1. DESCRIPCIÓN GENERAL	
Objetivo de la Auditoria:	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:	Verificar el estado de implementación del Modelo de Seguridad y Privacidad de la Información MSPI en la vigencia 2022-2023, a los siguientes procesos institucionales: - Proceso Misional: Estructuración, Gerencia y Administración de proyectos - Proceso Estratégico: Gestión Comercial y de Comunicaciones. - Proceso de Apoyo: Gestión de Bienestar y Talento Humano Bajo el Modelo de seguridad y privacidad de la información definido 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.
Procedimiento de la Auditoría	Proceso de Auditoria Interna
Auditor Líder	Yenny Dianith Barrios Gómez
Equipo Auditor:	Yenny Dianith Barrios Carolina Garzón
Fecha de la Auditoria	18/08/2023 al 06/10/2023
Dependencia a cargo del proceso auditado	Subdirección Administrativa y Financiera
Procesos Auditados	Política de Seguridad y Privacidad de la Información FONDECUN

2. ANÁLISIS Y EVALUACIÓN DE DATOS

METODOLOGIA:

El presente informe realiza el avance en la implementación del Modelo de Seguridad y Privacidad de la información de FONDECUN con relación a los cuatro pilares fundamentales la disponibilidad, la integridad, la confidencialidad y la autenticación, desde el punt de vista del líder del proceso y de los usuarios de los diversos activos de información.

El seguimiento se realiza por medio de la evaluación de la herramienta MSPI (diagnóstico de seguridad y privacidad de la información generada por MINTIC), basado en la guía del Modelo de Seguridad y Privacidad de la Información MSPI, mesas de trabajo realizadas con el Líder del Proceso de tecnología el Sr. Nelson Reina.

Así mismo se realiza evaluación de la adherencia de los funcionarios y contratistas a la Política de Seguridad y privacidad de la información, para la auditoria se seleccionan 3 diferentes procesos de la entidad. Siendo los procesos institucionales:

- Proceso Misional: Estructuración, Gerencia y Administración de proyectos
- Proceso Estratégico: Gestión Comercial y de Comunicaciones.
- Proceso de Apoyo: Gestión de Bienestar y Talento Humano Se pretende dar a conocer el nivel de madurez de los siguientes aspectos, dentro del Fondo de desarrollo de proyectos:

Durante la Auditoria, el equipo auditor utiliza 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 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.

NORMATIVIDAD APLICABLE

- Constitución Política de Colombia
- Ley 87 de 1993

- 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
- NTC ISO 27001
- Procesos y procedimientos del Sistema de Gestión de FONDECUN
- 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 Gestión Documental

ANALISIS

En cumplimiento del Programa Anual de Auditoria para la vigencia 2023, se desarrollará auditoria a la POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION MSPI – FONDECUN, de acuerdo al levantamiento de la información, generada en entrevistas con el líder del proceso, se evidencia que los avances se han generado en los 9 procesos de la entidad, sin generar avances específicos en algún proceso.

En el documento herramienta diagnóstico, se estipulan observaciones que se deben tener en cuenta para el mejoramiento de la calificación, se deja claridad que Lista de información para aquellas entidades que hayan avanzado en la fase de EVALUACIÓN DE DESEMPEÑO y Lista de información para aquellas entidades que hayan avanzado en la fase de MEJORA CONTINUA, no aplican para evaluación en FONDECUN puesto que se encuentra en etapa de implementación

Porcentaje de cumplimiento del MSPI en los procesos de la entidad	# total de procesos	# de procesos definidos en el alcance	Total, avance por procesos
Con base al alcance definido en la política de seguridad y el total de procesos de la entidad, indicar los siguientes datos	9	9	100%

SEGUIMIENTO A LA HERRAMIENTA DIAGNOSTICO DEL MSPI

Dentro de los resultados presentados por la herramienta de Diagnostico del Modelo de Privacidad de Seguridad de la Información – MPSI, se presentan las observaciones resultado del seguimiento a la implementación del MSPI, basado en diagnóstico de la vigencia 2023, con procedimientos de mejora. Se diligencian y entregan para conocimiento la Matriz de levantamiento de la información, matriz administrativa, matriz técnica, se da a conocer que la matriz PHVA no se diligencia teniendo en cuenta que esta, mide un ciclo de implementación y a la fecha del seguimiento el modelo se encuentra en implementación.

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO A

Para dar cumplimiento al objetivo propuesto, se toma como referencia el Documento Política de Seguridad y Privacidad de la Información MSPI, sus guías de orientación y la norma ISO 27001:2013. La Oficina de Control Interno reviso y analizó la información suministrada por el líder de la Oficina de Tecnologías de la Información, la dispuesta en el sitio Web de la entidad, y la recopilada a través de 5 mesas de trabajo de seguimiento y revisión documental, de acuerdo a la herramienta puesta a disposición por MINTIC. Los resultados obtenidos se reflejan en la siguiente matriz:

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	60	100	**EFECTIVO**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	65	100	**GESTIONADO**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	39	100	**REPETIBLE**
A.8	GESTIÓN DE ACTIVOS	19	100	**INICIAL**
A.9	CONTROL DE ACCESO	75	100	**GESTIONADO**
A.10	CRIPTOGRAFÍA	0	100	**INEXISTENTE**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	66	100	**GESTIONADO**
A.12	SEGURIDAD DE LAS OPERACIONES	60	100	**EFECTIVO**
A.13	SEGURIDAD DE LAS COMUNICACIONES	59	100	**EFECTIVO**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	60	100	**EFECTIVO**
A.15	RELACIONES CON LOS PROVEEDORES	20	100	**INICIAL**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	14	100	**INICIAL**

A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	24	100	**REPETIBLE**
A.18	CUMPLIMIENTO	54	100	**EFECTIVO**
PROMEDIO EVALUACIÓN DE CONTROLES		**44**	**100**	**EFECTIVO**

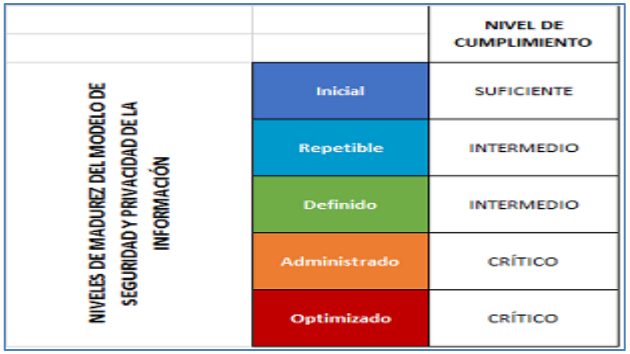
En este ítem se evidencia un puntaje de 44/100 para el año 2023, correspondiente a 14 componentes de la Norma Técnica 27001 a evaluar.

En comparación con a la evaluación realizada en 2022, se evidencia un avance de 18%, pasando de 26/100 a 44/100, pasando de una evaluación de control "REPETIBLE" a un nivel "EFECTIVO", teniendo de los 14 ítems evaluados, 5 en etapa efectivos, 3 gestionados, 3 en inicial, 2 repetibles y 1 Inexistente. En los ítems más avanzados están el control de Acceso, la seguridad física y del entorno, la Política de Seguridad de la Información y la organización de la Seguridad de la información.

A pesar que se han tenido avances en algunos ítems, se continúa en nivel bajo en el ítem Criptografía con 0% de avance, relación con los proveedores con 20% y Gestión de Incidentes de seguridad de la Información con 14%. Ítems que deben ser tenidos en cuenta para elaborar plan de acción que genere avances para la siguiente vigencia

NIVEL DE MADUREZ MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Con relación a los resultados obtenidos de 44/100 de la herramienta diligenciada, se aprecia que en la vigencia evaluada el Nivel de madurez del Modelo en la entidad, paso de un nivel de madurez CRITICO a un estado INTERMEDIO lo que de acuerdo a los niveles dados en el instrumento de identificación posesiona a la entidad en un NIVEL REPETIBLE que se define como "entidad en la cual existen procesos básicos de gestión de seguridad y privacidad de la información, existen controles que permite detectar algunos incidentes de seguridad, pero estos no se encuentran gestionados dentro del componente planificación del MSPI".



NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		NIVEL DE CUMPLIMIENTO
	Inicial	SUFICIENTE
	Repetible	INTERMEDIO
	Definido	INTERMEDIO
	Administrado	CRÍTICO
	Optimizado	CRÍTICO

TOTAL DE REQUISITOS CON CALIFICACIONES DE CUMPLIMIENTO	
CRÍTICO	0% a 35%
INTERMEDIO	36% a 70%
SUFICIENTE	71% a 100%

AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA)

Referente al avance en el ciclo PHVA, y en comparación con la vigencia anterior se evidencia avance de 12%, pasando en 2022 de 8% a un 21% en 2023. En comparación con la vigencia anterior se videncia que aumento el Componente de Panificación e Implementación, así mismo se evidencia gestión en el componente de Evaluación de Desempeño. No se evidencia avance en la Mejora Continua.

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2015	Planificación	13%	40%
2016	Implementación	2%	20%
2017	Evaluación de desempeño	5%	20%
2018	Mejora continua	0%	20%
TOTAL		21%	100%

Para dar cumplimiento a la planificación del MSPI se debe continuar robusteciendo los lineamientos dados para el normal funcionamiento del modelo, dando cumplimiento con lo mínimo exigido en la documentación que se encuentre aprobada. Así mismo fortalecer los procesos de capacitación, socialización y adherencia de los conocimientos por parte de los colaboradores de la entidad. Así mismos generar revisión de las actualizaciones en cada vigencia, garantizando la mejora continua y la revisión de los cambios normativos que afecten el modelo.

Para la próxima vigencia se debe evaluar la mejora continua, por medio del seguimiento de indicadores, evaluación de riesgos de Seguridad de información y seguimiento de planes de mejoramiento producto de la auditoria realizada.

CALIFICACIÓN FRENTE A MEJORES PRÁCTICAS EN CIBERSEGURIDAD (NIST)

Aunque se evidencian actividades de tecnologías de protección, efectivas, aun no se evidencia su impacto y consistencia, por lo cual la herramienta, no genera avance alguno en los ítems evaluados referente a la Ciberseguridad institucional, como lo refleja el siguiente cuadro.

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
Etiquetas de fila	CALIFICACIÓN ENTIDAD	NIVEL IDEAL CSF
IDENTIFICAR	0	100
DETECTAR	0	100
RESPONDER	0	100
RECUPERAR	0	100
PROTEGER	0	100

ENTREVISTA A PROCESOS

El proceso de auditoria, realiza entrevistas a 3 procesos seleccionados, relacionados con el fin de evaluar la adherencia y conocimiento de los funcionarios con relación a lineamiento y elementos de la Política de Privacidad de la Información de la entidad, así como el nivel de implementación de la misma. El equipo auditor por medio de entrevistas a los líderes de los procesos seleccionados, determina:

EVALUACION DE LINEAMIENTO	PROCESO ESTRATÉGICO: GESTIÓN COMERCIAL Y DE COMUNICACIONES	PROCESO MISIONAL: ESTRUCTURACIÓN, GERENCIA Y ADMINISTRACIÓN DE PROYECTOS	PROCESO DE APOYO: GESTIÓN DE TALENTO HUMANO

Conoce las políticas, procesos, procedimientos y formatos de MSPI. Recibe capacitación constante digital y presencial.	SI CUMPLE	SI CUMPLE	SI CUMPLE
Conoce los activos de información, su importancia dentro del proceso y su responsabilidad en el manejo.	SI CUMPLE	SI CUMPLE	SI CUMPLE
Conoce el Plan de Capacitación, Sensibilización y Comunicación de Seguridad de la Información	SI CUMPLE	SI CUMPLE	SI CUMPLE Se debe generar seguimiento a la adherencia de los conocimientos.
Conoce los responsables de los activos de información, así como los controles de seguridad que se debe manejar en cada activo, tanto virtual como físico.	SI CUMPLE	SI CUMPLE	SI CUMPLE
¿Se tienen identificados, documentadas e implementadas reglas para el uso aceptable de información y de activos	Organizados en drive según la estrategia de comunicación definida por carpetas. Se debe generar proceso de Manejo y Gestión Documento virtual.	SI CUMPLE	En el área de TTHH no se cuenta con procedimiento documentado y/o codificado del Ingreso, permanencia y retiro de personal.
Cuenta con plan de tratamiento de riesgos de seguridad de información. Se da cumplimiento a las actividades propuestas para evitar el riesgo	Informan no conocer el plan de tratamiento de riesgos de seguridad de información.	Informan no conocer el plan de tratamiento de riesgos de seguridad de información.	No se cuenta con información de manejo de Riesgos de tecnología en el proceso de TTHH
Se da cumplimiento a la política de escritorio limpio y pantalla limpia	El auditado no tienen puesto de trabajo definido en oficina.	Se evidencia desorganización de los archivos ubicados en el escritorio del computador de la auditada al igual que la poca organización en el escritorio físico	Conocen la política, explican que por falta de espacio en la entidad, no se puede dar cumplimiento al escritorio limpio, sin embargo, los documentos relevantes se encuentran en espacios de acceso restringido

Sabe que es Incidente de Seguridad de Información. Ha evidenciado alguno.	Si conocen los incidentes, sin embargo, Ellos no manejan computador dado por el fondo, el computador es propio, por lo cual no se reportan los incidentes.	Si conocen incidentes, se remiten al correo de sistemas.	Aunque se les informa el proceso en inducción el tema de incidentes, la actividad no la saben realizar, no existe formato o proceso.
Llevan a cabo las solicitudes para el uso de medios removibles	SI CUMPLE	SI CUMPLE	SI CUMPLE
Seguridad, permisos, responsabilidad del manejo de sistemas de información o aplicativos	SI CUMPLE	SI CUMPLE	SI CUMPLE
Seguridad, permisos, responsabilidad del manejo de correos electrónicos.	SI CUMPLE	SI CUMPLE	SI CUMPLE
Seguridad, permisos, responsabilidad del manejo de equipos de cómputo fuera de la entidad.	SI CUMPLE	SI CUMPLE	SI CUMPLE
Conocimientos de protección de información generada de la pérdida, destrucción, falsificación o alteración.	Activos de información en Backus en drive y servidor. Se debe revisar los Requisitos para la disponibilidad de los documentos electrónicos de archivo de archivo, de acuerdo a TRD.	No hay especio físico suficiente para disposición del archivo físico, por lo cual la protección documental es baja. Se debe revisar los Requisitos para la disponibilidad de los documentos electrónicos de archivo, de acuerdo a TRD. (drive)	SI CUMPLE (Deficiencia con los espacios para archivo).
Conoce el Plan de Continuidad de Negocio (BCP).	Informan no conocer el plan. Sin embargo, se cuenta con información en drive que	Informan no conocer el plan	Informan no conocer el plan, se realiza back up de la documentación cada 2 días y al finalizar la semana.

	resguarda la información		

De acuerdo a las entrevistas realizadas, se destaca el trabajo realizado el área de Tecnologías de la Información y las Comunicaciones, en el avance de la Implementación del Modelo de Seguridad y Privacidad MSPI, Si bien existen aspectos por mejorar, debemos resaltar los avances obtenidos a la fecha y el estado actual de la información allí contenida, mas aun teniendo en cuenta que el líder del proceso se encuentra como responsable de todo el modelo, del servicio de tecnología y de los servicios de apoyo y acompañamiento a los usuario.

Se evidencia que el área de talento humano, cuenta con lineamientos y reglas específicos para el control de acceso de personal no autorizado a la entidad y para el control de documentos especificaos del área (hojas de vida de funcionarios públicos).

Las áreas entrevistadas, conocen la documentación existente referente al MSPI, sin embargo, de acuerdo a diagnóstico elaborado, se encuentran en proceso de elaboración y codificación varios documentos que se deben socializar al interior de la entidad.

GESTION DOCUMENTAL

La revisión y análisis de este procedimiento, está dado bajo los lineamientos del Programa de Gestión documental de la Entidad, aprobado mediante resolución 028 del 14 de agosto del 2020, el cual está elaborado en cumplimiento de la Política Institucional de Gestión Documental en cumplimiento del Modelo integrado de Planeación y Gestión MIPG.

Una vez realizado el análisis de los activos de información, referente a la Gestión Documental, se evidencia debilidades con relación al espacio con el que se cuenta para la disponibilidad de los archivos documentales de gestión, siendo difícil el cumplimiento de la política de Escritorio Limpio, y el control de acceso restringido a información confidencial y/o reservada en la entidad.

El proceso de Talento humano tiene claridad con relación a la importancia y responsabilidad con la que se debe manejar los activos de información propios (hojas de vida).

Los procesos de Gestión Comercial y de Comunicaciones y el proceso Estructuración, Gerencia y Administración de Proyectos, manejan Activos de información en drives personales, institucionales y con back up en el servidor, sin embargo no se cuenta con lineamientos o reglamentos para la disponibilidad de los documentos electrónicos de archivo de acuerdo a TRD.

3. RECOMENDACIONES

El equipo auditor después de realizar la presente auditoria se permite realizara las siguientes recomendaciones, al proceso auditado de forma que se generen y propongan actividades de mejoramiento preventivas, en procura de evitar la materialización del riesgo y un posible incumplimiento de la normatividad.

- Se recomienda que el programa anual de auditorías de la Oficina de Control Interno tenga en cuenta la programación de al menos una auditoria al año, a los procesos misionales de la entidad, correspondiente a la implementación y maduración del Modelo de Privacidad y Seguridad de la Información.
- Es necesario elaborar documentos que, de cuentas de la Gestión y Clasificación de Incidentes de Seguridad de la Información, donde se describan las actividades para el tratamiento, reporte, manejo e investigación de los incidentes de seguridad
- Es necesario contar con el Oficial de Seguridad de la Información (Líder de Sistemas de Información y responsable de MSPI) de acuerdo a la normatividad
- Es necesario que el elemento de seguridad de la información (Oficial de Seguridad de la Información) opere de manera independiente a la Oficina de Tecnologías de la Información, por lo tanto, se recomienda que este perfil se pueda ubicar en un área como planeación, procesos o el área relacionada con gestión de riesgos.
- Se debe elaborar e implementar el procedimiento para la gestión y respuesta a los incidentes de seguridad en la información, de tal manera que se generen acciones preventivas a los mismos.
- Por parte del líder de Gestión Documental, se debe generar lineamientos o reglamentos para la disponibilidad de los documentos electrónicos de archivo de acuerdo a TRD, con el fin de garantizar la disponibilidad, confidencialidad e integridad de la información.

4. HALLAZGOS

Dentro de las NO conformidades que se generan luego del análisis de a información, se enuncian:

No.	HALLAZGO	DESCRIPCION
Hallazgo No. 1	No se cuenta con un Plan de Continuidad de Negocio	No se cuenta con un Plan de Continuidad de Negocio (BCP), debidamente formalizado y probado que garantice la continuidad de operación de FONDECUN en un evento catastrófico o atípico, por lo cual se incumplen lineamientos de Gobierno Digital MSPI, así como los estándares, marcos de referencia internacionales como ISO 22301, ISO 27000:2013 **Respuesta:** Se envió el plan de continuidad de negocio para ser aprobado por el comité de gestión el día 23 de agosto de 2023, al correo anieto@fondecun.gov.co, se anexa copia del correo. **Respuesta Equipo Auditor:** El hallazgo continua, se debe presentar el Plan de Continuidad de Negocio debidamente formalizado, publicado y socializado en la entidad. Se aconseja para la generación de la acción de mejora integrar a líder de Planeación.
Hallazgo No. 2	Bajo avance en el ciclo de funcionamiento e implementación del MSPI	Bajo nivel de implementación del MSPI, Incumplimiento del cronograma establecido para la Implementación del Modelo de Seguridad y Privacidad de la Información establecido por MINTIC, al revisar el avance de ejecución de las actividades contempladas en el sistema de acuerdo a herramienta de diagnóstico, para la implementación del MSPI se encontró que esté va en un 21% de un 100% que se programa realizar para el cumplimiento del modelo. **Respuesta Líder Proceso:** Desde el área de gestión Tecnológica se acepta el hallazgo y se continuaran las acciones para adelantar la implementación.
Hallazgo No. 3	No se realiza Gestión de Incidentes de Seguridad de la Información.	Se evidencian debilidades en la gestión de incidentes de seguridad de la información, no se realiza evaluación, seguimiento, ni prevención de los mismos, se incumple 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. **Respuesta:** De acuerdo con la guía Nro 21 para la gestión de incidentes de seguridad, se realiza actividades prevenir la ocurrencia de incidentes de seguridad de la información tales como Configuración y Administración de Dispositivos de Seguridad Informática, actualización de Parches de Seguridad, aseguramiento de plataformas con software

		antivirus, seguimiento al antivirus, se revisa configuraciones de usuarios, contraseñas y archivos compartidos, concientización a los usuarios en seguridad y se les indica que hacer en caso de una posible amenaza, se tiene el procedimiento para la gestión de incidentes de seguridad aprobado comité de gestión en la vigencia 2022, con el cual se busca gestionar los eventos de seguridad de la información para detectar y tratar con eficiencia, para ser evaluados y dar respuesta de la manera más eficiente y adecuada. **Respuesta Equipo Auditor:** El hallazgo continua, aunque se han adelantado acciones para la prevención de la ocurrencia de incidentes de seguridad en la entidad a nivel del área de Tecnología, aun no se cuenta con soportes de actividades para la detección, evaluación y análisis de los incidentes de seguridad, como lo indica el Capítulo 5.5. de 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.
Hallazgo No 04:	No se cuenta con matriz de riesgos de seguridad y ciberseguridad.	Los Procesos auditados, no cuenta de manera particular con la matriz de riesgos de seguridad y ciberseguridad de la información, tampoco conocen el Plan de tratamientos de Riesgos de FONDECUN, por lo cual la entidad es susceptible de perdida de confidencialidad, perdida de integridad y perdida de disponibilidad de los activos de información, incumpliendo las buenas prácticas y los lineamientos de los estándares ISO 27001, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas – Riesgos de gestión, corrupción y seguridad digital, establecidos en el Modelo Integrado de Planeación y Gestión **Respuesta:** Se envió la matriz de riesgo de seguridad para ser aprobada por el comité de gestión el día 23 de agosto de 2023, al correo anieto@fondecun.gov.co, se anexa copia del correo. **Respuesta Equipo Auditor:** El hallazgo continua, se debe presentar el Mapa de riesgos de seguridad y ciberseguridad, debidamente formalizado, publicado y socializado en la entidad. Se aconseja para la generación de la acción de mejora integrar a líder de Planeación

La Auditoría a la Política de Seguridad de la Información / SGSI, Política de Seguridad y Privacidad de la Información FONDECUN, se extendió en tiempos con relación a lo proyectado y previsto en el Plan de Auditoria, se da cumplimiento con el objetivo y alcance previsto, dando como resultado 8 Recomendaciones y 6 Hallazgos.

Para constancia se firma en Bogotá D.C., a los 27 días del mes de octubre del año 2023

Cordialmente,

YENNY DIANITH BARRIOS GÓMEZ
Jefe Oficina de Control Interno

Elaboró:
CAROLINA GARZON – CONTRATISTA OFICINA DE CONTROL INTERNO