A) HISTORIAL DE CAMBIOS

VERSIÓN	FECHA	JUSTIFICACIÓN DE LA MODIFICACIÓN
1	Septiembre2009	Lanzamiento del documento Políticas de TecnologíaInformática.
2	Junio 2010	Actualización del documento de Políticas.
3	9 de mayo de2019	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

B) REVISIONES Y APROBACIONES DEL DOCUMENTO

ELABORÓ	REVISÓ	APROBÓ
Nombre: Jesus Goyes Alvarado	Nombre: German Correa Amado	Nombre: Francisco Álvaro Ramírez Rivera
Cargo: Contratista Asesor Tecnologías de la Información.	Cargo: jefe Oficina Asesora de Planeación y Sistemas	Cargo: Director General
Fecha: 06/03/2023	Fecha: 15/03/2023	Fecha: 16/03/2023

REVISÓ	REVISÓ	REVISÓ
Nombre: Oscar Herrera Isaza	Nombre: Carolina Tobar Sierra	Nombre: Andrea del Pilar León Rodriguez
Cargo: Contratista Asesor Sistemas de Gestión	Cargo: Profesional Especializado Oficina Asesora de Planeación y Sistemas	Cargo: Profesional Especializado URO
Fecha: 14/03/2023	Fecha: 13/03/2023	Fecha: 08/03/2023

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	Subdirectora de Prestaciones Económicas
5	Subdirectora Administrativa y Financiera
6	Asesor de Control Interno

7	Coordinador Grupo 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 de Bienes y Servicios
13	Coordinadora Grupo Gestión Contable
14	Coordinadora Grupo de Tesorería
15	Profesional Unidad de Riesgo Operativo
16	Profesional de Gestión Tecnológica

Contenido

1. OBJETIVOS GENERALES.

- Fortalecer el componente de seguridad y privacidad de la información y contar con políticas que guíen el comportamiento personal y profesional de los funcionarios, contratistas y terceros sobre la información obtenida, generada o procesada por la entidad

- Permitir que la entidad trabaje bajo las mejores prácticas de seguridad y privacidad de la información, para que se cumplan los requisitos legales a los cuales está obligada, de conformidad con la misión institucional.

2. OBJETIVOS ESPECIFICOS.

- Minimizar el riesgo de los procesos misionales de la entidad

- Cumplir los principios de seguridad de la información

- Cumplir los principios de la función administrativa.

- Mantener la confianza de los funcionarios, contratistas y terceros

- Implementar el sistema de gestión de seguridad de la información - SGSI.

- Proteger los activos de información de la Entidad

- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.

- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, y usuarios de FONPRECON.

- Garantizar la continuidad del negocio frente a incidentes relacionados con la seguridad y privacidad de la información.

3. ALCANCE.

Para FONPRECON, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática, con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la información, acorde con las necesidades de los diferentes grupos de interés identificados.

El impacto de esta política aplica en una dinámica donde son partícipes sus funcionarios, contratistas, proveedores y la ciudadanía, basado en los siguientes principios:

- Las **responsabilidades** frente a la seguridad de la información serán aceptadas por cada uno de **los servidores, proveedores, o terceros**.
- FONPRECON **protegerá la información** generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos, frente al riesgo que se genera de los accesos **otorgados a terceros** (ej.: proveedores, afiliados, pensionados), o como resultado de la contratación de servicios de outsourcing.
- FONPRECON **protegerá la información** creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales por el **uso incorrecto** de esa información. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- FONPRECON **protegerá la información,** frente a las amenazas originadas por parte **del personal**.
- FONPRECON **protegerá las instalaciones** de procesamiento y la infraestructura tecnológica **que soporta sus procesos críticos**.
- FONPRECON **controlará la operación** de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- FONPRECON **implementará control de acceso** a la información, sistemas y recursos de red.
- FONPRECON garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- FONPRECON garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

- FONPRECON garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación.
- FONPRECON garantizará dentro del marco de cumplimiento las políticas, **obligaciones legales y regulatorias establecidas, en materia de seguridad de la información en el contexto del territorio Colombiano.**

4. APLICABILIDAD.

Esta política aplica a toda la entidad, servidores, contratistas y terceros de FONPRECON.

5. NIVEL DE CUMPLIMIENTO.

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento a la totalidad de la presente política.

El incumplimiento a la política de Seguridad y Privacidad de la Información traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

6. DEFINICIONES.

6.1 DEFINICIONES GENERALES DE LAS POLÍTICAS.

- **Política General de seguridad y privacidad de la información:** Documento de alto nivel que incluye la voluntad de la Alta Dirección de la Entidad para apoyar la implementación del Modelo de Seguridad y Privacidad de la Información. La política debe contener una declaración general por parte de la administración, donde se especifique sus objetivos, alcance, nivel de cumplimiento. La política debe ser aprobada y divulgada en la entidad.

- **Políticas específicas de Seguridad y Privacidad de la Información:** Manual de políticas, donde se describen los objetivos, alcances y el nivel de cumplimiento, que garanticen el adecuado uso de los Activos de información en la Entidad, definiendo las responsabilidades generales y específicas para la gestión de la seguridad de la información. En el manual de políticas de la entidad, se deben explicar de manera general, las políticas, los principios de seguridad y la normatividad pertinente. La entidad debe evaluar los requerimientos necesarios para ser ajustados o desarrollados en la elaboración de las políticas de seguridad y privacidad, así como en su implementación.

- **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. Para desarrollar esta actividad, la Guía No 3 de adopción del modelo MSPI, describe los procedimientos mínimos que se deberían tener en cuenta para la gestión de la seguridad al interior de la entidad.

6.2 DEFINICIONES DENTRO DE UNA CLASIFICACIÓN DE ACTIVOS.

- **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, es decir dentro de una organización se han de considerar todos los tipos de activos de información.
Fuente:http://www.mintic.gov.co/gestionti/615/articles5482_Guia_Seguridad_informacion_Mypimes.pdf

- **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, códigos ejecutables, datos de prueba).

- **Instalaciones:** Los lugares donde se hospedan los sistemas de información y comunicaciones (ejemplos: edificios, cuartos, vehículos, instalaciones de respaldo).

- **Otros:** Aquellos activos que no encajen en los tipos definidos.

- **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 muy significativa el cumplimiento de la misión de la entidad, procesos que son necesarios 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, Jefe TI, 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 de los 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).

6.3 DEFINICIONES EN CUANTO A LOS PILARES DE LA SEGURIDAD Y PRIVACIDAD.

- **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 encontrarse en diferentes medios o formas, y no solo en medios informáticos.
Fuente:http://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

- **Ciberseguridad:** Según el Conpes 3701 es la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

  Según ISACA (Information Systems Audit and Control Association) "es la protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información digital que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados".

- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos de información. [NTC 5411-1:2006].
  Fuente:http://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

- **Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada. [NTC 5411-1:2006].
  Fuente: http://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

- **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos entidades o procesos no autorizados. [NTC5411- 1:2006].
  Fuente: http://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

- **Vulnerabilidad:** Es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad de los sistemas. Las vulnerabilidades pueden hacer lo siguiente:
  - Permitir que un atacante ejecute comandos como otro usuario
  - Permitir a un atacante acceso a los datos, lo que se opone a las restricciones específicas de acceso a los datos
  - Permitir a un atacante hacerse pasar por otra entidad
  - Permitir a un atacante realizar una negación de servicio.

Fuente:http://www.mintic.gov.co/gestionti/615/articles5482_Guia_Seguridad_informacion_Mypimes.pdf

- **Ambiente de Pruebas**: Escenario con componentes tecnológicos de diferente marca y propósito, separado 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:** Escenario separado del ambiente de pruebas, donde interactúan componentes tecnológicos de diferente marca y propósito, que soportan los distintos servicios tecnológicos e información que se encuentra en operación y uso.

7. MARCO DE REFERENCIA

- **Circular Externa SFC 052 de 2007.** Por la cual la Superintendencia Financiera de Colombia incrementa los estándares de seguridad y calidad para el manejo de la información a través de medios y canales de distribución de productos y servicios que ofrecen a sus clientes y usuarios las entidades vigiladas por esta Entidad.
- **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. (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 información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre 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 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 1078 de 2015**. Por el cual se expide el Decreto único reglamentario del Sector de las Tecnologías de la información y las Telecomunicaciones.
- **CONPES 3854 de 2016.** Política Nacional de Seguridad Digital
- **Circular Externa 007 de 2018, expedida por la Superintendencia Financiera de Colombia**: Imparte instrucciones relacionadas con los requerimientos mínimos para la gestión del riesgo de ciberseguridad.
- **Decreto 1008 de 2018** por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 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 la ciberseguridad
- **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 de seguridad 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:** versión 4 de octubre de 2018 Departamento Administrativo de la Función Pública, riesgos de gestión, corrupción y seguridad digital.

8. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Mediante esta declaración general denominada Política de Seguridad y Privacidad de la Información, se establece la posición de la administración del FONDO DE PREVISIÓN SOCIAL DEL CONGRESO DE LA REPÚBLICA, en adelante FONPRECON, con respecto a la protección de los activos de información (la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

En este sentido, a continuación, se establecen 13 políticas generales de seguridad que soportan el SGSI de FONPRECON:

1. FONPRECON ha decidido **definir, implementar, operar y mejorar** de forma continua un Sistema de Gestión de Seguridad de la Información SGSI, derivado de la adopción del modelo de seguridad y privacidad de la información MSPI del MINTIC, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.

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

3. FONPRECON mantendrá actualizado el inventario de activos, como uno de los insumos fundamentales a la hora de identificar riesgos y diseño de controles.

4. FONPRECON protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de su actividad institucional.

5. 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 acuerdo con la clasificación de la información de su propiedad o en custodia.

6. FONPRECON protegerá su información de las amenazas originadas por parte del personal que intervenga en su administración, manejo o custodia.

7. FONPRECON protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

8. FONPRECON controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

9. FONPRECON implementará mecanismos de control de acceso a la información, sistemas y recursos de red.

10. 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 físico clasificada dentro del inventario de activos.

11. FONPRECON ejecutará una mejora efectiva de su modelo de seguridad, para enfrentar, mitigar o eliminar las debilidades asociadas con los sistemas de información.

12. FONPRECON garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en la identificación de riesgos, aplicación de controles y en el impacto que pueden generar los eventos.

13. FONPRECON garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales vigentes en materia de seguridad y privacidad de la información.

ANEXO 1. MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Objetivo:
Delimitar las políticas en cuanto a sus objetivos, alcances y nivel de cumplimiento, acorde con lo sugerido en la norma ISO 27001, para un adecuado uso de los activos de información al interior de la Entidad; definiendo las responsabilidades generales y específicas para la gestión de la seguridad de la información.

1. **ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN:**
   Establecer la instancia del gobierno corporativo en la que se tratan temas relativos a la seguridad de la información además de definir quiénes participan:

   a. **Instancia de alto nivel**: Comité de Gestión y Desempeño Institucional, instancia orientadora de la Gestión Tecnológica en FONPRECON (artículo primero de la Resolución 395 de 2019)
   b. **Frecuencia:** mínimo cuatro (4) veces al año y de forma extraordinaria las veces que el presidente del Comité lo considere conveniente.
      a. **Participantes:** Dirección General, Jefes Oficinas Asesoras, Subdirectores, Coordinadores, Unidad de Riesgo Operativo - URO, Gerente de Calidad.
      b. Alcance:
         i. Analizar el diagnóstico del estado de la seguridad de la información en FONPRECON, en cuanto a planes, políticas, procedimientos, mapas de riesgos y formular las recomendaciones que considere pertinentes.
         ii. Analizar viabilidad de adopción e implementación de directrices, políticas o recomendaciones gubernamentales, sectoriales y globales en materia de seguridad digital, seguridad de la información y ciberseguridad.
         iii. Revisar, analizar y recomendar acciones frente a eventos relacionados con ciberseguridad, es decir, tratar los casos de riesgos materializados relacionados con seguridad, privacidad o ciberseguridad

iv. Revisar y aprobar políticas en materia de seguridad, privacidad y ciberseguridad.
v. Revisar y establecer mecanismos para el cumplimiento de las políticas
vi. Revisar, acordar y aprobar actualización de inventario de activos
vii. Reportar a las instancias externas de interés (SIC, CSIRT Gobierno, entre otras) o internas (URO, control disciplinario, entre otras), las novedades o incidentes con relación a la seguridad, privacidad y ciberseguridad que impacten la confidencialidad, integridad y disponibilidad, de la información.

c. Instancia a nivel de proceso:

a. 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 y subprocesos.
b. 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 sea que esta se encuentre en formato digital, papel u otro.
c. Reportar a las instancias internas de interés (URO, Comité de gestión y desempeño institucional, instancia orientadora de la Gestión Tecnológica y que aborda los temas 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.

2. 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

a. Etapa de Selección:

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

b. Gestión y disposición final de documentos en cualquier formato, en

los 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.

b. Etapa de Vinculación:

a. 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 generales o específicos, normatividad vigente u otros instrumentos que se consideren dentro de la naturaleza de la información a la que se tendrá acceso.
b. Gestión y disposición final de documentación contractual, en cualquier formato, acorde con la normatividad en materia de tratamiento de datos personales, gestión documental y demás reglamentación vigente.
c. Socializar las políticas de seguridad de la información.

c. Etapa de Ejecución del empleo o contrato:

a. Exigir la aplicación de las políticas de seguridad de la información, basándose en los planes, políticas y procedimientos establecidos por la Entidad.
b. 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.

d. Etapa de Terminación o cambio de responsabilidades del empleo o contrato:

a. Establecer de forma clara, comunicar y hacer cumplir los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo al empleado o contratista.
a. Informar a los procesos interesados a fin de que se tomen las medidas correctivas en cuanto a 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 en torno a los activos de información.

3. GESTIÓN DE ACTIVOS Y DE INFORMACIÓN:

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

a. **Identificación y actualización de activos:** Con frecuencia cada 3 años, la OAPS coordina la actualización del inventario de activos, para consolidar en el formato del caso y someter a revisión y aprobación del comité.

Esta identificación, debe abarcar: equipamiento auxiliar, hardware, información, instalaciones, otros, procesos, recurso humano, red, servicios, software. Ver definiciones.

a. **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, así como de las leyes y normatividades vigentes que afecten a la Entidad en materia de sensibilidad y reserva.
b. **Etiquetado de activos:** Los activos que así lo permitan como el hardware, deben ser etiquetados, de forma que facilite su control y gestión.
c. **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 a efectos de entrega de activos físicos y de la información una vez finalizado el empleo, acuerdo o contrato que se tenga con la Entidad.
d. **Disposición final de los activos:** Adoptar procedimiento mediante el 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 re uso cuando los activos ya no se requieran mantener en operación.
e. Copia de seguridad de activos:
    i. Adoptar procedimientos desde el alcance del área que gestiona el activo de información, a fin de formalizar las tareas de copias de 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).

ii. Identificar estaciones de trabajo, cuya información se considere relevante y solicitar a la Oficina Asesora de Planeación y Sistemas, el agendamiento de copias de seguridad periódicas.
iii. Agendar pruebas periódicas de restauración de copias de seguridad.

f. Manejo de medios removibles:

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

b. Auditoría y control de activos:

a. Los sistemas de información deben incluir en su diseño y puesta en marcha, 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
b. 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, al menos una vez por trimestre, en cuanto a usuarios activos e inactivos, confidencialidad, integridad y disponibilidad de la información.
c. La información contenida en medio físico, debe ser objeto de auditoría, al menos una vez por trimestre, 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.
d. Los activos físicos (hardware) deben ser objeto de auditoría, con frecuencia semestral, en cuanto a verificación de estado, etiquetado y responsable asociado.
e. Los sistemas de control de acceso, deben ser objeto de auditoría de logs, en cuanto a verificación de acceso no autorizado, con frecuencia trimestral.

4. 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 accesos son electrónicos o físicos:

a. **Autorización, modificación y revocación de acceso:** Incluir en los procedimientos para control de acceso. según el alcance del área que gestiona el activo, a fin de establecer:
   a. Quiénes y cómo solicitan asignación, modificación o de derechos y/o privilegios, roles y permisos sobre las credenciales de acceso a los activos de información y servicios de tecnología.
   b. 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.
   c. 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.
   d. Quiénes y cómo solicitan asignación, modificación, revisión o revocación de derechos y/o privilegios de acceso para activos de información disponible en formato físico

b. **Responsabilidad manifiesta para los usuarios:** Desde el alcance de talento humano, contratación y calidad, establecer procedimiento para informar y exigir a los usuarios el cumplimiento de las políticas, dejando evidencia de la actividad.

c. **Gestión de acceso:** Incluir en los procedimientos de control de acceso, según el alcance del área que gestiona el activo, a fin de establecer:
   a. 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.
   b. Cómo se hace entrega de las credenciales de acceso

d. Gestión de Credenciales de acceso
   a. Las credenciales de acceso son personales e intransferibles y no deben prestarse, ni compartirse.
   b. Contraseñas con longitud y complejidad minina
   c. Contraseñas con vencimiento periódico
   d. Contraseñas para cambio obligatorio en el primer uso
   e. Contraseñas de gestión de servicios de TI, sin vencimiento, usadas para configuraciones de la infraestructura y plataforma tecnológica.

f. Contraseñas con cambio autónomo desde el alcance del usuario
g. Usuario con fecha de vencimiento para personas sujetas a vinculación por periodos de tiempo establecidos contractualmente.
h. Usuario sin vencimiento en el tiempo para funcionarios
i. Implementación de gestión de contraseñas cifradas, desde el diseño, desarrollo y puesta en marcha de soluciones tecnológicas

e. Control de acceso a redes, sistema y aplicaciones

a. 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 de control de acceso mediante credenciales de acceso seguro, con procedimientos de cifrado de contraseña y gestión centralizada de credenciales
b. Acceso restringido para el código fuente y sus versiones derivadas
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.

f. Teletrabajo o trabajo en casa

Las tareas de teletrabajo o trabajo en casa se realizan alineados a los acuerdos de confidencialidad, y el cumplimiento de requisitos mínimos de 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.

5. **CRIPTOGRAFÍA:** Asegurar el uso apropiado de los procedimientos para los cuales se requiere token criptográfico para proteger el procesamiento y resultados esperados:
   a. Los procesos que desarrollan tareas relativas a plataformas tanto públicas como privadas (SIIF, transmisión de información a la Superintendencia Financiera de Colombia, transmisión de información al 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.
   b. Así mismo, el proceso debe informar y exigir el uso personal e

intransferible del token criptográfico, así como de las credenciales de uso.

6. SEGURIDAD FÍSICA Y DEL ENTORNO

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

6.1.1 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 de la Entidad.
d. Tienen acceso los terceros, quienes requieren autorización del nivel jerárquico del caso, restringido al alcance de las labores específicas.

6.1.2 Bodega de archivo en la sede

a. Tienen acceso el Director General, Sub directores y gestores de archivo
b. Los demás requieren autorización del nivel jerárquico del caso, restringido al alcance del acceso otorgado

6.1.3 Bodega de archivo externa

a. Tienen acceso el Director General, Subdirectores ygestores de archivo
b. Los demás requieren autorización del nivel jerárquico del caso, restringido al alcance del acceso otorgado

6.1.4 Centro de datos

a. 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.
b. 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)

c. 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.

b. Seguridad de oficinas:

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

c. Protección contra amenazas externas y ambientales:

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

7. **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 no autorizadas
e. El mantenimiento de hardware y software, reubicación de los equipos, o instalación de software 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 y mesa de ayuda, 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 caso requiere 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 mediante sobre escritura, así como del concepto técnico del ingeniero de mesa de ayuda que realiza la actividad.
h. El puesto de trabajo debe mantenerse libre de equipos y dispositivos tales como medios removibles, tokens criptográficos, o documentos de trabajo, mientras no se estén usando.
i. El escritorio de los computadores del centro de datos debe permanecer limpios de scripts o documentación técnica que pueda comprometer la disponibilidad de la operación de este.
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.

8. **SEGURIDAD DE LAS OPERACIONES:** Asegurar las operaciones correctas y seguras:
   a. **Procedimientos de operación del centro de datos:** Documentar y poner a disposición del 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.
   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 paso a 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 seguimiento periódico al uso, proyección de crecimiento requerido con holgura y generación de informe para análisis y toma de decisiones.
   d. **Separación de ambientes:** La gestión de cambios, debe soportarse en una separación de ambiente de pruebas, desarrollo y producción.

e. Protección contra código malicioso:

a. Implementar la instalación, monitoreo y actualización permanente de solución antivirus en las estaciones de trabajo**.**

b. Implementar protección, monitoreo y actualización permanente en el borde de la red, con una solución de propósito específico tipo appliance UTM.

c. Mantener vigente la asistencia técnica del proveedor especializado en estas soluciones.

d. Brindar capacitación y sensibilización en esta materia al interior de la Entidad

f. Copias de respaldo:

a. Realizar copias de la información, software e imágenes de los componentes de la plataforma tecnológica.

b. Realizar pruebas mensuales de restauración, con su respectivo informe

c. Alcance de copias de respaldo para información y componentes del centro de datos, información de las estaciones de trabajo de directivos y de estaciones de trabajo que cada proceso haya identificado como relevantes.

d. Almacenamiento y conservación de copias en cintas magnéticas con custodia externa.

e. Conservación de copias en los medios de almacenamiento local por periodos cortos de tiempo.

g. **Gestión de logs – evidencias:** El responsable de la administración de un sistema de información, debe realizar gestión de logs, en cuanto a:

a. Conservar y revisar periódicamente los registros de actividades de usuarios, fallas o eventos de seguridad.

b. Estos registros o logs deben estar protegidos contra acceso no autorizado.

h. **Sincronización de relojes:** Los sistemas de información, plataforma tecnológica del centro de datos y estaciones de trabajo, sincronizan con los servidores de hora legal en Colombia y 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.

i. **Usuarios restringidos:** Los usuarios de red para gestión de las estaciones de trabajo, son usuarios restringidos sin privilegios administrativos, que les impide instalar o desinstalar software.

j. **Análisis de vulnerabilidades:** Al menos una vez por año, Gestión Tecnológica realiza un análisis de vulnerabilidades a fin de obtener las oportunidades de mejora e implementar los correctivos del caso.

k. **Ventanas de mantenimiento:** La intervención en la plataforma tecnológica de la Entidad con fines de auditoría, mantenimiento

preventivo o correctivo, deben acordarse en horarios no laborales e informar del impacto al interior de la Entidad a fin de minimizar las interrupciones en los procesos de negocio.

9. **SEGURIDAD DE LAS COMUNICACIONES:** Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información:
   a. Separar en subredes las áreas del centro de datos, estaciones de trabajo y DMZ
   b. Definir una zona desmilitarizada DMZ, donde operan los servicios que se publican directamente en internet como el sitio web, entre otros.
   c. 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.
   d. La red WIFI gratis para la gente, 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.
   e. Realizar monitoreo permanente de la disponibilidad de las redes.
   f. Red de internet con redundancia ante fallos

10. **TRANSFERENCIA DE INFORMACIÓN:** Mantener la seguridad de la información transferida dentro de Fonprecon y con cualquier Entidad externa:
   a. 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.
   b. Proteger las comunicaciones de correo electrónico, mediante aviso de privacidad en el pie de firma, certificado digital SSL y filtros de contenido.
   c. Proteger las comunicaciones electrónicas mediante recursos propios tipo nube y SFTP, mediante fecha de expiración y credenciales de acceso.
   d. Adoptar las medidas necesarias a fin de que la tercerización o uso de tecnologías de nube fuera del País, cuenten con legislación vigente en cuanto a seguridad y privacidad de la información

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

11.1 Análisis y requisitos de seguridad de la información: Estas consideraciones de seguridad deben incluirse en la contratación, diseño e implementación de nuevas soluciones o mejoras a los sistemas de información existentes:

a. No quemar direcciones IP en el código, en cambio ha de usarse los nombres completos o FQDN de los sistemas que intervienen.
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 prolongado de inactividad
g. Cerrar sesión automáticamente luego de 10 minutos de inactividad
h. Cifrado de la información en transporte
i. Certificado para IPv6 en convivencia con IPv4
j. Análisis de vulnerabilidades y penetración reiterativos en la fase de pruebas, con aplicación de mejoras hasta que ya no sean evidentes.

11.2 Desarrollo seguro:

a. Hacer uso del ambiente de pruebas y desarrollo antes de pasar a 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 de versiones del desarrollo
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

12. RELACIONES CON LOS PROVEEDORES: Asegurar la protección de los activos de Fonprecon que sean accesibles a los proveedores:

12.1 Acuerdo de confidencialidad: Diseñar e incluir un acuerdo de confidencialidad como parte integral de la contratación, que incluya al menos:

a. Marco legal y reglamentario relacionado con seguridad, privacidad, ciberseguridad y protección de datos en Colombia
b. 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.
c. Firmas de las dos partes identificando la calidad de persona natural o jurídica y fechas de suscripción del acuerdo
d. Que el acuerdo de confidencialidad se hace extensible aún después de terminada la vinculación con FONPRECON
e. Autonomía de Fonprecon para auditabilidad sobre la prestación del servicio
f. Establecer la formalidad de las comunicaciones, incluso para reportar anomalías o actividad sospechosa sobre el activo o servicio.
g. Reconocimiento del valor probatorio del acuerdo que se firme.

12.2 Tratamiento de riesgos:

a. Dentro del marco contractual, integrar requisitos para el acceso, procesamiento, almacenamiento e intercambio de información, así como las comunicaciones relacionadas y suministro de componentes de tecnología.
b. 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.

12.3 Gestión del servicio de proveedores:

12.3.1 Seguimiento:

a. Adoptar procedimiento para establecer los requisititos mínimos de seguimiento, revisión, auditoria, identificación de hitos con sus fechas y periodicidad del seguimiento. Incluir en el procedimiento, características y recomendaciones mínimas a la hora de contratar determinados servicios recurrentes.

b. Según la magnitud del servicio, adoptar indicadores que permitan la medición de alcance de los hitos.

12.3.2 Gestión de cambios:

a. Adoptar procedimiento de gestión de cambios en políticas, procedimientos, riesgos y controles de seguridad de los

activos, teniendo en cuenta la criticidad de la información, activos asociados y procesos involucrados como resultado de los servicios de los proveedores.

12.3.3 Adquisición de bienes y servicios:

a. 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 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.

13. GESTIÓN DE EVENTOS DE SEGURIDAD Y CIBERSEGURIDAD DE LA INFORMACIÓN: Asegurar un enfoque coherente y eficaz para la gestión y comunicación de eventos de seguridad y ciberseguridad:

13.1 Gestión y Reporte: Adoptar procedimiento para la gestión y reporte de incidentes de seguridad y ciberseguridad, que integre al menos:

i. Identificar los responsables de la gestión de eventos sobre los activos
ii. Cómo reportar internamente a la URO
iii. Quién reporta al Comité de gestión y desempeño institucional, instancia orientadora de la gestión tecnológica de la Entidad
iv. Quién debe reportar externamente
v. Exigir a todos los empleados y contratistas, reportar cualquier anomalía o actividad sospechosa en los sistemas o servicios de tecnología, al líder de su proceso.
vi. Clasificación según el impacto en evento, incidente de seguridad o ciberseguridad
vii. Recolección de evidencia
viii. Documentación de respuesta al evento

14. 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 plan de continuidad de negocio debe incluir los requisitos de seguridad que deben tenerse en cuenta en situaciones adversas, por ejemplo, en un desastre.
b. Complementar el plan de continuidad de negocio con los procedimientos necesarios para establecer e implementar la

continuidad de la seguridad de la información en situaciones adversas.

c. Las pruebas periódicas del plan de continuidad de negocio, debe incluir en su alcance, lo concerniente a la seguridad de la información.

15. **REDUNDANCIAS:** Asegurar la disponibilidad de instalaciones de procesamiento de información:
    a. Adoptar procedimiento que documente las redundancias aplicadas como planes de contingencia, a fin de fortalecer la disponibilidad en servicios de tecnología y plataforma tecnológica.
    b. Adoptar procedimiento que documente las redundancias aplicadas como planes de contingencia, a fin de fortalecer la disponibilidad de la gestión de procesos y procedimientos críticos como gestión de correspondencia, atención al usuario, gestión de archivo físico, entro otros.

16. **CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES:** Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la informacióny de cualquier requisito de seguridad:
    a. Identificar, documentar explícitamente y actualizar periódicamente para cada activo de información, la legislación, requisitos contractuales y demás normas aplicables en cuanto a:
        I. Derechos de propiedad intelectual
        II. Protección de registros
        III. Privacidad y protección de datos personales
        IV. Reglamentación de controles criptográficos

17. **REVISIÓN DE CUMPLIMIENTO:** Asegurar que la seguridad de la información se implementa y opera de acuerdo con las políticas y procedimientos organizacionales:
    a. Realizar revisiones a la gestión de la seguridad de la información y ciberseguridad en el marco de las políticas en esta materia, con el fin de:
        I. Mantener el ciclo de vida del sistema de gestión de seguridad, dentro de un intervalo de tiempo o cuando ocurran cambios significativos

        II. Los líderes de cada proceso revisan el cumplimiento de las políticas dentro de su área de responsabilidad

ANEXO 2. ACUERDO DE CONFIDENCIALIDAD

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 cumplimiento del marco contractual que me vincula con el **FONDO DE PREVISIÓN SOCIAL DEL CONGRESO DE LA REPÚBLICA - FONPRECON**, suscribo el presente **ACUERDO DE CONFIDENCIALIDAD,** mediante el cual reconozco que:

1. La seguridad, ciberseguridad y privacidad de la información, se sujeta a la legislación vigente en Colombia:
    I. Hábeas data: 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. (Habeas Data).
    II. Privacidad y protección de datos personales:
        a. 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.
        b. Decreto 1377 de 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
        c. 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.
        d. Sentencia C-020 de 2014 Corte Constitucional
        e. Sentencia T-444 de 2014 Corte Constitucional
    III. Protección de la información y de los datos: 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".
    IV. Ley de Transparencia: 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.
    V. Derechos de autor: Decreto 1360 de 1989, Ley 44 de 1993, Decreto 460 de 1995, Ley 565 de 2000, Ley 603 de 2000

VI. Las demás que se encuentren vigentes

2. Se entiende por información confidencial, toda aquella de carácter tecnológico, estratégico, conceptual, así como la relacionada con las operaciones de negocio presentes y futuras, bien sea que dicha información sea escrita, oral o visual, en forma electrónica o contenida en bases de datos y cualquier otro documento o dispositivo que contenga información relacionada con FONPRECON, que no tenga el carácter de divulgación pública.
3. Se define como datos personales, toda información que identifica a un individuo dentro del marco de la ley 1581 de 2012 y sus decretos reglamentarios.
4. Toda información relacionada con el objeto contractual es propiedad exclusiva de FONPRECON.
5. Que la confidencialidad de la información se hace extensible aún después de terminada la vinculación con FONPRECON.
6. FONPRECON se reserva el derecho de auditabilidad para registrar y monitorear todas las actividades realizadas, sin previo aviso.
7. En mi calidad de representante legal, si aplica,

Con base en lo anterior y para el desarrollo de las actividades enmarcadas dentro del alcance del vínculo contractual vigente, me comprometo a:

1. Reconocer que el uso de componentes tecnológicos (hardware y software) así como los procedimientos para acceso, generación y transformación de información confidencial, tienen como única finalidad el cumplimiento de mis obligaciones contractuales o funciones asignadas lo que no deriva en derechos alguno de propiedad intelectual sobre dicha información.
2. Socializar y extender el alcance de este acuerdo al equipo de trabajo, como resultado de mi liderazgo o en mi calidad de representante legal de la firma que represento
3. No usar indebidamente la información confidencial, en consecuencia, debo proteger la información contra el acceso no autorizado, modificación, destrucción, sustracción, falsificación, publicación, reproducción, revelación, entrega a terceros, o cualquier otro uso no autorizado, propendiendo por la INTEGRIDAD y AUDITABILIDAD.
4. Aplicar las medidas de seguridad exigidas por FONPRECON, en cuanto a políticas de TI, política de tratamiento de datos personales y los demás lineamientos que en materia de seguridad de la información estén vigentes.

5. Cumplir la normatividad legal y reglamentaria relacionada con seguridad, privacidad y protección de datos en Colombia.
6. Informar al supervisor del contrato en cuanto a materialización de riesgos, anomalías, actividad sospechosa, incidentes o eventos que puedan presentarse o identificarse dentro de la ejecución del objeto y alcance contractual, con relación a la seguridad, ciberseguridad y privacidad de la información.
7. Al finalizar el vínculo contractual, la Información confidencial suministrada que llegase a quedar sobre equipos tecnológicos o ambientes de desarrollo, pruebas y control de versiones del contratista o tercero, deberá ser sometida a procedimientos de:
    a. Consultar si Fonprecon requiere copia, acordando los medios de entrega
    b. Borrado seguro de la información, mediante procedimientos de sobre escritura certificando la realización de tales procedimientos.
    c. Disposición final de información concerniente a configuraciones bien sea en formato digital o en papel.
8. Ante el incumplimiento de las anteriores obligaciones asumiré la responsabilidad penal y/o disciplinaria y/o fiscal y/o civil a que hubiere lugar.

En consecuencia, firmo este acuerdo en día mes año:

PERSONA NATURAL ☐		REPRESENTANTE LEGAL ☐
Nombres	Número de cédula	Empresa
Cargo	Número de contrato y fecha	Firma

ANEXO 3 FORMATO PARA SOLICITUD Y AUTORIZACIÓN DE USO DE EQUIPOS PERSONALES EN LAS REDES DE COMUNICACIONES DE FONPRECON

Nombres y apellidos	
Tipo de equipo	Portátil Móvil Escritorio
Propósito del uso del equipo	
Empresa para la que trabaja actualmente	
Tiempo estimado del uso de este equipo	
A qué servicios de tecnología requiere acceso	
Cantidad de equipos	
Marca, modelo, serie	
Tiene instalado un antivirus licenciado	SI NO
Contiene algún software no licenciado	SI NO
Autorizo el monitoreo y auditabilidad de los equipos de forma automatizada mediante los sistemas de monitoreo de la Entidad, para detección de software no autorizado, fallos y amenazas de seguridad y ciberseguridad	
Autorizo la validación de esta información mediante el personal técnico de Fonprecon: Si autorizo___ No autorizo___	CUMPLE NO CUMPLE ➢ Computadores con Sistema operativo Microsoft Windows o MAC, instalado con el más reciente nivel de actualización disponible por el fabricante.
	CUMPLE NO CUMPLE ➢ Computadores con Sistema operativo Microsoft Windows o MAC con activación automática de descarga e instalación de actualizaciones
	CUMPLE NO CUMPLE ➢ Dispositivos móviles con ciclo de vida vigente del fabricante y con aplicación de las más recientes actualizaciones disponibles
	CUMPLE NO CUMPLE ➢ Antivirus instalado, configurado y licenciado (aplica el antivirus provisto por el sistema operativo Windows 10 o superior). No aplica antivirus de uso gratuito por sus limitaciones en capas de protección, sin registros de amenazas en cuarentena y ejecutar un análisis completo previo a la conexión a la red.
Comprendo que las actividades de soporte y mantenimiento son de alcance del propietario del equipo	SI NO
Conozco y he firmado el acuerdo de confidencialidad de Fonprecon	SI NO

_____
Aprobado jefe Oficina Asesora de Planeación y Sistemas

_____
Visto bueno, Dirección General