1. DESCRIPCIÓN GENERAL	
Objetivo de la Auditoria:	Verificar el avance, cumplimiento y mejora continua del Proceso Gestión de tecnológica, así como Verificar el estado de implementación del Modelo de Seguridad y Privacidad de la Información-MSPI de FONDECUN, en cumplimiento de los lineamientos de la Política de Gobierno Digital (antes gobierno en Línea) definida por el Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC, la norma NTC ISO/ 27001:2013 y políticas establecidas por la Entidad y los requisitos legales.
Alcance de la Auditoria:	Se desarrollará auditoria a los Planes y Programas del proceso Gestión de tecnología, de acuerdo con lineamientos de MIPG y la normatividad vigente, verificar el estado de implementación del Modelo de Seguridad y Privacidad de la Información MSPI en la vigencia 2024, a los siguientes procesos institucionales: ➢ Proceso de Apoyo: Gestión Administrativa, tecnológica y de recursos físicos. ➢ Proceso de Apoyo: Gestión de Bienestar y del Talento Humano ➢ Proceso Misional: Estructuración Gerencia Y Administración De Proyectos ➢ Proceso Estratégico: Gestión Comercial y de Comunicaciones Bajo el Modelo de seguridad y privacidad de la información definido por el Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC, las normas NTC ISO/ 27001:2013 y NTC 5854, políticas establecidas por la Entidad y los requisitos legales.
Procedimiento de la Auditoría	Auditoría interna
Auditor Líder	Yenny Dianith Barrios Gómez
Equipo Auditor:	Yenny Dianith Barrios Natali Padrón Aguilar

Fecha de la Auditoria	13/03/2025 al 07/04/2025
Dependencia a cargo del proceso auditado	Subgerencia Administrativa y Financiera
Procesos Auditados	Política de Seguridad y Privacidad de la Información FONDECUN Procedimientos: GESTION INFORMATICA (código GA-PR-02) Caracterización Gestión Documental (Código GA-CP-01) Norma ISO 27001 2023 NTC 5854 Modelo de Seguridad y Privacidad de la Información

2. ANÁLISIS Y EVALUACIÓN DE DATOS

METODOLOGIA:

Durante la Auditoria, el equipo auditor utilizó técnicas de auditoria generalmente aceptadas como:

- Entrevistas con el líder del proceso de cada procedimiento en análisis de, manejo y adherencia de la Política de Seguridad y Privacidad de la Información
- Revisión de la Normatividad aplicable a los procedimientos y planes seleccionados; que permitieran un análisis integral para las conclusiones de auditoría.
- Visitas de campo, de acuerdo a lo observado y revisado.
- Revisión documental a la formulación, desarrollo, socialización, seguimiento, evaluación y control del Modelo de Seguridad y Privacidad de la Información MSPI de FONDECUN.
- Revisión del cumplimiento de los lineamientos de la Política de Gobierno Digital (antes gobierno en Línea) definida por el Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC, la norma NTC ISO/ 27001:2013 y políticas establecidas por la Entidad y los requisitos legales.

Se realizará revisión a los siguientes documentos:

- Plan estratégico Tecnologías de la Información y las Comunicaciones – PETIC, vigencia 2024. (Aprobación, Socializaciones y seguimientos)
- Caracterización del Procedimiento de gestión de tecnología.
- Procedimientos del Proceso de gestión de tecnología.

- Formulación y Seguimiento de Plan de Acción 2023-2024.
- Formulación y Seguimiento Mapa de riesgos institucional y de corrupción, vigencia 2023 -2024
- Avances realizados al Modelo Integrado de Planeación y Gestión MIPG
- Planes de mejoramiento abiertos de auditorías anteriores. (internas y externas)
- Acta de Ultima transferencia documental realizada al archivo central de la entidad.
- Política de Seguridad y Privacidad de la Información
- Procedimientos de seguridad de información.
- Inventario de activos de información.
- Plan de tratamiento de riesgos de seguridad de la información.

NORMATIVIDAD APLICABLE

- Constitución Política de Colombia
- Ley 87 de 1993 Por la cual se establecen normas para el ejercicio del control interno en las Entidades
- NTC ISO 27001 2013
- Anexo 1 Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información
- Guía No. 4 seguridad y privacidad de la información
- Decreto No. 1083 de 2015 Relacionado a lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.
- Decreto 1008 de 2018 Por el cual se establecen los lineamientos generales de la política de Gobierno Digital
- Manual de Gobierno Digital - implementación de la política de Gobierno Digital (Decreto 1008 de 2018) - MinTIC
- Mapa de Riesgos Institucional
- Procesos y procedimientos del Sistema de Gestión de FONDECÚN
- Reportes de los sistemas de información de la Entidad.

ANEXOS

- Acta de Apertura de Auditoria.
- Plan de Auditoría Interna
- Listas de chequeo – Entrevista líder del proceso de Apoyo Gestión Administrativa, Tecnología y Recursos Físicos
- Soportes evidencias del informe.

ANALISIS

En cumplimiento del Programa Anual de Auditoria para la vigencia 2025, se desarrollará auditoria al PROCESO GESTIÓN ADMINISTRATIVA, TECNOLOGICA Y RECURSOS FISICOS.

DESARROLLO DE LA AUDITORÍA

Revisión Documental.
En el desarrollo de la auditoría, se tuvo en cuenta la documentación aportada por el proceso de apoyo auditado y la información suministrada por el o los funcionarios del área delegado (s) por el la Subgerencia para atender la auditoría.

Plan estratégico Tecnologías de la Información y las Comunicaciones – PETIC. (Aprobación, Socializaciones y seguimientos)	Durante la presente auditoría, se evidenció que el Plan Estratégico de la Información y las Comunicaciones - PETIC de la Entidad se encuentra aprobada mediante acta del 19 de enero de 2024. El PETIC fue socializado a los funcionarios y contratistas de FONDECÚN mediante correo electrónico el 20 de febrero de 2024, ahora bien, teniendo en cuenta que el PETIC es la hoja de ruta para la toma de decisiones en materia de Incorporación de Tecnologías de información y Comunicación, en cumplimiento de los lineamientos del Ministerio de las Tecnologías de la Información, se pudo verificar que se realizó seguimiento al Plan Estratégico de las Tecnologías de la Información y Comunicaciones PETIC como se especifica a continuación. Para garantizar la continuidad y de los servicios tecnológicos del Fondo de Desarrollo de Proyectos de Cundinamarca, se evidenciaron los siguientes contratos, adiciones y/o prorrogas:

Plan estratégico Tecnologías de la Información y las Comunicaciones – PETIC. (Aprobación, Socializaciones y seguimientos)

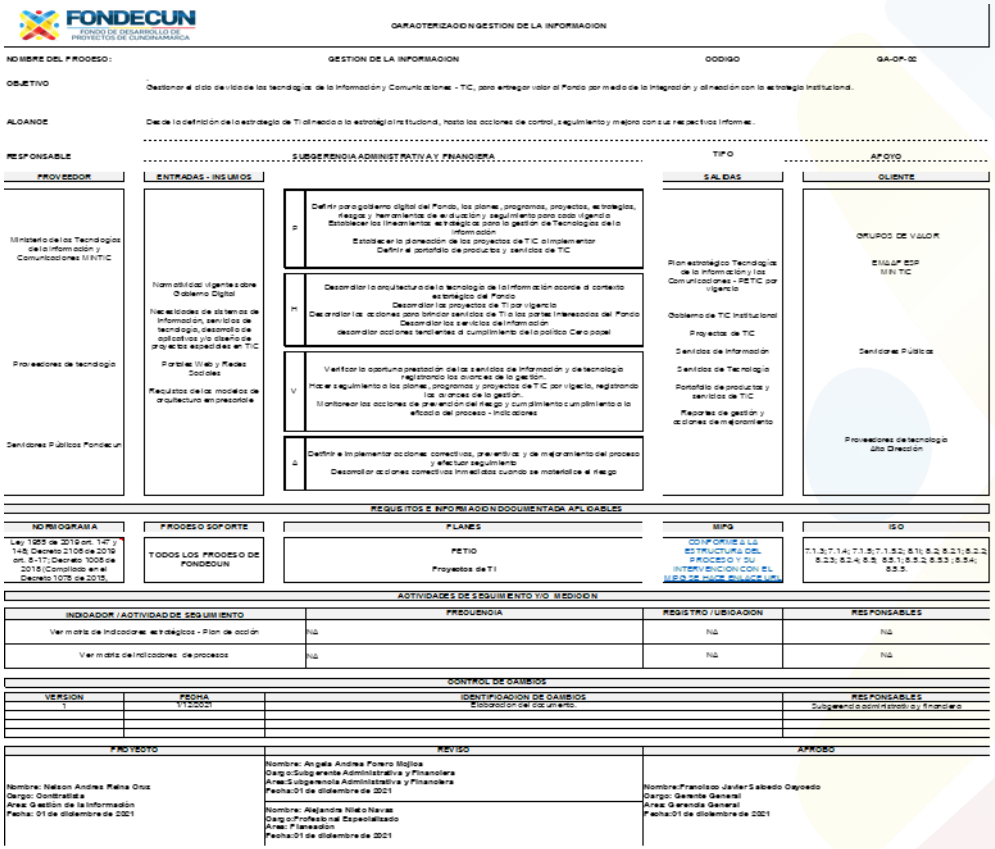
SERVICIO TI	CONTRATO
Actualización y fortalecimiento de la sede electrónica / portal web	Se realiza adición y prórroga del contrato 2023-0028, hasta abril 17 de 2024, generando nuevo contrato el 12 de abril de 2024 mediante proceso PMC-001-2024, contrato 2024-0209 hasta el 31 de diciembre de 2024
Análisis del sistema de información actual y evaluar su funcionalidad y servicio, para generar valor en los servicios y procesos	Se realiza el Contrato Nro. 2024-0271 "Prestar el servicio para la operación y el soporte bajo la modalidad SAAS (software as a service) en la nube con la actualización, capacitación y soporte del sistema de información ERP, de los módulos parametrizados para el Fondo de Desarrollo de Proyectos de Cundinamarca - Fondecun". el 02 de mayo de 2024.
Alquiler de equipos de tecnología y periféricos	Para la continuidad del servicio y asegurar los equipos tecnológicos para la entidad se realiza adición y prorroga al Contrato No. 2023-0981 hasta el 17 de julio de 2024, igualmente mediante el proceso SAMC-SI-001-2024 se realiza nuevo contrato Nro. 2024-0366 hasta el 18 de febrero de 2024.

SERVICIO TI	CONTRATO
Servicio de conectividad a internet canal dedicado.	Se realiza el 21 de febrero de 2024, para la continuidad del servicio de conectividad adición y prorroga a la OC Nro. 104985 contrato 2023-0181, hasta el 27 de junio de 2024. Mediante proceso IPMC-004-2024 se realiza contratación para el servicio de conectividad ampliando el canal de comunicaciones a 200 Mbps, el 26 de junio de 2024, contrato hasta el 1 de febrero de 2025
Contratación servicios correos electrónicos Microsoft 365	Se realiza contratación mediante AMP OC 126696 (Contrato 2024-0143) servicios de correos plataforma Microsoft 365 hasta el 15 de abril de 2024
Contratación apoyo a la gestión tecnológica.	Se realiza contratación del personal de apoyo a la gestión tecnológica mediante contrato 2024-0275 de fecha 7 de mayo de 2024 hasta el 31 de diciembre de 2024
Servicio de renovación membresía IPV6 anualidad ante LACNIC	Se suscribe contrato el 23 de mayo de 2024 contrato 2024-0293, realizando la renovación de la membresía por un año ante Lacnic
Mantenimiento AA y UPS	Se realiza contrato 2024-0621 Mantenimientos AA UPS, el 19 de diciembre de 2024
Mantenimiento preventivo a equipos de tecnología	Se realiza mantenimiento a equipos de tecnología (computadores, impresoras, escaner) durante el primer semestre de la vigencia con un total de 40 mantenimientos.
Gestión de Mesa de servicios de tecnología, soporte a usuario final.	Se atiende las diferentes solicitudes de soporte realizadas por el canal de mesa de ayuda, correos electrónicos y presencialmente
Capacitación - concientización recursos tecnológicos	Se envía por correo electrónico sensibilización tips de seguridad, se realiza en abril de 2024 capacitación de plataforma Microsoft 365, herramientas de colaboración en línea. Sensibilización con piezas graficas en papel tapiz de los equipos de cada usuario en temas de seguridad.

Es importante destacar que estos contratos y sus respectivas adiciones o prórrogas son fundamentales para asegurar el correcto funcionamiento y la actualización de los servicios tecnológicos, alineándose con los objetivos establecidos en el PETIC.

En el ejercicio de la presente auditoría, se logró evidenciar la existencia del documento GA-CP-02 Caracterización Gestión de la Información en el cual se encuentra el ciclo PHVA para el Fondo de Desarrollo

Caracterización del Procedimiento de gestión de tecnología.	de Proyectos de Cundinamarca-FONDECÚN, por otra parte, la caracterización cuenta con una única versión de fecha 1 de diciembre de 2021.



FONDECUN
FONDO DE DESARROLLO DE PROYECTOS DE CUNDINAMARCA

CARACTERIZACION GESTION DE LA INFORMACION

NOMBRE DEL PROCESO:	GESTION DE LA INFORMACION	CODIGO	GA-CP-02
OBJETIVO	Gestionar el ciclo de vida de las tecnologías de la información y Comunicaciones - TIC, para entregar valor al Fondo por medio de la integración y alineación con la estrategia institucional.		
ALCANCE	Desde la definición de la estrategia de TI alineada a la estrategia institucional, hasta las acciones de control, seguimiento y mejora con sus respectivos informes.		
RESPONSABLE	SUBGERENCIA ADMINISTRATIVA Y FINANCIERA	TIPO	APOYO

PROVEEDOR	ENTRADAS - INSUMOS		SALIDAS	CLIENTE
Ministerio de las Tecnologías de la Información y Comunicaciones MINTIC Proveedores de tecnología Servidores Públicos Fondecun	Normatividad vigente sobre Gobierno Digital Necesidades de sistemas de información, servicios de tecnología, desarrollo de aplicativos y/o diseño de proyectos especiales en TIC Portales Web y Redes Sociales Resultados de los modelos de arquitectura empresarial e	P: Definir para gobierno digital del Fondo, los planes, programas, proyectos, estrategias, riesgos y herramientas de evaluación y seguimiento para cada vigencia. Establecer los lineamientos estratégicos para la gestión de Tecnologías de la Información Establecer la planeación de los proyectos de TIC a implementar Definir el portafolio de productos y servicios de TIC H: Desarrollar la arquitectura de la tecnología de la información acorde al contexto estratégico del Fondo Desarrollar los proyectos de TI por vigencia Desarrollar las acciones para brindar servicios de TI a las partes interesadas del Fondo Desarrollar los servicios de información desarrollar acciones tendientes al cumplimiento de la política Cero papel V: Verificar la apertura prestación de los servicios de información y de tecnología registrando los avances de la gestión. Hacer seguimiento a los planes, programas y proyectos de TIC por vigencia, registrando los avances de la gestión. Monitorear las acciones de prevención del riesgo y cumplimiento cumplimiento a la eficacia del proceso - Indicadores A: Definir e implementar acciones correctivas, preventivas y de mejoramiento del proceso y efectuar seguimiento Desarrollar acciones correctivas inmediatas cuando se materialice el riesgo	Plan estratégico Tecnologías de la Información y las Comunicaciones - PETIC por vigencia Gobierno de TIC Institucional Proyectos de TIC Servicios de Información Servicios de Tecnología Portafolio de productos y servicios de TIC Reportes de gestión y acciones de mejoramiento	GRUPOS DE VALOR EMPLEADOS MINTIC Servidores Públicos Proveedores de tecnología Alta Dirección

REQUISITOS E INFORMACION DOCUMENTADA APLICABLES

NORMOGRAMA	PROCESO SOPORTE	PLANES	MIPG	ISO
Ley 1955 de 2019 art. 147 y 148; Decreto 2106 de 2019 art. 5-17; Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015.	TODOS LOS PROCESOS DE FONDECUN	PETIC Proyectos de TI	CONFORME A LA ESTRUCTURA DEL PROCESO Y SU INTERVENCION CON EL MEGA DE CADA ENLACE MIPG	7.1.3; 7.1.4; 7.1.5; 7.1.5.2; 8.1; 8.2; 8.2.1; 8.2.2; 8.2.3; 8.2.4; 8.5; 8.5.1; 8.5.2; 8.5.3 ; 8.5.4; 8.5.5.

ACTIVIDADES DE SEGUIMIENTO Y/O MEDICION

INDICADOR / ACTIVIDAD DE SEGUIMIENTO	FRECUENCIA	REGISTRO / UBICACION	RESPONSABLES
Ver matriz de Indicadores estratégicos - Plan de acción	NA	NA	NA
Ver matriz de Indicadores de procesos	NA	NA	NA

CONTROL DE CAMBIOS

VERSION	FECHA	IDENTIFICACION DE CAMBIOS	RESPONSABLES
1	1/12/2021	Elaboración del documento.	Subgerencia administrativa y financiera.

PROYECTO	REVISO	APROBO
Nombre: Nelson Andres Reina Cruz Cargo: Contratista Area: Gestión de la Información Fecha: 01 de diciembre de 2021	Nombre: Angela Andrea Forero Mojica Cargo:Subgerente Administrativa y Financiera Area:Subgerencia Administrativa y Financiera Fecha:01 de diciembre de 2021 Nombre: Alejandra Nieto Navas Cargo:Profesional Especializado Area: Planeación Fecha:01 de diciembre de 2021	Nombre:Francisco Javier Sabado Oyoque Cargo: Gerente General Area: Gerencia General Fecha:01 de diciembre de 2021

El documento se encuentra publicado en la página web de la Entidad.
Sin embargo, Se han realizado cambios en el mapa de procesos de la Entidad, por lo cual la caracterización también requiere actualización y cuenta con una única versión desde 2021.

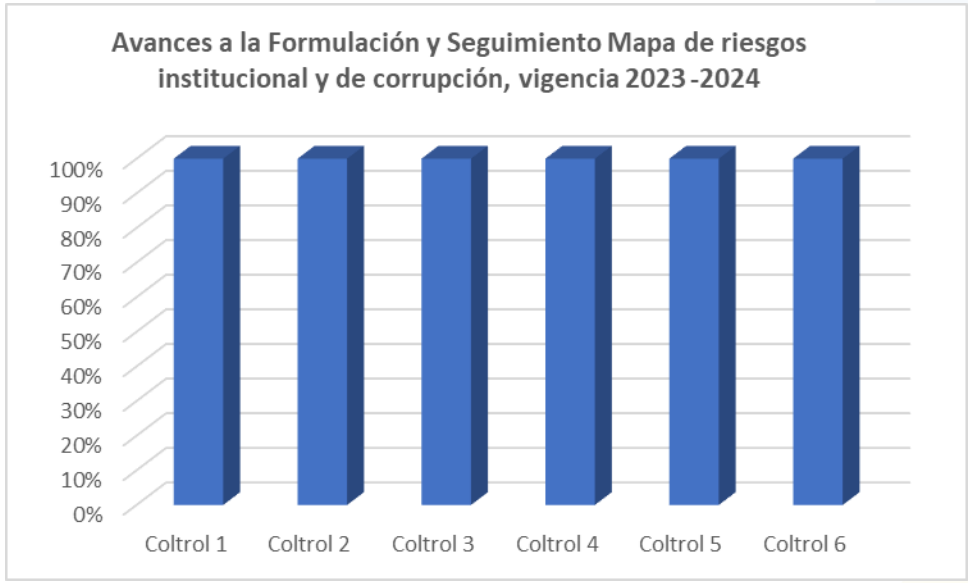
Procedimientos del Proceso de gestión de tecnología	GA-PR-07 Soporte técnico al usuario: Se verificó que se encuentra en la versión 02 de fecha 09/10/2023, debidamente publicado en la paina web de la Entidad en el siguiente link: https://fondecun.gov.co/formatos-procedimientos/ GA-PR-08 Mantenimiento: se evidencia que el procedimiento se encuentra en la versión 02 de fecha 09/10/2023, debidamente publicado en la paina web de la Entidad en el siguiente link: https://fondecun.gov.co/formatos-procedimientos/ GA-PR-09 Registro y creación de usuarios: El procedimiento, se encuentra en la versión 02 de fecha 09/10/2023, debidamente publicado en la paina web de la Entidad en el siguiente link: https://fondecun.gov.co/formatos-procedimientos/ En evaluación con el auditado, los procedimientos no requieren cambios toda vez que las rutas establecidas en los mismos funcionan de manera correcta.
Formulación y Seguimiento de Plan de Acción 2023-2024	Se evidencia que la Gestión Administrativa, Tecnológica y Recursos Físicos con el apoyo de la Oficina de Planeación formuló el plan de Acción 2024 en el siguiente link: https://fondecun.gov.co/plan-de-accion/#298-795-2024-1725026488. El Plan de Acción para la vigencia 2024 tuvo las siguientes siete (7) actividades para ejecutar por parte de la Gestión Administrativa, Tecnológica y Recursos Físicos: 1. Realizar el mantenimiento preventivo y correctivo de los equipos de cómputo, impresoras y equipos de red de la entidad. Una vez revisada la actividad se evidenció en la auditoría que realizaron dos mantenimientos a los equipos en la vigencia 2024 2. Adquirir los servicios tecnológicos requeridos por la entidad. (Contratos enlace de internet, alquiler de equipos, licencia antivirus, servicio de almacenamiento nube, mantenimiento de aire acondicionado - ups y Servicio hosting página web - correos)

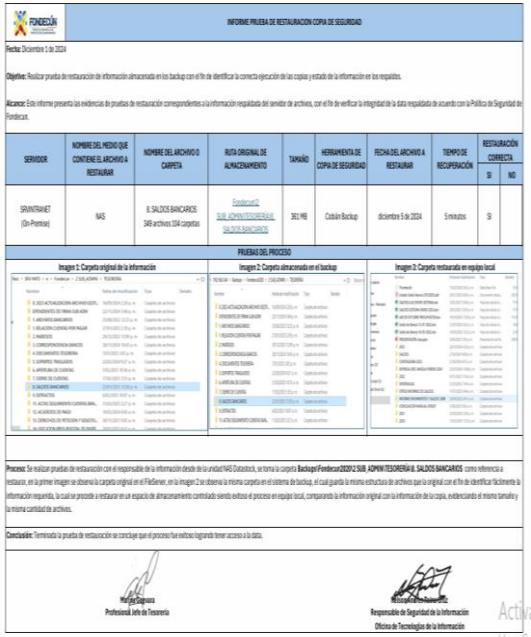
Formulación y Seguimiento de Plan de Acción 2023-2024	Como se indica en el PETIC, la Gestión administrativa, Tecnología y Recursos Físicos, realizó de manera oportuna la contratación para la continuidad de los servicios tecnológicos en FONDECÚN 3. Ampliación de la banda ancha de internet Para mejorar la calidad del servicio en cuanto al ancho de banda, se pudo verificar que se realizó el contrato 2024-0331 con el cual se garantiza internet a 200Mbps con el proveedor ETB hasta el 01/02/2025. 4. Estudios previos para la viabilidad de compra de equipo de cómputo para el equipo directivo. Por temas de presupuesto, se tomó la decisión de contratar el servicio de alquilar los equipos de cómputo. 5. Estudio y contratación e implementación de una solución de colaboración en línea que permita la comunicación y utilización de herramientas tecnológicas para mejorar el desempeño y optimización (flexible, colaboración on-line. Para mejorar el desempeño y optimizar de la colaboración en línea la Gestión Tecnología realizó la contratación del servicio de office 365, mediante el cual se implementan aplicaciones de colaboración en línea como Microsoft Teams, Micrsoft SharePoint, One Drive, permitiendo tener mejor comunicación entre los colaboradores de la entidad para la ejecución de actividades. 6. Revisar, actualizar y hacer seguimiento del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información. Mediante la evaluación realizado al mapa de riesgos, se evidencia la implementación del Plan Estratégico de Tecnologías de la Información, además, se verificaron los mantenimientos preventivos, Backup, campañas de seguridad, Gestión del Firewall y de la consola de antivirus, realizados por la Gestión Tecnología. 7. Revisar, actualizar y hacer seguimiento al Plan de Seguridad y Privacidad de la Información y PETI.

	Para la presente actividad se constató que se elaboró el Plan de Tratamiento de Riesgos de Seguridad y el plan de Seguridad y privacidad de la información los cuales fueron publicados en el sitio web de la Entidad, se adelantan acciones en el desarrollo de estos planes como: -Se realiza el levantamiento de activos de información -Se realiza sensibilización a los funcionarios y contratitas de la entidad mediante correos electrónicos en "Hábitos seguros que pueden evitar riesgos de Ciberseguridad", igualmente se sensibiliza con información con tips de seguridad en el fondo de pantalla de cada equipo. -Se realiza con la colaboración con el área de planeación el levantamiento de riesgos TIC el cual es presentado y se lleva control de las actividades propuestas para la gestión del riesgo. -En la ejecución del plan se desarrollan actividades para la contratación de servicios que permitan implementar controles de seguridad
Formulación y Seguimiento Mapa de riesgos institucional y de corrupción, vigencia 2023 -2024	Se evidencia la formulación y seguimiento al mapa de riesgos institucional de corrupción, y las mitigaciones de los mismos así: Causa del riesgo: Hurto o daño de información de la entidad debido a un virus o hackeo, intrusión y falta de integridad informática (HACKERS) Causa Raíz: Ausencia en la estructuración e implementación del Modelo de Seguridad y Privacidad de la Información - MSPI de la entidad. Descripción del riesgo: Posibilidad de pérdida de información o integridad de la misma, por manipulación indebida no autorizada de la información de la entidad. Control 1: El responsable de la gestión tecnológica, determina el estado de la plataforma tecnológica y realiza acciones técnicas para garantizar la continuidad del servicio o solicitar servicios especializados externos. Actividad para mitigar el riesgo: Proyectar e implementar el Plan estratégico de tecnologías de la información PETI para el periodo plan de acción, Plan de compras del área para la vigencia, presentar para aprobación al Comité Institucional de Gestión y Desempeño

Formulación y Seguimiento Mapa de riesgos institucional y de corrupción, vigencia 2023 -2024	Verificación de la auditoría: se evidencia el contrato Nro. 2024-0366 hasta el 18 de febrero de 2024. para el Alquiler de equipos tecnológicos y periféricos con instalación, configuración y mantenimiento para el Fondo de Desarrollo de Proyectos de Cundinamarca – Fondecún. Se realiza contratación del personal de apoyo a la gestión tecnológica mediante contrato 2024-0275 de fecha 7 de mayo de 2024 hasta el 31 de diciembre de 2024 Actualmente se está llevando el proceso IPMC-06-2024, para la contratación del mantenimiento del aire acondicionado y de las UPS de la entidad, proceso que está en etapa de evaluación de propuestas. Control 2: El responsable de la gestión tecnológica determina el estado de la plataforma tecnológica y establece el plan de mantenimiento y realiza las acciones técnicas para garantizar la continuidad de servicio o solicita servicios especializados externos. Actividad para mitigar el riesgo: Implementación y seguimiento a la ejecución del plan de mantenimiento, cumpliendo con el cronograma de actividades. Verificación de la auditoría: La presente auditoría evidenció la realización de dos mantenimientos en la vigencia 2024 a los equipos tecnológicos (computadores, impresoras, escáner). Control 3: El responsable del proceso en la etapa de planeación determina las necesidades de adquisición y asegura la contratación y licenciamiento del software de seguridad, antivirus y firewall. Actividad para mitigar el riesgo: Realizar las contrataciones dando cumplimiento a las actividades para ejecutar la planeación de los proyectos de TIC a implementar mediante la definición del portafolio de productos y servicios de TIC. Teniendo en cuenta lo manifestado por el auditado se prescinde de la renovación del contrato de licencias de antivirus. En su lugar, se llevarán a cabo los procesos de contratación necesarios para la renovación y actualización de los sistemas operativos Microsoft de los equipos de la Entidad. Esto permitirá aplicar y aprovechar las funcionalidades y prestaciones que ofrece Microsoft Defender, garantizando así una mayor seguridad y protección para nuestros sistemas.

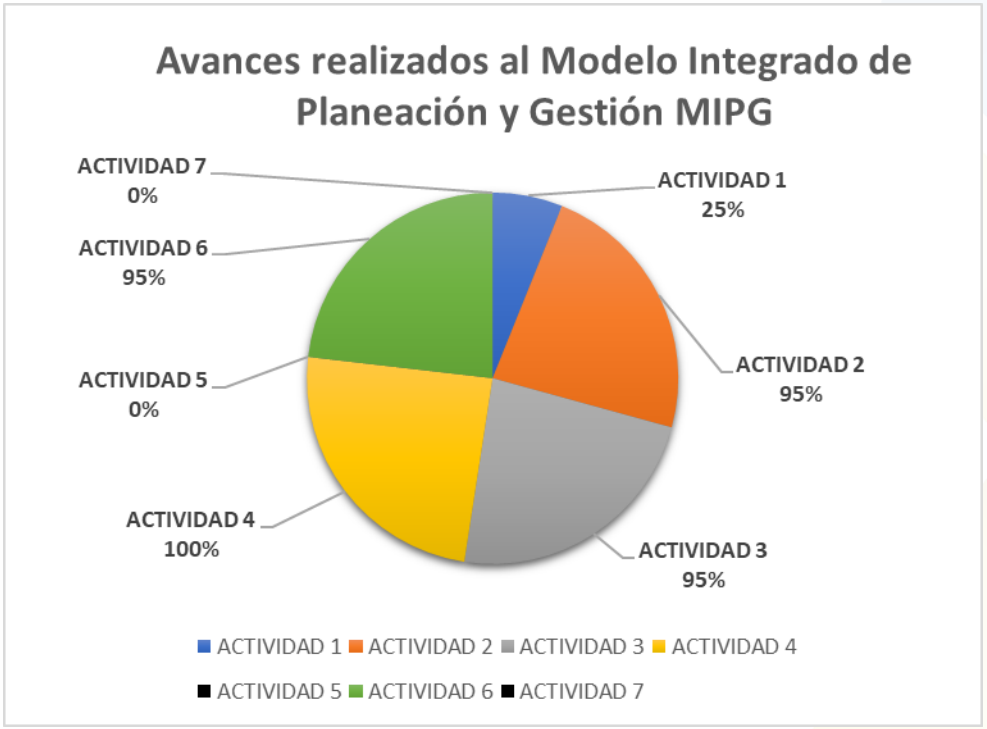
Formulación y Seguimiento Mapa de riesgos institucional y de corrupción, vigencia 2023 -2024	Control 4: El responsable del proceso traslada el conocimiento y buenas prácticas de ciberseguridad son los usuarios de la entidad, mediante proceso de Capacitación. Actividad para mitigar el riesgo: Realizar campañas o capacitación de Ciberseguridad a los usuarios de la entidad. Verificación de la auditoría: se realiza capacitación a los funcionarios y contratistas de la Entidad en Teams de ciberseguridad y manejo de servicios de tecnología, como políticas de usuario procedimiento de gestión de usuarios, gestión de usuarios y contraseñas, Control 5: Se realiza un monitoreo a través de la aplicación del antivirus y FIREWALL. Genera un informe y convoca al Comité Institucional de Gestión y Desempeño cuando se presente un incidente o evento potencial de seguridad de la información para gestionar de manera oportuna y efectiva los incidentes. Actividad para mitigar el riesgo: Realizar seguimiento y control al monitoreo a través de la aplicación del antivirus y FIREWALL. Generar informe. Verificación de la auditoría: Se realiza verificación de estado del antivirus básico de Microsoft defender el cual está incorporado en Windows de los equipos de la Entidad identificando que se esté actualizando, las aplicaciones se estén ejecutando para el control de seguridad, se verifica funcionalidad del firewall de la entidad control conectividad, verificación de tráfico entrante y saliente. Control 6: El responsable del proceso, mediante el plan de seguridad de la información implementa acciones que respalden la información con copias de seguridad. Actividad para mitigar el riesgo: Realizar backup periódico de la información internamente y un espacio externo a la entidad. Generar informe. Verificación de la auditoría: Durante el periodo se realiza y supervisa la ejecución de Backup de la formación de la Entidad, copias de seguridad realizadas diariamente según configuración el repositorio NAS (Network Attached Storage), se han realizado 169 procesos de Backup de información para los cuales se tiene los logs de registró de cada tarea completada actualizando la información.

Formulación y Seguimiento Mapa de riesgos institucional y de corrupción, vigencia 2023 -2024	 Se destaca el cumplimiento del 100% de los controles.
Avances realizados al Modelo Integrado de Planeación y Gestión MIPG **GOBIERNO DIGITAL**	En la verificación realizada al Modelo Integral de Planeación y Gestión -MIPG, se logró evidenciar que el proceso de gestión administración tecnológica realizó las siguientes actividades: Actividad: Incluir en el plan de tecnologías y el plan de contratación para la próxima vigencia la realización de análisis de vulnerabilidades de seguridad.

Avances realizados al Modelo Integrado de Planeación y Gestión MIPG **GOBIERNO DIGITAL**	En entrevista al auditado manifestó que la actividad fue programada para que el Informe de vulnerabilidades de seguridad, sea entregado en el mes de junio de 2025, por lo tanto, se incluyó en el plan de adquisiciones la contratación de análisis de vulnerabilidades de seguridad. Actividad: Realizar pruebas de recuperación del sistema de información con el contratista del sistema SIIWEB Teniendo en cuenta que el servicio se encuentra contratado, el proveedor envía registro de copias de seguridad realizadas evidenciando de esta forma que la actividad se ha llevado a cabo. Se evidencian dos (2) Informes de prueba de restauración copias de seguridad de fechas noviembre y diciembre de 2024:  

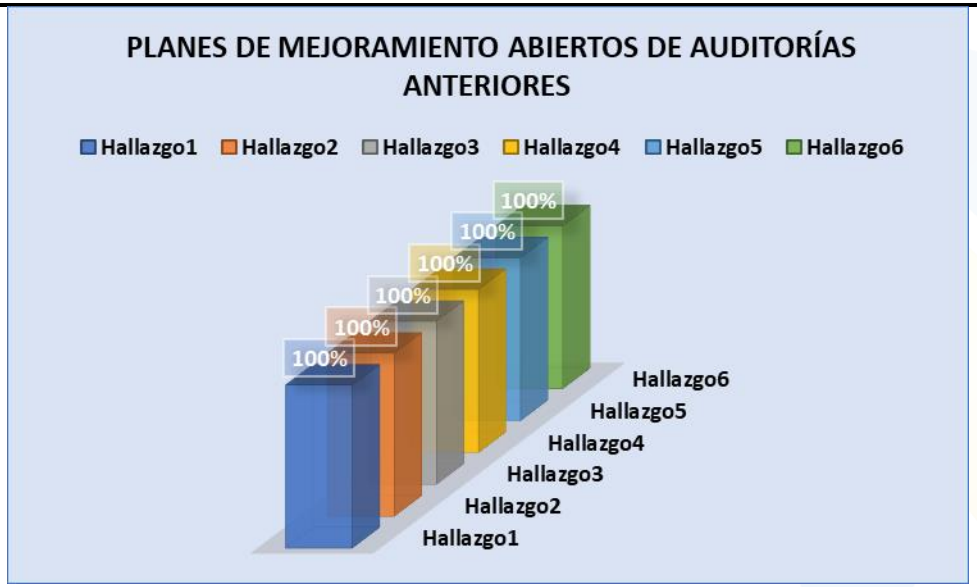
Avances realizados al Modelo Integrado de Planeación y Gestión MIPG **GOBIERNO DIGITAL**	En cada prueba de restauración se evidencia el servidor desde donde se realiza la copia, nombre del medio que contiene el archivo a restaurar, nombre del archivo o carpeta, ruta original de almacenamiento, tamaño, herramienta de copia de seguridad, fecha del archivo a restaurar, tiempo que tomó el respaldo y por último si la restauración fue exitosa o no. Actividad: Actualizar el conjunto de datos abiertos y se publicaran el portal datos.gov En la presente auditoría se evidencia que se realizaron dos actualizaciones una el 26 de marzo y 4 el septiembre de la vigencia de 2024, al conjunto de Datos Abiertos, y fueron publicados en la Página web de la Entidad en el siguiente link https://fondecun.gov.co/transparencia-y-acceso-a-la-informacion-publica-2021/#1636729281103-f3d0c118-f010 Entre los documentos 7.1.1 Registros de Activos de información 7.1.2 Índice de información clasificada y reservada 7.1.3 Esquema de publicación de información Una vez verificados los documentos en la página web de la Entidad, se evidencia que los documentos no están en formatos de la Entidad. Actividad: Actualizar y aprobar el inventario de activos de seguridad y privacidad de la información Se pudo verificar que se realizó el inventario de activos de información en agosto de 2024, sin embargo, no está aprobado, además el documento no se encuentra en formato de la Entidad. Actividad: Realizar seguimiento a la implementación de la hoja de ruta establecida en el PETIC En el ejercicio de auditoría se comprobó que en la vigencia 2024 se realizaron las actividades, como contratación de servicios de tecnología necesarios para el correcto funcionamiento de la Entidad, gestión seguridad mediante implementación de políticas de

Avances realizados al Modelo Integrado de Planeación y Gestión MIPG **GOBIERNO DIGITAL**	usuario, permisos de acceso, capacitaciones, los cuales hacían parte de la hoja de ruta del Plan Estratégico de las Tecnologías Informática -PETIC Actividad: Definir y actualizar procesos y procedimientos de gestión, gobierno y seguridad de TI Observación: no se evidencia avances en la actividad, el auditado manifiesta que la actividad se encuentra prevista para realizarse a junio de 2025 Actividad: Realizar pruebas de restablecimiento de información desde las copias de seguridad para asegurar la disponibilidad de los datos en caso de incidentes El auditado indica que se han realizado pruebas ejemplo: se verifica el Backup para constatar que la información se haya guardado completa-accesible, legible y actualizada, sin embargo, las pruebas no están programadas en un cronograma, se realizaron en fechas distintas al azar, además, no se cuenta con un informe de las mismas. Actividad: Realizar diagnostico con la herramienta de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI), presentándolo y aprobándolo el diagnóstico en el Comité de Gestión y Desempeño Institucional. Observación. No se evidencian avances de la actividad, el auditado manifiesta que la actividad se encuentra programada.

Avances realizados al Modelo Integrado de Planeación y Gestión MIPG **GOBIERNO DIGITAL**	 Es importante evaluar las dificultades que se han tenido para el cumplimiento de las actividades y programar nuevas acciones para que los avances sean óptimos.
	En la vigencia 2024, la Gestión Administrativa, Tecnológica contó un Plan de mejoramiento producto de auditoria internas, A continuación, los avances de las actividades:

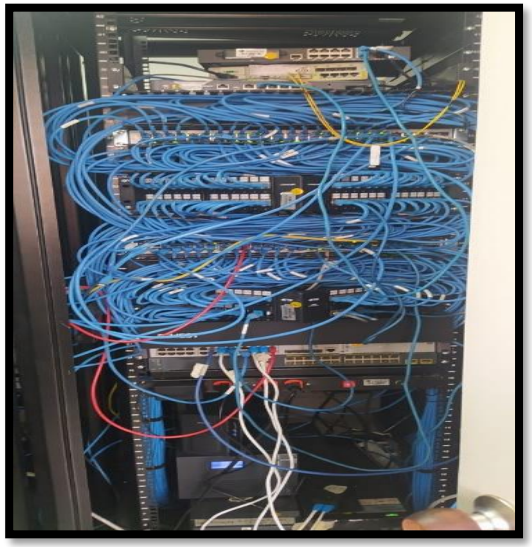
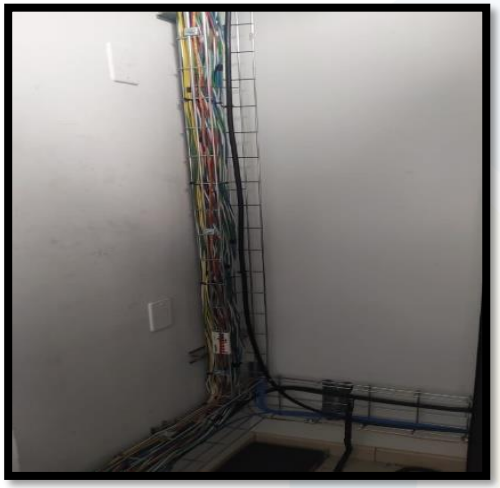
Planes de mejoramiento abiertos de auditorías anteriores	Hallazgo 1: No se cuenta con un Plan de Continuidad de Negocio Se verifica existencia del Plan de continuidad del negocio, el cual fue aprobado por Comité Institucional de Gestión y Desempeño, como consta en el acta del 13 de diciembre de 2023, además, la socialización de plan de contingencia y plan de continuidad mediante correo electrónico del 16 de enero de 2024 1. GA-PLA-01 Plan de contingencia informática 3. GA-PLA-03 Plan de continuidad, por lo tanto, el hallazgo fue subsanado. Hallazgo 2: Bajo avance en el ciclo de funcionamiento e implementación del MSPI Como avance la Gestión Tecnología se propuso en la vigencia 2024 adelantar la implementación de MSPI y a 31 de diciembre del mismo año tener un porcentaje de avance del 50% lo cual cumplió toda vez que se observó -Aprobación y socialización del plan de continuidad TIC -Mapa de riesgos de seguridad y ciberseguridad -PETI -Actualización inventario de activos -Plan de tratamiento de riesgos. Avance cumplido Hallazgo 3: No se socializa oportunamente el procedimiento de Gestión de incidentes seguridad, y el formato-informe incidentes de seguridad
Planes de mejoramiento abiertos de auditorías anteriores	Se evidencia la socialización a funcionarios y contratistas de la Entidad mediante correo electrónico el día 26 de enero de 2024 del procedimiento de Gestión de Incidentes código GA-PR-01 versión 01. Sin embargo, una vez se ingresa a la pagina web de la Entidad, se evidencia que el código GA-PR-01 pertenece al procedimiento control de documentos en la versión No. 02, y no al procedimiento Gestión de Incidentes. Subsanado con hallazgo nuevo Hallazgo 4: Realizar y socializar guía contacto con autoridades y grupos de interés, para el escalamiento de incidentes según la estructura de la entidad

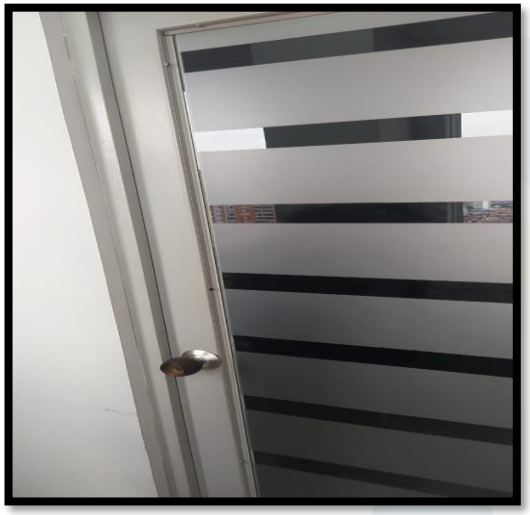
Planes de mejoramiento abiertos de auditorías anteriores	La presente auditoría evidencia la socialización a los funcionarios y contratistas de la Entidad mediante correo electrónico del día 26 de enero de 2024, de un documento denominado Guía de Contacto con Autoridades y Grupos de Interés, sin embargo, este carece de código, lo cual indica que no ha sido aprobado por el comité institucional o gestionado ante Planeación para el respectivo código de identificación. Subsanado con observación. Hallazgo 5: Realizar revisión del capítulo 5.5 de la guía-Guía Nro. 21 para la Gestión y Clasificación de Incidentes de Seguridad de la Información por parte del Ministerio de Tecnologías de la Información y las Comunicaciones, con el fin de completar las etapas y acciones propuestas para detectar, identificar, y gestionar incidentes de seguridad. Se realiza la gestión de usuarios de la Entidad configuración de permisos de acceso permitiendo tener control sobre los recursos e información. Se evidencian dos informes incidentes de seguridad de la información, en el respectivo formato y resueltos de acuerdo a los procedimientos establecidos para los mismos. Con lo anterior, el hallazgo es Subsanado Hallazgo 5: Mapa de riesgo incompleto en el tratamiento de riesgos El mapa de riesgos fue alimentado con el apoyo del área de planeación cual fue presentado y aprobado con 5 actividades para la Gestión Tecnológica.	

	 Cabe destacar que se realizaron las actividades pertinentes las cuales permitieron subsanar los 6 hallazgos producto de la auditoría anterior, sin embargo, es importante revisar las recomendaciones de los hallazgos 3 y 4.
Acta de Ultima transferencia documental realizada al archivo central de la entidad	Se evidencia acta de fecha 14 de noviembre de 2024 de la última transferencia documental realizada al archivo central de la Entidad debidamente diligenciado y firmada en el formato actualizado FORMATO ÚNICO DE INVENTARIO DOCUMENTAL Código: GA-FR-04
	Se evidencia la existencia de la Política general de Seguridad y privacidad de la Información, la cual se encuentra publicada, aprobada y socializada el 18 de abril 2024 por correo electrónico a los funcionarios y contratistas.

Política de Seguridad y Privacidad de la Información	Resolución No. 045 octubre de 2020, la cual se encuentra publicada en la página web de la Entidad link: https://fondecun.gov.co/normatividad-del-orden-territorial/#266-269-2020 Ruta: Transparencia-Normatividad- numeral 2.1.5.A Política y lineamientos sectoriales Carpeta año 2020 Observación: Una vez revisada la política de seguridad y privacidad de la información, se evidencia que en la misma falta incluir todas las dependencias de FONDECUN con roles y como responsables en cada área para el respectivo cumplimiento de la política ejemplo: Rol: Funcionarios y Contratistas / Responsabilidades: proteger los activos bajo su custodia, aplicando los controles de seguridad establecidos, realizar la entrega de activos de información en el momento en que se desvinculen de la Entidad. El cumplimiento de la política va desde la alta gerencia hasta los visitantes o proveedores de la Entidad, por lo que es importante delegar roles y responsabilidades a cada uno dentro de la política; también es importante, tener en cuenta y documentar en la política que el incumplimiento de la misma por cada uno de los responsables se configura como un incidente de seguridad. Por otra parte, no se evidencia en la política de seguridad responsabilidades del Oficial de Seguridad, FONDECÚN como Entidad pública debe contar con un oficial de seguridad y privacidad de la información el cual se encargará de planear, coordinar y administrar los procesos de seguridad de la información, también se encargará de difundir la cultura de seguridad informática entre otras responsabilidades. Ministerio TIC inauguró el Centro de Operaciones de Seguridad Nacional de Colombia (SOC) para blindar la ciberseguridad de las Entidades del país se recomienda revisar el SOC para ver en que se puede beneficiar la Entidad. Guía No. 4 de Mintic -Seguridad y privacidad de la información (habla de un Responsable de Seguridad de la Información para la Entidad)
Política de Seguridad y Privacidad de la Información	
Procedimientos de seguridad de información	Para la presente auditoría el proceso de apoyo Gestión Tecnología allegó los siguientes procedimientos: ➢ GA-PR-07 Soporte técnico al usuario ➢ GA-PR-08 Mantenimiento ➢ GA-PR-09 Registro y creación de usuarios

	Además, allega documento denominado lineamientos de seguridad informática fondo de desarrollo de proyectos de Cundinamarca- FONDECÚN, el cual contiene 12 políticas de seguridad de la información. Observación: revisar la posibilidad de que algunas políticas pueden convertirse en procedimientos en la Entidad.
Inventario de activos de información	Se evidencia documento en Excel Base de Datos de inventario de activos de información el cual se encuentra en formato de la Entidad, el auditado indica que se realizaron mesas de trabajo con las áreas, entre febrero y mayo de 2024 para el levantamiento de la información.
Plan de tratamiento de riesgos de seguridad de la información	Se evidencia documento denominado Plan de Tratamiento de seguridad 2024, sin embrago, no se le realizó seguimiento.
DATA CENTER	En recorrido por las instalaciones se tuvo acceso al Data Center de FONDECUN, al cual de la Entidad una sola persona tiene permiso para ingresar, la presente auditoría evidencia que la seguridad física y del entorno es muy baja teniendo en cuenta que no se cuenta con cámaras de seguridad en el pasillo, la puerta de ingreso es poco segura, una vez dentro se verifica que se cuenta con dos UPS, el cableado se encuentra en optimas condiciones, se cuenta con aire acondicionado en perfecto estado el cual garantiza el buen funcionamiento de los equipos en el centro de cómputo, sin embargo, se observan elementos tecnológicos como impresora multifuncional, teclado, entre otros dentro del Data Center que no deben estar en el lugar, el auditado manifestó que la Entidad no cuenta con el espacio suficiente por lo que se guardaron ahí.

DATA CENTER	  

DATA CENTER	   

En el ejercicio de la presente auditoría, se destaca las actividades realizadas por el funcionario a cargo del proceso de apoyo de la Gestión Tecnológica, toda vez que se evidenció avances y subsanaciones de hallazgos de auditorías anteriores, así como también se verificó avances significativos en la Implementación del Modelo de Seguridad y Privacidad MSPI y las acciones tendientes al cumplimiento de la norma ISO 27001.

GESTIÓN DE BIENESTAR Y DEL TALENTO HUMANO

En auditoría a la Gestión de bienestar y del Talento Humano donde se analizó y evaluó la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI.

El proceso de Talento humano, en el ejercicio de sus funciones da cumplimiento a sus responsabilidades como área responsable de:
Capacitaciones de inducción y reinducción a funcionarios y contratistas de la Entidad, dónde de acuerdo a la información relevante y transversal para funcionarios y contratistas, en conjunto con los líderes de procesos se realiza cronogramas y se tienen programadas tres (3) inducciones y reinducciones al año.

Los activos de información del proceso de TTHH, se encuentran en Drive y en red con restricciones para su acceso, los auditados tiene conocimientos de cuáles son sus activos entre los que mencionan circulares, resoluciones, actas, hojas de vida las cuales se encuentran en físico, cabe destacar que los activos de información del proceso de Talento Humano fueron actualizados en agosto de 2024.

En entrevista a las auditadas, se evidenció que se tiene conocimiento de la existencia del documento “Política de Seguridad y Privacidad de la Información”, sin embargo, fue necesario retroalimentarlas respecto al documento “Lineamientos de seguridad Informática” donde se encuentra las 12 políticas documentas por la Entidad, de las cuales algunas se aplican en el ejercicio de sus funciones.

Teniendo en cuenta que la planta de la Entidad es pequeña y que los cargos son específicos, el proceso de TTHH no cuenta con un procedimiento para el traslado entre áreas de funcionarios:

Se cuenta con el formato “VINCULACIÓN Y DESVINCULACIÓN DE PERSONAL” código: GTH-PR-03 el cual se encuentra en la versión 02 para el proceso de selección y vinculación de personal de la Entidad, las auditadas muestran la ruta en la página web donde se encuentra el documento en mención, y se hace un paso a paso de cómo se vinculan funcionarios ya sean de libre nombramiento y remoción, de planta y /o contratista, demostrando de esta forma que se tiene total conocimiento y dominio del procedimiento en el área.

Desde el proceso de Talento Humano se cuenta con usuarios funcionales a cargo de una funcionaria para el manejo de los aplicativos SIGEP II y SIIWEB Se realiza recorrido y se verifica in situ desde el archivo de las hojas de vida se solicitan dos hojas de vida de funcionarios al azar donde se verifica la existencia dentro de las obligaciones de los contratos un literal dentro de las obligaciones donde se especifica el acuerdo y confidencialidad de la información, por lo tanto, no se cuenta con un documento denominado "acuerdo de confidencialidad de la información".

El proceso de TTHH, cuenta con un diseño de seguridad perimetral el cual fue realizado por la ARL, en recorrido, se evidencia la existencia de señalización, rutas de evacuación, para lo cual las auditadas indican hay un plano de rutas de evacuación que se socializa en la inducción y reinducción a los funcionarios, la única zona segura de la Entidad son los baños.

Por otra parte, las hojas de vida se encuentran bajo llave y en custodia por una funcionaria, las hojas de vida de las personas que no están activas, se entregan al archivo de la Entidad para la gestión de acuerdo a TRD, sin embargo, actualmente se tienen un bajo estudio por lo cual no han sido remitidas al archivo.

Controles físicos de acceso a la Entidad: el proceso de TTHH controla el acceso a la Entidad mediante la asignación de tarjetas de proximidad a funcionarios y huella a contratistas, esto en conjunto con la administración del edificio a quien se le envía correo electrónico con el nombre y número de identificación de la persona y además especificando el tiempo al que tiene permitido el ingreso la persona, el cual para los funcionarios de planta se indica que de forma indefinida y contratistas hasta el termino de los respectivos contratos.

Incidentes de seguridad de información: Las auditadas reportan un único incidente de seguridad, el hurto de un equipo de cómputo, para lo cual, la información de las carpetas se encontraban respaldadas en un backup que se realiza desde la gestión tecnológica, se procedió a dar parte a las autoridades competentes y aunque existía un formato para retiro de computador de la Entidad, a raíz de lo sucedido teniendo en cuenta que el formato anterior no estaba por adopción y no estaba controlado
Actualmente se fortaleció y adoptó para más seguridad el formato denominado "Solicitud retiro de equipo" código GA-FR-29.

Controles por amenazas externas y ambientales adoptados por el proceso, como precaución el área cuenta con los activos de información digitalizados y guardados en la red a los cuales se les realiza backup desde el área de tecnología, en cuanto a las hojas de vida manifiestan que las mismas no se encuentran digitalizadas toda vez que en caso de un incidente se pueden recuperar descargándolas y solicitando a funcionarios y contratistas volver a firmarlas.

Como gestión física, a Entidad cuenta con seis (6) extintores y un (1) botiquín.

Sin procedimiento codificado para el préstamo de hojas de vida, en entrevista, las auditadas manifestaron que cuando se requiere una hoja de vida se deben enviar un correo electrónico a la funcionaria que custodia las hojas de vida, donde se debe especificar porqué y para qué se requiere la hoja de vida, con lo que la funcionaria busca en el expediente la o las paginas para el prestamos de las mismas, con lo anterior, se garantiza la privacidad y seguridad de la información toda vez que no se realiza el préstamo de la hojas de vida completa.

En verificación in situ, del puesto de trabajo de un funcionario del área de TTHH, se evidencia que el escritorio físico así como el virtual cuentan con elementos, aun cuando existe la política de escritorio limpio, para lo cual el funcionario indica que, el escritorio virtual se encuentra con muchas carpetas y archivos porque se le facilita mientras está trabajando, disponer de la información desde el escritorio y no dirigirse a los discos locales como el C o D donde deben estar almacenados, pero que una vez termina de trabajar con los mismos, los retira del escritorio.

PROCESO MISIONAL ESTRUCTURACIÓN GERENCIA Y ADMINISTRACIÓN DE PROYECTOS

En auditoria se verificó el estado de la implementación del modelo de seguridad y privacidad de la información al proceso, así como inventario de activos, riesgos de información y plan de tratamiento de riesgos obteniendo lo siguiente:

El auditado tiene conocimiento sobre el la política de seguridad de la información implementada en la Entidad, además, manifiesta que desde la gestión tecnológica y en jornadas de inducción y reinducción les comparten la información a los funcionarios y contratistas.

Se realiza retroalimentación sobre el documento “lineamientos seguridad informática” el cual contiene 12 políticas y de las cuales en el ejercicio de las actividades diarias los funcionarios del área de alguna manera implementan.

Por otra parte, el auditado indica que en el área son más de 80 contratistas y cada uno debe ser responsable de la organización de carpetas físicas y virtuales.

Activos de información: se identifica desconocimiento del documento “activos de información”, el auditado manifiesta no tener información acerca de si se realizó levantamiento de información respecto a los activos del área, sin embargo, indica que existe una carpeta de sharepoint con contratos derivados hojas de control y demás …

Las carpetas se actualizan a diario, pero no se lleva control a manera de inventario, solo manejan archivo digital de manera la cual se organiza de forma cronológica, por lo tanto, a la información producida por el área se le garantiza la disponibilidad, integridad y confidencialidad con el Sharepoint que además es administrado por los ingenieros de sistemas.
Teniendo en cuenta que no existe inventarios de activos, no se encuentra definido responsable por cada activo, sino que cada gerente que son 21, tienen la responsabilidad de custodiar la información producida.

Clasificación, etiquetado y manejo los activos de información: Desde el área de archivo envían una hoja de control y de esa manera se didnetifican los documentos.

El auditado manifestó no tener conocimiento al plan de tratamiento de riesgos, por lo tanto, no hay avances, además manifiesta que en el proceso no corren

riesgos porque la información esta resguardada con sharepoint y que además se realiza backup.

El auditado indica no tener conocimiento de qué es un incidente de seguridad de la información, se realiza retroalimentación, y el auditado manifiesta el procedimiento para reportar un incidente y que en su momento realizó el reporte de un incidente de seguridad de la información donde se vio afectada toda la Entidad por culpa de in virus en ese momento, por o que desde la gestión tecnológica se tomaron las acciones pertinentes para mitigar.

Se evidencia conocimiento acerca del procedimiento para para la solicitud de medios removibles de la Entidad, así como el retiro de permisos de aplicativos, carpetas y demás a funcionarios que se desvinculen de la Entidad, asignación de usuario, correo electrónico mediante formato implementado y codificado en Fondecún.

PROCESO ESTRATÉGICO GESTIÓN COMERCIAL Y DE COMUNICACIONES

En la evaluación de la auditoría se verificó el estado de la implementación del modelo de seguridad y privacidad de la información al proceso, así como inventario de activos, riesgos de información y plan de tratamiento de riesgos obteniendo lo siguiente:

El auditado tiene conocimiento sobre el la política de seguridad de la información implementada en la Entidad, además, manifiesta que, si ha sido capacitado en el presente año el 11 de marzo 2025 en el piso 20, y que las capacitaciones son en jornadas de inducción y reinducción de manera virtual y presencial.

Se realiza retroalimentación sobre el documento “lineamientos seguridad informática” el cual contiene 12 políticas y de las cuales en el ejercicio de las actividades diarias los funcionarios del área de alguna manera implementan.

Activos de información: se identifica desconocimiento del documento “activos de información”, sin embargo, cuenta con un repositorio de activos de información (pero no inventario) se realiza retroalimentación sobre la importancia del documento, por otra parte, manifiesta no conocer los activos de información del proceso como tal.

Sin responsables de activos de información, no obstante, la información que guarda el auditado en un repositorio la salvaguarda y mantiene actualizada.

No se cuenta con la clasificación de activos de información de acuerdo a la Confidencialidad, Integridad y Disponibilidad de la Información.

El área cuenta con el aplicativo SICOF: el cual requiere para el ingreso al sistema clave y usuario de acuerdo a solicitud verbal dada por el subgerente técnico interadministrativo se evidencia conocimiento de los documentos código EGAP-PR-01. - Desarrollo integral de los proyectos y/o contratos derivados EGAP-PR-02 - Ejecución y seguimiento de convenios o contratos interadministrativos EGAP-PR-03 - Novedades en la ejecución de la contratación EGAP-PR-04

El área no cuenta con plan de tratamiento de riesgos, se realiza retroalimentación, se evidencia la implementación de la política de escritorio limpio y pantalla limpia 5.13. políticas escritorio limpio y equipos desatendidos.

Con conocimientos solidos acerca de los incidentes de seguridad de la información, sin embargo, no conoce el procedo implementado para el reporte de un incidente de seguridad de la información, se realiza cambio de password para ingreso al equipo de computo cada tres meses, se realiza retroalimentación sobre el procedimiento para el reporte de incidentes de seguridad de la información actualmente en Fondecún.

Se tiene conocimiento de cómo se lleva a cabo la solicitud de medios removibles, y desde el área se cuenta con credenciales para el ingreso al aplicativo Sicof el cual es de la Entidad, actualmente un funcionario le asigna credenciales a los gerentes, y, para el retiro de credenciales, se emite un paz y salvo, el cual debe ir firmado por la subgerencia técnica, gestión documental y tecnologías, cuando el documento llega al área se verifica se cancelan credenciales en Sicof , por último en el área solo hay dos funcionarios de planta, cuando alguno falta, el otro sustituye y es una manera de garantiza ingreso a la información de SICOF y salvaguardar la privacidad de la información

Se evidencia que el auditado tiene conocimiento del proceso de cómo se realiza la asignación de correo electrónico, sin embargo, falta el conocimiento del procedimiento como tal una sola vez se realizó cambio de contraseña.

Algunos funcionarios del área realizan préstamo de equipos, sin embargo, el auditado no tiene conocimiento del procedimiento para la solicitud, entrega y devolución de equipos de cómputo.

La información producida se encuentra guardada en el repositorio de información Sharepoitn que se creó en Fondecún (carpeta comunicaciones)

VERIFICACIÓN CUMPLIMIENTO NORMA TÉCNICA NTC COLOMBIANA 5854 PAGINA WEB FONDECÚN

Se realizó entrevista al funcionario a cargo de la pagina web de la Entidad y se verificó la siguiente información:

Tabla No. 1: Verificación cumplimiento NORMA TÉCNICA NTC COLOMBIANA 5854
PAGINA WEB FONDECÚN https://fondecun.gov.co/

REQUISITO	PREGUNTA/DESCRIPCION	RESULTADO			OBSERVACIONES
		CUMPLE	NO CUMPLE	C.PARCIALMENTE	
REQUISITOS SOBRE IDENTIDAD VISUAL Y ARTICULACIÓN CON PORTAL ÚNICO DEL ESTADO COLOMBIANO GOV.CO.	TOP BAR (GOV.CO)	X			
	Top Bar o barra en la parte superior del sitio web, que redireccione al Portal Único del Estado Colombiano GOV.CO	X			
FOOTER O PIE DE PAGINA	Imagen del Portal Único del Estado Colombiano y el logo de la marca paísCO - Colombia	X			
	Nombre de la Entidad, como mínimo una dirección incluyendo el departamento (si aplica) y municipio o distrito.	X			
	Vínculo a redes sociales, para ser redireccionado en los botones respectivos.	X			
	Datos de contacto	X			
PREQUISITOS MINIMOS DE POLITICAS Y CUMPLIMIENTO LEGAL	Menú de Transparencia y Acceso a la Información Pública.	X			
	Política de privacidad y tratamiento de datos personales	X			cambiar formato del documento
	Política de derechos de autor y/o autorización de uso sobre los contenidos		X		no cumple ...esta la politica de tratamiento de datos, pero no esta linkeada
	Misión, visión, funciones y deberes.			X	no hay deberes
	Estructura orgánica - Organigrama	X			
1. INFORMACIÓN DE LA ENTIDAD	Mapas y cartas descriptivas de los procesos.			X	No hay cartas descriptivas
	Directorio Institucional incluyendo sedes, oficinas, sucursales, o regionales.	X			
2. NORMATIVA	Normativa de la Entidad o autoridad	X			
	Políticas, lineamientos y manuales.	X			
	Políticas y lineamientos sectoriales	X			
	Manuales	X			
	Normativa aplicable: decretos, resoluciones, circulares, directivas presidenciales, actos administrativos, autos o fallos judiciales que le apliquen (siempre que sea obligación su publicación) y que no se encuentren compilados, y demás normativa, incluyendo para entes territoriales las ordenanzas y los acuerdos municipales o distritales.	X			
3. CONTRATACIÓN	Plan Anual de Adquisiciones	X			hasta 2024
	Publicación de la información contractual.	X			
	Publicación de la ejecución de los contratos.	X			hasta 2024
	Manual de contratación, adquisición y/o compras.	X			tiene manual de contratacion y Las contrataciones se hacen a traves de ley 80 (manual de contratación) ejemlo hay contrato de papeleria
4. PLANEACIÓN	Planeación, Presupuesto e Informes	X			
	Presupuesto general de ingresos, gastos e inversión	X			HASTA 2024
	Ejecución presupuestal.	X			
	Proyectos de inversión	N/A			Excenta articulo 74 de la ley 1474 de 2011
	Plan de Acción.	X			
	Informes de gestión, evaluación y auditoría.	X			
7. DATOS ABIERTOS	7.1 Instrumentos de gestión de la información	X			
	7.2 Sección de Datos Abiertos.	X			
8. INFORMACIÓN ESPECÍFICA PARA GRUPOS DE INTERÉS	8.1. Información para Grupos Específicos	X			
	8.1.1. Información para niños, niñas y adolescentes.	X			
9. OBLIGACIÓN DE REPORTE DE INFORMACIÓN ESPECÍFICA POR PARTE DE LA ENTIDAD.	Obligación de reporte de información específica por parte de la entidad	X			La politica de seguridad e la indormackon del sitio web y proteccionde datos personales debe estar en pie de pagina linkeada
10. INFORMACIÓN TRIBUTARIA EN ENTIDADES TERITORIALES LOCALES	Información tributaria en Entidades territoriales locales	N/A			

Nivel de cumplimiento NTC 5854:

NIVEL NTC 5854	TOTAL	CUMPLE	NO CUMPLE	PARCIAL	NO APLICA	NO SE PUDO VALIDAR	% DE CUMPLIMIENTO
PORTAL ÚNICO DEL ESTADO COLOMBIANO GOV.CO.	2	2					100%
FOOTER O PIE DE PAGINA	4	4					100%
PREQUISITOS MINIMOS DE POLITICAS Y CUMPLIMIENTO LEGAL	3	2	1				95%
1. INFORMACIÓN DE LA ENTIDAD	4	2		2			94%
2. NORMATIVA	5	5					100%
3. CONTRATACIÓN	4	4					100%
4. PLANEACIÓN	6	6			1		100%
7. DATOS ABIERTOS	2	2					100%
8. INFORMACIÓN ESPECÍFICA PARA GRUPOS DE INTERÉS	2	2					100%
9. OBLIGACIÓN DE REPORTE DE INFORMACIÓN ESPECÍFICA POR PARTE DE LA ENTIDAD.	1	1					100%
10. INFORMACIÓN TRIBUTARIA EN ENTIDADES TERITORIALES LOCALES	1	1			1		100%
TOTAL	**34**	**31**	**1**	**2**	**2**	**0**	**91%**

3. RECOMENDACIONES

Proceso de Apoyo: Gestión Administrativa, tecnológica y de recursos físicos.

- Teniendo en cuenta que el Mapa de procesos de FONDECÚN pronto será actualizado, se recomienda actualizar la caracterización del procedimiento de gestión de tecnología una vez aprobado el nuevo mapa de procesos, en caso que la actividad se tenga prevista para el segundo semestre de la presente vigencia, se recomienda actualizar lo antes posible la caracterización del procedimiento y publicarlo en la página web de la Entidad.
- Se recomienda montar en formatos de la Entidad los documentos publicados en la página web, Registros de Activos de información, Índice de información clasificada y reservada y Esquema de publicación de información, los cuales se encuentran publicados actualmente sin formatos.
- Una vez el Inventario de Activos de Información esté aprobado, se recomienda montarlo en formato de la Entidad y publicarlo en la página web.
- Se recomienda incluir en el plan de acción de la Gestión Tecnología para la vigencia 2025, la definición y actualización de procedimientos de gestión,

gobierno y seguridad de las tecnologías de la información.

- Se recomienda establecer un cronograma donde se programen las pruebas de Backup´s, y se realicen informes de los resultados para tener un control de dicha actividad y dar cumplimiento a lo establecido por el MSPI, actualmente se realizan en fechas al azar.
- En aras de avanzar con el MSPI se recomienda realizar un diagnóstico del modelo en la Entidad para identificar que actividades hacen falta para la implementación total del Modelo -MSPI.
- Se recomienda revisar el código GA-PR-01, el auditado presentó el documento procedimiento de Gestión de Incidentes con dicho código, sin embargo, al ingresar y verificar en la página de la Entidad el cogido pertenece al procedimiento control de documentos en la versión No. 02.
- Se recomienda gestionar lo antes posible el código para el documento "Guía de Contacto con Autoridades y Grupos de Interés"
- Se recomienda actualizar la política de seguridad de la Información, una vez revisada, se evidencia que falta incluir roles y responsables de la Entidad, además, se debe nombrar o delegar el Oficial de Seguridad de la Información en la Entidad, revisar
  En la página del Ministerio TIC el Centro de Operaciones de Seguridad Nacional de Colombia (SOC), el cual se inauguró recientemente para blindar la ciberseguridad de las Entidades del país y la Guía No. 4 de Mintic -Seguridad y privacidad de la información (habla de un Responsable de Seguridad de la Información para la Entidad).
- Se recomienda revisar, actualizar, y crear nuevos formatos a documentos que actualmente se encuentran en archivos planos o en Word sin el respectivo proceso de control de cambios.
- Se recomienda que los documentos de seguimientos a planes o incidentes y demás, en la columna de "avance" o "seguimiento" se reporte junto con la actividad realizada, la fecha en que se reporta el avance, así como un link del soporte de los mismos con el objetivo de llevar la línea de tiempo y llevar un control real de los cumplimientos términos establecidos, a saber, se evidenciaron capacitaciones, sensibilizaciones, seguimientos sin fechas en los documentos de seguimientos.
- Se recomienda control de seguridad para el Data Center más robusto, el cual se encuentra expuesto con baja seguridad, su ubicación carece de cámaras de vigilancia y fortalecer la puerta de ingreso.
- Se recomienda dejar en el Data Center únicamente los equipos que hacen parte del lugar, tales como UPS, equipos de computación, almacenamiento, red y refrigeración, retirar impresora, teclado y demás, toda vez que el lugar no es idóneo para bodega.
- Aun cuando al Data Center tiene acceso un único funcionario, es importante que se tenga una planilla de registro de ingreso y salida donde además se debe reportar día, hora, motivo del ingreso.
- Se recomienda fortalecer el personal de la Gestión Tecnológica, aunque hasta el momento un solo funcionario se ha encargado de todo lo relacionado a las Tecnologías de la Información, se debe definir responsables dentro de área para MIPG, MSPI, PETIC y demás implementaciones que cada una son un universo y requieren de contante seguimiento, por lo cual, una sola persona no es suficiente toda vez que además requiere de un backup para

eventualidades, si la única persona a cargo de los sistemas de información en la Entidad por algún motivo debe faltar, se debe garantiza la continuidad de los servicios, planes, seguimientos establecidos.

- Realizar seguimiento a las actualizaciones del inventario de activos de información de la Entidad de manera periódica.
- Teniendo en cuenta que las políticas se encuentran condensadas en el documento "lineamientos seguridad informática Fodencún", se recomienda socializar semanalmente una política, describiendo de manera dinámica su aplicabilidad a los funcionarios y contratistas a través de correos electrónicos, grupos de whatsapp, escritorio virtual, pagina web de la Entidad y todas las herramientas tecnológicas con que cuenta Fondecún, lo anterior, teniendo en cuenta que en auditoria se logró evidenciar que en inducción y reinducción a los funcionarios y contratistas se les brinda la información, pero debido a que el documento es extenso, no se tienen presentes las políticas aun cuando de manera diaria aplican algunas en el ejercicios de sus funciones.
- Se recomienda verificar y controlar el acceso al Data Center se encuentra vulnerable, la puerta es poco segura, aunque un único funcionario cuenta con llave para su ingreso, no se evidencian cámaras de seguridad en el pasillo para ayudar en la custodia de la seguridad de la información, por lo tanto, el Data Center se encuentra expuesto y por ende toda la información de la Entidad.

Gestión de Bienestar y del Talento Humano

- Se recomienda la socialización de manera recurrente con respecto a las políticas de seguridad de la información implementadas en la Entidad, las cuales son 12 y cada funcionario y/o contratista en el ejercicio de sus actividades requiere la aplicabilidad de varias.
- Aunque se cuenta con los activos de información es importante que todos los funcionarios del área tengan conocimiento de cada uno de ellos.
- Se recomienda realizar seguimiento y a los riesgos de seguridad de la información del área
- Es importante definir un documento general de "acuerdo de confidencialidad y seguridad de la información" para firma de funcionarios y contratistas, aunque se encuentre un literal en los contratos de los funcionarios que haga referencia a la confidencialidad de la información, en el documento se puede dar mas alcance y lineamientos para el compromiso.
- Para el fortalecimiento de la seguridad, control y restricciones en la Entidad se recomienda la instalación de cámaras de seguridad.
- Se recomienda la implementación de una minuta en la recepción para el registro al ingreso y salida de equipos de cómputo de las instalaciones de la Entidad.
- Es importante la instalación de una red contraincendios
- Se recomienda adoptar la política ESCRITORIO LIMPIO Y EQUIPOS DESATENDIDOS la cual se encuentra en el literal 5.13. de los lineamientos de la política de seguridad informática

- Se recomienda digitalizar las hojas de vida de los funcionarios de la Entidad, si bien las mismas se encuentran cargadas en SIGEP II, es importante garantizar el aseguramiento de la totalidad de los documentos que se producen y se reciben de las hojas de vida de cada funcionario, a saber, cada carpeta se convierte en un expediente de la historia laboral donde además de los soportes con que se realiza la contratación, se deben archivar, memorandos, resoluciones, y demás información de cada uno de los funcionarios, esta información no se encontrará en SIGEP II, y la Ley 294 de 2000 establece que las Entidades pueden incorporar tecnologías de avanzada en la administración y conservación de sus archivos.
- Cumplir con la política de escritorio limpio tanto físico como virtual esto con el objetivo de proteger la información confidencial y sensible de los puestos de trabajo.

Proceso Misional Estructuración Gerencia Y Administración De Proyectos

- Se recomienda realizar el inventario de activos de información del área, donde se indique el grado de importancia a cada uno y se realice plan de tratamiento de riesgos, así como tener un control mediante seguimiento periódico y actualización del inventario de activos de manera constante.

- Solicitar a la oficina de planeación y gestión tecnológica, el apoyo para el levantamiento de inventario de activos del área, y reportar cambios y/o actualizaciones al inventario a la gestión tecnológica quien debe realizar seguimiento y mantener un control de los activos de información de toda la Entidad.

Proceso Estratégico Gestión Comercial Y De Comunicaciones

- Se recomienda realizar el inventario de activos de información del área, donde se indique el grado de importancia a cada uno y se realice plan de tratamiento de riesgos, así como tener un control mediante seguimiento periódico y actualización del inventario de activos de manera constante.

- Solicitar a la oficina de planeación y gestión tecnológica, el apoyo para el levantamiento de inventario de activos del área, y reportar cambios y/o actualizaciones al inventario a la gestión tecnológica quien debe realizar seguimiento y mantener un control de los activos de información de toda la Entidad.

Cumplimiento Norma Técnica Ntc Colombiana 5854 Pagina Web Fondecún

- Continuar con la buenas practicas y correcta aplicación de la norma técnica colombiana NTC 5854.

- Permanecer actualizado desde las Entidades que expiden las normas, en este caso El Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC), toda vez que la norma 5854 esta sujeta a cambios permanentemente.

- Se recomienda la actualización del formato del documento Política de privacidad y tratamiento de datos personales y los que en general se encuentren en formatos antiguos.
- Se recomienda, no recibir información para cargar en la página web que se encuentre en formatos desactualizados.
- Elaborar la política de derechos de autor y/o autorización de uso sobre los contenidos, lo anterior hace referencia únicamente a la página web.
- Realizar cartas descriptivas de los procesos, en el mapa de procesos publicado en la página web.

4. HALLAZGOS

A continuación, se enuncian 18 no conformidades que se generan luego del análisis de la información discriminados de la siguiente manera:

GESTIÓN ADMINISTRATIVA, TECNOLÓGICA Y DE RECURSOS FÍSICOS		
No.	**HALLAZGO**	**DESCRIPCIÓN**
Hallazgo 1	No se ha actualizado la caracterización del procedimiento de gestión tecnológica	Teniendo en cuenta que la caracterización del procedimiento de gestión tecnológica permite gestionar el ciclo de vida de las tecnologías de la información y comunicaciones y que el Mapa de Procesos de FONDECÚN tuvo cambios después de la caracterización, el ciclo PHVA contenido el documento GA-CP-02 de diciembre de 2021 se debe actualizar, para identificar las necesidades y desafíos de la Entidad en cuanto a tecnología. El auditado manifestó que actualmente el mapa de procesos tendrá cambios, por lo tanto, se recomienda realizar la actualización una vez esté aprobado el nuevo mapa de procesos.
Hallazgo 2	El Inventario de activos de información No está aprobado, además el documento no se encuentra en formato de la Entidad	De acuerdo al control A.8.1.1. de la norma técnica colombiana ntc-150-iec 27001, se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos. La presente auditoría conoció un documento en Excel denominado inventario de activos de información en agosto de 2024, sin embargo, no está aprobado y tampoco se encuentra en formato de la Entidad.
Hallazgo 3	Bajo avance al Modelo Integrado de Planeación y Gestión MIPG	No se realizaron actividades tendientes a la alineación al Modelo Integrado de Planeación MIPG tales como: -Definir y actualizar procesos y procedimientos de gestión, gobierno y seguridad de TI -Actualizar y aprobar el inventario de activos de seguridad y privacidad de la información - Realizar diagnostico con la herramienta de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI), presentándolo y aprobándolo el diagnóstico en el Comité de Gestión y Desempeño Institucional.

Hallazgo 4	Duplicidad del código de procedimiento GA-PR-01	una vez se ingresa a la página web de la Entidad, se evidencia que el código GA-PR-01 pertenece al procedimiento control de documentos en la versión No. 02, y no al procedimiento Gestión de Incidentes como se socializó teniendo en cuenta el plan de mejoramiento de la auditoría anterior, el presente hallazgo queda compartido entre las áreas Gestión Tecnológica y la Oficina de Planeación.
Hallazgo 5	Falta de códigos en los documentos Guía de Contacto con Autoridades y Grupos de Interés	Como actividad en el plan de mejoramiento se debía realizar y socializar guía contacto con autoridades y grupos de interés, para el escalamiento de incidentes según la estructura de la Entidad. de un documento denominado Guía de Contacto con Autoridades y Grupos de Interés, sin embargo, este carece de código, lo cual indica que no ha sido aprobado por el comité institucional o gestionado ante Planeación para el respectivo código de identificación. Se evidenció la socialización mediante correo electrónico del día 26 de enero de 2024
Hallazgo 6	Política de seguridad de la información incompleta	De acuerdo al Modelo de Privacidad y Seguridad de la Información MPSI y a la norma ISO 27001 en la política de seguridad y privacidad de la información, se deben involucrar todas las dependencias de FONDECUN con roles y como responsables para el respectivo cumplimiento de la política, una vez revisada la política actual le faltan roles como por ejemplo: Rol: Funcionarios y Contratistas / Responsabilidades: proteger los activos bajo su custodia, aplicando los controles de seguridad establecidos, realizar la entrega de activos de información en el momento en que se desvinculen de la Entidad. El control A.6.1.2 establece que hay que separar los deberes en la política. MISP: Articular con las áreas o dependencias de la entidad, los roles y responsabilidades necesarios para la adopción del MSPI
Hallazgo 7	Sin política de Teletrabajo	Una vez revisada la política de seguridad de la información, se evidenció el incumplimiento del control 6.2.2 Teletrabajo, las Entidades públicas deben tener establecida la política de Teletrabajo, en Colombia el teletrabajo está regulado por la Ley 2121 de 2021 y el Decreto 555 de 2022, el presente hallazgo queda compartido entre la dirección general, talento Humano y Gestión Tecnológica
Hallazgo 8	Plan de tratamiento de riesgos de seguridad de la información sin seguimientos	Incumplimiento del literal 7.3.3 del Modelo de Seguridad y Privacidad de la Información: Se evidencia documento denominado Plan de Tratamiento de seguridad 2024, sin embrago, no se le realizó seguimiento. Es necesario que de manera continua se realice seguimiento al Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, para garantizar que se cumplan los objetivos del plan y que se mejore constantemente.
Hallazgo 9	No se cuenta con Oficial de Seguridad de la Información	De acuerdo a las directrices del Ministerio de las Tecnologías MINTIC, el Modelo de Seguridad y Privacidad de la Información, la alta dirección debe nombrar o delegar un Oficial de Seguridad de la Información el cual es el responsable de la seguridad de la información de la Entidad ya sea esta grande o pequeña. Algunas de sus

		funciones son: ○ Desarrollar y gestionar la estrategia de seguridad de la información de la Entidad. ○ Identificar y gestionar los riesgos de seguridad de la información. ○ Desarrollar, implementar y supervisar las políticas de ciberseguridad alineadas con la misión y visión de la Entidad ○ Coordinar el equipo de ciberseguridad de la Entidad. ○ Fomentar la concienciación de todos los empleados en ciberseguridad, entre muchas funciones más.
Hallazgo 10	No se cuenta con hoja de vida de indicador	Una vez culminada las actividades del MSPI, se evalúa la efectividad de las acciones tomadas a través de los indicadores definidos en la fase de implementación que debe incluir la correcta interacción entre el MSPI, MIPG y los requerimientos de la Ley 1581 de 2012 "Protección de datos personales", Ley 1712 de 2014 "Ley de Transparencia y Acceso a la Información Pública", Decreto 2106 de 2019 o cualquier norma que las reglamente, adicione, modifique o derogue. Todos los indicadores de gestión de la seguridad de la información, deben contar con una hoja de vida.
Hallazgo 11	Continuidad de seguridad de la información y a gestión de continuidad del negocio sin publicación en página web	Teniendo en cuenta el control A.17.1 Continuidad de seguridad de la información y a gestión de continuidad del negocio, se evidencia la existencia del documento "Plan de contingencia con código GA-PLA-02", sin embargo, este no se encuentra publicado, por lo tanto, el presente hallazgo es compartido entre las áreas Planeación y Gestión Tecnológica
GESTIÓN DE BIENESTAR Y DEL TALENTO HUMANO		
No.	**HALLAZGO**	**DESCRIPCIÓN**
Hallazgo 1	Falta de conocimiento del documento "Lineamientos de seguridad informática"	Aunque el área es la encargada de coordinar las capacitaciones en la Entidad, al consultar a los auditados sobre las políticas de seguridad informática que aplica en el ejercicio de sus actividades, se evidenció el desconocimiento del documento "Lineamientos de seguridad informática" el cual contiene 12 políticas (se realizó retroalimentación).
Hallazgo 2	Falta de conocimiento y seguimiento a los riesgos de seguridad de la información	En el ejercicio de la auditoria fue necesario indicar a los auditados de la existencia de la matriz con los riesgos de seguridad de la información que cada área identificó, con lo cual se evidenció que no se hace un seguimiento y control documentado de manera periódica
Hallazgo 3	Incumplimiento de la	

	política 5.13. "políticas escritorio limpio y equipos desatendidos"	se verifica el escritorio de un funcionario del área de TTHH, donde se evidencia que tanto el escritorio físico como el virtual se encuentran saturados de elementos, los escritorios deben permanecer limpios con el objetivo de proteger la información confidencial y sensible de los puestos de trabajo
PROCESO MISIONAL ESTRUCTURACIÓN GERENCIA Y ADMINISTRACIÓN DE PROYECTOS		
No.	**HALLAZGO**	**DESCRIPCIÓN**
Hallazgo 1	Incumplimiento numeral 8.1.1 NTC ISO 27001 Inventario de Activos	El proceso estructuración gerencia y administración de proyectos, no cuenta con un inventario de activos, el cual se debe mantener actualizado
PROCESO ESTRATÉGICO GESTIÓN COMERCIAL Y DE COMUNICACIONES		
No.	**HALLAZGO**	**DESCRIPCIÓN**
Hallazgo 1	Incumplimiento numeral 8.1.1 NTC ISO 27001 Inventario de Activos	El proceso estructuración gerencia comercial y de comunicaciones, no cuenta con un inventario de activos, el cual se debe mantener actualizado
NORMA TÉCNICA NTC COLOMBIANA 5854 PROCESO ESTRATÉGICO GESTIÓN COMERCIAL Y DE COMUNICACIONES		
No.	**HALLAZGO**	**DESCRIPCIÓN**
Hallazgo 1	Falta Política de derechos de autor y/o autorización de uso sobre los contenidos	Al verificar con el auditado en la paina web se evidenció la falta de la Política de derechos de autor y/o autorización de uso sobre los contenidos Requisito Mínimo De Políticas Y Cumplimiento Legal

OBSERVACIONES: Es importante fortalecer la gestión de incidentes de seguridad de la información, en cuenta a evaluación, seguimiento y prevención de los mismos, para dar total cumplimiento a la Guía No. 21 para la Gestión y Clasificación de Incidentes de Seguridad de la Información por parte del Ministerio de Tecnologías de la Información y las Comunicaciones.

El personal para la Gestión Tecnológica se debe fortalecer, el funcionario a cargo realiza actividades y funciones que se deben descentralizar de un único funcionario para que la implementación de normas, políticas, demás directrices en cuanto a tecnología pueden no solo implementarse sino también realizarse los respectivos seguimientos y mejoras continuas, la presente auditoria hace un reconocimiento especial al ingeniero a cargo de la gestión tecnológica de la Entidad.

La Auditoría realizada se ejecutó de acuerdo con lo estipulado el Plan de Auditoria elaborado para tal fin, y se cumplió con el objetivo y alcance previsto en el mismo. Se genera Informe con diecisiete (17) hallazgos a los cuales se les deben generar Plan de Mejoramiento, teniendo en cuenta las recomendaciones descritas.

Para constancia se firma en Bogotá D.C., a los 02 días del mes de mayo del año 2025.

Cordialmente,

YENNY DIANITH BARRIOS GÓMEZ
Jefe Oficina de Control Interno

Elaboró:

Natali Padrón Aguilar- Contratista Oficina de Control Interno

APROBACIÓN DEL INFORME DE AUDITORÍA		
Nombre Completo	**Responsabilidad** (cargo)	**Firma**
Natali Padrón Aguilar- Contratista Oficina de Control Interno	**Elaborado Por:** Natali Padrón Aguilar- Contratista Oficina de Control Interno	
YENNY DIANITH BARRIOS GÓMEZ Jefe Oficina de Control Interno	**Aprobado por:** YENNY DIANITH BARRIOS GÓMEZ Jefe Oficina de Control Interno	