INFORME AUDITORÍA INTERNA AL SISTEAM DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Informe año: 2023	**Ciclo**		
Fecha de elaboración:	**DD**	**MM**	**AAAA**
	07	**08**	**2023**

INFORMACIÓN RELACIONADA CON LA AUDITORIA INTERNA REALIZADA EN LA VIGENCIA ANTERIOR						
PROCESO(S) AUDITADO(S) VIGENCIA ANTERIOR:	**RELACIONE LOS PROCESOS:**		**Informe No.**			
			Fecha Realización Auditoría:	**DD**	**MM**	**AAAA**
				09	**08**	**2022**
ESTRATÉGICOS:						
MISIONALES:						
APOYO:	Unidad de Informática y el Grupo de Proyectos Especiales en Tecnología de la Dirección Ejecutiva de Administración Judicial – DEAJ.					
EVALUACIÓN Y MEJORA:						
Nombre del Auditor Interno:			Se elaboró y ejecutó el Plan de Mejoramiento de la Auditoria Interna desarrollado por Auditado.	**SI**	**NO**	
Nombre del Auditado:				**X**		
Se socializó el Informe final de la Auditoria Interna realizada en la sesión de cierre de la auditoria.	**SI**	**NO**	Se elaboró y ejecutó el Plan de Mejoramiento de la auditoria externa- Auditoria del ICONTEC	**SI**	**NO**	
	X			**X**		
Se formalizó (firmó) el informe de la auditoria interna realizado.	**SI**	**NO**	Se cerraron todos los hallazgos de las auditorias anteriores, en la auditoría realizada en la vigencia anterior.	**SI**	**NO**	
	X			**X**		
Quedó copia del informe final de auditoria interna realizado en la Dependencia.	**SI**	**NO**	Se realizó seguimiento y acompañamiento para el cierre de los hallazgos por parte de los Líderes de Proceso.	**SI**	**NO**	
	X			**X**		
OBSERVACIONES:						

INFORMACIÓN RELACIONADA CON LA AUDITORIA INTERNA REALIZADA EN LA VIGENCIA ACTUAL					
PROCESO(S) A AUDITADAR EN LA PRESENTE VIGENCIA:	**RELACIONE LOS PROCESOS:**	**Informe No.**			
ESTRATÉGICOS:		**Fecha Realización Auditoría:**	**DD**	**MM**	**AAAA**
MISIONALES:					
APOYO:	Unidad de Informática y Grupo de Proyectos Especiales de Tecnología de la Dirección Ejecutiva de la Administración Judicial - DEAJ.		**02**	**08**	**2023**
EVALUACIÓN Y MEJORA:					

1. INFORMACIÓN GENERAL

Auditoría No.		**Fecha de inicio**	**DD**	**MM**	**AAAA**	**Fecha de cierre**	**DD**	**MM**	**AAAA**
			02	**08**	**2023**		**04**	**08**	**2023**

AUDITOR LIDER			**EQUIPO AUDITOR**		
NOMBRES Y APELLIDOS	**DATOS DE CONTACTO**		**NOMBRES Y APELLIDOS**	**DATOS DE CONTACTO**	
	CELULAR	**E-MAIL**		**CELULAR**	**E-MAIL**
Claudia Paola Andrade Murillo	305 733 45 71	claudiapaolaandrade@hotmail.com	N.A.	N.A.	N.A.

2. OBJETIVO, ALCANCE Y COBERTURA DE LA AUDITORÍA:

OBJETIVO:

Determinar la conformidad del Sistema de gestión de seguridad de la información, a partir de la validación de los requisitos de la norma ISO 27001:2013 y las directrices establecidas por la Entidad, con el fin de velar por el mantenimiento del SIGCMA.

ALCANCE:

El SGSI aplica a la Unidad de Informática y Grupo de Proyectos Especiales de Tecnología de la Dirección Ejecutiva de la Administración Judicial.

COBERTURA DEL PROGRAMA (Especifique las Sedes a Auditar):

Unidad de Informática y el Grupo de Proyectos Especiales en Tecnología de la Dirección Ejecutiva de Administración Judicial – DEAJ.

Proveedores

- ERNST & YOUNG SAS
- THE BEST EXPERIENCE IN TECHNOLOGY S.A.

CRITERIOS DE LA AUDITORIA:

ISO 27001:2013, ISO 19011, Requisitos legales aplicables al SGSI, Lineamientos definidos por la organización, documentos internos (Manuales, Procedimientos e Informes de auditorías internas y externas)

3. RESULTADOS DE LA AUDITORÍA INTERNA AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

CONTRATO 028-2023 CONSORCIO EY I2SS CSJ
Participantes: Daniel Ortiz, Diana Aguirre, Jonathan Vargas, Yanci Castellanos, Johana Chipatecua, William Espinosa, Carlos Galindo, Laura Almeida, Mariela Londoño, Francisco Méndez, William Espinosa.

Se realiza auditoria al proveedor, bajo el objeto contractual: *Consolidar la estrategia de seguridad de la información, continuidad del negocio y ciberseguridad que cubra todos los procesos de la cadena de valor de la Rama Judicial a nivel nacional* (a la fecha 4 meses de ejecución).

De acuerdo con las cláusulas del contrato se validan las siguientes:

Obligaciones Oficina de Seguridad de la Información:

- El proveedor debe garantizar a través de una herramienta tecnológica (No Excel) el monitoreo de los controles del Anexo A, de la Norma 27001:2013

  El monitoreo se realiza a través de la herramienta Power Apps (creada por el proveedor) la cual esta alineada a los controles de la ISO 27001, en las seccionales se está realizando un diagnóstico sobre la aplicación de los controles de la norma, como también se va a realizar la identificación de riesgos, el Análisis de Impacto al Negocio- BIA, identificación de activos de información e inventario de bases de datos que contienen datos personales

- El proveedor deberá realizar auditoría a proveedores en el marco del cumplimiento de la norma 27001:2013.

  Se evidencia el formato de evaluación proveedores contiene 68 preguntas de la norma ISO 27001 y las siguientes secciones: políticas de seguridad, organización de la SI, seguridad de recursos humanos, gestión de activos, acceso lógico, cifrado de información, seguridad física y ambiental, seguridad en las operaciones, seguridad en las comunicaciones, adquisición de desarrollo, relación proveedores, gestión de incidentes y cumplimiento. Se evidencio correo del 27 de julio de 2023 donde le envían a 10 proveedores este formato para su diligenciamiento con el fin de tomar las acciones respectivas frente a los proveedores que no tienen implementado los controles.

- Liderar la definición del Plan de Continuidad del Negocio (BCP) y Recuperación antes desastres (DRP), su implementación y pruebas periódicas al interior del CSJ y a nivel seccional

  Se evidencia metodología del análisis de impacto en los servicios, asi mismo, en la Herramienta Power Apps están definidas las preguntas para realizar el BIA la cual se aplicará en la segunda semana del mes de agosto del 2023 al Complejo Judicial de Paloquemao, el BIA se aplicará a procesos misionales y de apoyo.

- Proponer estrategias para la sensibilización y concientización de la importancia de la Seguridad de la Información, Ciberseguridad y Protección de Datos Personales a toda la entidad.

  Se toma muestreo de las sensibilizaciones realizadas:

  - ✓ Taller de capacitación en el SGSI y datos personales al complejo de Paloquemao
  - ✓ Sensibilización sobre la importancia de la SI, ciberseguridad y protección de datos personales en la administración de justicia.
  - ✓ Jornada de capacitación en ISO 27001:2013 ciberseguridad en la ciudad de Popayán evidencia en la página web de la entidad en el micrositio del SIGMA. junio 30
  - ✓ Jornada de sensibilización del sistema integrado de gestión sistema penal acusatorio de Bogotá, comité nacional del SIGMA. Mayo 23 al 25
  - ✓ TIPS seguridad "seguridad Segura" correo del 17 de mayo 2023
  - ✓ TIPS Autogestionar contraseñas correo del 29 de mayo de 2023
  - ✓ Tips Spear Phishing correo del 6 de junio de 2023

Equipo Central De Monitoreo y Reacción:

- ECMR-02/Informe e Instrumento: Después de validar un incidente y la actividad realizada por el atacante o comportamiento malicioso. Proporcionar análisis por escrito ("guion gráfico de ataque"), criticidad, detalles sin procesar, recomendaciones de remediación y mitigación, y acciones de contención sugeridas al final de cada investigación de

incidente que sea validada.

Se evidencia informe del incidente presentado el 17 de mayo de 2023 intrusión en el portal de Azure de la Rama Judicial - intrusión de origen desconocido, el incidente se maneja bajo la metodología NIST y fase de ataque Killchain.

- ECMR-03/ Informe: Deben proporcionar métricas y hallazgos relacionados con las actividades de análisis forense de Endpoints realizadas por el ECMR, identificar malware persistente

  Se evidencia informe de Ciberseguridad de junio 2023, Informe forense junio 2023 del incidente presentado el 17 de mayo de 2023 intrusión en el portal de Azure de la Rama Judicial - intrusión de origen desconocido.

- ECMR-07: Realizar los procesos de hacking ético a los diferentes sistemas de información de la Rama Judicial, a través de metodologías y las buenas prácticas para este fin.

  El proceso lo manejan bajo las metodologías OWASP, impacto SVSS, OSSTMM Informe hacking ético del 18 de julio de 2023 (5 servidores, instancia de bases de datos, dirección pública y privada, dirección URL, se idéntica vulnerabilidades, nivel del riesgo, resumen de explotación de las vulnerabilidades, recomendaciones y conclusiones).

- El proveedor deberá realizar los mantenimientos preventivos y correctivos adecuados para asegurar la continua disponibilidad e integridad de la infraestructura de los servicios en coordinación con los grupos internos

  - ✓ Reporte del 26 de abril de 2023 trabajo realizado para mejorar las capacidades de detección, protección y respuesta de la rama judicial (análisis de los casos de uso, análisis de falsos positivos, implementación multi factor rapid 7, reducir el riesgo de intrusión.
  - ✓ En la reunión de empalme con el proveedor anterior se identifican lo riesgo de transición de arquitectura tecnología, procedimientos,
  - ✓ Mejorar las capacidades de detección, protección y respuesta de la rama judicial, se presenta la transición del servicio los riesgo del servicio, el modelo de relación y el doble factor de autenticación, depuración de usuarios.

- TC-02: Gestión del Cambio: Se evidencia la versión 1 del documento *"*Estrategia y Plan de Cambio y Sensibilización del Sistema de Gestión de Seguridad de la Información y de Ciberseguridad*"*, asi mismo se evidencio piezas de video de activos de información, protección de datos personales y del SGSI para darlos a conocer en el despliegue de la estrategia.

- **Equipo de Trabajo**: De acuerdo con el perfil que describe el contrato, se validó la formación académica del Consultor Senior en Arquitectura TI y Riesgos Informáticos y del Consultor Estratégico en Seguridad de la información, Ciberseguridad y Seguridad Informática, se evidenciaron diplomas de pregrado y postgrado.

CONTRATO 329 THE BEST EXPERIENCE IN TECHNOLOGY S.A
Se realiza auditoria al proveedor, bajo el objeto contractual: "*Adquirir la suscripción del licenciamiento de uso y soporte técnico para el gestor documental Bestdoc como herramienta de transición para garantizar la continuidad del servicio de gestión documental de los expedientes judiciales y la atención prioritaria de incidentes, así como la generación de soluciones que respondan a las a las necesidades de la Rama Judicial".*

Participantes: Manuel Rincón, Deisy Osorio, David Bermudez

De acuerdo con las cláusulas del contrato se validan las siguientes:

1. Entregar el certificado de la Suscripción del Licenciamiento de uso del Gestor Documental Bestdoc sin límite de usuarios por diez meses

   - Se evidencia correo del 18 de enero de 2023 enviado al supervisor del contrato el Sr. Juan Sebastián Idárraga Profesional del Grupo de Proyectos Especiales de Tecnología, donde se adjunta el acuerdo de licenciamiento y el certificado de uso de la herramienta (hasta el 31 de octubre de 2023); la información que se maneja a través de la herramienta queda almacenada en las bases de datos de la entidad.

2. Prestar el Soporte técnico especializado para la atención de incidentes de nivel 2 y 3:
   Nivel 2 incidencias de la herramienta – respuesta inmediata
   Nivel 3 mantenimientos especializados
   Procedimiento atencion de incidentes (del proveedor)
   - Se observa análisis de vulnerabilidades de la herramienta Bestdoc
   - Se toma muestra de la atencion de los casos del 1 de junio de 2023 y del 31 de julio de 2023, donde se dio respuesta dentro del rango de tiempo.
   - Informe de consolidado de casos de enero a julio, correo enviado el 27 de julio al supervisor del contrato

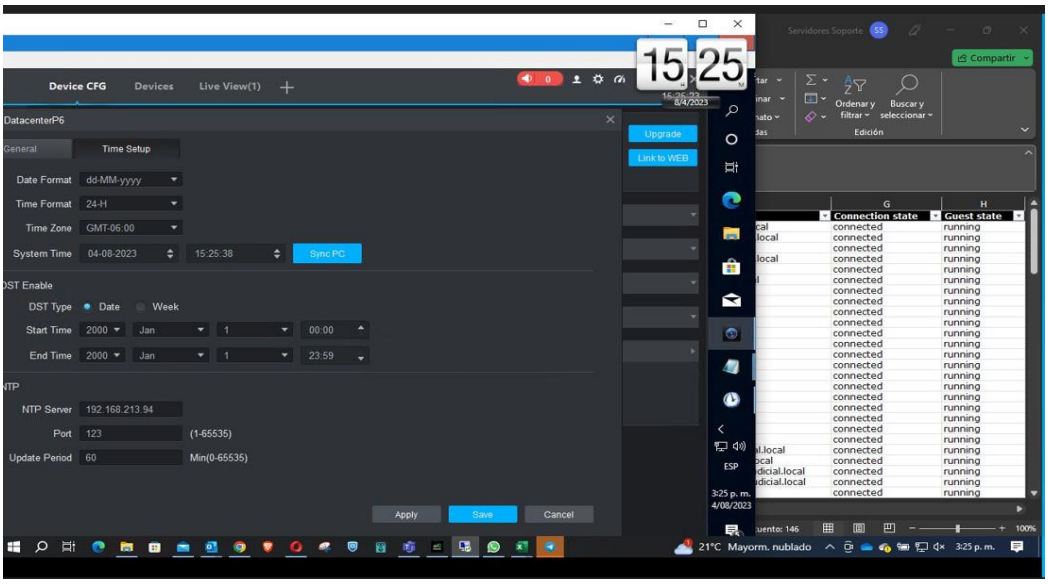
3. Prestar el servicio de funcionalidades adicionales para el gestor documental Bestdoc, correspondiente a 5.000 horas de desarrollo para la implementación de las funcionalidades que se encuentran acotadas en el Anexo Técnico. (ver que han desarrollado)
   - Se crearon 2 nuevas funcionales a la herramienta Bestdoc “TRD Maestras” y “Cierre de Carpetas del Expediente”, la cuales estaban listas desde el 31 de enero de 2023, sin embargo, de acuerdo con correos evidenciados la entidad envió el 19 de julio la homologación de las TRD y el 27 de julio los correos electrónicos que deben estar asociados a las áreas, lo que ha atrasado la puesta en producción de estas funcionalidades.

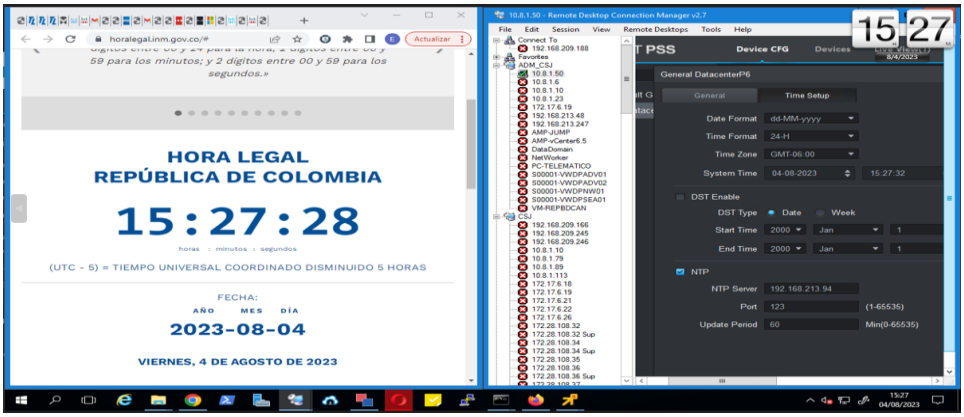
4. Contar con los siguientes medios a disposición de la Entidad de manera permanente: Dirección, números telefónicos locales, números de celular, correo electrónico y nombre de los contactos a través del cual se recibirá cualquier requerimiento de la Entidad"

   - Se evidencia en la propuesta comercial en el ítem 11.2.2. el canal para recibir las solicitudes de soporte es a través del correo electrónico soportebestdoc@bextsa.com

A.12.4.4. Sincronización de relojes

- Se realizó visita a los data center que se encuentran ubicados en la sede del CAN, donde se validó la sincronización de los relojes de acuerdo con la hora oficial del Instituto Nacional de Metrología de Colombia, a continuación, las evidencias:

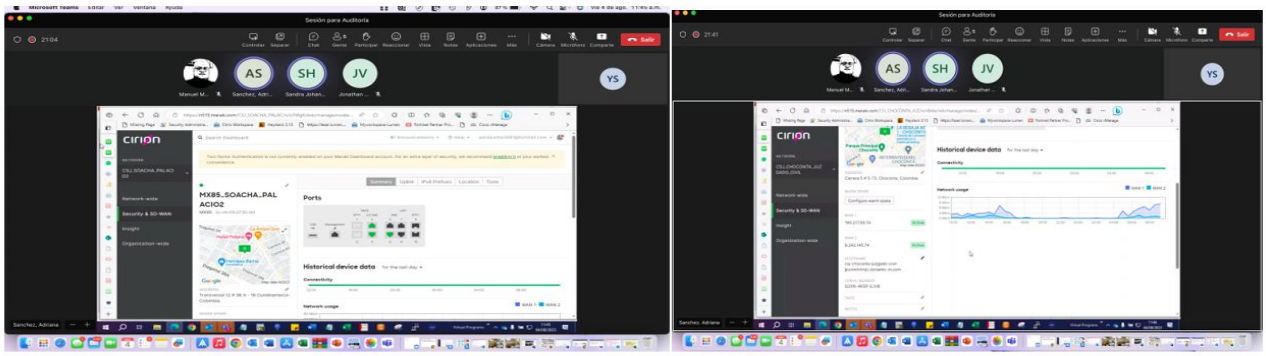




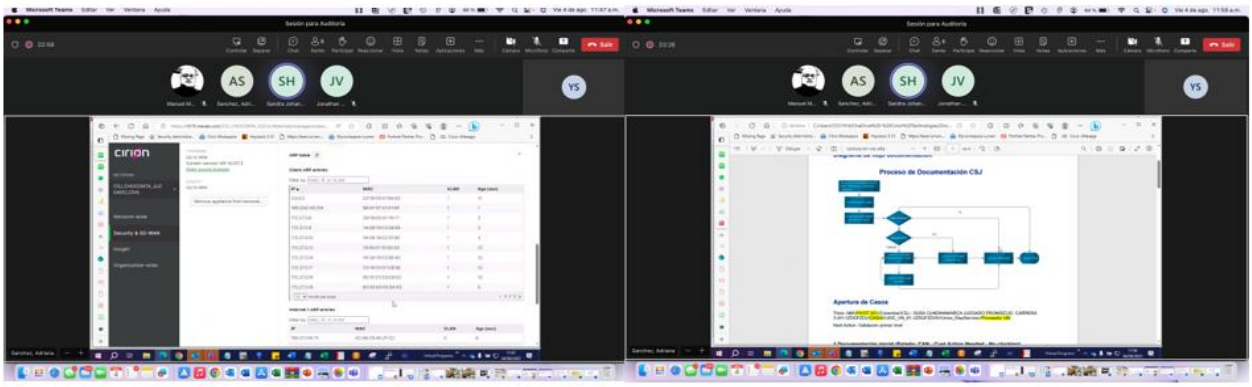
A.13.1. Gestión de la Seguridad en las Redes:

- La entidad cuenta con una red de tipología estrella, el proveedor “CIRION TECHNOLOGIES brinda seguridad a más de 1400 enlaces que conforma la red corporativa y datos a nivel país y la seguridad perimetral la maneja el proveedor “IFX" quien monitorea y garantiza la disponibilidad de los enlaces y tiempos de respuesta.
- Actualmente la entidad cuenta con interventoría para estos dos contratos.
- Se realizó reunión virtual con el proveedor “CIRION TECHNOLOGIES”, se validó disponibilidad de canales, la trazabilidad de los casos se registra en la herramienta OPS Console y cuentan con un procedimiento de atencion de casos

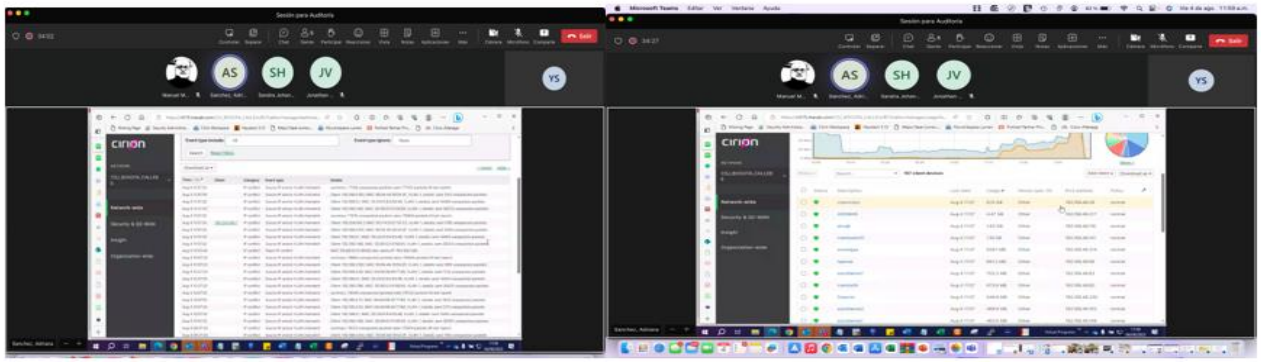
Se evidencio corte de fibra óptica en el enlace de Soacha, el cual ya estaba siendo atendido, como se observa en las siguientes capturas de pantalla:



Atención:



Log de eventos:



3.1. RESULTADO DETALLADO

NO.	DESCRIPCIÓN DEL HALLAZGO	PROCESO	CONFORMIDAD (En las columnas NC y Observación anotar el requisito a que aplica la Evidencia; en la Columna Criterios de auditoria /anotar el numeral de los requisitos auditados)		
			NC	OBSERVACION	CRITERIOS DE AUDITORÍA
1	No se evidenciaron las acciones para abordar los riesgos y oportunidades, como tampoco la forma de evaluar la eficacia de estas acciones.	Unidad de Informática y el Grupo de Proyectos Especiales en Tecnología de la Dirección Ejecutiva de Administración Judicial – DEAJ.	X		6.1. Acciones para tratar riesgos y oportunidades
2	Se evidencio que no hay coherencia entre los objetivos de seguridad de la información y la política de seguridad de la información, asi mismo, no se evidencio la planeación de los objetivos para logarlos, como también no han sido comunicados. De acuerdo con la muestra tomada: Política: *"… se compromete a la protección de los activos de información, manteniendo un nivel de exposición al riesgo que permita responder por la integridad, confidencialidad y disponibilidad de la información…"* Objetivo: *Establecer fundamentos para los esquemas de gobierno en SI a través de:* *Definición, mantenimiento y articulación permanente con el Modelo estratégico de Seguridad de la Información, el Plan Sectorial de desarrollo, los Pilares estratégicos de los procesos del CSdj, Modelo de Arquitectura Empresarial, el*	Unidad de Informática y el Grupo de Proyectos Especiales en Tecnología de la Dirección Ejecutiva de Administración Judicial – DEAJ.	X		6.2. Objetivos de seguridad de la información y planes para lograrlos

	PETD y el Plan Decenal del sistema de Justicia…				
3	No se evidenciaron los planes de tratamiento para los riesgos identificados para el SGSI	Unidad de Informática y el Grupo de Proyectos Especiales en Tecnología de la Dirección Ejecutiva de Administración Judicial – DEAJ.	X		8.3. Tratamiento de los riesgos de seguridad de la información
4	Se evidencio que no se entregó a tiempo la información *(homologación de las TRD y correos electrónicos que deben estar asociados a las áreas),* al proveedor THE BEST EXPERIENCE IN TECHNOLOGY, Toda vez que estas funcionales el proveedor las tenía listas desde el 31 de enero y de acuerdo con los correos evidenciados la entidad envió el 19 de julio la homologación de las TRD y el 27 de julio los correos electrónicos que deben estar asociados a las áreas, lo que ha atrasado la puesta en producción de estas funcionalidades.	Unidad de Informática y el Grupo de Proyectos Especiales en Tecnología de la Dirección Ejecutiva de Administración Judicial – DEAJ.	X		8.1 Planificación y control operacional *"la organización debe asegurar que los procesos contratados externamente estén controlados"*

3.2 FORTALEZAS

- Compromiso de la Unidad de Informática y el Grupo de Proyectos Especiales en Tecnología de la Dirección Ejecutiva de Administración Judicial – DEAJ con el sistema de gestión de seguridad de la información.
- Proveedores comprometidos con experiencia y conocimientos de acuerdo con el objeto del contrato
- Herramienta Power Apps para la gestión de los controles de Seguridad de la información
- Herramienta Bestdoc para la gestión documental
- Interventoría para los contratos de redes.
- Percepción y atención por parte de los proveedores, directores y funcionarios en el desarrollo de la auditoria
- Datacenter con control de acceso biométrico, bitácora, cableado organizado, UPS con sus respectivos mantenimientos, sensores, cámaras de seguridad al interior del data center y en los pasillos.

3.3 OPORTUNIDADES DE MEJORA

ERNST & YOUNG SAS

- En la herramienta Power Apps donde se realiza la gestión de riesgos y activos incluir en los campos notas de ayuda para facilitar su diligenciamiento.
- Fortalecer los informes forenses, donde se evidencie la aplicación de la metodología forense identificar, recolectar, preservar, extraer, documentar y evidencias que sean aceptables durante un procedimiento legal o administrativo, asi mismo proporcionar las métricas de análisis forense.
- Fortalecer la ejecución de mantenimientos preventivos y correctivos elaborando un plan con la entidad, para asegurar la continua disponibilidad e integridad de la infraestructura de los servicios.

THE BEST EXPERIENCE IN TECHNOLOGY

- Se sugiere que el proveedor utilice el procedimiento de gestión de incidentes como también utilizar la herramienta de gestión dispuesta por la entidad.
- Definir la periodicidad de entrega de la gestión de casos atendidos por el proveedor .
- En el informe de soportes incluir los tiempos de atención de los casos.

UNIDAD DE INFORMÁTICA Y EL GRUPO DE PROYECTOS ESPECIALES EN TECNOLOGÍA DE LA DIRECCIÓN EJECUTIVA DE ADMINISTRACIÓN JUDICIAL – DEAJ.

Contexto:

- Revisar y ajustar la redacción en la matriz DOFA con el propósito de no dar lugar a diferentes interpretaciones
- En la matriz DOFA incluir como "Fortaleza", el tema de uso y apropiación de las herramientas tecnológicas que dispone la entidad y las sensibilizaciones de seguridad de la información que se realizan.
- Ampliar la identificación de las necesidades y expectativas de las partes interesadas en temas relacionados con seguridad de la información.

Alcance:

- Fortalecer el alcance de implementación del SGSI incluyendo infraestructura tecnológica, necesidades de las partes interesadas, ubicación geográfica, asi mismo, mencionar que no se presentan exclusiones de controles del Anexo A.

Liderazgo:

- Aunque se evidencio el compromiso por parte de la alta dirección, se sugiere realizar sesiones de trabajo donde se validen las actualizaciones o nuevos documentos del SGSI, incluyendo la política sus objetivos y el alcance, asi mismo conservar la evidencia.

Recursos:

- Teniendo en cuenta que los cargos que responden a las funciones establecidas para mantener el sistema de gestión seguridad de la información ya están creados, se sugiere evaluar la posibilidad de formalizar esta división con el fin de darle el estatus que se requiere para cumplir las funciones establecidas en el plan estratégico de transformación digital y por ende en el plan sectorial de desarrollo.
- Según el acuerdo PCSJA22-12033 de Dic/2022 donde se crean los cargos con funciones y responsabilidades en seguridad de la información, ciberseguridad y privacidad se sugiere evaluar la viabilidad de ampliar la información relacionada con los requisitos de formación a Ingenieros Electrónicos, Ciencias de la Información y otras profesiones que han emergido dado las tendencias tecnológicas en Seguridad de Información, Ciberseguridad y Privacidad, asi mismo, se sugiere evaluar la posibilidad de ampliar el nivel de capacidades de los cargos actuales toda vez que los profesionales asignados a estos roles y responsabilidades en su mayoría son de perfiles básicos, operativos y en el entorno actual se requieren de perfiles altos, especializados con altas capacidades técnicas.

Comunicaciones:

- Fortalecer el ítem "3.5. Acciones" del documento "Estrategia y Plan de Cambio y Sensibilización del SGSI y Seguridad" el flujo de las comunicaciones internas y externas del SGSI.

Información Documentada:

- Asegurar que toda la documentación del SGSI que se crea o actualiza cumpla con los lineamientos de elaboración o actualización de documentos establecidos por la entidad.

Tratamiento de los Riesgos de Seguridad de la Información:

- Definir donde se va a documentar el contexto del proceso, para que se alinee con la metodología de riesgos que la entidad ha establecido.
- Para mayor entendimiento en el diligenciamiento de la herramienta Power Apps en el campo "Fecha" colocar "Fecha de Terminación", para evitar confusiones.
- Fortalecer la "Declaración de Aplicabilidad CSJ-GPET-PDA" incluyendo como se cumple cada uno de los controles, con el propósito de facilitar su entendimiento.
- En el documento "Metodología de Gestión de Riesgos de SGSI, Ciberseguridad y Datos Personales", incluir como se va a obtener por parte de los dueños de los riesgos, la aprobación del plan de tratamiento de riesgos y la aceptación de los riesgos residuales.

Seguimiento, Medición, Análisis y Evaluación:

- Revisar la redacción de los objetivos de los indicadores, es recomendable que inicie con un verbo en infinitivo y que mencione la intención de lo que se desea medir.
- Fortalecer el análisis del resultado de los indicadores que se encuentran registrados en la "Matriz de Análisis del SGSI "
- Identificar en el SGSI que se va a medir a través de indicadores o a través de seguimientos.

- Incluir dentro de la ficha de los indicadores quien es el responsable de analizar y evaluar los resultados, asi mismo, definir y establecer las acciones cuando los indicadores no cumplen la meta.

No conformidades y acciones correctivas

- Fortalecer el "Informe técnico de sincronización CCTV-Biométricos DC CAN, incluyendo el impacto funcional de la implementación de la sincronización del servicio NTP", actividad que corresponde al plan de acción del hallazgo relacionado con la sincronización de relojes el cual fue identificado en la auditoría externa.

Mejora:

- Además de las mejoras de la creación y actualización de los documentos del SGSI, tener en cuenta todas las mejoras que la entidad ha implementado o ha adquirido que aportan a la mejora continua del SGSI.

Controles del Anexo A:

A.5.Políticas de la seguridad de la información

- Formalizar el "Manual de Políticas de Seguridad de la Información, Ciberseguridad y Datos Personales" previa la auditoría externa.

A.8.1. Responsabilidad por los activos

- En la herramienta Power Apps incluir el campo "Tipo de Activo" para facilitar la identificación y mayor comprensión para el usuario.

A. 9.1. Requisitos del negocio para control de acceso

- En el "Manual de Políticas de SI", política 5.7 "Gestión Acceso de Usuarios" ítem (a), definir quienes son los responsables del reporte de la gestión de usuarios para los funcionarios de planta, contratistas y con base en esta información actualizar el "Procedimiento Gestión de Usuarios".

A. 9.2. Gestión de acceso de usuarios

- Asegurar revisar y actualizar el "Procedimiento Gestión de Usuarios", donde se establezcan las actividades de acuerdo como la entidad actualmente las está realizando, asi mismo tener en cuenta las posibles novedades (eje: vacaciones, renuncia, licencias de trabajo, licencias de maternidad, jubilación, fallecimiento, terminación de contrato, entre otras) que se puede presentar para la gestión de las cuentas de los usuarios.

A.11. Seguridad física y del entorno

- Se recomienda instalar el sistema de protección contra incendios en el data center ubicado en el 5 piso de la sede del CAN

A.13.2. Transferencia de información:

- En el "Procedimiento Transferencia de Información", incluir los controles que la entidad aplica para este proceso y no están documentados.
- Se sugiere que el formato de "Acuerdo de Confidencialidad para Realizar Transferencia de Información" sea validado por el área jurídica de la entidad.

A.14. Adquisición, desarrollo y mantenimiento de sistemas:

- En la actualidad la entidad no cuenta con contratos de desarrollo de software o desarrollos internos, en virtud que está alineando el "Plan de Transformación Digital" con el "Plan Nacional de Desarrollo" y el "Plan Sectorial de Desarrollo 2023-2026" de la Rama Judicial, los cuales establecen objetivos específicos que conllevan al redireccionamiento de la política en materia tecnología de toda la organización.

A.15.1.2. Tratamiento de la seguridad dentro de los acuerdos con los proveedores:

- Se sugiere que la entidad fortalezca el análisis de vulnerabilidades que realiza al software de los proveedores

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

- Tener en cuenta la formalización e implementación del plan de continuidad de seguridad de la información previo a la auditoría externa.

A.18.1.4. Privacidad y protección de información de datos personales

- Fortalecer el cumplimiento de la ley 1581 de 2012 Protección de Datos Personales

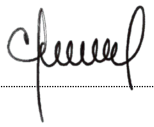
3.4 CONCLUSIONES

Se concluye que el sistema de gestión es conveniente y adecuado, sin embargo, es necesario que se tomen las acciones pertinentes para atender los hallazgos de No Conformidad identificados en esta auditoría; de la misma forma, se sugiere revisar en detalle las oportunidades de mejora descritas, para que en caso de que la organización lo considere pertinente, tome las acciones apropiadas.

Asegurar que la documentación que esta en proceso de creación y /o actualización se formalice y sea divulgada a la mayor brevedad.

4. NOMBRES Y FIRMAS

AUDITADO		
NOMBRE	**FIRMA**	**FECHA**
CARLOS FERNANDO GALINDO FRANCISCO JAVIER GONZÁLEZ JORGE ELIECER PACHÓN WILLIAM ESPINOSA SANTAMARIA MARIO FERNANDO SARRIA HELIO RIGOBERTO SALAZAR		

AUDITOR LIDER		
NOMBRE	**FIRMA**	**FECHA**
CLAUDIA PAOLA ANDRADE MURILLO		**Agosto 11 de 2023**