



Plan estratégico de seguridad y privacidad de la información

PESI 2024 – 2027

**Fondo de Prestaciones Económicas,
Cesantías y pensiones – FONCEP**

Versión 4

Sede Principal

Carrera 6 Nro. 14-98

Edificio Condominio Parque Santander

Teléfono: +571 307 62 00 || www.foncep.gov.co



FONDO DE
PRESTACIONES ECONÓMICAS,
CESANTÍAS Y PENSIONES

CONTENIDO

1.	Introducción	3
2.	Objetivos.....	3
3.	Alcance.....	3
4.	Normatividad	4
5.	Definiciones	5
6.	Política de Seguridad de la Información	5
7.	Marco Estratégico.....	6
8.	Metodología utilizada	8
9.	Situación actual.....	9
10.	Sistemas de Información.....	13
11.	Roles y responsabilidades de Seguridad y privacidad de la Información.....	14
12.	Definición y priorización de actividades.....	21
13.	Actividades Clave	21

Sede Principal

Carrera 6 Nro. 14-98

Edificio Condominio Parque Santander

Teléfono: +571 307 62 00 || www.foncep.gov.co

1. Introducción

El Fondo de Prestaciones Económicas, Cesantías y Pensiones (FONCEP) tiene como misión gestionar y garantizar el manejo eficiente y seguro de la información relacionada con las prestaciones sociales de los servidores públicos de Bogotá, D.C. La naturaleza sensible de los datos financieros y personales administrados exige el cumplimiento riguroso de los lineamientos de seguridad y privacidad establecidos a nivel nacional, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de la información.

La creación de un Plan Estratégico de Seguridad de la Información - PESI adopta una postura alineada con los objetivos estratégicos de FONCEP, los objetivos de la Oficina de Informática y Sistemas (OIS) y en el marco del cumplimiento de la política de Gobierno Digital y Seguridad Digital. Este plan cimienta transversalmente la seguridad en toda la infraestructura tecnológica y apoya el logro de los objetivos de la entidad.

2. Objetivos

2.1 Objetivo General

Definir y establecer una estrategia de Seguridad de la Información, la cual es liderada por la Oficina de Informática y Sistemas (OIS) de la Entidad e implementada para responder a las necesidades de establecer planes, controles, procesos, procedimientos y proyectos que tiene la institución para lograr sus objetivos estratégicos institucionales y preservar la confidencialidad, integridad y la disponibilidad sobre los activos de información.

Garantizar la seguridad y privacidad de la información gestionada por FONCEP, mediante la implementación de medidas, controles y estrategias que aseguren la confidencialidad, integridad, disponibilidad y privacidad de los datos, en cumplimiento de las normativas nacionales, la Política de Gobierno Digital y los estándares internacionales aplicables.

2.2 Objetivo de Seguridad de la Información

Dar lineamiento para la implementación y aplicación de la gestión de la seguridad y privacidad de la información. Generar una cultura y apropiación de trabajo enfocada a la toma de conciencia para la protección y el uso adecuado de la información por parte de los servidores públicos, contratistas y colaboradores de FONCEP.

Asegurar que los riesgos asociados a seguridad digital estén alineados con la metodología del Manual de gestión de los riesgos.

Mantener un enfoque de cumplimiento estricto de los requisitos legales, normativos o contractuales aplicables y relativos al tratamiento y protección de la información.

3. Alcance

El presente plan aplica a todos los procesos, sistemas tecnológicos, activos de información y usuarios internos y externos que interactúan con la información administrada por FONCEP, abarcando desde la gestión de datos sensibles hasta la infraestructura tecnológica y los riesgos asociados a la ciberseguridad, con el fin de garantizar la protección de la información en cumplimiento de las normativas nacionales y la Política de Gobierno Digital.

4. Normatividad

A continuación, se relaciona el marco normativo relacionado con el Plan Estratégico de Seguridad de la Información - PESI:

Marco Normativo	Descripción
Ley 1581 de 2012 - Protección de Datos Personales	Establece el marco general para el tratamiento de datos personales, garantizando los derechos de los titulares de la información.
Ley 1266 de 2008 - Ley de Habeas Data	Regula el manejo de información financiera, crediticia y comercial, aplicable a las bases de datos administradas por FONCEP.
Ley 1712 de 2014 - Ley de Transparencia y del Derecho de Acceso a la Información Pública	Reglamenta el acceso a la información pública, garantizando su manejo responsable y seguro, seguridad social.
Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector TIC	Obliga a las entidades públicas a implementar medidas de seguridad digital y lineamientos de privacidad en sus procesos, sistemas y activos de información.
Decreto 1083 de 2015 - Decreto Único Reglamentario del Sector de Función Pública	Establece la integración de planes estratégicos al Plan de Acción de las entidades públicas y promueve la gestión articulada de los sistemas de información.
Decreto 2106 de 2019 - Simplificación de Trámites	Requiere a las entidades públicas disponer de sistemas de gestión documental electrónica y estrategias de seguridad digital que aseguren la integridad, disponibilidad y autenticidad de la información.
Resolución 500 de 2021 - Estrategia de Seguridad Digital	Adopta el Modelo de Seguridad y Privacidad de la Información (MSPI) como habilitador de la Política de Gobierno Digital, estableciendo lineamientos para la gestión de riesgos, incidentes de seguridad digital y estándares de seguridad.
Resolución 3564 de 2015 - Gestión de Riesgos de Seguridad	Define los lineamientos y estándares para la implementación de controles de seguridad en la infraestructura tecnológica y los sistemas de información.
Resolución 4870 de 2023 - Modelo Integrado de Gestión (MIG) y Sistema Integrado de Gestión (SIG)	Establece la necesidad de articular los sistemas de gestión de las entidades públicas con la Política de Gobierno Digital, incluyendo el fortalecimiento de la seguridad y privacidad de la información.

5. Definiciones

Seguridad de la Información: Según la ISO/IEC 27001:2022, la seguridad de la información se define como la preservación de la confidencialidad, integridad y disponibilidad de la información, así como otros aspectos relevantes como la autenticidad, responsabilidad, no repudio y confiabilidad. En el contexto de MINTIC, la Política de Gobierno Digital establece que la seguridad de la información incluye medidas técnicas y administrativas para proteger los activos de información en cumplimiento del Decreto 1078 de 2015.

Privacidad de la Información: Según la ISO/IEC 27701:2019, la privacidad se refiere a la gestión adecuada de la información personal, garantizando su procesamiento conforme a principios de protección de datos. En Colombia, el Decreto 1377 de 2013 y la Ley 1581 de 2012 (Ley de Protección de Datos Personales) regulan la privacidad y el manejo de datos personales en las entidades públicas y privadas.

Confidencialidad: Según la ISO/IEC 27000:2022, la confidencialidad es la propiedad de la información que garantiza que solo las personas, entidades o procesos autorizados puedan acceder a ella. En el contexto de MINTIC, el Modelo de Seguridad y Privacidad de la Información (MSPI) hace énfasis en proteger la confidencialidad como uno de los pilares fundamentales de la gestión de riesgos de información.

Integridad: La ISO/IEC 27000:2022 define la integridad como la propiedad que asegura que la información no ha sido alterada de manera no autorizada y se mantiene exacta y completa. En el contexto de MINTIC, la integridad es esencial para garantizar la confiabilidad de los datos utilizados en los procesos de toma de decisiones.

Disponibilidad: Según la ISO/IEC 27000:2022, la disponibilidad es la propiedad que asegura que la información está accesible y utilizable por quienes la necesitan, en el momento en que se requiere. En la normativa de MINTIC, la disponibilidad se garantiza mediante planes de continuidad y recuperación ante desastres, como lo exige la Resolución 500 de 2021.

PESI: El plan estratégico de seguridad de la información determina los objetivos a cumplir para salvaguardar la información en sus pilares de confidencialidad, integridad y disponibilidad.

PETI: Plan Estratégico de TI, de acuerdo con el Marco de Referencia de Arquitectura Empresarial para la Gestión de TI del Estado colombiano, el Plan Estratégico de las Tecnologías de la Información y comunicaciones, es el artefacto que se utiliza para expresar la Estrategia de TI. El PETI hace parte integral de la estrategia de la institución y es el resultado de un adecuado ejercicio de planeación estratégica de TI.

6. Política de Seguridad de la Información

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

Por lo tanto, todas las personas naturales y jurídicas que laboran en el FONDO DE PRESTACIONES

Sede Principal

Carrera 6 Nro. 14-98

Edificio Condominio Parque Santander

Teléfono: +571 307 62 00 || www.foncep.gov.co



FONDO DE
PRESTACIONES ECONÓMICAS,
CESANTÍAS Y PENSIONES

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

La Política general de seguridad de la información de FONCEP se encuentra soportada por lineamientos, normas y procedimientos específicos los cuales guían la gestión adecuada de la información. Lo anterior fue socializado en el Comité institucional de Gestión y Desempeño No. 03 de 2021 y aprobado en la Junta Directiva Sesión No. 12 del 17 de noviembre de 2021

7. Marco Estratégico

De acuerdo al Plan Estratégico Institucional 2024 - 2027 (publicado en Transparencia: 4. Planeación, Presupuesto e Informes | Fondo de Prestaciones Económicas, Cesantías y Pensiones | FONCEP) y el Plan Estratégico de Tecnologías de la Información - PETI donde se incluyen disposiciones del acuerdo 761 de 2020 por medio del cual se adopta el plan de desarrollo distrital para el período y que se constituye como referente para todas las entidades Distritales, donde se plantean dos (2) líneas estratégicas sobre la cuales se deben definir las metas, actividades e insumos.

Sede Principal

Carrera 6 Nro. 14-98

Edificio Condominio Parque Santander

Teléfono: +571 307 62 00 || www.foncep.gov.co



FONDO DE
PRESTACIONES ECONÓMICAS,
CESANTÍAS Y PENSIONES



FONDO DE
PRESTACIONES ECONÓMICAS,
CESANTÍAS Y PENSIONES



Plan Estratégico Institucional 2024 - 2027

METAS INSTITUCIONALES

Propósito Superior

Potencializar la misionalidad de la entidad identificando e implementando oportunidades técnicas, operativas, legales y tecnológicas que permitan transformarse y ser referente en la gestión de lo público.

LÍNEA ESTRATÉGICA 1

1. FORTALECER LA CAPACIDAD ORGANIZACIONAL PARA GESTIONAR EFICIENTEMENTE LA GESTIÓN PENSIONAL DEL DISTRITO **16.67 %**

Busca fortalecer y resolver problemáticas y dificultades de la gestión prestacional, documental, de servicios tecnológicos y desarrollo organizacional de la entidad.



LÍNEA ESTRATÉGICA 2

2. IMPLEMENTAR UNA ESTRATEGIA QUE PERMITA DAR A CONOCER LA POLÍTICA DE ATENCIÓN AL PENSIONADO Y SU IMPACTO A LOS PENSIONADOS DEL FONCEP **25.00 %**

Busca gestionar la implementación de la política de atención al pensionado, promoviendo la ampliación de la oferta de servicios con diferentes entidades para el acceso de los pensionados a servicios de apoyo de que generen bienestar físico y psicológico, y así fortalecer el relacionamiento con este grupo de valor.



1. IMPLEMENTAR LA ESTRATEGIA DE DESARROLLO ORGANIZACIONAL Y GESTIÓN PRESTACIONAL

DOCUMENTOS DE INVESTIGACIÓN
Vigencia

● 50.00 %



2. IMPLEMENTAR LA ESTRATEGIA DE GESTIÓN DOCUMENTAL

SISTEMA DE GESTIÓN DOCUMENTAL ACTUALIZADO
Vigencia

● 0.00 %



3. RENOVAR EL 100% DEL PROGRAMA TECNOLÓGICO Y DE GOBIERNO DIGITAL

CAPACIDAD EN LA PRESTACIÓN DE SERVICIOS DE TECNOLOGÍA
Vigencia

● 0.00 %



4. IMPULSAR LA IMPLEMENTACIÓN DE LA POLÍTICA DE ATENCIÓN AL PENSIONADO EN EL FONCEP

ESPACIOS DE INTEGRACIÓN DE OFERTA PÚBLICA GENERADOS
Vigencia

● 25.00 %



Ilustración 1 Marco Estratégico Fuente: Plan Estratégico Institucional 2024 -2027

De acuerdo con las actividades claves y propuesta de valor definidos en el Plan Estratégico de Tecnologías de la Información - PETI del FONCEP que incluyen:

7.1 Propuestas de Valor

Línea estratégica 1: Fortalecer la capacidad organizacional para gestionar eficientemente la gestión pensional del distrito.

7.2 Metas institucionales:

Implementar la estrategia de desarrollo organizacional y gestión prestacional.

Implementar la estrategia de gestión documental.

Renovar el 100% del programa tecnológico y de Gobierno Digital.

Sede Principal

Carrera 6 Nro. 14-98

Edificio Condominio Parque Santander

Teléfono: +571 307 62 00 || www.foncep.gov.co



FONDO DE
PRESTACIONES ECONÓMICAS,
CESANTÍAS Y PENSIONES

Específicamente, en los temas de seguridad de la información se cuenta con la meta “Renovar el 100% del programa tecnológico y de Gobierno Digital.” La cual destaca a la seguridad como parte fundamental y transversal del negocio, por esta razón es necesario generar gobierno, lineamientos y acciones que permitan a la entidad mantener segura y disponible su información.

Por lo anterior, la sofisticación del uso y estrategia de Tecnología de Información conlleva la necesidad y obligación de mejorar las herramientas de seguridad. En todo el mundo los ataques cibernéticos se han incrementado con métodos innovadores. En Colombia, las instituciones de seguridad se están vinculando a la Estrategia TI para aumentar la capacidad del Estado de enfrentar las amenazas informáticas, pues en el momento presenta grandes debilidades, pese a que existen iniciativas gubernamentales, privadas y de la sociedad civil que buscan contrarrestar sus efectos, no hay una coordinación interinstitucional apropiada. Por esta razón la seguridad es parte fundamental y transversal del negocio, por esta razón es necesario generar gobierno y lineamientos que permitan a la entidad mantener segura y disponible su información.

8. Metodología utilizada

Teniendo en cuenta que el PESI constituye un soporte y apoyo en la implementación del SGSI, el primero se basa en la metodología utilizada por el Plan Estratégico de Tecnologías de la Información, de igual manera se basa en los siguientes documentos:

- Modelo de Seguridad y Privacidad de la Información (MSPI - 2022).
- Norma internacional NTC/ISO 27001:2022.
- Gobierno digital (establecida mediante el Decreto 1008 de 2018).
- Decreto 1499 de 2017 (Modelo Integrado de Planeación y Gestión).

8.1. Planeación

A partir de los lineamientos del Modelo de Seguridad y Privacidad de la Información – MSPI (2025) y la implementación del Sistema de Gestión de Seguridad de la Información; se toma como base el ciclo de mejoramiento continuo PHVA, procurando que el SGSI del FONCEP, se revise de forma continua y se ajuste a las dinámicas y los cambios en la infraestructura y los procesos de la Entidad.

Los componentes de cada fase del ciclo son las siguientes:



Ciclo PHVA del proceso de Seguridad y Privacidad

Ilustración 2 Metodología PHVA Fuente: MinTIC

9. Situación actual

Apoyados en la herramienta “INSTRUMENTO DE EVALUACIÓN MSPI (2021 - 2022)” se obtuvieron los resultados del análisis de brecha sobre la efectividad de los controles con los siguientes resultados.

No.	Evaluación de Efectividad de controles			EVALUACIÓN DE EFECTIVIDAD DE CONTROL
	DOMINIO	Calificación Actual	Calificación Objetivo	
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	70	100	GESTIONADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	75	100	GESTIONADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	80	100	GESTIONADO
A.8	GESTIÓN DE ACTIVOS	72	100	GESTIONADO
A.9	CONTROL DE ACCESO	85	100	OPTIMIZADO
A.10	CRIPTOGRAFÍA	60	100	EFFECTIVO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	79	100	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	76	100	GESTIONADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	78	100	GESTIONADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	66	100	GESTIONADO
A.15	RELACIONES CON LOS PROVEEDORES	80	100	GESTIONADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	69	100	GESTIONADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	70	100	GESTIONADO
A.18	CUMPLIMIENTO	80	100	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES		74	100	GESTIONADO

Tabla 1 Evaluación de efectividad de controles.

Fuente: instrumento de evaluación de MSPI (Modelo de Seguridad y Privacidad de la Información) FONCEP

Se evidencia que se han disminuido algunos de los dominios principalmente:

A.5 Política de Seguridad de la información de 100 a 70.

A.8 Gestión de activos de 100 a 72.

A.14 Adquisición, desarrollo y mantenimiento de sistemas de 100 a 66.

A.17 Aspectos de seguridad de la información de la gestión de la continuidad del negocio de 100 a 72.

A.11 Seguridad física y del entorno de 100 a 79.

Tema (Cláusula Anexo A)	Dominios Anteriores Mapeados	Calificación 27001:2022
5. Controles Organizacionales (37 controles)	Políticas (A.5), Organización (A.6), Activos (A.8), Proveedores (A.15), Incidentes (A.16), Continuidad (A.17), Cumplimiento (A.18)	73.7
6. Controles de Personas (8 controles)	Seguridad de los Recursos Humanos (A.7)	80.0
7. Controles Físicos (14 controles)	Seguridad Física y del Entorno (A.11)	79.0
8. Controles Tecnológicos (34 controles)	Acceso (A.9), Criptografía (A.10), Operaciones (A.12), Comunicaciones (A.13), Adquisición/Dev (A.14)	73.0
NUEVO PROMEDIO GENERAL		74.0

Tabla 2 Evaluación de efectividad de controles ISO 27001:2022

Fuente: instrumento de evaluación de MSPI (Modelo de Seguridad y Privacidad de la Información) FONCEP



Ilustración 3 Brechas de Seguridad.

Fuente: instrumento de evaluación de MSPI (Modelo de Seguridad y Privacidad de la Información) FONCEP

A partir de la evaluación de la calificación de MSPI (2023 - 2024), se identifica un aumento en la calificación con respecto al periodo previo (de 68 a 74), esto debido al alza en la calificación de la efectividad de múltiples controles, los cuales repercuten en la clasificación global.



Ilustración 4 Brechas Anexo 27001:2022

Fuente: instrumento de evaluación de MSPI (Modelo de Seguridad y Privacidad de la Información) FONCEP

A partir de la evaluación de la calificación de MSPI (2025), se identifica una leve disminución la calificación con respecto al periodo previo, esto debido al cambio en los dominios y lineamientos de múltiples controles, los cuales repercuten en la clasificación global.

FONCEP cuenta con 64 riesgos relacionados con seguridad de la información asociados a los activos de la información críticos de cada proceso, así mismo presenta los informes de segunda línea de defensa los cuales se pueden consultar en el botón de transparencia de la entidad.

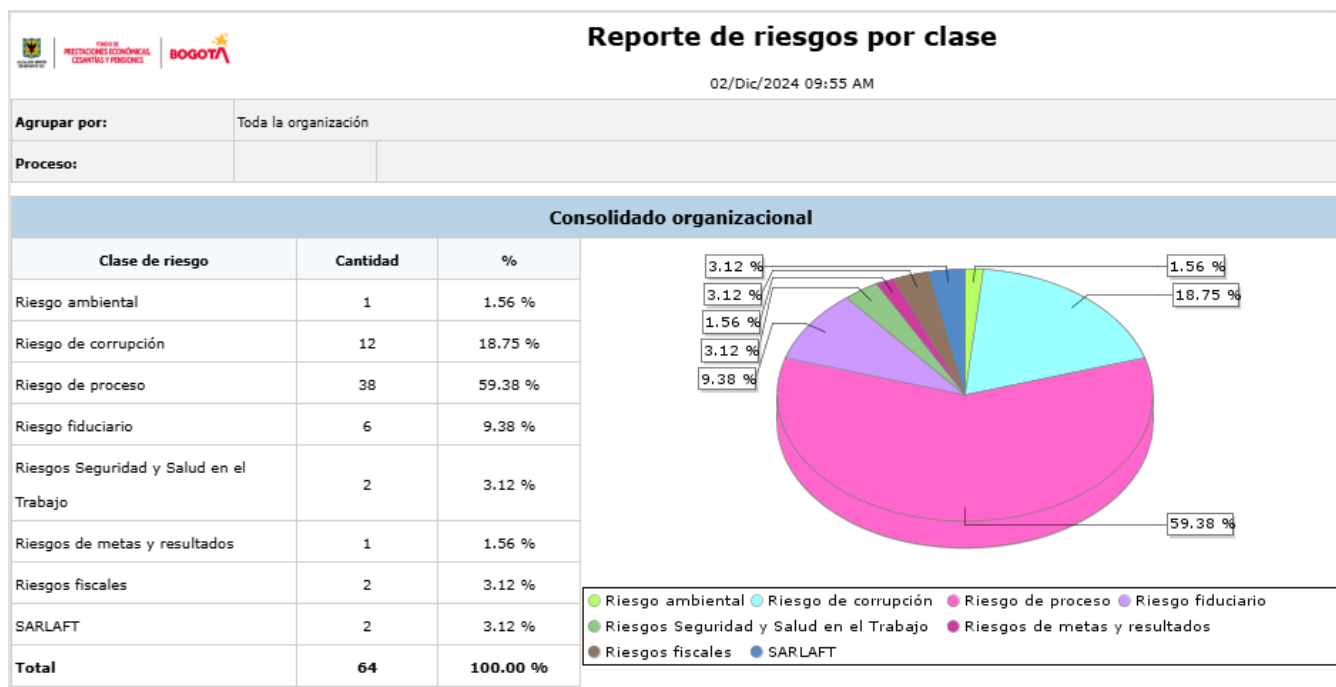


Ilustración 5 Riesgos FONCEP – Seguridad de la información

La Oficina de Informática y Sistemas es segunda línea de defensa de los riesgos de seguridad de la información y brinda acompañamiento a los procesos de la entidad para implementar la metodología de gestión del riesgo de FONCEP, identificando los activos de información con criticidad más alta por proceso, estableciendo causas, efectos, controles y acciones de tratamiento. Además, el Plan de acción Institucional cuenta con actividades marcadas con el clasificador del Plan de tratamiento de riesgos de seguridad de la información.

La matriz de riesgos esta publicada en la página web de la entidad en la siguiente ruta: [Transparencia: 4. Planeación, Presupuesto e Informes | Fondo de Prestaciones Económicas, Cesantías y Pensiones | FONCEP](#)

10. Sistemas de Información

El dominio de sistemas de información permite a la entidad orientar durante la implementación del dominio de sistemas de información. Adicional a lo anterior para el Min TIC este dominio posibilita que FONCEP muestre a partir de mejores prácticas concretas como se implementa el dominio de sistemas de información, del marco de referencia de arquitectura empresarial para la gestión de TI de Colombia.

La entidad hoy no cuenta con políticas y lineamientos de gestión de sistemas de información institucional, esto ocasiona que cada requerimiento organizacional lo atienda cada área por medio de las capacidades técnicas del tercero que adjudique el contrato, de igual manera se promueve la proliferación de estilos de arquitectura de software en cada sistema de información desarrollado, al igual que uso de tecnologías propietarias o libres de las cuales el grupo de sistemas de información del FONCEP no tendrá capacidad para soportar o hacer mantenimiento correctivo y preventivo por la especialidad del conocimiento, generando así dependencia con el roadmap del proveedor, de igual manera al no tener un estilo de arquitectura definido para la construcción de las plataformas tecnológicas del ejército, ni un catálogo de servicios normalizado se obliga a los proyectos a hacer integraciones por base de datos o construcción de silos de información que replican datos generando un acoplamiento fuerte con otras plataformas.

Para más información de los Sistemas de información verificar El Plan Estratégico de Tecnologías de la Información (PETI) sección 7.4 ruta de publicación en la página web de la entidad:

Transparencia: 4. Planeación, Presupuesto e Informes | Fondo de Prestaciones Económicas, Cesantías y Pensiones | FONCEP

Sede Principal

Carrera 6 Nro. 14-98

Edificio Condominio Parque Santander

Teléfono: +571 307 62 00 || www.foncep.gov.co



FONDO DE
PRESTACIONES ECONÓMICAS,
CESANTÍAS Y PENSIONES

11. Roles y responsabilidades de Seguridad y privacidad de la Información

11.1 Organigrama FONCEP

El Organigrama de FONCEP establece la ubicación de la Oficina de Informática y Sistemas, responsable de la seguridad de la información, como se muestra a continuación:



Ilustración 6 Ilustración 5 Organigrama FONCEP.

Fuente: <https://www.FONCEP.gov.co/transparencia/organizacion>

Sede Principal

Carrera 6 Nro. 14-98

Edificio Condominio Parque Santander

Teléfono: +571 307 62 00 || www.foncep.gov.co



FONDO DE
PRESTACIONES ECONÓMICAS,
CESANTÍAS Y PENSIONES

11.2 Roles y responsabilidades

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

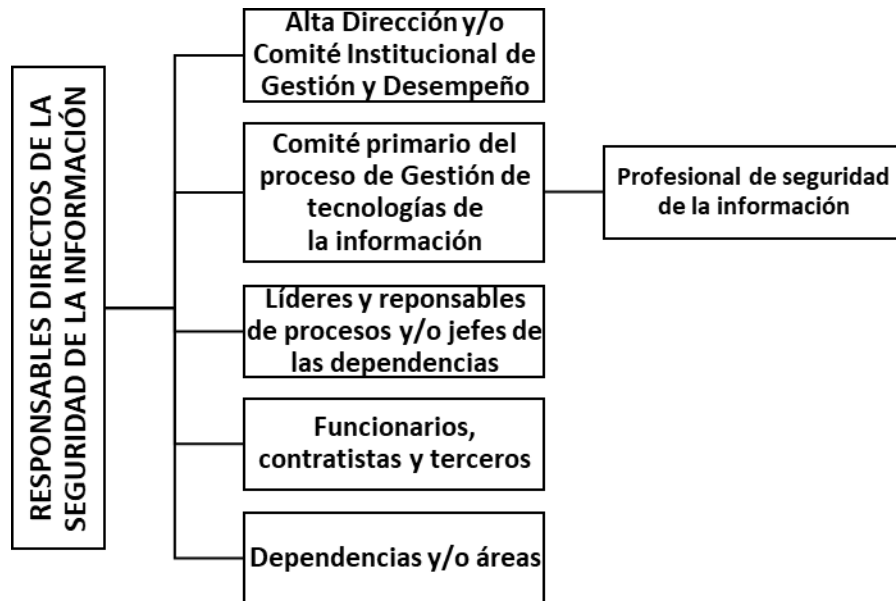


Ilustración 7 Responsables seguridad de la información en FONCEP

Fuente: elaboración propia

Sede Principal

Carrera 6 Nro. 14-98

Edificio Condominio Parque Santander

Teléfono: +571 307 62 00 || www.foncep.gov.co



FONDO DE
PRESTACIONES ECONÓMICAS,
CESANTÍAS Y PENSIONES

Roles	Responsabilidades y Funciones
Alta Dirección y/o Comité Institucional de Gestión y Desempeño	<ul style="list-style-type: none"> • Garantizar que la seguridad de la información tenga los lineamientos necesarios y pertinentes para la protección de los activos de información y se aplique en la Entidad. • Velar por la protección de la información que se gestiona en las dependencias, vigilando en primera instancia la propia de acuerdo con las políticas y normas de seguridad de la información del FONCEP, al igual que realizar el levantamiento de los activos de información de cada una de sus áreas y/o dependencias. • La Dirección General es la encargada de dar los lineamientos de la política de seguridad de la información y delega las responsabilidades de documentación sobre seguridad de la información a la persona responsable quien se apoya en la Oficina de Informática y Sistemas para las definiciones y modificaciones que pueda requerir esta política con el transcurso del tiempo. Cualquier cambio a la política debe ser revisada por la Dirección General, Líder de Proceso de gestión de tecnologías de la información y el profesional de seguridad de la información , en los casos que aplique, y aprobada mediante las disposiciones del procedimiento de administración de los elementos de planeación y gestión que establece la Entidad. • Aprobar el Plan de Acción Institucional, el cual contiene el plan seguridad y privacidad de la información, tratamiento de riesgos de seguridad de la información, actividades relacionadas con políticas de gobierno y seguridad digitales. • Apoyar y poner a disposición los recursos necesarios para la • implementación y aplicación del Modelo MSPI.

Roles	Responsabilidades y Funciones
Comité primario del proceso de Gestión de tecnologías de la información	<ul style="list-style-type: none"> • Proporcionar los servicios de TI en forma oportuna, completa y segura logrando que dichos servicios estén protegidos contra accesos no autorizados estableciendo los controles necesarios y mecanismos de control de acceso lógico. • Brindar el acceso a la información y a los recursos informáticos de la Entidad solicitado y aprobado por el jefe del área de la dependencia. • Está encargado de dar los lineamientos y metodologías para elaborar y actualizar las políticas, normas, pautas y procedimientos relativos a seguridad de la información. • Responsable de coordinar el análisis de riesgos, indicadores estratégicos y de proceso, seguimiento a las actividades del Plan de acción Institucional, Plan de seguridad y privacidad de la información, Plan de tratamiento de riesgos de seguridad y privacidad de la información y Plan Estratégico de las Tecnologías de la Información y Comunicaciones. • Efectuar la evaluación y revisión de la situación de FONCEP en cuanto a seguridad de la información, incluyendo el análisis de incidentes ocurridos y que afecten la seguridad. • Coordinar la implementación y aplicación del Modelo de Seguridad y privacidad de la Información - MSPI. • Velar por la aplicación y cumplimiento de la política de seguridad digital en FONCEP. • Revisar los diagnósticos del estado de la seguridad de la información en nombre de la Entidad. • Plasmar las necesidades de seguridad. • Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de FONCEP. • Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar, riesgos. • Realizar revisiones periódicas del MSPI y según los resultados de esta revisión definir las acciones pertinentes. Promover la difusión y sensibilización de la seguridad de la información dentro de la Entidad. • Poner en conocimiento de la Entidad, los documentos generados al interior del proceso de gestión de tecnologías de la información que impacten de manera transversal a la misma. • Salvaguardar el código fuente de las aplicaciones o sistemas de información con control de acceso y restricción de privilegios. • Realizar campañas de seguridad de la información para los colaboradores del FONCEP.

Roles	Responsabilidades y Funciones
Profesional de seguridad de la información	<ul style="list-style-type: none"> • Apoyar en el seguimiento y monitoreo, de las herramientas, equipos y componentes que hacen parte de la infraestructura de ciberseguridad y de seguridad de la información de FONCEP, así como en la elaboración y actualización de la documentación relacionada con los componentes de infraestructura de ciberseguridad y de seguridad de la información de FONCEP. • Brindar apoyo en la realización de la parametrización y ajustes necesarios a la infraestructura de ciber seguridad y de seguridad de la información con que cuenta el FONCEP, cumpliendo con los lineamientos de la Oficina de Informática y de Sistemas. • Brindar apoyo en el seguimiento permanente de la infraestructura y proponer mejoras para su validación y gestión, proyectando documentos de carácter técnico tendientes a mejorar el rendimiento de los elementos administrados. • Brindar apoyo en la gestión y monitoreo del uso de las VPN asignadas a los usuarios autorizados dentro del FONCEP. • Revisar, monitorear, tomar medidas y acciones preventivas y correctivas, en los casos que se considere afectado el funcionamiento y desempeño de la plataforma de telecomunicaciones. • Apoyar en la evaluación y mantener actualizados los componentes de la infraestructura de ciberseguridad y de seguridad de la información con que cuenta el FONCEP a nivel de firmware. • Mantener Backup de las configuraciones de los equipos de comunicaciones administrados y socializarlos al líder de infraestructura de forma periódica. • Elaborar los diagnósticos del estado de la seguridad de la información en nombre de la Entidad.
Líderes y responsables de procesos y/o jefes de las dependencias	<ul style="list-style-type: none"> • Definir los roles tecnológicos que se le deben asignar a cada uno de los usuarios de su dependencia, realizar el seguimiento adecuado, solicitar las modificaciones cuando sea necesario y el retiro cuando el usuario deje de pertenecer a la Entidad o tenga un cambio de dependencia. • Realizar la aprobación de cambios referente a los servicios ofrecidos por la Oficina de Informática y Sistemas, así como la definición de usuarios que podrán acceder a los sistemas y los niveles de accesos otorgados a cada usuario para el cumplimiento de sus funciones. • Realizar la identificación y actualización de los activos de información de cada uno de los procesos de la Entidad. • Liderar la actualización de los riesgos de seguridad asociados a su proceso.

Roles	Responsabilidades y Funciones
	<ul style="list-style-type: none"> • Velar por el cumplimiento de los controles establecidos sobre los activos de la información a su cargo. • Realizar seguimiento a las acciones de tratamiento de los riesgos de seguridad de la información a su cargo. • Los jefes de las áreas y/o dependencias de la Entidad son los responsables de definir los roles que se le deben asignar a cada uno de los usuarios de su dependencia, realizar el seguimiento adecuado, solicitar las modificaciones cuando sea necesario y el retiro cuando el usuario deje de pertenecer a la Entidad. • Cada dependencia y/o área verifica y dará uso a los documentos, procedimientos, manuales, instructivos y formatos del proceso de gestión de tecnologías de la información.
Funcionarios, contratistas y terceros	<ul style="list-style-type: none"> • Son todos aquellos que prestan algún servicio profesional a la Entidad y que en algunos casos tendrán acceso a la información y a los activos tecnológicos de la Entidad, para la ejecución de sus labores profesionales según los compromisos adquiridos con FONCEP. • Acatar las cláusulas de confidencialidad con la Entidad cuando requieran conocer, acceder o manejar información confidencial. • Reportar los incidentes de seguridad, eventos sospechosos y/o el mal uso de los recursos institucionales de los cuales tenga conocimiento. • Es responsabilidad de toda persona vinculada a la Entidad conocer y aplicar la política de seguridad de la información. • Los funcionarios y contratistas deben dar uso adecuado de los recursos asignados (equipos de cómputo, impresoras, puesto de trabajo, software, entre otros) y/o servicios informáticos (cuentas de usuario, carpetas compartidas, correo electrónico institucional, intranet, internet, datos e información, sistemas de información, entre otros) de acuerdo con las normas y procedimientos establecidos por la Entidad. • Los funcionarios y contratistas deben proteger y no transferir el usuario y la contraseña asignada por la Entidad a otra persona o funcionario, ni utilizar otra cuenta de usuario para el ingreso a los recursos de la Entidad y responder por todas las operaciones efectuadas y la información registrada con esta cuenta de usuario. • No se permite conectar a la red o instalar dispositivos (móviles o fijos tales como portátiles, celulares, tabletas, teléfonos inteligentes, enrutadores, agendas electrónicas, puntos de acceso inalámbrico) que no sean autorizados por la Oficina de Informática y Sistemas o el director o jefe del área o dependencia a la quien pertenezca el usuario.

Roles	Responsabilidades y Funciones
	<ul style="list-style-type: none"> La conexión remota a la red de área local de la Entidad debe ser hecha a través de una conexión segura y será solicitada por el jefe del área que la requiera y validada y asignada por la Oficina de Informática y Sistemas.
<p>Dependencias y/o áreas</p>	<ul style="list-style-type: none"> El área de Talento Humano está encargada de la contratación de los profesionales o la vinculación de funcionarios y personal de planta idóneos. Al momento de la vinculación de los colaboradores de la Entidad aceptan el cumplimiento de la política general de seguridad de la información, así como, los lineamientos relacionados. La Subdirección Jurídica, está encargada de los contratos y validar que en ellos se estipule el cumplimiento de la política general de seguridad de información. La Oficina de Control Interno valida y comunica la información en los informes trimestrales de los riesgos de la Entidad que sirven de insumo para evaluar las falencias y hacer los ajustes correspondientes, especialmente a los riesgos de seguridad de la información. Además, la Oficina de Control Interno realiza auditorias para el seguimiento de las políticas de seguridad digital y gobierno digital. La Oficina de Informática y Sistemas como segunda línea de defensa realiza el monitoreo de los riesgos de seguridad de la información para identificar las materializaciones, necesidad de acciones de tratamiento y fortalecer los controles. La Subdirección Financiera y Administrativa realiza los procesos disciplinarios conforme a el hallazgo o situación de incumplimiento de la política general de seguridad de la información y lineamientos relacionados.

Tabla 3 Roles y responsabilidades Fuente: Elaboración propia

12. Definición y priorización de actividades

De acuerdo con la alineación de los dominios de la norma ISO 27001:2022 con respecto al Plan Estratégico de las Tecnologías de la Información (PETI) y los objetivos estratégicos del FONCEP, se identificaron las actividades dentro del Plan de acción Institucional relacionadas con la política de seguridad digital y Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, con el fin de contar con una arquitectura de seguridad coherente y un esquema de defensa en profundidad, que le permita a la Entidad contar con elementos que mejoren el nivel de Seguridad de la Información de esta.

13. Actividades Clave

El Plan de implementación de Seguridad y Privacidad de la Información se ejecuta de acuerdo con el siguiente cronograma, al cual se le hace seguimiento mes a mes:

Estrategia	Gestión	Actividades	Tareas	Responsable de la Tarea	Evidencia	Fechas Programación Tareas	
						FechaInicio	FechaFinal
Seguridad de la Información Privacidad y Datos Personales Seguridad Digital Seguridad de Datos Transparencia y Control de Acceso	Gestión Activos de Información	Definir lineamientos para el levantamiento de activos de información	Enviar comunicación a todos los líderes de las dependencias del FONCEP, solicitando a los gestores designados que se realice el levantamiento de información de su correspondiente área.	Equipo OIS/Planeación	Comunicación SIDEAF	01-jul-2026	30-ago-2026
		Consolidar la actualización del inventario de activos de la información con el fin de realizar una correcta gestión de los riesgos de seguridad de la información	Actualización del inventario de activos de información por alguna de las siguientes novedades: Actualizaciones al proceso al que pertenece el activo, Adición de actividades al proceso, Inclusión de un nuevo activo, Cambios o migraciones de sistemas de información en donde se almacenan o reposan activos de la ubicación ya inventariados, Materialización de riesgos que cambian la criticidad del activo.	Gestores de cada proceso	Correo electrónico, (Formato Diligenciado)	1-sep-2026	30-oct-2026
		Publicación de Activos de Información	Validar y aceptar los activos de información para su publicación en SVE por cada líder de proceso.	Enlace de cada proceso, Equipo OIS	Memorando de aceptación	1-sep-2026	30-oct-2026
	Gestión de Riesgos	Actualización de lineamientos de riesgos	Apoyar cuando se requiera la actualización de la política, metodología y lineamientos de la gestión de riesgos	Equipo de Gestión de Riesgos	Correos electrónicos, Documentación actualizada en SVE	01-08-2026	30-sep-2026
		Sensibilización	Socialización de lineamientos y herramienta para la Gestión de Riesgos de Seguridad y privacidad de la Información y Seguridad Digital	Equipo de Gestión de Riesgos	Listas de asistencia, (Correos electrónicos)	01-ago-2026	30-ago-2026
		Seguimiento Fase de Tratamiento	Esta actividad hace referencia al seguimiento que se realiza trimestralmente en el comité primario al cumplimiento de los controles establecidos para el riesgo "Posibilidad de recibir dación o beneficio a nombre propio o de un tercero en la entrega, uso, alteración o modificación indebida de las bases de datos."	Equipo de Gestión de Riesgos	Seguimiento mapas de riesgos, seguimiento plan operativo	01-mar-2026	15-ago-2026

Sede Principal

Carrera 6 Nro. 14-98

Edificio Condominio Parque Santander

Teléfono: +571 307 62 00 || www.foncep.gov.co



FONDO DE PRESTACIONES ECONÓMICAS, CESANTÍAS Y PENSIONES

		Gestionar los incidentes y/o ataques de Seguridad de la Información identificados	Realizar un informe de los ataques además del seguimiento a los incidentes de seguridad de la información reportados a la mesa de servicio de acuerdo con lo establecido en el procedimiento definido.	Especialistas OTI - Gestión de seguridad y Privacidad de la Información	Correos electrónicos, seguimiento al reporte de incidentes	01-sep-2026	15-nov-2026
		Eventos/ vulnerabilidades	Realizar seguimiento a los informes de eventos y vulnerabilidades asociados a CIRST SGSI	Profesional de la OIS, encargado de la Gestión de Incidentes de Seguridad de la Información.	correos electrónicos	01-sep-2026	30-nov-2026
	Plan de Continuidad del Negocio.	Documentación de Valoración de Riesgos de Interrupción	Revisar y/o actualizar el documento de Valoración de Riesgos de interrupción para el plan de continuidad de la operación - BIA	Equipo de Continuidad del Negocio	Documento Valoración de Riesgos de interrupción para el plan de continuidad de la operación actualizado en SVE	01-jun-2026	30-ago-2026
	Implementación de estrategias de continuidad	Documentación de Estrategias de Continuidad	Realizar prueba integral sobre la plataforma tecnológica del DRP.	Equipo de Continuidad del Negocio	Documento Estrategias de Continuidad de la Operación actualizado en SVE	01-sep-2026	30-oct-2026
		Documentación del Plan de continuidad de la Operación	Realizar prueba piloto de pruebas de recuperación de sistemas de información.	Equipo de Continuidad del Negocio	Documento del Plan de continuidad de la Operación	01-oct-2026	30-nov-2026

Tabla 4 Actividades PESI priorizadas 2026

HOJA DE RUTA PROYECTOS DE TI

Para las actividades claves establecidas en el PESI, se han establecido una serie de actividades en el Plan de Acción 2026 por cada ítem de gestión, a ser desarrollados durante la vigencia:

Gestión	Nombre de la actividad	Descripción de la actividad	Fecha inicial	Fecha final
Activos de Información	Levantamiento de activos de información, en todas las áreas del FONCEP.	Enviar comunicación a todos los líderes de las dependencias del FONCEP, solicitando a los gestores designados el levantamiento de información de su correspondiente área.	01/07/2026	30/08/2026

Sede Principal

Carrera 6 Nro. 14-98

Edificio Condominio Parque Santander

Teléfono: +571 307 62 00 || www.foncep.gov.co

**FONDO DE
PRESTACIONES ECONÓMICAS,
CESANTÍAS Y PENSIONES**

	Consolidar la actualización del inventario de activos de la información con el fin de realizar una correcta gestión de los riesgos de seguridad de la información	Es necesaria consolidar la actualización del inventario de activos de la información, para tener claridad de los cambios que se deben implementar los riesgos de seguridad de la información, proteger los activos teniendo en cuenta la confidencialidad, integridad, disponibilidad y privacidad de los datos, y así se implemente la Resolución No. DG - 00072 del 29 de septiembre de 2022 de la política general de la seguridad de la información y los lineamientos asociados	01/09/2026	30/10/2026
	Publicación de los activos de información	Validar y aceptar los activos de información para su publicación en los sitios de web del FONCEP y en el Portal de datos abiertos.	01/09/2026	30/10/2026
Gestión de Riesgos	Realizar la actualización de los ajustes de los riesgos de la seguridad de la información	Esta actividad corresponde a realizar la revisión de las solicitudes de ajustes a los riesgos de seguridad de la información de los procesos de FONCEP, acorde a los lineamientos establecidos, y aprobar los ajustes necesarios de acuerdo con la actualización de los activos de la información, cumpliendo con el rol de segunda línea de defensa.	01/08/2026	30/09/2026
	Realizar sensibilización y/o socialización sobre la gestión de riesgos de seguridad de la información.	Realizar capacitaciones o sensibilizaciones en temas relacionados con seguridad de la información a los colaboradores del FONCEP, para contribuir a la protección de los activos de información.	01/08/2026	30/08/2026
	Realizar seguimiento en el comité primario al cumplimiento de los controles establecidos para el riesgo.	Esta actividad hace referencia al seguimiento que se realiza trimestralmente en el comité primario al cumplimiento de los controles establecidos para el riesgo "Posibilidad de recibir dativa o beneficio a nombre propio o de un tercero en la entrega, uso, alteración o modificación indebida de las bases de datos."	03/03/2026	15/12/2026
	Gestionar los incidentes y/o ataques de Seguridad de la Información identificados	Realizar un informe de los ataques además del seguimiento a los incidentes de seguridad de la información reportados a la mesa de servicio de acuerdo con lo establecido en el procedimiento definido. notificación obligatoria a COLCERT y CSIRT-PONAL, y la clasificación por severidad (Baja, Media, Alta, Crítica) definida en el nuevo procedimiento de incidentes.	01/09/2026	15/11/2026
	Realizar análisis de los eventos / vulnerabilidades del FONCEP	Esta actividad junto con la participación del CSIRT Gobierno o ColCert o un CSIRT sectorial permite analizar las probables amenazas con las que cuenta el FONCEP.	01/09/2026	30/11/2026

Plan de Continuidad del Negocio	Realizar la actualización del plan de continuidad del negocio	Llevar a cabo la actualización del plan de continuidad de negocio con la finalidad de establecer el paso a paso para responder frente a una interrupción y así reanudar, recuperar y restaurar la operación de manera oportuna la prestación del servicio, de acuerdo con los objetivos de continuidad de la entidad, este plan deberá contener el análisis de impacto plan de respuesta y recuperación.	03/02/2026	30/11/2026
Implementación de estrategias de continuidad	Realizar prueba integral sobre la plataforma tecnológica del DRP.	Esta actividad corresponde a realizar la prueba integral sobre la plataforma tecnológica del DRP implementada en la nube de Oracle, con la finalidad de identificar el tiempo requerido para recuperar el servicio ante un desastre.	01/09/2026	30/10/2026
	Realizar prueba piloto de pruebas de recuperación de sistemas de información.	Esta actividad corresponde a realizar una prueba piloto sobre un sistema de información designado por la OIS	01/10/2026	30/11/2026

Tabla 5 Hoja de ruta proyectos 2026

CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DE LA MODIFICACIÓN
		Creación y adopción del documento.
1	Noviembre 2022	Se asocia al nuevo proceso adoptado, la aprobación se realizó mediante Comité Institucional de Gestión y Desempeño en la sesión 04 del 25 de octubre de 2022. Reemplaza el DCO-APO-GST-002 Plan estratégico de seguridad y privacidad de la información:
		<ul style="list-style-type: none"> - 001 de enero de 2022. Creación del documento. - 002 de mayo de 2022. Se anexó la normatividad relacionada y se actualizo el Marco Estratégico. - 003 de noviembre de 2022. Se actualiza la información estratégica.
2	Mayo 2024	<ul style="list-style-type: none"> - Se actualizó el organigrama de FONCEP y la ilustración de - riesgos por clase.
3	Noviembre 2024	<ul style="list-style-type: none"> - Se actualizó el organigrama de FONCEP - Se actualizo la tabla de responsabilidades, así como también las estrategias y normativa correspondiente
4	Diciembre 2025	<ul style="list-style-type: none"> - Actualización integral para alinear el PESI con el MSPI 2025, incluyendo la nueva Hoja de Ruta de proyectos, el manual de lineamientos bajo ISO 27001:2022. - Actualización normativa - Actualización de acuerdo con el MSPI (2025)