



COMUNICACIÓN INTERNA

PARA: SERGIO CORTES RINCON

Director General
Dirección General

JACKELINE DE LEON WILLIS

Subdirectora Financiera y Administrativa - Subdirección Financiera y
Administrativa

ANDREA MARCELA RINCON C

Subdirectora de Prestaciones Economicas - Subdirección de Prestaciones
Económicas

ANGELICA VALDERRAMA MUÑOZ

Subdirectora Jurídica - Subdirección Jurídica

MILENA DEL PILAR SANDOVAL GOMEZ

Jefe Oficina - Oficina de Informática y Sistemas

JOAQUIN MANUEL GRANADOS RODRIGUEZ

Jefe Oficina - Oficina Asesora de Planeación

JOAQUIN MANUEL GRANADOS RODRIGUEZ

Asesor (E) - Grupo Comunicaciones y Servicio al ciudadano

DE: ALEXANDRA YOMAYUZA CARTAGENA

Jefe Oficina
Oficina Asesora de Control Interno

ASUNTO: Informe final de auditoría al cumplimiento de las disposiciones vigentes de Gobierno Digital, Seguridad Digital y Protección de datos personales.

En desarrollo del plan anual de auditorías de FONCEP de la vigencia 2024, la Oficina de Control Interno realizó auditoría al cumplimiento de las disposiciones vigentes de Gobierno Digital, Seguridad Digital y Protección de datos personales en el marco del Modelo Integrado de Planeación y Gestión – MIPG, al corte de la vigencia 2023 y el avance entre enero y septiembre de 2024, cuyos resultados se dan a conocer en el documento adjunto.

A partir de los resultados del presente informe, se observó que el sistema de control interno asociado al cumplimiento de las disposiciones de gobierno digital, seguridad digital y protección de datos personales es susceptible de mejora, en la medida que se implementen las siguientes recomendaciones y se reformule el plan de mejoramiento frente a las situaciones evidencias en el informe.

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

- Realizar los ajustes técnicos requeridos en la página web de la entidad para dar cumplimiento al criterio web de la resolución 1519 de 2020 del MinTIC “*CC15. Advertencias bien ubicadas*”, para que el ciudadano visualice correctamente las alertas de formularios.
- Establecer un control que permita actualizar los documentos en datos abiertos acorde con las últimas versiones emitidas y publicadas por la entidad.
- Continuar con la aplicación de las encuestas para determinar la publicación y uso de datos abiertos, analizar sus respuestas y tomar acciones de acuerdo con las recomendaciones y observaciones recopiladas.
- Realizar semestralmente ejercicios de aprovechamiento de datos abiertos que fortalezcan la rendición de cuentas, incentiven la participación ciudadana y mejoren la innovación pública, de acuerdo con lo establecido en el anexo técnico de la circular 064 de 2021.
- Documentar los procesos de interoperabilidad internos y con otras entidades y definir un plan de contingencia en el caso de fallas en el servicio.
- Avanzar en la etapa de planeación de automatización de trámites, revisar los trámites y reportar los que no se puedan digitalizar, con el fin de dar cumplimiento a los términos establecidos en el decreto 088 de 2022.
- Continuar con las acciones necesarias para la publicación en la carpeta ciudadana de los trámites del FONCEP, de acuerdo con la normatividad vigente.
- Avanzar en la implementación de tecnologías de la cuarta revolución industrial que faciliten la interacción con otras entidades del Estado y la prestación de servicios del FONCEP.
- Actualizar el documento manual de arquitectura continuidad y catálogo de servicios para eventos de contingencias DRP.
- Establecer controles de acuerdo con el resultado del autodiagnóstico de seguridad de la información, así como las recomendaciones de la OCI incluidas en la Tabla 1- Verificación controles MSPI.
- Implementar los indicadores de seguridad y privacidad de la información para la mejora continua, de acuerdo con el anexo 1 del Modelo de Seguridad y Privacidad de la Información del MinTIC.
- Actualizar el “Formato de designación para sustitución provisional – ley 1204 de 2008 código FOR-MIS-GRP-019 de 2020” para incluir la política de tratamiento de datos personales de FONCEP.
- Establecer de manera clara los responsables de seguridad de la información y de protección de datos personales, indicando cargo y funciones para la administración y custodia de datos.
- Fortalecer el control “Asegurar el adecuado seguimiento a los requerimientos e incidencias de software, infraestructura, pcs y periféricos” establecido para evitar la posible materialización del riesgo “Recursos tecnológicos gestionados incumpliendo los objetivos del proceso”.



- Reformular el plan de mejoramiento frente a los hallazgos formulados por la OCI en el informe radicado ID 551266 del 27 de julio de 2023, de tal manera que permita subsanar la causa raíz identificada.

Cordialmente

Firmado Electrónicamente

por ALEXANDRA YOMAYUZA CARTAGENA

Fecha: 2024-10-31 10:00

d6fb2d91afb8d14b30edb042809f949c922bde8fc8e96d8334d65dbf902b0dcb

ALEXANDRA YOMAYUZA CARTAGENA
Jefe de Oficina de Control Interno

ALEXANDRA YOMAYUZA CARTAGENA
Jefe Oficina
Oficina Asesora de Control Interno

Actividad	Nombre	Cargo	Dependencia	Firma
Revisó	CESAR AUGUSTO FRANCO VARGAS	Contratista	Oficina Asesora de Control Interno	
Proyectó	GLADYS PARRA GIL	Tecnico Operativo	Oficina Asesora de Control Interno	

Documento producido automáticamente por el Sistema de Gestión de Documentos Electrónicos de Archivo del FONCEP - SIDEAF, en plena conexidad con la Resolución DG - 00024 del 14 de Abril de 2023.

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



Nombre del informe

Auditoría al cumplimiento de las disposiciones vigentes de Gobierno Digital, Seguridad Digital y Protección de datos personales.

1. Objetivo

Verificar el cumplimiento de las disposiciones vigentes de Gobierno Digital, Seguridad Digital y Protección de datos personales en el marco del Modelo Integrado de Planeación y Gestión – MIPG, al corte de la vigencia 2023 y el avance de lo adelantado durante el año 2024.

2. Alcance

Verificación de los componentes de la política de gobierno digital, gobernanza, innovación pública digital, habilitadores como arquitectura, seguridad digital, cultura y apropiación, servicios ciudadanos digitales, servicios y procesos inteligentes, decisiones basadas en datos, así como los avances en la implementación del modelo de gestión de riesgos de seguridad digital y avance en el manejo de la protección de datos personales al corte de 2023 y acciones adelantadas entre los meses de enero a septiembre de la vigencia 2024.

Adicionalmente la OCI revisó el reporte FURAG, correspondiente al año 2023 y realizado en mayo del año 2024 cuyos resultados se incluyen en el alcance de la presente auditoría respecto a las políticas de Gobierno Digital y Seguridad Digital.

3. Metodología

El seguimiento se realizó con base en el marco internacional para la práctica de la auditoría interna aplicando las técnicas de auditoría dentro de las que se incluyen la observación, análisis, evaluación y verificación de la información remitida por la Oficina de Informática y Sistemas – OIS y la verificada directamente por la Oficina de Control Interno - OCI para la generación del presente informe.

Se consultaron las siguientes fuentes de información: Suite Visión Empresarial - SVE, la página web del FONCEP, lo reportado en el aplicativo FURAG y demás herramientas que permitieron evidenciar la aplicación de la política de gobierno digital en la entidad, así como la información suministrada por la Oficina de Informática y Sistemas.

Mediante el radicado 3-2024-06313 de 21 de agosto de 2024 la OCI solicitó información a la Oficina de Informática y Sistemas respecto a los componentes de la política de gobierno y seguridad digital, así como el tratamiento de datos personales en el interior del FONCEP, esta solicitud fue contestada por la OIS el día 2 de septiembre de 2024 mediante el radicado 3-2024-06597.

El informe preliminar fue comunicado mediante el radicado 3-2024-08229 del 25 de octubre de 2024, frente al cual no se recibieron observaciones por parte de la Oficina de Informática y Sistemas.

4. Marco Normativo

- Ley 1712 de 06 de marzo de 2014 mediante la cual “Se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”.

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



- Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales.
- Decreto 767 de 2022 “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 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”
- Decreto 088 de 2022 “Por el cual se adiciona el Título 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los artículos 3, 5 Y 6 de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea
- Decreto 189 de 2020 “Por el cual se expiden lineamientos generales sobre transparencia, integridad y medidas anticorrupción en las entidades y organismos del orden distrital y se dictan otras disposiciones”
- Decreto 1008 de 14 de junio de 2018 que define los lineamientos, estándares y acciones a ejecutar por parte de los sujetos obligados de esta Política de Gobierno Digital.
- Decreto 1078 de 2015 único reglamentario del sector de las TIC.
- Resolución 1519 de 2020 “Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.”
- Manual de Gobierno Digital MinTIC vigente
- Directiva 05 de 2020 “Directrices sobre gobierno abierto de Bogotá”
- Resolución 1117 de 2022 “Por la cual se establecen los lineamientos de transformación digital para las estrategias de ciudades y territorios inteligentes de las entidades territoriales, en el marco de la Política de Gobierno Digital.
- Resolución 1126 de 2021 que modifica la resolución 2710 de 2017 Por la cual se establecen los lineamientos para la adopción del protocolo IPv6
- Lineamientos y metodologías en usabilidad para Gobierno en línea.
- Norma Técnica Colombiana NTC 5854
- ISO.27001:2022
- ISO 27032:2012

5 Resultados

5.1 Componentes de Gobierno Digital implementados en la entidad

Para el presente informe se tuvo en cuenta lo establecido en el manual de Gobierno Digital Interactivo establecido en la página web del Ministerio de las TIC en el enlace <https://gobiernodigital.mintic.gov.co/portal/Manual-de-Gobierno-Digital/>, acorde con el decreto 767 de 2022 “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 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones” en el cual se analizan los siguientes elementos:

Sede Principal

Carrera 6 Nro. 14-98

Edificio Condominio Parque Santander

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



ALCALDÍA MAYOR
DE BOGOTÁ D.C.

FONDO DE
PRESTACIONES ECONÓMICAS,
CESANTÍAS Y PENSIONES



5.1.1 Gobernanza

Tiene como objetivo desarrollar la implementación de la Política de Gobierno Digital bajo un modelo de gobernanza basado en el relacionamiento entre el orden nacional y territorial, y el nivel central y descentralizado involucrando a los grupos de interés en la toma de decisiones.

En lo referente a este componente de Gobierno Digital, la OCI verificó los siguientes elementos:

Accesibilidad: de acuerdo con el MinTIC en el contexto colombiano, ha venido asumiéndose como las condiciones que se incorporan en sitios y herramientas web que favorecen el que usuarios en condiciones de deficiencia tecnológica, física o sensorial o en condiciones particulares de entornos difíciles o no apropiados, puedan hacer uso de estos recursos de la Web.

Al respecto, la OCI observó que en la página web de la entidad se encuentra la certificación del cumplimiento de los criterios de accesibilidad establecidos en la Matriz de Transparencia y Acceso a la Información Pública (ITA) de fecha 26 de julio de 2024 firmada por el Asesor de Comunicaciones y Servicio al Ciudadano (E), así como la Jefe de la Oficina de Informática y Sistemas. Pese a lo anterior se evidenció que en el documento publicado en la página web de la entidad no está certificado el aspecto de la matriz “e. *¿Los formularios o casillas de información tienen advertencias e instrucciones claras con varios canales sensoriales (p. ej. Campos con asterisco obligatorios, colores, ayuda sonora, mayúscula sostenida)?*”, el cual se observó parcialmente implementado y que de acuerdo con el informe de diagnóstico del cumplimiento de los criterios de accesibilidad y usabilidad web del desarrollo del contrato 156 de 2024 en el aspecto “CC15. Advertencias bien ubicadas” hace falta realizar ajustes técnicos para que del lado del cliente se visualicen correctamente las alertas de formularios, por lo que **se recomienda** revisar el criterio faltante y tomar las medidas para su total implementación.

Por otro lado, la OCI verificó que la página web de la entidad ofrece opciones de contraste, tamaño de letras, y centro de relevo que direcciona a la página del MinTIC al momento de ser requerido. También se evidenció mediante una muestra no estadística que los documentos PDF, y Excel verificados permiten la lectura y toma de información para ser reutilizable o para lectura en caso de discapacidad visual.

Como parte de los informes presentados por la Oficina de Informática y Sistemas de los criterios de accesibilidad, se observó el cumplimiento de accesibilidad AA, pero al ser de gran importancia garantizar el acceso universal y continuo de los usuarios, **se recomienda** continuar con la implementación y mejoras en los aspectos de accesibilidad hasta llegar al nivel “AAA”.

Datos abiertos: Hace referencia a los datos primarios que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización de forma libre y sin restricciones.

La OCI evidenció respecto a este componente que en la página web de FONCEP, en el numeral 7 del vínculo de transparencia y acceso a la información pública se encuentran publicados los datos abiertos de los documentos requeridos conforme con el anexo 2 de la resolución 1519 de 2020 y la matriz ITA de medición de transparencia y acceso a la información pública en las entidades públicas, no obstante al revisar las páginas web <https://www.datos.gov.co/> y <https://datosabiertos.bogota.gov.co/> los archivos publicados en las bases de datos abiertos no corresponden con la última versión publicada en la página web de la entidad por lo que **se**

Sede Principal

Carrera 6 Nro. 14-98

Edificio Condominio Parque Santander

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



ALCALDÍA MAYOR
DE BOGOTÁ D.C.

FONDO DE
PRESTACIONES ECONÓMICAS,
CESANTÍAS Y PENSIONES



recomienda mantener un control que permita actualizar los documentos en datos abiertos acorde con las últimas versiones emitidas y publicadas por la entidad.

De otro lado se observó que en el espacio de datos abiertos de la página web de la entidad en el numeral 7, se estableció una encuesta de uso y satisfacción de datos abiertos, la cual al momento de la revisión del presente informe el formulario se encontraba como inexistente, imposibilitando a los visitantes para calificar y/u opinar con relación a estos datos, por lo que **se recomienda** mantener la encuesta habilitada con respecto al uso y satisfacción de datos abiertos, y establecer un enlace a Bogotá Te Escucha con instrucciones para que los ciudadanos puedan solicitar nuevos datos abiertos de acuerdo con lo establecido en el anexo técnico de la circular 064 de 2021.

Con relación a los ejercicios de aprovechamiento de datos, la Oficina de Control Interno evidenció que durante los días 08 y 12 de abril de 2024 se realizó una encuesta con relación al conocimiento y uso de datos abiertos en la entidad, en esta actividad se evidenció la participación de 44 personas entre las que se incluyen ciudadanos y servidores de la entidad. En el resultado del ejercicio se observó que hay un alto desconocimiento de los datos abiertos y lugares de consulta de los mismos, por lo que **se recomienda** continuar con la aplicación de las encuestas, analizar sus respuestas y tomar acciones de acuerdo con las recomendaciones y observaciones recopiladas y tener en cuenta lo establecido en el anexo técnico de la circular 064 de 2021 “*Guía orientadora para la implementación de la Directiva 005 de 2021 - Datos Abiertos*” en lo referente a la realización semestral de ejercicios de aprovechamiento de datos abiertos que fortalezcan la rendición de cuentas, incentiven la participación ciudadana y mejoren la innovación pública.

En lo referente al cumplimiento de lo establecido en la Guía para el uso y aprovechamiento de datos abiertos en Colombia versión 7 agosto de 2021, la OCI observó la existencia del plan de apertura, mejora y uso de datos que está publicado en suite visión empresarial Código: DCO-APO-GTI-003 Versión: 004 de diciembre de 2023 con definiciones y actividades planteadas para el año 2023 y 2024, así como la capacitación que se realizó en el mes de abril de 2024 para los servidores de la entidad. Se **recomienda** socializar el contenido del documento y establecer estrategias para el aprovechamiento de datos en el plan de apertura y uso de datos abiertos, con la programación de actividades del año.

Interoperabilidad: Esta característica se encuentra definida como el ejercicio de colaboración entre organizaciones para intercambiar información y conocimiento en el marco de sus procesos de negocio, con el propósito de facilitar la entrega de servicios en línea a ciudadanos, empresas y a otras entidades. (Marco de Interoperabilidad para el Gobierno en línea, Versión 2010).

Al respecto de este componente se observó el informe denominado “Mecanismos de Interoperabilidad Implementados en FONCEP con otras Entidades de septiembre 2024, en este se evidencia el funcionamiento de la interoperabilidad de la Oficina Virtual y de los servicios de consulta:

- a. **Registraduría Nacional del estado Civil:** De acuerdo con esta aplicación se puede revisar la base de los fallecidos y otros datos, en caso de falla se reporta mediante el aplicativo GLPI, y tiene como contingencia la consulta mediante Secretaría de Salud y Ministerio de Salud donde se manejan archivos RUAF.
- b. **Fiduoccidente:** Mediante esta interoperabilidad se pueden generar y cancelar los pagos concernientes a las Cuotas partes pensionales. El reporte de falla lo realiza el área de Tesorería notifica cualquier novedad sobre la no operabilidad del servicio y es FIDUOCCIDENTE quien se encarga de revisar y restablecer



el servicio. En caso de contingencia, las entidades cuotapartistas pueden generar la factura con código de barras y realizar los pagos en el Banco de Occidente.

- a. **Cesantías:** A través de la Oficina Virtual de la Página WEB del FONCEP, las entidades distritales que manejan actualmente cesantías retroactivas con FONCEP, pueden tener acceso a trámites relacionados con cesantías. En caso de falla se reporta mediante herramienta GLPI. Como medida de contingencia tiene a disposición del área de Cesantías la Aplicación Misional de Cesantías, a través de la cual pueden cargar las nóminas y novedades enviadas por las entidades distritales.
- a. **Historia Laboral:** Esta aplicación tiene como objeto que las entidades Adscritas al Distrito para PASIVOCOL MINISTERIO, carguen las certificaciones de los pagos de los aportes pensionales de sus empleados y los archivos evidencias de los pagos. En caso de falla se reporta mediante herramienta GLPI, no tiene plan de contingencia.
- a. **Empresa de Acueducto y Alcantarillado EAAB:** el FONCEP se encarga de la dispersión del pago de las pensiones de los Pensionados de la EAAB, la conexión y transferencia de los archivos de nómina. En caso de falla se reporta mediante GLPI o mesa de ayuda de la empresa de acueducto. No hay Plan de Contingencia asociado.

Se observó en el Plan Estratégico de Tecnologías de la Información código: DCO-APO-GST-003, versión: 003 de diciembre de 2023 menciona las 2 ramas de la Oficina Virtual y establece la operación de las mismas.

Por otra parte, se evidenció que el FONCEP durante el año 2022 implementó a nivel interno el Manual de Interoperabilidad código: MOI-APO-GTI-002 versión 001 el cual establece el modelo conceptual del marco de interoperabilidad, los sistemas de integración del modelo misional, los sistemas de integración de modelos estratégicos, y los sistemas de integración de información apoyo; no obstante, no incluyo como es el funcionamiento de la interoperabilidad con las otras entidades ni establece como se puede reportar fallas o mecanismos en caso de contingencias por lo que **se recomienda** documentar los procesos de interoperabilidad internos y con otras entidades y definir un plan de contingencia en el evento de fallas en el servicio.

Trámites: Este aspecto hace referencia al conjunto de acciones realizadas por los usuarios de la entidad para adquirir un derecho o cumplir con una obligación prevista en la ley, este inicia cuando el particular activa el aparato a través de una petición o solicitud y termina cuando la administración pública se pronuncia sobre el mismo aceptando o negando la solicitud.

Al corte del 10 de octubre de 2024, el FONCEP tiene publicados en el numeral 5 de transparencia y acceso a la información pública 26 trámites y servicios, de los cuales 7 tienen acceso por medio de la Oficina Virtual. La OCI evidenció que los 26 trámites y servicios se encuentran publicados en la página de “trámites y servicios Bogotá”, así como en la página “Gov.co”, de igual manera se evidenció la racionalización del trámite “**Novedades de nómina - Certificación de estudios**” el cual fue actualizado en la página del SUIT desde el 07 de octubre de 2024.

Respecto a la automatización de trámites en la entidad, en cumplimiento de lo establecido en el Decreto 088 de 2022, la OCI observó la realización del cronograma con las fechas de la automatización de los 26 trámites de la entidad con fechas programadas hasta el año 2027. **Se recomienda** realizar la planeación, revisar los trámites y reportar los que no se puedan digitalizar con el fin de dar cumplimiento a los términos establecidos en la normatividad vigente.

Sede Principal

Carrera 6 Nro. 14-98

Edificio Condominio Parque Santander

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



ALCALDÍA MAYOR
DE BOGOTÁ D.C.

FONDO DE
PRESTACIONES ECONÓMICAS,
CESANTÍAS Y PENSIONES



Servicios internos mediante el aplicativo GLPI: Este punto se refiere al servicio que se tiene internamente en la entidad para atender los requerimientos de los funcionarios del FONCEP en lo que respecta a servicios informáticos internos y reporte de fallas de estos.

La OCI realizó seguimiento mediante la aplicación GLPI, revisando a partir de una muestra no estadística el historial y funcionamiento de algunos de los casos reportados por este medio, encontrando los siguientes casos que no han sido cerrados a la fecha de seguimiento:

- Se observó al respecto que frente al caso incidencia ID 2024001506 de 08 de abril de 2024 relacionado con consulta de página web de MinTIC y función pública, se encuentra en estado “ESPERA” y a la fecha de seguimiento no ha tenido solución de fondo.
- En cuanto a la incidencia ID 2024002405 de 25 de mayo de 2024 relacionado certificado de Pensión se encuentra en el estado de ESPERA, y aún no se ha dado solución al caso, por lo que enviaron al proveedor para revisión.
- Se observó respecto a la ID 2024002512 de 06 de mayo de 2024 relacionada con una funcionalidad nueva en el aplicativo OP que se encuentra en “CURSO” sin solución al 15 de octubre de 2024.
- Frente a la incidencia ID 2024002407 del 25 de mayo de 2024 relacionada con cerrar actividades de notificación en SIDEAF se encuentra en curso y al 15 de octubre no ha presentado solución.

En los siguientes documentos se encuentran establecidos los términos para la atención de los requerimientos GLPI de mesa de ayuda, que en ningún caso deben exceder tres meses: Instructivo catálogo de servicios de tecnologías de la información - TI código: INS-APO-GTI-008 versión 03 de noviembre de 2023, el Procedimiento de gestión de mesa de ayuda código: PDT-APO-GTI-001 versión: 002 de octubre de 2023 y el Manual para desarrollo y soporte de software código: MOI-APO-GTI-004 versión: 002 de octubre de 2023. Al respecto, frente a la muestra seleccionada, la OCI observó incumplimiento en la oportunidad de respuesta de la mesa de ayuda frente a las disposiciones internas. Al respecto, se hace necesario **reformular el plan de mejoramiento** establecido frente al hallazgo identificado por la OCI en 2023 por incumplimiento a los términos de atención de GLPI.

De igual forma se observó que, los indicadores “ATENCIÓN A NUEVAS FUNCIONALIDADES Y MANTENIMIENTO DE SOFTWARE Y APLICATIVOS” y “ATENCIÓN DE REQUERIMIENTOS DE INFRAESTRUCTURA, PCS Y PERIFÉRICOS” presentaron al corte del 30 de septiembre de 2024 un avance del 89% y cumplimiento del 104%, frente a una meta del 85%. Entre las variables establecidas para el cálculo de los indicadores, se observan requerimientos reprogramados para ser atendidos en el periodo y de otros periodos que no se han solucionado, situación que se puede generar por la falta de efectividad del control “Asegurar el adecuado seguimiento a los requerimientos e incidencias de software, infraestructura, pcs y periféricos” asociado al riesgo “Recursos tecnológicos gestionados incumpliendo los objetivos del proceso”, al respecto, **se recomienda** fortalecer el control establecido para evitar la posible materialización del riesgo. Es de mencionar que, para el caso de la atención de nuevas funcionalidades y mantenimiento de software y aplicativos, se indica por parte de la responsable de proceso las limitaciones presentadas para la contratación del equipo de desarrolladores para la vigencia.

Carpeta Ciudadana Digital: De acuerdo con lo dispuesto en el artículo 4 de la Resolución 02160 del 23 de octubre de 2020 se estableció lo siguiente “*Estándares de implementación de los Servicios Ciudadanos Digitales contenidos en la Guía para vinculación y uso de los servicios ciudadanos digitales. Las autoridades señaladas en el artículo 2.2.17.1.2. del Decreto 1078 de 2015, deberán cumplir las condiciones y estándares establecidos en la Guía para vinculación y uso de los servicios ciudadanos digitales que se encuentran señaladas en el anexo 2 de la presente*”

Sede Principal

Carrera 6 Nro. 14-98

Edificio Condominio Parque Santander

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



ALCALDÍA MAYOR
DE BOGOTÁ D.C.

FONDO DE
PRESTACIONES ECONÓMICAS,
CESANTÍAS Y PENSIONES



resolución, para la preparación, adecuación, integración, uso y apropiación de los servicios ciudadanos digitales, a través de los cuales podrán integrar a sus sistemas de información los mecanismos de autenticación digital, interoperabilidad, carpeta ciudadana digital y vincularlos al Portal Único del Estado colombiano”.

La OCI observó que desde la Oficina Asesora de Planeación se inició el trámite con la Agencia Nacional Digital para la inclusión de los trámites en la Carpeta Ciudadana, mediante el registro de los formularios correspondientes, los cuales fueron remitidos a la Agencia en correo del 11 de septiembre de 2024, de igual manera en el mes de octubre se llevaron a cabo nuevas reuniones para adelantar la gestión y se estableció una analista para ayudar a FONCEP en el cargue de la información. **Se recomienda** continuar con el complemento de los requisitos correspondientes para la finalización y publicación en la carpeta ciudadana de los trámites del FONCEP de acuerdo con la normatividad vigente.

5.1.2 Innovación pública digital

Este elemento transversal busca desarrollar la implementación de la Política de Gobierno Digital con un enfoque transversal basado en el relacionamiento de los grupos de interés, generando valor público a través de la introducción de soluciones novedosas, creativas y que hagan uso de las Tecnologías de la Información y las Comunicaciones.

Respecto a lo establecido en el plan nacional de desarrollo 2022-2026 -Ley 2294 de 2023 como parte del objetivo de transformación digital como un motor de oportunidades e igualdad, específicamente el numeral 6: “Fortalecer el Gobierno Digital para tener una relación eficiente entre el Estado y el ciudadano, que lo acerque y le solucione sus necesidades, a través del uso de datos y de tecnologías digitales para mejorar la calidad de vida”, la OCI observó que FONCEP ha adelantado lo siguiente:

- 1.- Uso y aprovechamiento de la infraestructura de datos públicos, y datos abiertos: Al respecto se observó que el FONCEP cuenta con los datos abiertos exigidos en el numeral 7 de transparencia de acuerdo con la matriz ITA de la procuraduría y la resolución 1519 de 2020 del MinTIC, sin embargo algunos se encuentran desactualizados.
- 2.- Interoperabilidad entre los sistemas de información públicos a través de una plataforma. Con relación a este aspecto se observó que se ha adelantado la solicitud ante la Agencia Nacional Digital para la implementación de los trámites en la Carpeta Ciudadana.
- 3.- Uso de servicios de nube. Se observó que FONCEP tiene adquirido el servicio de nube donde actualmente maneja servicios, funcionamiento y seguridad a manera interna.
4. Utilización de tecnologías emergentes de la cuarta revolución industrial que faciliten la prestación de servicios del Estado a través de nuevos modelos incluyendo, pero no limitado a, tecnologías de desintermediación, DLT (Distributed Ledger Technology), análisis masivo de datos (Big data), inteligencia artificial (AI), Internet de las Cosas (IoT), Robótica y similares. Se observó la implementación del asistente virtual JOCEP en la página web de la entidad. **Se recomienda** avanzar en la implementación de las tecnologías necesarias para la interacción con otras entidades y con los ciudadanos.
5. Vinculación entre el Estado y sus usuarios a través del Portal Único del Estado colombiano. En el portal web de FONCEP se cuenta con vínculo que direcciona a Gov.co, en donde están registrados los trámites de la entidad.
6. Inclusión de programas de uso de tecnología para participación ciudadana y gobierno abierto en los procesos misionales de las entidades públicas. Al respecto de este punto la OCI observó que, en el numeral 6 de

Sede Principal

Carrera 6 Nro. 14-98

Edificio Condominio Parque Santander

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



ALCALDÍA MAYOR
DE BOGOTÁ D.C.

FONDO DE
PRESTACIONES ECONÓMICAS,
CESANTÍAS Y PENSIONES



transparencia están los parámetros de participación para los ciudadanos con los elementos estipulados en el anexo N° 2 de la Resolución 1519 de 2020 del Mintic, de igual manera se han establecido en la página web de la entidad mecanismo de participación como la plataforma FONCEP te escucha y la huella de gestión que permite observar y dar opiniones en lo referente a la rendición de cuentas en la entidad.

7. Implementación de uso de medios de pago electrónico por parte de la entidad. Se observó que la entidad cuenta con la opción de pago por medio de PSE de cuotas partes pensionales en el enlace de Oficina Virtual <https://landingfoncep.datasoftingenieria.com.co/#/>.

5.1.3 Habilitadores Transversales

Estos hacen referencia a las capacidades que les permiten a las entidades públicas ejecutar las líneas de acción de la política de gobierno digital y son:

A- **Arquitectura:** Este habilitador busca desarrollar capacidades para el fortalecimiento institucional implementando el enfoque de arquitectura empresarial en la gestión, gobierno y desarrollo de los proyectos con componentes de Tecnologías de la información.

La OCI observó los siguientes documentos en los que se establece la arquitectura de la Entidad:

- Manual de Arquitectura Empresarial MOI-APO-GTI-001 de noviembre de 2022.
- Manual de Arquitectura y Catálogo de Datos Información MOI-APO-GTI-007 de diciembre de 2022.
- Manual de arquitectura y catálogo de sistemas de información MOI-APO-GTI-003 de noviembre de 2022.
- Manual de arquitectura, continuidad y catálogo de servicios e infraestructura tecnológica MOI-APO-GTI-005 de octubre de 2023.

En los documentos se observó la descripción de la arquitectura de los sistemas de la entidad, sin embargo se encontró que no están todos los sistemas documentados, que los responsables que establecen en caso de activación de DRP y continuidad del negocio de servicios tecnológicos esta desactualizado, que aún falta complementar los bloques de construcción de los diferentes sistemas como es el caso de los aplicativos funcionales de la parte misional de la entidad en los cuales solo se observan de manera descriptiva, no permitiendo identificar su funcionamiento y arquitectura completa por elementos, y dar posible solución en caso de falencias; por lo anterior **se recomienda** revisar cada uno de los sistemas, documentarlos y completarlos identificando las posibles brechas acorde con lo establecido en los documentos hoja de ruta de arquitectura empresarial del MinTIC.

Adicional a lo anterior, de acuerdo con las recomendaciones del Furag de los últimos años tener en cuenta las siguientes recomendaciones:

- Desarrollar una hoja de ruta de arquitectura empresarial y hacer seguimiento a la implementación de la entidad.
- Actualizar las vistas de información de la arquitectura de información para todas las fuentes.
- Implementar procesos o procedimientos de calidad de datos para mejorar la gestión de los componentes de la información de la entidad.
- Implementar un plan de aseguramiento de calidad durante el ciclo de vida de los sistemas de información que incluya criterios funcionales y no funcionales.

Sede Principal

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



ALCALDÍA MAYOR
DE BOGOTÁ D.C.

FONDO DE
PRESTACIONES ECONÓMICAS,
CESANTÍAS Y PENSIONES



- Definir y aplicar una guía de estilo en el desarrollo de los sistemas de información de la entidad e incorporar los lineamientos de usabilidad definidos por el MINTIC, y las demás en el punto de fortalecimiento de arquitectura empresarial y de la gestión de T.I.

A1- Implementación del Protocolo IPv6: De acuerdo con lo informado por la Oficina de Informática y sistemas mediante el comunicado 3-2024-02339 de 14 de marzo de 2024 se menciona que de acuerdo con las pruebas realizadas la página web de FONCEP, esta cumple con los protocolos de conectividad IPv6, sin embargo en las revisiones que ha realizado la OCI en el mes de octubre de 2024 se observó que aún sigue persistiendo la falla y que algunas páginas web como es el caso de la página de MinTIC, y de función pública no funcionan por protocolo IPv6, esto de acuerdo con las pruebas realizadas en el link <https://test-ipv6.com/index.html.es>. Al respecto, **se recomienda** revisar las limitaciones que se están presentando, para no afectar el acceso a portales de entidades públicas y reformular el plan de mejoramiento establecido frente al hallazgo de la OCI en 2023, para cumplir con las disposiciones de MinTIC.

B- Cultura y apropiación: Este habilitador busca desarrollar capacidades para el acceso, uso y aprovechamiento de Tecnologías de la Información y las Comunicaciones. Busca promover el uso y apropiación de estas entre las personas en situación de discapacidad y fomenta la inclusión con enfoque diferencial.

En lo que respecta a este habilitador, la OCI el cumplimiento de los requisitos de accesibilidad web en la página de la entidad, comprobando las herramientas de ayuda con las que cuenta, y la revisión de la accesibilidad de los documentos PDF y Excel en los cuales no se encontró problemas para su acceso.

De igual manera la OCI evidenció que se incluyó vínculo a información para niños, niñas y adolescentes con contenido adicional de fácil entendimiento para ellos, información para mujeres relacionada con protección e información con enfoque diferencial para ellas relacionadas con los servicios de Secretaría de la Mujer, y la información para otros grupos de valor que tiene un calendario con las actividades de Bogotá para el interés general de cualquier ciudadano.

Para mejorar los aspectos de cultura y apropiación, el MinTIC ha realizado las siguientes recomendaciones frente al diagnóstico de gobierno digital 2023:

- Capacitar a servidores y contratistas de la entidad en temáticas de la política de gobierno digital tales como gobernanza, innovación pública, seguridad y privacidad de la información, arquitectura T.I , cultura y apropiación, servicios ciudadanos digitales, decisiones basadas en datos entre otros.
- Formular lineamientos sobre ciudades y territorios inteligentes en la entidad, teniendo en cuenta las dimensiones del modelo de madurez de ciudades y territorios inteligentes (medio ambiente, hábitat, personas, calidad de vida, desarrollo económico y gobernanza.

C- Seguridad y privacidad de la información: Este habilitador busca desarrollar capacidades a través de la implementación de los lineamientos de seguridad y privacidad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de datos.

La OCI evidenció la implementación de la política mediante los siguientes documentos:

Sede Principal

Carrera 6 Nro. 14-98

Edificio Condominio Parque Santander

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



ALCALDÍA MAYOR
DE BOGOTÁ D.C.

FONDO DE
PRESTACIONES ECONÓMICAS,
CESANTÍAS Y PENSIONES



- Política de seguridad de la información. Se observó que se encuentra publicada en la página web de la entidad en el enlace <https://www.foncep.gov.co/politicas-de-seguridad-de-la-informacion-y-proteccion-de-datos-personales>, acorde con lo establecido en el anexo 2 de la resolución 1519 del MinTIC y la matriz ITA de la Procuraduría General de la Nación.

Al respecto de esta política se observó que fue acogida mediante la resolución DG - 00072 del 29 de septiembre de 2022 y plasmada en el manual de modelo de seguridad y privacidad de la información Código: MOI-APO-GST-001 Versión: 004.

La política cumple parcialmente con la organización y elementos establecidos en la plantilla modelo del MinTIC que contiene las pautas de generación de este documento, evidenciando que no se encuentran los siguientes ítems: Compromiso de la alta dirección, capítulo de sanciones, y el de seguimiento, medición, análisis, y evaluación del SGSI, por lo que **se reitera la recomendación** de evaluar la pertinencia de adecuarlo y ajustarlo con los elementos faltantes establecidas en las orientaciones del Ministerio.

- El Manual de modelo de seguridad y privacidad de la información Código: MOI-APO-GTI-006 Versión: 001 de noviembre de 2022 en el cual se observó que está ajustado con el modelo del MinTIC, sin embargo, **se recomienda** incluir el capítulo de sanciones derivadas del incumplimiento de las políticas de seguridad de la información a nivel interno.
- Plan Estratégico de Seguridad de la Información del FONCEP. Código : DCO-APO-GTI-001 versión 003 de diciembre de 2023, al respecto de este documento la OCI observó que cumple con los elementos establecidos por el MinTIC de acuerdo con el documento guía, pero que sin embargo no estableció expresamente las actividades programadas en el año 2024, el cronograma de las mismas y el presupuesto asignada para cada una, razón por la que **se recomienda** que en la proyección de este documento de las próximas vigencias se incluyan todas las actividades a realizar de manera directa tal y como está dispuesto en la guía del MinTIC.

Como parte de la revisión, la OCI evidenció que en junio del 2024 se diligenció por parte de la Oficina de Informática y sistemas el autodiagnóstico del modelo de seguridad y privacidad de la información del MinTIC donde se observó que hay brechas de seguridad en algunos aspectos como criptografía, gestión de activos de información, gestión de incidentes de seguridad de la información, adquisición, desarrollo y mantenimiento de sistemas, aspectos de continuidad del negocio, entre otros arrojando un resultado PHVA del 67% o intermedio, teniendo en cuenta esas brechas **se recomienda** establecer acciones dentro del plan de acción de las próximas vigencias encaminadas a subsanar los aspectos donde aún se presentan deficiencias, de igual manera hacer seguimiento continuo dentro de los planes PETI y PESI de la entidad donde se permita ver el avance y mejora de los aspectos, continuar con el diligenciamiento de los autodiagnósticos de manera anual y establecer indicadores de seguridad y privacidad de la información al interior de la entidad.

Teniendo en cuenta lo anterior y la evaluación del MPSI de la entidad la OCI verificó los siguientes aspectos de acuerdo con la norma 27001:2022 sobre los que se emiten las siguientes recomendaciones:

Tabla 1- Verificación controles MSPI

Numeral	Política	Control	Resultado interno
5.2 A.6.1.1 MSPI	Funciones y responsabilidades en materia de seguridad de la información. Roles y responsabilidades para la seguridad de información	Las funciones y responsabilidades de seguridad de la información se deben definir y asignar de acuerdo con las necesidades de la organización. Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	Se observó que el Manual de modelo de seguridad y privacidad de la información Código: MOI-APO-GTI-006 Versión: 001 en su capítulo 5 trae un cuadro donde se establece las funciones y responsabilidades teniendo en cuenta la organización de la entidad, establece responsables, quienes deben gestionar los riesgos y discrimina las actividades de acuerdo con los roles, sin embargo teniendo en cuenta que el profesional de seguridad de la información es contratista se recomienda tener en cuenta lo mencionado por el DAFP en cuanto garantizar de manera continua el personal encargado de este aspecto sin dejar posibles espacios o brechas .
8.1 AD.2.2.1	Dispositivos finales del usuario Política para dispositivos móviles	La información almacenada, procesada o accesible a través de los dispositivos de punto final del usuario debe estar protegida. Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	La OCI evidenció que en el Manual de modelo de seguridad y privacidad de la información Código: MOI-APO-GTI-006 Versión: 001 trae en el capítulo 6.4.1.6 Lineamientos de uso de equipos portátiles y dispositivos móviles, sin embargo se evidenció que no se cumplen todos los parámetros establecidos para el uso de móviles, como es el caso de autenticación de los correos electrónicos en los celulares y la configuración con herramientas en caso del uso de celulares o equipos externos, por lo que se recomienda revisar la pertinencia de establecer los controles y medidas de seguridad para los dispositivos móviles que tengan acceso a información institucional.
5.10 A.8.1.3	Uso aceptable de la información y los activos asociados. Uso aceptable de los activos.	Se deben identificar, documentar y aplicar normas para el uso aceptable y procedimientos para el manejo de la información y otros activos asociados. Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	Se observó que la entidad en el Manual de modelo de seguridad y privacidad de la información Código: MOI-APO-GTI-006 Versión: 001 y en el Procedimiento gestión de activos de información código: PDT-APO-GTI-012 versión 001 de noviembre de 2022 tiene establecido el uso y manejo de estos activos a nivel interno con los responsables de cada uno de ellos. Adicionalmente, la OCI observó que para la vigencia 2024 se realizó la actualización de los activos con los responsables de procesos, sin embargo, no se han identificado, documentado e implementado reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información por lo que Se recomienda continuar con actividades encaminadas a la protección de este aspecto fundamental para validar los controles ante posibles riesgos de seguridad.
5.4 A.17.1.1	Responsabilidades de gestión Responsable de la continuidad.	La administración debe exigirle a todo el personal que aplique la seguridad de la información de acuerdo con la política de seguridad de la información establecida, las políticas y los procedimientos específicos de cada tema. Planificación de la continuidad de la seguridad de la información	La OCI observó que en el “Manual De Arquitectura, Continuidad, Catálogo De Servicios E Infraestructura Tecnológica” código MOI-APO-GTI-005 versión 3 se identifican los responsables de la continuidad del negocio, sin embargo, se observó que el documento está desactualizado, por lo que se recomienda: verificar que los documentos se encuentren actualizados y socializados.
8.27 A.14.2.5	Arquitectura de sistemas seguros y principios de ingeniería segura Principios de construcción de sistemas seguros	Los principios para la ingeniería de sistemas seguros deben establecerse, documentarse, mantenerse y aplicarse a cualquier actividad de desarrollo de sistemas de información. Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de	La OCI evidenció que en el interior de la entidad no hay una política de desarrollo seguro ni una guía que contenga los principios de arquitectura que deben establecerse para la construcción de los aplicativos por lo que se recomienda: revisar la pertinencia de la implementación de la política y guía para la construcción de arquitectura basada en principios seguros.

Numeral	Política	Control	Resultado interno
		implementación de sistemas de información.	
6.7	Trabajo remoto	Deben implementarse medidas de seguridad cuando el personal trabaja de forma remota para proteger la información a la que se accede, procesa o almacena fuera de las instalaciones de la organización. Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	Como parte de la revisión que se está realizando actualmente, se observó que el Manual de modelo de seguridad y privacidad de la información Código: MOI-APO-GTI-006 Versión: 001 en su capítulo 11 establece pautas y requerimientos técnicos para la realización del teletrabajo donde incluye todas las políticas y lineamiento técnicos que deben tener en cuenta los funcionarios y contratistas para la utilización de los equipos y las redes de manera remota. Adicionalmente, se observó que para el ingreso a los activos de información internos se debe realizar mediante conexión VPN.
A.6.2.2	Teletrabajo		

Fuente: Elaboración propia

Adicionalmente a lo anterior se realizó una visita a la Oficina de Informática y Sistemas para verificar el funcionamiento de los backups de acuerdo con lo establecido en el Procedimiento gestión de backup código: PDT-APO-GTI-006 versión: 003 y el Manual de arquitectura, continuidad, catálogo de servicios e infraestructura tecnológica código: MOI-APO-GTI-005 versión: 003 donde se pudo evidenciar la recuperación de información de las bases de datos y el aplicativo SUIT VISION de acuerdo con las los backups de prueba realizada por la OIS, adicionalmente se observó el control de los mismos y la disponibilidad en el caso de requerirse, adicionalmente se informó que las carpetas que están en atlas también están gestionada mediante el servicio de nube que se presta mediante la Orden de Compra 129436 de 2024.

5.1.4 Verificación de la información correspondiente al tratamiento de datos personales

En lo que respecta a la política de tratamiento de datos personales en la entidad dispuesta por la Ley 1581 de 2012, la OCI observó que en la página web se publicó la política en el enlace <https://www.foncep.gov.co/politicas-de-seguridad-de-la-informacion-y-proteccion-de-datos-personales>, en donde se estableció que esta se aplicará a todas las bases de datos y/o archivos que contengan datos personales y que sean objeto de tratamiento por FONCEP, considerado como responsable y/o encargado del tratamiento de estos datos.

La política se adoptó mediante la resolución 0072 del 29 de septiembre de 2022 y se encuentra reglamentada en el capítulo 6.3 del manual de modelo de seguridad y privacidad de la información.

En el manual de modelo de seguridad y privacidad de la información se evidenció que los aspectos regulados están basados de acuerdo con los principios rectores basados en la ley 1581 de 2012, la identificación del FONCEP como responsable del tratamiento de estos datos, las finalidades para la protección de los mismos, los deberes del titular, los derechos de los usuarios, los lineamientos para rectificación, supresión y actualización y la atención a peticiones, quejas y reclamos de los titulares de datos personales.

Como parte de la verificación realizada por la OCI, se observó que en la página web de la entidad no se comparten datos de los pensionados dando de esta manera cumplimiento a la norma.



En lo que respecta a la información de los funcionarios y contratistas, se observó que en las bases de datos se siguen compartiendo datos de funcionarios y contratistas diferentes a lo establecido en el parágrafo 2 del artículo 9 de la ley 1712 de 2014, así como en el listado de la matriz ITA de la Procuraduría General de la Nación, razón por la cual **se reitera la recomendación** de ajustar la información publicada de funcionarios y contratistas personas naturales, de tal forma que se incluya solo lo establecido en la norma y lo mencionado en la Circular Externa Única Código CCE-EICP-MA-06 Versión 03 de 27 de diciembre de 2023 de Colombia Compra Eficiente.

Por otra parte, la Oficina de Control Interno verificó el reporte de las bases de datos a la Superintendencia de Industria y Comercio – SIC en la plataforma Registro nacional de base de datos - RNBD en cumplimiento de lo dispuesto en el artículo 25 de la Ley 1581 de 2012, Decreto 886 de 2014 y compilado en el Decreto 1074 de 2015.

Al respecto, la OCI observó que FONCEP realizó la actualización en la plataforma correspondiente desde el 14 de marzo del 2024 estableciendo las siguientes bases como las que están funcionando actualmente: SIGEF, SIDEAF, BONPENS, Terceros, SISLA, CESANTIAS, HISTORIA LABORAL, CARTERA, y se inhabilitó la Vista Única que según lo informado por la Oficina de Informática y Sistemas solo era un compilador de información. De igual forma se realizó reunión con la Oficina de Informática y Sistemas el día 10 de octubre de 2024 donde se verificó la base Terceros y su funcionamiento, donde además se entregó la certificación de la actualización de la base de datos de FONCEP que vence el 25 de marzo de 2025.

Finalmente se realizó visita al segundo piso de la torre A de la entidad para verificar si los documentos entregados a los usuarios contienen la política de tratamiento de datos para la atención en FONCEP, en donde se observó que los siguientes si la tienen:

-Solicitud Copia código FOR-APO-GDO 09 Versión 005 de 2020

-Formato Solicitud novedades nomina de pensionados código FOR-MIS-GRP-021 Versión 004 de 2020

-Formato de recepción de peticiones, quejas reclamos, sugerencias y/o denuncias código FOR-EST-SCI 002 de 2023

-Formato único de solicitud pensional código FOR-MIS-GRP-017 Versión 005 de 2020

Sin embargo, el Formato de designación para sustitución provisional – ley 1204 de 2008 código FOR-MIS-GRP-019 de 2020 no contiene la política de tratamiento de datos por lo que **se recomienda** actualizar el formato incluyendo la cláusula del tratamiento de datos para dar cumplimiento a la normatividad vigente.

5.1.5 Servicios Ciudadanos Digitales

Esta habilitador busca desarrollar mediante soluciones tecnológicas, las capacidades para mejorar la interacción con la ciudadanía y organizar su derecho a utilización de medios digitales ante la administración pública.

Al respecto de este punto la OCI observó que actualmente FONCEP cuenta con 26 trámites relacionados en el numeral 5 del vínculo de transparencia y acceso a la información pública del portal web institucional, los cuales direccionan a la Guía de trámites y servicios de Bogotá.



De igual manera el FONCEP cuenta con una oficina virtual en el vínculo <https://www.foncep.gov.co/servicio-ciudadano/oficina-virtual> que contempla trámites pensionales, cesantías, historia laboral, pagos de cuotas partes y consulta de terceros.

Así mismo, se observó la realización de encuestas sobre la prestación de los servicios de la entidad y temas de interés sobre la rendición de cuentas, Huella de gestión, noticias, Gózate Bogotá además del botón de denuncias en el marco de las normas que regulan el gobierno abierto en la capital.

5.2 Roles y responsabilidades de la política

La OCI evidenció que en el manual de modelo de seguridad y privacidad, código MOI-APO-GTI-006 versión : 001 se establece en el capítulo 5 los roles y responsabilidades de la política de seguridad de la información, sin embargo en el caso del responsable de seguridad no se menciona quién es o en qué cargo se encuentra esta responsabilidad, por lo que **se recomienda** establecer de manera clara y precisa el responsable o el cargo, se encuentra atendiendo a las recomendaciones de la calificación de la evaluación FURAG 2023.

Por otra parte, se evidenció que no hay claridad sobre quien es el responsable de la protección de datos personales o el custodio de datos de la entidad, por lo que **se recomienda** establecer de manera clara en los reglamentos internos quién tiene el rol de la protección y direccionamiento de la ciudadanía, quién de atender los reclamos en caso de inconformidad con el manejo, quién el custodio y quién el responsable de monitorear las respuestas que se den en caso de estos reclamos.

5.3 Planes de acción y Planes de seguridad y privacidad de la información 2023 y 2024

En lo que respecta al año 2023, se observó un total de 57 actividades a realizar por parte de la Oficina de informática y sistemas, estas fueron evaluadas en el informe de evaluación por dependencias radicado 3-2024-01106 del 30 de enero de 2024 dando un resultado de cumplimiento del 98% con 56 actividades cumplidas, posteriormente la OIS mediante radicado 3-2024-02339 del 14 de marzo indica el avance que ha habido durante el 2024 para la implementación del protocolo IPv6 (actividad 57) y validar la observación del informe, sin embargo, a la fecha se observa que sigue persistiendo la falla con el protocolo, razón por la cual se debe continuar con la actividad de la implementación hasta su culminación para de esta manera validar su cumplimiento nuevamente.

Para el año 2024 de acuerdo con el Plan de acción versión 5 establecido en la página web de la entidad desde el 16 de julio se observa 39 actividades asociadas a la Oficina de Informática y Sistemas, en el aplicativo SUIT VISION se observa que hay 51 actividades a realizar, que incluyen las asociadas al plan de choque establecido por la Dirección para el último trimestre del año.

En lo referente al año 2024 se observan 22 actividades del plan de acción institucional versión 5 asociadas a seguridad y privacidad de la información **se recomienda** tomar las medidas necesarias para cumplir con las actividades programadas en la fecha establecida para ello.



5.4 Verificación de la información reportada en FURAG

La OCI realizó la verificación de las evidencias cargadas en el aplicativo SVE, en la página web de la entidad, y en la documentación reportada para el FURAG 2023 frente a los puntos establecidos en el manual de gobierno digital y frente a lo transmitido en el mes de mayo de 2024.

De acuerdo con la verificación realizada por la OCI, se estableció que las preguntas relacionadas con la política de gobierno digital y seguridad de la información reportadas al FURAG de la vigencia 2023, presentan diferencias o recomendaciones frente a las evidencias verificadas, las cuales se relacionan en el Anexo 1 y que se resumen a continuación en los siguientes aspectos.

Tabla 1 Verificación políticas de gobierno y seguridad digital FURAG-2023

Preguntas que no cuentan con evidencia, o que no coincide con lo mencionado en las respuestas FURAG.	98 a y b, 108 a, 137 b, 142
Preguntas sobre las cuales se establecen recomendaciones para la mejora continua.	97 a y b, 117 b, 141 b

Fuente: Elaboración propia a partir del FURAG 2023

Adicional a lo anterior la Función Pública publicó recomendaciones en el enlace <https://app.powerbi.com/view?r=eyJrIjoizDQzOTAyNTQzNTZlNTY0NDh0LTgyNGMtMzA5NTRkM2I1NzE5IiwidCI6IjU1MDNhYWMyLTdhMTUzNDZhZi1iNTIwLTJhNjc1YWQxZGYxNiIsImMiOjR9> sobre las preguntas que no fueron contempladas por la entidad y frente a las políticas de Gobierno Digital y Seguridad y Privacidad de la Información para mejorar frente a los resultados para la mejora en la calificación, entre las cuales se destacan las siguiente .

- Aprobar y publicar la licencia de datos abiertos en la entidad, mediante la cual se determina el alcance, uso y aprovechamiento que los particulares o terceros interesados puedan efectuar sobre los mismos.
- Automatizar los trámites inscritos por la entidad en el Sistema Único de Información de Trámites (SUIT)
- Capacitar a servidores y contratistas de la entidad en temáticas de la política de gobierno digital tales como gobernanza, innovación pública, seguridad y privacidad de la información, arquitectura T.I, cultura y apropiación, servicios ciudadanos digitales, dediciones basadas en datos, estado abierto entre otros.
- Contar con un catálogo interno de datos maestros de la entidad.
- Formular y ejecutar estrategias de ciudades y territorios inteligentes en la entidad
- Habilitar funcionalidades que permitan a los usuarios hacer seguimiento en línea del estado de los tramites total o parcialmente en línea de la entidad.
- Contar con un plan de continuidad del negocio BCP, definido, documentado e implementado para los procesos críticos y misionales.
- Designar un área responsable de la seguridad digital
- Realizar pruebas de recuperación de cada uno de los sistemas de información críticos.

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

6. Evaluación de los controles de riesgos

En el desarrollo de la presente auditoría se verificó que FONCEP al 30 de septiembre de 2024 contaba con 18 riesgos de seguridad de la información asociados a la disponibilidad, integridad y confidencialidad de la información de los procesos y 50 controles asociados a los mismos. En la matriz de riesgos de seguridad digital al corte del 30 de septiembre de 2024 los riesgos se encuentran gestionados y monitoreados, adicionalmente se observó en el mapa de riesgos de seguridad de la información que, del total de riesgos identificados, el 11% (2) de ellos se encuentran ubicados en zona de riesgo baja, 50% (8) en zona de riesgo moderada, 17% (3) en la zona de riesgo alta y un 22% (4) en zona de riesgo extrema. Del total de los 50 controles definidos en los 18 riesgos de seguridad de la información se observaron 9 controles detectivos y 41 preventivos. **Se recomienda** mantener capacitadas a las áreas constantemente acerca de las posibles amenazas que pueden existir dentro de sus procesos, revisar cuáles son los puntos sobre los que se puede presentar impactos adversos por la materialización de riesgos, identificándolos y clasificándolos según el tipo de riesgo.

De igual forma una vez revisada la plataforma Suite Visión Empresarial (SVE) y teniendo en cuenta del alcance del presente informe, se evaluaron los siguientes riesgos y controles del proceso Gestión de tecnologías de la información:

Tabla 2 Riesgos y controles

Tipo de riesgo	Riesgo	Control
Operacional	Recursos tecnológicos gestionados incumpliendo los objetivos del proceso.	Garantizar la definición de los requisitos adecuados
		Asegurar el adecuado seguimiento a los requerimientos e incidencias de software e infraestructura, pcs y periféricos
		Asegurar la calidad y los tiempos del servicio prestado
		Asegurar la gestión del conocimiento
		Asegurar la adecuada definición de necesidades y requerimientos
Seguridad de la información	Pérdida de la confidencialidad e integridad de los activos de información de tipo software, hardware, datacenter, bases de datos del proceso de Gestión de tecnologías de la información.	Asegurar la asignación o retiro de acceso a los activos de información de la entidad
		Asegurar que los colaboradores de la entidad tengan información relacionada con el funcionamiento y uso de las herramientas de Microsoft y GLPI
		Verificar que los backups se encuentren en buen estado
		Asegurar la correcta clasificación de los activos de la Información del FONCEP
		Asegurar la parametrización
		Asegurar que se realice el mantenimiento de los equipos de cómputo por parte de la mesa de ayuda
		Garantizar el correcto funcionamiento del antivirus
Corrupción	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.	Asegurar el uso adecuado de la información
		Asegurar la correcta asignación de los activos de información de la entidad a los servidores y contratistas
		Asegurar la implementación de la política de seguridad y privacidad de la información
		Verificar el cumplimiento de los pasos a producción

Fuente: Plataforma SVE



La OCI observó que en el aplicativo SVE se registró el monitoreo de los riesgos y controles del 15 de octubre de 2024 con las respectivas evidencias y análisis por cada uno.

En cuanto a los atributos de eficiencia e informativos de los controles, se relaciona lo observado por la OCI:

Tabla 3 Resultado a la verificación a la efectividad de los controles

Atributos	Criterios	Observación OCI
Eficiencia	Tipo: Preventivo, detectivo o correctivo	Se observaron 17 controles de los cuales: 15 son preventivos, y 2 detectivos.
	Implementación: Automático o manual	La totalidad de los controles se ejecutan de forma manual
Informativos	Documentado o sin documentar	Los controles se encuentran documentados
	Frecuencia continua o aleatoria de ejecución	La ejecución de los controles se realiza de forma continua.
	Evidencia con registro o sin registro	Hay aprobación del monitoreo del 15 de octubre por parte del responsable de la OIS

Fuente: Elaboración propia

A partir de lo verificado por la OCI se evidenció que aún siguen habiendo incumplimientos en los términos del requerimientos GLPI de acuerdo con los manuales y procedimientos internos , por lo que **no se evidencia la efectividad del control** “Asegurar el adecuado seguimiento a los requerimientos e incidencias de software e infraestructura, pcs y periféricos”, razón por la cual se recomienda establecer acciones tendientes a fortalecer el control y/o identificar nuevos controles, para garantizar el cumplimiento de los términos de los GLPI, atendiendo las disposiciones del Instructivo catálogo de servicios de tecnologías de la información - TI código: INS-APO-GTI-008 versión: 003.

Adicionalmente, se observó que en el mes de julio de 2024 se establecieron 3 acciones de mejoramiento relacionadas con el riesgo “Recursos tecnológicos gestionados incumpliendo los objetivos del proceso”, derivado de la indisponibilidad de servicios tecnológicos y sistemas de información al momento de realizar ventana de mantenimiento para la instalación de los switch core. Las acciones tienen fecha de ejecución entre los meses de septiembre y diciembre de 2024.

7. Seguimiento Plan de Mejoramiento

7.1 Seguimiento Plan de mejoramiento Interno

Para el presente seguimiento se observaron las siguientes acciones correspondiente con el plan de mejoramiento interno de la Oficina de Informática y Sistemas:

DESCRIPCIÓN DEL HALLAZGO	DESCRIPCIÓN DE LA ACCIÓN	FECHA DE INICIO	FECHA FIN	Cumplimiento y efectividad	SEGUIMIENTO REPORTADO POR LA OCI FRENTE AL RESPONSABLE ACCIÓN
Hallazgo 133: Se observó en la auditoría a Gobierno Digital que en el proceso de gestión de tecnologías de la información se presentaron casos registrados en la mesa de ayuda a través de la herramienta GLPI pendientes de atención desde el año 2022, sin que se haya evidenciado una gestión efectiva ni justificación de los atrasos, situación que conlleva al incumplimiento de los plazos establecidos en el Instructivo catálogo de servicios de tecnologías de la información TI Código: INS-APO-GTI-008 Versión: 001, lo que denota la falta de aplicación de los puntos de control del Procedimiento de gestión de mesa de ayuda Código: PDT-APO-GTI-001 Versión: 001, generando una posible materialización del riesgo “recursos tecnológicos gestionados incumpliendo los objetivos del proceso”.	Hacer un seguimiento a los casos asignados en GLPI a cada ingeniero de la Oficina de Informática y Sistemas para verificar la calidad y los tiempos del servicio prestado.	18/08/2023	15/12/2023	Cumplida No efectiva	Se evidenció por parte de la OCI, las bitácoras de la Oficina de Informática y Sistemas con el seguimiento de los GLPI y requerimientos en los comités primarios por parte de la OIS, sin embargo al revisar el aplicativo se observó que aún hay requerimientos que están excediendo el tiempo del Instructivo catálogo de servicios de tecnologías de la información - ti código: ins-apo-gti-008 versión: 003 razón por la cual no se considera que fue efectiva la acción y se debe reformular el plan de mejoramiento.
	Actualizar la documentación de respuesta de requerimiento del proceso relacionada con la atención oportuna a los requerimientos e incidencias en GLPI, dado los lineamientos que se van a plantear para esa atención.	01/09/2023	31/10/2023	Cumplida No efectiva	Se evidenció la actualización del Instructivo catálogo de servicios de tecnologías de la información - ti código: ins-apo-gti-008 versión: 003 actualizado en noviembre de 2023, el Manual para desarrollo y soporte de software código: moi-apo-gti-004 versión: 002 de octubre de 2023, y el Procedimiento de gestión de mesa de ayuda código: pdt-apo-gti-001 versión: 001 de octubre de 2023, sin embargo los términos establecidos en los mismos se han excedido en la actual revisión, razón por la cual no se considera que fue efectiva la acción y se debe reformular el plan de mejoramiento
Hallazgo 134 A partir de la verificación de la aplicación de las disposiciones del MinTIC respecto a la adopción del protocolo IPv6 en FONCEP, se observó que a la fecha de seguimiento no se tenía implementado el protocolo, incumpliendo con el plazo establecido en la resolución 1126 de 2021 y reiterado en la Circular No. 000015/22, el cual venció el 31 de diciembre de 2022, situación que podría llegar a materializar el riesgo “infraestructura tecnológica dispuesta por debajo de la meta establecida”, con las consecuencias respecto a las limitaciones del internet para seguir funcionando normalmente, mayor costos a futuro y afectación en el tiempo de las operaciones y servicios de internet, razón por la cual se deberá establecer la causa raíz originadora de la situación evidencia y formular el plan de mejoramiento que permita subsanarla.	Implementar parcialmente el IPV6 en FONCEP detallando las brechas y soluciones encontradas, así como los avances durante la vigencia en las fases priorizadas.	01/03/2023	31/10/2023	Cumplida No efectiva	La OCI evidenció la realización del informe del contrato 158 de 2023 en la que se explica los avances que tuvo la implementación del IPv6 durante el año 2023 y las dificultades que aún se siguen presentando debido a la falta de una membresía LACNIC, adicionalmente se realizaron pruebas para verificar la implementación pero se observó que aún no se cuenta en la red con este protocolo y se sigue incumpliendo la normatividad, razón por la cual no se considera que fue efectiva la acción y se debe reformular el plan de mejoramiento.

DESCRIPCIÓN DEL HALLAZGO	DESCRIPCIÓN DE LA ACCIÓN	FECHA DE INICIO	FECHA FIN	Cumplimiento y efectividad	SEGUIMIENTO REPORTADO POR LA OCI FRENTE AL RESPONSABLE ACCIÓN
Hallazgo 135: Se observó que, al corte del mes de junio de 2023, FONCEP no tiene actualizadas las bases de datos ni la política de tratamiento de datos en el RNBD de la Superintendencia de Industria y Comercio, tal como lo dispone el artículo 25 de la Ley 1581 de 2012 y el artículo 2.2.2.26.3.3. del Decreto 1074 de 2015, situación derivada de la falta de identificación de los roles que intervienen en el cargue de la información y ausencia de controles para mantener actualizado el RNBD, lo que podría llegar a materializar riesgos asociados a la falta de oportunidad y calidad de la información y a posibles sanciones por parte de la SIC.	Coordinar la actualización de las bases de datos en el Registro Nacional de Bases de Datos – RNBD	01/09/2023	31/10/2023	Cumplida Efectiva	La OCI evidenció que ya fueron actualizadas las bases de datos en el aplicativo del RNBD de la Superintendencia de Industria y Comercio cumpliendo con las actividades correspondientes
	Documentar la actualización de las bases en el Registro Nacional de Bases de Datos – RNBD	01/11/2023	15/12/2023	Cumplida Efectiva	La OCI evidenció que ya fueron actualizadas las bases de datos en el aplicativo del RNBD de la Superintendencia de Industria y Comercio cumpliendo con las actividades correspondientes
	Actualizar las bases en el Registro Nacional de Bases de Datos – RNBD	01/11/2023	15/12/2023	Cumplida Efectiva	La OCI evidenció que ya fueron actualizadas las bases de datos en el aplicativo del RNBD de la Superintendencia de Industria y Comercio cumpliendo con las actividades correspondientes

A partir de la verificación realizada por la OCI a las acciones del plan de mejoramiento establecidas para la vigencia 2023, así como lo observado en el presente informe respecto al incumplimiento de los términos para resolver oportunamente los GLPI y la no implementación del protocolo Ipv6, se observó que las acciones formuladas a no han sido efectivas a pesar de haberse cumplido al 100%, razón por la cual se requiere la reformulación del plan de mejoramiento.

Para el presente seguimiento no se observó que haya acciones suscritas para la Oficina de Informática y Sistemas en el plan de mejoramiento suscrito con la Contraloría de Bogotá.

8. Conclusiones

A partir de los resultados del presente informe, se observó que el sistema de control interno asociado al cumplimiento de las disposiciones de gobierno digital, seguridad digital y protección de datos personales es susceptible de mejora, en la medida que se implementen las recomendaciones indicadas y se reformule el plan de mejoramiento frente a las situaciones evidencias en el presente informe.

Esta auditoría deja presente que las recomendaciones plasmadas dentro del informe son producto de las situaciones encontradas de acuerdo con las evidencias presentadas y revisadas, por consiguiente, le corresponde al líder del proceso revisar si las acciones implementadas o las que llegasen a desplegar son las más efectivas para proporcionarle al sistema de control interno los elementos de seguridad y confiabilidad necesarios para el logro de los objetivos institucionales.

9. Recomendaciones

- Realizar los ajustes técnicos requeridos en la página web de la entidad para dar cumplimiento al criterio web de la resolución 1519 de 2020 del MinTIC “CC15. Advertencias bien ubicadas”, para que el ciudadano visualice correctamente las alertas de formularios.
- Establecer un control que permita actualizar los documentos en datos abiertos acorde con las últimas versiones emitidas y publicadas por la entidad.
- Continuar con la aplicación de las encuestas para determinar la publicación y uso de datos abiertos, analizar sus respuestas y tomar acciones de acuerdo con las recomendaciones y observaciones recopiladas.
- Realizar semestralmente ejercicios de aprovechamiento de datos abiertos que fortalezcan la rendición de cuentas, incentiven la participación ciudadana y mejoren la innovación pública, de acuerdo con lo establecido en el anexo técnico de la circular 064 de 2021.
- Documentar los procesos de interoperabilidad internos y con otras entidades y definir un plan de contingencia en el caso de fallas en el servicio.
- Avanzar en la etapa de planeación de automatización de trámites, revisar los trámites y reportar los que no se puedan digitalizar, con el fin de dar cumplimiento a los términos establecidos en el decreto 088 de 2022.
- Continuar con las acciones necesarias para la publicación en la carpeta ciudadana de los trámites del FONCEP, de acuerdo con la normatividad vigente.
- Avanzar en la implementación de tecnologías de la cuarta revolución industrial que faciliten la interacción con otras entidades del Estado y la prestación de servicios del FONCEP.
- Actualizar el documento manual de arquitectura continuidad y catálogo de servicios para eventos de contingencias DRP.
- Establecer controles de acuerdo con el resultado del autodiagnóstico de seguridad de la información, así como las recomendaciones de la OCI incluidas en la Tabla 1- Verificación controles MSPI.
- Implementar los indicadores de seguridad y privacidad de la información para la mejora continua, de acuerdo con el anexo 1 del Modelo de Seguridad y Privacidad de la Información del MinTIC.
- Actualizar el “Formato de designación para sustitución provisional – ley 1204 de 2008 código FORMIS-GRP-019 de 2020” para incluir la política de tratamiento de datos personales de FONCEP.
- Establecer de manera clara los responsables de seguridad de la información y de protección de datos personales, indicando cargo y funciones para la administración y custodia de datos.
- Fortalecer el control “Asegurar el adecuado seguimiento a los requerimientos e incidencias de software, infraestructura, pcs y periféricos” establecido para evitar la posible materialización del riesgo “Recursos tecnológicos gestionados incumpliendo los objetivos del proceso”.
- Reformular el plan de mejoramiento frente a los hallazgos formulados por la OCI en el informe radicado ID 551266 del 27 de julio de 2023, de tal manera que permita subsanar la causa raíz identificada.

Actividad	Nombre	Cargo	Dependencia	Firma
Revisó y aprobó	Alexandra Yomayuzo Cartagena	Jefe Oficina	Oficina de Control Interno	
Proyectó	Cesar Augusto Franco V	Contratista	Oficina de Control Interno	

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

Anexo 1. Verificación política de Gobierno y Seguridad Digital FURAG-2023
Oficina de Control Interno - FONCEP

Pregunta FURAG 2023	Opciones de respuesta	Selección y respuesta FONCEP	Observación OCI
98. ¿La entidad reportó en la herramienta de seguimiento habilitada por el Ministerio TIC (https://micrositios.mintic.gov.co/ipv6/control/app/login.php) el avance en la adopción de IPv6?	Documento de activación de políticas de seguridad para IPv6 (Fase 2)	Se realizó el Informe IPv6 Foncep en el que se documentó las políticas de enrutamiento y pruebas de conectividad. La creación de políticas en IPv6. Pág. 12. Además, lo que prueba su funcionalidad, ya que la navegación en la red esta soportada bajo el protocolo IPv6. Pág. 12.	La OCI evidenció reporte de la implementación del protocolo IPv6 en el link del MinTIC en la vigencia 2019, sin que se hubiera actualizado el avance en los cortes siguientes, razón por la cual no se considera que la respuesta cuente con evidencia suficiente, por lo que se recomienda fortalecer los controles del envío del reporte de información FURAG
	Informe de pruebas piloto y de implementación de IPv6 (Fase 2 y 3)	La adopción de IPv6 se encuentra actualmente la entidad en fase de implementación y evaluación y durante el 2023 se efectuó la configuración a nivel de seguridad perimetral y de nube y, se activó el portal web de la entidad operativo en protocolo IPv6 compatible IPv4, se anexa el informe con la prueba piloto y de implementación. https://foncep.gov.co/sharepoint.com/b/s/REPOSITORIOFURAG/EZuW6Rjd2MROjnY1B8nq10UBR50PDVoz1NZFjKChPPCCOA?e=E7tsDR	
	Acta de cumplimiento a satisfacción sobre el funcionamiento e implementación de los elementos que fueron intervenidos con IPv6		
Pregunta FURAG 2023	Opciones de respuesta	Selección y respuesta FONCEP	Observación OCI
108. ¿La entidad elaboró un diagnóstico de seguridad y privacidad de la información para la vigencia 2023, construido a través de la herramienta de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI)?	Se elaboró y se aprobó por parte del Comité de Gestión y Desempeño Institucional	Para el 2023 se evaluó la efectividad y eficacia de los indicadores implementados en el 2022 asociado al documento "Indicadores MSPI_2022_V1".	No se evidenció el autodiagnóstico ni el documento indicadores que mencionaron como evidencia en el reporte FURAG, razón por la cual no se considera que la respuesta cuente con evidencia suficiente, por lo que se recomienda fortalecer los controles del envío del reporte de información FURAG.
	Se elaboró, pero no se aprobó por parte del Comité de Gestión y Desempeño Institucional		
	No		
Pregunta FURAG 2023	Opciones de respuesta	Selección y respuesta FONCEP	Observación OCI
137. ¿Cuáles de los siguientes lineamientos establecidos en el Decreto 1263 de 2022 se cumplieron en los proyectos de Transformación Digital formulados o ejecutados por la entidad durante el 2023?	Uso de infraestructura de datos dando cumplimiento al Plan Nacional de Infraestructura de Datos, la línea de acción de decisiones basadas en datos y el habilitador de seguridad y privacidad de la información		
	Interoperabilidad entre los sistemas de información públicos para suministro e intercambio de la información conforme a los principios señalados en la Ley 1581 de 2012	FONCEP cuenta con el Manual de interoperabilidad, el cual esta basado en el marco de interoperabilidad del MinTIC, brindando así una herramienta que permita robustecer los servicios de Tecnologías de la Información para mejorar la calidad de la información y responder efectivamente las necesidades institucionales. Además, esta documentado en el PETI la interoperabilidad de los trámites o servicios, PÁG. 123. Además, se cuenta con el Manual de Interoperabilidad de FONCEP, brindando así una herramienta que permita robustecer los servicios de Tecnologías de la Información para mejorar la calidad de la información y responder efectivamente las necesidades institucionales. https://foncep.gov.co	La OCI observó que la información reportada frente al Plan Estratégico de Tecnologías de la Información PETI no coincide con lo mencionado en la respuesta de FURAG, ni en el documento se observa la explicación de la interoperabilidad de los trámites como lo presentaron en el reporte FURAG, razón por la cual no se considera que la respuesta cuente con evidencia suficiente, por lo que se recomienda fortalecer los controles del envío del reporte de información FURAG
	Uso de mecanismos de digitalización y automatización de trámites, servicios y procesos y su vinculación al Portal Único del Estado Colombiano		
	Uso de mecanismos de agregación de demanda, como acuerdos marco de precios vigentes u otros mecanismos que hayan sido establecidos por la Agencia Nacional de Contratación Pública o la modalidad de contratación contenida en el marco de la Política de compras y contratación pública		
	Implementación, migración y uso de servicios de nube, en armonía con el principio de neutralidad tecnológica y normatividad vigente		
	Uso de mecanismos exploratorios de regulación como Sandbox		
	Uso de tecnologías emergentes tales como inteligencia artificial, internet de las cosas (IoT), big data o blockchain		
Ninguno de los anteriores			
Pregunta FURAG 2023	Opciones de respuesta	Selección y respuesta FONCEP	Observación OCI
142. Indique el porcentaje del presupuesto total asignado a la Seguridad Digital (Ciberseguridad), para la protección de los datos digitales en la entidad (Costos de personal, herramientas, IPS/IDS, firewall, Antivirus, EDR, servidores, sistemas, licencias etc.):	N/A	8.99	La OCI observó que los valores reportados para el año 2023, lo ejecutado y lo enviado no coinciden con el porcentaje reportado en el aplicativo ni la evidencia cargada razón por la cual se recomienda establecer las razones por las cuales se presentan las diferencias en los valores reportados y fortalecer los controles del reporte de la información en FURAG

Pregunta FURAG 2023	Opciones de respuesta	Selección y respuesta FONCEP	Observación OCI
97. ¿Qué actividades de las fases 2 y 3 del modelo de adopción de IPv6 ya implementó la entidad?	Documento de activación de políticas de seguridad para IPv6 (Fase 2)	Se realizó el Informe IPv6 Foncep en el que se documentó las políticas de enrutamiento y pruebas de conectividad. La Creación de políticas en IPv6. Pág. 12. Además, lo que prueba su funcionalidad, ya que la navegación en la red esta soportada bajo el protocolo IPv6. Pág. 12. https://foncepgovco.sharepoint.com/:b/s/REPOSITORIOFURAG/EZuw6Rjd2MROjnY1B8mq10UBR50PDVozdNZFjKChPPCCOA?e=E7tsDR	Respecto a esta actividad se observó que aún está en proceso de implementación en el portal web de la entidad el protocolo y que no ha sido aún establecido en su totalidad se recomienda tomar las medidas correspondientes para finalizar el proceso de implementación del protocolo y dar cumplimiento a la normatividad vigente.
	Informe de pruebas piloto y de implementación de IPv6 (Fase 2 y 3)	La adopción de IPv6 se encuentra actualmente la entidad en fase de implementación y evaluación y durante el 2023 se efectuó la co La adopción de IPv6 se encuentra actualmente la entidad en fase de implementación y evaluación y durante el 2023 se efectuó la configuración a nivel de seguridad perimetral y de nube y, se activó el portal web de la entidad operativo en protocolo IPv6 compatible IPv4, se anexa el informe con la prueba piloto y de implementación. https://foncepgovco.sharepoint.com/:b/s/REPOSITORIOFURAG/EZuw6Rjd2MROjnY1B8mq10UBR50PDVozdNZFjKChPPCCOA?e=E7tsD	
	Acta de cumplimiento a satisfacción sobre el funcionamiento e implementación de los elementos que fueron intervenidos con IPv6		
Pregunta FURAG 2023	Opciones de respuesta	Selección y respuesta FONCEP	Observación OCI
117. Para vincularse al servicio de interoperabilidad, ¿la entidad dispuso de un servidor con las características establecidas en el anexo 2 del Decreto 620 de 2020?	Sí, y cuenta con las evidencias:		
	No		Se observa que la entidad no cuenta con el servidor del anexo 2 para la vinculación y uso de servicios digitales, al respecto se recomienda ver la pertinencia de implementar el servidor en la entidad en caso de necesitarse para la vinculación y uso de los servicios digitales
Pregunta FURAG 2023	Opciones de respuesta	Selección y respuesta FONCEP	Observación OCI
141. ¿La entidad tiene designado un responsable de la Seguridad Digital - (Ciberseguridad)? Sí, y pertenece a la planta de personal Sí, es un contratista No tiene a nadie designado	Sí, y pertenece a la planta de personal		
	Sí, es un contratista		Se observó en las funciones de la Jefe de Oficina de Informática y Sistemas se cuenta con la función: "Dirigir actividades para asegurar la implementación, actualización y mantenimiento del Sistema de Seguridad de la Información del FONCEP, siguiendo las políticas internas". En la respuesta suministrada en FURAG se indicó que se tiene un contratista como responsable de la seguridad digital, se recomienda revisar la respuesta que se dé para la próxima medición.
	No tiene a nadie designado		

Convenciones

Color amarillo	Respuestas que no cuentan con evidencia, o que no coincide con lo mencionado en las respuesta Furag
Color verde	Respuestas sobre las cuales se establecen recomendaciones para la mejor continua