A) HISTORIAL DE CAMBIOS

VERSIÓN	FECHA	JUSTIFICACIÓN DE LA MODIFICACIÓN
1	09-2009	Lanzamiento del documento Políticas de Tecnología Informática.
2	06- 2010	Actualización del documento de Políticas.
3	9/05/2019	Se incluye en el documento la introducción, objetivogeneral, objetivos específicos, ámbito de aplicación, marco legal, violación de las políticas, se revisaron y actualizaronlas políticas de tecnologías de la información.
4	30/08/2019	Actualización de los siguientes numerales: 6. Definiciones 8.8. Seguridad de la información: Confidencialidad 8.9 Desarrollo de software 8.16 Acuerdo de confidencialidad
5	13/11/2020	• Cambio de título • Redefinición del contexto, alineado con: Modelo de Seguridad y Privacidad de la Información – MSPI de MINTIC, objetivo estratégico de la Entidad "Consolidar el sistema de seguridad de la información" y la norma ISO 27001 • Separación entre políticas generales y manual de políticas específicas, donde este último es un anexo.
6	16/03/2023	En la política 4. Control de acceso en el literal e. Control de acceso a redes, sistema y aplicaciones. Se agrega los numerales: c. Uso de equipos personales, sujeto a autorización de la Oficina Asesora de Planeación y Sistemas, mediante formato descrito en el ANEXO 3, para el cumplimiento de requisitos de línea base de controles de seguridad. d. Los servidores públicos y contratistas de la entidad no podrán almacenar información reservada en ningún dispositivo de almacenamiento personal. Se agrega el ANEXO 3. FORMATO PARA SOLICITUD Y AUTORIZACIÓN DE USO DE EQUIPOS PERSONALES EN LAS REDES DE COMUNICACIONES DE FONPRECON ANEXO 2. ACUERDO DE CONFIDENCIALIDAD**,** se actualiza la redacción de este texto alineado al uso de equipos no suministrados por Fonprecon: Todo vínculo contractual que implica el acceso en algún nivel a la información de FONPRECON, visitas temporales de terceros, contratistas o funcionarios que requieren la conexión de computadores o dispositivos móviles a las redes de comunicación de la Entidad y cuyos equipos no son suministrados por Fonprecon, debe incluir el siguiente acuerdo de confidencialidad En la política 7. GESTIÓN DE EQUIPOS: se agrega el numeral j j. Las personas externas a FONPRECON que ingresen equipos de cómputo personales, deben registrarlos en la planilla de ingreso y retiro de elementos provista por la empresa de seguridad. La seguridad de los elementos ingresados es responsabilidad del propietario del equipo
7	10/07/2024	Alinear al contexto de seguridad de la información, ciberseguridad y protección de la privacidad de conformidad con: • Norma técnica colombiana NTC-ISO/IEC 27001:2022 • Guía técnica colombiana GTC-ISO/IEC 27032:2020

B) REVISIONES Y APROBACIONES DEL DOCUMENTO

ELABORÓ	REVISÓ	APROBÓ
Nombre: Jesus Goyes Alvarado	Nombre: German Armando Correa Amado	Nombre: Luis Enrique Cortés Callejas
Cargo: Contratista Asesor Seguridad y Ciberseguridad	Cargo: Jefe Oficina Asesora de Planeación y Sistemas	Cargo: Director General (E)
Fecha: 02/07/2024	Fecha: 09/07/2024	Fecha: 10/07/2024

REVISÓ	REVISÓ	REVISÓ
Nombre: Oscar Herrera Isaza	Nombre: Lilia Alexandra Muñoz Moreno	Nombre: Diana Marcela Burgos
Cargo: Contratista Asesor Sistemas de Gestión	Cargo: Profesional Oficina Asesora de Planeación y Sistemas	Cargo: Profesional Oficina Asesora de Planeación y Sistemas
Fecha: 08/07/2024	Fecha: 03/07/2024	Fecha: 04/07/2024

REVISÓ
Nombre: Julián David Lara Romero
Cargo: Coordinador Grupo Interno Administrativo y de Gestión Judicial Oficina Asesora Jurídica
Fecha: 05/07/2024

C) LISTA DE DISTRIBUCIÓN

N°	NOMBRE Y CARGO
1	Director General
2	Jefe Oficina Asesora de Planeación y Sistemas
3	Jefe Oficina Asesora Jurídica
4	Subdirector de Prestaciones Económicas
5	Subdirector Administrativo y Financiero
6	Asesor de Control Interno
7	Coordinador Grupo Interno de Gestión de Cartera
8	Coordinador Grupo de Talento Humano
9	Coordinadora Grupo de Afiliaciones e Historia Laboral
10	Coordinadora Grupo de Archivo y Correspondencia
11	Coordinador Grupo Administrativo y de Gestión Judicial
12	Coordinador Grupo Interno de Trabajo Gestión de Bienes y Servicios y de Presupuesto
13	Coordinadora Grupo Gestión Contable
14	Coordinadora Grupo de Tesorería
15	Profesional Unidad de Riesgo Operativo
16	Profesionales de Gestión Tecnológica

Contenido

1. OBJETIVO GENERAL.

Establecer las reglas, directrices, lineamientos y las medidas organizacionales, tecnológicas, técnicas y físicas, de conformidad con el modelo de Seguridad y Privacidad de la Información (MSPI) definido por la política de gobierno digital, el sistema general de gestión de seguridad de la entidad SGSI, con la finalidad de evitar, prevenir y mitigar los riesgos que puedan comprometer confidencialidad, integridad y disponibilidad de los activos de información.

2. OBJETIVO ESTRATÉGICO

Dentro de la planeación estratégica organizacional se plantea este objetivo con vigencia de 4 años a partir del 2023:

- Consolidar el sistema de gestión de seguridad de la información - SGSI

3. OBJETIVOS ESPECIFICOS.

- Mitigar los riesgos de los procesos de la entidad
- Abordar los principios de seguridad de la información: confidencialidad, integridad y disponibilidad
- Dar cumplimiento a los requisitos legales y normativos en materia de ciberseguridad, seguridad y privacidad de la información.
- Mantener la confianza en los grupos de valor
- Fortalecer el sistema de gestión de seguridad de la información - SGSI.
- Proteger los activos de información
- Establecer las políticas, procedimientos e instructivos en materia de ciberseguridad y seguridad de la información.
- Generar un cambio organizacional mediante la concienciación en ciberseguridad, seguridad y privacidad
- Fortalecer la continuidad del negocio

4. ALCANCE.

Forman parte del alcance de estas políticas:

- Todos los activos de información con datos y/o en cualquier estado ya sea de reposo, conservación, transporte, consulta, transformación y/o independientemente del medio (digital, manuscrita, fonética, impresa), presentación y aplicable a cualquier lugar geográfico en el cual se encuentre ubicada.

- Todos los activos tecnológicos que posibilitan la conservación, almacenamiento, transporte, consulta, transformación

- Todos los procesos de la entidad y sus interacciones con los grupos de valor donde interviene el uso de los activos de información

5. APLICABILIDAD.

El presente documento, sus anexos y procedimientos, es de cumplimiento obligatorio para:

1. Toda la entidad, las subdirecciones, sus oficinas asesoras, funcionarios públicos, contratistas, proveedores y todas aquellas personas y/o terceros que debido al cumplimiento de sus funciones compartan, utilicen, recolecten, procesen, intercambien y/o consulten información de la Entidad.
2. Los procesos internos que traten Activos de información en cumplimiento de sus objetivos.
3. Contratistas, funcionarios, proveedores y demás grupos de interés que se les haya concedido acceso a los activos de información dentro de un lapso definido para fines específicos de actividades de apoyo, misionales u otras definidas dentro de un alcance contractual o funciones
4. Entidades de vigilancia y control que se les haya concedido acceso a los activos de información dentro de un lapso definido para fines específicos de actividades propias de su misionalidad.

6. SANCIONES POR INCUMPLIMIENTO

El incumplimiento a las políticas del presente documento traerá consigo, procesos disciplinarios, sanciones por incumplimiento de contratos y las actuaciones legales de conformidad con la legislación colombiana y lo estipulado por el organismo de función pública y la oficina de control interno disciplinario, así como de los acuerdos internacionales de los que forme parte vinculante el estado colombiano

De acuerdo con lo anterior, las siguientes son algunas de las actuaciones que pueden causar un incumplimiento de las presentes Políticas:

1. No firmar los acuerdos de Confidencialidad o incumplir dicho acuerdo.
2. Incumplir cualquiera de las políticas o lineamientos del presente documento.
3. No reportar oportunamente los Incidentes de Seguridad y/o violaciones a la política de seguridad y privacidad de la información cuando se tenga conocimiento de ello.

4. No cumplir con los controles establecidos por la entidad para la protección de los Activos de Información.
5. Ingresar a sitios restringidos o áreas sensibles sin previa autorización o acompañamiento de personal autorizado.
6. No mantener la confidencialidad en sus credenciales de acceso a los servicios tecnológicos de la entidad
7. Compartir credenciales de acceso a servicios tecnológicos de la entidad
8. Hacer uso de la red interna para obtener, mantener o difundir contenido que vaya en contra del código de ética de la entidad.
9. Recibir o enviar Información confidencial de la entidad a través de cualquier medio sin la trazabilidad de la autorización del nivel apropiado.
10. Acceso a la red interna con dispositivos no autorizados.
11. Distribuir o enviar software malicioso utilizando los activos tecnológicos de la entidad.
12. Retirar de las instalaciones de la entidad activos de información sin la trazabilidad de autorización del nivel apropiado.
13. Instalar software no autorizado en los equipos de trabajo.
14. No cumplir con la política de tratamiento de datos personales.
15. Hacer uso de software de propósito específico para distribuir malware, alterar o detener las operaciones tecnológicas
16. Hacer uso de software de propósito específico para escanear las redes y configuraciones de la infraestructura tecnológica
17. Mantener copias de activos de información en cualquier lugar geográfico sin la trazabilidad de autorización del nivel apropiado.
18. Liderar, participar activamente o posibilitar afectaciones a la confidencialidad, integridad o confidencialidad de la información.

7. REVISIÓN DE CUMPLIMIENTO

Esta actividad la realiza la oficina asesora de control interno, dada su gestión independiente de los procesos, en la frecuencia y alcance aprobada en comité de control interno, en lo concerniente al seguimiento del cumplimiento de estas políticas y en general del sistema general de seguridad de la información SGSI.

En caso de existir incumplimiento, se comunicará a la instancia administrativa pertinente, para su análisis y decisiones a las que haya lugar.

8. ENTRADA EN VIGENCIA

Las políticas de seguridad y privacidad de la Información en la presente versión, rigen a partir de la fecha de aprobación de este documento

9. DEFINICIONES.

- **Política de seguridad de la información:** Documento de alto nivel o que es entendible por todos los interesados, que establece un conjunto de reglas, pautas y procedimientos adoptados

la entidad con el objetivo propender por un uso adecuado y seguro de los activos de información.

- **Procedimientos de Seguridad de la Información:** Desarrollar y formalizar procedimientos que permitan gestionar la seguridad de la información en cada uno de los procesos definidos en la entidad.
- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- **Análisis de Riesgo**: Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo. (ISO/IEC 27000).
- **Auditoría**: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).
- **Autorización**: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)
- **Bases de Datos Personales**: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)
- **Ciberseguridad**: Preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio.
- **Ciberespacio**: Entorno complejo que resulta de la interacción de las personas, el software y los servicios a través de internet, por medio de dispositivos tecnológicos y redes conectados al mismo, que no existen en forma física alguna.
- **Ciberdelito**: Actividad delictiva donde servicios o aplicaciones en el ciberespacio se utilizan o son el objetivo de un crimen o donde el ciberespacio es la fuente, herramienta, blanco o el lugar de un delito.
- **Ciberprotección**: Condición de estar protegido contra consecuencias físicas, sociales, espirituales, financieras, políticas, emocionales, laborales, psicológicas, educacionales u otro tipo de consecuencias por falla, daño, error, accidente, o cualquier evento en el ciberespacio que podría ser considerado no deseable.
- **Ciberintruso**: Personas u organizaciones que se registran y mantienen en direcciones URL que se asemejan a las referencias o nombres de otras organizaciones en el mundo real.
- **Hacking (piratería informática):** Acceso intencional a un sistema informático sin la autorización del usuario o el propietario.
- **Hacktivismo:** Realizar piratería informática con un propósito o motivación política o social
- **Control**: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Botnet**: Software de control remoto, específicamente una colección de bots maliciosos, que se ejecutan de manera autónoma o automáticamente en computadoras comprometidas.
- **Bot**: Programa de software automatizado utilizado para llevar a cabo tareas específicas.
- **Cookie**: Datos de intercambio en aplicaciones web a través del navegador de internet
- **Datos Abiertos**: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de

cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)

- **Información Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
- **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.
- **Activos de información:** Son ficheros y bases de datos, contratos y acuerdos, documentación del sistema, manuales de los usuarios, material de formación, aplicaciones, software del sistema, equipos informáticos, equipo de comunicaciones, servicios informáticos y de comunicaciones, utilidades generales como por ejemplo iluminación, energía y aire acondicionado y las personas, que son al fin y al cabo las
  que en última instancia generan, transmiten y destruyen información, esdecir dentro de una organización se han de considerar todos los tipos deactivos de información.
- **Equipamiento Auxiliar:** Se consideran a los equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos (ejemplos: fuentes de alimentación, sistemas de alimentación ininterrumpida (ups), generadores eléctricos, equipos de climatización, cableado, cable eléctrico, fibra óptica, mobiliario (armarios, etc.), cajas fuertes).
- **Hardware:** Se consideran los medios materiales físicos destinados a soportar directa o indirectamente los servicios que presta la organización,almacenan temporal o permanente datos y son soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos (ejemplos: servidores, portátiles, equipos de mesa,tablets, celulares, agendas electrónicas, equipo virtual, equipamiento de respaldo, impresoras, scanner, dispositivos criptográficos, módems, switch, router, firewall, central telefónica, teléfonos IP, discos, discos virtuales, CD-ROM, DVD, memorias USB, cintas magnéticas).
- **Información:** La información es un activo abstracto que es almacenado en equipos (normalmente agrupado como ficheros o bases de datos) o es transferido de un lugar a otro por los medios de transmisión de datos(ejemplos: información personal, información estratégica, ficheros, copias de respaldo, datos de configuración, datos de gestión interna, datos de acceso (usuarios, contraseñas), logs, códigos fuentes, códigosejecutables, datos de prueba).
- **Instalaciones:** Los lugares donde se hospedan los sistemas de información y comunicaciones (ejemplos: edificios, cuartos, vehículos, instalaciones de respaldo).
- **Procesos:** Los procesos son una serie de pasos que se enfocan en lograr un resultado especifico (ejemplos: procesos cuya perdida o degradación hacen imposible llevar a cabo la misión de la entidad, procesos que contienen procesos secretos o implican tecnología propietaria, propietarios que si modifican, pueden afectar de manera muysignificativa el cumplimiento de la misión de la entidad, procesos que sonnecesarios para que la organización cumpla con los requisitos contractuales, legales o reglamentarios).
- **Recurso Humano:** Aquellas personas que, por su conocimiento, experiencia y criticidad para el proceso, son consideradas activos de información (ejemplos: viceministros, coordinador de infraestructura, JefeTI, etc.).
- **Red:** Incluye tanto instalaciones dedicadas como servicios de comunicaciones contratados a

terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro (ejemplos: red telefónica, red de datos, comunicaciones radio, red inalámbrica, red local, red metropolitana, Internet).

- **Servicios:** Satisfacen una necesidad de los usuarios (ejemplos: Internet,páginas de consulta, directorios compartidos, Intranet, acceso remoto a cuenta local, correo electrónico, transferencia de ficheros (ftp)).
- **Software:** Se le pueden dar múltiples denominaciones (programas,aplicativos, desarrollos, etc.), se refiere a tareas que han sido automatizadas. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación delos servicios (ejemplos: software de aplicación, interfaces, software del sistema, herramientas de desarrollo y otras utilidades relacionadas,navegador web, cliente de correo electrónico, sistema de gestión de bases de datos, ofimática, antivirus, sistema operativo, gestor de máquinas virtuales, sistema de copias de seguridad).
- **Seguridad de la información:** La seguridad de la información es el conjunto de medidas técnicas, operativas, organizativas y legales que permiten a las organizaciones proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma. El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarseen diferentes medios o formas, y no solo en medios informáticos.
- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo delos activos de información.
- **Disponibilidad:** Propiedad de que la información sea accesible yutilizable por solicitud de una entidad autorizada.
- **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos entidades o procesos no autorizados.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.
- **Ambiente de Pruebas:** Escenario con activos tecnológicos separados del ambiente de producción, con el propósito de probar los resultados del desarrollo o mantenimiento de software u otros componentes de hardware o software, antes de su publicación final en el ambiente productivo.
- **Ambiente Productivo:** Activos de diferente propósito, que soportan los distintos servicios tecnológicos que se encuentran en operación y uso con objetivos de soportar los procesos misionales y de apoyo.

10. MARCO DE REFERENCIA

- **Constitución Política de Colombia**. Artículo 15.
- **Circular Externa 007 de 2018, expedida por la Superintendencia Financierade Colombia**: Imparte instrucciones relacionadas con los requerimientos mínimos para la gestión del riesgo de ciberseguridad.
- **Ley 1266 de 2008,** parcialmente reglamentada por el Decreto 1081 de 2015**:** 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. (Habeas Data).

- **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 informacióny de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".
- **Ley 1712 de 2014:** Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- **Ley 1581 de 2012:** Reconoce y protege el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada.
- **Decreto 1377 de 2013:** Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- **Decreto 886 de 2014:** Por el cual se reglamenta el artículo 25 de la Ley 1581 de2012, 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 1078 de 2015**. Por el cual se expide el Decreto único reglamentario delSector de las Tecnologías de la información y las Telecomunicaciones.
- **Decreto 1008 de 2018** por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte2 del Libro 2 del Decreto número 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- **Resolución FONPRECON 253-2014:** Por la cual se definen lineamientos para políticas en materia de Seguridad de la Información.
- **Resolución FONPRECON 517 de 2017:** por la cual se crea el comité de Gestión y Desempeño Institucional.
- **Resolución FONPRECON 395 DE 2019:** por la cual se modifica la Resolución 517 de 2017 (artículo primero: funciones del Comité de Gestión y Desempeño Institucional, como instancia orientadora de la Gestión Tecnológica en la Entidad)
- **Circular interna FONPRECON 20192000000044 del 08-04-2019:**Lineamientos para copia de seguridad para archivos en las estaciones de trabajo.
- **Estándar Internacional ISO/IEC 27032:** Marco de referencia para laciberseguridad
- **Norma Técnica Colombiana NTC/ISO/ IEC 27001:** Marco de referencia para para la seguridad de la información
- **Modelo de seguridad y privacidad de la información – MINTIC:** Establecido por MINTIC para dar cumplimiento a lo establecido en el componente deseguridad y privacidad de la información de la estrategia de gobierno digital.
- **Guía para la Administración del riesgo y el diseño de controles de las entidades públicas:** Departamento Administrativode la Función Pública, riesgos de gestión, corrupción y seguridad digital.

11. PRINCIPIOS

El Fondo de Previsión Social del Congreso de la República, en adelante FONPRECON, establece los siguientes principios que enmarcan el fortalecimiento y la mejora continua del sistema general de seguridad de la información SGSI, mediante la implementación de las políticas de este documento:

1. FONPRECON opera y mejora de forma continua el Sistema de Gestión de Seguridad de la Información SGSI, derivado de la adopción del modelo de seguridad y privacidad de la información MSPI delMINTIC, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.
2. FONPRECON dispondrá los recursos humanos, técnicos, tecnológicos y financieros de acuerdo con su planeación y disponibilidad financiera para la implementación de controles físicos y tecnológicos con el fin de mitigar los riesgos operativos y de ciberseguridad derivados de amenazas internas, externas, cibernéticas, conocidas y emergentes (cibercrimen, ciberdelito, entre otras) que afecten la confidencialidad, integridad y disponibilidad de la información de conformidad con los requisitos legales y reglamentarios vigentes.
3. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas por la Entidad y aceptadas con carácter decumplimiento mandatorio por cada uno de los empleados, contratistas o terceros.
4. FONPRECON mantendrá actualizado el inventario de activos, como uno de los insumos fundamentales a la hora de identificar riesgos y diseño de controles.
5. FONPRECON protegerá la información generada, procesada o resguardada porlos procesos de negocio y activos de información que hacen parte de su actividad institucional.
6. FONPRECON protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos, reputacionales o legales debido a un uso incorrecto de
   esta. Para ello se identificarán los riesgos y aplicación de controles de acuerdocon la clasificación de la información de su propiedad o en custodia.
7. FONPRECON protegerá su información de las amenazas originadas por parte del personal que intervenga en su administración, manejo o custodia.
8. FONPRECON protegerá las instalaciones de procesamiento y la infraestructuratecnológica que soporta sus procesos críticos.
9. FONPRECON controlará la operación de sus procesos de negocio garantizandola seguridad de los recursos tecnológicos y las redes de datos.
10. FONPRECON implementará mecanismos de control de acceso a la información, sistemas, recursos de red e instalaciones.
11. FONPRECON intervendrá para que la seguridad sea parte integral del ciclo de vida de los sistemas de información, así como de la información en medio físicoclasificada dentro del inventario de activos.
12. FONPRECON ejecutará una mejora efectiva de su modelo de seguridad, para enfrentar, mitigar o eliminar las debilidades asociadas con los sistemas de información y demás activos.
13. FONPRECON garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en la identificación de escenarios adversos, riesgos, alternativas de operación en contingencia y aplicación de controles, así como el análisis del impacto que se

puedan generar.

14. FONPRECON garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales vigentes en materia de seguridad y privacidad de lainformación.

12. POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

A continuación, se establecen las siguientes políticas que soportan el Sistema de Gestión de Seguridad de la Información SGSI de la entidad:

12.1 POLÍTICA DE ROLES Y RESPONSABILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN

Nivel	Responsabilidades	Responsable
Estratégico	▪ Definir y aprobar la estrategia informática y de seguridad digital que permita lograr los objetivos y minimizar los riesgos de la operación. ▪ Definir la prestación del servicio ▪ Autorizar la adquisición de bienes y servicios relacionados y requeridos para garantizar la seguridad de la información ▪ Revisar y aprobar planes, políticas, procedimientos, manuales del sistema general de seguridad de la información – SGSI ▪ Orientar y decidir acerca de la adopción de controles ▪ Comunicar al consejo directivo y otras instancias pertinentes ▪ Exigir a los procesos y demás grupos de valor, el cumplimiento de las políticas de seguridad de la información ▪ Garantizar el ejercicio de los derechos de los titulares de los datos personales	Dirección General Alta dirección
Táctico	▪ Asesorar a la entidad en la mejora continua del SGSI ▪ Fomentar la implementación de la Política de Gobierno Digital ▪ Diseñar y aplicar estrategias de capacitación y sensibilización en materia de seguridad y privacidad, ciberseguridad, datos personales ▪ Seguir y controlar la estrategia de seguridad digital, que permita la minimización de riesgos. ▪ Monitorear y gestionar la prestación del servicio ▪ Gestionar la adquisición de bienes y/o servicios relacionados y requeridos para garantizar la seguridad de información ▪ Convocar el comité estratégico de seguridad, ciberseguridad y datos personales ▪ Liderar la actualización del catálogo de activos y su respectiva clasificación ▪ Comunicar a la alta dirección y otras instancias pertinentes	Jefe Oficina de Planeación y Sistemas
Táctico	▪ Liderar la gestión de riesgos de seguridad. ▪ Gestionar el desarrollo e implementación de políticas, normas, directrices y procedimientos de seguridad de gestión de TI e información. ▪ Definir mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de implantación de las medidas de seguridad. ▪ Supervisar la respuesta a incidentes, así como la investigación de violaciones de la seguridad, ayudando con las cuestiones disciplinarias y legales necesarias. ▪ Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio. ▪ Realizar y/o supervisar pruebas de vulnerabilidad sobre los diferentes servicios tecnológicos para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información	Jefe Oficina de Planeación y Sistemas Gestión tecnológica
Táctico	▪ Brindar asesoría a los procesos de la Entidad en temas jurídicos y legales que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información. ▪ Brindar asesoría al Comité de seguridad, ciberseguridad, datos personales y continuidad de negocio, en materia de temas normativos, jurídicos y legales vigentes que involucren acciones ante las autoridades competentes ▪ Representar a la Entidad en procesos judiciales ante las autoridades competentes relacionados con seguridad y privacidad de la información, ▪ Apoyar y asesorar a los procesos en la clasificación de Información clasificada y reservada del catálogo de activos de Información, de acuerdo con la regulación vigente	Oficina Asesora Jurídica
Operativo	▪ Establecer los requerimientos mínimos de seguridad que deberán cumplir los sistemas de información a desarrollar, actualizar o adquirir. ▪ Apoyar la implementación segura de los sistemas de información, de acuerdo con la normatividad vigente, estándares, buenas prácticas, políticas sectoriales y lineamientos de la entidad. ▪ Desarrollar pruebas periódicas de vulnerabilidad sobre los diferentes sistemas de información para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información. ▪ Liderar el proceso de gestión de incidentes de seguridad, así como la posterior investigación de dichos eventos para determinar causas posibles responsables y recomendaciones de mejora para los sistemas afectados. ▪ Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio	Jefe Oficina de Planeación y Sistemas Gestión tecnológica

Nivel	Responsabilidades	Responsable
Operativo	▪ Revisión desde una instancia independiente a los procesos y demás grupos de interés, en intervalos planificados o cuando ocurran cambios significativos, que se garantice la confidencialidad, integridad y disponibilidad de la información a través de los distintos componentes implementados en el SGSI, así como el cumplimiento de las obligaciones legales y regulatorias relacionadas con la seguridad de la información	Oficina Asesora de Control Interno
Operativo	▪ Desarrollar el plan de formación y sensibilización de la entidad incorporando. ▪ Supervisar los resultados del plan de formación y sensibilización establecido, con el fin de identificar oportunidades de mejora. ▪ Participar en la elaboración de los planes de gestión de cambio, garantizando la inclusión del componente de seguridad de la información en la implementación de los proyectos de TI	Jefe Oficina de Planeación y Sistemas Gestión tecnológica
Operativo	▪ Asesorar la toma de decisiones en incidencias contractuales ▪ Verificar que los contratos o convenios, cuenten con cláusulas de derechos de autor, confidencialidad y no divulgación de la información según sea el caso. ▪ Controlar y salvaguardar la información de datos personales del personal de planta de la Entidad, en concordancia con la normatividad vigente. ▪ Realizar la gestión de vinculación, capacitación, desvinculación del personal de planta dando cumplimiento a los controles y normatividad vigente relacionada con seguridad y privacidad de la información.	Sub director administrativo y financiero Grupo de contratación Grupo de talento humano
Operativo	Adoptar estrategias para continuidad de negocio y desarrollarlas durante las pruebas respectivas	Lideres de proceso
Operativo	Adoptar o actualizar procedimientos, planes, manuales, formatos y demás documentación necesaria para llevar los controles al nivel operativo de los procesos	Lideres de proceso
Operativo	Activar o desactivar los accesos a los activos de información y servicios tecnológicos de acuerdo con las solicitudes del caso	Administradores de sistemas de información y operaciones tecnológicas
Operativo	Reportar a la unidad de riesgo operativo, los riesgos materializados, acciones sospechosas, incumplimiento de las políticas de este documento	Funcionarios, contratistas, terceros
Operativo	Revisar, documentar y orientar la identificación y el tratamiento de riesgos, de acuerdo con las políticas de gestión de riesgos y mapas de riesgos de los procesos	Coordinador de unidad de riesgo operativo URO
Operativo	Revisar la trazabilidad del uso y acciones de los sistemas de información Reportar a URO incidentes o no conformidades	Administradores de sistemas de información
Operativo	Revisar la trazabilidad del uso y acciones de los servicios tecnológicos Reportar a URO incidentes o no conformidades	Administradores de la operación tecnológica
Operativo	Autorizar el acceso o cambio de acceso a los servicios tecnológicos y activos de información, especificando el nivel requerido y la temporalidad y solicitarlo al área pertinente	Lideres de proceso
Operativo	Informar a los interesados la terminación de vínculos contractuales, visitas temporales de ejercicios de auditoría y otros, a fin de aplicar la finalización de accesos a servicios tecnológicos y activos de información	Coordinador del grupo de talento humano Coordinador del grupo de contratación
Operativo	Asegurar que los grupos de valor comprenden sus responsabilidades frente a la seguridad de la información de acuerdo con el rol que desempeñan Asegurar que los grupos de valor conocen y aplican las políticas de este documento	Coordinador del grupo de talento humano Jefe Oficina de Planeación y Sistemas
Operativo	Leer y aplicar las políticas de seguridad de la información en las labores que lo vinculan con la entidad	Funcionarios, contratistas, terceros, visitantes en tareas temporales

12.2 POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Fondo de Previsión Social del Congreso de la República, protege los activos de información de conformidad con los requisitos legales y reglamentarios vigentes mediante estándares, buenas prácticas, estrategias, planes, políticas y procedimientos, definidos, aprobados y socializados en los grupos de interés, adoptando controles apropiados de alcance organizacional, personal, físicos y tecnológicos con el fin de mitigar los riesgos operativos y de seguridad digital derivados de amenazas internas, externas, cibernéticas, conocidas y emergentes (cibercrimen,

ciberdelito, entre otras) que afecten la confidencialidad, integridad y disponibilidad de los activos.

12.3 POLÍTICA DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN:

Establece la instancia del gobierno corporativo en la que se tratan temas relativos a la seguridad de la información además de definir quiénes participan:

12.3.1 **Instancia de alto nivel**: Comité estratégico de seguridad de la información, dato personales, ciberseguridad y continuidad de negocio (Resolución 0662 del 25 de octubre de 2022), en la cual, se definen los participantes y su alcance.

12.3.2 Instancia a nivel de proceso:

1. Es responsabilidad de cada líder de proceso, propender por la adopción de planes, procedimientos, controles y demás mecanismos tendientes a la planeación, implementación y seguimiento de las políticas que aplican para el proceso.
2. Es responsabilidad de cada líder de proceso, definir de forma clara e inequívoca, así como auditar, la separación de deberes y responsabilidades, es decir, quiénes (funcionarios, contratistas,terceros, gestión de proyectos, etc.) tienen acceso para creación, alimentación, edición, consulta o custodia de la información ya seaque esta se encuentre en formato digital, papel u otro.
3. Reportar a las instancias internas de interés las acciones sospechosas o incidentes la seguridad, privacidad y ciberseguridad que impacten la confidencialidad, integridad y disponibilidad, de la información.

12.4 POLÍTICA DE SEGURIDAD DE LOS RECURSOS HUMANOS

Asegurar que los servidores y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran, desde los grupos de talento humano, contratación, jefes de proceso y supervisores de contratos:

12.4.1 Etapa de Selección:

1. Llevar a cabo las validaciones de antecedentes, y documentación aportada, acorde con la legislación, reglamentaciones y reglas de negocio.

2. Gestión y disposición final de documentos en cualquier formato, enlos casos en los que no se finaliza con una vinculación a la Entidad, acorde con la normatividad en materia de tratamiento de datos personales y demás reglamentación vigente.

12.4.2 Etapa de Vinculación:

1. Establecer de forma clara, dentro del contexto del acuerdo contractual, con

servidores, contratistas u otros terceros, las responsabilidades de las dos partes en cuanto a la seguridad, ciberseguridad y privacidad de la información, apoyándose para ello, en acuerdos de confidencialidad, normatividad vigente u otros instrumentos que se consideren dentro de la naturaleza de la información a la que se tendrá acceso.

2. El jefe del proceso o el supervisor del contrato deben definir los roles y permisos necesarios según el cargo, actividades y responsabilidades, partiendo de la premisa de asignar el menor privilegio. Estos roles y permisos deben solicitarse a los administradores de sistemas de información y operaciones tecnológicas y comunicarse a los interesados.
3. Gestión y disposición final de documentación contractual, en cualquier formato, acorde con la normatividad en materia de tratamiento de datos personales, gestión documental y demásreglamentación vigente.
4. Socializar las políticas de seguridad de la información.
5. Incluir firmado el acuerdo de confidencialidad del formato del anexo 1 de este documento
6. Incluir en los alcances y obligaciones contractuales, lo concerniente a derechos de autor y propiedad intelectual

12.4.3 Etapa de Ejecución del empleo o contrato:

1. Exigir la aplicación de las políticas de seguridad de la información, basándose en los planes, políticas y procedimientos establecidos por la Entidad.
2. Reportar a las instancias internas de interés (URO, Comité de gestión y desempeño institucional, instancia orientadora de la Gestión Tecnológica, Comité de seguridad, privacidad y ciberseguridad, entre otros) las novedades o incidentes con relación a la seguridad, privacidad y ciberseguridad que impacten la confidencialidad, integridad y disponibilidad, de la información.

12.4.4 Etapa de Terminación o cambio de responsabilidades del empleo o contrato:

1. Establecer de forma clara, comunicar y hacer cumplir los deberesde seguridad de la información que permanecen válidos despuésde la terminación o cambio de empleo al funcionario, contratista o tercero.
2. Informar a los procesos interesados a fin de que se tomen las medidas correctivas en cuanto al cambio o terminación de privilegios de acceso a sistemas de información o acceso a bodegas de custodia y demás controles de acceso. y generación de paz y salvos o informes en torno a los activos de información.

12.5 POLÍTICA DE GESTIÓN DE ACTIVOS Y DE INFORMACIÓN:

Identificar los activos de la Entidad y definir las responsabilidades de protección apropiadas:

12.5.1 **Identificación y actualización de activos:** En una frecuencia programada o cuando una situación lo amerite, la oficina asesora de planeación y sistemas

junto al grupo de archivo (Gestión documental) y calidad, coordinan la actualización del inventario de activos, paraconsolidar en el formato del caso y someter a revisión y aprobación delcomité de gestión y desempeño.
Esta identificación, debe abarcar: equipamiento auxiliar, hardware, información, instalaciones, procesos, recurso humano, red, servicios, software, entre otros que se consideren relevantes.

12.5.1.1 **Clasificación de Activos:** La clasificación de los activos debe realizarse de manera específica, en función de su categoría bien sea físico o digital, la criticidad, sensibilidad y reserva, las características de seguridad como confidencialidad, integridad y disponibilidad, si contiene o no datos personales, así como de las leyes y normatividades vigentes que afecten a la Entidad en materia de sensibilidad y reserva.

12.5.1.2 **Etiquetado de activos:** Los activos que así lo permitan como el hardware, deben ser etiquetados, de forma que facilite su control ygestión.

12.5.1.3 **Devolución de los Activos:** Las áreas de almacén, talento humano o contratación, deben establecer obligatoriedad de aplicación de formato de paz y salvo, para funcionarios, contratistas o terceros aefectos de entrega de activos físicos y de la información una vez finalizado el empleo, acuerdo o contrato.

12.5.1.4 **Disposición final de los activos:** Adoptar procedimiento medianteel cual se realice el análisis, documentación y toma de decisiones alineadas con buenas prácticas, normatividad medio ambiental, tablas de retención y demás estándares en gestión documental, entre otros, contemplando como mínimo: conceptos técnicos, borrado seguro, depreciación, eliminación, retiro, traslado o reutilización cuando los activos ya no se requieran mantener en operación.

a. **Copia de seguridad de activos:**

1. Adoptar procedimientos desde el alcance del área que gestionael activo de información, a fin de formalizar las tareas de copiasde seguridad, tanto para la información en físico (ejemplo: digitalización de hojas de vida o expedientes) como digital(ejemplo: copia de información del centro de datos).
2. Identificar estaciones de trabajo, cuya información se considererelevante y solicitar a la Oficina Asesora de Planeación y Sistemas, el agendamiento de copias de seguridad periódicas.
3. Agendar pruebas periódicas de restauración de copias de seguridad.

b. **Manejo de medios removibles:**

1. Implementar procedimientos para el control del uso de medios removibles.
2. Adopción de acuerdos de confidencialidad para protección contra acceso no autorizado, uso indebido o corrupción durante el transporte o almacenamiento en un tercero

c. **Auditoría y control de activos:**

1. Los sistemas de información deben incluir en su diseño y puesta enmarcha, gestión de logs para trazabilidad e identificar las acciones que realiza un funcionario, contratista o tercero sobre los activos de información como consulta, generación, procesamiento, borrado, edición, en donde se identifique acción realizada, estampilla de tiempo y el usuario o datos personales, entre otros y se deben conservar las evidencias de autorizaciones de acceso ya sea en formato digital o físico según aplique
2. Desde el área funcional y quienes tengan el rol de administradores de un determinado sistema de información, deben realizar auditoria a los logs de trazabilidad, en cuanto a usuarios activos e inactivos, acciones sospechosas, inusuales o no asignadas.
3. La información contenida en medio físico, debe ser objeto deauditoría, desde el alcance de los responsables de su custodia, en cuanto a la completitud del inventario, disponibilidad en préstamo o bodega, cumplimiento de protocolos de préstamo y consulta, cumplimiento de plazos para devolución, acciones en caso de pérdida de documentos en préstamo o custodia.
4. Los activos físicos (hardware) deben ser objeto de auditoría, en cuanto a verificación de estado, etiquetadoy responsable asociado.
5. Los sistemas de control de acceso, deben ser objeto de auditoría de logs, en cuanto a verificación de acceso no autorizado.

12.6 POLÍTICA DE CONTROL DE ACCESO

La Entidad determina en esta política, los mecanismos de protección, los límites y procedimientos frente a la administración y responsabilidad, relacionados con los accesos a la información, sin importar si estos accesosson digitales o físicos:

12.6.1 **Autorización, modificación y revocación de acceso:** Incluir en los procedimientos para control de acceso. según el alcance del área quegestiona el activo, a fin de establecer:

1. Quiénes y cómo solicitan asignación, modificación o de derechos y/o privilegios, roles y permisos sobre las credenciales de accesoa los activos de información y servicios de tecnología.
2. Quiénes y cómo solicitan revocación de derechos y/o privilegios, roles y permisos sobre las credenciales de acceso a los activos de información y servicios de tecnología.
3. Quiénes y cómo se autorizan credenciales de acceso con privilegios superiores (Super Usuarios) utilizados para la administración de infraestructura, centro de datos, aplicaciones, sistemas de información, bases de datos, entre otros.
4. Quiénes y cómo solicitan asignación, modificación, revisión orevocación de derechos y/o privilegios de acceso para activos de información disponible en formato físico

12.6.2 **Gestión de acceso:** Incluir en los procedimientos de control deacceso, según

el alcance del área que gestiona el activo, a fin de establecer:

1. Estándar de creación de credenciales de acceso. Para los casos de activos de información en formato físico, se debe adoptar un formato de control de acceso.
2. Cómo se hace entrega de las credenciales de acceso

12.6.3 Gestión de identidades

1. Controlar el ciclo completo de las identidades desde la creación, modificación y revocación.
2. Identificar las cuentas de usuarios con metadatos que permitan identificar la persona, el área o proceso, datos de contacto, inicio y cambios del ciclo de vida
3. Las credenciales de acceso son personales e intransferibles
4. Contraseñas con longitud y complejidad minina
5. Contraseñas con vencimiento periódico
6. Contraseñas para cambio obligatorio en el primer uso
7. Contraseñas de gestión de servicios de TI, con cambio periódico, usadas para configuraciones y acceso de la plataforma y servicios tecnológicos.
8. Contraseñas con cambio autónomo desde el alcance del usuario de servicios tecnológicos
9. Usuario con fecha de vencimiento para personas sujetas a vinculación por periodos de tiempo establecidos contractualmente.
10. Usuario sin vencimiento en el tiempo para funcionarios
11. Implementación de gestión de contraseñas cifradas, desde el diseño, desarrollo y puesta en marcha de soluciones tecnológicas

12.6.4 Control de acceso a redes, sistema y aplicaciones

1. El acceso a los canales de comunicación de redes locales por cable, inalámbricas e internet, así como a la información y la funcionalidad que posibilitan tanto el software como los sistemas de información, se sujetan a los lineamientos decontrol de acceso mediante credenciales de acceso seguro, con procedimientos de cifrado de contraseña y gestión centralizada de credenciales
2. Acceso restringido para personal autorizado por la oficina asesora de planeación y sistemas, al código fuente del software de aplicaciones, bases de datos, scripts y sus versiones derivadas en cualquier lenguaje o framework.
3. Acceso restringido para personal autorizado por la oficina asesora de planeación y sistemas, a los manuales técnicos de instalación y configuraciones de los servicios tecnológicos.
4. Uso de equipos personales, sujeto a autorización de la Oficina Asesora de Planeación y Sistemas, mediante formato descrito en el ANEXO 2 de este documento, para el cumplimiento de requisitos.
5. Los funcionarios, contratistas y terceros no podrán almacenar información reservada en ningún dispositivo de almacenamiento personal, sin la mediación de una autorización del nivel directivo pertinente.

6. Acceso remoto seguro vía VPN, sujeto a autorización del nivel apropiado y cumplimiento de requisitos mínimos de seguridad en el equipo remoto.

12.6.5 Teletrabajo o trabajo en casa

Las tareas de teletrabajo o trabajo en casa se realizan alineados a losacuerdos de confidencialidad, y el cumplimiento de requisitos mínimosde seguridad tales como el uso de redes seguras VPN, antivirus y software con soporte del fabricante y los demás documentados en el procedimiento de atención de incidentes – mesa de ayuda.

12.7 POLÍTICA DE CRIPTOGRAFÍA: Asegurar el uso apropiado de los procedimientos para los cuales se requiere token criptográfico para proteger el procesamiento y resultados esperados:

1. Los procesos que desarrollan tareas relativas a plataformas tanto públicas como privadas (SIIF, transmisión de información a la Superintendencia Financiera de Colombia, transmisión de informaciónal Ministerio de Salud a través de la plataforma SISPRO, establecimientos financieros, etc.), deben adoptar procedimientos que documenten las actividades de: solicitud, asignación, revocación, renovación, instalación, devolución, mesas de ayuda, tiempo de vida,renovación de credenciales, con relación al token criptográfico requerido.
2. Recomendar el uso personal e intransferible del token criptográfico, así como de las credenciales de uso, desde el alcance del líder del proceso.

12.8 POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO

12.8.1 **Perímetros de Seguridad:** Perímetros físicos de seguridad donde se encuentra información crítica, sensible o se realice almacenamiento y/o procesamiento de información:

12.8.2 Sede de la Entidad, Pisos 2 y 3 del Edificio World Service

a. El coordinador del grupo de talento humano coordina con la administración del edificio, la asignación o retiro de credenciales de acceso biométrico para funcionarios y contratistas.
b. El coordinador del grupo de talento humano autoriza la asignación o retiro de acceso biométrico a los pisos que ocupa la Entidad
c. Tienen acceso servidores y contratistas y se controla mediante sistemas biométricos y credenciales distintivas dela Entidad.
d. Tienen acceso los terceros, quienes requieren autorizacióndel nivel jerárquico del caso, restringido al alcance de las labores específicas.

12.8.3 Bodega de archivo en la sede

Tienen acceso el director general, Sub directores y gestores de archivo
Los demás requieren autorización del nivel jerárquico del caso, restringido al alcance del acceso otorgado

12.8.4 Bodega de archivo externa

Tienen acceso el director general, subdirectores y gestores de archivo

Los demás requieren autorización del nivel jerárquico del caso, restringido al alcance del acceso otorgado

12.8.5 Centro de datos

Tienen acceso el director general, el jefe de la Oficina Asesora de Planeación y Sistemas, los funcionarios y contratistas en cuyo alcance de sus funciones o contrato incluya gestión y administración de infraestructura o plataforma tecnológica contenida en el centro de datos.

El jefe de la Oficina Asesora de Planeación y Sistemas autoriza la asignación, traslado o retiro de credenciales de acceso (tarjeta de proximidad y acceso biométrico)

Los demás requieren autorización del jefe de la oficina de Planeación y Sistemas, restringido al alcance del acceso otorgado, además de registro en bitácora de ingreso.

12.8.6 Seguridad de oficinas:

Mantener la continuidad en la presencia de personal devigilancia
Control de acceso no autorizado mediante personal devigilancia
Mantener activos los controles de acceso biométrico
Continuidad en la operación de video cámaras de vigilancia en un horario 7x24

12.8.7 Protección contra amenazas externas y ambientales:

Los espacios para centralizar expedientes físicos son cerrados, con control de acceso y condiciones mínimas de temperatura.

El espacio destinado al centro de datos es cerrado, protegido con cerradura y control de acceso biométrico exclusivo, con condiciones mínimas de energía y temperatura.

12.9 POLÍTICA DE GESTIÓN DE EQUIPOS: Prevenir la pérdida, daño, robo o compromisos de activos, y la interrupción de las operaciones de la entidad, en este sentido, los equipos se usan y gestionan mediante las siguientes directrices:

a. Control físico de inventario de equipos tecnológicos y puestos de trabajo, mediante placa de código de barras y asignación de responsable.
b. Control lógico de inventario de equipos tecnológicos, mediante software de propósito, con actualización en tiempo real en variables de software instalado, versiones, logs, usuarios conectados, especificaciones, configuraciones, entre otros.
c. Los computadores se ubican en puestos de trabajo conectados a la red eléctrica regulada
d. La red eléctrica regulada y la red local de comunicaciones LAN, se protege mediante canaleta desde el centro de cableado hasta el puesto de trabajo, para evitar conexiones y derivaciones noautorizadas, interferencias o daños.

e. El mantenimiento de hardware y software, reubicación de los equipos, o instalación de software en el punto final del usuario, lo realiza personal autorizado de la Oficina Asesora de Planeación y Sistemas, en atención a solicitudes especificas con las autorizaciones del caso o de forma proactiva mediante actividades preventivas, a través de su proceso de Gestión Tecnológica, asegurando siempre la conservación de la información y configuraciones del caso.

f. El retiro de equipos de la sede con el software e información del casorequiere autorización del nivel apropiado.

g. La disposición final o reutilización debe realizarse previo retiro de la información para conservación o reubicación, ya sea por retiro de los medios de almacenamiento o borrado seguro de los mismos mediantesobre escritura, así como del concepto técnico de gestión tecnológica que realiza la actividad y en coordinación con almacén, bienes y servicios para el traslado del activo a almacén.

h. El puesto de trabajo debe mantenerse libre de equipos y dispositivos no autorizados tales como medios removibles

i. Los equipos como tokens criptográficos, o documentos de trabajo deben mantenerse bajo protección, mientras no se estén usando.

j. El escritorio de los sistemas operativos del centro de datos y del punto final del usuario, debe permanecer limpio de documentación confidencial.

k. Las personas externas a FONPRECON que ingresen equipos personales, deben registrarlos en la planilla de ingreso y retiro de elementos provista por la empresa de seguridad. La seguridad de los elementos ingresados es responsabilidad del propietario del equipo.

l. Los equipos del centro de datos se disponen, organizan y documentan en gabinetes organizados según los roles de los equipos de comunicación, servidores, cableado, potencia, aire, servicios de voz, monitoreo, entre otros.

m. Las impresoras se controlan mediante clave de acceso personalizada para todas las funcionalidades.

n. Los usuarios de las impresoras se obligan a no dejar material en periféricos como impresora, escáner, entre otros, que pueda poner en riesgo información catalogada en algún grado de confidencialidad, datos personales o privilegiada.

12.10 POLÍTICA DE SEGURIDAD DE LAS OPERACIONES: Asegurar las operaciones correctas y seguras:

a. **Procedimientos de operación del centro de datos:** Documentar, proteger y otorgar acceso al personal autorizado, los procedimientos de gestión y administración del centro de datos, integrando red eléctrica, gabinetes, redes de comunicación, direccionamiento IP, versiones de sistemas operativos, vigencia de garantía, credenciales de acceso, modo de operación en físico y virtual, esquemas de copias de seguridad, aire acondicionado,

configuraciones entre otros catálogos necesarios.

b. **Gestión de cambios:** Controlar los cambios a nivel de hardware, software e instalaciones, integrando en la documentación, evidencias de pruebas, controles, objetos o componentes afectados, actas de pasoa producción con las aprobaciones del caso.

c. **Gestión de la capacidad:** Control de los recursos de almacenamiento, procesamiento, comunicación y demás aspectos que se consideren relevantes, mediante procedimiento que permita el seguimientoperiódico al uso, proyección de crecimiento requerido y generación de informe para análisis y toma de decisiones.

d. **Separación de ambientes:** La gestión de cambios, debe soportarse enuna separación de ambiente de pruebas, desarrollo y producción.

e. **Protección contra código malicioso:**
   1. Implementar la instalación, monitoreo y actualización permanente de las soluciones de seguridad a nivel de equipos de punto final de usuarios, centro de datos y seguridad de borde.
   2. Implementar protección y actualización permanente en el borde de la red, con una solución de propósito específico tipo appliance UTM con controles automatizados para malware, detección y prevención de intrusos, amenazas persistentes, geolocalización, filtrado web, control de aplicaciones, entre otros que puedan ser necesarios.
   3. Monitorear el estado y la trazabilidad de las soluciones de seguridad.
   4. Mantener vigente la asistencia técnica del proveedor especializado en estas soluciones.
   5. Brindar capacitación y sensibilización en esta materia al interior de la Entidad

f. **Copias de respaldo:**
   1. Ejecutar y actualizar el plan de copias de seguridad
   2. Realizar copias de la información, software y configuraciones de los activos de información.
   3. Realizar pruebas mensuales de restauración, con su respectivo informe, con alcance de copias de cintas en custodia y copias de almacenamiento local.
   4. Alcance de copias de respaldo para activos de información del centro de datos, información de las estaciones de trabajo para directivos, coordinadores y de equipos que cada proceso haya identificado como relevantes.
   5. Almacenamiento y conservación extendida de copias en cintas magnéticas con custodia externa.
   6. Conservación de copias de conservación en los medios de almacenamiento de la solución de copias de seguridad, por periodos cortos de tiempo.

g. **Gestión de logs – evidencias:** El responsable de la administración de un

sistema de información o de las operaciones tecnológicas, debe realizar gestión de logs, en cuanto a:

1. Conservar y revisar periódicamente los registros de actividades de usuarios, fallas o eventos de seguridad.
2. Estos registros o logs deben estar protegidos contra acceso no autorizado.
3. Informar acciones sospechosas, fallas o advertencias a la unidad de riesgo operativo o gestión tecnológica

h. **Sincronización de relojes:** Los sistemas de información, equipos centro de datos y estaciones de trabajo, sincronizan con los servidores de hora legal en Colombia de la entidad inm.gov.co en redundancia en servidores org de la zona horaria para Colombia, como fuente de referencia de tiempo, mediante recursos de red conocidos como controladores de dominio y reglas de control de salida a internet en la seguridad de borde.

i. **Usuarios restringidos:** Los usuarios de red en los equipos de punto final de usuarios, son usuarios restringidos con el menor privilegio, sin permisos administrativos, que les impide instalar, desinstalar software o alterar las configuraciones. Los accesos para otros servicios tecnológicos también se otorgan con el menor privilegio posible.

j. **Análisis de vulnerabilidades:** La oficina asesora de planeación y sistemas a través de su proceso de Gestión Tecnológica realiza análisis de vulnerabilidades sobre los activos de información a fin de obtener las oportunidades de mejora e implementar los correctivos del caso, así como el trámite de los correctivos que requieren inversión.

k. **Ventanas de mantenimiento:** Requiere autorización de la dirección general y de procesos misionales, así como alinearse a los procedimientos de control de cambios y paso a producción, pruebas satisfactorias en ambientes separados para tales fines y acordarse en horarios no laborales, así como informar del impacto y recomendaciones a los grupos de interés.

l. La oficina de planeación y sistemas mantiene vigentes la contratación de servicios especializados para la gestión de seguridad, ciberseguridad y continuidad de negocio.

12.11 POLÍTICA DE SEGURIDAD EN LAS COMUNICACIONES: Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información:

1. Separar las redes en subredes para el centro de datos, estaciones de trabajo, internet, VPN, WIFI y DMZ
2. Definir una zona desmilitarizada DMZ, donde operan los servicios que se publican directamente en internet como el sitio web, entre otros.
3. El acceso a las redes locales e internet se hace mediante las credenciales de acceso otorgadas a cada persona, con restricciones según perfil y roles asignados en el directorio activo.
4. La red WIFI gratis para la gente es un portal cautivo, no usa credenciales y su

uso es responsabilidad del visitante. Su disponibilidad e instrucciones se informan de manera visible en el área de atención al usuario.

5. Realizar monitoreo permanente de la disponibilidad de las redes.
6. Red de internet con redundancia ante fallos mediante dos canales con proveedor diferente que a su vez el servicio de cada proveedor tiene características de redundancia.

12.12 POLÍTICA DE TRANSFERENCIA DE INFORMACIÓN: Mantener la seguridad de la información transferida dentro de Fonprecon y con cualquier Entidad externa:

1. Desde el alcance de cada proceso, adoptar procedimientos para que la transferencia de información se haga en un marco de formalidad con los acuerdos de confidencialidad generales y específicos según el caso y estableciendo los mecanismos de transferencia.
2. Proteger los tokens físicos y digitales asignados para transmitir información financiera, enviar información a órganos de control y vigilancia, firmar documentos
3. Adoptar las medidas necesarias a fin de que la tercerización o uso de tecnologías de nube fuera del país, cuenten con legislación vigente encuanto a seguridad y privacidad de la información
4. Para enviar información que por su tamaño no es posible adjuntar en un correo electrónico, hacer uso de los recursos disponibles para este propósito dentro de la solución y licencia de ofimática asignada al funcionario.
5. Las comunicaciones electrónicas oficiales de la entidad se realizan mediante el uso de las cuentas de correo corporativo con el dominio @fonprecon.gov.co, desde el alcance del jefe del proceso o su delegado previamente autorizado.
6. No utilice los canales de comunicación de la entidad como el correo electrónico corporativo, mensajes de texto, líneas de whatsapp, redes sociales y líneas telefónicas, para transmitir, gestionar o promover información de interés personal o actividades distintas a la misionalidad de la entidad u objetivos del proceso o contrato mediante el cual se encuentra vinculado.

12.13 POLÍTICA PARA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS: Asegurar que la seguridad sea parte integral de los sistemas de información durante todo su ciclo de vida:

12.13.1 **Análisis y requisitos de seguridad de la información:** Consideraciones transversales de seguridad, ciberseguridad y datos personales para la contratación, diseño e implementación de nuevas soluciones o mejoras sobres activos de información:

a. No quemar direcciones IP en el código, en cambio ha de usarselos nombres completos o FQDN de los sistemas queintervienen.

b. Incluir el registro de logs e interface de consulta y gestión de estos para el administrador del sistema de información.
c. Autenticación con usuario y contraseña donde la contraseña debe estar cifrada
d. Interface de cambio de contraseña desde la gestión del dueño de las credenciales
e. Longitud mínima y complejidad de contraseña
f. Desactivación automática de usuarios por tiempo prolongadode inactividad
g. Cerrar sesión automáticamente luego de 10 minutos deinactividad
h. Cifrado de la información en transporte
i. Certificado para IPv6 en convivencia con IPv4
j. Análisis de vulnerabilidades y penetración reiterativos en la fasede pruebas y producción, con aplicación de mejoras hasta que ya no sean evidentes.
k. Las demás consideraciones que se incluyen en los procedimientos para gestión de proveedores en tecnología y metodología para el desarrollo y mantenimiento de software

12.13.2 Desarrollo seguro:

a. Hacer uso del ambiente de pruebas y desarrollo antes de pasara producción
b. El ambiente de pruebas y desarrollo debe operar en una red diferente a la de producción, haciendo uso de redes internas en el caso de plataformas virtuales.
c. Mantener control del código fuente y versiones del desarrollo, con acceso restringido para el personal autorizado
d. Las pruebas deben contemplar tanto la funcionalidad como la seguridad dentro de un marco establecido de criterios de aceptación de resultados
e. Los datos generados en el ambiente de pruebas deben ser protegidos y borrados cuando la solución ha sido pasada a producción
f. Las demás consideraciones que se incluyen en los procedimientos para gestión de proveedores en tecnología y metodología para el desarrollo y mantenimiento de software

12.14 POLÍTICA PARA RELACIONES CON LOS PROVEEDORES: Asegurar la protección de los activos de Fonprecon que sean accesibles a los proveedores:

a. Incluir el acuerdo de confidencialidad del anexo 1 de este documento, como parte integral de la contratación, que incluye un marco: legal y reglamentario, privacidad, ciberseguridad y protección de datos, requisitos de tratamiento de los activos al finalizar el objeto contractual, en los casos en que estos hayan sido alojados en la sede del proveedor, firmas de las partes, extensible aún después de terminada la vinculación, autonomía de Fonprecon para auditabilidad sobre el cumplimiento.
b. Establecer la formalidad de las comunicaciones, incluso para reportar anomalías o actividad sospechosa sobre el activo o servicio.

c. Tratamiento de riesgos: Dentro del marco contractual, integrar requisitos para el acceso, procesamiento, almacenamiento e intercambio de información. Especificar dentro del marco contractual, los riesgos asociados a la entrega, gestión o intervención de activos por parte del proveedor, acordando la forma de tratamiento.
d. Establecer los requisititos mínimos de seguimiento, revisión, auditoria, identificaciónde hitos con sus fechas y periodicidad del seguimiento.
e. Según la magnitud del servicio o proyecto, adoptar indicadores que permitan la medición de alcance de los hitos.
f. Adoptar los lineamientos de gestión de cambios de los activos, teniendo en cuenta la criticidad de la información, activos asociados y procesos involucrados como resultado de los servicios de los proveedores.
g. Gestión de mejora continua de la documentación derivada de proyectos, servicios, nuevos activos o mejoras, tales como políticas, planes, procedimientos, riesgos y controles de seguridad entre otros
h. La adquisición de bienes y servicios se realiza de conformidad con los lineamientos para la contratación del Estado colombiano, acuerdos marco de precios, normatividad vigente en materia de derechos de autor y propiedad intelectual y conforme a las condiciones y acuerdos de niveles de servicio dentro del marco de contratación con un tercero, además de los lineamientos y directrices corporativas definidos en la Entidad.
i. El marco contractual debe integrar el alcance pertinente para derechos de licenciamiento, protección de derechos de autor y propiedad intelectual sobre el conocimiento y productos generados en la entidad, así como de los productos adquiridos.

12.15 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DE NEGOCIO: Gestión de la continuidad de negocio dentro del marco de la seguridad y ciberseguridad de la información.

a. El líder de cada proceso identifica y documenta las estrategias para operar en contingencia ante los diferentes escenarios adversos identificados y documentados.
b. La oficina de planeación y sistemas coordina las pruebas periódicas a desarrollar desde el alcance de los procesos para el plan de continuidad de negocio al menos una vez en cada vigencia.
c. La oficina de planeación y sistemas coordina las pruebas de recuperación de desastres tecnológicos a través del proceso de gestión tecnológica.
d. La oficina de planeación y sistemas consolida las oportunidades de mejora de las pruebas de continuidad de negocio y recuperación de desastres tecnológicos para presentarlos en el comité estratégico de seguridad de la información.
e. La alta dirección examina y aprueba las oportunidades de mejora que considere pertinentes para las estrategias de continuidad de negocio y recuperación de desastres tecnológicos, asignando los recursos humanos, técnicos,

tecnológicos, logísticos y financieros para su implementación.

12.16 POLÍTICA DE REDUNDANCIAS: Asegurar la disponibilidad de instalaciones de procesamiento de información:

a. La oficina de planeación y sistemas a través del proceso de gestión tecnológica, implementa las redundancias requeridas para asegurar la disponibilidad de las operaciones de conformidad con las decisiones y aprobaciones de la alta dirección, a nivel de servicios de canales de internet, infraestructura tecnológica y condiciones de operación del centro de datos
b. La oficina de planeación y sistemas a través del proceso de gestión tecnológica documenta las configuraciones de las redundancias aplicadas y las protege con acceso restringido a personal autorizado.
c. La oficina de planeación y sistemas mantiene vigentes los contratos de gestión, administración, mantenimiento, soporte y suministro para los activos de información.

12.17 POLÍTICA DE CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES:

Incluir en el marco contractual, las obligaciones legales, estatutarias, de reglamentación o relacionadas con seguridad de la información, derechos de propiedad intelectual, protección de registros, privacidad y protección de datos personales, reglamentación de controles criptográficos.

12.18 POLÍTICA DE EVALUACIÓN Y TRATAMIENTO DE RIESGOS

La oficina asesora de planeación y sistemas a través de la unidad de riesgo realiza la gestión de riesgos en el siguiente alcance:

1. Establecer metodología, principios y directrices para la gestión de riesgos que realizan los procesos (identificación de activos, riesgos, diseño e implementación de controles, tratamiento de riesgos, monitoreo, reporte de incidencias).
2. Abordar temáticas de riesgos operativos, riesgos de corrupción, riesgos digitales y ciberseguridad, riesgos financieros.
3. Adoptar y formalizar la metodología alineada con los objetivos de la entidad, directrices de la función pública, organismos de vigilancia y control, normatividad vigente, MIPG, estándares nacionales e internacionales.
4. Desarrollar en una frecuencia planeada o cuándo una situación lo amerite, el comité estratégico de riesgos, revisión y mejora continua.
5. Educar y sensibilizar en la gestión de riesgos a funcionarios y contratistas.
6. Monitoreo, seguimiento, documentación y orientación a los procesos para el tratamiento de riesgos materializados.
7. Gestiona y orienta en el uso del sistema de información para reporte de riesgos.
8. La Oficina asesora de planeación y sistemas dispone una herramienta de software para el reporte de riesgos materializados y no conformidades.

9. todos los funcionarios, contratistas y terceros están obligados a reportar cualquier anomalía o actividad sospechosa en los sistemas o servicios de tecnología, así como la materialización de riesgos a través de la herramienta tecnológica dispuesta para tal finalidad o mediante correo electrónico dirigido a la unidad de riesgo operativo URO y la oficina de planeación y sistemas y líder de su proceso.
10. La oficina de planeación y sistemas a través de su proceso de gestión tecnológica lidera la documentación, toma de evidencia, respuesta, contención y recuperación a incidentes tecnológicos
11. La oficina de planeación y sistemas a través de la unidad de riesgo operativo URO, coordina el reporte de incidentes a organismos de control y vigilancia pertinentes
12. La oficina de planeación y sistemas lidera la puesta en marcha del procedimiento de gestión de crisis ante un escenario adverso que afecte la normalidad de la operación
13. Mantener actualizado el catálogo de contacto con autoridades, organismos de control y vigilancia, grupos especializados en respuesta a incidentes CSIRT.

12.19 POLÍTICA DE GESTIÓN DE LA SEGURIDAD EN EL CIBERESPACIO

La oficina asesora de planeación y sistemas planea y ejecuta a través de su proceso de gestión tecnológica, la adopción, gestión y mantenimiento de los controles para visibilidad y control de amenazas cibernéticas, tales como:

1. Detección, identificación y control de intrusos
2. Geolocalización
3. Ataques persistentes
4. Controles para amenazas conocidas (phishing, botnet, ransomware, spyware)
5. Rastreo de la internet profunda (Deep web) o redes oscuras (Dark web) en busca de información comprometida de la entidad en estas zonas del cibercrimen y ciberdelito.
6. Rastreo de compromiso de credenciales de acceso en servicios de internet.
7. Correlación de eventos de diferentes activos para inteligencia de amenazas.
8. Los administradores de las soluciones de seguridad de borde y equipos de punto final de usuarios mantienen activos y actualizados el software de protección contra amenazas.
9. Dimensionar y documentar los controles requeridos para servicios en la nube desde el alcance del proveedor y de los usuarios del servicio
10. Los administradores de las operaciones tecnológicas mantienen los activos tecnológicos en los niveles de versiones y actualización adecuados y más recientes disponibles por el fabricante.

13 FORMATOS Y ANEXOS

1. Anexo 1 acuerdo de confidencialidad: A01- POL-DEI-005

2. Anexo 2 formato **de autorización de conexión de equipos personales a las redes de comunicación de la entidad de forma temporal o permanente, local o remota**: A02- POL-DEI-005