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 políticas 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:

- **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"
- **Resolución 305 del 20 de octubre 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."
- **NORMA TÉCNICA NTC-ISO-IEC COLOMBIANA 27001** "La NTC ISO 27001 es una norma colombiana que hace posible que las organizaciones aseguren la confidencialidad y al mismo tiempo la integridad de toda la información."
- **GUÍA TÉCNICA GTC-ISO/IEC COLOMBIANA 27002** "Guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información."
- **Comité institucional de gestión y desempeño No. 8 del 31 de julio de 2019** "Por medio del cual aprueba el Manual de Modelo de Seguridad y Privacidad de la Información"

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

- **Constitución Política** "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".
- **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".
- **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".
- **Decreto 2952 de 2010** "Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008".
- **Ley 1581 de 2012** "Por la cual se dictan disposiciones generales para la protección de datos personales".
- **Decreto 1377 de 2013** "Por el cual se reglamenta parcialmente la Ley 1581 de 2012".
- **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 103 de 2015,** "Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones".
- **Ley 1755 de 2015**, a través de la cual se regula el derecho de petición incorpora en el numeral 3 del artículo 24 información con carácter reservado, entre otros casos, el referente a historial laboral y los expedientes pensionales, en su parágrafo determina que, para efecto de la solicitud de dicha información sólo podrá ser solicitada por el titular de la información, por sus apoderados o por personas autorizadas con facultad expresa para acceder a esa información.
- **Decreto 1080 del 26 de mayo de 2015**, en la Parte VIII, Título III del, establece nuevas disposiciones y aclara temas relacionados con la gestión de la información pública en cuanto a su divulgación, publicación, recepción, clasificación y reserva, así como también, la elaboración de instrumentos de gestión de la información y de seguimiento.
- **Decreto 1080 de 2015**, Artículo 2.8.7.4.2. con relación a los documentos de información pensional, que cuando una entidad tenga a su cargo el reconocimiento y pago de pensiones y, entre en un proceso de liquidación, deberá entregar a la entidad

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

que se determine en el Acto Administrativo el conjunto de todos los archivos físicos y electrónicos de conformidad con los parámetros del mencionado Decreto y con los procedimientos establecidos por el Archivo General de la Nación.

- **Sentencias de la Corte Constitucional: C-1011 de 2008** "Mediante la cual se estudia la exequibilidad de la Ley Estatutaria 1266 de 2008 y C-748 de 2011 mediante la cual se estudia la exequibilidad de la Ley Estatutaria 1581 de 2012"

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.
Confidencialidad	Es la propiedad que impide la divulgación de información a individuos, entidades o procesos no autorizados
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)

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

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.
Información	Conjunto organizado de datos procesados, que constituyen un mensaje.
Integridad	Correctitud y completitud de la información en una base de datos.
MSPI	Modelo de Seguridad y Privacidad de la Información
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.
Titular	Persona natural o jurídica cuyos datos sean objeto de tratamiento.
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**

Introducción

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 un Sistema de Gestión de la Seguridad de la Información (SGSI), 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. El SGSI protege los activos de información de una organización, independientemente del medio en que se encuentre.

La seguridad de la información se establece mediante la implementación de un conjunto adecuado de políticas, procesos, procedimientos de la organización, controles, hardware y software; pero lo más importante, mediante comportamientos éticos de las personas.

La seguridad de la información es la preservación de los principios básicos de la confidencialidad, integridad y disponibilidad de esta y de los sistemas implicados en su tratamiento. Estos tres pilares se definen como:

- Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados.
- Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- Disponibilidad: Acceso a la información y los sistemas de tratamiento de esta por parte de los usuarios autorizados cuando lo requieran.

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

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), ha expedido la RESOLUCIÓN No. DG—0231 - 11 JUL 2016.

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**

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**

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**

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**

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

Desarrollo del Manual

1. Alcance de la política de seguridad de la información

Teniendo como marco la norma técnica NTC-ISO/IEC 27001 en su versión 2013, las políticas de seguridad de la información del FONDO DE PRESTACIONES ECONOMICAS, CESANTIAS Y PENSIONES – FONCEP, están dirigidas a:

- 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.
- Todos los recursos y activos de información de la Entidad.
- Todos los procesos y procedimientos de la Entidad.
- Toda la infraestructura tecnológica y los Sistemas de Información que soportan la funcionalidad de la Entidad y todas las sedes físicas de la Entidad.

2. Política general de Seguridad de la Información

El FONDO DE PRESTACIONES ECONOMICAS, CESANTIAS Y PENSIONES – FONCEP, como entidad responsable del pago de cesantías y reconocimiento y pago de pensiones a las servidoras y servidores públicos del Distrito Capital, con régimen de retroactividad, afiliados al FONCEP; es consiente 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 protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad al interior de la Entidad.

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

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 políticas, normas y procedimientos específicos los cuales guiaran la gestión adecuada de la información.

3. Objetivos específicos de seguridad de la información

Para cada uno de los 114 controles contenidos en los 14 objetivos de control definidos en el Anexo A de la norma ISO-IEC- 27001-2013, se deben establecer la declaración de aplicabilidad que permitan a la Entidad proteger su información; los cuales deben ser implementados de acuerdo con las metas y objetivos relacionados en el Plan Estratégico 2016-2019.

Consciente de sus necesidades actuales el FONCEP implementar un Modelo de Seguridad y Privacidad de la Información (MSPI), como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información de la Entidad.

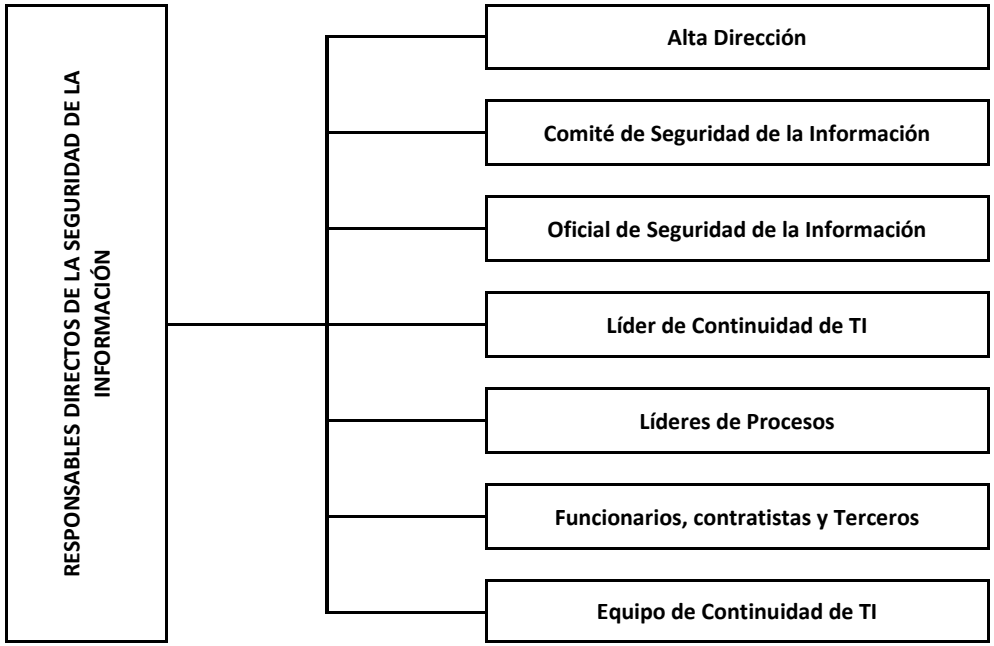
4. Implementación del MSPI

Para la implementación del MSPI, se ha incluido en el plan estratégico el proyecto denominado “Implementar el Modelo de Seguridad y Privacidad de la Información (MSPI)”, y su control se realizará mediante la metodología establecida por la Entidad.

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

5. Roles y Responsabilidades generales de la seguridad de la información.

La asignación y delimitación de responsabilidades para asegurar que se implanta y satisfacen 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. A continuación, se describe el gobierno de la seguridad de la información para FONCEP: Los siguientes entes son responsables, en distintos grados, frente a la seguridad de la información en la Compañía:



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

Roles	Responsabilidades y Funciones
Alta Dirección	El equipo de la alta dirección y el Comité de Seguridad de la Información son responsables de garantizar que la seguridad de la información se aborde adecuadamente en toda la Entidad. Cada uno de los funcionarios de la alta dirección son los responsables de velar por la protección de la información que se gestiona en su área 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. La Dirección General es el dueño de la política de seguridad de la información y delega las responsabilidades de documentación sobre seguridad de la información a la persona responsable de la SGSI quien se apoyará en la Oficina de Informática y Sistemas para las definiciones y modificaciones que pueda requerir esta política con el trascurso del tiempo. Cualquier cambio a la política deberá ser aprobado por el Director General, Dueño de Proceso TI y Jefe de Infraestructura y/o Oficial de Seguridad Informática. Velar por la aplicación del Plan de Continuidad de TI, así como formular, y gestionar las modificaciones en el mismo, y someterlas a aprobación por parte de la Junta Directiva. Validar los procesos críticos empresariales que se deban considerar en el Plan de Continuidad de TI, así como la estimación del tiempo máximo que puede soportar la Entidad con la interrupción del servicio, producto del incidente que se presente. Asegurar que se formulen, evalúen, y mantengan actualizados los Planes de Continuidad de TI, por parte de los responsables de los procesos críticos, y que se divulguen a todos los funcionarios, contratistas y proveedores de servicios. Se entiende como plan de continuidad de TI, un plan documentado y probado con el fin de responder ante una emergencia de manera adecuada, logrando así el mínimo impacto en la operación del negocio. Garantizar que se documenten y mantengan actualizados y disponibles los procedimientos para hacer frente a un incidente, desde que éste se presenta, hasta la restauración o vuelta a la normalidad, tanto en lo que se refiere al accionar interno como externo a la Empresa.

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

	Asegurar que las funciones y responsabilidades detalladas en los planes de continuidad de negocio, se asignen al personal idóneo para la atención de los incidentes. El mismo criterio se aplicará al plan de sucesión en caso de incidentes. Velar porque se cumpla con los planes de capacitación al personal, tanto titular como sucesor en los roles que debe desempeñar en caso de incidentes. Asegurar que, como parte de los planes de continuidad, se elaboren y actualicen los planes de comunicación interna y externa, para aplicar cuando se presente un incidente. Establecer el mecanismo para asegurar que se considere la opinión de los sujetos interesados en la elaboración de los planes. Asegurar que se mantenga actualizada la evaluación de proveedores de insumos para los procesos críticos y que se evalúen periódicamente los requerimientos de repuestos en stock para esos procesos críticos. Asegurar que los planes de continuidad incluyan en forma detallada los roles ante la presencia de un incidente y que se realicen las pruebas de validación y efectividad de estos planes, así como de control del tiempo requerido para la restauración de las operaciones. Asegurar que, ante cambios significativos en los procesos empresariales, se actualice el plan de continuidad de TI.
Comité de Seguridad de la Información	Está encargado de elaborar y actualizar las políticas, normas, pautas y procedimientos relativos a seguridad de la información. También es responsable de coordinar el análisis de riesgos, planes de contingencia y prevención de desastres. Durante sus reuniones, el Comité efectuará 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. El Comité de Seguridad de Información de la Entidad, será el responsable de velar por el cumplimiento del plan de implementación del MSPI. El Comité deberá asegurar que exista una dirección y apoyo gerencial para soportar la administración y desarrollo de iniciativas sobre seguridad de la información, a través de compromisos apropiados y uso de recursos adecuados en el organismo, así como de la formulación y mantenimiento de una política de seguridad de la información a través de todo el organismo.

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

	Funciones del comité. • Coordinar la implementación del Modelo de Seguridad y privacidad de la Información al interior de la entidad. • Revisar los diagnósticos del estado de la seguridad de la información en Nombre de la entidad. • Acompañar e impulsar el desarrollo de proyectos de seguridad. • 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. • Recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información. • Aprobar el uso de metodologías y procesos específicos para la seguridad de la información. • Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar, riesgos. • Realizar revisiones periódicas del SGSI (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes. • Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad. • Poner en conocimiento de la entidad, los documentos generados al interior del comité de seguridad de la información que impacten de manera transversal a la misma. • Las demás funciones inherentes a la naturaleza del Comité.

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

Oficial de Seguridad de la Información	El Oficial de seguridad de la información de FONCEP o quien haga sus veces, debe definir los procedimientos para aplicar la Política de seguridad informática y seleccionar los mecanismos y herramientas adecuados que permitan aplicar las políticas dentro del FONCEP • Aplicar conocimientos, habilidades, herramientas, y técnicas a las actividades que permitan la implementación del MSPI • Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación de la entidad. • Generar el cronograma de la implementación del Modelo de Seguridad y privacidad de la información. • Planear, implementar y hacer seguimiento a las tareas, fechas, costos y plan de trabajo de los objetivos específicos del cronograma definido. • Realizar un seguimiento permanente a la ejecución de los planes de trabajo, monitoreando los riesgos de seguridad digital y reportar al Comité de seguridad en caso de ser necesario. • Trabajar de manera integrada con el grupo o áreas asignadas

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

Líder de Continuidad de TI	Es el encargado de dirigir y liderar todas las actividades del plan de continuidad de TI. Es responsable de declarar la contingencia ante el escenario de interrupción del centro de cómputo principal, con base en las decisiones tomadas por el Equipo de Continuidad del Negocio o en situaciones donde amerite realizar su activación inmediata. Responsabilidades • Identificar los posibles riesgos de aspectos tecnológicos que afectan la continuidad de la operación normal de la Entidad y que ponen al descubierto debilidades del plan de continuidad. • Mantener comunicación constante entre Coordinadores de Recuperación del Negocio durante el estado de contingencia. • Entregar los reportes correspondientes al Comité Directivo sobre el estado de la recuperación. • Salvaguardar la confidencialidad, integridad y disponibilidad de los activos, información, datos y servicios de TI de la Entidad. • Coordinar con el Comité Directivo, la actualización, mantenimiento y probar el plan de continuidad de TI. • Evaluar y solicitar los recursos requeridos para establecer y mantener la estrategia de recuperación y contingencia de la entidad. • Monitorear los reportes sobre el estado de recuperación o evaluación durante una contingencia. • Velar por la ejecución del debido análisis causa – raíz del evento que ocasionó la contingencia.
Líderes de Procesos	Son los responsables de la aprobación de cambios o desarrollos adicionales sobre un sistema, así como la definición de usuarios que podrán acceder al sistema y los niveles de accesos otorgados a cada usuario para el cumplimiento de sus funciones con respecto a esta aplicación. Son los responsables de la identificación y actualización de los activos de información de cada uno de los procesos de la Entidad.

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

Funcionarios, Contratistas, Terceros y Proveedores	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 la Entidad. Estos deben firmar un acuerdo de confidencialidad con la Entidad cuando requieran conocer, acceder o manejar información confidencial o alguno de sus clientes. Es responsabilidad de toda persona vinculada como funcionario de carrera administrativa, libre nombramiento y remoción, provisionalidad, temporalidad, contratista o pasante; reportar los incidentes de seguridad, eventos sospechosos y/o el mal uso de los recursos institucionales de los cuales tenga conocimiento.
Equipo de Continuidad de TI	Conformado por los líderes designados o delegados de los procesos críticos quienes son los responsables de liderar y evaluar la funcionalidad de la operación del Plan de Continuidad de TI e informar al Líder de Continuidad de TI cualquier cambio que afecte las estrategias definidas en el mismo.

6. Otras políticas asociadas

Adicionalmente se definen las siguientes políticas, que determinan el comportamiento y los lineamientos que se deben cumplir en materia de seguridad de la información.

6.1 Organización de la seguridad de la información

6.1.1 Objetivo

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

Garantizar un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la entidad y establecer los lineamientos de seguridad de la información en el uso de opciones de teletrabajo y el uso de dispositivos móviles.

6.1.2 Política

Se debe establecer la organización interna y los roles para el manejo de la seguridad de la información, estableciendo contactos con las autoridades y grupos de interés en la materia, a fin de poder contar con las directrices y apoyo requerido en el proceso de implementación del Modelo de Seguridad y Privacidad de la Información.

Se debe implementar esquemas de seguridad de la información, en el manejo de los proyectos de la Entidad y definir políticas y gestión de seguridad para el manejo de dispositivos móviles que se conecten a la red interna de la Entidad y para los esquemas de teletrabajo que se implementen.

6.2 Seguridad de los Recursos Humanos.

6.2.1 Objetivo

Establecer las responsabilidades del personal en materia de Seguridad de la Información, las necesidades de capacitación y los procedimientos de manejo de incidentes, con el objeto de reducir el riesgo de error humano, fraude o mal uso de los bienes de información.

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

6.2.2 Política

Desde la vinculación del personal al FONCEP, se deben tener controles que permitan verificar la idoneidad e identidad, ética profesional y conducta. Los términos y condiciones de empleo o trabajo deben establecer la responsabilidad de los funcionarios, temporales, supernumerario y contratistas, por la seguridad de los activos de información, que van más allá de la finalización de la relación laboral o contractual, por lo que se debe firmar un acuerdo de confidencialidad por todas las personas vinculadas a la Entidad, independiente de su forma de vinculación.

El personal vinculado al FONCEP, deben cooperar con los esfuerzos por proteger la información y ser responsables de actualizarse en cada materia, así como consultar, en caso de duda o desconocimiento de un procedimiento formal, ya que esto no lo exonera de una acción disciplinaria que deba llevarse a cabo cuando se incurra en violaciones a las políticas, controles o normas de seguridad.

Para la implementación de esta política se debe tener en cuenta entre otros los siguientes principios.

6.2.3 Funciones y responsabilidades

Todas las personas vinculadas al FONCEP como funcionario de carrera administrativa, libre nombramiento y remoción, provisionalidad, temporalidad, contratista y pasante; deben tener claramente definidas sus funciones y su rol y responsabilidades en cuanto a la Seguridad de la Información dentro de la Entidad. Adicionalmente, se deben establecer las responsabilidades y derechos legales del empleado o contratista en cuanto a aspectos de propiedad intelectual, protección de la información y leyes aplicables.

6.2.4 Selección

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

Todas las personas vinculadas al FONCEP como funcionario de carrera administrativa, libre nombramiento y remoción, provisionalidad, temporalidad, contratista y pasante; deben ser adecuadamente seleccionados, de acuerdo con el Manual del Funciones del cargo y deben aceptar las políticas de Seguridad de la Información establecidas y definidas, las cuales deben ser conocidas por el empleado o contratista en el momento de su vinculación. Cuando la vinculación se realice por intermedio de terceros, se debe especificar la responsabilidad de ellos en el proceso de selección y la forma en que se debe manejar cualquier incumplimiento de los requisitos establecidos.

6.2.5 Términos y condiciones laborales

Existirá una Cláusula de confidencialidad y buen manejo de la información, para todos los usuarios del Sistema de Información o funcionarios del FONCEP, la cual se hará conocer al momento de hacer entrega del usuario creado para cada uno, y se incluirá de manera expresa esta cláusula en los contratos de servicio firmados con otras empresas o con contratistas directos del FONCEP o con terceros. Este requerimiento también se debe aplicar al caso de contratación de personal temporal o cuando se permita el acceso a los recursos informáticos del FONCEP a usuarios externos y se definirá y asignará claramente las responsabilidades para llevar a cabo la terminación o el cambio a nivel laboral.

6.2.6 Responsabilidades de la Dirección

La dirección exigirá que los empleados, contratistas y usuarios externos apliquen la seguridad según las políticas y los procedimientos establecidos por el FONCEP.

6.2.7 Educación, formación y concientización sobre la seguridad de la información.

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

Los funcionarios del FONCEP serán entrenados y capacitados para las funciones y cargos a desempeñar con el fin de proteger adecuadamente los recursos y la información de la entidad. En los casos en que así se establezca, este entrenamiento debe cubrir a personal contratista, o terceros, cuando sus responsabilidades lo exijan. Existirá 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 Informática detalladas en este documento y la necesidad de respaldarlas y aplicarlas de manera permanente.

6.2.8 Proceso disciplinario

Todos los incidentes de seguridad ocurridos en el FONCEP deben ser investigados con el fin de determinar sus causas y responsables. Los procesos derivados de los reportes y análisis de los Incidentes de Seguridad deben ser manejados por el área encargada en el FONCEP, de acuerdo con el resultado de la incidencia.

6.2.9 Devolución de activos

En el retiro de cualquier funcionario de la Entidad, independiente de su modalidad de vinculación, se debe contar con un procedimiento para garantizar que todos los activos de información manejados y asignados al funcionario se transfieran al FONCEP y se elimine con seguridad la información del equipo del usuario.

Se documentará y transferirá a la entidad el conocimiento que sea importante para la continuidad de las operaciones que tenga un empleado, contratista o usuario de terceras partes.

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

6.2.10 Retiro de los derechos de acceso

Los derechos de acceso de todos los empleados, contratistas o usuarios de terceras partes a la información y a los servicios de procesamiento de información se retirarán al finalizar su contratación laboral, contrato o acuerdo o se deben ajustar después de un cambio o traslado del funcionario.

6.3 Tratamiento de datos personales.

6.3.1. Alcance

La política de tratamiento y protección de Datos Personales presentada a continuación se aplicará a todas las bases de datos y/o archivos que contengan datos personales y que sean objeto de tratamiento por FONCEP, considerado como responsable y/o encargado del tratamiento de estos datos.

6.3.2. Ámbito de aplicación

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

1. Principios

Para la interpretación e implementación de la presente política, se aplicarán, de manera armónica e integral, los siguientes principios:

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

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.

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;

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

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 la misma.

6.3.3. 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

6.3.4. Tratamiento y finalidades

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

El tratamiento que realizará 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.
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.

c) 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.
d) Gestionar, normalizar, cobrar y recaudar la cartera hipotecaria del Fondo de Ahorro y Vivienda Distrital – FAVIDI.
e) 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.

6.3.5. 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.

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

f) Tramitar las consultas y reclamos formulados en los términos señalados en la presente política.

6.3.6. 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:

- 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.

6.3.7. 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:

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

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.
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.

6.3.8. Procedimiento para 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 seguirá el siguiente procedimiento, 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 las mismas:

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, podrán solicitar a FONCEP:
   - Información sobre los datos personales del Titular que son objeto de tratamiento.

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

- Información respecto del uso que se le ha dado por FONCEP a sus datos personales.
- Salvo norma legal especial y so pena de sanción disciplinaria, toda petición deberá resolverse dentro de los quince (15) días siguientes a su recepción.
- 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:

- La corrección o actualización de la información.
- 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.

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

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.

6.3.9. Seguridad de la Información

FONCEP aplicará las mejores prácticas para la seguridad, discreción, protección, almacenamiento y confidencialidad de los Datos Personales de los titulares. Verificará cuando corresponda, la procedencia de las excepciones legales para entregar los datos personales a las autoridades y en los casos pertinentes.

6.3.10. Vigencia de la política

La presente política rige a partir de la fecha de su aprobación y publicación en el portal web de la entidad y deja sin efectos las demás disposiciones institucionales que le sean contrarias.
En el evento de surgir alguna circunstancia no contemplada en la presente política, se reglamentará de acuerdo al Régimen General de Protección de Datos Personales vigente en Colombia.
Actualizaciones de la política: FONCEP puede modificar la presente política en la medida que se actualice la normatividad aplicable en los casos que por su gestión administrativa o misional así lo requiera, en tal evento se publica en la página web de la entidad.

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.

El Proceso de Gestión de Servicios de TI del FONCEP, pone a disposición de los funcionarios, proveedores y terceros, los recursos tecnológicos necesarios para el soporte a los procesos de la entidad.
Para FONCEP la información es considerada como un activo de valor estratégico, por esta razón se deberán implementar los mecanismos necesarios que garanticen un adecuado tratamiento en el ciclo de vida de la información, especialmente para los casos que requieren mantener la disponibilidad de la misma.
Se deberá preservar la seguridad de la información dando cumplimiento a los principios de Confidencialidad, Integridad y Disponibilidad de la información de la organización. La información de la organización deberá mantenerse disponible a las personas autorizadas para ello en el momento en que se necesite. La organización deberá identificar mecanismos que permitan que las actividades de respaldo y recuperación de la información sean adecuadas costo / beneficio. Los niveles de protección y clasificación establecidos para la información de la organización deberán ser mantenidos en todo momento. (Acceso, toma de respaldo, backup, transporte, recuperación, otros). Por lo tanto, se deben mantener los controles y medidas establecidas para esto. Los usuarios de la organización son responsables de alojar la información que necesita ser respaldada en los lugares establecidos para ello. Los usuarios respaldarán y protegerán, con medidas que eviten accesos de personas no autorizadas, aquellos activos digitales de información que estén almacenados en elementos de TI de uso personal, que les hayan sido asignados. Se deberán preservar los lineamientos de acuerdo a la sensibilidad y nivel de clasificación de seguridad. Los usuarios son responsables de aplicar los controles para la protección de la información según su nivel de clasificación. Así mismo deberán alertar al área del CRIE y la División de Sistemas cuando un activo digital de información requiera medidas especiales de protección. Los funcionarios de la organización deberán seguir los procedimientos de respaldo de la información y realizar su seguimiento.

6.4.1 Objetivo

Mantener un inventario de activos o bienes de información, así como los propietarios y responsables de su gestión para establecer un nivel de protección adecuado para los mismos.

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

6.4.2 Política

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 los criterios que dicte el Comité de Seguridad de la Información del FONCEP. A partir de esta clasificación se establecerán los niveles de protección orientados a determinar a quién se le permite el manejo de la información, el nivel de acceso a la misma y los procedimientos para su manipulación. La clasificación debe revisarse periódicamente y atender a los cambios que se presenten en la información o la estructura que puedan afectarla.

6.4.2.1. Políticas de uso generales

- 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 dará lugar a las acciones disciplinarias y/o legales que correspondan. El ingreso y utilización de estos sistemas implica su consentimiento con esta política.
- 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.
- 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.

6.4.2.2. Políticas de Uso de Contraseñas

- El proceso de Gestión de Servicios TI establecerá el uso de contraseñas para los recursos informáticos sensibles.
- 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.

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 contraseña de la cuenta de usuario asignada por primera vez debe ser cambiada en el primer inicio de sesión
- Las contraseñas deben cumplir con los siguientes requisitos:
  - Tener mínimo ocho caracteres.
  - Contener caracteres en mayúsculas y minúsculas (es decir, Aa-Zz)
  - Contener caracteres numéricos (0 a 9)
  - Contener por lo menos un carácter especial (!@#$%^&*()_+|~-=\ `{}[]:";'<>?,./)
- Se debe exigir el cambio de contraseña de red, del correo institucional o de cualquier recurso donde aplique, cada 90 días, advirtiendo sobre este cambio al usuario a partir de 5 días antes de su vencimiento.
- La Mesa de Ayuda de Gestión de Servicios TI no restablecerá contraseña a un usuario, a menos que éste mismo lo solicite.
- 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.

6.4.2.3. Políticas de Uso de Recursos Compartidos

- Las carpetas compartidas son una herramienta de trabajo necesario, pero con altos riesgos que pueden afectar la confidencialidad, integridad y disponibilidad de la información, por lo tanto, es responsabilidad de los usuarios de este recurso su preservación.
- No se permite el uso de carpetas compartidas en equipos de escritorio. La entidad provee este recurso centralizado y con las medidas de seguridad requeridas.
- Gestión de Servicios TI provee la configuración de acceso a la carpeta, a través de la Mesa de Servicios y previa autorización de los directores de área del funcionario o a quien él delegue.
- Se debe definir el tipo de acceso y los perfiles estrictamente necesarios sobre la carpeta (lectura, escritura, modificación y borrado).
- Este servicio debe ser desactivado una vez se pierda el vínculo laboral o contractual de los funcionarios y/ proveedores o terceros respectivamente.
- El proceso de Gestión de Servicio TI, en caso de tratase de información confidencial o crítica para la entidad, debe incluir estas carpetas en las copias diarias de respaldo de información.

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

- De acuerdo con la clasificación de la información contenida en las carpetas compartidas, el acceso debe delimitarse a los usuarios autorizados por los responsables de la información y deben ser protegidas con contraseñas obligatoriamente.
- No está permitido utilizar sitios web para compartir información, salvo los autorizados por el proceso de Gestión de Servicios TI.

6.4.2.4. Políticas de Uso de Internet.

- El proceso de Gestión de Servicios de TI proveerá el servicio de internet para la entidad de forma segura, implementará los mecanismos necesarios para controlar el acceso a internet de acuerdo con los perfiles definidos.
- 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.
- 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.
- Ante la falta de control sobre sitios web no autorizados, todos los funcionarios, proveedores o terceros deben abstenerse de visitar declarados como no seguros, pornográficos o páginas de organizaciones delincuenciales o terroristas.
- El uso de Internet está restringido para descargar música, videos y juegos, o practicar juegos en línea.
- 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.
- No está permitido en ninguna circunstancia, aunque por fallas en el control el sistema lo permita, descargar o instalar o modificar programas ya instalados, no licenciados o no autorizados por el proceso de Gestión de Servicios TI en los computadores de la Entidad.

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

- Los funcionarios, proveedores o terceros no podrán 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.

6.4.2.5. Políticas de Uso de Correo Electrónico.

- El servicio de correo electrónico del FONCEP debe ser autorizado por directores de área del funcionario o a quien él delegue, y provisto por el proceso de Gestión de Servicios de TI. Solo podrá ser utilizado para fines laborales. Así mismo el uso desde dispositivos móviles debe ser autorizado por el proceso de Gestión de Servicios TI previa revisión de las medidas de seguridad. En el caso de proveedores o terceros, debe ser autorizado por el supervisor del contrato.
- 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
- Este servicio debe ser desactivado una vez se pierda el vínculo laboral o contractual de los funcionarios y/ proveedores o terceros respectivamente.
- La entidad podrá, 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.
- La emisión de cuentas de correo electrónico se realizará de la siguiente manera: La primera letra del nombre y el apellido completo con el dominio foncep.gov.co. En caso de que ya exista la cuenta se utilizará la letra inicial del segundo nombre.
- Los funcionarios, proveedores o terceros no podrán 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 o raza o invasión a la privacidad.
- No se permite el envío de correos masivos sin previa autorización del proceso de Gestión de Servicios TI.
- Está prohibido el envío de archivos ejecutables.
- No está permitido el reenvío automático de mensajes a direcciones de correo externas.
- En ningún caso acepte, abra ni comparta 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

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

- Se deben eliminar periódicamente los mensajes innecesarios.
- La firma de los correos electrónicos será obligatoria tanto para funcionarios de planta como proveedores o terceros y deberá contener: Nombre y Apellidos, Cargo o Proyecto, Nombre Entidad, Teléfono de contacto fijo o celular y/o extensión.
- Los correos electrónicos deben contener la sentencia de confidencialidad que debe incluirse inmediatamente después de la firma con el siguiente contenido:
  "CONFIDENCIALIDAD: La información transmitida a través de este correo electrónico es confidencial y dirigida única y exclusivamente para uso de su(s) destinatario(s). Su reproducción, lectura o uso está prohibido a cualquier persona o entidad diferente, sin autorización previa por escrito. Esta comunicación puede contener información protegida por derechos de autor. Si usted lo ha recibido por error, por favor notifíquelo inmediatamente al remitente y elimínelo de su sistema. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización del remitente será sancionado de acuerdo con las normas legales vigentes. Las opiniones, conclusiones y otra información contenida en este correo, no relacionadas con el FONCEP, deben entenderse como personales y de ninguna manera son avaladas por la empresa."

6.4.2.6. Políticas de Uso de Software.

- Ningún funcionario, proveedor o tercero puede instalar software licenciado o libre que no esté autorizado por Gestión de Servicios TI.
- 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.
- No está permitida la distribución del software licenciado o de propiedad de la entidad.

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

6.4.2.7. Políticas de Uso de Equipos Portátiles y Dispositivos Móviles.

- En caso de que el dispositivo móvil sea de propiedad de la entidad y sea asignado a un funcionario o en el caso que se autorice el acceso a información sensible por medio de dispositivos móviles como correo electrónico, propiedad de los funcionarios, proveedores o terceros, se deben tener en cuenta las siguientes normas de seguridad:
  - El dispositivo móvil debe estar guardado en un lugar no visible en sitios públicos.
  - El dispositivo móvil debe estar configurado para bloqueo automático a través de medios disponibles de configuración tales como contraseña, patrón huella dactilar, etc.
  - Debe contar con el uso de aplicación de antivirus.
  - No está permitido el acceso a la red corporativa desde dispositivos móviles cuando se accede mediante redes de acceso públicas, sin los mecanismos de acceso seguro.
- El proceso de Gestión de Servicios TI debe establecer las configuraciones aceptables para los dispositivos móviles institucionales o personales que hagan uso de los servicios de la entidad.
- El proceso de Gestión de Servicios TI debe contar con la opción de borrado remoto de información en los dispositivos móviles corporativos, evitando la divulgación no autorizada de información en caso de pérdida o hurto.
- El proceso de Gestión de Servicios TI debe incluir los dispositivos móviles a los procesos de copias de seguridad para la información contenida en los dispositivos móviles corporativos donde aplique.
- Los usuarios deben evitar usar los dispositivos en lugares inseguros para evitar pérdida o robo de estos.
- 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.
- Los usuarios deben evitar la instalación de programas desde fuentes desconocidas; solo Gestión de Servicios TI está autorizada para instalar software en ellos.
- Los usuarios deben evitar conectar los dispositivos móviles por puerto USB a cualquier computador o red pública.
- Los usuarios no deben almacenar videos, fotografías o información personal en los dispositivos móviles asignados.
- FONCEP debe adquirir pólizas de seguro con las entidades autorizadas con el objeto de cubrir los posibles eventos de pérdida o robo de los dispositivos móviles, portátiles y equipos de escritorio.

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

6.4.2.8. Política de Uso Periféricos y Medios de Almacenamiento Extraíbles.

- 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.
- El proceso de Gestión de Servicios TI debe propender los medios necesarios para evitar el uso de medio removibles en: servidor de Archivos, carpetas compartidas de forma segura, el uso del Drive del correo electrónico y otros medios
- El proceso de Gestión de Servicios TI gestionará el uso y retiro de los dispositivos removibles de forma segura.
- El proceso de Gestión de Servicios TI debe implantar los controles que regulen el uso de periféricos y medios de almacenamiento en la plataforma tecnológica de la entidad, de acuerdo con los lineamientos y condiciones establecidas.
- 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.

6.4.2.9. Políticas de Uso de Conexiones Remotas

- El proceso de Gestión de Servicios TI pondrá a disposición de los usuarios el acceso remoto solicitado por directores de área del funcionario o a quien él delegue e implementará los métodos y controles de seguridad necesarios para salvaguardar los activos de información.
- Los usuarios que realizan conexión remota deben aplicar las normas relacionadas a esta política, en especial sobre contraseñas, control de acceso, uso adecuado de los recursos, etc.
- Los usuarios únicamente deben establecer conexiones remotas en computadores previamente identificados y, en ninguna circunstancia, en computadores públicos.

6.4.2.10. Políticas de Confidencialidad de los Datos Personales.

- De acuerdo con la LEY ESTATUTARIA 1581 DE 2012, mediante la cual se dictan disposiciones generales para la protección de datos personales, la Entidad debe salvaguardar la información de datos personales y contenida en sus bases de datos y guardar confidencialidad sobre los mismos

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

- Todo funcionario, contratista y/o tercero debe guardar la confidencialidad de la información, especialmente sobre los datos personales de los ciudadanos registrados en las bases de datos de la Entidad a que tenga acceso.
- Las aplicaciones misionales no deben permitir, en lo posible, la consulta de los datos personales de los ciudadanos. En su defecto no permitir su copia, reproducción y/o divulgación sin previa autorización.
- El acceso a ésta solo debe ser autorizada por quien se haya definido como el responsable de la Información.
- Esta información se clasificará en un nivel alto de clasificación de confidencialidad, de acuerdo con la clasificación adoptada por la Entidad.

6.4.2.11. Políticas de Uso de Aplicaciones

- El acceso a las aplicaciones del FONCEP deben ser solicitadas por los directores de área o quien éste delegue, de acuerdo con el procedimiento establecido.
- Se debe contar con la definición de los responsables de cada aplicación quienes serán los responsables de autorizar los accesos a funcionarios, contratistas y/o terceros.
- Cada usuario de la Entidad debe contar con un usuario por cada aplicación o servicio que requiera de forma personal e intransferible.
- 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 Será responsabilidad del autorizador del acceso a cada aplicación la asignación del rol y menú de aplicaciones, de acuerdo con el procedimiento establecido.
- Los usuarios deberán informar a Gestión de Servicios TI si cuenta con un rol u opciones no autorizadas que vulneren cualquier activo de información.
- 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**

6.4.2.12. Políticas de equipos de usuario desatendido

- Con el fin de evitar pérdidas, daños o accesos no autorizados a la información, todos los funcionarios 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.
- El proceso de Gestión de Servicios TI diseñará y pondrá 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 de estar inactivo el equipo
- El funcionario custodio del equipo de cómputo es responsable por el cuidado, uso y seguridad del mismo y de la información manejada en él.
- El proceso de Gestión de Servicios TI iniciará un plan de concientización dirigido a los usuarios de FONCEP para que cambien su cultura y adopten esta política.
- 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. Todas las estaciones de trabajo deben usar el papel tapiz y el protector de pantalla corporativo, el cual se activará automáticamente después de cinco (5) minutos de inactividad y se podrá desbloquear únicamente con la contraseña del usuario.

6.4.2.13. Políticas de disposición y reutilización de equipos

- Los equipos de cómputo de FONCEP serán ubicados e instalados por personal perteneciente al proceso de Gestión de Servicios TI.
- El proceso de Gestión de Servicios TI tendrá como línea base un inventario tecnológico completo de los equipos informáticos, el cual deberá estar siempre actualizado con las novedades que se presenten en los equipos
- Para la instalación de los equipos de cómputo se deberán 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.

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

- Los equipos de cómputo serán 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.
- No está permitido el consumo de alimentos o bebidas cerca de los equipos
- Cuando los equipos de cómputo sean devueltos por cualquier causa, se deberá borrar por completo toda la información almacenada en su(s) disco(s) duro(s), en lo posible con un formateo completo a bajo nivel.
- 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 y la reinstalación del Sistema y de las aplicaciones.
- 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.
- Corresponderá al proceso de Gestión de Servicios TI en coordinación con el responsable de cada área, promover y difundir los mecanismos necesarios y adecuados de respaldo y salvaguarda de los datos y de los sistemas de información y los generados por los usuarios con sus respectivas herramientas de oficina.
- La información que se encuentre en otros medios y que sea desechada, debe ser destruida de acuerdo con los niveles identificados en el proceso de análisis de riesgos, o en procesos de revisión realizados por parte del proceso de Gestión de Servicios TI.
- El comité de seguridad o el responsable de Seguridad Informática debe precisar el tipo de información que se puede mantener en equipos portátiles o dispositivos removibles, aún si estos no son propiedad del FONCEP (caso computadores personales).
- No se debe retirar información, en ningún formato, de las instalaciones del FONCEP, sin la debida autorización previa por parte del Director de Área.

Para la implementación de esta política se debe tener en cuenta entre otros los siguientes principios.

6.4.3 Inventario de activos

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

El FONCEP mantendrá un inventario de los activos o bienes de Información, estableciendo Claramente el propietario del activo y el valor cualitativo para cada una de sus características de Confidencialidad, Integridad y Disponibilidad de forma tal que permita a la organización identificar sus activos y el valor e importancia de cada uno de ellos.

6.4.4 Propiedad de los activos

Cada activo informático estará claramente identificado y además debe tener un propietario asociado, quien es el responsable de su utilización y administración.

6.4.5 Uso aceptable de los activos

Se identifica, documenta e implementan las reglas sobre el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de la información.

6.4.6 Clasificación de la información

La información en el FONCEP está clasificada de forma tal que permita a los usuarios dar buen uso de la misma, por lo tanto, todos los usuarios deben respetar la protección de dicha información.

Se debe contar con una política de clasificación de la información, que permita identificarla, catalogarla y documentarla de acuerdo con la criticidad de la misma dentro de la organización, a las normas vigentes y la ley de transparencia.

Los propietarios de la información son responsables por la clasificación de la misma. Cada uno de ellos, es responsable de asegurar el apropiado nivel de seguridad y protección de la información. La clasificación se revisa de manera periódica por el propietario, y la definición debe ser aprobada por el Responsable de Área y/o Líder Funcional y los usuarios que tengan permisos para accederla deben utilizarla estrictamente para el propósito de la organización.

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

Está expresamente prohibido utilizar información perteneciente al FONCEP para uso y beneficio personal.

6.4.7 Etiquetado y manejo de la información

Toda información en formato electrónico e impreso perteneciente al FONCEP estará debidamente identificada mediante un rótulo o etiqueta (label), el cual permita establecer por parte del usuario la categoría de Clasificación del bien dentro del FONCEP. Esta identificación corresponde a lo expresado en el punto anterior.

6.4.8. Seguimiento y Control

Con el fin de velar por el correcto uso de los recursos informáticos, a través de los mecanismos formales y técnicos que se considere oportunos, el FONCEP comprobará, ya sea de forma periódica o cuando por razones específicas de seguridad o del servicio y cuando resulte conveniente, la correcta utilización de dichos recursos. En caso de evidenciar que alguien utiliza de forma incorrecta aplicaciones, datos y cualquier otro recurso informático, se le comunicará tal circunstancia y se le brindará la formación necesaria para el correcto uso de los recursos.

En caso de apreciarse mala fe en la incorrecta utilización, el FONCEP ejercerá las acciones que legalmente le amparen para la protección de sus derechos.

6.4.9. Actualización de la Política

Debido a la propia evolución de la tecnología, las amenazas de seguridad y a las nuevas normas legales en la materia, el FONCEP se reserva el derecho a modificar esta Política cuando sea necesario. Los cambios realizados en esta Política serán divulgados a todos los empleados, proveedores y terceros a los que les aplique, utilizando los medios que se consideren pertinentes.

6.5 Control de acceso

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

El proceso de Gestión de Servicios TI del FONCEP, - como responsables de proporcionar los servicios de TI en forma oportuna, completa y segura debe propender porque dichos servicios estén protegidos contra accesos no autorizados estableciendo los controles necesarios y mecanismos de control de acceso lógico.

El objetivo de la seguridad informática es proteger los recursos informáticos valiosos de la organización, tales como la información, el hardware o el software. A través de la adopción de las medidas adecuadas, la política de seguridad informática ayuda a la organización cumplir sus objetivos, protegiendo sus recursos financieros, sus sistemas, su reputación, su situación legal, y otros bienes tanto tangibles como inmateriales. Debe verse a la seguridad informática, no como un objetivo en sí mismo, sino como un medio de apoyo a la consecución de los objetivos de la organización.

La política de seguridad informática es una invitación a cada uno de los miembros de la organización a reconocer la información entre otras como uno de los activos principales. Esta política debe concluir en una posición consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos críticos de la organización.

Este documento recoge las políticas y procedimientos relacionadas con la infraestructura tecnológica de FONCEP en cuanto a los lineamientos referentes a temas como manejo de correo electrónico, estudio y manejo de nuevas adquisiciones, responsabilidades administrativas, integración con diferentes áreas de la organización, lineamientos sobre gestión de incidencias y revisión de aspectos relevantes frente a mecanismos preventivos y correctivos, todo bajo los conceptos de seguridad informática.

Desarrollar una política de seguridad informática significa planear, organizar, dirigir y controlar las actividades tecnológicas para mantener y garantizar la integridad física de los recursos informáticos, así como resguardar los activos de la organización.

6.5.1 Objetivo.

Definir las pautas generales para asegurar un acceso controlado a la información y a las aplicaciones de la Entidad.

6.5.2 Política

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

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 entregará las claves respectivas para el adecuado uso de la información y los recursos.
Para la implementación de esta política se debe tener en cuenta entre otros los siguientes principios.

Los jefes de las áreas 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.

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.

Los funcionarios deben proteger y no transferir el usuario y la palabra clave asignado 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.
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.
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 auditorías de las actuaciones realizadas con estas conexiones.

Se deben establecer los procedimientos requeridos para la implementación de esta política.

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

6.5.2.1. **Políticas de Uso Generales.**

- El proceso de Gestión de Servicios TI debe establecer un procedimiento de Gestión de Usuarios de Servicios de TI, que contemple la creación, modificación, bloqueo o eliminación de las cuentas de usuario para proveer acceso seguro a los servicios de TI del FONCEP.
- El proceso de Gestión de Servicios TI debe asegurar que los servicios de TI del FONCEP cuenten con métodos de autenticación que evite accesos no autorizados. De igual forma definirá las buenas prácticas para que los desarrollos de los sistemas de información cuenten con controles que no permitan el acceso no autorizado.
- El proceso de Gestión de Servicios TI debe implementar los controles para la identificación y autenticación de los funcionarios, proveedores y/o terceros para el acceso a los servicios de TI.
- Los directores o jefes de área 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 procedimiento establecidos para tal fin por el proceso de Gestión de Servicios TI
- 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.
- Los directores o jefes de área 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.
- 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.
- 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.
- 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.

6.5.2.2. **Políticas de Gestión de usuarios.**

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

- El proceso de Gestión de Servicios TI asignará una cuenta de usuario para el control de acceso lógico para cada funcionario, contratista, proveedor y/o tercero a los servicios de TI, garantizando que tengan acceso únicamente a los servicios y privilegios necesarios para el desarrollo de sus labores.
- El proceso de Gestión de Servicios TI garantizará dentro de lo posible, la alineación del acceso a los servicios, a las políticas de uso de contraseñas.
- El proceso de Gestión de Servicios TI debe establecer un procedimiento que asegure la eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre los servicios de TI, de manera oportuna cuando los funcionarios, contratistas, proveedores y/o terceros se desvinculen, cumplan los encargos, toman licencias o vacaciones.

6.5.2.3. **Políticas de Acceso a Aplicaciones de Negocio.**

- Los propietarios o administradores de los sistemas de información o aplicaciones deben definir los perfiles o roles de usuario, especialmente de aplicaciones de negocio.
- 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.
- 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 que puedan presentar a raíz de privilegios no autorizados o que exceden las necesidades para los que fueron autorizados.
- 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.
- Los usuarios deben utilizar diferentes perfiles para los ambientes de desarrollo, pruebas y producción, para reducir el riesgo de realizar actividades en ambientes equivocados.

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

- El proceso de Gestión de Servicios TI 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 y/o tester tengan acceso limitado y controlado a los ambientes de producción.
- El proceso de Gestión de Servicios TI debe salvaguardar el código fuente de las aplicaciones de negocio con control de acceso y restricción de privilegios.
- Las aplicaciones de negocio construidas o adquiridas por el FONCEP deben contar con autenticación de usuario y contraseña seguros.
- Las aplicaciones de negocio construidas o adquiridas con antelación a la aprobación de esta política, por el FONCEP deben alinearse, en lo posible, con el manual de desarrollo seguro definido por el proceso de Gestión de Servicios TI. Las aplicaciones por desarrollar después de la puesta en ejecución de esta política deben alinearse con el manual.

6.5.2.4. **Política de Privilegios Especiales**

- El proceso de Gestión de Servicios TI propenderá por una administración segura de la plataforma tecnológica que soporta los servicios de TI, monitoreando las actividades de los usuarios administradores.
- Solo se otorgará 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.
- El proceso de Gestión de Servicios TI dará acceso por medio de cuentas personalizadas con privilegios especiales a cada uno de los administradores.

6.5.3. Seguimiento y Control.

Con el fin de velar por el correcto uso de los recursos informáticos, a través de los mecanismos formales y técnicos que se considere oportunos, el FONCEP comprobará, ya sea de forma periódica o cuando por razones específicas de seguridad o del servicio y cuando resulte conveniente, la correcta utilización de dichos recursos. En caso de evidenciar que alguien utiliza de forma incorrecta aplicaciones, datos y cualquier otro recurso informático, se le comunicará tal circunstancia y se le brindará la formación necesaria para el correcto uso de los recursos.

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

En caso de apreciarse mala fe en la incorrecta utilización, el FONCEP ejercerá las acciones que legalmente le amparen para la protección de sus derechos.

6.5.4. Actualización de la Política.

Debido a la propia evolución de la tecnología, las amenazas de seguridad y a las nuevas normas legales en la materia, el FONCEP se reserva el derecho a modificar esta Política cuando sea necesario. Los cambios realizados en esta Política serán divulgados a todos los empleados, proveedores y terceros a los que les aplique, utilizando los medios que se consideren pertinentes.

6.6 Criptografía y seguridad de intercambio de información

Una política de seguridad criptográfica es un documento que especifica normas de uso en relación con la criptografía, e incluye estándares para su implantación en la organización. Algunos de los usos de la criptografía incluyen los mecanismos de autenticación, firma electrónica e irrefutabilidad, confidencialidad o integridad.
Esta política es conforme con los requisitos de seguridad y proporcionalidad correspondientes a los sistemas electrónicos de apoyo a procedimientos administrativos, establecidos en las normas que regulan el uso de los medios electrónicos en los servicios públicos.
Los contenidos de esta política de seguridad criptográfica se han estructurado para cubrir los controles previstos en la norma internacional ISO/IEC 27002:2006 y las recomendaciones contenidas en las Guías de Seguridad de las TIC CCN-STIC-405 y CCN-STIC-807 del Centro Criptológico Nacional.
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.
Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, 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.

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

El FONCEP por medio del proceso de Gestión de Servicios TI, implementará los controles de seguridad cuando se realiza un intercambio de información que asegure que ésta se encuentre protegida entre los directos responsables.

La política de intercambio de información busca mantener la seguridad de la información y del software cuando hay un intercambio de información dentro de FONCEP u otras organizaciones y que es lo que se va a hacer cuando se va a traer información de otra empresa, un soporte, cuando se tiene que transportar cierta cantidad de información a otra empresa externa o que de otra empresa traigan alguna información. Esta política consta de 5 ítems para asegurar la seguridad de dicha información.

6.6.1 Objetivo

Definir la utilización de medios criptográficos adecuados para proteger la confidencialidad, autenticidad o integridad de la información en los eventos que lo establezca la entidad.

Establecer las políticas de seguridad de la información, especialmente a las políticas tendientes a preservar la confidencialidad, integridad y disponibilidad de la información cuando se genera una trasferencia de información ya sea interno o externo.

6.6.2 Política

Para la información que se considere susceptible de proteger criptográficamente, ya sea de los sistemas de información o que se requiera intercambiar con otras entidades; se debe garantizar la utilización de esquemas seguros de cifrado para su conservación o intercambio.
En caso de requerirse Se deben definir procedimientos y protocolos de cifrado y descripción de la información, en forma segura.

La información con carácter reservado o que por los procesos en que se utilice esté expuesta a riesgos de pérdida de confidencialidad se debe cifrar.

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

El encargado del Sistema de Gestión de Seguridad de la Información de FONCEP determinará los mecanismos de cifrado de datos que mejor se ajusten a las necesidades específicas de cada tipo de información sugiriendo el asimétrico como el óptimo.

Las contraseñas para cifrado de información se deben proteger y gestionar siguiendo los controles de seguridad definidos para la protección de contraseñas de FONCEP.

Para el cifrado de información se utilizarán algoritmos de **cifrado asimétricos contenidos en varios protocolos entre ellos PGP, SSH, TLS, etc.**

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.

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. (Ver el procedimiento de intercambio de información)

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 esta política por los involucrados.

Las llaves de cifrado tendrán una vigencia máxima de 6 meses, posterior a este tiempo debe actualizarse para garantizar que esta no sea revelada.

Los usuarios autorizados para acceder remotamente a la información de FONCEP, deben hacerlo a través de servicio de **VPN SSL** y solo se otorgará acceso a su estación de trabajo a través del servicio de escritorio remoto.

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 máquina que el usuario autorizado va a utilizar para este acceso remoto debe cumplir con los requerimientos de seguridad de FONCEP. (Ver el procedimiento de intercambio de información).

6.6.2.1 Usos no autorizados

Está prohibido cifrar información con mecanismos no autorizados por el Sistema de Gestión de Seguridad de la Información de FONCEP

Está prohibido cifrar información sin la autorización del custodio de la información.

Está prohibido revelar las claves privadas de cifrado de información a personal no autorizado.

6.6.2.2 Responsabilidades

Los responsables de información, procesos, procedimientos o actividades que impliquen procesamiento, transmisión o almacenamiento de información empleando medios electrónicos deben solicitar mediante los procedimientos definidos por FONCEP, el cifrado de la información clasificada como RESERVADA que esté bajo su responsabilidad.

Los responsables de áreas y procesos de FONCEP son los responsables de documentar, divulgar y actualizar los procedimientos para el cifrado de información incluidas las actividades de generación, gestión y protección de las claves empleadas para el cifrado de información contando con el apoyo del proceso de Gestión de Servicios TI

6.6.2.3 Política de Uso Generales para seguridad de intercambio de información.

El intercambio de información de la empresa, entre organizaciones o terceras partes debe estar controlado y se deben cumplir todas las legislaciones y normas que correspondan.

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

- Para mantener una adecuada protección de la información FONCEP, establece procedimientos y controles de intercambio por medio de la utilización de todo tipo de servicios de comunicación.

- Los intercambios de información se deben realizar en base a acuerdos formales y acuerdos de confidencialidad.

- Considerar los siguientes controles para proteger los datos en tránsito:

  - Los funcionarios que requieran almacenar información sin cumplir con las características enunciadas deberán exponer sus razones y solicitar la aprobación del proceso de Gestión de Servicios TI, quien después de un análisis de riesgo sobre el tema, emitirá su concepto.

  - Revisar y/o actualizar periódicamente la actualización de los acuerdos de confidencialidad los cuales le dan la autorización al usuario para realizar el intercambio de información.

  - Revisar las Evidencias de entrega (logs) en caso de fallas en la transmisión o transmisión incompleta.

6.6.2.4 Política de transferencia digital.

- Utilizar siempre el protocolo de transferencia de información segura HTTPS en las comunicaciones con las entidades externas.

- Disponer de herramientas de cifrado, asimétrico preferiblemente para aplicarlas en el intercambio de información. (Ver política de criptografía).

- Tener disponibilidad de certificados digitales en caso de necesitarse en el intercambio de información con otras entidades.

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

- FONCEP por medio del proceso de Gestión de Servicios TI, debe entregar las herramientas necesarias para cifrar la información que los diferentes usuarios requieran almacenar o transportar a otras dependencias internas o externas.

6.6.2.5 Política de transferencia física.

- La información que circula en medios informáticos del FONCEP durante su trasporte físico, debe estar protegida contra acceso no autorizado, uso inadecuado o corrupción

- Los medios informáticos o de transporte físico de información del FONCEP deben estar lo suficientemente protegidos contra daño físico que pueda ocurrir durante su transporte. Todo objeto que trasladar debe ser embalado y protegido correctamente con cajas de cartón y protectores de icopor para el caso de PC o servidores críticos

- Los empleados del FONCEP no deben revelar información sensible del proyecto por medios telefónicos, para evitar la escucha o interpretación de su llamada por personas extrañas

- Si es una memoria USB o disco duro externo, el transporte de información restringida se debe realizar mediante contenedores o espacios cifrados.

- Diligenciar una autorización del traslado por parte de la dirección o comité encargado del traslado de información o líder del proceso.

- Implementar Etiquetas para sellar las cajas, sobres o medios donde se almacena la información física.

- Registrar y firmar actas de envío y de recepción de la correspondencia

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

6.6.3 Seguimiento y Control.

La política de controles criptográficos debe ser revisada cada seis meses o cuando se presenten eventos que obliguen a su actualización.

En caso de evidenciar que alguien utiliza de forma incorrecta aplicaciones, datos y cualquier otro recurso informático, se le comunicará tal circunstancia y se le brindará la formación necesaria para el correcto uso de los recursos.

En caso de apreciarse mala fe en la incorrecta utilización, el FONCEP ejercerá las acciones que legalmente le amparen para la protección de sus derechos.

6.6.4 Actualización de la Política.

Debido a la propia evolución de la tecnología, las amenazas de seguridad y a las nuevas normas legales en la materia, el FONCEP se reserva el derecho a modificar esta Política cuando sea necesario. Los cambios realizados en esta Política serán divulgados a todos los empleados, proveedores y terceros a los que les aplique, utilizando los medios que se consideren pertinentes.

6.7 Seguridad Física.

6.7.1 Objetivo.

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

Prevenir el acceso no autorizado, el daño y la interferencia de la información y de las instalaciones en donde se encuentren sistemas de procesamiento de información del FONCEP.

6.7.2 Política.

Se deben establecerse 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.

Para la implementación de esta política se debe tener en cuenta entre otros los siguientes principios.

Las instalaciones o sitios físicos donde se procesa información son:

- Centros de cómputo principales o alternos.
- Áreas con equipos de cómputo, ya sean de procesamiento o dispositivos de comunicación.
- Áreas donde se almacenen papelería, hojas membretadas, documentos con valor comercial o títulos valor.
- Áreas donde se encuentren almacenados dispositivos de información.
- Áreas de almacenamiento de dispositivos de respaldo datos (CD, Discos Duros, Cintas etc.).
- Áreas de impresión o fax.
- Despachos de los directivos o personal que tenga acceso a información sensible de la entidad.
- Área de Tesorería
- Área de Nómina
- Áreas de monitoreo.
- Centro de Cableado de datos o telefónico.

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

- Estaciones de trabajo.

Políticas Asociadas al Acceso Físico

- Los funcionarios deben portar el carné que los identifica como tales en un lugar visible mientras se encuentren en las instalaciones de la entidad. Así mimo los visitantes, proveedores, contratista y terceros deben portar el carné provisional.
- Las puertas de acceso a los diferentes pisos de la entidad deben permanecer cerradas con llave con el fin de controlar el ingreso y salida de visitantes y funcionarios.
- El personal de seguridad de la recepción del edificio debe llevar un registro de todos los visitantes /usuarios que se dirigen al segundo piso (área de atención al ciudadano). Así mismo debe existir comunicación permanente entre ambas empresas y coordinación para solicitar apoyos con los posibles incidentes que se presenten en las áreas comunes que afecten la seguridad de la entidad.
- El ingreso y salida de equipos de cómputo de cada piso, debe contar con la autorización por escrito del Jefe Administrativo.
- Todo bolso, cartera y/o paquete que ingrese los funcionarios/visitantes de la entidad, deberán ser revisados por el personal de seguridad dispuesto en cada piso, dejando registro en las minutas de los números de serie de los equipos.
- 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.
- 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.
- El acceso a las áreas sensibles de la entidad como centro de cómputo, oficinas de la dirección, etc, y la central de monitoreo es restringido. Por este motivo cada ingreso debe quedar registrado en la minuta con hora de ingreso y salida de los visitantes.

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

- 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 funcionario correspondiente.

6.7.2.1 Política Asociada a la Consulta de las Grabaciones de las Cámaras del Circuito Cerrado de Televisión – CCTV del FONCEP.

6.7.2.1.1 Consideraciones Generales.

Las personas autorizadas para acceder a las grabaciones del CCTV, sólo tendrán 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 Jefe Administrativo encargado de la supervisión y control de la seguridad física y el sistema de CCTV, no entregará copias de grabaciones, ni certificará las imágenes grabadas.

Se encuentran excluidos del servicio de consulta de grabaciones de las cámaras del CCTV todos aquellos eventos en los cuales los servidores públicos o visitantes, por descuido o negligencia propia, hayan sufrido pérdida o daño de sus bienes o efectos personales o de aquellos asignados bajo su tenencia, responsabilidad y custodia.

No podrá 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, podrá solicitarse al Jefe Administrativo aduciendo las debidas evidencias o justificaciones.

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

6.7.2.1.2 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.

6.7.2.1.3 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 Jefe Administrativo 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. f) Piso del FONCEP o dependencia especifica en la que usted presume que ocurrieron los hechos que usted requiere consultar.

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 serán atendidas las solicitudes que contengan la información mínima

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

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 Jefe Administrativo responderá negativamente su solicitud indicándole las razones por las cuales ésta no será atendida.

¿Qué Hacer si su 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 la misma ante el Jefe Administrativo, a través del mismo medio que utilizó para su solicitud inicial. Preferiblemente indique la fecha o número de radicación (si lo hubo) en que presentó la solicitud inicial. El jefe Administrativo no reconsiderará 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 Jefe Administrativo le informará el lugar, fecha y hora en la que usted puede consultar los videos obtenidos de las cámaras del CCTV.

No se podrán 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 será acompañado por el personal designado por el Jefe Administrativo.

¿Cómo Concluye la Consulta?

Al finalizar la consulta, se diligenciará la minuta de Solicitudes y constancias de consultas a las grabaciones CCTV" suscrito por el delegado del Jefe Administrativo y si es del caso, el delegado de la empresa de vigilancia que acompañaron la misma. Si la consulta fue radicada mediante oficio por un ente de control, esta se responderá con un

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

oficio (Correspondencia Externa Enviada – SIGEF). En el oficio se consignarán las observaciones a que hubiere lugar y se dejará constancia en relación con el cumplimiento total por parte de la entidad de la solicitud efectuada.

Recomendaciones

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.

6.7.2.2 Política Asociada a la Seguridad de los Equipos

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.

- 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.
- Se deben tener controles apropiados referentes a:
  - Robo: Todos los visitantes proveedores o terceros, que ingresen a las instalaciones de la entidad deberán poseer una identificación que permita saber la dependencia autorizada a visitar o por la cual transitar. En el caso de Proveedores o terceros deberán contar con el permiso para permanecer en la entidad, siempre con la supervisión del responsable de sus labores

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

- Humo o Fuego: En todos los centros de procesamiento, sin excepción, deberán existir detectores de calor y humo, instalados en forma adecuada para detectar el más mínimo indicio de incendio. Los detectores deberán ser probados de acuerdo a las recomendaciones del fabricante o al menos una vez cada 6 meses.

  Se deben tener extintores de incendios debidamente probados, y con capacidad de detener fuego generado por equipo eléctrico, papel o químicos especiales.

- 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 podrá, por ninguna razón llevar consigo material explosivo (Por ejemplo, químicos especiales, pólvora o gases explosivos)
- 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.

  Las áreas en donde se tenga equipos de procesamiento de información, no se permitirá fumar, tomar ningún tipo de bebidas o consumir alimento.

  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.

- El correcto uso de UPS (Uninterruptable power suply): 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.

  Se deben tener interruptores eléctricos adicionales, localizados cerca de las salidas de emergencia, para lograr un rápido apagado de los sistemas en caso de una falla o contingencia. Las luces de emergencia deben funcionar en caso de fallas en la potencia eléctrica.

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

6.7.2.3 Política Asociada a los Centro de Cómputo y Centros de Cableado

- El acceso al centro de cómputo o a los centros de cableado debe ser autorizado por funcionarios de la oficina de sistemas autorizados. Los proveedores, terceros y visitantes siempre deberán estar acompañados de un funcionario de dicha Oficina.
- Se debe registrar el ingreso de los visitantes al centro de cómputo y a los centros de cableado, en una bitácora.
- 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.
- Se asegurará 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.
- 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.
- Las labores de mantenimiento de redes eléctricas, de voz y de datos, deben ser realizadas por personal idóneo y apropiadamente autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos.

6.7.2.3.1 Instalación y Mantenimiento del Cableado

- El cableado de la red debe ser instalado y mantenido por ingenieros o proveedores calificados con el fin de garantizar su integridad. Conectores de pared no utilizados deben ser sellados y su estado debe ser formalmente notificado.
- Las conexiones de potencia deben tener su respectivo polo a tierra.
- El cableado de la red debe ser protegido de intercepción o daño, por ejemplo, usando canaletas que lo protejan.
- Los cables de potencia deben estar separados de acuerdo a las normas técnicas, de los de comunicaciones.

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

6.7.2.3.2 Mantenimiento de los Equipos

- Se debe contar de forma constante con el soporte y mantenimiento adecuado para los equipos de procesamiento de información.
- Se debe contar con las pólizas de seguros contra pérdidas y daños, adecuados para los equipos de procesamiento.
- Se debe realizar mantenimientos preventivos y correctivos sobre la plataforma tecnológica de la entidad.
- Se deberán realizar mantenimientos sobre los equipos de acuerdo a 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 sensitiva y los requerimientos de las pólizas de aseguramiento.

6.7.2.3.3 Equipos Fuera de las Instalaciones

- El uso de equipos de procesamiento de la información o software, fuera de las instalaciones de la entidad, debe ser autorizado por el proceso de Gestión de Servicios TI y el director del área responsable del empleado, contratista, proveedor o tercero. Esto aplica para Computadores personales, Agendas electrónicas, teléfonos móviles, etc.
- No dejar los equipos desatendidos en zonas públicas. Los computadores personales deben evitar su apariencia y ser llevados como equipaje de mano.
- El trabajo remoto debe estar sujeto a controles especiales, considerando las recomendaciones aplicadas cuando su uso es de tipo interno.

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

6.7.2.3.4 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 a la política de backup y será realizado por personal autorizado del proceso de Gestión de Servicios TI.

6.7.2.4 Política de Escritorios y Pantalla Limpia

- La entidad debe adoptar una política de escritorios limpios para papeles, y medios de información, junto con una política de pantalla limpia, con el fin de reducir los riesgos por pérdida, daño a la información durante o fuera de las horas de trabajo.
- Cuando sea apropiado, papeles y medios de información deben estar asegurados en gabinetes de escritorio o especiales, en horas fuera de horario de oficina.
- Información confidencial y crítica para la organización debe ser asegurada preferiblemente en archivadores resistentes a impacto, fuego e inundación.
- Los computadores personales no se deben dejar desatendidos dentro de una sesión abierta, se debe contar con bloqueo automático con un tiempo de desatención no mayor a 1 minuto.

6.7.2.4.1 Uso de Fax u otros Medios no Digitales.

- Esta política considera las amenazas asociadas con el uso del Fax u Otros Medios NO Digitales, dado el riesgo que supone la inseguridad del medio, dado que información confidencial puede ser revelada a personas no autorizadas.

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

- La información sensitiva o confidencial solo puede ser enviada vía Fax u Otros Medios NO Digitales cuando no exista un medio digital seguro, ambos el dueño y el receptor deben autorizar la transmisión de antemano.
- El envío por estos medios debe ser supervisado por el propietario de la información y por el receptor de la misma.

6.7.2.4.2 Uso de Impresoras.

- La variedad de la información que se envía a las impresoras puede alternar entre información pública e información confidencial, dado que información confidencial puede ser revelada a personas no autorizadas.
- 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.

6.7.2.4.3 Presencia de Extraños en las Instalaciones.

- Todos los visitantes, proveedores o terceros, deben estar debidamente identificados con carnet de visitantes durante su estadía en la entidad.
- Todos los empleados deben estar vigilantes a la presencia de personas extrañas sin identificación visible dentro de las instalaciones de la entidad y en ese caso reportar inmediatamente a la seguridad de la entidad.
- Todos los visitantes, proveedores o terceros deben ser acompañados durante su estadía en la entidad, debido a la existencia de información confidencial o posible hurto.
- Los visitantes, proveedores o terceros que lleven dispositivos como videograbadoras, cámaras fotográficas, grabadoras, sniffers, analizadores de datos, (ej: hardware especial) etc, no podrán utilizarlos dentro de las instalaciones de la entidad, sin la debida autorización formal emitida por Gestión de Servicios TI y los responsables de la seguridad del edificio.

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

6.7.2.4.4 Recepción de Mercancía

- La recepción de mercancía en la entidad requerirá de un primer control e inspección por parte de la seguridad del edificio en recepción y posteriormente se dará la respectiva autorización para su ingreso y entrega en el sitio respectivo.
- 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.
- 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.

6.7.2.4.5 Traslado de Información Física

- La información física incluye medio digitales o en papel y deben ser protegidos cuando son transportados fuera de la entidad.
- 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. Del mismo modo los documentos físicos.
- 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
- El transporte de activos de información solo debe contratarse con compañías autorizadas por la entidad.

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

6.7.2.5 Seguimiento y Control.

Con el fin de velar por el correcto uso de los recursos informáticos, a través de los mecanismos formales y técnicos que se considere oportunos, el FONCEP comprobará, ya sea de forma periódica o cuando por razones específicas de seguridad o del servicio y cuando resulte conveniente, la correcta utilización de dichos recursos. En caso de evidenciar que alguien utiliza de forma incorrecta aplicaciones, datos y cualquier otro recurso informático, se le comunicará tal circunstancia y se le brindará la formación necesaria para el correcto uso de los recursos.

En caso de apreciarse mala fe en la incorrecta utilización, el FONCEP ejercerá las acciones que legalmente le amparen para la protección de sus derechos.

6.7.2.6 Actualización de la política.

Debido a la propia evolución de la tecnología, las amenazas de seguridad y a las nuevas normas legales en la materia, el FONCEP se reserva el derecho a modificar esta Política cuando sea necesario. Los cambios realizados en esta Política serán divulgados a todos los empleados, proveedores y terceros a los que les aplique, utilizando los medios que se consideren pertinentes.

6.7.3 Perímetro de seguridad física

El FONCEP debe definir claramente las áreas seguras con el fin de proteger instalaciones de procesamiento de información. Para el efecto, deben ser protegidas con controles de ingreso físico, que permitan el acceso solamente al personal autorizado, y permitan la implementación de mecanismos de registro de todo ingreso y egreso de funcionarios y visitantes que deban acceder a diferentes áreas seguras establecidas en la entidad.

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

6.7.4 Controles de acceso físico

El control de acceso para los funcionarios en las áreas seguras se debe hacer mediante el uso de tarjetas magnéticas de aproximación, preferiblemente utilizando mecanismos de doble autenticación, acompañadas de mecanismos que permitan implementar registros de auditoría de los accesos.

Todo el personal del FONCEP debe usar de forma permanente y en un lugar visible su identificación como funcionario o contratista.

Los visitantes deben portar en todo momento la identificación suministrada en el control de ingreso al edificio. Queda prohibida la permanencia de visitantes sin supervisión en las áreas seguras. En cualquier caso, las visitas deben ser autorizadas directamente por un responsable.

Las áreas Seguras deben ser definidas en un documento de carácter confidencial de uso restringido al interior del Grupo de Seguridad, con base en los resultados del Análisis de Riesgos y Valoración e Identificación de Activos.

Los medios de respaldo deben ser almacenados en zonas aisladas, separadas de las áreas de procesamiento, con control de acceso físico restringido y protegidas contra amenazas físicas similares a los centros de procesamiento de información.

El grupo de apoyo de la Seguridad de la Información debe realizar revisiones periódicas de los niveles de acceso y privilegios establecidos, y debe actualizar los niveles definidos, de forma periódica.

Queda prohibido el almacenamiento de material o sustancias inflamables en las áreas seguras, en las áreas definidas para Centros de Cómputo, y en áreas consideradas de alto riesgo.

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

No se permite el ingreso de funcionarios, contratistas o visitantes, sin las autorizaciones correspondientes o que no sigan el procedimiento adecuado. Se deben establecer los procedimientos de ingreso al edificio por el área encargada de la protección de las instalaciones, y debe ser tomado como procedimiento de apoyo a esta política.

Los funcionarios del FONCEP no deben permitir que personas desconocidas o no autorizadas atraviesen las puertas u otras entradas con control físico de acceso, al mismo tiempo en que lo hacen ellos, y que se pueda evitar de esa forma su control.

Los equipos como fotocopiadoras y faxes deben estar ubicados en zonas con control de acceso restringido, y se debe controlar su uso por parte de personal autorizado solamente, para lo cual debe existir un registro de su utilización. Se debe tener especial cuidado en su uso (incluyendo las impresoras), para garantizar que no permanezca en ellas, sin atención, material con información sensible, y que no se use papel reciclado que contenga información crítica o confidencial.

6.7.5 Protección contra amenazas externas y ambientes

Deben existir protecciones físicas contra daño por incendio inundación, terremoto, explosión, manifestaciones sociales y otras formas de desastre natural o artificial.

Los materiales combustibles o peligrosos se deben almacenar a una distancia prudente de las áreas de seguridad.

Los suministros a granel tales como los materiales de oficina, no se deben almacenar en un área segura. Se deben suministrar equipos apropiados contra incendios y deben ser ubicados adecuadamente.

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

6.7.6 Trabajo en áreas seguras

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

6.7.7 Áreas de carga, despacho y acceso público

Los puntos de acceso tales como las áreas seguras de carga y despacho y otros puntos por donde pueda ingresar personal no autorizado a las instalaciones de deben controlar, si es posible, aislar de los servicios de procesamiento de información para evitar el acceso no autorizado.

6.7.8 Escritorios y pantalla limpia

El personal del FONCEP, debe conservar su escritorio libre de información propia de la entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento. El personal de la Entidad debe bloquear la pantalla de su computador con el protector de pantalla designado por la entidad, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo.
Al imprimir documentos de carácter público o reservado, estos deben ser retirados de la impresora inmediatamente.

6.7.9 Ubicación y protección de los equipos

La infraestructura de procesamiento de datos (equipos de hardware y software, y elementos de red y comunicaciones que se utilicen para el tratamiento de información) debe estar protegida de manera física o con controles lógicos, contra

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

amenazas de carácter ambiental, y de los peligros generados por accesos no autorizados. Los dispositivos y mecanismos de protección deben estar alienados con base en el análisis de riesgos.
La red de datos debe ser protegida de accesos y conexiones físicas no autorizadas, así como de daños o interferencias que puedan afectar la integridad y disponibilidad de la información, mediante mecanismos físicos o lógicos.

6.7.10 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 Ininterrumpible (UPS).

6.7.11 Seguridad del cableado

El acceso a los módulos de cableado y a los cuartos de cableado debe ser controlado y solo podrá acceder personal autorizado.

6.7.12 Mantenimiento de los equipos

Todos los equipos de procesamiento de información, de transmisión de datos y de soporte de la infraestructura, elementos de red; deben contar con los contratos de mantenimiento apropiados de acuerdo con su nivel de criticidad y a los requerimientos de disponibilidad identificados, y con una Hoja de Vida donde esté establecida la frecuencia de revisión y mantenimiento.

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

6.7.13 Seguridad de los equipos fuera de las instalaciones

Los equipos portátiles deben estar protegidos por mecanismos antirrobo o con elementos como guayas de seguridad, en adición a los controles lógicos establecidos.

Cuando un equipo de cómputo deba repararse, éste no saldrá del edificio sin tener una autorización firmada por parte del director del área a la cual pertenece o está asignado el equipo, y por el Director de 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.

6.7.14 Seguridad en la reutilización o eliminación de los equipos

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 y la reinstalación del Sistema y de las aplicaciones.

La información que se encuentre en otros medios y que sea desechada, debe ser destruida de acuerdo con los niveles identificados en el proceso de análisis de riesgos, o en procesos de revisión realizados por parte del Grupo de Seguridad.

6.7.15 Retiro de propiedad

El comité de seguridad o el responsable de Seguridad Informática debe precisar el tipo de información que se puede mantener en equipos portátiles o dispositivos removibles, aún si estos no son propiedad del FONCEP (caso computadores personales).

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

No se debe retirar información, en ningún formato, de las instalaciones del FONCEP, sin la debida autorización previa por parte del Director de Área.

6.8 Seguridad de las Operaciones.

6.8.1 Objetivo.

Garantizar la existencia de procedimientos, registros y guías de trabajo debidamente documentados, con el fin de asegurar el mantenimiento y operación adecuada de la infraestructura informática del FONCEP.

6.8.2 Política.

Deben documentarse los procedimientos y responsabilidades de administración y seguridad que sean necesarios en cada ambiente tecnológico y físico, 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. Debe buscarse una adecuada segregación de funciones.

Deben garantizarse una adecuada planificación y aprobación de los sistemas de información que consideren o provean las necesidades de capacidad futura.

Deben considerarse protecciones contra software malicioso y un adecuado mantenimiento y administración de la infraestructura, así como un adecuado cuidado de los medios de almacenamiento y seguridad en el intercambio de información.

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

Para la implementación de esta política se debe tener en cuenta entre otros los siguientes principios

6.8.3 Procedimientos de operación documentados

Deben existir procedimientos, registros y guías de trabajo debidamente documentados, con el fin de asegurar el mantenimiento y operación adecuada de la infraestructura informática y de Sistemas en el FONCEP. A cada procedimiento debe tener responsable para su definición y mantenimiento.

6.8.4 Gestión del cambio

Todo cambio a la infraestructura informática debe estar controlado y ser realizado de acuerdo con los procedimientos definidos por el FONCEP, con el fin de asegurar que los cambios efectuados no afecten la disponibilidad e integridad de la información y los servicios.

6.8.5 Separación de las instalaciones de desarrollo, ensayo y operación

Para la gestión de las operaciones de los sistemas de información en el FONCEP, deben existir mecanismos que permitan contar con ambientes de desarrollo, pruebas y operación, para todos los aplicativos con los que se cuente los archivos fuente y pruebas y operación, para los que no se cuente con los archivos fuente.

6.8.6 Controles contra códigos maliciosos

La Infraestructura de red debe estar protegida para asegurar que no se ejecuten virus o códigos maliciosos, mediante la utilización de un sistema de “Antivirus” para todos los equipos que formen parte de la infraestructura del FONCEP.

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

El sistema de control de virus debe contar con los procesos y contratos de soporte necesarios para mantenerlo actualizado y es responsabilidad del usuario y del Administrador de Red asegurar que el software Antivirus no sea deshabilitado por ningún motivo

6.8.7 Respaldo de la información

Deben existir procedimientos explícitos de resguardo y recuperación de la información que incluyan especificaciones acerca del traslado, frecuencia, identificación y períodos de retención de la misma. Estos procedimientos deben establecer el uso de sistemas de inventario e identificación de los medios magnéticos, la identificación de la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a la información resguardada.

El procedimiento de gestión de copias de respaldo debe incluir los aspectos relacionados con las pruebas periódicas de verificación de las copias de respaldo.

Toda información resguardada en medios magnéticos debe almacenarse en lugares que cumplan con máximas medidas de protección, en cajas o gabinetes de seguridad y el sitio debe contar con mecanismos de detección de humo, calor y humedad, incendio y control de acceso físico.

6.8.8 Registros del administrador y del operador

Todas las actividades de operación realizadas por los administradores de sistemas de la infraestructura deben estar debidamente registradas y se deben revisar periódicamente por el personal encargado para este propósito dentro del Grupo 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**

6.8.9 Instalaciones de software en sistemas operativos y Restricción sobre la instalación de software

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

6.9 Seguridad de las comunicaciones

6.9.1 Objetivo.

Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información.

6.9.2 Política.

Deben documentarse los procedimientos y responsabilidades de administración y seguridad que sean necesarios en el manejo de las redes de la Entidad, garantizando un adecuado control, mantenimiento, así como el seguimiento a los incidentes de seguridad que puedan presentarse.

Para la implementación de esta política se debe tener en cuenta entre otros los siguientes principios

6.9.3 Controles de las redes

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

Debe existir un conjunto de controles físicos y lógicos para el acceso a los diferentes recursos informático, con el fin de garantizar el buen uso de los mismos y mantener los niveles de seguridad.

6.9.4 Seguridad de los servicios de red

Se debe garantizar el monitoreo de los elementos físicos de la red y el tráfico de información que se transporta, a fin de establecer las necesidades de los recursos, su buen desempeño y uso inadecuado de los recursos.

Los servicios de correo e internet deben ser usados por los funcionarios estrictamente para realizar actividades de la entidad, con el cuidado de no realizar procesos masivos que afecten el desempeño de los servicios.

6.9.5 Políticas y procedimientos para transferencia de información

Los intercambios de información y de software se deben basar en una política de intercambio, ejecutar según los acuerdos de intercambio y cumplir la legislación correspondiente.

6.9.6 Acuerdos sobre transferencia de información

Para el intercambio de Información con organizaciones o con usuarios externos, se debe establecer un Acuerdo de Confidencialidad, donde queden especificadas las responsabilidades para cada una de las partes.

6.9.7 Mensajería electrónica

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

Cada usuario es responsable por el contenido de todas las comunicaciones que almacene o envíe utilizando su cuenta de correo electrónico. Los usuarios no deben enviar mensajes que puedan afectar la imagen de la entidad o generar daño en entes externos.

Está prohibido el uso de la cuenta de correo electrónico del FONCEP, asignada al funcionario, para efectos personales ajenos a las funciones y actividades propias de su cargo.

Queda prohibido la descarga e instalación de software o programas no autorizados desde Internet, así como archivos del tipo música, video, y ejecutables en cualquier formato, sin la respectiva autorización del jefe de área.

6.10 Adquisición, desarrollo y mantenimiento de sistemas

6.10.1 Objetivo

Garantizar que la Política de Seguridad esté incorporada a los sistemas de información.

6.10.2 Política

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. Además, se establecerán controles para cifrar la información confidencial y se buscará evitar la posibilidad de una acción indebida

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

por parte de un usuario del sistema. Igualmente, se deben asegurar los archivos del sistema y mantener un control adecuado de los cambios que puedan presentarse.

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), 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. Estos controles deben estar soportados por procedimientos específicos de manejo y control de información.

Para la implementación de esta política se debe tener en cuenta entre otros los siguientes principios.

6.10.3 Análisis y especificación de los requisitos de seguridad

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, controles, registros de auditoría y características o especificaciones de seguridad asociados a él y a su implantación, además del análisis de riesgo y de impacto derivado en una posible falla.

6.10.4 Procedimientos de control de cambios de los sistemas

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

Se debe implementar un procedimiento de control de cambio para los sistemas, que permita realizar toda la trazabilidad de las solicitudes, los cuales deben asegurar que sólo los cambios autorizados sean implantados. Se debe dar una aprobación formal por parte de las áreas propietarias de la información (funcionalidad), para que los programas sean implantados en los entornos de producción. Se debe mantener un registro de todas las implantaciones realizadas en el ambiente de producción para identificar quién, cuándo y dónde se realizó la instalación. Este procedimiento debe ser funcional para los desarrollos realizados directamente por FONCEP, como los contratados.

El procedimiento, debe contemplar todos los pasos requeridos en el control de cambios como son: Definición detallada de la necesidad, solicitud, viabilidad, análisis, diseño, desarrollo, pruebas, aprobación, documentación e implementación en el ambiente de producción; incorporando en los pasos requeridos los lineamientos y necesidades en cuanto a la seguridad de la información.

6.11 Relaciones con los proveedores

Toda entidad cuenta con información a la cual debe preservar su confidencialidad, integridad y mantener su disponibilidad, cuando se expone al conocimiento de una tercero o proveedor en mayor o menor grado y cuya pérdida o uso indebido pueden deteriorar o provocar indisponibilidad de los sistemas de información que afectan el normal desarrollo de la operación, produciendo efectos negativos en la calidad del servicio y el valor o propósitos sociales de la entidad, así mismo daños en su reputación.

6.11.1 Objetivo

Garantizar que la relación con los proveedores este claramente definida y ajustada a las necesidades de Seguridad de la de información.

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

6.11.2 Política

Se debe asegurar que riesgos asociados con la tercerización de servicios y bienes, deben tener un adecuado manejo de las condiciones de seguridad de la información, en las fases de selección del tercero, contratación, ejecución, finalización y retiro.

Se debe contar con acuerdo de confidencialidad y niveles de servicio que permitan cumplir con las políticas de seguridad de la información y realizar seguimiento permanente de su cumplimiento.

6.11.2.1 Política General de Seguridad de la Información del FONCEP

El FONDO DE PRESTACIONES ECONÓMICAS, CESANTIAS Y PENSIONES – FONCEP, ha establecido como política general de la seguridad de la información:

El FONDO DE PRESTACIONES ECÓNOMICAS, CESANTIAS Y PENSIONES – FONCEP, como entidad responsable del pago de cesantías y reconocimiento y pago de pensiones a las servidoras y servidores públicos del Distrito Capital, con régimen de retroactividad, afiliados al FONCEP; es consiente 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 protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos 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 ECONÓMICAS, 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.

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

6.11.2.1.1 Principios de seguridad de la información

Los principios que se debe cumplir para lograr los objetivos de seguridad de la información son los siguientes:

- Todo el personal debe conocer y responder por la seguridad de la información que gestiona de acuerdo con sus funciones.
- Se deben tomar medidas para implementar los controles de seguridad de la información que apliquen en los procesos de la Entidad.
- Se debe promover una cultura organizacional de mejora continua orientada a la seguridad de la información.
- Las máximas autoridades de la Entidad deben comprometerse con la difusión, consolidación y cumplimiento de las políticas de seguridad de la información.
- Se deben mantener las políticas, normativas y procedimientos actualizados, con el fin de asegurar su vigencia y nivel de eficacia.
- Se debe hacer seguimiento a los riesgos de seguridad de la información y tomar acciones cuando los cambios den como resultado riesgos que no sean aceptables.
- Se deben analizar y aplicar las medidas pertinentes cuando se presenten situaciones que puedan poner a la Entidad en situación de incumplimiento frente a las políticas, procedimientos, leyes y reglamentos relacionados con la seguridad de la información.
- Las políticas, controles implementados, al igual que la ejecución del MSPI, será revisada con regularidad como parte del proceso del mejoramiento continuo, o cuando se identifiquen cambios en la Institución, su estructura, sus objetivos o alguna condición que afecten, para asegurar que sigue siendo adecuadas y ajustadas a los requerimientos identificados.
- Los activos de información serán identificados y clasificados para establecer los mecanismos de protección necesarios.

6.11.2.1.2 Responsabilidades generales FONCEP

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

Las responsabilidades generales de las acciones para cumplir con los requisitos de la política y controles de seguridad de la información requeridos por la Entidad son:

- El equipo de la alta dirección y el Comité de Seguridad de la Información son responsables de garantizar que la seguridad de la información se aborde adecuadamente en toda la Entidad.
- Cada uno de los funcionarios de la alta dirección son los responsables de velar por la protección de la información que se gestiona en su área 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.
- Cada líder de proceso debe garantizar que se incluyan los lineamientos dados en las políticas y normas de seguridad de la información en sus procesos.
- El Comité de Seguridad de Información de la Entidad, será el responsable de velar por el cumplimiento del plan de implementación del MSPI.
- Toda persona vinculada como funcionario de carrera administrativa, libre nombramiento y remoción, provisionalidad, temporalidad, contratista o pasante; será responsable de proteger la información a la cual acceda y procesa, para evitar su pérdida, alteración, destrucción o uso indebido.
- Es responsabilidad de toda persona vinculada como funcionario de carrera administrativa, libre nombramiento y remoción, provisionalidad, temporalidad, contratista o pasante; reportar los incidentes de seguridad, eventos sospechosos y/o el mal uso de los recursos institucionales de los cuales tenga conocimiento.
- Es responsabilidad de la Oficina de Comunicaciones, dar a conocer la presente política y todas las actuaciones que se realicen para la implementación del MSPI.
- Es responsabilidad del área de Recursos Humanos, incluir los temas de seguridad de la información en los procesos de inducción y reinducción.

6.11.2.2. Responsabilidades Generales para Proveedores o Terceros

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

Los usuarios de los proveedores y terceros deben observar las siguientes responsabilidades:

- Cada usuario será responsable de su identificador y todo lo que de él se derive, por lo que es imprescindible que este sea únicamente conocido por el propio usuario; no deberá revelarlo al resto de usuarios bajo ningún concepto.
- El usuario será responsable de todas las acciones registradas en los sistemas informáticos de FONCEP con su usuario y clave de acceso.
- Los usuarios deberán seguir las directivas definidas en relación a la gestión de las contraseñas.
- Los usuarios deberán asegurar que los equipos quedan protegidos cuando estén desatendidos.
- Se establecerán las siguientes políticas de escritorio limpio para proteger documentos en papel y dispositivos de almacenamiento removibles con el fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo:
    - Almacenar bajo llave, cuando corresponda, los documentos en papel y los medios informáticos, en mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.
    - No dejar desatendidos los equipos asignados a funciones críticas y bloquear su acceso cuando sea estrictamente necesario.
    - Asegurar la confidencialidad de los documentos tanto en los puntos de recepción y envío de información (correo postal, máquinas de escáner y fax) como en los equipos de fotocopiadora, fax y escáner.
    - La reproducción o envío de información con este tipo de dispositivos queda bajo la responsabilidad del usuario.
    - Los listados con datos de carácter personal o información confidencial deberán almacenarse en lugar seguro al que únicamente tengan acceso personal autorizado.
    - Los listados con datos de carácter personal o información confidencial deberán eliminarse de manera segura una vez no sean necesarios.
- En caso de identificarse incidentes o debilidades relacionadas con la seguridad de la información, se prohíbe a los usuarios la realización de pruebas para detectar y/o utilizar esta supuesta debilidad o incidente de seguridad.

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

- Todos los puestos de usuario con conectividad a recursos informáticos del FONCEP estarán controlados por el proceso de Gestión de Servicios TI del FONCEP.
- Ningún usuario intentará por ningún medio transgredir el sistema de seguridad y las autorizaciones, ni dispondrá de herramientas que puedan realizarlo.
- Se prohíbe la captura de tráficos de red por parte de los usuarios, salvo que se estén llevando a cabo tareas de auditoría expresamente autorizadas.
- Cuando se desatienda un puesto durante un periodo corto de tiempo el usuario deberá activar su bloqueo. Cuando se termina la jornada de trabajo se debe apagar el equipo.

6.11.2.3. Normas Específicas para Proveedores o terceros.

Todo personal vinculado a un proveedor o tercero que presta sus servicios FONCEP, está afectado por las políticas de seguridad de la información definidas en el presente documento. Las incidencias que se produzcan por efectos del incumplimiento de éstas por parte del personal de los proveedores o terceros serán evaluadas por el FONCEP, el cual determinará las medidas a adoptar.
A continuación, se definen las normas de actuación frente al uso de los sistemas de información o al tratamiento de la información por parte de todo el personal vinculado a un proveedor o tercero.

- Para hacer uso de los sistemas de información o acceder a la información del FONCEP de forma autónoma o supervisada es imperativo conocer, aceptar y cumplir la presente Política.
- Para hacer uso de los sistemas de información o acceder a la información del FONCEP de forma autónoma o supervisada, debe contar con la autorización previa y ser informado de dicha autorización.
- Proteger la información confidencial a la que tenga acceso, perteneciente o provista por los afiliados o terceros al FONCEP de toda divulgación no autorizada, modificación, destrucción o uso indebido, ya sea de manera accidental o no.

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

- Hacer un uso adecuado de los sistemas de información y redes de telecomunicaciones que utilice y tenga acceso y no permitir por intermedio suyo el accesos o usos no autorizados, interrupciones de operaciones, destrucción o robo.

6.11.2.4. Normas para preservar la confidencialidad de la Información.

Para preservar la característica de Confidencialidad de la información se deben implementar los controles adecuados que no permitan la revelación no autorizada cuando se transmite a través de segmentos de red o cuando se procesa y almacena dentro de la entidad.

Dado lo anterior se definen las normas de cara a la confidencialidad de la información:

- Se debe establecer un acuerdo de confidencialidad desde la etapa precontractual con todos los proveedores o terceros. Las políticas o normas de seguridad en cuanto a su confidencialidad tendrán efectos por el tiempo estipulado en dicho acuerdo.
- Toda información tiene el carácter de confidencial, salvo aquella información a la que se tenga acceso por medio de canales públicos.
- Se debe preservar el carácter de confidencialidad a la información confidencial a la que tienen acceso, contra divulgación no autorizada, modificación, destrucción o mal uso, cualquiera que sea el medio en que se encuentre contenida dicha información.
- No se transmitirá la información confidencial en ningún tipo de soporte, sin que esté debidamente autorizado.
- La información confidencial impresa se mantendrá en un lugar seguro.
- No se podrá utilizar la información a la que tenga acceso, para usos ajenos a la relación contractual con la entidad, y por el tiempo estipulado en el acuerdo de confidencialidad establecido entre las partes.
- La posesión de información a la que se tenga acceso autorización en virtud del contrato establecido para la prestación de servicios es estrictamente temporal, sin que ello le confiera derecho alguno de posesión, titularidad o copia sobre dicha información.

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

- Asimismo, se debe hacer la devolución de dicha información inmediatamente después de la finalización de las labores y la relación contractual que han originado el uso temporal de la misma.

6.11.2.5. Control de Acceso Físico a Instalaciones.

A continuación, se definen las normas para el control de acceso a las instalaciones de la entidad.

- El personal externo no podrá permanecer ni ejecutar trabajos en las áreas restringidas sin supervisión.
- Se consideran áreas especialmente protegidas:
  - Oficina de OSI.
  - Centros de Cómputo.
  - Instalaciones que contengan racks y elementos de red y comunicación.
  - Dirección del FONCEP.
  - Instalaciones de Electricidad.
  - Cualquier otra que se defina como tal en cada momento.
- El acceso a las áreas especialmente protegidas está controlado por un sistema Biométrico que requiere un permiso específico y por tiempo limitado, facilitado por la OSI y autorizado por el área responsable del proveedor o tercero.
- Se limitará el acceso a las áreas especialmente en el tiempo de acuerdo con la duración de la prestación de los servicios, y se autorizará únicamente cuando sea necesario y siempre bajo la vigilancia de personal autorizado. El sistema biométrico mantendrá un registro de todos los accesos de personas ajenas a la entidad.
- Se acompañará a los visitantes en áreas protegidas y el sistema registrará la fecha y hora de su entrada y salida. Dichas personas deberán ir provistos de la debida tarjeta de identificación o permiso correspondiente. Sólo se permitirá el acceso previa identificación de la persona de contacto en FONCEP.

6.11.2.6. Uso Apropiado de los Recursos

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

Los recursos que el FONCEP pone a disposición del personal externo, independientemente del tipo que sean (informáticos, datos, software, redes, sistemas de comunicación, etc.), están disponibles exclusivamente para complementar las obligaciones y propósito para la que fueron contratados. Por lo tanto, queda terminantemente prohibido:

- El uso de estos recursos para actividades no relacionadas con el propósito del servicio, o bien la extralimitación en su uso.
- Los equipos y/o aplicaciones que no estén especificados como parte del software o de los estándares de los recursos informáticos propios del FONCEP o bajo su supervisión.
- Introducir en los sistemas de información o la red corporativa contenidos obscenos, amenazadores, inmorales u ofensivos.
- Introducir voluntariamente cualquier tipo de malware (programas, macros, applets, controles ActiveX, etc.), dispositivo lógico, dispositivo físico o cualquier otro tipo que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los recursos informáticos.
- El proveedor tendrá la obligación de utilizar los programas antivirus y sus actualizaciones para prevenir la entrada en los sistemas de cualquier elemento destinado a destruir o corromper los datos informáticos.
- Intentar obtener otros derechos o accesos distintos a aquellos que les hayan sido asignados.
- Intentar acceder a áreas restringidas de los sistemas de información sin la debida autorización.
- Intentar distorsionar o falsear los registros “log” de los sistemas de información.
- Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos informáticos.
- Poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros usuarios, o dañar o alterar los recursos informáticos.
- Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos. Estos actos podrían constituir un delito de daños, según la legislación vigente.
- Cualquier archivo introducido en la red corporativa o en el puesto de trabajo del usuario a través de soportes automatizados, Internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos

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 estas normas y, en especial, las referidas a propiedad intelectual, protección de datos de carácter personal y control de virus.

6.11.2.7. Protección de los Recursos del Proveedor o Tercero.

Los recursos propios de los proveedores o terceros deberán protegerlos contra software malicioso siempre y cuando hagan parte de la red de comunicaciones o se transfiera información a la plataforma tecnológica de la entidad.

- Se mantendrán los sistemas al día con las últimas actualizaciones de seguridad disponibles.
- El software antivirus se deberá instalar y usar en todos los equipos personales, (Tablet, Portátiles, PDA, etc.) para reducir el riesgo operacional asociado con los virus u otro software malicioso.
- El software antivirus deberá estar siempre habilitado. Se establecerá una actualización automática, así como de bloqueo frente a la detección de virus informáticos.

6.11.2.8. Intercambio de Información.

A continuación, se presentan las normas para el intercambio de datos que se pueda producir por efectos del contrato de prestación de servicios o bienes entre los proveedores y terceros y el FONCEP:

- Los usuarios no deben ocultar o manipular su identidad bajo ninguna circunstancia.
- En los casos en que el FONCEP asigne un usuario genérico para usuario de dominio o correo electrónico, por ejemplo, será responsabilidad del proveedor o tercero mantener una relación actualizada de las personas que utilizan dicho usuario genérico en cada momento.
- La distribución de información ya sea en formato digital o papel se realizará mediante los dispositivos facilitados por el FONCEP para tal efecto y con la finalidad exclusiva de facilitar las funciones del puesto. el FOCNEP se reserva, en función del riesgo identificado, la implementación de medidas de control, registro y auditoría sobre estos dispositivos de difusión.
- En relación al intercambio de información, se considerarán no autorizadas las siguientes actividades:

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

- Transmisión o recepción de material protegido por Copyright infringiendo la Ley de Protección Intelectual.
- Transmisión o recepción de toda clase de material pornográfico, mensajes o bromas de una naturaleza sexual explícita, declaraciones discriminatorias raciales o de género y cualquier otra clase de declaración o mensaje clasificable como ofensivo o ilegal.
- Transferencia de archivos a terceras partes no autorizadas de material del FONCEP o material que confidencial.
- Transmisión o recepción de archivos que infrinjan la Ley de Protección de Datos de Carácter Personal o directrices del FONCEP.
- Transmisión o recepción de juegos y/o aplicaciones no relacionadas con el negocio.
- Participación en actividades de Internet como grupos de noticias, juegos u otras que no estén directamente relacionadas con el negocio.
- Todas las actividades que puedan dañar la buena reputación del FONCEP están prohibidas en Internet y en cualquier otro lugar. Esto se refiere también a actividades realizadas para el propio beneficio económico del usuario o de terceras partes, y a actividades de naturaleza política.

- Toda salida de información que contenga datos de carácter personal (tanto en soportes informáticos como en papel o por correo electrónico) sólo podrá ser realizada por personal autorizado y con el debido permiso.

6.11.2.9. Uso del Correo Electrónico

La cuenta de correo electrónico es una herramienta que el contratista debe aportar para el desempeño de los trabajos contratados.

Se establece como política general que los usuarios externos no dispondrán de una dirección de correo del FONCEP.

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

De forma excepcional, en consideración a las circunstancias que se justifiquen, y siempre previa autorización expresa, un usuario externo podría disponer de una dirección de correo del FONCEP. En tal caso, el responsable del servicio del FONCEP debe elaborar la solicitud que deberá ser evaluada conjuntamente por Recursos Humanos y por Gestión de Servicios TI.

La utilización del correo electrónico por parte de los usuarios externos estará sujeta a las siguientes normas:

- Se considera al correo electrónico una herramienta más de trabajo provista al usuario con el fin de ser utilizada conforme al uso para el cual está destinada. Esta consideración permitirá al FONCEP a implementar sistemas de control destinados a velar por la protección y el buen uso de este recurso. Esta facultad, no obstante, se ejercerá salvaguardando la dignidad del usuario y su derecho a la intimidad.
- El sistema de correo electrónico del FONCEP no deberá ser usado para enviar mensajes fraudulentos, obscenos, amenazadores u otro tipo de comunicados similares.
- Los usuarios no deberán crear, enviar o reenviar mensajes publicitarios o piramidales (mensajes que se extienden a múltiples usuarios spam).
- No está permitida la transmisión vía correo electrónico de información que contenga datos de carácter personal, salvo que este expresamente permitido.
- No está permitida la transmisión vía correo electrónico de información confidencial del FONCEP salvo que la comunicación electrónica esté bien cifrada y el envío este expresamente permitido.

6.11.2.10. Conectividad a Internet.

La utilización de internet por parte de los usuarios externos estará sujeta a las siguientes normas:

- Internet es una herramienta de trabajo. Todas las actividades en Internet deberán estar en relación con tareas y actividades de trabajo. Los usuarios no deben buscar o visitar sitios que no sirvan como soporte al servicio prestado al FONCEP.

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

- El FONCEP se reserva el derecho de, en lo permitido por el marco legal, y sin aviso previo, limitar el acceso total o parcial a Internet a partir de la red informática y terminales del FONCEP.
- El acceso a Internet desde la red corporativa se restringe por medio de dispositivos de control incorporados en la misma. La utilización de otros medios de conexión deberá ser previamente validada y estará sujeta a las anteriores consideraciones sobre el uso de Internet.
- Los usuarios no deberán usar el nombre, símbolo, logotipo o símbolos similares al del FONCEP en ningún elemento de Internet (correo electrónico, páginas web, etc.) no justificado por actividades estrictamente laborales.
- Únicamente se permitirá la transferencia de datos de o a Internet en conexión con las actividades del servicio prestado al FONCEP. La transferencia de información no relativa a estas actividades (por ejemplo, la descarga de juegos de ordenador, ficheros de sonido y contenidos multimedia) está prohibida.

6.11.2.11. Usuarios y Contraseñas.

El personal de proveedores de servicios que accede a los sistemas de información del FONCEP dentro de su ámbito de trabajo, es responsable de asegurar que los datos, las aplicaciones y los recursos informáticos sean usados únicamente para el desarrollo del objeto del contrato. Este personal está obligado a utilizar los recursos del FONCEP y los datos contenidos en ellos sin incurrir en actividades que puedan ser consideradas ilícitas o ilegales. Para obtener el acceso a los sistemas de información este personal debe disponer de un acceso autorizado (identificador de usuario y contraseña) sobre el que, como usuarios de sistemas de información, deben observar los siguientes principios de actuación y buenas prácticas:

- Cuando el usuario recibe su identificación de acceso a los sistemas de FONCEP se considera que acepta formalmente la Política de Seguridad vigente.
- Las credenciales de acceso son personales e intransferibles. En los casos de accesos con usuarios genéricos, es el proveedor o tercero responsables del recibo y salvaguarda.

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

- Todos los usuarios con acceso a un sistema de información dispondrán de una única autorización de acceso compuesta de usuario y contraseña.
- Los intentos de log-in sin éxito son limitados en número y son registrados tengan éxito o no.
- Los usuarios son responsables de toda actividad relacionada con el uso de su acceso autorizado.
- Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.
- Los usuarios no deben revelar bajo ningún concepto su usuario y/o contraseña a otra persona ni mantenerla por escrito a la vista ni al alcance de terceros.
- Es muy recomendable que los usuarios no utilicen las mismas contraseñas para uso personal y profesional.
- Los accesos autorizados temporales se configurarán para un corto período de tiempo. Una vez expirado dicho período, se desactivarán de los sistemas.
- Si un usuario tiene sospechas de que su acceso autorizado (usuario y contraseña) está siendo utilizado por otra persona, debe proceder de inmediato al cambio de su contraseña y contactar con la Mesa de Ayuda del FONCEP para notificar la incidencia.

6.11.2.12. Conexión a la Red

Sobre la conexión a la red se establecen las siguientes normas:

- El acceso de usuarios remotos estará sujeto al cumplimiento de procedimientos de autenticación previa validación del acceso.
- El FONCEP se reserva el derecho de, sin aviso previo, bloquear, suspender, alterar o monitorizar los servicios soportados en su red informática y puestos a disposición de los proveedores.
- No se deberá conectar a ninguno de los recursos de FONCEP ningún tipo de equipo de comunicaciones (tarjetas, módems, etc.) que posibilite conexiones alternativas no controladas a la red corporativa.
- Nadie deberá conectarse a la red corporativa a través de otros medios que no sean los definidos.

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

6.11.2.13. Control de Acceso Lógico.

Existe un proceso formal para la gestión de accesos a los usuarios a todos los sistemas de Información del FONCEP, el cual contiene las siguientes normas:

- Se debe asegurar la comunicación de las normas y responsabilidades en el uso de los sistemas de información del FONCEP a los usuarios al autorizarles cualquier acceso a los sistemas.
- Para cada sistema existe un conjunto de perfiles y privilegios que se atribuyen a los usuarios de acuerdo a sus necesidades.
- Los privilegios de acceso a los sistemas se atribuyen a los usuarios considerando las necesidades efectivas para el desempeño de sus funciones, no debiendo ser atribuidos ni por exceso ni por defecto.
- Los sistemas de información del FONCEP, por omisión, bloquean el acceso a los usuarios no autorizados.
- Los accesos y respectivos privilegios solo se implementan en los sistemas después de obtener todas las aprobaciones necesarias.
- Se mantiene un registro formal de todos los usuarios autorizados y respectivos privilegios de acceso a los sistemas del FONCEP.
- Los privilegios de acceso a los sistemas autorizados a los usuarios son revocados de forma automática, cuando termina su relación profesional con el FONCEP.
- Se realiza una revisión periódica con el fin de eliminar o bloquear cuentas redundantes o innecesarias.
- Los usuarios deben tener asociados, identificadores individuales (user ID), protegidos por contraseña.
- El uso de identificadores genéricos (cuentas genéricas o de grupo) se debe permitir solo en casos excepcionales debidamente justificados, aprobados y registrados.
- Las cuentas genéricas tienen asociado un usuario individual responsable de esa cuenta por parte del proveedor y/o terceros
- La nomenclatura utilizada en la generación de los identificadores obedece a reglas definidas por el FONCEP, definiendo reglas que regulen la nomenclatura a adoptar en la creación de user ID.

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

- El identificador debe ser personal, de uso exclusivo y único para todos los sistemas (cuando sea técnicamente viable).
- Los identificadores de los usuarios que ya no tienen vínculo con el FONCEP no pueden ser atribuidos a otros usuarios, excepto en áreas de gran rotación de personas.
- En los casos de áreas de gran rotación referidas en el punto anterior, debe existir una aprobación formal de la excepción por el responsable del área.
- Para las excepciones debe quedar registrado y mantenido un histórico de las personas asociadas a un user ID y en qué periodo de tiempo.
- El FONCEP se reserva el derecho de, sin aviso previo, bloquear, suspender, modificar y monitorizar a los usuarios de sus sistemas y los respectivos privilegios de acceso.

6.11.2.14. Propiedad Intelectual.

En relación a la Propiedad Intelectual se aplicarán las siguientes políticas:

- Los proveedores y/o terceros que acceden a Internet a partir de la red informática y terminales del FONCEP son responsables de respetar los derechos de propiedad intelectual aplicables a los contenidos accedidos.
- Se garantizará el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual.
- Queda estrictamente prohibido el uso de programas informáticos sin la correspondiente licencia.
- Asimismo, queda prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o invención protegida por la propiedad intelectual sin la debida autorización.
- El FONCEP únicamente autorizará el uso de material producido por el mismo, o material autorizado o suministrado al mismo por su titular, conforme los términos y condiciones acordadas y lo dispuesto por la normativa vigente.

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

6.11.2.15. Incidencias.

En el caso de detectarse alguna incidencia relacionada con los sistemas de información se seguirán las siguientes normas:

- Todo el personal externo deberá ponerse en contacto con la Mesa de Ayuda en caso de que detecte cualquier incidencia relacionada con la información o los recursos informáticos del FONCEP.
- Cualquier usuario podrá trasladar al responsable de la Mesa de Ayuda sugerencias y/o debilidades, que pueda tener relación con la seguridad de la información y las directrices contempladas en la presente Política.
- Se deberá notificar al responsable de la Mesa de Ayuda cualquier incidencia que se detecte y que afecte o pueda afectar a la seguridad de los datos de carácter personal, pérdida de información impresa y/o medios lógicos, sospechas de uso indebido del acceso autorizado por otras personas, recuperación de datos, etc.
- La Mesa de Ayuda centraliza la recopilación, análisis y gestión de las incidencias recibidas.

6.11.3. Seguimiento y Control.

Con el fin de velar por el correcto uso de los recursos informáticos, a través de los mecanismos formales y técnicos que se considere oportunos, el FONCEP comprobará, ya sea de forma periódica o cuando por razones específicas de seguridad o del servicio resulte conveniente, la correcta utilización de dichos recursos. En caso de evidenciar que alguien utiliza de forma incorrecta aplicaciones, datos y cualquier otro recurso informático, se le comunicará tal circunstancia y se le brindará, la formación necesaria para el correcto uso de los recursos.
En caso de apreciarse mala fe en la incorrecta utilización, el FONCEP ejercerá las acciones que legalmente le amparen para la protección de sus derechos.

6.11.4. Actualización de la Política.

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

Debido a la propia evolución de la tecnología, las amenazas de seguridad y a las nuevas normas legales en la materia, el FONCEP se reserva el derecho a modificar esta Política cuando sea necesario. Los cambios realizados en esta Política serán divulgados a todos los proveedores y terceros de servicios a las que les aplique utilizando los medios que se consideren pertinentes. Es responsabilidad de cada empresa proveedora garantizar la divulgación y conocimiento de la Política de Seguridad más reciente del FONCEP por parte de su personal.

6.12 Gestión de incidentes de seguridad de la información

6.12.1 Objetivo.

Gestionar las incidencias que afectan a la seguridad de la Información.

6.12.2 Política.

Se debe asegurar que se haga una adecuada evaluación del impacto en el FONCEP frente a los eventos de seguridad relevantes, en los cuales las políticas de seguridad 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 del mismo. 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. La Entidad debe contar con los procedimientos que se consideren necesarios para el reporte, control, seguimiento, recolección de evidencias, solución, mejoramiento y aprendizaje

6.13 Aspectos de seguridad de la información de la gestión de continuidad de negocio

6.13.1 Objetivo.

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

Considerar la continuidad de seguridad de la información en los procesos de gestión de la continuidad de negocio de la Entidad.

6.13.2 Política.

El FONCEP debe incluir los requisitos de seguridad de la información en los procesos de gestión de continuidad de negocio en toda la organización.

Se debe desarrollar e implementar planes para mantener o recuperar las operaciones y asegurar la disponibilidad de la información con las condiciones de calidad requeridos por la Entidad, después de la interrupción o la falla de los procesos críticos para la entidad. Dichos planes deben cumplir con los requisitos de seguridad de la información definidos por las políticas de seguridad de la información establecidas en este documento.

Se debe procurar que las instalaciones de procesamiento la Entidad, cuente redundancia suficiente para cumplir los requisitos de disponibilidad requeridos y realizar pruebas de simulación de varios escenarios posibles de emergencias y lograr buscando la recuperación de información en los tiempos y condiciones definidos.

6.14 Cumplimiento

6.14.1 Objetivo.

Prevenir los incumplimientos de las leyes penales o civiles, de las obligaciones reglamentarias o contractuales y de las exigencias de seguridad.

6.14.2 Política.

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

Garantizar que la gestión de la seguridad dé cumplimiento adecuado a la legislación vigente para lo cual analizará los requisitos legales aplicables a la información que se gestiona incluyendo los derechos de propiedad intelectual, los tiempos de retención de registros, privacidad de la información, uso adecuado de recursos de procesamiento de información y uso de criptografía.

Para la implementación de esta política se debe tener en cuenta los siguientes principios.

6.14.3 Identificación de la legislación aplicable.

El FONCEP establece que, ante cualquier requerimiento o implementación relacionada con los sistemas de información, se deben observar las leyes y regulaciones vigentes para asegurar los requisitos regulatorios que apliquen.

6.14.4 Derechos de propiedad intelectual (DPI).

Deben existir controles y se deben ejecutar revisiones de su aplicación para asegurar que se están respetando los derechos de propiedad intelectual del material contenido en los sistemas de información utilizados por la entidad.

Deben existir mecanismos que permitan un control estricto de las licencias de software utilizadas en la Entidad, garantizando que se tenga el permiso o adquisición necesario para su uso.

El Administrador de cada plataforma debe mantener el control de todas las licencias de software adquiridas e instaladas.

Se deben realizar revisiones periódicas a los sistemas de información, servidores y estaciones de trabajo, a fin de verificar que no se tenga instalado software no licenciado y autorizado previamente, de acuerdo con el procedimiento de autorización de software. El usuario es responsable por la instalación y utilización de programas no autorizados en su computador.

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

6.14.5 Protección de los registros de la organización.

Todos los registros que el líder funcional y los jefes de área definan como importantes para el FONCEP, deben guardarse en sitios seguros con el fin de evitar pérdidas, destrucción y falsificaciones. La solicitud debe realizarse en forma explícita por parte del propietario de la información.

6.14.6 Protección de los datos y privacidad de la información personal.

Los registros de personal y sus datos privados establecidos por la normatividad deben almacenarse en lugar seguro para evitar robo de información privada que pueda afectar la integridad de los usuarios del FONCEP.

Se debe establecer el tiempo de retención apropiado, determinado por la legislación colombiana vigente, para el almacenamiento de los registros identificados.

6.14.7 Reglamentación de los controles criptográficos.

Se deben utilizar controles criptográficos que cumplan todos los acuerdos, las leyes y los reglamentos pertinentes

6.14.8 Cumplimiento con las políticas y las normas de seguridad.

Los Directivos y el Comité de Seguridad de la Información, debe asegurar que todas las políticas, normas, procedimientos y estándares definidos para el FONCEP son cumplidas en su totalidad.

6.14.9 Verificación del cumplimiento técnico.

Los sistemas de información del FONCEP, deben ser revisados periódicamente para verificar que cumplan con los estándares de seguridad definidos.

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

Toda actividad de Auditoría debe estar planificada y acordada con el cotte de seguridad de la información, previo a su ejecución de modo que no afecte a la operatoria diaria del Sistema y evitar interrupciones graves en toda la plataforma tecnológica.

6.15 Conexión Segura del Teletrabajo

El FONCEP por medio de la Gerencia de Talento Humano, definirá lineamientos para controlar la modalidad de Teletrabajo en sus oficinas como instrumento para promover la modernización de la organización, la inserción laboral, reducir el gasto en las Instituciones Públicas, incrementar la productividad del funcionario, el ahorro de combustibles, la protección del medio ambiente, y favorecer la conciliación de la vida personal, familiar y laboral, mediante la utilización de las Tecnologías de la Información y las Comunicaciones TIC´s

La figura del Teletrabajo se define como aquella modalidad de prestación de servicios de carácter no presencial, en virtud de la cual un funcionario público, puede desarrollar parte de su jornada laboral mediante el uso de medios telemáticos desde su propio domicilio, u otro lugar habilitado al efecto, siempre que las necesidades y naturaleza del servicio lo permitan, y en el marco de la política de conciliación de la vida personal, familiar y laboral de los funcionarios públicos.

Como en cualquier otra actividad que involucre equipos conectados a Internet, hay ciertas medidas a tener en cuenta para garantizar la seguridad. Todo lo relacionado con los equipos de trabajo, la responsabilidad y los costos debe estar definido claramente antes de implementar un formato de teletrabajo. Por ejemplo, si se usan dispositivos personales o la compañía los proporciona, o si hay un soporte técnico adecuado para resolver problemas de acceso y seguridad, así como definir quiénes pueden acceder a qué información.

6.15.1 Objetivo.

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

Definirá lineamientos para controlar la modalidad de Teletrabajo en sus oficinas como instrumento para promover la modernización de la organización, la inserción laboral, reducir el gasto en las Instituciones Públicas, incrementar la productividad del funcionario, el ahorro de combustibles, la protección del medio ambiente, y favorecer la conciliación de la vida personal, familiar y laboral, mediante la utilización de las Tecnologías de la Información y las Comunicaciones Tics

6.15.2 Política.

La presente política tiene por objeto 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. Este documento formara parte de la política general de Teletrabajo de FONCEP.

- El funcionario de FONCEP deberá satisfacer los siguientes requisitos: a) Ser funcionario de FONCEP. b) Contar con el aval del área correspondiente. c) Contar con un espacio físico de acuerdo a la Ley 6727 de riesgos de trabajo y su normativa. d) Tener acceso a internet en el lugar señalado para teletrabajar. e) Suscribir un contrato laboral que regula la prestación de los servicios que presta al FONCEP, bajo la modalidad de teletrabajo.

- 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.

- El teletrabajador se encuentra en la obligación de velar por el cuidado y buen uso que se dé al equipo que le fue asignado, así como también, deberá acatar todas las directrices y normatividades que se apliquen 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**

- Es deber del Teletrabajador, dar un uso adecuado a los equipos proporcionados por esta Entidad, 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 los mismos será trasladada al Teletrabajador, sin perjuicio de las acciones disciplinarias o fiscales que procedan.

- 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.

- 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.

- Los funcionarios no deben compartir sus cuentas de usuario y contraseñas, ni desatender su sesión de Teletrabajo, ni utilizar conexiones no confiables (conexiones Wi-Fi abiertas, acceder a conexiones y/o redes públicas, módems USB), conjuntamente deben adherirse a los lineamientos de seguridad de la información definidos por FONCEP.

- Los funcionarios deben utilizar diferentes cuentas de usuario en el equipo, una cuenta para los entornos confiables (Teletrabajo) y otra para asuntos personales.

- Los propietarios de los activos de información velarán 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.

- Los propietarios de los activos de información deben monitorear periódicamente los accesos a los entornos confiables (Teletrabajo) asignados a los funcionarios.

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

- 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.

- 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.

- El proceso de Gestión de Servicios TI 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.

- 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.

- El proceso de Gestión de Servicios TI 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.

- 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.

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

- La Oficina de Planeación de FONCEP debe realizar una valoración de los riesgos existentes en los entornos confiables (Teletrabajo), en la sensibilidad de la información a la cual se accederá, en las vulnerabilidades presentes en las comunicaciones y en las amenazas de los accesos no autorizados.

- El Grupo de Talento Humano debe certificar que los funcionarios autorizados para Teletrabajo del Instituto firmen un acuerdo y/o cláusula de confidencialidad, un documento de aceptación de la Política de Seguridad de la Información y un permiso de revisión y/o auditoría por parte de la Entidad; conjuntamente debe certificar que los funcionarios autorizados, fueron sensibilizados y/o capacitados en los riesgos, conceptos y responsabilidades relacionados con ejecutar su actividad o labor a través de Teletrabajo (ejemplo de responsabilidades: sobre la clasificación de información, sobre la divulgación no autorizada de información, sobre el cumplimiento de las políticas de seguridad de la información de la Entidad).

6.15.3 Seguimiento y Control.

La política de Teletrabajo debe ser revisada cada seis meses o cuando se presenten eventos que obliguen a su actualización.
En caso de evidenciar que alguien utiliza de forma incorrecta aplicaciones, datos y cualquier otro recurso informático, se le comunicará tal circunstancia y se le brindará la formación necesaria para el correcto uso de los recursos.
En caso de apreciarse mala fe en la incorrecta utilización, el FONCEP ejercerá las acciones que legalmente le amparen para la protección de sus derechos.

6.15.4 Actualización de la Política.

Debido a la propia evolución de la tecnología, las amenazas de seguridad y a las nuevas normas legales en la materia, el FONCEP se reserva el derecho a modificar esta Política cuando sea necesario. Los cambios realizados en esta Política serán divulgados a todos los teletrabajadores, utilizando los medios que se consideren pertinentes.

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

CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DE LA MODIFICACIÓN
001	Septiembre de 2017	Creación y Adopción del Documento El documento pertenecía al proceso de Gestión de Administración de activos.
002	Julio 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 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. Unificar documentos relacionados con políticas ya existentes dentro del manual

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Sandra Milena Velásquez **Mónica C. chacón H.** **Enlace del proceso** Profesional OIS	**José Ebert Bonilla Olaya** **Responsable del proceso** Jefe de la Oficina Informática y Sistemas **Alejandra Paola Suárez Franco** **Asesor OAP** Profesional OAP	**José Ebert Bonilla Olaya** **Líder del proceso** Jefe de la Oficina Informática y Sistemas **Cristian Mauricio Amaya Martínez** **Jefe OAP**

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