1. INFORMACIÓN GENERAL

TIPO DE AUDITORÍA	**Auditoría a procesos**		
INFORME PRELIMINAR		**INFORME FINAL**	**X**
PROCESO AUDITADO	OAP - Proceso de Gestión Tecnológica		
LÍDER DEL PROCESO	Miguel Leonardo Calderón Marín.		
OBJETIVO DE LA AUDITORÍA	Evaluar la eficiencia y eficacia de los controles generales de la función TIC y hacer seguimiento al avance de documentación de los procesos y procedimientos del MSPI. Realizar seguimiento de las acciones de mejora en ejecución de la Auditoría de controles generales de la Gestión Tecnológica relacionados con la infraestructura TIC y los servicios de la mesa de ayuda.		
ALCANCE DE LA AUDITORÍA	1. Evaluar la eficiencia y eficacia de los controles generales de a función TIC y hacer seguimiento al avance de documentación de los procesos y procedimientos del MSPI con enfoque en los dominios A9 (controles de acceso), A12 (Seguridad de las operaciones), A13 (Seguridad de las comunicaciones) y mesa de ayuda. 2. Realizar seguimiento de las acciones de mejora en ejecución de la Auditoría de controles generales de la Gestión Tecnológica relacionados con la infraestructura TIC y los servicios de la mesa de ayuda. 3. Presentar Informe Final de auditoría, que contenga desde el punto de vista técnico las oportunidades de mejora identificadas para el proceso de Gestión Tecnología para el sistema de control interno del IDEP, según el alcance de la auditoría y presentar las recomendaciones para implementar en la organización, lo anterior en el formato establecido por la Entidad.		
CRITERIOS DE LA AUDITORÍA	• PRO-GT-12-05 Mantenimiento de Infraestructura Tecnológica • PRO-GT-12-07 Registro de Activos de Información software, hardware y servicio del IDEP • PRO-GT-12-10 Mesa de Servicios		

	• PRO-GT-12-12 Control de cambios de gestión tecnológica
MARCO LEGAL	• Resolución 500 de marzo 10 de 2021 Mintic • Resolución 746 de 2022 Mintic • ISO 27001:2013 • Ley 1581 de 2012
LIMITACIONES DE LA AUDITORIA	En la presente auditoría no se presentaron limitaciones.
EQUIPO AUDITOR:	Yadira Velosa Poveda

1. INFORMACIÓN GENERAL 1

2. DESARROLLO DE LA AUDITORIA 3

3. FORTALEZAS 4

4. HALLAZGOS – NO CONFORMIDADES 4

5. RECOMENDACIONES Y/O ASPECTOS A MEJORAR 5

5.1. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 5
5.1.1. RECOMENDACIONES 6
5.2. ADMINISTRACIÓN DE ACCESOS Y SEGURIDAD LÓGICA 7
5.2.1. SEGURIDAD DE LA RED 7
5.2.2. SEGURIDAD SERVICIOS DE CORREO 12
5.2.3. SEGURIDAD DE INTERNET Y PC ´S 13
5.2.4. SEGURIDAD DE ARCHIVOS FUENTES Y DOCUMENTOS 17
5.2.5. APLICATIVOS Y BASES DE DATOS 19
5.2.6. GESTIÓN DE ACCESOS 22
5.2.7. RECOMENDACIONES 24
5.3. PROCEDIMIENTOS DE BACKUP Y RECUPERACIÓN 26
5.3.1. RECOMENDACIONES 28
5.4. MESA DE AYUDA 29
5.4.1. RECOMENDACIONES 31

6. CONCLUSIONES 32

2. DESARROLLO DE LA AUDITORIA

La auditoría se ejecutó conforme a lo establecido por la entidad en sus Procedimientos de Auditorías Internas con el apoyo en algunos lineamientos y buenas prácticas del Manual para la Implementación de la Política de Gobierno Digital Versión 7 abril de 2019.

Para efectos de la auditoría se adelantó el seguimiento a la implementación de acciones de mejora resultado de la auditoria del año 2022, para los escenarios planteados en el alcance, junto con la revisión de la configuración de controles en la plataforma tecnológica del IDEP.

En el marco de la auditoría se realizaron las siguientes actividades:

1. Entrevistas con los responsables de procesos, proyectos y gestión de activos TIC.
2. Levantamiento de información documental como evidencia de planeación, ejecución, seguimiento y acciones de mejora.
3. Inspección remota y captura de evidencias de la configuración de activos de la plataforma TIC.
4. Análisis documental y de evidencias.
5. Identificación de oportunidades de mejora, elaboración de informe y emisión de recomendaciones.

El área que suministró la información fue el proceso de Tecnología de la Información y Comunicaciones

La estructura del presente informe para cada escenario del alcance incluye los siguientes elementos:

Observaciones: Corresponden a los aspectos positivos (fortalezas) y negativos (debilidades) identificadas para el proceso de Gestión de Tecnología de Información y las Comunicaciones. Se utiliza la siguiente nomenclatura:

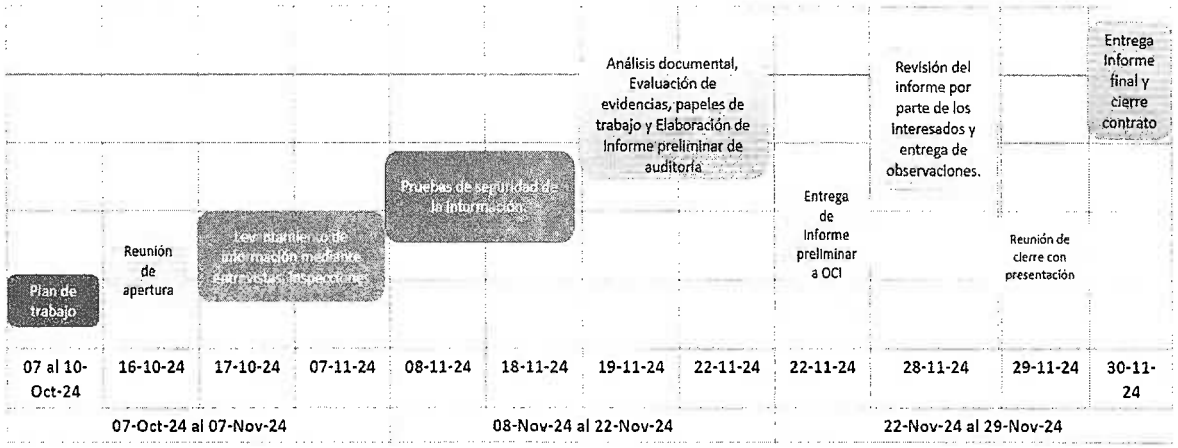
 Observación Positiva.

Observación positiva con opción de mejora.

 Observación negativa que amerita una acción de mejora.

Recomendaciones: Corresponde a las oportunidades de mejora que deben ser atendidas por el proceso de Gestión Tecnológica en respuesta a los hallazgos negativos o debilidades identificados en el ejercicio de la auditoría y que son la fuente para determinar y priorizar las acciones de mejoramiento. Vale aclarar que los hallazgos positivos no derivan en recomendaciones.

La auditoría fue ejecutada de acuerdo con la siguiente línea de tiempo.



3. FORTALEZAS

- Para este período de evaluación se evidenció la contratación de personal adicional y especializado para la OAP, lo que permite tener más nivelada la carga en las responsabilidades asignadas a esta oficina.

- Se realizó un levantamiento de información detallado sobre la infraestructura de red, identificando las áreas críticas de mejora para desarrollar un plan de acción adecuado lo que permitirá al IDEP actualizar su tecnología e implementar prácticas de seguridad más robustas y eficientes.

- El esquema utilizado para el alojamiento y respaldo de los documentos de usuario final es el uso de carpetas compartidas en la unidad TRD continúa configurado de forma adecuada, de acuerdo lo especificado en el instructivo para el almacenamiento de la información en carpetas compartidas.

- Los sistemas Humano y GOOBI S.A.S – tienen debidamente gestionada la legalidad de su uso a favor del IDEP y de propiedad del contratista.

- Se realizó un informe de diagnóstico de la situación actual de la mesa de ayuda que permitió establecer un plan de trabajo para implementar la herramienta de GLPI, con la cual se busca mejorar el servicio, la oportunidad de atención y medir eficazmente la gestión.

4. HALLAZGOS – NO CONFORMIDADES

La auditoría de controles generales no corresponde a una auditoría de cumplimiento del sistema de gestión de calidad, por lo tanto, se da reconocimiento a los instrumentos y procedimientos aplicados por la OAP para la gestión y operación de los servicios tecnológicos sin

condicionamiento de que dichos instrumentos o procedimientos sean documentos controlados del sistema de gestión.

En la presenta auditoría se identificaron oportunidades de mejora y se emitieron recomendaciones para atenderlas.

5. RECOMENDACIONES Y/O ASPECTOS A MEJORAR

5.1. Políticas de seguridad de la información

La Política de seguridad y privacidad de la información fue actualizada y aprobada en el Comité Institucional de Gestión y Desempeño de julio de 2024, aún no se ha formalizado su publicación, se atendieron las recomendaciones emitidas por la auditoría en la vigencia 2022, sin embargo, en esta versión no se evidencia la articulación entre lo que está declarado con lo implementado, su redacción está orientada hacia donde van.

Se continua con la suscripción del compromiso de cumplimiento de las políticas de seguridad de la información para los funcionarios y contratistas que ingresan a la entidad, como un insumo para la concientización, educación y capacitación sobre la seguridad de la información (control 7.2.2 ISO 27002:2013). Se reitera que, si bien la concientización es importante, también lo es que las políticas registradas sean consecuentes con los controles implementados en la plataforma tecnológica. Adicionalmente, este formato en la actualidad se está diligenciando en físico y posteriormente se digitaliza. Como oportunidad de mejora se recomienda implementarlo digitalmente.

Como instrumentos de planeación y seguimiento se cuenta con el documento PL-GT-12-04 Plan Seguridad y Privacidad de la Información 2024, el cual fue actualizado en agosto de 2024, se estructuró conforme a la implementación del ciclo PHVA del Modelo de Seguridad y Privacidad de la Información y a las metas trazadas para vigencia 2024. Se tienen descritas las actividades a realizar y los entregables, sin embargo, no se evidencia el factor tiempo, lo que permite llevar un control de su cumplimiento. Las acciones propuestas ayudan a fortalecer la implementación del MSPI, no cubren los dominios y tampoco están articuladas con las brechas identificadas en el autodiagnóstico.

Se mantiene la recomendación de la auditoría del 2022, respecto a la Declaración de aplicabilidad, la cual no se ha adelantado en el IDEP con la elaboración del marco documental de políticas, procedimientos, instructivos y formatos, incluyendo claramente las justificaciones y soportes para la exclusión de controles, que incluya entre otros:

- ✓ Manual de políticas de Seguridad de la Información
- ✓ Un Plan de capacitación, sensibilización y comunicación de seguridad de la información (control 7.2.2 ISO 27002:2013). Junto a un plan de gestión del cambio

asociado a las restricciones de las políticas y los nuevos procedimientos. Esto articulado con el dominio de uso y apropiación del MRAE.

- ✓ Implementación de los controles de seguridad de la información en la plataforma TIC de manera incremental de los más complejo a los más simple.
- ✓ Verificación técnica de vulnerabilidades.
- ✓ El levantamiento y planeación de los documentos comunes en el sistema integrado de gestión y la planeación de la salida escalonada de documentos de acuerdo con el avance en implementación.

5.1.1. Recomendaciones

N°.	Recomendación 2020
1.	Se evidencian algunas mejoras en la construcción de instrumentos documentales y en el formato y valoración del inventario de activos. De igual manera, se han realizado acciones para socializar y formalizar el cumplimiento de políticas de seguridad. Sin embargo, todavía no se evidencia la existencia de un Plan de Implementación de MSPI detallado para lograr las 4 dimensiones. Tener en cuenta que la implementación de los dominios no se realiza por orden de la norma, sino de acuerdo con los esfuerzos de su implementación, sensibilización y puesta en operación real.
2.	Atender la fase de diagnóstico conforme al Anexo 1, diligenciando el instrumento conforme a las instrucciones de MINTIC para obtener un análisis de brecha que permita establecer las actividades del plan de seguridad y privacidad de la información 2023. Ver instructivo: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/
3.	Una vez adelantado el diagnostico, elaborar el plan de seguridad y privacidad de la información incluyendo para cada uno de los siguientes dominios de gestión las actividades pertinentes con respecto a la brecha. • Activos de Información • Gestión de Riesgos • Gestión de Incidentes de Seguridad y Privacidad de la Información • Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación • Matriz de verificación de Requisitos Legales de Seguridad de la Información • Plan de Continuidad del Negocio • Oportunidades de mejoras SGSI • Planeación • Gobierno Digital en articulación con MIPG y MSPI • Auditorías Internas y Externas • Revisión de los controles de la norma ISO 27001:2013 • Indicadores SGSI • Vulnerabilidades Protección de datos personales
4.	Una vez establecido el plan determinar recursos humanos y técnicos para su ejecución y escalar a la alta dirección.
5.	Actualizar y/o construir los productos de la fase de planeación

N°.	Recomendación 2020
	• Alcance MSPI • Acto administrativo con las funciones de seguridad y privacidad de la información. • Política de seguridad y privacidad de la información. • Documento de roles y responsabilidades asociadas a la seguridad y privacidad de la información • Procedimiento de inventario y Clasificación de la Información e infraestructura crítica • Metodología de inventario y clasificación de la información e infraestructura crítica • Procedimiento de gestión de riesgos de seguridad de la información • Plan de tratamiento de riesgos de seguridad de la información • Declaración de aplicabilidad • Manual de políticas de Seguridad de la Información Plan de capacitación, sensibilización y comunicación de seguridad de la información
6.	En el marco de atención del MSPI, al elaborar la declaración de aplicabilidad, definir el inventario de documentos que deben ser elaborados para atender los controles de la norma que sean aplicables. A continuación, se adjunta una relación resumen de los controles ISO 27002:2013 Relacionar los documentos construidos y ajustarlos al diagnóstico.

5.2. Administración de accesos y seguridad lógica

5.2.1. Seguridad de la red

Se actualizó el diagrama de infraestructura actual, donde según el documento denominado "LEVANTAMIENTO DE INFORMACION DE RED ACTUAL DEL IDEP Y PROPUESTA DE MEJORA" y lo evidenciado por la auditoria se identificaron las siguientes falencias:

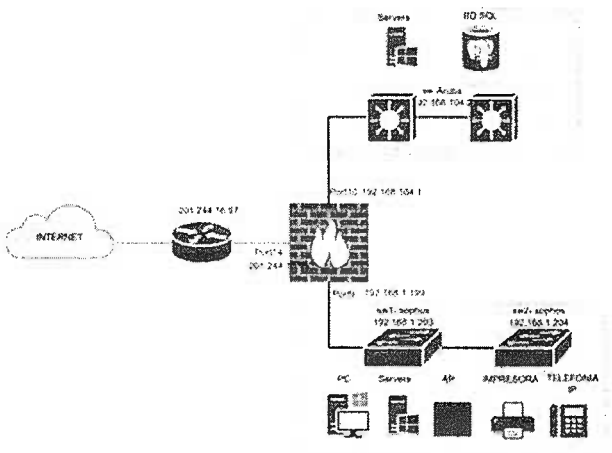
- El firewall Fortinet 500D, no ofrece ninguna funcionalidad a nivel de seguridad, actualmente funciona como enrutador, la licencia se encuentra vencida desde el 2023, lo que genera riesgo de posibles vulnerabilidades por obsolescencia del dispositivo, y al no tener actualizaciones de seguridad, ni soporte del fabricante, la entidad se expone a posibles ataques y/o falta de prestación de servicios por daños no soportados.

- Se ha identificado que la red actual presenta una configuración de tipo red plana, donde todos los dispositivos están conectados dentro del mismo segmento de red y comparten el mismo dominio de broadcast, sin ningún tipo de segmentación implementada. Al operar sin segmentación, el tráfico de broadcast se distribuye a todos los dispositivos de la red, lo que puede generar los siguientes problemas:
  - ✓ **Rendimiento degradado:** El tráfico innecesario afecta la eficiencia de la red, ya que todos los dispositivos procesan cada paquete de broadcast, lo que aumenta la latencia y el uso de los recursos.
  - ✓ **Mayor superficie de ataque:** Una red plana facilita que un atacante, una vez dentro, tenga visibilidad y acceso a todos los dispositivos conectados. Esto incrementa el riesgo de movimientos laterales, donde un atacante puede explorar y comprometer otros sistemas.

- ✓ **Dificultad en el control de accesos:** Sin segmentación, no se pueden aplicar controles específicos de acceso entre distintos grupos de dispositivos o usuarios, lo que dificulta la implementación de políticas de seguridad efectivas.
- ✓ **Problemas de escalabilidad:** A medida que la red crece, un diseño plano se vuelve insostenible, ya que el incremento en el tráfico broadcast afecta de manera exponencial el rendimiento.

El modelo de red actual presenta limitaciones, ya que no ofrece escalabilidad ni resiliencia ante fallas. Estas son capacidades fundamentales que sí puede garantizar un modelo de arquitectura basado en una estructura por capas. En el diseño actual, todos los equipos de capa 2 están funcionando exclusivamente como dispositivos de acceso, lo que genera una arquitectura plana y carente de los beneficios que aporta una jerarquía estructurada.

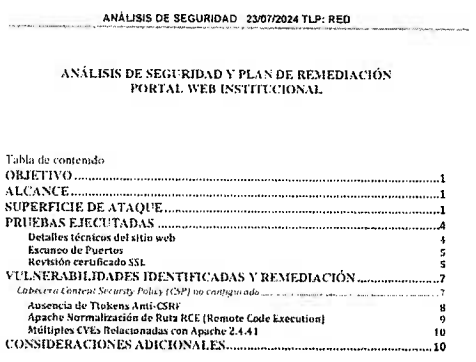
Sin redundancia ni mecanismos de conmutación por error *(failover)*, la red es vulnerable a fallas de dispositivos o enlaces individuales. Esto implica que una interrupción en un solo componente crítico puede afectar a toda la red. No hay un diseño de respaldo que permita mantener la operación en caso de incidentes.



A nivel de la solución de conectividad Wi-Fi actual, se identificó que algunos de los equipos conectados son de particulares de contratistas y/o funcionarios. Esta situación puede afectar la experiencia de los usuarios que se conectan de forma inalámbrica, generando una percepción de lentitud, inestabilidad y bajo rendimiento.

La entidad está adelantando el proceso de selección y adquisición de un firewall que garantice la seguridad perimetral con las ultimas características y actualizaciones. Se evidenció que en la ficha técnica se incluyeron los servicios de transferencia de conocimiento y soporte. Se recomienda dentro de la transferencia incluir el uso de las herramientas de monitoreo y la interpretación de las alertas.

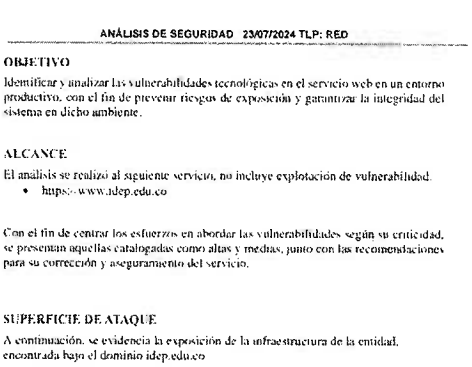
El IDEP en el mes de julio de 2024 realizó avances en el análisis de vulnerabilidades sobre el portal Web y la ejecución de su plan de remediación, como se evidencia a continuación:


ANÁLISIS DE SEGURIDAD 23/07/2024 TLP: RED

ANÁLISIS DE SEGURIDAD Y PLAN DE REMEDIACIÓN
PORTAL WEB INSTITUCIONAL

Tabla de contenido

OBJETIVO 1
ALCANCE 1
SUPERFICIE DE ATAQUE 1
PRUEBAS EJECUTADAS 4
Detalles técnicos del sitio web 4
Escaneo de Puertos 5
Revisión certificado SSL 5
VULNERABILIDADES IDENTIFICADAS Y REMEDIACIÓN 7
Cabecera Content Security Policy (CSP) no configurado 7
Ausencia de Tokens Anti-CSRF 8
Apache Normalización de Ruta RCE (Remote Code Execution) 9
Múltiples CVEs Relacionadas con Apache 2.4.41 10
CONSIDERACIONES ADICIONALES 10


ANÁLISIS DE SEGURIDAD 23/07/2024 TLP: RED

OBJETIVO

Identificar y analizar las vulnerabilidades tecnológicas en el servicio web en un entorno productivo, con el fin de prevenir riesgos de exposición y garantizar la integridad del sistema en dicho ambiente.

ALCANCE

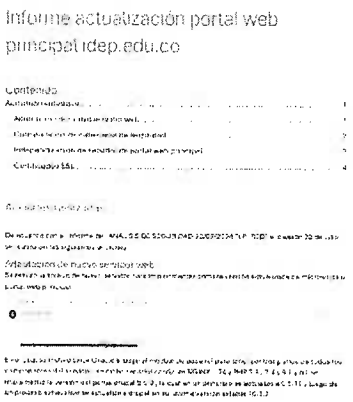
El análisis se realizó al siguiente servicio, no incluye explotación de vulnerabilidad:

- https://www.idep.edu.co

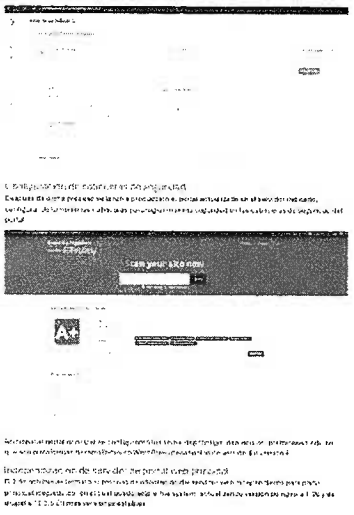
Con el fin de centrar los esfuerzos en abordar las vulnerabilidades según su criticidad, se presentan aquellas catalogadas como altas y medias, junto con las recomendaciones para su corrección y aseguramiento del servicio.

SUPERFICIE DE ATAQUE

A continuación, se evidencia la exposición de la infraestructura de la entidad, encontrada bajo el dominio idep.edu.co


Informe actualización portal web principal idep.edu.co

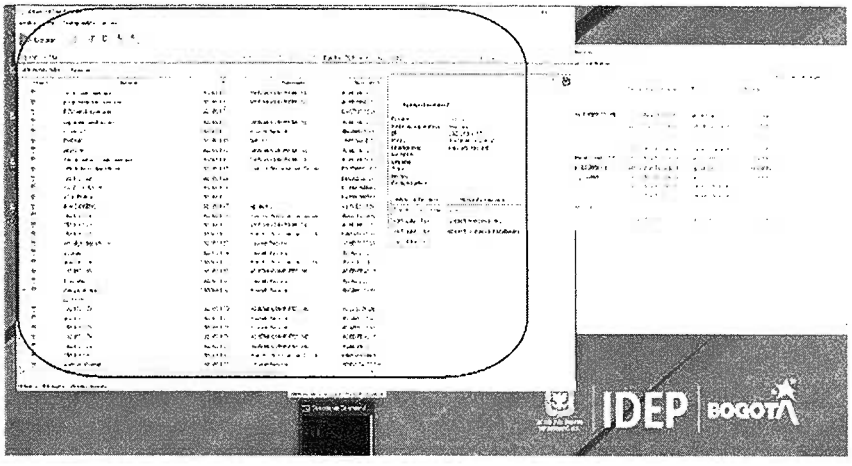
Contenido



Se recomienda continuar con este tipo de análisis periódicamente como buena práctica, ejecutando el respectivo plan de remediación lo que le permitirá al IDEP contar con sitios seguros.

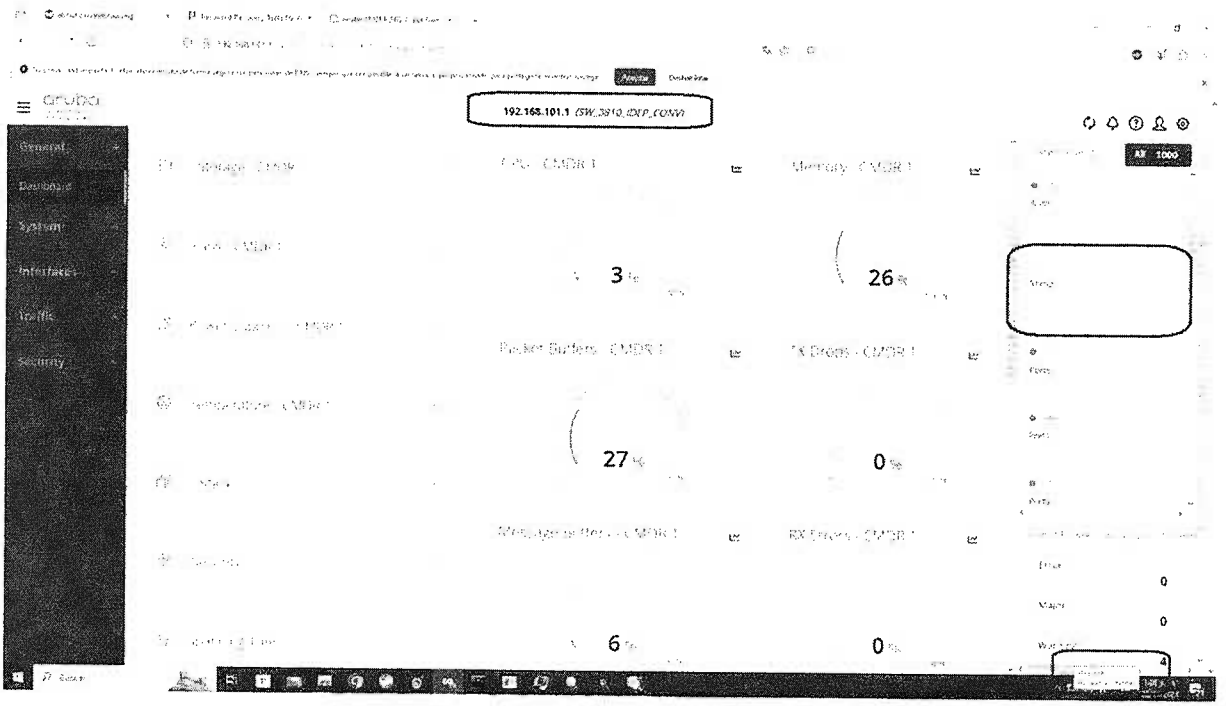
Durante las pruebas realizadas por la auditoría, se observó que aún no se han implementado: controles de acceso a las redes inalámbricas WiFi a las que tienen acceso los equipos de la Entidad, configuraciones de las VLAN's y las otras oportunidades de mejora relacionas en los informes de auditoria anteriores relacionadas con el firewall debido a que se espera la adquisición de los nuevos equipos para proceder a su implementación. La falta de estos controles conlleva que no se apliquen las políticas de seguridad y navegación establecidas por el proceso, lo cual representa un riesgo significativo para la gestión de la seguridad de la información.

En la siguiente imágenes se evidencia que aún se permiten escaneos y que la red aún no está segmentada correctamente:

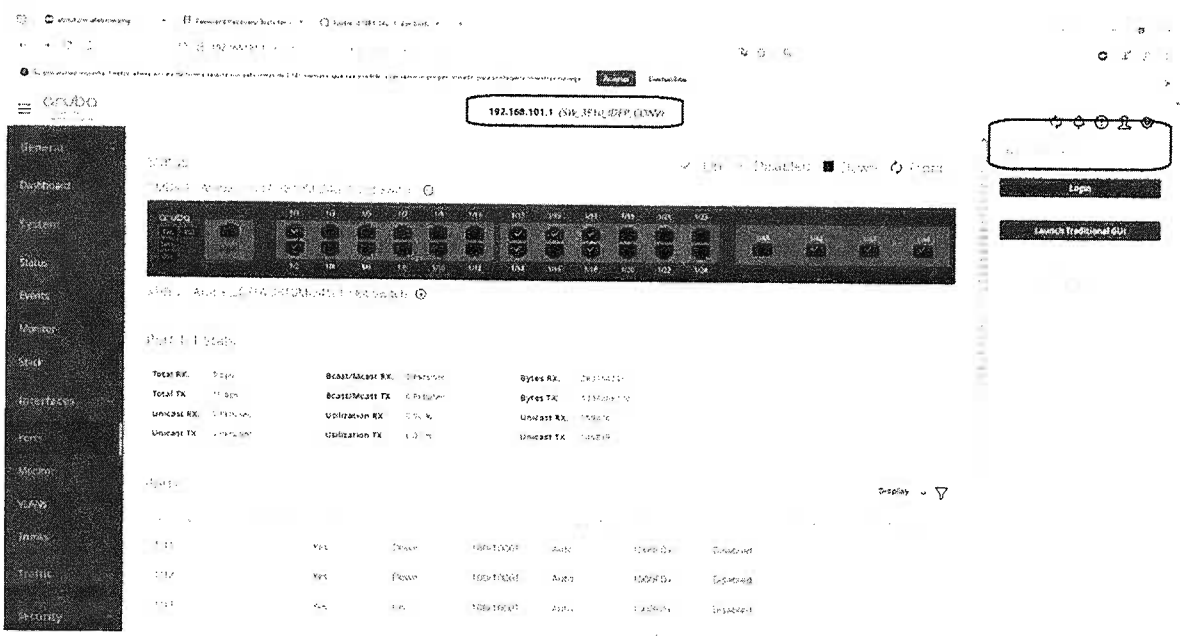


- En los escaneos realizados, se identificó que la consola de configuración del switch Aruba con dirección IP 192.168.101.1, ubicado en el segmento destinado a la base de datos según el diagrama de red proporcionado, se encuentra expuesta y accesible sin autenticación o utilizando las credenciales predeterminadas de fábrica (usuario: "Admin", contraseña: "Admin"). Este hallazgo representa una vulnerabilidad crítica, asociado a los siguientes riesgos:
    - **Exposición de Configuración Sensible:** Un atacante podría acceder a la consola y realizar cambios en la configuración del switch, comprometiendo la estabilidad y seguridad de la red.
    - **Riesgo de Ataques de Denegación de Servicio (DoS):** Al modificar parámetros clave, como el manejo de tráfico o las reglas de enrutamiento, se podrían generar interrupciones intencionales en la operación de la red, afectando la disponibilidad de los servicios.
    - **Posibilidad de Escalamiento de Ataques:** La falta de protección en el acceso podría facilitar la captura de información crítica, como tablas de enrutamiento, VLANs configuradas y detalles de dispositivos conectados, que pueden ser utilizados para planificar ataques más sofisticados.

-Imagen de evidencia de acceso sin usuario al switch Aruba, en el recuadro rojo se muestra la alerta de violación de acceso con el usuario asignados automáticamente por el dispositivo: *public*:



-Imagen de evidencia de acceso con el usuario administrador: "operador" al switch Aruba, con este usuarios se podrían realizar modificaciones a la configuración:



- Cabe anotar que en la restructuración y adquisición de nuevos equipos se tiene contemplada esta implementación. Adicionalmente, en los diagnósticos realizados como parte de la planificación para la implementación de la nueva infraestructura de TI, se ha identificado la necesidad de fortalecer las capacidades de seguridad internas. Para ello, se tiene contemplada la sincronización del firewall con los endpoints de la red. Esta medida permitirá una detección y monitoreo más efectivos de posibles ataques internos, ya que el firewall podrá identificar y reaccionar ante actividades sospechosas o no autorizadas en los dispositivos finales conectados a la red. La integración de estas tecnologías facilitará una protección más granular y en tiempo real, asegurando que cualquier intento de intrusión o comportamiento anómalo sea detectado.
- Además, se prevé la inclusión de herramientas de monitoreo que ayudarán a subsanar las falencias detectadas en la infraestructura actual. Estas herramientas proporcionarán visibilidad constante sobre el estado de la red, permitiendo identificar vulnerabilidades, anomalías en el tráfico de datos, y posibles puntos débiles en la seguridad que puedan ser explotados.

5.2.2. Seguridad servicios de correo

La entidad cuenta con el documento MN-GT-12-16, Manual de Administración y Gestión de las Cuentas de Correo del IDEP, el cual establece lineamientos para la correcta gestión y administración de las cuentas de correo electrónico utilizadas por los usuarios. Sin embargo, este manual aún no está integrado de manera formal al plan de contingencia de la institución, lo que limita su aplicabilidad en situaciones de emergencia o recuperación ante desastres. Integrar este manual con el plan de contingencia es crucial para garantizar la continuidad operativa de la comunicación institucional en caso de incidentes que afecten el sistema de correo electrónico.

- Actualmente, el manejo del correo electrónico en la entidad se realiza a través de la suite de Google, lo que permite una gestión de las cuentas y una integración con otros servicios de colaboración. No obstante, la entidad está en proceso de elaboración de la ficha técnica para la adquisición e implementación de Microsoft 365, que ofrecerá ventajas en términos de estandarización, seguridad, colaboración y administración centralizada.

A pesar de que la transición a Microsoft 365 está en marcha, actualmente no se han implementado herramientas ni configuraciones que permitan sincronizar las cuentas del directorio activo del IDEP con las cuentas de correo electrónico. La falta de esta sincronización dificulta el proceso de creación de nuevos usuarios, la eliminación de cuentas obsoletas y la administración general de las cuentas de correo. Además, sin esta integración, no se asegura que las políticas de seguridad configuradas en el directorio activo sean obligatorias para las cuentas de correo, lo que podría generar vulnerabilidades en la gestión de usuarios y la protección de la información.

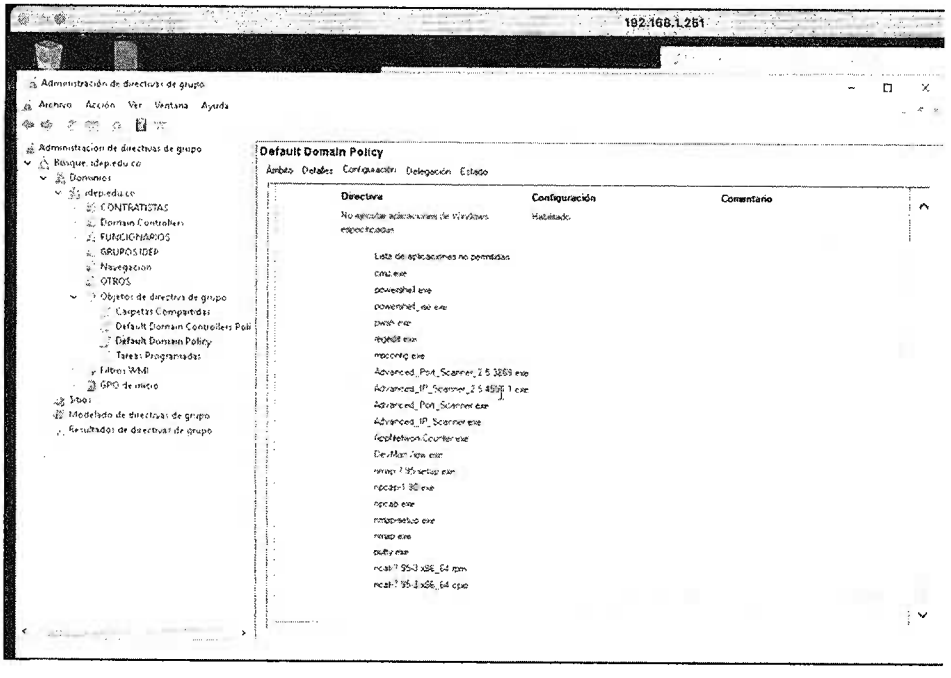
- Sin embargo, esta sincronización y la implementación de las políticas de seguridad serán parte integral del proceso de implementación de Microsoft 365. La integración del directorio activo con el correo electrónico permitirá que la creación, modificación y eliminación de cuentas de usuario se realice de manera automatizada, garantizando que las políticas de seguridad aplicadas en el dominio se extiendan de forma coherente a las cuentas de correo electrónico.

A pesar de los avances pendientes, la entidad ya ha implementado una autenticación de doble factor (MFA) para las cuentas de correo electrónico, lo cual representa una medida para mejorar la seguridad y minimizar el riesgo de suplantación de identidad. Esta capa adicional de seguridad reduce significativamente las posibilidades de que un atacante acceda a las cuentas, incluso si obtiene la contraseña del usuario, lo que mejora la protección de la información institucional y personal.

En resumen, aunque la entidad aún está en proceso de implementación de las herramientas necesarias para una integración más eficiente y segura de las cuentas de correo con el directorio activo, ya se están tomando medidas, como la habilitación de la autenticación de doble factor, para mitigar los riesgos asociados. El próximo paso será asegurar la sincronización completa entre el directorio activo y las cuentas de correo mediante la implementación de Microsoft 365, lo que permitirá una administración más centralizada, eficiente y segura de las cuentas de los usuarios.

5.2.3. Seguridad de Internet y PC ´s

En la configuración de la aplicación de directivas de grupo se ha definido una lista de aplicaciones no permitidas, como se detalla a continuación. Sin embargo, durante las pruebas realizadas por el equipo de auditoría, se observó que este control no cumple con su objetivo de forma efectiva:

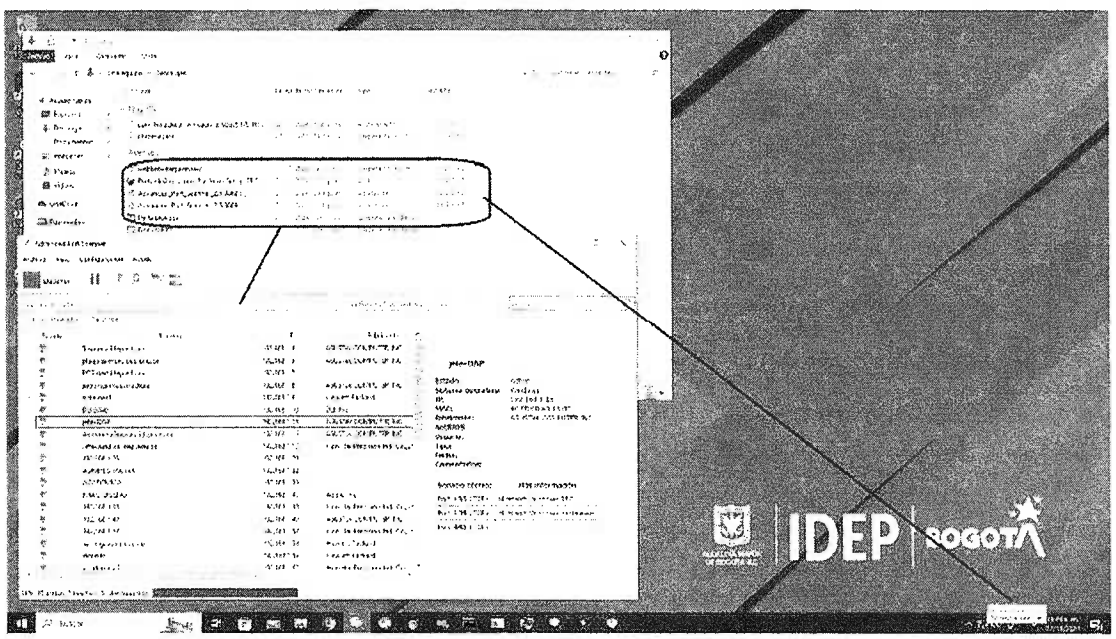


En las pruebas realizadas por la auditoría, se evidencia que no están activas las configuraciones destinadas al control de descargas y la ejecución de aplicaciones portables, si bien aún se encuentran implementadas aun las políticas de restricción: de instalaciones, de acceso al panel de control y de ejecución de scripts (PowerShell) y comandos (cmd) en los equipos de los usuarios que están unidos al dominio de la Entidad, el auditor logró evadir las políticas de seguridad implementadas al descargar y/o ejecutar software portable en el equipo de la entidad asignado para las pruebas. Este tipo de software, que no requiere instalación para funcionar, permitió al auditor realizar una serie de actividades que comprometen la seguridad, entre ellas:

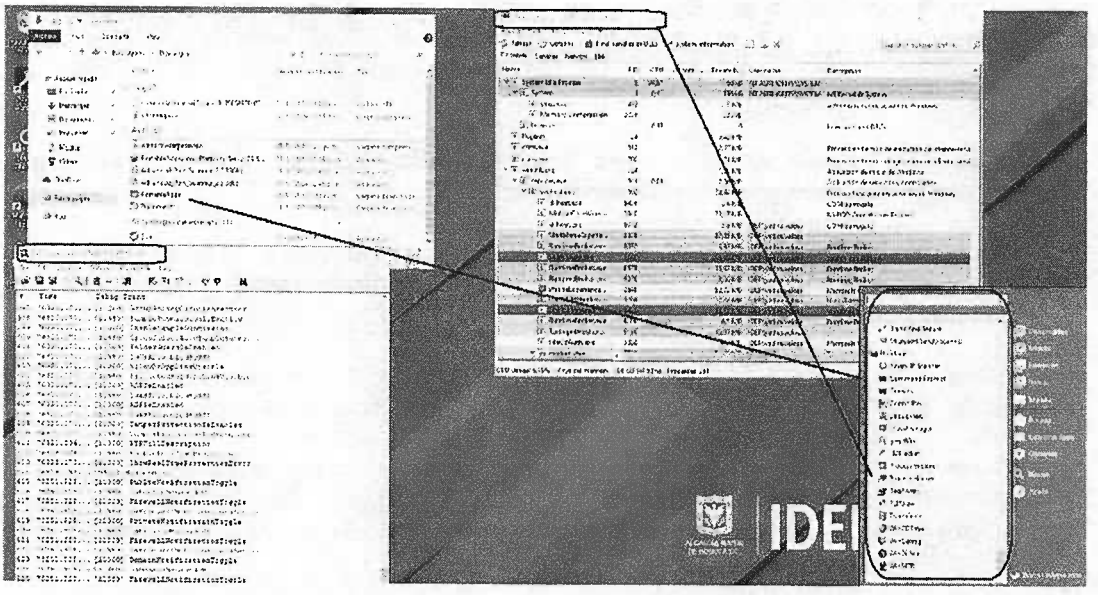
- ✓ Escaneos de red: Identificación de dispositivos, servicios y vulnerabilidades dentro de la red de la entidad.
- ✓ Ejecución de software FTP: Posibilidad de transferir archivos desde o hacia servidores, lo que podría facilitar la exfiltración de datos.
- ✓ Acceso al CMD portable: Ejecución de comandos sin restricciones, abriendo la posibilidad de ejecutar scripts o realizar configuraciones no autorizadas.
- ✓ Ejecución de software peligroso: Uso de herramientas comúnmente utilizadas para planificar y ejecutar ataques, lo que demostró la capacidad de comprometer el entorno de seguridad.

En las siguientes imágenes se muestra evidencia de estos casos:

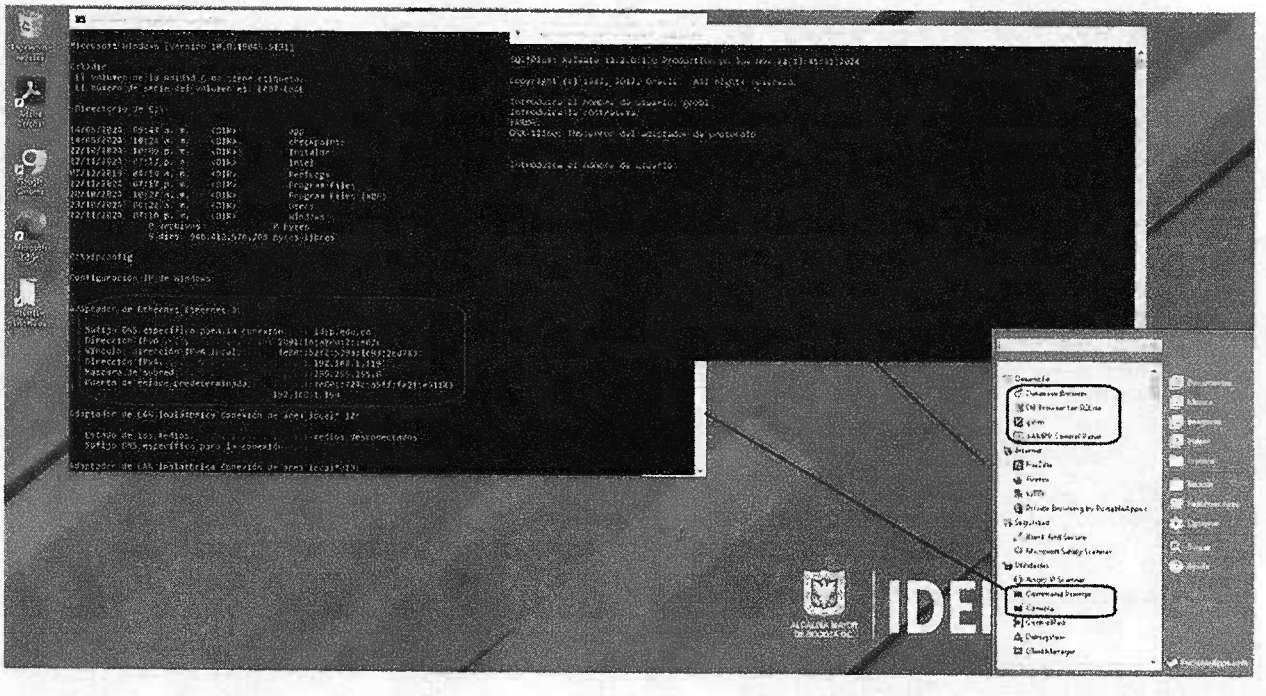
-Evidencia de descarga de aplicaciones y ejecución en su versión portable para escaneos de red:



-Evidencia de descarga y ejecución de suite de aplicaciones portables con ejecución de software malicioso y utilizado para ataques a la seguridad:



-Evidencia ejecución de *cmd* portable y consola portable con posibilidad de conexión a base de datos:



No se cuenta con un sistema de control de navegación que permita gestionar y restringir el acceso a sitios web no autorizados o potencialmente peligrosos. Además, la protección antivirus

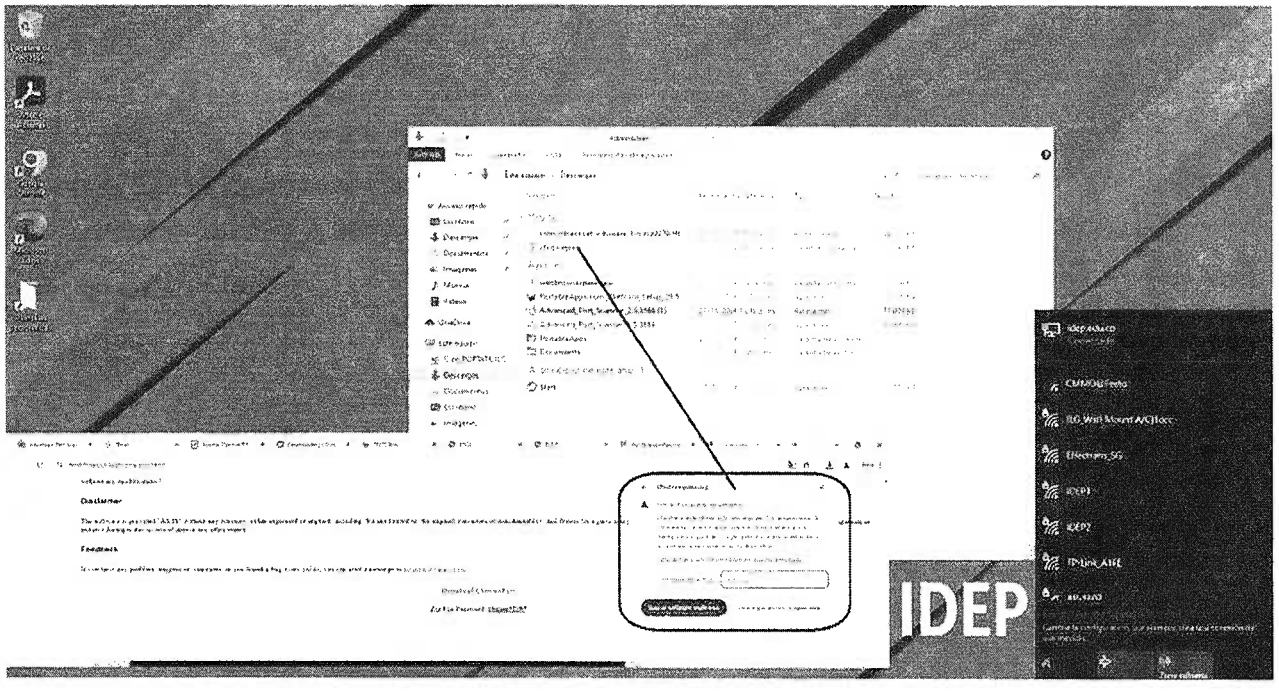
existente se limita al software por defecto de Windows, lo que deja expuestas múltiples vulnerabilidades al no ofrecer controles avanzados, como la gestión de dispositivos de almacenamiento externo, políticas estrictas para la descarga de archivos o la supervisión del tráfico web.

- ✓ Los usuarios pueden acceder sin restricciones a sitios web de riesgo, incluyendo aquellos clasificados como peligrosos o con contenido malicioso.

- ✓ También se permite el acceso a páginas de ocio, como juegos en línea, lo que no solo representa un riesgo de seguridad, sino que también puede afectar la productividad de los empleados.

- ✓ La falta de una solución integral de protección dificulta el monitoreo y control sobre dispositivos USB, unidades externas, y otros medios susceptibles a infecciones.

- ✓ Aunque el antivirus detecta algunos archivos maliciosos, como en el caso de prueba con la herramienta ChromePass en la siguiente imagen, no bloquea la descarga automáticamente, lo que deja abierta la posibilidad de ejecución y propagación de amenazas.



Estos hallazgos evidencian que, aunque existen configuraciones iniciales para limitar acciones riesgosas, no son lo suficientemente robustas como para impedir la ejecución de software

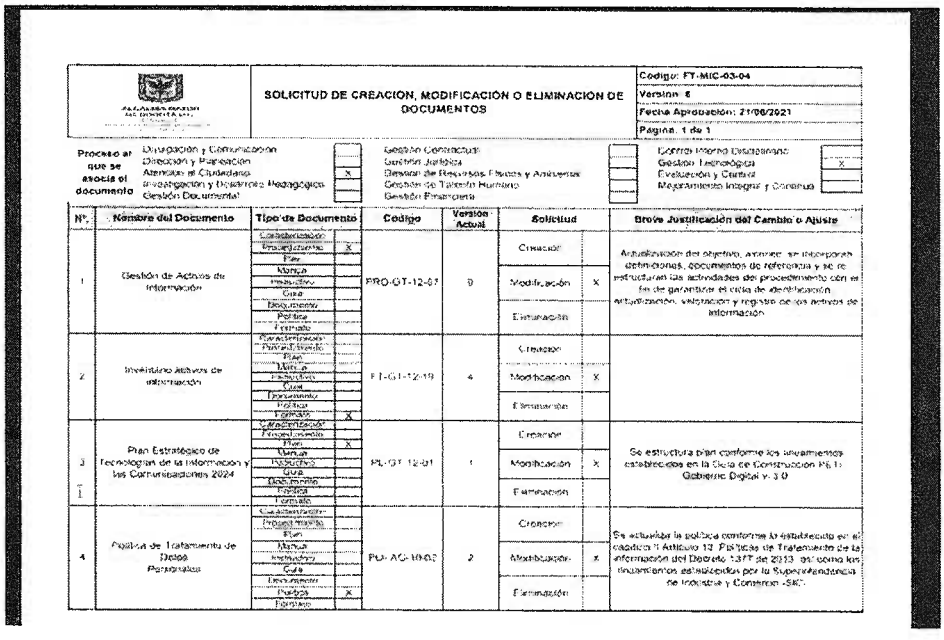
portable. Este tipo de herramientas representa un riesgo significativo, ya que permite evadir controles básicos y ejecutar acciones potencialmente maliciosas sin dejar rastro en sistemas de monitoreo tradicionales.

Si bien se ha contemplado el fortalecimiento de estas protecciones dentro del proceso de reestructuración y en la implementación de nuevas adquisiciones tecnológicas, el retraso en su ejecución representa una vulnerabilidad crítica. Las demoras en la implementación de estas medidas dejan a la entidad expuesta a múltiples amenazas, incluyendo:

- **Ataques dirigidos:** Aprovechando la falta de control efectivo sobre herramientas maliciosas.
- **Acceso no autorizado:** A través de software que elude restricciones actuales.
- **Compromiso de datos sensibles:** Lo que podría derivar en pérdidas financieras, reputacionales o legales.

5.2.4. Seguridad de Archivos Fuentes y Documentos

El IDEP tiene planeado para el mes de noviembre realizar la actualización de activos de información, se actualizó el procedimiento y el formato inventario de activos tecnológicos y se está trabajando articuladamente con Gestión Documental.



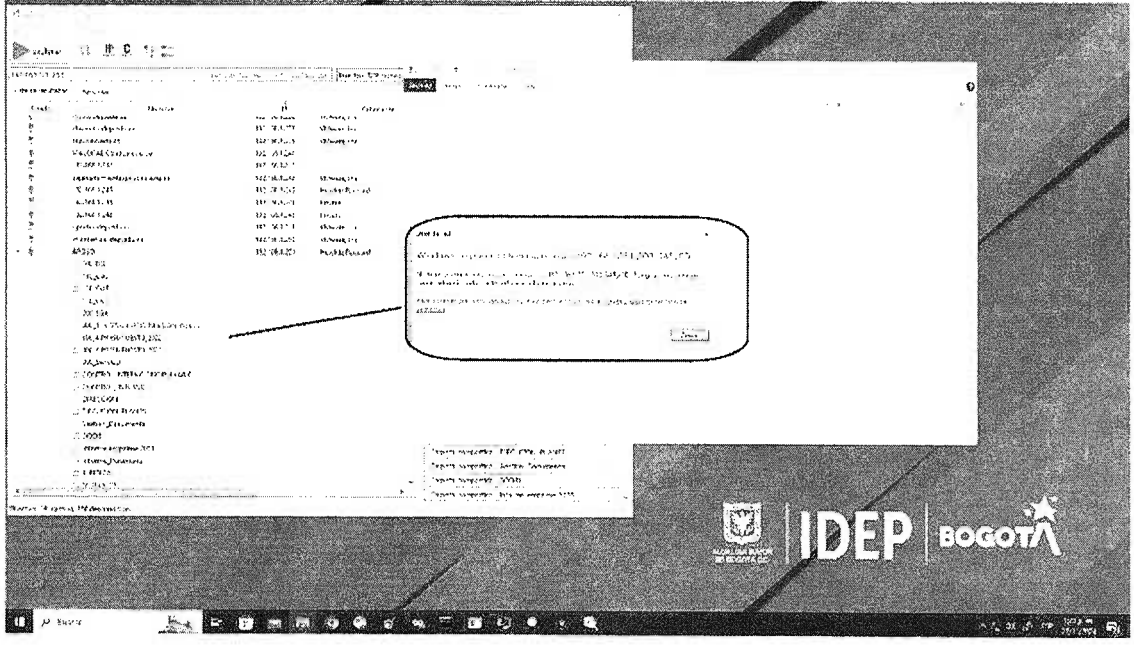
SOLICITUD DE CREACION, MODIFICACIÓN O ELIMINACIÓN DE DOCUMENTOS

Código: FT-MIC-03-04 | Versión: 6 | Fecha Aprobación: 21/06/2021 | Página: 1 de 1

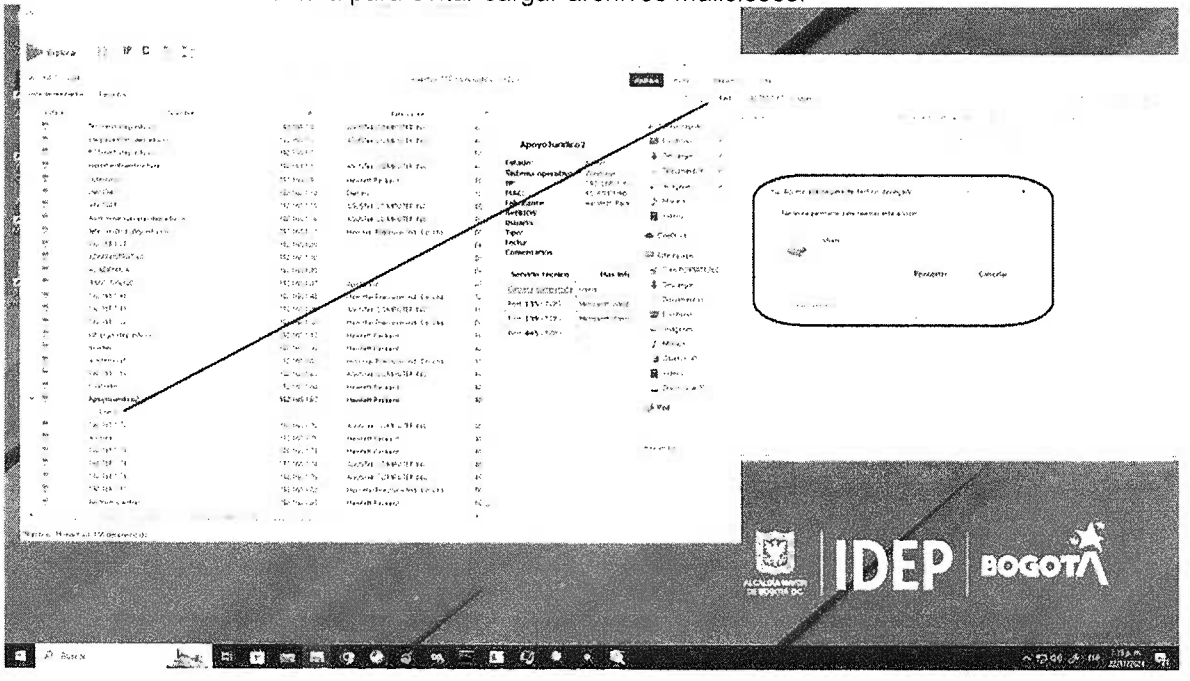
Proceso al que se asocia el documento: Direccionamiento y Comunicaciones; Dirección y Planeación; Atención al Ciudadano; Investigación y Gobierno Pedagógicos; Gestión Documental; Gestión Contractual; Gestión Jurídica; Dinamizar de Recursos Físicos y Ambientes; Gestión de Talento Humano; Gestión Financiera; Control Interno Disciplinario; Gestión Tecnológica (X); Evaluación y Control; Mejoramiento Integral y Continuo

Nº.	Nombre del Documento	Tipo de Documento	Código	Versión Actual	Solicitud		Breve Justificación del Cambio o Ajuste
1	Gestión de Activos de Información	Caracterización; Procedimiento (X); Plan; Manual; Instructivo; Guía; Documento; Política; Formato	PRO-GT-12-07	9	Creación		Actualización del objetivo, alcance, se incorporan definiciones, documentos de referencia y se re estructuran las actividades del procedimiento con el fin de garantizar el ciclo de identificación, actualización, valoración y registro de los activos de información
					Modificación	X	
					Eliminación		
2	Inventario Activos de Información	Caracterización; Procedimiento; Plan; Manual; Instructivo; Guía; Documento; Política; Formato (X)	FT-GT-12-19	4	Creación		
					Modificación	X	
					Eliminación		
3	Plan Estratégico de Tecnologías de la Información y las Comunicaciones 2024	Caracterización; Procedimiento; Plan (X); Manual; Instructivo; Guía; Documento; Política; Formato	PL-GT-12-01	1	Creación		Se estructura plan conforme los lineamientos establecidos en la Guía de Construcción PETI Gobierno Digital v. 3.0
					Modificación	X	
					Eliminación		
4	Política de Tratamiento de Datos Personales	Caracterización; Procedimiento; Plan; Manual; Instructivo; Guía; Documento; Política (X); Formato	PO-AC-10-02	2	Creación		Se actualiza la política conforme lo establecido en el capítulo II Artículo 12 Políticas de Tratamiento de la información del Decreto 1377 de 2013 así como los lineamientos establecidos por la Superintendencia de Industria y Comercio -SIC-
					Modificación	X	
					Eliminación		

Durante las pruebas realizadas por la auditoría, se evidenció que no se encontró información expuesta en los escaneos realizados, ni recursos sin protección, como se evidencia en la siguiente imagen, lo cual es un aspecto positivo. A pesar de esto, se debe seguir trabajando en la trazabilidad de los permisos y establecer protocolos claros para manejar las excepciones o desviaciones del plan original.



Se evidencia que las algunas carpetas que si bien se pueden acceder mediante escaneos de red tiene control de escritura para evitar cargar archivos maliciosos:



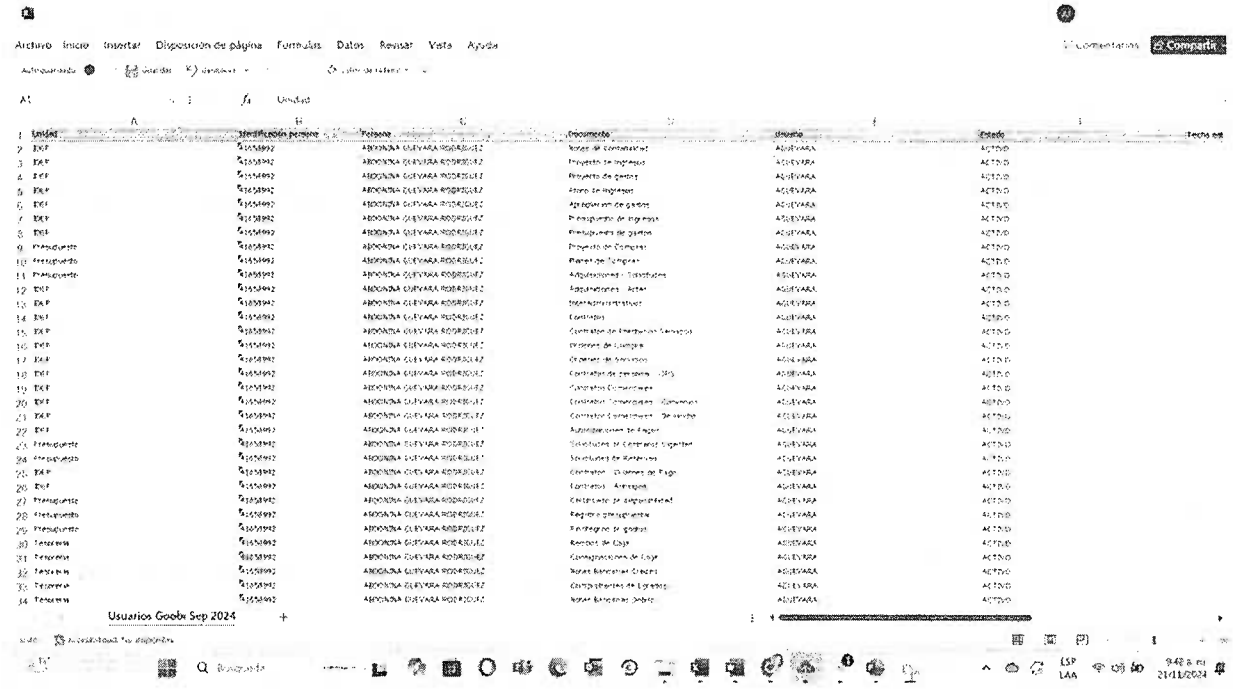
En las pruebas realizadas por la auditoria se evidencia que en los servicios de almacenamiento en la nube (Google Drive) no se encuentra información expuesta y los permisos de acceso a unidades compartidas se encuentra correctamente configurados.

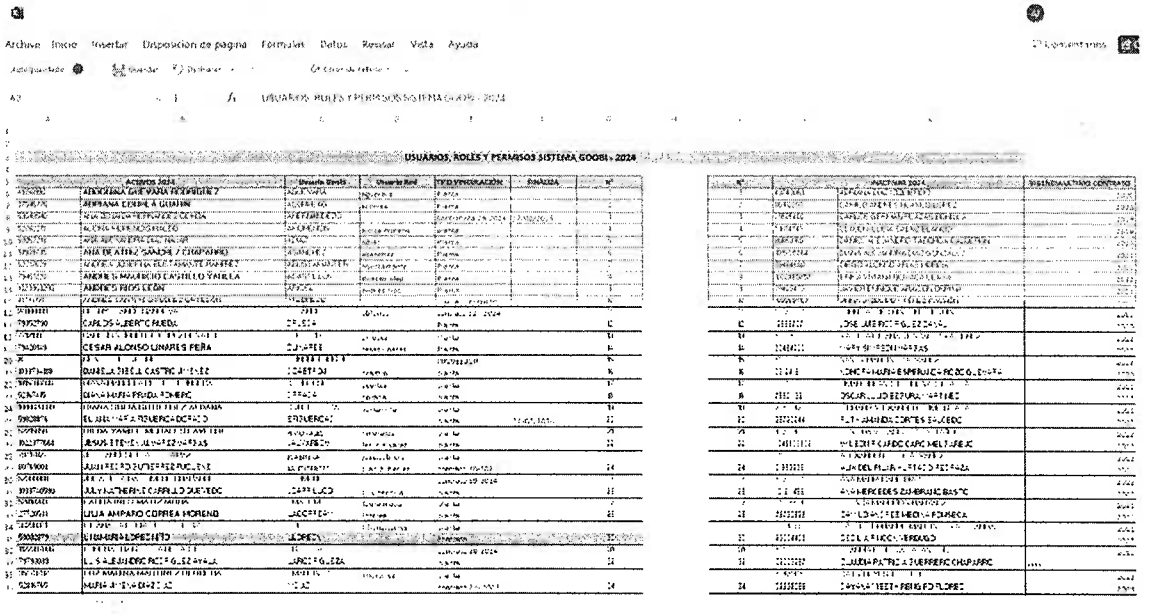
Aún no se han adoptado métodos, ni instructivos de protección de archivos, documentos o unidades de almacenamiento mediante el uso de protección de contraseñas, encriptación de medios y archivos que permitan garantizar la confidencialidad de la información así clasificada en caso de pérdida de unidades de almacenamiento o equipos portátiles, o en caso de que se puedan acceder a carpetas sin protección con esta información.

5.2.5. Aplicativos y bases de datos

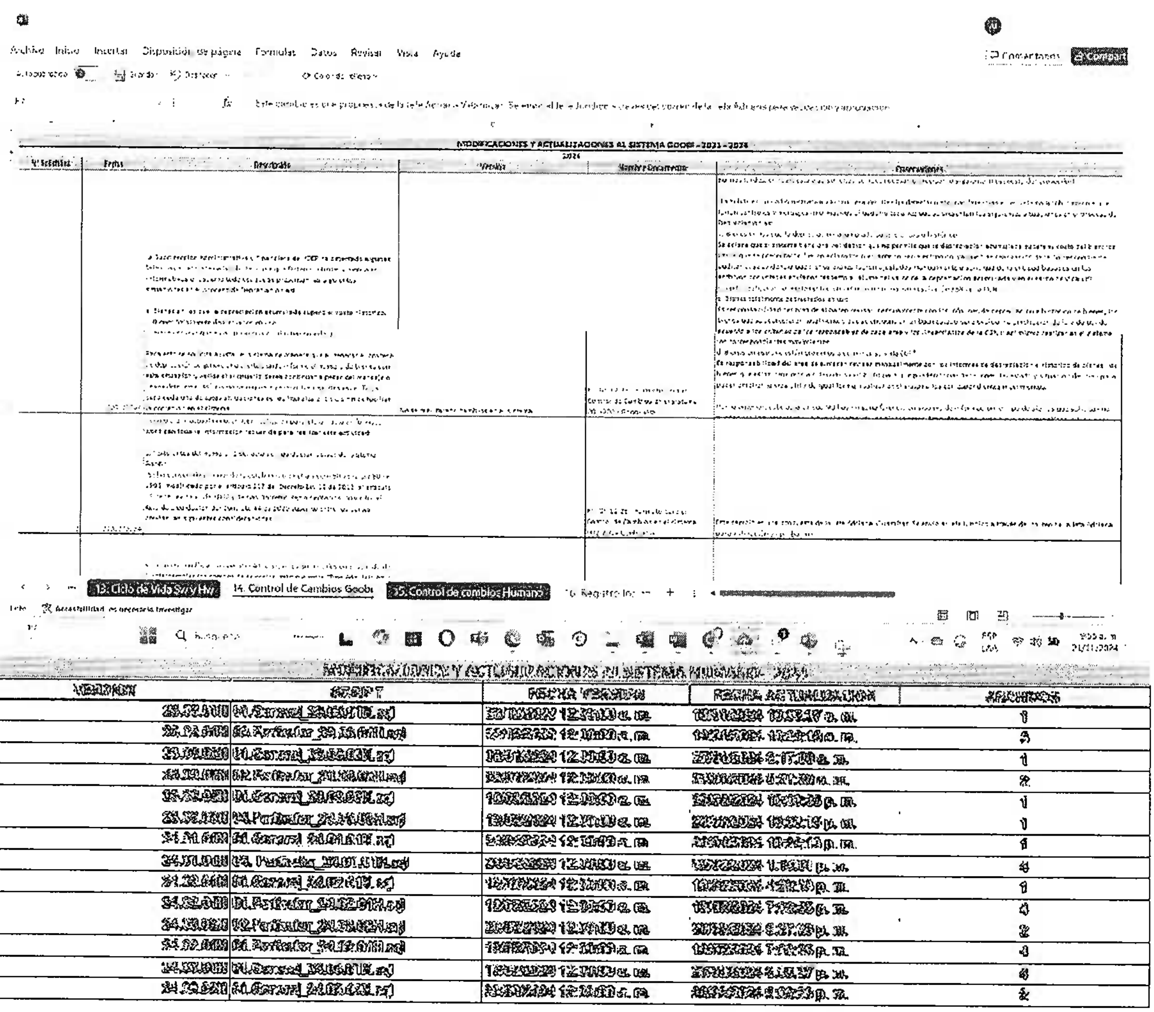
El sistema Goobi genera un listado de usuarios con los permisos asignados y con base en esta información periódicamente se hace un control de usuarios, en este sistema de información los permisos son asignados por usuario y están articulados con el dominio.

El proveedor suministró un script para la inactivación de usuarios, el cual debe afinarse para que se ejecute correctamente.

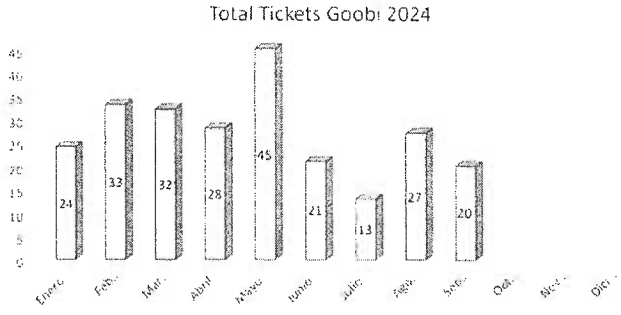




Se continúa diligenciando correctamente la bitácora de cambios y versionamiento a los sistemas de información en el Plan de Mantenimiento y Monitoreo 20224, de igual manera se lleva un control estricto debidamente documentado en los formatos de estadísticas de tickets en Excel y consecuentes informes de supervisión, como se muestra en las siguientes imágenes:



ESTADÍSTICAS GOOBI – 2024

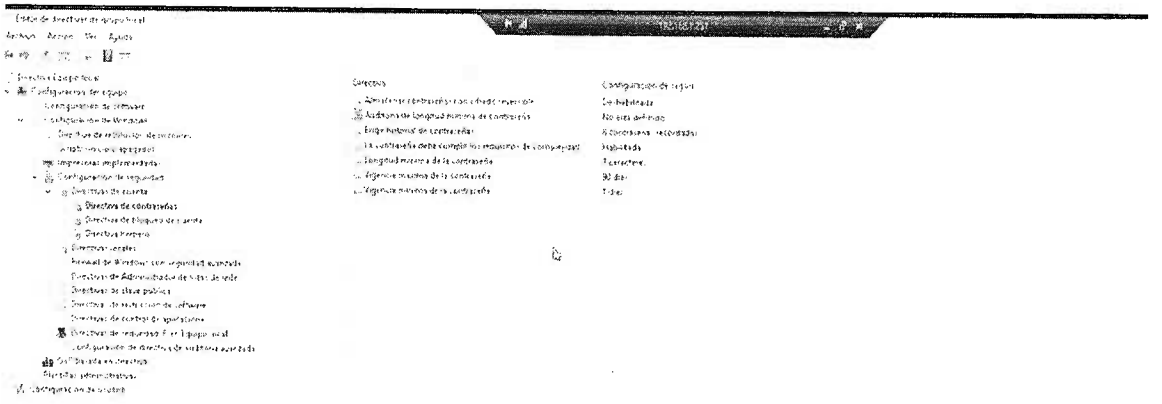


Mes	Total Ticket	Trimestre	
Enero	24		
Febrero	33		
Marzo	32	I	89
Abril	28		
Mayo	45		
Junio	21	II	94
Julio	13		
Agosto	27		
Septiembre	20	IV	60
Octubre			
Noviembre			
Diciembre		V	0
TOTAL	243		243

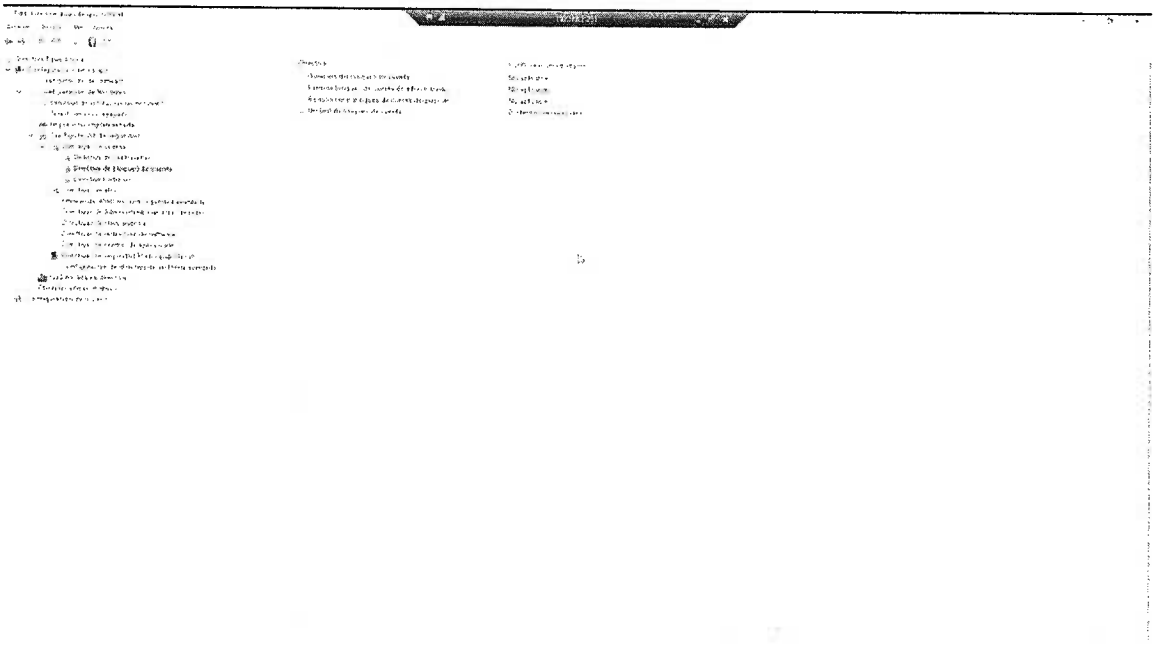
Se recomienda aprovechar la coyuntura de cambio en la herramienta de mesa de ayuda e incluir que la Gestión de control de cambios a nivel de hardware y software se realice en esta herramienta.

5.2.6. Gestión de accesos

👍 La configuración de seguridad de directivas de cuentas/contraseñas se encuentra correctamente configurada, como se evidencia a continuación:



Aún no se tiene implementada la directiva de bloqueo, la cual permitiría tener un control sobre los accesos fallidos y evitar ataques automatizados de fuerza bruta.



No se ha documentado el catálogo de servicios conforme al instrumento de Mintic, Anexo 1. Herramienta para la construcción del PETI.xlsx sesiones 3 y 5, que es el insumo para definir la gestión de accesos de la entidad.

- Para los servicios de página web y micrositios, aun no se ha implementado del cambio periódico obligatorio ni doble factor de autenticación de contraseñas.
- No se evidencian avances en los procedimientos de gestión de accesos, se recomienda hacer un mapeo de la documentación, revisar los instrumentos que se han elaborado y validar la pertinencia de integrarlos o actualizarlos.
- Actualmente, la Entidad no cuenta con una estrategia automatizada para el control de los usuarios administradores locales en los equipos de cómputo. Aunque se ha deshabilitado el usuario predeterminado "Administrador" y se utiliza un usuario denominado "admin", el proceso de gestión, control y cambio periódico de estas contraseñas se realiza de forma manual.
- Aunque el IDEP no desarrolle software se deben definir e implementar controles de acceso al código fuente del portal Web y de los micrositios.

5.2.7. Recomendaciones

N°.	Recomendación 2024
7.	Asegurar que el nuevo firewall o equipo de seguridad perimetral cuente con licencias activas, actualizaciones automáticas y soporte técnico. Incluir configuraciones avanzadas para seguridad perimetral, como inspección profunda de paquetes, prevención de intrusiones (IPS) y control de aplicaciones.
8.	Incluir en el plan de transferencia de conocimiento formación sobre la operación, monitoreo e interpretación de alertas del nuevo firewall.
9.	Segmentar el tráfico en diferentes VLAN's según criterios como función (usuarios, servidores, dispositivos IoT), ubicación geográfica o nivel de acceso. Esto reducirá el tamaño del dominio de broadcast y permitirá un mejor control del tráfico.
10.	Integración del firewall con endpoints: Sincronizar el firewall con las estaciones finales para detectar y mitigar posibles amenazas internas en tiempo real.
11.	Seguridad inter-VLAN: Configurar reglas estrictas de acceso entre VLAN's y establecer listas de control de acceso (ACLs) para restringir el tráfico innecesario. Establecer reglas en los switches o routers para limitar el tráfico entre segmentos de red, permitiendo solo las comunicaciones estrictamente necesarias.
12.	Garantizar que en la ejecución del plan de reestructuración de la arquitectura de red se utilice el modelo jerárquico planteado con separación entre capas de acceso, distribución y núcleo para mejorar la escalabilidad y la resiliencia.
13.	Configurar contraseñas seguras y personalizadas en todos los dispositivos de red. Deshabilitar las cuentas predeterminadas en elementos de red activos y limitar el acceso solo a usuarios autorizados. Usar métodos de autenticación multifactor (MFA) para accesos administrativos a consolas y elementos activos de red que lo permita
14.	Asegurar la sincronización completa entre el directorio activo y las cuentas de correo mediante la implementación de Microsoft 365
15.	Actualizar las políticas de seguridad para reflejar las configuraciones nuevas y alinearlas con la implementación del MSPI.
16.	Implementar soluciones que permitan monitorear el estado de los dispositivos y el tráfico de

N°.	Recomendación 2024
	red para identificar puntos de fallo o vulnerabilidades. Configurar alertas específicas para eventos críticos, como intentos de acceso no autorizados o tráfico inusual en la red.
17.	Realizar talleres sobre las nuevas políticas y mejores prácticas de seguridad para todos los empleados. Realizar evaluaciones independientes periódicas para verificar el cumplimiento de los controles y la efectividad de las nuevas medidas implementadas.
18.	Implementar un Sistema de Control de Navegación estricto en la implementación del nuevo firewall y antivirus: Restringir accesos a sitios no autorizados o peligrosos. Monitorear y registrar actividades de navegación.
19.	Configurar restricciones más robustas para evitar descargas y ejecución de software portable. Implementar soluciones como AppLocker o políticas de listas blancas para permitir solo software aprobado.
20.	Implementar herramientas para el monitoreo continuo del estado de la red, evaluar la posibilidad de implementar soluciones SIEM y realizar análisis regulares de vulnerabilidades y ejecutar planes de remediación basados en los resultados.
21.	Implementar políticas que estipulen el uso obligatorio de encriptación para medios de almacenamiento portátiles y que se establezcan procedimientos claros para proteger la información clasificada, a fin de reducir la vulnerabilidad ante incidentes de seguridad.
22.	Garantizar que, en la configuración del almacenamiento en la nube dispuesto para la entidad, se realice una depuración de los permisos asignados a los usuarios en las carpetas compartidas. Asimismo, se debe verificar los grupos a los que pertenecen dichos usuarios, con el fin de evitar que puedan acceder a información que no les corresponde.
23.	Integrar el Manual MN-GT-12-16 al plan de contingencia institucional para garantizar continuidad operativa en emergencias.
24.	Extender la autenticación multifactor a los otros servicios y sistemas de información de la Entidad.
25.	Implementar una rutina automatizada que notifique periódicamente sobre usuarios inactivos o con permisos no utilizados, para asegurar la eficiencia en la gestión de accesos en los sistemas de información y aplicativos de la Entidad
26.	Aprovechar el cambio en la herramienta de mesa de ayuda para incorporar funcionalidades de control de cambios a nivel de hardware y software. Esto permitirá centralizar la trazabilidad y documentación de cambios, mejorando la gestión de riesgos asociados.
27.	Implementar una política de bloqueo de cuentas tras un número determinado de intentos fallidos. Configurar notificaciones para administradores en caso de bloqueos recurrentes, lo que ayudará a detectar posibles ataques de fuerza bruta.
28.	Completar la documentación del catálogo de servicios según los lineamientos del MinTIC (instrumento PETI, Anexo 1). Este catálogo debe servir como insumo para definir y estructurar la gestión de accesos de manera integral y alineada con los objetivos de la entidad.
29.	Realizar un mapeo completo de la documentación y recursos compartidos existentes, identificando vacíos o inconsistencias. Actualizar los procedimientos de gestión de accesos alineándolos con los controles del MSPI.
30.	Implementar herramientas de gestión centralizada para usuarios administradores locales, como Microsoft LAPS (Local Administrator Password Solution) u otras soluciones similares, que permitan la rotación y gestión segura de contraseñas administrativas locales. Establecer una política formal para la rotación periódica de contraseñas administrativas, minimizando los riesgos asociados a una gestión manual.

N°.	Recomendación 2024
31.	Definir e implementar controles de acceso al código fuente del portal web y micrositios, incluso si el IDEP no desarrolla software. Esto incluye: Gestión de permisos para repositorios de código, doble factor de autenticación para usuarios con acceso al código, monitoreo y auditoría de accesos a repositorios.

5.3. Procedimientos de Backup y Recuperación

Aunque en el inventario de activos de información contempla aspectos relacionados con los backups, aún no se cuenta con un formato de Plan de Backup's unificado que permita, en un único documento, identificar de forma rápida y clara todos los objetos a los que se les está generando copias de seguridad, sus frecuencias, tiempos de retención, responsables y disposición final de todas las copias de seguridad de la información respaldada, para así poder recuperarla de forma ágil y oportuna, como se había recomendado en el informe de la auditoria anterior. En la siguiente imagen se muestra nuevamente un ejemplo de lo cómo debería ser este formato:

N°	Información a respaldar	Detalles del respaldo	Responsable	Herramienta utilizada	Frecuencia/ Hora de Ejecución	Retención Inicial	Medio Inicial/ruta	Retención Final	Medio final/ruta	Ubicación custodia alterna	Evidencia de ejecución	Evidencia de No Conformidad y acción correctiva	Evidencia de prueba restauración	Procedimiento relacionado
Explicación	Indique el tipo de información a respaldar de acuerdo a lo establecido en DS-GER-015	Explique el propósito del respaldo y en que consiste	Funcionario responsable de ejecución, verificación, acciones correctivas y pruebas	herramienta de backup utilizada	frecuencia de ejecución acordada con los propietarios de la información cuando aplique	tiempo de retención en el primer medio de backup	ruta y/o medio donde se almacena el primer backup	Tiempo de Retención cuando se lleva a custodia alterna	ruta y/o Medio de Retención cuando se lleva a custodia alterna	Ubicación fuera de las instalaciones	en que archivos y ubicación se almacenan los logs de la ejecución	en que archivos y ubicación se almacenan las evidencias de acciones correctivas frente a logs fallidos o errores en pruebas de restauración	fecha y evidencia de las pruebas de restauración periódicas y efectivas	Nombre del procedimiento SIG relacionado

Se han evaluado diferentes herramientas automatizadas para implementar un sistema centralizado y estandarizado de administración de copias de seguridad. No obstante, aún no se ha tomado una decisión definitiva respecto a la adquisición de alguna de las opciones analizadas. Debido a esta situación, el proceso de generación de copias de seguridad continúa dependiendo, en su mayor parte, de métodos manuales, tales como:

- **Ejecución de scripts personalizados:** Los cuales requieren supervisión constante.
- **Copias manuales de información:** Realizadas por funcionarios y/o contratistas de la Oficina de Administración de Proyectos (OAP).

Lo situación anterior implica:

- **Mayor tiempo de dedicación:** Se debe invertir un tiempo considerable en actividades repetitivas, reduciendo su capacidad para atender otras tareas prioritarias.
- **Alta probabilidad de errores humanos**: La dependencia de procesos manuales aumenta el riesgo de omisiones, inconsistencias o fallos en la ejecución, lo que puede comprometer la integridad de las copias de seguridad
- **Falta de estandarización:** Al no contar con un sistema centralizado, las copias de seguridad pueden no estar organizadas ni gestionadas de manera uniforme, dificultando la **recuperación en caso de contingencias.**

- **Riesgos en la continuidad del negocio**: La ausencia de un sistema automatizado y confiable puede derivar en la pérdida de información crítica, afectando significativamente la operación de la Entidad.

Es fundamental considerar que, durante el periodo de implementación del nuevo firewall y antivirus, la entidad enfrenta una mayor exposición a posibles ataques de ransomware. Esta situación aumenta significativamente el riesgo de pérdida de información crítica, dado que las defensas actuales pueden no ser suficientes para prevenir este tipo de amenazas. Por lo tanto, se recomienda fortalecer de manera prioritaria la estrategia de copias de seguridad. Esto implica garantizar que las copias sean realizadas con regularidad, almacenadas en ubicaciones seguras (Nube, offline o en redes segmentadas), y sometidas a pruebas periódicas de restauración para asegurar su funcionalidad en caso de un incidente.

La adopción de una herramienta automatizada y la estandarización del proceso de copias de seguridad permitirá:

- ✓ Reducir significativamente el tiempo invertido por el personal en actividades operativas.
- ✓ Minimizar los riesgos asociados a errores humanos.
- ✓ Garantizar la protección y disponibilidad de la información crítica.
- ✓ Aumentar la capacidad de respuesta ante incidentes de pérdida de datos o ciberataques.

Además, es necesario revisar y mejorar las políticas de gestión de accesos, educación a los usuarios sobre ciberseguridad, y la implementación de medidas temporales que mitiguen los riesgos mientras se completan las implementaciones de seguridad planificadas.

Si bien las copias de seguridad se entregan para caja fuerte mediante una acta para su custodia, como ilustra en la imagen siguiente, aun no se ha documentado el procedimiento de almacenamiento alterno a los equipos de la Entidad, de los medios generados por las copias de seguridad, con disponibilidad permanente y sin restricciones geográficas. Cabe anotar que se envía una copia del disco backup al igual que los discos históricos a la caja fuerte en el Archivo Central del IDEP ubicado en la Secretaría de Educación, las llaves el ingreso a esta caja fuerte se encuentra a cargo de Gestión Tecnológica por esta razón no hay un memorando del envío de estos discos.

ACTA No. 225

CUSTODIA DE BACKUPS EN LA CAJA FUERTE

En Bogotá el día 01 del mes de noviembre del 2024, se reunieron los funcionarios Nelson Ricardo Corredor Cruz, Tesorero General del IDEP y César Alonso Linares Peña, Técnico Operativo de la Oficina Asesora de Planeación, en acuerdo con el funcionario que tiene a su cargo la Caja Fuerte decidimos que se guardaría el disco duro de backups así:

Se retira el disco duro interno DISCO BACKUP UNO con el fin de realizar el próximo Backup semanal.

Se aclara que este disco duro se entregará para su custodia al Tesorero de la entidad quien lo resguardará en la caja fuerte del Instituto, en las siguientes condiciones:

- Sobre perfectamente sellado relacionando placa del disco No. R1821
- Disco en pleno funcionamiento
- Lugar de resguardo del disco en la caja fuerte será en lugar libre de riesgos de golpes, caídas no intencionales, etc., lugar que será definido por el Tesorero y avalado por el responsable del disco quien es el Técnico Operativo de la Oficina Asesora de Planeación.

Que para constancia se firma por los que en ella intervinieron, a los 01 días del mes de noviembre del 2024

NELSON RICARDO CORREDOR CRUZ
Tesorero General

CÉSAR ALONSO LINARES PEÑA
Técnico Operativo - OAP

No se tiene un procedimiento formal de pruebas de restauración donde se establezca la periodicidad, el tipo de pruebas a realizar y los resultados.

5.3.1. Recomendaciones

N°.	Recomendación 2024
32.	Priorizar la adquisición e implementación de una herramienta automatizada para la gestión de copias de seguridad que cumpla con las recomendaciones emitidas por la auditoria. Asegurarse de realizar pruebas piloto para evaluar su funcionalidad antes de la implementación total.
33.	Desarrollar un formato único detallado para el Plan de Copias de Seguridad, que incluya: ✓ Identificación de la información respaldada: Listado completo de los objetos respaldados. ✓ Frecuencia y retención: Detalles sobre la frecuencia de las copias y tiempos de retención. ✓ Ubicación de backups y logs: Especificación de las ubicaciones de las copias y los archivos de logs. ✓ Permisos de acceso y seguridad: Información sobre los accesos y la seguridad de las copias. ✓ Formatos de novedades y restauraciones aleatorias: Documentación de incidentes y validación de la efectividad de los backups mediante restauraciones aleatorias. Este formato debe ser independiente del software de backup, proporcionando una visión integral y alineada con el control 12.3 del MSPI. Establecer una política para revisar y actualizar el Plan de Backups al menos una vez al año o tras cambios significativos en la infraestructura tecnológica.
34.	Desarrollar la documentación del procedimiento de almacenamiento alterno: Redactar un

N°.	Recomendación 2024
	procedimiento que contemple: ✓ Movilización segura de medios físicos a ubicaciones fuera de las instalaciones principales. ✓ Uso de almacenamiento geográficamente distribuido (p. ej., almacenamiento en la nube). ✓ Métodos de recuperación rápida en caso de desastres que afecten múltiples ubicaciones.
35.	Crear el procedimiento de pruebas de restauración y formalizarlo, asegurando que el procedimiento incluya: ✓ Frecuencia de las pruebas: Realizarlas trimestralmente como mínimo. ✓ Alcance: Evaluar la restauración total y parcial de datos para asegurar la integridad y accesibilidad de los respaldos. ✓ Escenarios simulados: Probar restauraciones en escenarios de contingencia como fallos de servidores, ataques de ransomware o desastres naturales. ✓ Resultados documentados: Registrar los resultados de cada prueba, identificando errores y proponiendo mejoras para garantizar la funcionalidad del proceso de restauración. ✓ Capacitación en restauración: Entrenar al personal técnico en procedimientos de restauración para minimizar tiempos de respuesta ante incidentes reales.
36.	Revisar periódicamente las políticas y herramientas de respaldo implementadas ante la aparición de nuevas amenazas como ransomware más sofisticado o cambios en la regulación de protección de datos.

5.4. Mesa de ayuda

De acuerdo con las recomendaciones emitidas en los informes de auditoría de vigencias anteriores, y con base en las debilidades identificadas en el sistema de mesa de ayuda de la Entidad, se acogió la recomendación de implementar el sistema de gestión mesa de ayuda GLPI. el cual se encuentra al momento de la auditoria en proceso de implementación.

Como parte de este proceso, se realizó un diagnóstico detallado sobre la situación actual del servicio de mesa de ayuda, con el objetivo de:

- ✓ Evaluar las necesidades existentes: Identificar las áreas críticas que requieren optimización en el manejo de solicitudes y soporte técnico.
- ✓ Analizar los procesos operativos: Examinar la forma en que se gestiona actualmente la recepción, seguimiento y resolución de incidentes.
- ✓ Revisar los recursos disponibles: Determinar las capacidades tecnológicas y humanas necesarias para asegurar una implementación exitosa.

Como resultado de este informe se estableció el siguiente cronograma de implementación:

GLPI IDEP

CRONOGRAMA IMPLEMENTACION GLPI IDEP						
ITEM	ENTREGABLES	OCTUBRE	NOVIEMBRE	DICIEMBRE	ENERO	FEBRERO
1	Documento con el análisis y la documentación de los procesos actuales utilizados para la gestión de solicitudes e incidentes, identificando flujos de trabajo, con el fin de establecer una línea base para la parametrización del sistema de mesa de ayuda.					
2	Documento con el catálogo de servicios conforme a las necesidades actuales de la entidad, identificando y documentando los servicios ofrecidos, junto con sus correspondientes tipos de solicitudes e incidentes.					
3	Entrega de un ambiente no productivo del sistema de gestion de mesa de ayuda cumpliendo con los estandares de seguridad y desempeño requeridos, configurando la infraestructura necesaria, incluyendo bases de datos, servidores web y cualquier otro componente que garantice la operatividad del sistema.					
4	Ejecución de un plan de pruebas sobre el sistema, asegurando el correcto funcionamiento del sistema de gestion de mesa de ayuda, así como la implementacion del agente OCS para el control de inventario tecnologico de la entidad					
5	Entrega del sistema de gestion de mesa de ayuda en produccion de acuerdo a los estandares de seguridad establecidos					

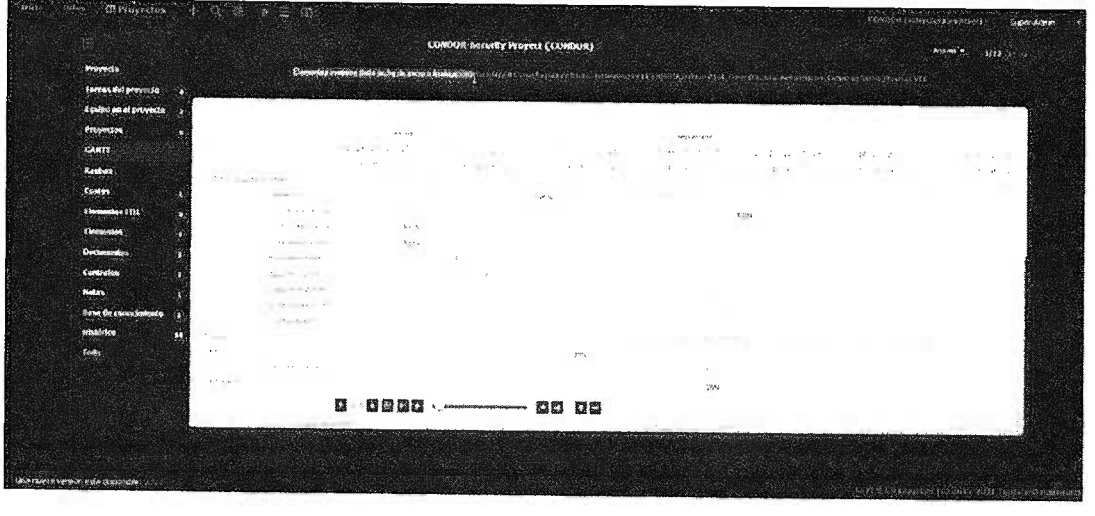
De acuerdo con lo anterior, en esta auditoría no se realiza una revisión específica del sistema de mesa de ayuda actual. Sin embargo, se enumeran las siguientes funcionalidades clave a tener en cuenta durante el proceso de implementación del sistema **GLPI**, basadas en los hallazgos y debilidades identificados en informes de auditorías previas. Estas funcionalidades se basan en los hallazgos y debilidades identificados en informes de auditorías previas y deben incluirse en una lista de verificación para la aceptación y puesta en producción del sistema.

Por lo tanto, se reitera la importancia de cumplir con las recomendaciones emitidas en auditorías anteriores para garantizar que el sistema GLPI incorpore las siguientes características esenciales:

- ✓ Que permita configurar horarios para el cálculo adecuado de los Acuerdos de Nivel de Servicio (ANS).
- ✓ Que permita configurar diferentes tipos de solicitudes hasta mínimo dos niveles jerárquicos: incidentes soporte, requerimientos de desarrollo, incidentes de seguridad, requisitos de adquisiciones de software o hardware, propuestas, etc.
- ✓ Que permita configurar diferentes agentes de atención externos e internos clasificados por Agentes internos TIC, Agentes internos de negocio, agentes externos proveedores.
- ✓ Que permita establecer ANS de acuerdo con la tipología de solicitudes y de agentes.
- ✓ Que permita una relación jerárquica entre solicitudes para aquellos casos en que una solicitud se segrega en varias tareas y de su cumplimiento dependa el estado de atención de la solicitud original.
- ✓ Que permita instalar un agente en los PC para que todas las solicitudes sean gestionadas por este medio con el fin de eliminar la carga operativa de la digitación de llamadas y correos y el riesgo de error humano. Adicionalmente la centralización de la información optimiza los tiempos de atención y la obtención de información estadística.
- ✓ Que permita generar reportes e indicadores de gestión.
- ✓ Que permita instalar agente de escaneo de red para llevar la trazabilidad entre solicitud, usuario y equipo
- ✓ Que permita adjuntar archivos tanto a la solicitud principal como a las tareas de la bitácora de atención.

- ✓ Que permita aplicar escalamientos.
- ✓ Que integre un inventario de hardware y software por medio de agente.

5.4.1. Recomendaciones

N°.	Recomendación 2024
37.	Asegurar que en la implementación del GLPI se incluyan la implementación de todas las características presentadas en este informe.
38.	Dejar la herramienta actual para consulta y descartar la migración. Esta recomendación se emite debido a las falencias y debilidades identificadas en la mesa de ayuda anterior, así como a la alta complejidad operativa que implica un proceso de migración desde dicha herramienta. Estas limitaciones podrían generar demoras significativas en la implementación del nuevo sistema de mesa de ayuda.
39.	Definir que los informes que necesite la entidad se generen automáticamente desde la herramienta y no se tengan que hacer procesos adicionales para obtener estadísticas e indicadores.
40.	Estructurar el catálogo de servicios, definiendo claramente los ANS para definir las métricas que se van a tener en cuenta
41.	Controlar el inventario de hardware y software a través de agentes establecidos en la herramienta y validar que estos agentes funcionen en las todos los dispositivos de la Entidad.
42.	Implementar el plan de mantenimiento preventivo en la herramienta GLPI, esto puede lograrse utilizando las funcionalidades de gestión de proyectos o gestión de contratos. Estas opciones permiten asociar tareas de mantenimiento a cualquier elemento del inventario y programarlas para fechas específicas. Además, con los complementos disponibles, es posible incluir cronogramas de tipo Gantt, lo que facilita el seguimiento y control de las actividades planificadas. A continuación, se presenta un ejemplo de un diagrama para un proyecto configurado en GLPI: 

6. CONCLUSIONES

En el marco de la evaluación realizada por la Oficina de Control Interno desde el año 2020, se evidencio de manera reiterativa, que la capacidad de los recursos humanos asignada a la función de tecnología resultaba insuficiente para atender la envergadura de los proyectos y actividades de operación tecnológica, al igual que la implementación de la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la información.

Por esta razón, si bien los recursos humanos demostraron en cada vigencia su compromiso con la entidad y con implementar buenas prácticas, los avances alcanzados no lograban la expectativa, especialmente en lo relacionado con la Gestión Estratégica de tecnología y el Gobierno TI.

Por esta razón, se identifica como una fortaleza que para la vigencia 2024, se evidenció la contratación de personal adicional y especializado para la OAP, lo que permite tener más nivelada la carga en las responsabilidades asignadas a esta oficina.

Sin embargo, dada la reciente vinculación de los nuevos colaboradores, se evidencian iniciativas y mejoras en el enfoque de abordaje, pero aún persisten las debilidades identificadas en vigencias anteriores. El nuevo equipo ha estado enfocado en el diagnóstico de la situación actual para desarrollar un plan de acción adecuado, lo que permitirá al IDEP actualizar su tecnología, desarrollar la Política de Gobierno Digital, e implementar prácticas de seguridad más robustas y eficientes

Evidencia del enfoque de adopción de mejores prácticas es el informe de diagnóstico de la situación actual de la mesa de ayuda que permitió establecer un plan de trabajo para implementar la herramienta de GLPI, con la cual se busca mejorar el servicio, la oportunidad de atención y medir eficazmente la gestión.

A su vez, se han adelantado los procesos contractuales de soluciones de seguridad perimetral que aportan herramientas para el establecimiento de controles.

Sin embargo, cabe resaltar que, en el proceso de transición de nuevas adquisiciones, la entidad está expuesta en la seguridad de la información dado que adolecen de la plataforma y controles necesarios para proteger la entidad, lo cual implica la urgencia de atender de manera prioritaria el riesgo latente.

El cuerpo del informe presenta las debilidades encontradas que soportan el riesgo latente reportado por la Oficina de control Interno.

Por esta razón, en el presente informe se pone de manifiesto que las debilidades persisten hasta tanto los planes de acción puedan ser implementados, pero resultan un insumo aportado por la oficina de control interno para establecer focos de atención y remediación a corto, mediano y largo plazo, que podrán ser evaluados en el marco del Plan de auditoría 2025.

	Nombre / Cargo	Firma
Aprobó	Yamile Morales Laverde – Jefe Oficina Control Interno	
Revisó	Yadira Velosa Poveda – Contratista	
Elaboró	Yadira Velosa Poveda - Contratista	
Los arriba firmantes declaramos que hemos revisado el presente documento y loencontramos ajustado a las normas y disposiciones legales y/o técnicas vigentes		