# PROCESO: GESTIÓN DE SERVICIOS DE TI
# MANUAL DE MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## OBJETIVO:

Establecer la política general de seguridad de la Información, alcance, condiciones generales y lineamientos adicionales, las cuales son de obligatorio cumplimiento para las personas que laboran en el FONCEP independiente de su tipo de vinculación, alineada con la estrategia de Gobierno Digital, adoptadas para salvaguardar la Información como activo fundamental de la Entidad.

## ALCANCE:

Aplica a todos los procesos por ser de carácter institucional.

## NORMATIVIDAD:

- **Junta Directiva Sesión No. 12 del 17 de Noviembre de 2021** "Por medio del cual se aprueba la Política General de Seguridad de la información del Manual de Modelo de Seguridad y Privacidad de la Información."
- **Decreto 807 de 2019** "Por medio del cual se reglamenta el Sistema de Gestión en el Distrito Capital y se dictan otras disposiciones"
- **Ley 1755 de 2015** "Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo"
- **Decreto 103 de 2015** "Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones".
- **Decreto 368 de 2014** "Por el cual se reglamentan las operaciones mediante sistemas de financiación previstas en el artículo 45 de la Ley 1480 de 2011".
- **Decreto 886 de 2014** "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos".
- **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".
- **Decreto 2573 de 12 diciembre de 2014** "Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones"
- **Decreto 1377 de 2013** "Por el cual se reglamenta parcialmente la Ley 1581 de 2012".
- **Ley 1581 de 2012** "Por la cual se dictan disposiciones generales para la protección de datos personales".
- **Decreto 2952 de 2010** "Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008".



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

ALCALDÍA MAYOR DE BOGOTÁ D.C.
FONDO DE PRESTACIONES ECONÓMICAS, CESANTÍAS Y PENSIONES

- **Ley 1273 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 y las comunicaciones, entre otras disposiciones".
- **Resolución 305 de 2008** "Por la cual se expiden políticas públicas para las Entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre."
- **Ley 1266 de 2008** "Por la cual se dictan las disposiciones generales del hábeas 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".
- **Sentencias de la Corte Constitucional: C-1011 de 2008** "Por la cual se dictan las disposiciones generales del hábeas 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"
- **NORMA TÉCNICA NTC-ISO-IEC COLOMBIANA 27001** "Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos"
- **NORMA TÉCNICA NTC-ISO-IEC COLOMBIANA 27002** "Tecnología de la información. Técnicas de seguridad. Código de practica para la gestión de la seguridad de la información"
- **Constitución Política 1991** "Artículos 15, 20 y 74 sobre acceso a la información"
- **Ley 527 de 1991** "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 establecen las Entidades de certificación y se dictan otras disposiciones".

| **DEFINICIONES** |
|---|
| **Término – Definición** |
| **Activo:** Se denomina activo a aquello que tiene algún valor para la Entidad y por tanto debe protegerse. |
| **Administración remota:** Funcionalidad de algunos programas que permiten realizar ciertos tipos de acciones desde un equipo local y que las mismas se ejecuten en otro equipo remoto. |
| **Amenaza:** Son códigos diseñados por ciberdelincuentes cuyo objetivo es el de variar el funcionamiento de cualquier sistema informático, sobre todo sin que el usuario infectado se dé cuenta. |
| **Archivo log:** Grabación secuencial en un archivo o en una base de datos de todos los acontecimientos (eventos o acciones) que afectan a un proceso particular (aplicación, actividad de una red informática, etc.). De esta forma constituye una evidencia del comportamiento del sistema. |
| **Ataque:** Método por el cual un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático (ordenador, red privada, etcétera). |



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

| |
|---|
| **Aviso de Privacidad:** Comunicación verbal o escrita generada por el responsable, dirigida al Titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades que se pretende dar a los datos personales. |
| **Base de Datos:** Conjunto organizado de datos personales que sea objeto de tratamiento. |
| **Cifrado:** Es una solución de seguridad versátil: puede aplicarse a datos como una contraseña, o de forma más amplia, a datos de un archivo o incluso a datos contenidos en medios de almacenamiento. |
| **Confidencialidad:** Garantía de que la información personal será protegida para que no sea divulgada sin consentimiento de la persona. Dicha garantía se lleva a cabo por medio de un grupo de reglas que limitan el acceso a esta información. |
| **Contingencia:** Modo de ser de lo que no es necesario ni imposible, sino que puede ser o no ser el caso. En general la contingencia se predica de los estados de cosas, los hechos, los eventos o las proposiciones. |
| **Cuenta:** Colección de información que indica al sistema operativo los archivos y carpetas a los que puede tener acceso un determinado usuario del equipo, los cambios que puede realizar en él y sus preferencias personales, como el fondo de escritorio o el protector de pantalla. |
| **Dato Personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. |
| **Dato Sensible:** Información que afecta la intimidad de las personas o cuyo uso indebido puede generar discriminación (origen racial o étnico, orientación política, convicciones filosóficas o religiosas, pertinencia a sindicatos u organizaciones sociales o derechos humanos, datos de salud, vida sexual y biométricos). |
| **Disponibilidad:** Es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. |
| **Encargado del tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del Tratamiento. En los eventos en que el responsable no ejerza como Encargado de la base de datos, se identificará expresamente quién será el Encargado. |
| **GPO:** Group Policy Object o directiva de grupo es un conjunto de reglas que controlan el entorno de trabajo de cuentas de usuario y cuentas de equipo. Tomado de: https://www.techopedia.com/definition/12818/group-policy-object-gpo. |
| **Información:** Conjunto organizado de datos procesados, que constituyen un mensaje. |
| **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. |
| **MSPI:** Modelo de Seguridad y Privacidad de la Información. |
| **Periféricos:** es un dispositivo externo al ordenador que está conectado a el pero que no es parte del equipo principal y que permite la entrada y salida de información desde o hacia el propio ordenador. En resumen, son dispositivos que se conectan al ordenador para meter o sacar información. Tomado de: https://www.areatecnologia.com/informatica/perifericos.html. |
| **Responsable del tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos. El Encargado es el que realice el tratamiento de los datos personales por cuenta del Responsable. Tomado de: https://www.sic.gov.co/preguntas-frecuentes-pdp#:~:text=El%20Responsable%20del%20Tratamiento%20de,personales%20por%20cuenta%20del%20Responsable. |
| **Titular:** Persona natural o jurídica cuyos datos sean objeto de tratamiento. |



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

ALCALDÍA MAYOR DE BOGOTÁ D.C.
FONDO DE PRESTACIONES ECONÓMICAS, CESANTÍAS Y PENSIONES

| |
|---|
| **Transferencia:** La transferencia de datos tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país. |
| **Transmisión:** Tratamiento de datos personales que implica la comunicación de estos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento por el encargado por cuenta del responsable. |
| **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. |



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

ALCALDÍA MAYOR DE BOGOTÁ D.C.
FONDO DE PRESTACIONES ECONÓMICAS, CESANTÍAS Y PENSIONES

**CONTENIDO:**





**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

ALCALDÍA MAYOR DE BOGOTÁ D.C.
FONDO DE PRESTACIONES ECONÓMICAS, CESANTÍAS Y PENSIONES

**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

ALCALDÍA MAYOR DE BOGOTÁ D.C.
FONDO DE PRESTACIONES ECONÓMICAS, CESANTÍAS Y PENSIONES

**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

## DESARROLLO DEL MANUAL:

### Introducción

Este documento se elaboró con la recopilación de los lineamientos necesarios para el cumplimiento de la Política general de la seguridad de la información, contempla los roles y responsabilidades, dado que El FONDO DE PRESTACIONES ECONOMICAS, CESANTIAS Y PENSIONES – FONCEP es consciente que la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de la protección de la confidencialidad, integridad y disponibilidad, así como la administración y priorización de los riesgos de seguridad digital, continuidad de negocio y la consolidación de una cultura de seguridad al interior de la Entidad.

Por ello, es importante aclarar que la información es el activo más importante de una organización y adopta diferentes formas como: impresa, escrita, papel, digital, correo electrónico, páginas web, archivos magnéticos, sistemas de información, videos, o conversaciones como medio fundamental de la comunicación del ser humano.

Por su naturaleza, importancia y disponibilidad de la información, cada día está más expuesta a amenazas y vulnerabilidades, por lo tanto, la seguridad de la información es la protección de la información contra una amplia gama de amenazas; para minimizar los daños y garantizar la continuidad del negocio.

El propósito de la seguridad y privacidad de la información no es garantizar que no se presenten vulnerabilidades, sino garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización en forma sistemática, estructurada, continua, repetible, eficiente, adaptada a los cambios que se produzcan en la organización y con los soportes documentales apropiados.

Además, establece mediante la implementación de un conjunto adecuado de lineamientos, procesos, procedimientos de la organización, controles, hardware y software; pero lo más importante, mediante comportamientos éticos de las personas. Y busca la preservación de los principios básicos de la confidencialidad, integridad y disponibilidad de esta y de los sistemas implicados en su tratamiento.



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

ALCALDÍA MAYOR DE BOGOTÁ D.C.
FONDO DE PRESTACIONES ECONÓMICAS, CESANTÍAS Y PENSIONES

La dirección como máxima autoridad dentro de la organización, debe establecer de forma clara las líneas de actuación y manifestar su apoyo y compromiso incondicional a la seguridad de la información, con el fin de garantizar su implementación en toda la organización y sus procesos.

El tal sentido, la Entidad en cumplimiento de las revisiones permanentes que se debe realizar a la política y al compromiso que tiene para el proceso de implementación del Modelo de Seguridad y Privacidad de la Información (MSPI).

## 1. Política general de seguridad de la información

El Fondo de Prestaciones Económicas, Cesantías y Pensiones – FONCEP, como Entidad responsable del pago de cesantías, reconocimiento y pago de pensiones a las servidoras y servidores públicos del Distrito Capital, con régimen de retroactividad, afiliados al FONCEP, gestiona, normaliza, cobra y recauda la cartera hipotecaria del Fondo de Ahorro y Vivienda Distrital – FAVIDI; es consciente que la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de la protección de la confidencialidad, integridad y disponibilidad, así como la administración de riesgos de seguridad digital, continuidad de negocio y la consolidación de una cultura de seguridad al interior de la Entidad.

Por lo tanto, todas las personas naturales y jurídicas que laboran en el FONDO DE PRESTACIONES ECONOMICAS, CESANTIAS Y PENSIONES – FONCEP, serán responsables por el cumplimiento de las políticas, controles, normas, procedimientos y estándares vigentes respecto a la seguridad de la información, permitiendo a la Entidad, identificar y minimizar los riesgos a los cuales se expone su información y establecer una cultura de seguridad que garantice el cumplimiento de los requerimientos legales, contractuales y técnicos mediante la adopción de las mejores prácticas.

La Política general de seguridad de la información de FONCEP se encuentra soportada por lineamientos, normas y procedimientos específicos los cuales guían la gestión adecuada de la información.

Lo anterior fue socializado en el Comité institucional de Gestión y Desempeño No. 03 de 2021 y aprobado en la Junta Directiva Sesión No. 12 del 17 de Noviembre de 2021.



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

## 2. Alcance de la política de seguridad de la información

La política de seguridad de la información del FONDO DE PRESTACIONES ECONOMICAS, CESANTIAS Y PENSIONES – FONCEP y sus lineamientos, están dirigidas a:

1. Todas las personas vinculadas al FONCEP como funcionario de carrera administrativa, libre nombramiento y remoción, provisionalidad, temporalidad, contratista y pasante; así como al personal vinculado con firmas que prestan servicios al FONCEP y visitantes.
2. Todos los recursos y activos de información de la Entidad.
3. Todos los procesos y procedimientos de la Entidad.
4. Toda la infraestructura tecnológica y los sistemas de información que soportan la funcionalidad de la Entidad y todas las sedes físicas de la Entidad.

## 3. Nivel de cumplimiento

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

## 4. Objetivo general de la política de seguridad de la información

Cumplir con los requisitos de seguridad, definidos en el Modelo de Seguridad y Privacidad de la Información de la Política de Gobierno Digital, que ayudan, mediante su implementación y aplicación, a preservar la confidencialidad, integridad y disponibilidad de la información, así como la relación de los procedimientos asociados a los lineamientos establecidos que permitan asegurar la protección y persistencia de esta.

## 5. Objetivos específicos de seguridad de la información

1. Dar lineamiento para la implementación y aplicación de la gestión de la seguridad y privacidad de la información.
2. Generar una cultura y apropiación de trabajo enfocada a la toma de conciencia para la protección y el uso adecuado de la



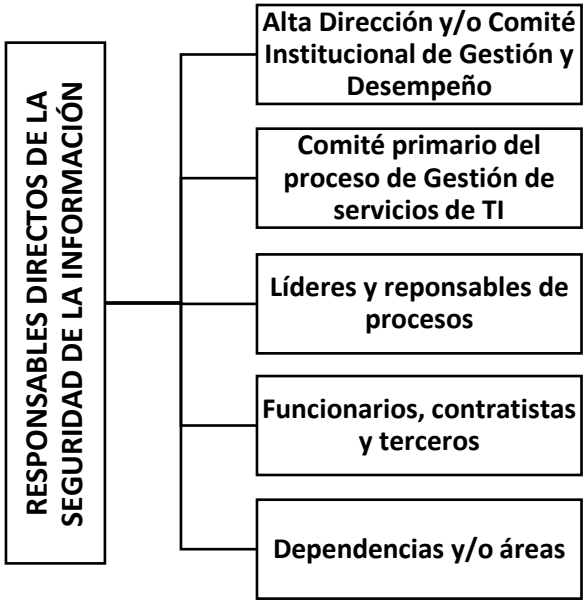
**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

ALCALDÍA MAYOR DE BOGOTÁ D.C.
FONDO DE PRESTACIONES ECONÓMICAS, CESANTÍAS Y PENSIONES

información por parte de los servidores públicos, contratistas y colaboradores de FONCEP.
3. Asegurar que los riesgos asociados a seguridad digital estén alineados con la metodología del Manual de gestión de los riesgos.
4. Mantener un enfoque de cumplimiento estricto de los requisitos legales, normativos o contractuales aplicables y relativos al tratamiento y protección de la información.

## 5. Roles y responsabilidades generales de la seguridad de la información

La asignación y delimitación de responsabilidades para asegurar que se aplican los objetivos propuestos en la presente Política de Seguridad de la información para FONCEP; requieren del establecimiento de unas determinadas funciones encargadas de los aspectos generales de gestión de la seguridad de la información. Los siguientes entes son responsables, en distintos grados, frente a la seguridad de la información en FONCEP:






**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

ALCALDÍA MAYOR DE BOGOTÁ D.C.
FONDO DE PRESTACIONES ECONÓMICAS, CESANTÍAS Y PENSIONES

| Roles | Responsabilidades y Funciones |
|---|---|
| **Alta Dirección y/o Comité Institucional de Gestión y Desempeño** | • Garantizar que la seguridad de la información tenga los lineamientos necesarios y pertinentes para la protección de los activos de información y se apliquen en la Entidad.<br>• Velar por la protección de la información que se gestiona en las dependencias, vigilando en primera instancia la propia de acuerdo con las políticas y normas de seguridad de la información del FONCEP, al igual que realizar el levantamiento de los activos de información de cada una de sus áreas y/o dependencias.<br>• La Dirección General es la encargada de dar los lineamientos de la política de seguridad de la información y delega las responsabilidades de documentación sobre seguridad de la información a la persona responsable quien se apoya en la Oficina de Informática y Sistemas para las definiciones y modificaciones que pueda requerir esta política con el trascurso del tiempo.<br>• Cualquier cambio a la política debe ser revisada por la Dirección General, Líder de Proceso de gestión de servicios de TI y Oficial de Seguridad Informática, en los acasos que aplique, y aprobada mediante las disposiciones del procedimiento de administración de los elementos de planeación y gestión que establece la Entidad.<br>• Aprobar el Plan de Acción Institucional, el cual contiene los planes de continuidad, seguridad y privacidad de la información, tratamiento de riesgos de seguridad de la información, actividades relacionadas con políticas de gobierno digital y seguridad digital.<br>• Apoyar y poner a disposición los recursos necesarios para la implementación y aplicación del Modelo MSPI. |
| **Comité primario del proceso de Gestión de servicios de TI** | • Está encargado de dar los lineamientos y metodologías para elaborar y actualizar las políticas, normas, pautas y procedimientos relativos a seguridad de la información.<br>• Responsable de coordinar el análisis de riesgos, indicadores estratégicos y de proceso, seguimiento a las actividades del Plan de acción Institucional, Plan de seguridad y privacidad de la información, Plan de tratamiento de riesgos de seguridad y privacidad de la información y Plan Estratégico de las Tecnologías de la Información y Comunicaciones.<br>• Efectuar la evaluación y revisión de la situación de FONCEP en cuanto a seguridad de la información, incluyendo el análisis de incidentes ocurridos y que afecten la seguridad. |



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

| Roles | Responsabilidades y Funciones |
|---|---|
| | • Coordinar la implementación y aplicación del Modelo de Seguridad y privacidad de la Información - MSPI.<br>• Velar por la aplicación y cumplimiento de la política de seguridad digital en FONCEP.<br>• Revisar los diagnósticos del estado de la seguridad de la información en Nombre de la Entidad.<br>• Plasmar las necesidades de seguridad.<br>• Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de FONCEP.<br>• Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar, riesgos.<br>• Realizar revisiones periódicas del MSPI y según los resultados de esta revisión definir las acciones pertinentes.<br>• Promover la difusión y sensibilización de la seguridad de la información dentro de la Entidad.<br>• Poner en conocimiento de la Entidad, los documentos generados al interior del proceso de gestión de servicios de TI que impacten de manera transversal a la misma.<br>• Realizar campañas de seguridad de la información para los colaboradores del FONCEP. |
| **Líderes de procesos** | • Realizar la aprobación de cambios referente a los servicios ofrecidos por la Oficina de Informática y Sistemas, así como la definición de usuarios que podrán acceder a los sistemas y los niveles de accesos otorgados a cada usuario para el cumplimiento de sus funciones.<br>• Realizar la identificación y actualización de los activos de información de cada uno de los procesos de la Entidad.<br>• Liderar la actualización de los riesgos de seguridad asociados a su proceso.<br>• Velar por el cumplimiento de los controles establecidos sobre los activos de la información a su cargo.<br>• Realizar seguimiento a las acciones de tratamiento de los riesgos de seguridad de la información a su cargo. |
| **Funcionarios, Contratistas y Terceros** | • Son todos aquellos que prestan algún servicio profesional a la Entidad y que en algunos casos tendrán acceso a la información y a los activos tecnológicos de la Entidad, para la ejecución de sus labores profesionales según los compromisos adquiridos con FONCEP.<br>• En el contrato se estipulan unas cláusulas de confidencialidad con la Entidad cuando requieran conocer, acceder o manejar información confidencial. |

CODIGO DEL FORMATO: FOR-EST-MIP-003
VERSION:007

| Roles | Responsabilidades y Funciones |
|---|---|
| | • Reportar los incidentes de seguridad, eventos sospechosos y/o el mal uso de los recursos institucionales de los cuales tenga conocimiento.<br>• Es responsabilidad de toda persona vinculada a la Entidad conocer y aplicar la política de seguridad de la información. |
| **Dependencias y/o áreas** | • El área de Talento Humano está encargada de la contratación de los profesionales o la vinculación de funcionarios y personal de planta idóneo.<br>• La Oficina Asesora de Jurídica, está encargada de los contratos y validar que en ellos se estipule el cumplimiento de la política general de seguridad de información.<br>• La Oficina de Control Interno valida y comunica la información en los informes trimestrales de los riesgos de la Entidad que sirven de insumo para evaluar las falencias y hacer los ajustes correspondientes, especialmente a los riesgos de seguridad de la información.<br>• La Oficina de Informática y Sistemas como segunda línea de defensa realiza el monitoreo de los riesgos de seguridad de la información para identificar las materializaciones, necesidad de acciones de tratamiento y fortalecer los controles.<br>• La Subdirección Financiera y Administrativa realiza los procesos disciplinarios conforme a el hallazgo o situación de incumplimiento de la política general de seguridad de la información y lineamientos relacionados.<br>• Los jefes de las áreas y/o dependencias de la Entidad son los responsables de definir los roles que se le deben asignar a cada uno de los usuarios de su dependencia, realizar el seguimiento adecuado, solicitar las modificaciones cuando sea necesario y el retiro cuando el usuario deje de pertenecer a la Entidad.<br>• Cada dependencia y/o área verifica y dará uso a los documentos, procedimientos, manuales, instructivos y formatos del proceso de Gestión de servicios de TI. |

## 6. Lineamientos de la política

Adicionalmente se definen los siguientes los lineamientos que se deben cumplir en materia de seguridad de la información:



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

## 6.1. Lineamientos generales

1. El proceso de Gestión de Servicios TI del FONCEP, - es responsable de proporcionar los servicios de TI en forma oportuna, completa y segura logrando que dichos servicios estén protegidos contra accesos no autorizados estableciendo los controles necesarios y mecanismos de control de acceso lógico.
2. El acceso a la información y a los recursos informáticos de la Entidad debe ser solicitado y aprobado por el jefe del área de la dependencia y asignados por la Oficina de Informática y Sistemas, quien entrega las claves respectivas para el adecuado uso de la información y los recursos.
3. Los jefes de las áreas y/o dependencias de la Entidad son los responsables de definir los roles que se le deben asignar a cada uno de los usuarios de su dependencia, realizar el seguimiento adecuado, solicitar las modificaciones cuando sea necesario y el retiro cuando el usuario deje de pertenecer a la Entidad o tenga un cambio de dependencia.
4. Los funcionarios deben dar uso adecuado de los recursos asignados (equipos de cómputo, impresoras, puesto de trabajo, software, entre otros) y/o servicios informáticos (cuentas de usuario, carpetas compartidas, correo electrónico institucional, intranet, internet, datos e información, sistemas de información, entre otros) de acuerdo con las normas y procedimientos establecidos por la Entidad.
5. Los funcionarios deben proteger y no transferir el usuario y la contraseña asignada por la Entidad a otra persona o funcionario, ni utilizar otra cuenta de usuario para el ingreso a los recursos de la Entidad y responder por todas las operaciones efectuadas y la información registrada con esta cuenta de usuario.
6. No se permite conectar a la red o instalar dispositivos (móviles o fijos tales como portátiles, celulares, tabletas, teléfonos inteligentes, enrutadores, agendas electrónicas, puntos de acceso inalámbrico) que no sean autorizados por la Oficina de Informática y Sistemas o el director o jefe del área o dependencia a la quien pertenezca el usuario.
7. La conexión remota a la red de área local de la Entidad debe ser hecha a través de una conexión segura y será solicitada por el jefe del área que la requiera y validada y asignada por la Oficina de Informática y Sistemas. Las condiciones de infraestructura y de seguridad, las proporcionará la Oficina de Informática y Sistemas. En lo posible se debe contar con registros de las conexiones realizadas por los usuarios autorizados.



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

## 6.2. Educación, formación y concientización sobre la seguridad de la información

Existe un programa continuo de concientización en seguridad de la Información, de forma que les permita recibir la capacitación adecuada y periódica, de forma tal que se encuentre en condiciones de comprender el alcance y contenido de las políticas de Seguridad de la información detalladas en este documento y la necesidad de respaldarlas y aplicarlas de manera permanente.

Por ello se establecen campañas de seguridad de la información para comunicar mediante correo electrónico a los colaboradores de FONCEP, la información más relevante en cuanto a navegación segura, salvaguardar la información, incidentes de seguridad, navegación cifrada, ciberamenazas, activos de información, riesgos de seguridad de la información, lectura segura de correo, entre otros, que debe contener un lenguaje claro, sencillo y preciso. Lo anterior, liderado por la Oficina de Informática y Sistemas.

**El profesional de la OIS, trimestralmente asegura que los colaboradores de la Entidad tengan información relacionada con el funcionamiento y uso de las herramientas de Microsoft con las que cuenta la Entidad, mediante comunicaciones de la OIS relacionadas con los sistemas de respaldo ofertados (backup al momento de retiro), recomendación de salvaguardar archivos de interés institucional, descarga de resultados antes de eliminación del instrumento de recolección y uso de cuentas institucionales para tal fin. En caso de presentarse dudas adicionales por los usuarios se incluyen en las comunicaciones OIS del siguiente trimestre. La evidencia son las comunicaciones enviadas a los colaboradores de la Entidad por los medios oficiales acordados.** 🔍

## 6.3 Tratamiento de datos personales

Los lineamientos de tratamiento y protección de Datos Personales presentados a continuación se aplican a todos los archivos que contengan datos personales que sean objeto de tratamiento por FONCEP, considerado como responsable y/o encargado del tratamiento de estos datos.

La política de tratamiento y protección de Datos Personales debe ser conocida y aplicada por todos las dependencias y colaboradores de FONCEP.



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

ALCALDÍA MAYOR DE BOGOTÁ D.C.
FONDO DE PRESTACIONES ECONÓMICAS, CESANTÍAS Y PENSIONES

### 6.3.1 Principios rectores de tratamiento de datos personales

Para la interpretación e implementación de la presente política, se aplican, de manera armónica e integral, los siguientes principios[1]:

a. **Legalidad**: El Tratamiento de datos es una actividad reglada que debe sujetarse a lo establecido en la Ley 1581 de 2012 y en las demás disposiciones que desarrollen.
b. **Finalidad**: El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular.
c. **Libertad**: El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.
d. **Veracidad o calidad**: La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.
e. **Transparencia**: En el Tratamiento debe garantizarse el derecho del Titular a obtener del Responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.
f. **Acceso y circulación restringida**: El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley.
   Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley.

[1] Fuente: Superintendencia de Industria y Comercio: https://www.sic.gov.co/preguntas-frecuentes-pdp#:~:text=PRINCIPIO%20DE%20FINALIDAD%3A,expreso%20e%20informado%20del%20Titular.



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

g. **Seguridad**: La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
h. **Confidencialidad**: Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de esta.

### 6.3.2 Identificación del responsable y/o encargado del tratamiento de datos personales

El Fondo de Prestaciones Económicas, Cesantías y Pensiones - FONCEP con domicilio en la carrera 6 N. 14-98 Edificio Condominio Parque Santander torre A, Bogotá – Colombia, identificado con el número de identificación tributaria NIT 860041163-8.

Línea gratuita fuera de Bogotá: 018000119929. Disponibles días hábiles de lunes a viernes 7:00 a.m. a 4:00 p.m. Jornada continua.

Línea dentro de Bogotá 307 62 00 Ext. 214. Disponibles días hábiles de lunes a viernes 7:00 a.m. a 4:00 p.m. Jornada continua.

Correo electrónico: servicioalciudadano@foncep.gov.co.

### 6.3.3 Tratamiento y finalidades

El tratamiento que realiza FONCEP será el de recolectar, almacenar, procesar, usar y transmitir o transferir (según corresponda) los datos personales, atendiendo de forma estricta los deberes de seguridad y confidencialidad ordenados por la Ley 1581 de 2012 y el Decreto 1377 de 2013, con las siguientes finalidades:

a. Reconocer y pagar el auxilio de cesantías correspondiente al régimen de retroactividad, a las servidoras y servidores públicos del Distrito Capital afiliados al Fondo.



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

**b.** Pagar las obligaciones pensionales de carácter legal y convencional que por competencia le correspondan al Fondo de Pensiones Públicas de Bogotá, D.C., cuya administración asume conforme a las disposiciones y mecanismos legales establecidos en la normatividad vigente sobre la materia.

Literal adicionado por el artículo 119 del Acuerdo Distrital 645 de 2016.

**a.** Verificar y consolidar la información laboral del Sistema de Seguridad Social en Pensiones de las Entidades del Sector Central y las Entidades descentralizadas a cargo del Fondo de Pensiones Públicas de Bogotá.
**b.** Gestionar, normalizar, cobrar y recaudar la cartera hipotecaria del Fondo de Ahorro y Vivienda Distrital – FAVIDI.
**c.** Cuando FONCEP reciba información que le haya sido transferida por otras Entidades debido a su solicitud le dará el mismo tratamiento de confidencialidad y seguridad que le proporciona a la información producida por FONCEP.

### 6.3.4 Deberes del FONCEP en la protección de los datos personales

**a.** Garantizar al titular el efectivo ejercicio del derecho de Hábeas Data.
**b.** Solicitar y conservar la autorización otorgada por el titular.
**c.** Conservar la información bajo las condiciones de seguridad para impedir su adulteración, perdida, consulta, uso o acceso no autorizado o fraudulento.
**d.** Asegurar que la información sea veraz, completa, exacta, actualizada, comprobable y comprensible.
**e.** Rectificar la información cuando sea incompleta y comunicar lo pertinente al responsable del tratamiento de los datos.
**f.** Tramitar las consultas y reclamos formulados en los términos señalados en la presente política.

### 6.3.5 Lineamientos para la actualización, rectificación, supresión de datos y revocación de la autorización de tratamiento de datos personales

De conformidad con lo previsto en el artículo 15 de la Ley 1581 de 2012, los titulares que consideren que la información contenida en una base de datos debe ser objeto de actualización, rectificación o supresión de datos, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la ley 1581 de 2012, podrán presentar un reclamo ante FONCEP, el cual será tramitado bajo cualquiera de los siguientes parámetros:



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

- El reclamo se realizará mediante solicitud dirigida a FONCEP con la identificación del titular, descripción de los hechos que dan lugar al reclamo, la dirección y los documentos que soporten la reclamación. Si el reclamo resulta incompleto se requerirá al interesado dentro de los (5) días siguientes a la radicación de este, para que subsane las fallas. Transcurridos 2 meses desde la fecha del requerimiento sin que el solicitante presente la información requerida, se dará por entendido que ha desistido de la solicitud.

- Una vez recibido el reclamo completo se incluirá en la(s) base(s) de dato(s) respectivas una leyenda que indique que el reclamo se encuentra en trámite y el motivo de este, en un término no mayor a dos (2) días hábiles.

- El término máximo para su atención será de quince (15) días hábiles a partir de la radicación de este, en caso de que no sea posible atender el reclamo se informará al peticionario, este tiempo no podrá exceder por ningún motivo los ocho (8) días hábiles siguientes al vencimiento del primer término.

### 6.3.6 Derechos del titular de los datos personales

De acuerdo con lo previsto por la normatividad vigente aplicable en materia de protección de datos, los siguientes son los derechos de los titulares de los datos personales, los cuales los pueden ejercer en cualquier momento:

a) Acceder en forma gratuita a los datos proporcionados a FONCEP que hayan sido objeto de tratamiento.
b) Conocer, actualizar y rectificar su información frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o a aquellos cuyo tratamiento esté prohibido.
c) Presentar queja ante la Superintendencia de Industria y Comercio por infracciones en lo dispuesto por la Ley 1581 de 2012 y las demás normas que la modifiquen, adicionen o complementen, una vez haya agotado el trámite de reclamo ante el responsable o encargado del tratamiento de datos personales.



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

d) Solicitar la supresión del dato cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales, el cual procederá cuando la autoridad haya determinado que FONCEP en el tratamiento haya incurrido en conductas contrarias a la Constitución o la normatividad vigente.
e) Conocer la política de tratamiento de datos de la Entidad y a través de ella, el uso o finalidad que se le dará a sus datos personales.
f) Identificar al responsable en FONCEP que dará trámite y respuesta a sus solicitudes.
g) Los demás señalados por el artículo 8 de la Ley 1581 de 2012.

### 6.3.7 Atención y respuesta a peticiones, consultas, quejas y reclamos de los titulares de datos personales

Los titulares de los datos personales que estén siendo recolectados, almacenados, procesados, usados y transmitidos o transferidos por FONCEP, podrán ejercer en cualquier momento sus derechos a conocer, actualizar y rectificar la información.

Para el efecto, se siguen los siguientes pasos de conformidad con la Ley de Protección de Datos Personales:

**a.** FONCEP ha dispuesto los siguientes medios para la recepción y atención de peticiones, consultas, quejas y reclamos que permiten conservar prueba de estas:



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

ALCALDÍA MAYOR DE BOGOTÁ D.C.
FONDO DE PRESTACIONES ECONÓMICAS, CESANTÍAS Y PENSIONES


**b.** Atención y respuesta a peticiones y consultas: El Titular o su apoderado, puede solicitar a FONCEP:

1. Información sobre los datos personales del Titular que son objeto de tratamiento.
2. Información respecto del uso que se le ha dado por FONCEP a sus datos personales.

3. Salvo norma legal especial y so pena de sanción disciplinaria, toda petición deberá resolverse dentro de los quince (15) días siguientes a su recepción.



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

ALCALDÍA MAYOR DE BOGOTÁ D.C.
FONDO DE PRESTACIONES ECONÓMICAS, CESANTÍAS Y PENSIONES

4. Cuando no fuere posible atender la petición o consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando cuando se atenderá su petición o consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

**c.** Atención y respuesta a quejas y reclamos: El titular o sus apoderados, podrán solicitar a FONCEP, a través de una queja o reclamo presentado mediante los canales ya indicados:

1. La corrección o actualización de la información.
2. Que se subsane o corrija el presunto incumplimiento a cualquiera de los deberes contenidos en la Ley de Protección de Datos Personales.

La solicitud deberá contener como mínimo la descripción de los hechos que dan lugar a la queja o reclamo, la dirección y datos de contacto del solicitante. Si la queja o reclamo se presentan incompletos, FONCEP deberá requerir al interesado dentro de los cinco (5) días siguientes a la recepción de la queja o reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido de la queja o reclamo.

En caso de que la dependencia que reciba la queja o reclamo no sea competente para resolverla, deberá dar traslado al Área de Atención al Ciudadano para que la remita al área que corresponda en FONCEP, en un término máximo de dos (2) días hábiles e informará de lo ocurrido al interesado.

Una vez recibida la queja o reclamo completo, se incluirá en la Base de Datos, en el aparte correspondiente, una leyenda que diga "reclamo en trámite" y el motivo de este, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que la queja o reclamo sea resuelto.

El término máximo para atender la queja o el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender la queja o el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá la queja o reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

### 6.4 Gestión de activos de información

Toda la información sensible del FONCEP, así como los Activos de Información donde ésta se almacena o procesa, son inventariados, asignándoles un responsable y clasificarlos de acuerdo con los requerimientos de seguridad de la información y conforme al Procedimiento de Gestión de activos.

La Entidad protege la información generada, procesada o resguardada por los procesos en la prestación del servicio a la ciudadanía y en el cumplimiento de las funciones y activos de información que hacen parte de los mismos. Por ello, los colaboradores de la Entidad deben evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información.

#### 6.4.1 Lineamientos generales

1. Los recursos informáticos, así como la información en ellos contenida es propiedad de la Entidad y su uso está restringido únicamente para propósitos de su negocio, reservándose el derecho de monitorearlo en cualquier momento. Cualquier utilización, modificación o acceso no autorizado a los sistemas de información da lugar a las acciones disciplinarias y/o legales que correspondan. El ingreso y utilización de estos sistemas implica su consentimiento con esta política.
2. Es deber de los funcionarios, proveedores y terceros dar el uso apropiado a los recursos informáticos a los que tenga acceso y en ningún caso podrán ser utilizados para realizar actividades fuera de la ley, que afecte el buen nombre de la Entidad y que maximice el riesgo de materializar una amenaza contra los activos de información.
3. Todos los funcionarios, proveedores y terceros, deben conocer y apropiar las políticas de uso aceptable de los recursos y dar un uso racional y eficiente de ellos.

#### 6.4.1.1 Lineamientos uso de contraseñas

1. La Oficina de Informática y Sistemas, asigna un usuario y contraseña a la red institucional, y acceso a los sistemas de información y los roles y/o privilegios de uso de las herramientas asignadas, conforme a la solicitud de los líderes de proceso.



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

ALCALDÍA MAYOR DE BOGOTÁ D.C.
FONDO DE PRESTACIONES ECONÓMICAS, CESANTÍAS Y PENSIONES

2. El uso de usuario y contraseñas son personales e intransferibles. Es responsabilidad de cada uno de los funcionarios, proveedor o terceros que tenga acceso a los recursos de información de la Entidad salvaguardar su contraseña.
3. La contraseña de la cuenta de usuario asignada por primera vez debe ser cambiada en el primer inicio de sesión.
4. Las contraseñas deben cumplir con los siguientes requisitos:
    a. Tener mínimo ocho caracteres.
    b. Contener caracteres en mayúsculas y minúsculas (es decir, Aa-Zz)
    c. Contener caracteres numéricos (0 a 9)
    d. Contener por lo menos un carácter especial (!@#$%^&*()_+|~-=\ `{}[]:";'<>?,./).
5. La mesa de ayuda del proceso de Gestión de Servicios TI restablece contraseñas a un usuario por medio de la solicitud correspondiente, y conforme a lo establecido en el Instructivo catálogo de servicios de tecnologías de la información – TI.
6. El usuario debe evitar mantener un registro (por ejemplo, en papel, archivos electrónicos) de las contraseñas, a menos que se pueda almacenar de forma segura.

#### 6.4.1.2 Lineamientos de uso de recursos compartidos

1. Las carpetas compartidas son una herramienta de trabajo necesario, es responsabilidad de los usuarios de este recurso su preservación y buen uso, ya que puede afectar la confidencialidad, integridad y disponibilidad de la información.
2. Se debe definir el tipo de acceso y los perfiles estrictamente necesarios sobre la carpeta (lectura, escritura, modificación y borrado).
3. Este servicio debe ser desactivado una vez se pierda el vínculo laboral o contractual de los funcionarios y/ proveedores o terceros respectivamente.
4. No está permitido compartir información de la Entidad en sitios web externos, salvo los autorizados por el proceso de Gestión de Servicios TI.

#### 6.4.1.3 Lineamientos de uso de internet



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

ALCALDÍA MAYOR DE BOGOTÁ D.C.
FONDO DE PRESTACIONES ECONÓMICAS, CESANTÍAS Y PENSIONES

1. El proceso de Gestión de Servicios de TI provee el servicio de internet para la Entidad de forma segura, implementa los mecanismos necesarios para controlar el acceso a internet de acuerdo con los perfiles definidos.
2. El uso de Internet es exclusivo para asuntos laborales. Su uso está prohibido para obtener de manera ilegal material con derechos de autor marcas, secretos empresariales o cualquier otro derecho intelectual de otra persona o instalar software que no ha sido aprobado o licenciado por el proceso Gestión de Servicios TI.
3. El acceso al servicio de internet, redes sociales y mensajería instantánea debe ser autorizado por directores de área del funcionario o a quien él delegue, y provisto por el proceso de Gestión de Servicios TI, quien debe monitorear su uso apropiado por medio de herramientas de monitoreo y análisis de tráfico. En el caso de proveedores o terceros, debe ser autorizado por el supervisor del contrato.
4. Ante la ausencia parcial o permanente de control de navegación en Internet, todos los funcionarios, proveedores o terceros deben abstenerse de visitar sitios web relacionados con contenido pornográfico, páginas de organizaciones delincuenciales o terroristas, descarga o propagación de software malicioso, entre otros sitios web que puedan afectar la integridad de la red de FONCEP.
5. El uso de Internet está restringido para descargar música, videos y juegos, o practicar juegos en línea.
6. Para la utilización de los servicios de radio, videos y televisión sobre internet, deben ser autorizados por directores de área del funcionario o a quien él delegue, exponiendo las causas de la excepción ante el proceso de Gestión de Servicios TI, quien se encargará de otorgar los permisos necesarios.
7. Está prohibido bajo cualquier circunstancia, descargar o instalar, no licenciados o no autorizados, también la alteración o modificación de programas ya instalados y avalados por el proceso de Gestión de Servicios TI en los computadores de la Entidad.
8. Los funcionarios, proveedores o terceros no pueden utilizar los medios de la Entidad para el acceso a internet para realizar actos que van en contra de la ley: ilegales, inmorales o engañosos. Así mismo para realizar amenazas, injurias, calumnias, obscenidades o pornografía, actos discriminatorios de género o raza o invasión a la privacidad.

#### 6.4.1.4 Lineamientos de uso de correo electrónico

1. El servicio de correo electrónico del FONCEP debe ser autorizado por directores de área o dependencia del funcionario o delegado para realizar la solicitud, y provisto por el proceso de Gestión de Servicios de TI. Solo podrá ser utilizado para fines laborales. En el caso de proveedores o terceros, debe ser autorizado por el supervisor del contrato.



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

2. El buzón de correo es personal e intransferible. El dueño de la cuenta debe velar por su seguridad protegiendo su clave de acceso. El usuario es el único responsable por el buen uso de su cuenta de correo electrónico.
3. Este servicio debe ser desactivado una vez se pierda el vínculo laboral o contractual de los funcionarios y/ proveedores o terceros respectivamente, mediante la solicitud de retiro de servicios de TI estipulado en el Instructivo catálogo de servicios de tecnologías de la información - TI.
4. La Entidad puede, en caso de ver afectada la seguridad de los activos de información, revocar el acceso a los servicios de correo electrónico, inspeccionar y monitorear el servicio de correo.
5. Los funcionarios, proveedores o terceros no pueden utilizar el correo electrónico de la Entidad para enviar mensajes que van en contra de la ley: ilegales, inmorales o engañosos. Así mismo para realizar amenazas, injurias, calumnias, obscenidades o pornografía, actos discriminatorios de género, raza o invasión a la privacidad.
6. En ningún caso se debe aceptar, abrir ni compartir mensajes de correos con archivos adjuntos de origen desconocido. Si lo recibe consulte inmediatamente con la mesa de ayuda del proceso Gestión de Servicios TI, en los medios mencionados en el Instructivo catálogo de servicios de tecnologías de la información - TI.
7. Se deben eliminar periódicamente los mensajes innecesarios.
8. La firma de los correos electrónicos será obligatoria para funcionarios de planta y opcional para proveedores o terceros y deberá contener: Nombre y Apellidos, Cargo o Proyecto, Nombre Entidad, Teléfono de contacto fijo o celular y/o extensión.
9. Los correos electrónicos deben contener la sentencia de confidencialidad que debe incluirse inmediatamente después de la firma con el siguiente contenido:
   "IMPORTANTE. Este documento es propiedad del Fondo de Prestaciones Económicas, Cesantías y Pensiones –FONCEP. La información contenida en ésta comunicación es confidencial y solo puede ser utilizada por la persona natural o jurídica a la cual está dirigida. Si no es el destinatario autorizado, cualquier retención, difusión, distribución o copia de este mensaje, se encuentra prohibida y sancionada por la ley. Si por error recibe este mensaje, favor reenviar y borrar el mensaje recibido inmediatamente. El FONCEP, no asumirá responsabilidad ni su institucionalidad se verá comprometida si la información, opiniones o criterios contenidos en este correo no están directamente relacionados con las funciones regentadas. Las opiniones de este mensaje son exclusivas de su autor."
   SECTOR HACIENDA - Fondo de Prestaciones Económicas, Cesantías y Pensiones – FONCEP.

**El profesional de la OIS, trimestralmente asegura que los colaboradores de la Entidad tengan información relacionada con el funcionamiento y uso de las herramientas de Microsoft con las que cuenta la Entidad, mediante comunicaciones de la OIS relacionadas**



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

**con los sistemas de respaldo ofertados (backup al momento de retiro), recomendación de salvaguardar archivos de interés institucional, descarga de resultados antes de eliminación del instrumento de recolección y uso de cuentas institucionales para tal fin. En caso de presentarse dudas adicionales por los usuarios se incluyen en las comunicaciones OIS del siguiente trimestre. La evidencia son las comunicaciones enviadas a los colaboradores de la Entidad por los medios oficiales acordados.**

#### 6.4.1.5 Lineamientos de uso de software

1. Ningún funcionario, proveedor o tercero puede instalar software licenciado o libre que no esté autorizado por Gestión de Servicios TI.
2. El software licenciado o autorizado por la Entidad solo debe ser utilizado para las funciones propias del cargo, no está permitido utilizarlo para apropiar, divulgar u hacer uso indebido de la información a la que se tenga acceso por medio de él.
3. No está permitida la distribución del software licenciado o de propiedad de la Entidad.

#### 6.4.1.6 Lineamientos de uso de equipos portátiles y dispositivos móviles

1. La Oficina de Informática y Sistemas debe establecer las configuraciones aceptables para los dispositivos móviles institucionales o personales que hagan uso de los servicios de la Entidad.
2. Además, debe velar por que en caso de pérdida o hurto el dispositivo que es de propiedad de la Entidad pueda contar con un borrado seguro para prevenir el acceso no autorizado a información confidencial de la Entidad. O en su defecto, se deberá procurar implementar mecanismos de cifrado de disco completo.
3. Los usuarios no deben modificar las configuraciones de seguridad de los dispositivos móviles, ni desinstalar el software provisto con ellos al momento de su entrega.
4. Los usuarios deben evitar la instalación de programas desde fuentes desconocidas; solo Gestión de Servicios TI está autorizada para instalar software en ellos.
5. Los usuarios deben evitar la extracción de información por medio de puerto USB en cualquier computador de la Entidad.
6. Los usuarios no deben almacenar videos, fotografías o información personal en los dispositivos móviles asignados.



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

### 6.4.1.7 Lineamientos de uso periféricos y medios de almacenamiento extraíbles

1. El uso de periféricos y medios de almacenamiento extraíbles están prohibidos sin la autorización por parte de los directores de área del funcionario o por quien él delegue.
2. El proceso de Gestión de Servicios TI debe brindar los medios necesarios para evitar el uso de medios removibles en: servidores, unidades de almacenamiento, entre otros dispositivos que contengan información confidencial.
3. El proceso de Gestión de Servicios TI gestiona el uso y retiro de los dispositivos removibles de forma segura.
4. Los funcionarios y el personal provisto por terceras partes deben acoger las condiciones de uso de los periféricos y medios de almacenamiento establecidos por Gestión de Servicios TI.

### 6.4.1.8 Lineamientos de uso de aplicaciones

1. El acceso a las aplicaciones del FONCEP deben ser solicitadas por los directores de área y/o dependencia o quien éste delegue, de acuerdo con el Instructivo catálogo de servicios de tecnologías de la información - TI.
2. Los dueños de los activos de información relacionados con aplicaciones o sistemas de información serán los responsables de autorizar los accesos a funcionarios, contratistas y/o terceros.
3. Cada usuario debe contar con el rol de acceso definido y las opciones de menú de cada servicio o aplicación de acuerdo con su cargo y responsabilidad. Es responsabilidad del autorizador del acceso a cada aplicación la asignación del rol y menú de aplicaciones, de acuerdo con el procedimiento establecido.
4. Los usuarios deben informar a Gestión de Servicios TI si cuenta con un rol u opciones no autorizadas que vulneren cualquier activo de información.

5. Está prohibida la instalación de aplicaciones de administración de base de datos, administración de sistemas o aplicaciones no licenciadas o no autorizadas por el proceso de Gestión de Servicios TI. De requerir el uso de estas aplicaciones debe solicitarse por medio de la Mesa de Ayuda quien evaluará la pertinencia y viabilidad de la autorización.



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

### 6.4.1.9 Lineamientos de equipos de usuario desatendido

1. Con el fin de evitar pérdidas, daños o accesos no autorizados a la información, todos los colaboradores de FONCEP deben mantener la información restringida o confidencial bajo llave cuando sus puestos de trabajo se encuentren desatendidos o en horas no laborales. Esto incluye: Documentos impresos, CD, Dispositivos de almacenamiento USB y medios removibles en general.
2. El proceso de Gestión de Servicios TI diseña y pone en ejecución el control a los equipos desatendidos por los usuarios por medio de una GPO del controlador de dominio con un bloqueo de pantalla a un tiempo determinado (un minuto) de estar inactivo el equipo.
3. El colaborador es el custodio del equipo de cómputo, por consiguiente, es responsable por el cuidado, uso y seguridad de este y de la información manejada en él.
4. La Oficina de Informática y Sistemas cuenta con un plan de concientización dirigido a los usuarios de FONCEP para que cambien su cultura y adopten estos lineamientos.
5. Todos los usuarios son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren del puesto de trabajo, la cual se podrá desbloquear sólo con la contraseña del usuario. Cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos apagados.
6. Todas las estaciones de trabajo deben usar el papel tapiz y el protector de pantalla corporativo, el cual se activa automáticamente después de cinco (5) minutos de inactividad y se puede desbloquear únicamente con la contraseña del usuario.

### 6.4.1.10 Lineamientos de disposición y reutilización de equipos

1. Los equipos de cómputo de FONCEP son alistados por personal perteneciente al proceso de Gestión de Servicios TI.
2. El proceso de Gestión de Servicios TI tiene como línea base un inventario tecnológico completo de los equipos informáticos, el cual debe estar siempre actualizado con las novedades que se presenten en los equipos.



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

3. Para la instalación de los equipos de cómputo se debe tener en cuenta las recomendaciones hechas por los fabricantes en cuanto a exposición a campos magnéticos, temperatura máxima del ambiente, protección eléctrica y demás condiciones técnicas definidas por el manual de instalación.
4. Los equipos de cómputo deben ser instalados de tal forma que puedan tener una ventilación adecuada y se minimice el riesgo de robo, incendio, golpes, inundaciones, polvo, vibraciones y radiación electromagnética.
5. No está permitido el consumo de alimentos o bebidas cerca de los equipos.
6. Cuando los equipos de cómputo sean devueltos por cualquier causa, se debe borrar por completo toda la información almacenada en su(s) disco(s) duro(s), en lo posible con un formateo completo a bajo nivel.
7. Toda la información que se encuentre en equipos de usuarios y que van a ser reutilizados debe ser borrada y se debe realizar un formateo completo de los discos, la reinstalación del Sistema y de las aplicaciones.
8. Corresponde al proceso de Gestión de Servicios TI recibir, monitorear y verificar al momento de la devolución, que el activo exista en el inventario de hardware de los equipos de cómputo.
9. Corresponde al proceso de Gestión de Servicios TI en coordinación con el responsable de cada área, promover y difundir los mecanismos necesarios adecuados de respaldo, salvaguarda de los datos, de los sistemas de información y los generados por los usuarios con sus respectivas herramientas de oficina.
10. No se debe retirar información, en ningún formato, de las instalaciones del FONCEP, sin la debida autorización previa por parte del Director de área y/o dependencia.

## 6.5 Control de acceso

### 6.5.1 Lineamientos generales

1. El proceso de Gestión de Servicios TI establece el procedimiento de Gestión de Mesa de Ayuda de TI, que contemple la creación, modificación, bloqueo o eliminación de las cuentas de usuario para proveer acceso o retiro seguro a los servicios de TI del FONCEP.
2. El proceso de Gestión de Servicios TI debe asegurar que los servicios de TI de FONCEP cuenten con métodos de autenticación que evite accesos no autorizados, mediante el usuario y contraseña.



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

3. Los directores o jefes de área y/o dependencia son los responsables de solicitar y autorizar el acceso a los servicios de TI para los funcionarios, contratistas, proveedores y/o terceros que laboran en sus áreas, por medio del Instructivo catálogo de servicios de tecnologías de la información - TI.
4. El proceso de Gestión de Servicios TI es el responsable de la creación de las cuentas de usuarios solicitados y autorizados por las áreas para el acceso a los servicios.
5. Los directores o jefes de dependencia deben verificar que los accesos otorgados a los usuarios cuenten con los permisos para los que fueron autorizados. En caso de que los permisos excedan o no sean suficientes deberá notificarlo al proceso de Gestión de Servicios TI para su ajuste.
6. Antes de hacer uso de los servicios de TI los funcionarios, contratistas, proveedores y/o terceros deben contar con la notificación de la Mesa de Ayuda sobre el acceso autorizado.
7. Todo funcionario, contratista, proveedor y/o tercero que haga uso de los servicios de TI debe contar con una cuenta de usuario de Dominio, excepto cuando para la prestación del servicio no lo permita.
8. Los usuarios de los servicios de TI del FONCEP deben hacer buen uso del usuario y contraseña asignados para el acceso a estos y son responsables de los usos inadecuados que se hagan de ellos.

### 6.5.2 Lineamientos de acceso a aplicaciones o sistemas de información

1. Los propietarios o administradores de los sistemas de información o aplicaciones deben definir los perfiles o roles de usuario, especialmente de aplicaciones o sistemas de información.
2. Los directores o jefes de área deben autorizar los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles o roles definidos según las necesidades de uso.
3. Los directores o jefes de área y/o dependencia deben custodiar y asignar los accesos de sus colaboradores manteniendo la seguridad, y en caso de que la persona responsable no esté disponible y el jefe o director considere pertinente, asigne un rol o persona de respaldo que pueda atender o administrar los accesos, es decir, exista un mecanismo de custodia que permita por lo menos a dos personas del área o dependencia conocer los accesos o en su defecto mantener en dos personas el rol de la persona ausente o administrador.
4. Los propietarios o administradores de los sistemas de información o aplicaciones deben monitorear periódicamente los perfiles o roles definidos en los sistemas de información y los privilegios asignados a los usuarios que acceden a ellos, informando de cualquier riesgo de seguridad de la información, que puedan presentar a raíz de privilegios no autorizados o



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

que exceden las necesidades para los que fueron autorizados. Lo anterior, mediante los controles a los activos de la información de cada proceso, que evidencia trimestralmente con el monitoreo de riesgos de seguridad de la información, el acceso a los activos más críticos, y de allí solicitar el ajuste de ser si es necesario.

5. El proceso de Gestión de Servicios TI debe proporcionar ambientes separados para desarrollo, pruebas y producción. Cada uno debe contar con infraestructura independiente para evitar que las actividades de uno pongan en riesgo el otro, especialmente los de producción.
6. Los usuarios deben utilizar diferentes perfiles para los ambientes de desarrollo, pruebas y producción, para reducir el riesgo de realizar actividades en ambientes equivocados.
7. La Oficina de Informática y Sistemas debe establecer los controles a los ambientes productivos para conceder acceso únicamente para usuarios finales de acuerdo con los roles solicitados, y asegurar que los desarrolladores tengan acceso limitado y controlado a los ambientes de producción.
8. El proceso de Gestión de Servicios TI debe salvaguardar el código fuente de las aplicaciones o sistemas de información con control de acceso y restricción de privilegios.

### 6.5.3 Lineamientos de privilegios especiales

1. El proceso de Gestión de Servicios TI realiza una administración segura de la plataforma tecnológica que soporta los servicios de TI, monitoreando las actividades de los usuarios administradores.
2. Solo se otorgan permisos especiales de administración a los funcionarios, contratistas y/o proveedores cuyo manual de funciones o contrato respectivamente, especifiquen esas funciones de administración o gestión de la plataforma.
3. El proceso de Gestión de Servicios TI otorga acceso por medio de cuentas personalizadas con privilegios especiales a cada uno de los administradores.

## 6.6 Criptografía y seguridad de intercambio de información

El FONCEP por medio del proceso de Gestión de Servicios TI implementará los controles criptográficos con la gestión de llaves para asegurar la confidencialidad de la información de la Entidad en los casos que sean establecidos.



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

1. Todas las áreas o dependencias, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido. Por ejemplo: Data Center y centro de monitoreo.
2. Las contraseñas para cifrado de información se deben proteger y gestionar siguiendo los controles de seguridad definidos para la protección de contraseñas de FONCEP.
3. Los computadores portátiles, medios de almacenamiento removibles y medios de respaldo que contengan información clasificada con carácter reservado deben ser sometidos a cifrado de datos.
4. Cuando se utilicen sistemas de intercambio de información como correos electrónicos, sistemas de transferencias de datos o sistemas de información para intercambio de datos con otras Entidades del estado en los que viaje información con carácter reservado deben emplear mecanismos de cifrados autorizados por los responsables de áreas y procesos de FONCEP.
5. Al realizar el cifrado de información, se debe mantener copia de las llaves de cifrado en lugar seguro de forma que la recuperación de la información cifrada sea factible en caso de ausencia temporal o permanente del custodio de la información cifrada. Para esto se debe diligenciar acta de custodia de llaves cada vez que sea aplicada este lineamiento por los involucrados.
6. Las llaves de cifrado tendrán una vigencia limitada, posterior a este tiempo debe actualizarse para garantizar que esta no sea revelada.
7. Los usuarios autorizados para acceder remotamente a la información de FONCEP, deben hacerlo a través de servicios tipo **VPN SSL** o similar. Mediante este mecanismo se les otorgará acceso remoto a los recursos de la red de forma segura y cifrada.

### 6.6.1 Lineamiento general para seguridad de intercambio de información

Los intercambios de información con terceros se deben realizar basados en acuerdos formales y acuerdos de confidencialidad orientados en las obligaciones generales de los contratos de OPS: “Guardar total reserva de la información que por razón del servicio y desarrollo de sus actividades obtenga. Esta es de propiedad de FONCEP, y solo salvo expreso requerimiento de autoridad competente podrá ser divulgada” y “Conocer y aplicar durante la ejecución de sus obligaciones contractuales, las Políticas de seguridad de la información del FONCEP”, “Aplicable a proveedores y terceros” y “De uso apropiado de los activos de información”.



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

**El profesional de contratación de la OIS, cada vez que se realice una contratación dentro de la OIS, verifica que se incluyan las funciones en los contratos de prestación de servicios relacionadas con seguridad de la información. En caso de desviación se debe corregir y ajustar las funciones antes de pasar la documentación a jurídica. La evidencia de este control son los estudios previos que están disponibles en Atlas.** 🔍

### 6.6.2 Lineamientos de transferencia digital

1. Utilizar siempre el protocolo de transferencia de información segura HTTPS en las comunicaciones con las Entidades externas.
2. Disponer de herramientas de cifrado, asimétrico preferiblemente para aplicarlas en el intercambio de información. (Ver lineamientos de criptografía).
3. Tener disponibilidad de certificados digitales en caso de necesitarse en el intercambio de información con otras Entidades.

### 6.6.3 Lineamientos de transferencia física

1. Los empleados del FONCEP no deben revelar información sensible por medios telefónicos, para evitar la escucha o interpretación de su llamada por personas extrañas.
2. Si es una memoria USB o disco duro externo, el transporte de información restringida se debe realizar mediante contenedores o espacios cifrados.

## 6.7 Seguridad Física

### 6.7.1 Lineamiento general

Se debe establecer áreas seguras para la gestión, almacenamiento y procesamiento de información en el FONCEP; que en lo posible deben contar con protecciones físicas y ambientales acordes a los activos que protegen, incluyendo perímetros de seguridad, controles de acceso físicos, controles especiales en áreas de mayor sensibilidad, seguridad de los equipos, seguridad en el suministro eléctrico y cableado, condiciones ambientales de operación y sistemas de contención, detección y extinción de incendios adecuados que preserven el medio ambiente.



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

Las instalaciones o sitios físicos donde se procesa información son:

- **a.** Centros de cómputo principales o alternos.
- **b.** Áreas con equipos de cómputo, ya sean de procesamiento o dispositivos de comunicación.
- **c.** Áreas donde se almacenen papelería, hojas membretadas, documentos con valor comercial o títulos valor.
- **d.** Áreas donde se encuentren almacenados dispositivos de información.
- **e.** Áreas de almacenamiento de dispositivos de respaldo datos (CD, Discos Duros, Cintas etc.).
- **f.** Áreas de impresión o fax.
- **g.** Despachos de los directivos o personal que tenga acceso a información sensible de la Entidad.
- **h.** Área de Tesorería.
- **i.** Área de Nómina.
- **j.** Áreas de monitoreo.
- **k.** Centro de Cableado de datos o telefónico.
- **l.** Estaciones de trabajo.

1. Los colaboradores de FONCEP deben portar el carné que los identifica como tales en un lugar visible mientras se encuentren en las instalaciones de la Entidad. Así mismo los visitantes, proveedores, contratista y terceros deben portar el carné provisional o de visitante.
2. Las puertas de acceso a los diferentes pisos de la Entidad deben permanecer cerradas para acceso biométrico con el fin de controlar el ingreso y salida de visitantes y colaboradores.
3. El personal de seguridad de la recepción del edificio debe llevar un registro de todos los visitantes /usuarios que se dirigen al segundo piso (espacio de atención al ciudadano o usuario).
4. El ingreso y salida de equipos de cómputo de cada piso, debe contar con la autorización por escrito del Jefe de la Subdirección Financiera y Administrativa.
5. Todo bolso, cartera y/o paquete que ingrese los colaboradores/visitantes de la Entidad, debe ser revisados por el personal de seguridad dispuesto en cada piso, dejando registro en las minutas de los números de serie de los equipos.
6. El área de talento humano debe mantener un listado actualizado de funcionarios y contratistas el cual debe entregarse al personal de seguridad para que realicen el respectivo control de ingreso.



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

7. La recepcionista del segundo piso (atención al ciudadano) debe realizar las respectivas llamadas de autorización de ingreso a los pisos, de aquellos visitantes que una vez realizada la consulta o diligencia deseen reunirse adicionalmente con algún funcionario de la Entidad.
8. El acceso al área de tesorería debe quedar registrado en la minuta con hora de ingreso y salida de los visitantes.
9. Para el ingreso al Data center se debe diligenciar el Formato relación personal para ingreso al data center FOR-APO-GST-016.
10. El personal de la empresa de vigilancia asignado a cada piso debe anunciar a los visitantes con el fin de determinar si su ingreso es autorizado o no por el colaborador correspondiente.

### 6.7.2 Lineamiento asociado a la consulta de las grabaciones de las cámaras del circuito cerrado de televisión – CCTV del FONCEP

#### 6.7.2.1 Consideraciones Generales

Las personas autorizadas por la Subdirección Financiera y Administrativa para acceder a las grabaciones del CCTV, sólo tienen acceso a las imágenes a manera de consulta; exceptuando cuando el material video gráfico se requiera como prueba dentro de un proceso adelantado por una autoridad civil, penal, fiscal o disciplinaria competente, que conforme a las normas de procedimiento así lo solicite. El Asesor responsable del área administrativa encargado de la supervisión y control de la seguridad física y el sistema de CCTV, no entrega copias de grabaciones, ni certifica las imágenes grabadas.

No puede solicitarse consulta de grabaciones para determinar los movimientos o recorridos de personas determinadas al interior del edificio, salvo que esta información sea requerida dentro de las pruebas decretadas en un proceso penal, fiscal, civil o disciplinario. No obstante, si se presenta algún evento que requiera verificar las grabaciones, puede solicitarse al Asesor responsable del área administrativa aduciendo las debidas evidencias o justificaciones.

Recuerde que la seguridad es asunto de todos. Cuide sus objetos personales y custodie bien los documentos y elementos que tiene a cargo. No guarde elementos de valor, títulos valores ni medios transaccionales en su puesto de trabajo. Tenga en cuenta que no existe una cámara de seguridad para monitorear cada puesto de trabajo, pues el objetivo del CCTV es ser elemento de persuasión y disuasión, así como contribuir al control de zonas estratégicas de la infraestructura física de la Entidad.



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

#### 6.7.2.2 Usuarios, beneficiarios y/o destinatarios del servicio

Todas aquellas personas, naturales o jurídicas, usuarias del servicio de vigilancia y seguridad privada contratado por el FONCEP, con un interés legítimo y concreto de consultar las grabaciones de una o algunas de las cámaras de seguridad que conforman el CCTV, así como los representantes de la empresa de vigilancia contratada para la prestación del servicio.

Se consideran legítimamente interesados en la consulta de las grabaciones, los entes y organismos de control interno y externo, las autoridades judiciales y de policía y los usuarios o visitantes que hayan sufrido algún daño o pérdida cuya responsabilidad pudiera derivarse de falla o negligencia en la prestación del servicio de vigilancia.

#### 6.7.2.3 Desarrollo del protocolo de consulta

##### ¿Cómo solicitar la consulta?

Si usted cumple con lo establecido en el presente protocolo, puede solicitar la consulta de las grabaciones del CCTV, para lo cual debe dirigirse por escrito o correo electrónico ante el Asesor responsable del área administrativa del FONCEP. Este documento debe contener como mínimo:

- **a.** Nombre e identificación del solicitante.
- **b.** Dirección de notificación, indicando un correo electrónico como medio de comunicación.
- **c.** Descripción del motivo de la solicitud de consulta, indicando el interés particular que le asiste para conocer el contenido del video.
- **d.** Razones que le permitan presumir que el motivo de la consulta se debe a falla o negligencia en la prestación del servicio de vigilancia. e) Año, mes, día y hora en la que supone que ocurrieron los hechos cuya grabación es de su interés consultar.
- **e.** Piso del FONCEP o dependencia especifica en la que usted presume que ocurrieron los hechos que usted requiere consultar.



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

No es obligatorio adjuntar documento alguno con la solicitud de consulta, pero el interesado puede aportar los que considere pertinente. Tenga en cuenta que sólo son atendidas las solicitudes que contengan la información mínima exigida. En caso de presentar solicitudes en las cuales se evidencie que el interés de la consulta corresponde a eventos excluidos de este servicio, el Asesor responsable del área administrativa responderá negativamente su solicitud indicándole las razones por las cuales ésta no será atendida.

**¿Qué hacer si la solicitud es respondida negativamente?**

Si usted por error omitió alguno de los requisitos de la solicitud puede corregir, o completar la información y solicitar una reconsideración de esta ante el Asesor responsable del área administrativa, a través del mismo medio que utilizó para su solicitud inicial. Preferiblemente indique la fecha del correo electrónico en que presentó la solicitud inicial. El asesor responsable del área administrativa no reconsidera solicitudes relativas a los eventos excluidos del servicio de consulta.

**¿En cuánto tiempo y dónde pueden consultarse las grabaciones?**

En un término máximo de quince (15) días hábiles, contados a partir del día siguiente al recibo de su solicitud, el Asesor responsable del área administrativa le informa el lugar, fecha y hora en la que usted puede consultar los videos obtenidos de las cámaras del CCTV.

No se pueden utilizar aparatos de alta tecnología para grabar los videos que se están revisando. Está prohibido el acceso de cámaras y grabadoras de cualquier tipo al sitio de consulta. Tenga en cuenta que durante la consulta el solicitante debe estar acompañado por el personal designado por el Asesor responsable del área administrativa.

**¿Cómo concluye la consulta?**

Si la consulta fue radicada mediante oficio por un ente de control, esta se responde con un oficio (Correspondencia Externa Enviada – SIGEF). En el oficio se consignan las observaciones a que hubiere lugar y se deja constancia en relación con el cumplimiento total por parte de la Entidad de la solicitud efectuada.

### 6.7.4 Lineamientos asociados a la seguridad de los equipos



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

ALCALDÍA MAYOR DE BOGOTÁ D.C.
FONDO DE PRESTACIONES ECONÓMICAS, CESANTÍAS Y PENSIONES

En lo referente a la ubicación de computadores y hardware en general, se debe tener especial cuidado contra fallas del sistema de control del medio ambiente, y otras amenazas que puedan afectar la normal operación del sistema.

1. Se debe tener un estricto monitoreo sobre fallas en el control de la temperatura o humedad que pueden afectar la operación de los sistemas de información.
2. Se deben tener controles apropiados referentes a:

   a) Robo: Todos los visitantes proveedores o terceros, que ingresen a las instalaciones de la Entidad deben poseer una identificación que permita saber la dependencia autorizada a visitar o por la cual transitar. En el caso de Proveedores o terceros debe contar con el permiso para permanecer en la Entidad, siempre con la supervisión del responsable de sus labores.
   b) Humo o Fuego: En todos los centros de procesamiento, sin excepción, deben existir detectores de calor y humo, instalados en forma adecuada para detectar el más mínimo indicio de incendio. Los detectores deben ser probados de acuerdo con las recomendaciones del fabricante.
   c) Se deben tener extintores de incendios debidamente probados, y con capacidad de detener fuego generado por equipo eléctrico, papel o químicos especiales.
   d) Explosivos: Todos los visitantes proveedores o terceros, personal de la Entidad o contratistas que ingresen o esté cercano a un área de procesamiento o áreas restringidas, no pueden, por ninguna razón llevar consigo material explosivo (Por ejemplo, químicos especiales, pólvora o gases explosivos).
   e) Interferencia Eléctrica y/o Radiación electromagnética: El cableado de la red debe ser protegido de interferencias por ejemplo usando canaletas que lo protejan. Los cables de potencia deben estar separados de los de comunicaciones, siguiendo las normas técnicas.
   f) Las áreas en donde se tenga equipos de procesamiento de información, no se permite fumar, tomar ningún tipo de bebidas o consumir alimento.
   g) Los equipos deben ser protegidos de fallas de potencia u otras anomalías de tipo eléctrico. Los sistemas de abastecimiento de potencia deben cumplir con las especificaciones de los fabricantes de los equipos.
   h) El correcto uso de UPS (Uninterruptible power supply): Se debe probar según las recomendaciones del fabricante, por lo menos una vez al año, de tal forma que garanticen el suficiente tiempo para realizar las funciones de respaldo en servidores y aplicaciones.



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

### 6.7.4 Lineamiento asociado a los centros de cómputo y centros de cableado

1. El acceso al centro de cómputo o a los centros de cableado debe ser autorizado por funcionarios de la Oficina de Informática y Sistemas autorizados. Los proveedores, contratistas, terceros y visitantes siempre deben estar acompañados de un funcionario de dicha Oficina.
2. Se debe contar con algún tipo de registro del ingreso por escrito de los visitantes al centro de cómputo y a los centros de cableado.
3. Se debe restringir el acceso físico al centro de cómputo y los centros de cableado, en los eventos de desvinculación o cambio en las labores de un funcionario o contratista autorizado.
4. Se asegura las condiciones físicas y medioambientales necesarias para la protección y correcto funcionamiento de la plataforma tecnológica ubicada en el centro de cómputo y centros de cableado; adecuando sistemas de control de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas eléctricos de contingencia, sistemas de vigilancia y monitoreo. Estos sistemas se deben monitorear de manera permanente.
5. En lo posible, el centro de cómputo y los centros de cableado deben estar separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.
6. Las labores de mantenimiento de redes eléctricas, de voz y de datos debe llevar control de la programación de los mantenimientos preventivos.

#### 6.7.4.1 Instalación y mantenimiento del cableado

1. Conectores de pared no utilizados deben ser sellados y su estado debe ser formalmente notificado.
2. Las conexiones de potencia deben tener su respectivo polo a tierra.
3. El cableado de la red debe ser protegido de intercepción o daño, por ejemplo, usando canaletas que lo protejan.
4. Los cables de potencia deben estar separados de acuerdo con las normas técnicas, como: NTC 2050, NTC 169, NTC 171, NTC 332, NTC 979, NTC 1630, NTC 3363 o NTC105, según aplique.



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

ALCALDÍA MAYOR DE BOGOTÁ D.C.
FONDO DE PRESTACIONES ECONÓMICAS, CESANTÍAS Y PENSIONES

#### 6.7.4.2 Mantenimiento de los equipos

1. Se debe contar de forma constante con el soporte y mantenimiento adecuado para los equipos de procesamiento de información.
2. Se debe contar con las pólizas de seguros contra pérdidas y daños, adecuados para los equipos de procesamiento.
3. Se debe realizar mantenimientos preventivos y correctivos sobre la plataforma tecnológica de la Entidad. Verificar Procedimiento de mantenimiento preventivo y correctivo PDT-APO-GST-019.
4. Se deberán realizar mantenimientos sobre los equipos de acuerdo con las recomendaciones del fabricante y ser realizados únicamente por personal autorizado, considerando el hecho que, si se tuviera que enviar fuera de las instalaciones, se debe tener en cuenta la información sensible y los requerimientos de las pólizas de aseguramiento.

#### 6.7.4.3 Destrucción de equipos y re-uso

Los dispositivos de almacenamiento de información deben ser dados de baja y borrados de manera segura a través del uso de herramientas especiales que garanticen y verifiquen que no quede información remanente, evitando que dicha información quede expuesta a personal no autorizado, previa copia de respaldo de la información sensible que repose en el dispositivo de acuerdo con el Procedimiento gestión de Backup PDT-APO-GST-017 y es realizado por personal autorizado del proceso de Gestión de Servicios TI.

### 6.7.5 Lineamiento de escritorios y pantalla limpia

1. La Entidad debe tener escritorios limpios para papeles, y medios de información, junto con una pantalla limpia, con el fin de reducir los riesgos por pérdida, daño a la información durante o fuera de las horas de trabajo.
2. Cuando sea apropiado, papeles y medios de información deben estar asegurados en gabinetes de escritorio o especiales, en horas fuera de horario de oficina.
3. Información confidencial y crítica para la organización debe ser asegurada preferiblemente en archivadores resistentes a impacto, fuego e inundación.



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

### 6.7.6 Lineamientos de uso de impresoras

1. Cuidar que la información confidencial impresa no sea conocida por personas que no deben tener acceso a la misma.
2. La información clasificada como altamente confidencial no debe ser nunca enviada a una impresora de la red, sin que exista una persona autorizada para cuidarla durante y después de la impresión.

### 6.7.7 Lineamientos recepción de mercancía

1. La recepción de mercancía en la Entidad requiere de un primer control e inspección por parte de la seguridad del edificio en la recepción, posteriormente se da la respectiva autorización para su ingreso y entrega en el sitio respectivo.
2. Todo dispositivo que ingrese a la Entidad debe ser inspeccionado por la compañía de seguridad rigurosamente con el fin de identificar material peligroso y que coincida con su respetiva autorización de ingreso.
3. Las áreas de recibo de mercancía deben estar debidamente identificadas para evitar el acceso a las instalaciones por parte de terceros, especialmente a centros de procesamiento o áreas restringidas.

### 6.7.8 Lineamientos traslado de información física

1. La información física incluye medio digitales o en papel y deben ser protegidos cuando son transportados fuera de la Entidad.
2. Los medios digitales deben ir protegidos con encriptación de datos. En su defecto debe tener una seguridad física que prevenga el acceso indebido y daños físicos que puedan presentarse en el momento del tránsito de los activos. Así mismo los documentos físicos.
3. El FONCEP debe asegurar que las compañías trasportadoras cuenten con las medidas de seguridad necesarias para la protección de la confidencialidad de la información. Solo deben contratarse con compañías que dentro de sus procesos y servicios contemplen medidas de seguridad de la información que cumplan con las políticas de la Entidad.
4. El transporte de activos de información solo debe contratarse con compañías autorizadas por la Entidad.

### 6.7.9 Lineamiento trabajo en áreas seguras

Las actividades de limpieza en las áreas seguras deben ser controladas estrictamente por el responsable de la infraestructura.



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

ALCALDÍA MAYOR DE BOGOTÁ D.C.
FONDO DE PRESTACIONES ECONÓMICAS, CESANTÍAS Y PENSIONES

### 6.7.10 Lineamiento servicios de suministro

Toda la red eléctrica debe ser regulada. Para el centro de Cómputo y para algunas áreas de procesamiento debidamente identificadas, se debe instalar equipos de Suministro de Energía de Forma Interrumpible (UPS).

### 6.7.11 Lineamientos de seguridad de los equipos fuera de las instalaciones

1. Los equipos portátiles deben estar protegidos por mecanismos antirrobo o con elementos como guayas de seguridad, en adición a los controles lógicos establecidos.
2. Cuando un equipo de cómputo deba repararse, éste no debe salir del edificio sin tener una autorización firmada por parte del director del área y/o dependencia a la cual pertenece o está asignado el equipo, y por el profesional encargado de los Recursos Físicos, donde se detalle su número de serie, marca y modelo. Se debe llevar un registro estricto con los datos de la empresa y la persona que se lleva dicho equipo. Para cualquier traslado de equipos o dispositivos que contengan información y archivos, los mismos deben ser borrados para evitar la fuga de información.

## 6.8 Seguridad de las operaciones

### 6.8.1 Lineamiento general

1. Seguir lo estipulado en el procedimiento gestión de los cambios de TI del proceso de gestión de servicios de TI, garantizando un adecuado control de cambios y el seguimiento a estándares de seguridad que deben definirse, así como el seguimiento a los incidentes de seguridad que puedan presentarse.
2. Garantizar una adecuada planificación y aprobación de los sistemas de información que consideren o provean las necesidades de capacidad futura.
3. Monitorear el funcionamiento del antivirus para la protección de la información de la Entidad.



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

4. Mantenimiento de los Firewall Fortinet, ya que permite la creación de redes seguras y proporcionan una protección amplia, integrada y automatizada contra amenazas emergentes y sofisticadas.

### 6.8.2 Instalaciones de software en sistemas operativos y restricción sobre la instalación de software

Solo personal designado por el Oficina de Informática y Sistemas está autorizado para instalar software o hardware en los PC, portátiles, servidores e infraestructura de telecomunicaciones la Entidad.

## 6.9 Adquisición, desarrollo y mantenimiento de sistemas

### 6.9.1 Lineamiento general

Se debe asegurar un adecuado análisis e implementación de los requerimientos de seguridad en el software desde su diseño, ya sea interno o adquirido y debe incluir garantías de validación de usuarios, datos de entrada y salida, así como de los procesos mismos, de acuerdo con la clasificación de los activos a gestionar en la herramienta.

Para todos los sistemas automáticos que operen y administren información para el FONCEP, se deben buscar que se pueda realizar registro de los eventos de seguridad y permitir el monitoreo de accesos indebidos e intrusiones y la activación de archivos de registro de auditoría (Logs), establecido en el Procedimiento de gestión de logs, que permitan determinar y demostrar las distintas acciones modificaciones que sufre esa información crítica y que pueda ser evaluada y auditada por el dueño del activo de la información.

Toda la información utilizada y almacenada en los distintos sistemas informáticos, debe tener un responsable o dueño directo quien es el encargado de establecer los niveles de clasificación aplicable, según lo dicta el Procedimiento gestión de activos.

### 6.9.2 Análisis y especificación de los requisitos de seguridad en la adquisición de software



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

ALCALDÍA MAYOR DE BOGOTÁ D.C.
FONDO DE PRESTACIONES ECONÓMICAS, CESANTÍAS Y PENSIONES

La inclusión de un nuevo producto de software en el FONCEP o control de cambio a los aplicativos existentes, debe estar precedida de la definición de los requerimientos funcionales y características o especificaciones de seguridad asociados a él y a su implantación.

## 6.10 Gestión de incidentes de seguridad de la información

### 6.10.1 Lineamiento general

Se debe asegurar que se haga una adecuada evaluación del impacto en el FONCEP frente a los eventos de seguridad relevantes, en los cuales la política de seguridad o sus lineamientos hayan sido desatendidas o traspasadas y realizar planes de atención de incidentes y mejora de procesos, para aquellos eventos que resulten críticos para la supervivencia de este. Estos planes deben considerar medidas técnicas, administrativas y de vínculo con Entidades externas; deben probarse y revisarse periódicamente; y deben estar articulados en todo el organismo con los diferentes tipos de recursos tecnológicos y no tecnológicos. FONCEP debe contar con los procedimientos que se consideren necesarios para el reporte, control, seguimiento, recolección de evidencias, solución, mejoramiento y aprendizaje.

## 6.11 Teletrabajo

Seguir lo estipulado acorde a los lineamientos para el teletrabajo del proceso de Gestión de Talento Humano, que tiene como objetivo: Evaluar, seleccionar, vincular y hacer seguimiento a los servidores públicos vinculados en la modalidad de teletrabajo incluyendo las condiciones mínimas requeridas para teletrabajar, garantizando el cumplimiento de lo pactado en el acuerdo del teletrabajo y buscando una percepción positiva de esta modalidad laboral en el Fondo de Prestaciones, Cesantías y Pensiones - FONCEP.

### 6.11.1 Lineamientos técnicos del teletrabajo

El objeto es establecer los lineamientos técnicos en seguridad de la información necesarios para aplicar el Teletrabajo de conformidad con las nuevas tecnologías de la Información y Comunicación desarrolladas o que lleguen a serlo dentro del FONCEP, con la finalidad de cuidar la confidencialidad, integridad y disponibilidad de la información de FONCEP.



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

1. El funcionario de FONCEP debe cumplir los siguientes requisitos:

   **a.** Ser funcionario de FONCEP.
   **b.** Postulación a teletrabajo.
   **c.** Diligenciar los formatos relacionados con el teletrabajo del proceso de Gestión de Talento Humano.
   **d.** Contar con el aval del área de Talento Humano y el jefe inmediato de la dependencia correspondiente.
   **e.** Contar con un espacio físico de acuerdo con la Ley 6727 de riesgos de trabajo y su normativa.
   **f.** Tener acceso a internet en el lugar señalado para teletrabajar.
   **g.** Acto administrativo o Resolución por la cual se autoriza a un funcionario realizar su propósito principal y sus funciones mediante teletrabajo suplementario en FONCEP.

2. Resguardar la confidencialidad y seguridad de la información que utilice y a la que pueda acceder en el desempeño de sus funciones, evitando por todos los medios un uso inapropiado de la misma, según se establece en la normativa institucional.
3. Es deber del teletrabajador, dar un uso adecuado a los equipos proporcionados por esta Entidad (si aplica), así como a las herramientas que la misma, ponga a su disposición y a utilizarlas exclusivamente con los fines laborales definidos. En caso de efectuarse un uso indebido de los equipos de cómputo suministrados, conforme con los lineamientos consagrados por esta Entidad, la responsabilidad por el daño o pérdida de estos será trasladada al teletrabajador, sin perjuicio de las acciones disciplinarias o fiscales que procedan.
4. De igual manera, es deber del teletrabajador reintegrar los equipos informáticos que se le hayan asignado, en condiciones que permitan su funcionamiento, una vez finalizada la modalidad de teletrabajo.
5. Los teletrabajadores del FONCEP son responsables de las acciones y operaciones ejecutadas en los mismos, así como de las acciones realizadas a través del usuario y contraseña asignados, conjuntamente son garantes de la seguridad física del sitio de teletrabajo y deben cumplir con el esquema de licenciamiento definido por la Entidad.
6. Los funcionarios no deben compartir sus cuentas de usuario y contraseñas, ni desatender su sesión de Teletrabajo, ni utilizar conexiones no confiables (conexiones Wifi-abiertas, acceder a conexiones y/o redes públicas, módems USB), conjuntamente deben adherirse a los lineamientos de seguridad de la información definidos por FONCEP.
7. Los propietarios de los activos de información deben velar por la autorización, asignación, modificación y cancelación de privilegios de accesos a los entornos confiables (Teletrabajo), de acuerdo con los perfiles establecidos y las necesidades de uso.



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

ALCALDÍA MAYOR DE BOGOTÁ D.C.
FONDO DE PRESTACIONES ECONÓMICAS, CESANTÍAS Y PENSIONES

8. Los propietarios de los activos de información deben monitorear periódicamente los accesos a los entornos confiables (Teletrabajo) asignados a los funcionarios.
9. Los propietarios de los activos de información deben definir los sistemas y servicios internos autorizados para el entorno de Teletrabajo, debe acoger los horarios de trabajo definidos por FONCEP y comunicar los horarios a los funcionarios asignados a Teletrabajo.
10. El proceso de Gestión de Servicios TI debe asignar los accesos a los entornos confiables (Teletrabajo) del FONCEP, debe definir un esquema para el licenciamiento de software, para la gestión de las actualizaciones y las versiones del software instaladas en los dispositivos utilizados para Teletrabajo.
11. La Oficina de Informática y Sistemas debe controlar el acceso a los entornos confiables (Teletrabajo), conjuntamente debe garantizar que los funcionarios asignados a teletrabajo cuentan con medidas de seguridad para los equipos asignados y/o utilizados para Teletrabajo (conexión VPN, actualización periódica del sistema operativo, del software antivirus, antimalware, Firewall, el usuario no tiene permisos para instalar software), con conexión de asistencia remota y con herramientas de borrado remoto de dispositivos.
12. El proceso de Gestión de Servicios TI debe establecer la conexión y asistencia remota, para el borrado remoto de dispositivos y para revocar los permisos del usuario en caso de emergencia. Simultáneamente deben tener un registro de todos los dispositivos utilizados para teletrabajo. Igualmente debe contar con un registro o log de accesos válidos y rechazados.
13. La Oficina de Informática y Sistemas debe proporcionar repositorios para el almacenamiento de la información gestionada en los entornos confiables (Teletrabajo); proporcionar rutinas y medios de respaldo, establecer un acceso controlado y con restricción de privilegios.
14. El proceso de Gestión de Servicios TI debe suministrar acceso al escritorio virtual o utilizar un arranque dual, para dividir los entornos de trabajo (entorno Teletrabajo y entorno personal) y debe proteger los datos del entorno de teletrabajo a través del cifrado de la información a para evitar cambios no autorizados y fugas de información.

## CONTROL DE CAMBIOS

| VERSIÓN | FECHA | DESCRIPCIÓN DE LA MODIFICACIÓN |
|---|---|---|
| 001 | Septiembre de | Creación y Adopción del Documento. El documento pertenecía al proceso de Gestión de |



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

| | | |
|---|---|---|
| | 2017 | Administración de activos. |
| 002 | Julio de 2019 | Adición del capítulo 6.3 Política del tratamiento de datos personales y capítulo 5 roles y responsabilidades. |
| 003 | Agosto de 2020 | Cambio en la plantilla vigente<br>Complementar y especificar aspectos relacionados con la actual política de tratamiento de datos personales en cuanto normativa, definiciones, objeto de FONCEP, actualización, rectificación, supresión de datos y revocación de la autorización de tratamiento de datos personales, canales presenciales y no presenciales.<br>Unificar documentos relacionados con políticas ya existentes dentro del manual |
| 004 | Diciembre de 2021 | Actualización de la Política general de seguridad de la información, ajuste de los lineamientos y consideraciones generales. Racionalización del documento dando mayor claridad y haciéndolo más concreto en su contenido. |

| ELABORADO POR: | REVISADO POR: | APROBADO POR: |
|---|---|---|
| María del Pilar Segura González<br>**Enlace**<br>Profesional OIS | Wilson Barrios Delgado<br>**Responsable del proceso**<br>Jefe OIS<br><br>Alejandra Paola Suarez Franco<br>**Asesor OAP**<br>Profesional OAP | Wilson Barrios Delgado<br>**Líder del proceso**<br>Jefe OIS<br><br>Cristian Mauricio Amaya Martínez.<br>**Jefe OAP** |



**Sede Principal**
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

ALCALDÍA MAYOR DE BOGOTÁ D.C.
FONDO DE PRESTACIONES ECONÓMICAS, CESANTÍAS Y PENSIONES