre sitios geográficamente dispersos.

- Administrar la identidad y el acceso de una fuerza laboral remota que cumpla con los requisitos de seguridad corporativos y las necesidades de facilidad de uso de los colaboradores.
- Implementación de soluciones de administración de dispositivos móviles para abordar el uso de dispositivos móviles personales aprobados y emitidos por la entidad para fines administrativos.
- Protección de los derechos de propiedad intelectual de la organización, tanto por el software como por otros contenidos que puedan estar protegidos por derechos de propiedad intelectual.
- Proceso de devolución de datos y equipamiento en caso de finalización del empleo.
- Garantizar la protección de la información confidencial y estrictamente confidencial que se llegue a manejar en trabajo en casa debido al ejercicio de las labores.
- Evitar compartir con otros usuarios el computador o si es estrictamente necesario crear un usuario diferente que no tenga acceso a la información que se pueda almacenar en el computador.
- Guardar toda la información en la nube y no dejar archivos en el PC.

8.15.4. Protección perimetral externa

Un incremento en las conexiones remotas puede aumentar la superficie de ciberataque de una organización. Las organizaciones pueden proteger sus perímetros externos mediante:

- Implementación del control de acceso a la red (NAC) para autenticar y validar dispositivos, y aplicar políticas de seguridad antes de permitirles conectarse a redes corporativas en la oficina o remotas.
- Bloquear las estaciones de trabajo de los usuarios y las computadoras portátiles emitidas por la entidad con una configuración de seguridad definida, administrar la configuración de forma centralizada y no asignar privilegios administrativos a los usuarios finales.
- Implementación de capacidades de aislamiento y análisis forense de punto final remoto que cumplan con los requisitos de la cadena de custodia forense.
- Implementar capacidades que admitan la recopilación y el análisis de datos de puntos finales remotos para identificar actividades no autorizadas.

8.15.5. Servicios en la nube

Los servicios en la nube pueden ofrecer importantes costos, eficiencia, resistencia y posibles beneficios de seguridad sobre el almacenamiento de datos y las alternativas de alojamiento de aplicaciones. Pero estos beneficios requieren que los servicios en la nube se adopten y administren de manera deliberada y estratégica. La entidad debe considerar:

- Adoptar estrategias formales para el uso de servicios en la nube.
- Desarrollar inventarios completos del uso actual de la nube en la entidad y racionalizar el uso de múltiples servicios.
- Definir políticas de almacenamiento de datos que describan las condiciones requeridas para el uso de servicios en la nube, almacenamiento en centros de datos y almacenamiento local, particularmente para información confidencial.

8.15.6. Operaciones cibernéticas

El entorno operativo posterior a la pandemia será diferente. La Federación Nacional de Departamento debe considerar:

- Supervisar la recopilación y el análisis central de alertas de ciberseguridad y registros de auditoría para detectar y responder a actividades sospechosas / maliciosas.
- Revisar y actualizar los perfiles de VPN y las reglas de firewall para que los colaboradores reciban los privilegios apropiados que dependen de los roles.
- Implementar o actualizar procesos para obtener la aprobación de los propietarios de datos y sistemas para el aprovisionamiento y desprovisionamiento de VPN remotas y otras cuentas asociadas con aplicaciones comerciales críticas.
- Deshabilitar el túnel dividido para los perfiles de VPN para evitar que los colaboradores remotos accedan a Internet directamente desde sus computadoras portátiles personales al mismo tiempo que acceden a los sistemas de información corporativos.
- Crear un mecanismo simple para marcar y reenviar correos electrónicos sospechosos para análisis técnico.
- Aprovisionamiento de soluciones de acceso seguro con capacidad suficiente para el mayor número de usuarios remotos y protección de seguridad en puntos finales.
- Aplicar actualizaciones de software a los dispositivos informáticos emitidos por la entidad y que son de uso de los colaboradores para trabajos remotos.

- Habilitación de la autenticación multifactor para VPN y sistemas de información crítica.
- Aumentar la capacidad de ayuda de IT y las horas de operación para manejar los mayores requisitos de servicio de una fuerza de trabajo remota.

8.15.7. Ciberataques

En época de pandemia, en el mundo han aumentado los ciberataques; Colombia ocupa el puesto número 6 en delitos cibernéticos, se ha identificado en estos últimos tiempos un incremento en la suplantación de sitios Web, en la interceptación de datos informáticos, así como en el delito de daños informáticos.

Medidas preventivas a Implementar

1. Mantener el sistema operativo y las aplicaciones permanentemente actualizadas, procurando las actualizaciones automáticas.
2. Efectuar copia de la información (respaldo) tanto en medios físicos como en la nube.
3. Instalar antivirus y firewalls.
4. Limitar el número de personas que pueden hacer cambios en el sistema operativo.
5. No abrir archivos adjuntos o enlaces, aún de aquellos procedentes de fuentes de confianza como bancos o tiendas online.
6. Mantener la confidencialidad de las contraseñas y cambiarlas cada 3 meses, las cuales deberán contar al menos con 8 caracteres, incluyendo números y letras (mayúsculas y minúsculas).
7. Cerrar las sesiones al terminar de trabajar.
8. Cuidar la información que se comparte, particularmente en las redes sociales.

Acciones a ejecutar en caso de un Ciberataque

- No pagar rescate porque se financia a los criminales y no siempre se recuperan los archivos secuestrados. Además, en muchos casos, sólo se recibe la clave para poder desencriptar la información, pero no erradica la amenaza al no borrar o limpiar permanentemente el virus del ordenador infectado, lo que permite a los piratas atacar nuestra información cuantas veces quieran y mantener a la misma como rehén en más de una ocasión.
- Avisar a las autoridades y guardar copia del correo electrónico infectado.
- Desconectar el dispositivo para evitar la propagación.
- Formatear el disco duro.
- Reinstalar el sistema y las aplicaciones, ejecutando las actualizaciones disponibles.

- Restaurar los archivos bloqueados a partir de copias de seguridad.

La Federación Nacional de Departamentos en aras de conservar la finalidad de la información, deber crear una cultura de protección, ya que las amenazas de nuevos ataques cibernéticos estarán siempre latentes en el entorno digital. Las modalidades de tales ataques son un fenómeno cambiante y cada vez serán más complejas y dañinas. Esta actividad ilegal y nociva representa un grave riesgo económico para las organizaciones. Por ello es indispensable crear una cultura de protección entre los usuarios de los sistemas informáticos, ya que cualquier inversión en infraestructura y sistemas de protección resultará inútil sin capacitación en el tema de la seguridad.

DIDIER ~~TAVERA AMADO~~

Director Ejecutivo FND

Elaboró: Colaboradores Proceso GTE

Reviso: Gerente de Tecnología

Aprobó: Comité de Gestión y desempeño

9. CONTROL DE CAMBIOS

No. Versión	Ítem del cambio	Motivo del cambio	Fecha del cambio
1	Versión inicial del documento	Elaboración de la política	05/10/2018
2	General. Se tienen en cuenta requisitos para ISO 27001	Actualización de la política	16/12/2022

10. CONTROL DE CAMBIOS

Elaboró: Colaboradores proceso GTE **Fecha:** 21/09/2022	**Revisó:** Secretaria Privada Dirección Ejecutiva. **Fecha:** 21/10/2022 **Revisó:** Colaborador SIG/Oficina de Planeación **Fecha:** 20/12/2022	**Aprobó**: Comité de Gestión y Desempeño **Fecha:** 21/10/2022