INFORME DE AUDITORÍA

PROCESO DE GESTIÓN TECNOLÓGICA

OFICINA DE CONTROL INTERNO

Angela Johanna Marquez Mora
JEFE DE LA OFICINA DE CONTROL INTERNO

EQUIPO AUDITOR
Luz Yadira Velosa Poveda
Jorge Javier Vidal Ortiz

PERIODO EVALUADO
11/10/2021 al 15/12/2021

FECHA DEL INFORME
27/12/2021

Contenido

1. INFORMACIÓN GENERAL

1.1. DESTINATARIOS DE LA AUDITORÍA

La presente auditoría tiene como destinatarios principales:

a) La Secretaria de Despacho, como Representante Legal de la Secretaría Distrital de la Mujer y responsable del Sistema de Control Interno.
b) La Jefa de la Oficina Asesora de Planeación, como Lideresa del Proceso de Gestión Tecnológica.

1.2. EQUIPO AUDITOR

El equipo auditor asignado para llevar a cabo la presente evaluación es el siguiente:

- Luz Yadira Velosa Poveda – Contratista Oficina de Control Interno.
- Jorge Javier Vidal Ortiz – Auxiliar Administrativo Oficina de Control Interno.

1.3. PERIODO DE DESARROLLO DEL TRABAJO DE AUDITORÍA

El trabajo de auditoría se desarrolló de conformidad con la metodología que se detalla en el numeral 5 del presente informe, iniciando con la etapa de planeación en el mes de octubre de 2021, donde se realizó la reunión de apertura de la auditoría el 22 de octubre de 2021, para proceder a la recopilación de información específica y el desarrollo de las pruebas de recorrido necesarias para sustentar las conclusiones de auditoría, y finalizando la misma con la reunión de cierre el día 20 de diciembre de 2021, y la entrega del informe final antes del 31 de diciembre de 2021.

2. OBJETIVO DE LA AUDITORÍA

Evaluar los controles generales de la función TIC y el estado de avance de la documentación del proceso de conformidad con el modelo de seguridad y privacidad de la información (MSPI), así como emitir recomendaciones de mejora.

3. ALCANCE DE LA AUDITORIA

La presente auditoría comprende la evaluación sobre la gestión de los controles generales del proceso de Gestión Tecnológica, específicamente en los siguientes aspectos:

- Verificar el estado de implementación del modelo de seguridad y privacidad de la información (MSPI),
- al proceso Gestión Tecnológica de la SDMujer.
- Verificar el estado de implementación de mecanismos de accesibilidad web, conforme a la norma técnica NTC 5854, al proceso Gestión Tecnológica de la SDMujer.
- Evaluar si los procesos de gobierno de TIC de la entidad apoyan las estrategias y los objetivos de la entidad.
- Realizar la evaluación independiente de la administración de riesgos del proceso de Gestión
- Tecnológica y proporcionar información sobre la eficiencia, efectividad e integridad de los controles tecnológicos según sea apropiado a las actividades de control específicas.

- Evaluar las prácticas de confiabilidad e integridad de la información de la Entidad.

4. CRITERIOS DE LA AUDITORIA

Se aplica como referente los lineamientos emitidos por el Ministerio de Tecnologías de la Información y Comunicaciones mediante el Manual para la Implementación de la Política de Gobierno Digital Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2) Versión 7 Abril de 2019. Lineamientos de la Norma internacional ISO/IEC 27001:2013 y las guías del Modelo de Seguridad y Privacidad de la Información, con derechos reservados por parte del Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la estrategia de Gobierno en Línea. Algunos lineamientos COBIT – Gobierno de TI, algunos lineamientos del marco de trabajo ITIL, y la Norma Técnica Colombiana (NTC) 5854 de accesibilidad a páginas web.

5. METODOLOGÍA

El presente ejercicio auditor se realizó en el marco de las normas de auditoria generalmente aceptadas en Colombia, el *"Estatuto de Auditoría para la Secretaría Distrital de la Mujer*" y los lineamientos proferidos desde el *"Código de Ética para el Ejercicio de Auditoría Interna"* aprobados por el Comité Institucional de Coordinación de Control Interno de la Secretaría Distrital de la Mujer.

Tipo de Auditoria:

El presente trabajo es una auditoría de Controles Generales, por lo anterior se aclara que 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 el proceso de gestión tecnológica para la gestión y operación de servicios tecnológicos sin condicionamiento de que dichos instrumentos o procedimientos sean documentos controlados del sistema de gestión.

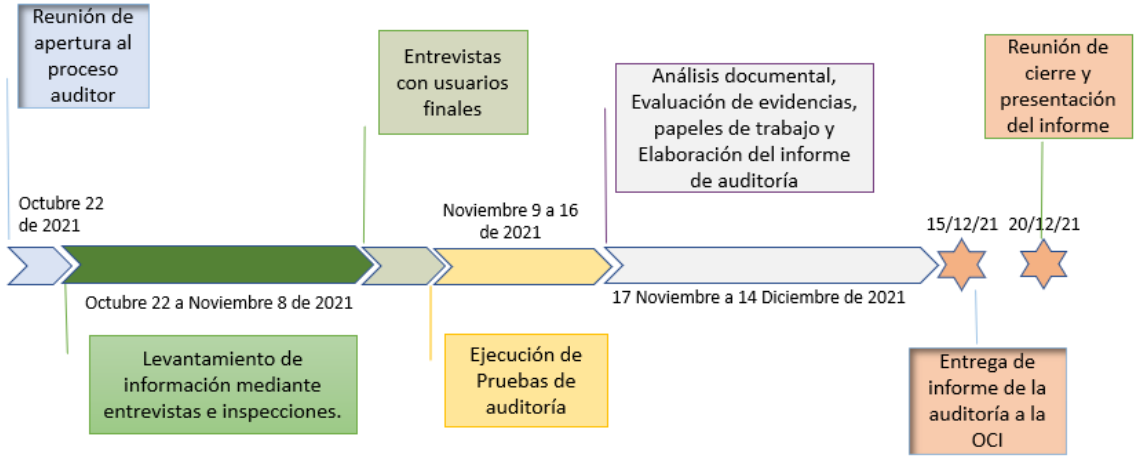
Planeación de la Auditoría:

Se adelantaron las siguientes actividades conforme al programa de auditoría acordado entre las partes en acta de apertura del 22 de octubre de 2021.

1. Entrevistas con los responsables de procesos, proyectos o gestión de activos TIC
2. Levantamiento de información documental como evidencia de planeación, ejecución, seguimiento y acciones de mejora
3. Inspección de configuración de activos de la plataforma TIC.
4. Ejecución de pruebas de Auditoría
5. Entrevistas con 4 usuarios finales para indagar percepción del servicio y seguridad.
6. Análisis de evidencias y elaboración de informe
7. Socialización de resultados.

Se presenta la línea de tiempo de la auditoría:

Grafica 1 Línea de tiempo de la auditoria



Fuente: Elaboración propia Acta de apertura de la Auditoria

Se acuerda con el proceso auditado el cronograma de sesiones de levantamiento de información e inspecciones

Grafica 2 Programa de sesiones de auditoria

ACTIVIDAD DE AUDITORÍA	INTERLOCUTOR	HORA	CRONOGRAMA
			Mes 1 OCTUBRE: 21 | 22 | 25 | 26 | 27 | 28 | 29 — Mes 2 NOVIEMBRE: 2 | 3 | 4 | 5 | 8 | 9 | 10 | 11 | 12 | 16 | 17 | …
Sesiones de levantamiento de información y entrevistas con el proceso auditado, temas:			
- Planeación Estratégica de TI (PETI). (7 Dominios), indicadores e informes.	Andrés Cadena Gleidy Jerez Miguel Bernal Nicolas Rey Alejandro Mayorga Jerson Murillo	8:00 am	4
- Organización de Funciones y Comunicación: Colaboradores internos, terceros, seguridad de recurso humano.			2
- Plan de Administración de Riesgos y Contingencias. - Activos de Información -Plan de Continuidad.	Andrés Cadena	8:00 am	4
Implementación del Modelo de Seguridad y Privacidad de la Información: Política de Seguridad (MSPI): Declaración de aplicabilidad, política, manual, plan MSPI	Andrés Cadena	3.00 pm	2
Implementación del Modelo de Seguridad y Privacidad de la Información: Política de Seguridad (MSPI): Procedimientos, guías, formatos e instructivos.	Andrés Cadena	2.00 pm	4
Desarrollo y Adquisición de Sistemas de información: Gestión de proveedores de sistemas de Información, Metodologías de desarrollo de software interno y/o por encargo a terceros, Administración de Requerimientos, desarrollo, pruebas, aceptación y despliegue, Licenciamiento y propiedad intelectual.	Gleidy Jerez	9.00 am	3
Seguridad de la Red. Seguridad de Aplicativos y bases de datos, Seguridad de Archivos Fuentes y Documentos, Seguridad de Servicios de Correo e Internet y Acceso de Terceros.	Miguel Bernal	2.00 pm	3
Adquisición y Actualización – Gestión de Cambios. Mantenimiento de Hardware y Software.	Gleidy Jerez	2:00 pm	3
Mesa de Servicio.	Miguel Bernal	2.00 pm	3
Implementación de mecanismos de accesibilidad web, conforme a la norma técnica NTC 5854.	Nicolas Rey	2.00 pm	3
Seguridad Física	Miguel Bernal	9:00 am	2
Entrevista a usuarios (5)			2 | 2 | 1

Fuente: Elaboración propia Acta de apertura de la Auditoria

Desarrollo de la Auditoria:

La auditoría se ejecutó conforme al programa acordado entre las partes, ejecutando las siguientes actividades:

- Se establecieron las siguientes sesiones de levantamiento de información y verificación de controles con los interlocutores de la Oficina Asesora de Planeación:

Tabla 1 Lista de sesiones de levantamiento de información

Sesión	Fecha y hora
Sesión N°1 MSPI - Auditoría Gestión TIC	viernes 22/10/2021 3:00 p. m.
Sesión 2. Desarrollo y Adquisición de Sistemas de información	lunes 25/10/2021 9:00 a. m.
Sesión 3. Adquisición y Actualización, Gestión de Cambios, Mantenimiento de Hardware y Software	lunes 25/10/2021 2:00 p. m.
Sesión 4. Implementación de mecanismos de accesibilidad web	martes 26/10/2021 2:00 p. m.
Sesión 5. Planeación Estratégica de TI, Organización TIC	miércoles 27/10/2021 8:00 a. m.
Sesión 6. Riesgos, activos y continuidad	jueves 28/10/2021 8:00 a. m.
Sesión 7. Mesa de Servicio	jueves 28/10/2021 2:30 p. m.
Sesión 8. Seguridad Física	viernes 29/10/2021 9:00 a. m.
Sesión 9. MSPI – instrumentos	viernes 29/10/2021 2:30 p. m.
Sesión 10. Controles de seguridad	martes 2/11/2021 2:00 p. m.

Fuente: Elaboración propia.

- Se revisaron los controles generales de los escenarios planteados en el alcance, junto con la revisión de la configuración de controles en la plataforma tecnológica de la Secretaría Distrital de la Mujer.
- La visita al centro de cómputo se realizó el día 29 de octubre de 2021
- El área que suministro la información es la Oficina Asesora de Planeación responsable del Proceso Gestión Tecnológica.
- Se adelantaron entrevistas con 4 usuarios de servicios TIC con el fin de identificar la percepción del servicio de mesa de ayuda, conocimiento de políticas de seguridad y gestión de contraseñas a servicios.

Tabla 2 Lista de entrevistas con áreas usuarias

Sesión	Fecha y hora
Talento Humano	10/11/21
Gestión Documental	5/11/21
Gestión de conocimiento	4/11/21
Gestión del Conocimiento – Desarrollo	8/11/21

Fuente: Elaboración propia.

- Se desarrollaron pruebas básicas de seguridad de manera remota y presencial, e los capítulos correspondientes a pruebas de seguridad técnicas se incluyen imágenes de evidencia.

Como última etapa, con la información identificada y consolidada a lo largo del proceso auditor se construye el informe de auditoría el cual se da a conocer en la reunión de cierre y es enviado a quien lidera el área y proceso auditado. Las conclusiones del informe de auditoría se describen a través de fortalezas y debilidades; estas últimas que a su vez están compuestas por dos tipos, las oportunidades de mejora y los hallazgos, cuyas definiciones se detallan a continuación:

- **Oportunidad de mejora**: Hace referencia a la identificación de temas problemáticos y mejoras potenciales sobre una situación específica identificada a lo largo del proceso auditor con su respectiva recomendación. Dicha situación puede llegar a ser reiterativa y podría llegar a tener efectos sobre el cumplimiento de los objetivos de los procesos institucionales, por lo que es necesario identificarlas, analizarlas y tomar decisiones sobre su tratamiento.

- **Hallazgo de auditoría**: Es un hecho relevante que se constituye en un resultado determinante en la evaluación de un proceso o un asunto en particular, al realizar la comparación de La Condición (situación detectada o hechos identificados) con El Criterio que se refiere al deber ser (cumplimiento de normas, reglamentos, lineamientos o procedimientos); y además para mayor claridad se complementa estableciendo sus Causas (qué originó la diferencia encontrada) y Efectos (situaciones adversas que pueden ocasionar la diferencia encontrada). Los hallazgos deben ser objeto de formulación de acciones tendientes a eliminar de fondo las causas que las originaron, las cuales harán parte del correspondiente plan de mejoramiento.

  Para efectos visuales, en el presente informe se utiliza la siguiente nomenclatura:

   Fortaleza.

   Oportunidad de mejora.

   Oportunidad de mejora con atención prioritaria.

A su vez las recomendaciones corresponden a las oportunidades de mejora que deben ser atendidas por la OAP en respuesta a los resultados negativos o debilidades identificados en el ejercicio de la auditoría y que son la fuente para determinar y priorizar las acciones del Plan de Mejoramiento. Vale aclarar que los hallazgos positivos no derivan en recomendaciones.

Es de aclarar que el término "**Plan de Mejoramiento**" hace referencia al instrumento que recoge y articula todas las acciones prioritarias que se emprenderán para mejorar aquellas características que tendrán mayor impacto en los resultados esperados, el logro de los objetivos de la entidad y la ejecución del plan de acción institucional. Su objetivo primordial es promover que la gestión de la entidad se desarrolle en forma eficiente y transparente, a través de la adopción y cumplimiento de las acciones correctivas y/o de la implementación de metodologías orientadas al mejoramiento continuo.

6. DESARROLLO DEL EJERCICIO AUDITOR

6.1. GESTIÓN Y GOBIERNO DE TECNOLOGIA

6.1.1. GESTIÓN ESTRATÉGICA DE TI

6.1.1.1. FORTALEZAS Y OPORTUNIDADES DE MEJORA

Es de anotar que el Plan Estratégico de Tecnologías de la Información y las Comunicaciones– PETI, debe hacer parte integral del Plan de Acción de la entidad, conforme al Decreto 612 de 2018 (Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado), por lo cual, se espera que esté articulado con los demás planes de la entidad y en especial con sus objetivos

institucionales, para que las acciones del PETI fortalezcan las dimensiones y políticas del Modelo Integrado de Planeación y Gestión – MIPG sobre las cuales puede tener injerencia.

Con este propósito entre otros, el MINTIC emitió en julio de 2019 nuevas directrices en la *G.ES.06 Guía para la construcción del PETI versión 2*, que incorpora una metodología y se actualiza el contenido para la construcción del PETI con un enfoque de Arquitectura en la planeación de la Tecnología para la Transformación Digital. Es importante anotar que las 4 fases involucran a todas las áreas de la entidad como parte de la articulación del PETI.

- Así las cosas, para la construcción del documento "*Plan Estratégico de TI - PETI 2020-2024.pdf*", estructurado y presentado por la Oficina Asesora de Planeación con vigencia 2020 a 2024 publicado en la página de la entidad, se han aplicado en gran medida estas nuevas directrices, los interlocutores del proceso de gestión TIC, manifiestan que se planea finalizar la actualización y articulación en el año 2022.

Con respecto al avance en las siguientes 4 fases establecidas en la Guía 6 se emiten las observaciones:

Imagen 1 Fases para la construcción del PETI

Fuente: Elaboración propia basada en la Guía 6 Mintic

- Se ha involucrado correctamente a las siguientes áreas de la entidad, pero al registrar los nombres propios no se indica a que área corresponde, ya que, si bien es importante señalar a los participantes, es recomendable relacionar el área para efectos de rotación de representantes.
    - Planeación
    - Tecnologías de la Información
    - Áreas Misionales

- Atención al Ciudadano
- Dirección de Gestión Administrativa y Financiera
- Secretaría General (Representante legal)
- Oficina de control interno
- Áreas de apoyo

👍 Se identificaron correctamente las metas y objetivos de las áreas para discriminar la estrategia de la organización.

👍 En la sesión 3 se identificaron correctamente los servicios de la entidad incluyendo los servicios tecnológicos prestados por la función tecnológica de la OAP. La lista de servicios es consecuente con los servicios tecnológicos declarados en el PETI. Puede mejorarse diligenciando completamente todos los atributos para que la calificación de la sesión 5 sea más exacta.

👍 En la sesión 4 están identificadas las capacidades de la entidad y su relación con los recursos tecnológicos que la soportan. Este articulado con el PETI en el aparte "**Alineación de TI con los Procesos – Áreas**" donde se relacionan los recursos tecnológicos que apoyan cada proceso y las oportunidades de mejora.

👍 La sesión 5 arroja el listado de servicios de mayor impacto de acuerdo con los valores diligenciados en la sesión 3. El resultado arroja los siguientes de mayor impacto sobre 30 puntos.

- PAGINA WEB
- INVESTIGACIÓN DE CONDUCTAS PRESUNTAMENTE DISCIPLINABLES DE LAS SERVIDORAS Y LOS SERVIDORES DE LA SDMUJER.
- REVISAR Y BRINDAR ACOMÁÑAMIENTO EN LA ESTRUCTURACIÓN DE LOS ESTUDIOS PREVIOS
- TRAMITAR LAS MODIFICACIONES CONTRACTUALES
- TRAMITAR LOS PROCESOS Y CONTRATOS A TRAVES DE LAS PLATAFORMAS DISPUESTAS POR LA NORMATIVIDAD COLOMBIANA
- GESTIONAR LOS PAGOS A CARGO DE LA ENTIDAD
- RADICAR LA CORRESPONDENCIA EN ORFEO
- PETICIONES Y CONCEPTOS JURÍDICOS
- REVISIÓN DE PROYECTOS DE NORMA
- DEFENSA JUDICIAL
- LLEVAR SEGUNDA INSTANCIA DE LOS PROCESOS DISCIPLINARIOS
- NOTIFICACIONES DE ACTOS ADMINISTRATIVOS EXPEDIDOS POR LA SDMUJER
- ATENCIÓN SOCIOJURIDICA

👍 La sesión 6 arroja el resultado del análisis DOFA, en el cual se identifican principalmente debilidades de los sistemas de información o servicios tecnológicos, requisitos de capacitación, la necesidad de contar con un sistema de contratación, de autoservicios para certificaciones de contratos y no estar preparados para afrontar la interoperabilidad con otras entidades. Se identifican igualmente fortalezas, oportunidades y amenazas.

👉 El proceso de Gestión Tecnológica aporto algunos elementos al análisis DOFA, pero puede mejorarse incluyendo elementos tales como: los resultados de estadísticas de mesa de ayuda que evidencien incidentes que se convierten en problemas y las debilidades asociadas a seguridad de la información por adolecer de un Firewall al momento de la auditoría.

👍 La sesión 7 fue atendida correctamente en cuanto a la normatividad aplicable y los factores externos que afectan positiva y negativamente la entidad

👉 El instrumento ha sido diligenciado solo hasta la fase 2, sesión 8 Caracterización de Usuarios, por lo tanto, no aporta todos los elementos para la construcción de la estrategia de TI y construcción del PETI y la hoja de ruta de proyectos con el nuevo modelo de la Guía 6 Mintic. Vale aclarar que esto no fue impedimento para la construcción del PETI con el que cuenta la entidad, solamente que debe ser actualizado a 2022 con las nuevas directrices.

Vale aclarar que el avance en el instrumento aporta elementos de evidencia de el involucramiento de las áreas en la construcción del PETI, ya que este no es responsabilidad única de la gestión tecnológica.

Con respecto al documento "*Plan Estratégico de TI - PETI 2020-2024.pdf*", se emiten las siguientes observaciones

👉 De manera complementaria se han diligenciado los instrumentos del MODELO DE GESTIÓN IT4+, para obtener un análisis de brecha de los 6 dominios de la anterior versión del Marco de Referencia de arquitectura empresarial, el cual fue actualizado al 31/10/2019 incluyendo el dominio de seguridad. Sin embargo, resulta útil dado que la medición de brecha del MSPI se construye con el instrumento de autodiagnóstico MSPI dispuesto por Mintic.

Imagen 2 Dominios MRAE

Fuente: Elaboración propia basada en MAE.G.GEN.01 Mintic

👉 Se cuenta con el procedimiento GT-PR-11 ACTUALIZACIÓN DEL PLAN ESTRATÉGICO PETI, que en

términos generales establece los pasos para su construcción, sin embargo no está totalmente articulado con las 4 fases Guía 6 MinTic, no hace referencia a los 7 dominios del MRAE y no menciona actividades de seguimiento al cumplimiento de la hoja de ruta de proyectos vigencia anterior, medición por indicadores y como insumos para cada actualización anual con los componentes de mejora continua como resultado de la retrospectiva.

👍 En el enfoque estratégico se incluye correctamente: los objetivos estratégicos de la entidad, "Alineación de TI con los Procesos – Áreas" donde se relacionan los recursos tecnológicos que apoyan cada proceso y las Tendencias Tecnológicas, como elemento de insumo de "oportunidades" para el análisis DOFA

👉 En el dominio de servicios tecnológicos se incluye correctamente el listado que es consecuente con el instrumento del PETI, sin embargo se afirma que: "….se garantiza que los requerimientos de servicios de TI de los usuarios son atendidos bajo unos protocolos de servicios claros relacionados con la disponibilidad, seguridad y oportunidad", lo cual no es del todo preciso dadas las debilidades en materia de controles de seguridad expuestos en el numeral 6.2.2. de este informe.

👍 Se desarrolla correctamente el dominio de sistemas de información y su mantenimiento, se incluyen las fichas de caracterización, el ciclo de vida de los sistemas de información y su gestión de soporte.

👍 Se desarrolla correctamente la descriptiva de infraestructura tecnológica y arquitectura. Tienen correctamente implementado el IPV6.

👉 El dominio de información se refiere a iniciativas relacionadas con: Herramientas de análisis tales como bodegas de datos, herramientas de inteligencia de negocios y modelos de análisis, y describe las siguientes 4 iniciativas, pero esto no se refleja en los proyectos efectivamente adelantados por el proceso de gestión de tecnología, pese a que si están relacionados con proyectos declarados en la hoja de ruta:

- 1. Gobierno de datos
- 2. Ecosistemas para análisis de datos
- 3. Interoperabilidad de datos
- 4. Desarrollo de capacidades para el personal técnico y usuarios

👉 Pese a que el PETI hace referencia a la trasformación digital como elemento relevante, todavía no se han abordado proyectos concretos de esta naturaleza. La OAP manifiesta que "gestión del Conocimiento" es el responsable de establecer los proyectos asociados con analítica de datos e inteligencia artificiar y/o Machine Learning. Esto es válido desde el punto de vista de articulación de los proyectos, pero en todo caso el proceso de Gestión Tecnológica es el articulador y administrador de la plataforma tecnológica que soporte estos proyectos y en todo caso debe ser receptor de la trasferencia de conocimiento tecnológica para generar autonomía en la Secretaría de la Mujer en la evolución y adaptación de la plataforma a nuevos retos del Conpes 3975 que Define la Política Nacional de Transformación Digital e Inteligencia Artificial.

👍 El dominio de uso y apropiación se describe de manera correcta y se relacionan las capacitaciones impartidas por la OAP. A su vez, el PLAN INSTITUCIONAL DE FORMACIÓN Y CAPACITACIÓN relaciona correctamente el eje de trasformación digital, e incluye eventos en el plan de acción, igualmente se incluye la Socialización de la política de seguridad de la información y protección de datos. En la práctica no hay un plan de capacitaciones formal, pero se han construido correctamente componentes de autoaprendizaje tales como videos que ilustran el uso de sistemas de información. Se lleva un plan básico de capacitación al que se hace seguimiento:

Imagen 3

Id	Temática	Nombre	Objetivo	Evidencia	Grupo de impacto	encargado	CRONOGRAMA DE CAPACITACIÓN 2021						
							junio	julio	agosto	septiembre	octubre	noviembre	diciembre
1	Herramientas colaborativas	Apropiación herramienta Colaborativas Microsoft 365	Reforzar conocimientos manejo y uso adecuado de las herramientas.	Lista de asistencia	Nivel Directivo, funcionarias(0s) y/o Contratistas	miguel				x			
2	Sensibilización en seguridad de la información	Divulgación y sensibilización en temas de seguridad de la información	Sensibilizar a las funcionarias(os) y contratistas en temas de seguridad de la información	Lista de asistencia	Nivel Directivo, funcionarias(0s) y/o Contratistas	andres			x		x		
3	Mesa de Ayuda	Divulgación y sensibilización en la herramienta de mesa de ayuda.	Sensibilizar a las funcionarias(os) y contratistas en el uso y apropiación de la herramienta de solicitud de soporte de la entidad.	Lista de asistencia	funcionarias(0s) y/o Contratistas	angie		x					
4	Sistema de Gestión documental – Orfeo	Uso de la herramienta de gestión documental - Orfeo	Reforzar conocimiento en el uso de la herramienta y nuevas funcionalidades	Lista de asistencia	Nivel Directivo, funcionarias(0s) y/o Contratistas	Francisco	Evidencias de las capacitaciones Francisco Bravo						
5	Simisional	Uso de la herramienta misional de la entidad	Reforzar conocimiento en el uso de la herramienta y nuevas funcionalidades	Lista de asistencia	Nivel Directivo, funcionarias(0s) y/o Contratistas	Julian	Consultar con julian si ha realizado reinducción de SIMISIONAL						
6	PETI	Sensibilización del PETI	Sensibilizar a las funcionarias(os) y contratistas en la apropiación del PETI	Lista de asistencia	Funcionarias(0s) y/o Contratistas	Jerson				x		x	

El dominio de seguridad está declarado, sin embargo, los avances reportados no son del todo consecuentes con la implementación real de instrumentos y de controles en la plataforma tecnológica. Los resultados se presentan en el numeral 6.2 de este informe.

No existen Planes tácticos o cronogramas para los 16 proyectos declarados en el PETI, se evidencia que no existen instrumentos de planeación detallada, seguimiento al avance y control de calidad de los entregables de proyectos contra criterios de aceptación, que permitan alcanzar los objetivos para los cuales fueron identificados los proyectos y controlar la efectiva asignación de recursos a su implementación, logrando equilibrio entre valor ganado y la inversión. Adolecer de planeación de proyectos no solo impide controlar su avance, sino que limita la gestión de la capacidad instalada del recurso humano, al no contar con instrumentos de medición de esfuerzo para las tareas a cargo de cada colaborador.

Los siguientes son los proyectos declarados en el PETI y su estado de atención real, frente a los que se evidencia un bajo avance en su implementación con respecto a lo programado para la vigencia 2021. Las observaciones se emiten con base en las entrevistas con el área y con la publicación de avance del PETI a junio de 2021. (se resaltan en verde los proyectos que presentan avance a cargo de la OAP).

Tabla 3 Observaciones sobre proyectos PETI

Nombre Proyecto	Estado
Arquitectura Empresarial	El proyecto se proyectó para iniciar fase 1 en segundo semestre de 2021, pero no se ha abordado. La nueva estrategia de abordaje es contratar una persona especialista en el tema.
Construcción de la estrategia de Gobierno de TI	El proyecto se proyectó para iniciar fase 1 en segundo semestre de 2021, pero no se ha abordado. Se presenta una dependencia con el abordaje del proyecto de arquitectura empresarial.
Portafolio, programas y proyectos (PPTI).	Se está adelantando una solución en PHP para llevar el registro y seguimiento a las actividades de gestión de procesos inicialmente de adquisición, junto con la bitácora de tareas realizadas. Con rediseño puede ser adaptable a planeación y seguimiento a actividades de proyectos. Luego de esta tabla se emiten algunas observaciones de mejora

Nombre Proyecto	Estado
Expedientes y Documentos Electrónicos	El sponsor del proyecto es la Dirección Administrativa, lo cual se argumenta como justificación para no conocer el estado de avance e implementación. En las entrevistas con el personal de gestión tecnológica, no se tiene conocimiento del nivel de cumplimiento con el modelo de requisitos del Archivo Distrital para Sistema de Gestión de Documentos Electrónicos de Archivo. Es de anotar que los proyectos del PETI son aquellos que atienden entre otros a requerimientos de la entidad, pero la articulación tecnológica y de gestión de proyectos de TI para su atención corresponde a los responsables de tecnología. Sistemas ha apoyado en el desarrollo del FUID en apoyo a la gestión de inventarios físicos, pero la gestión y mantenimiento de Orfeo está bajo el control de la dirección administrativa.
Calidad de Datos	Se aplaza para el año 2022 y se considera un proyecto de Gestión del Conocimiento, sin embargo, es fundamental la participación de gestión tecnológica toda vez que es de su competencia la implementación de estrategias de calidad de datos (dominio de información MRAE), el conocimiento detallado de las fuentes de información de la entidad. Y las técnicas de automatización para componentes de extracción, trasformación y transporte de datos en la plataforma tecnológica. Se manifiesta que Gestión de Conocimiento ha adquirido la suite de Azure para analítica de datos, lo cual requiere la intervención de la Función TIC para avalar las condiciones del servicio, del aprovisionamiento y la trasferencia de conocimiento tecnológico hacia la entidad.
Datawarehouse y herramientas de inteligencia de negocios (BI).	No hay avance y se considera un proyecto de Gestión del Conocimiento, sin embargo, es fundamental la participación de gestión tecnológica toda vez que es de su competencia la implementación de soluciones tecnológicas y el aprovisionamiento y mantenimiento de infraestructuras TIC
Sistema de gestión de Seguridad de la Información -SGSI	A la fecha se ha avanzado en la construcción de instrumentos metodológicos, pero no se han implementado a cabalidad los controles en la plataforma, no se ha finalizado el inventario de activos de información con calificación de criticidad, no se han gestionado los riesgos de seguridad de la información y no se ha construido instrumentos para trasferencia del conocimiento ni para la medición de la efectividad de los controles y acciones de mejora. Las observaciones se emiten en el numeral 6.2
Plan de restauración del negocio (BRP - Business Recovery Plan) y el Plan de continuidad del negocio (BCP - Business Continuity Plan).	Se aplaza para 2022. Esta es una decisión recomendable ya que el Plan de continuidad debe construirse una vez se haya finalizado la estructuración del tratamiento de riesgos sobre activos críticos.
CIOM VIRTUAL.	Proyecto a cargo de la dirección de territorialización con apoyo de tecnología.
Sistema de Información Jurídica	Pertenece a la oficina asesora jurídica y se ha previsto atenderlo por Orfeo.
Trámites en línea	No se identifican tramites en línea en la página de la entidad. Los PQRSD se direcciona a **Bogotá te escucha.**
Gobierno Digital	Estas actividades si están incluidas en el Plan Operativo Anual y son objeto de seguimiento y medición a través del seguimiento trimestral a los planes de acción. Esta enfocado a las recomendaciones FURAG. Se lleva el seguimiento en el documento “Plan mejora agosto 2021 Gob digital final”

Nombre Proyecto	Estado
Sistema de Información para la gestión de Informes de Cuentas Ordenes de Prestación de Servicios - ICOPS	El proyecto se ejecutó y el sistema se encuentra en uso productivo.
Interoperabilidad SDMUJER	A la fecha no hay construidas soluciones de interoperabilidad. Gestión de Conocimiento esta liderando el tema y no se ha involucrado al proceso de Gestión Tecnológica, dada la importancia de un diseño integrado de arquitectura de interoperabilidad que minimice las construcciones de software y maximice la reutilización de componentes.
Modernización infraestructura tecnológica	Se incluyen correctamente los proyectos de modernización de la infraestructura en el Plan de adquisiciones, para la vigencia 2021 se destacan la adquisición de la solución de seguridad perimetral y la solución de backups. Las actividades de este proyecto se desglosan en el Seguimiento PETI 2021 sobre el cual se realiza seguimiento periódico.
Página web SDMUJER	Se encuentra en permanente actualización, para el caso del responsable de accesibilidad, se llevan tableros de control de los ajustes y avance en implementación.

Fuente: Elaboración propia.

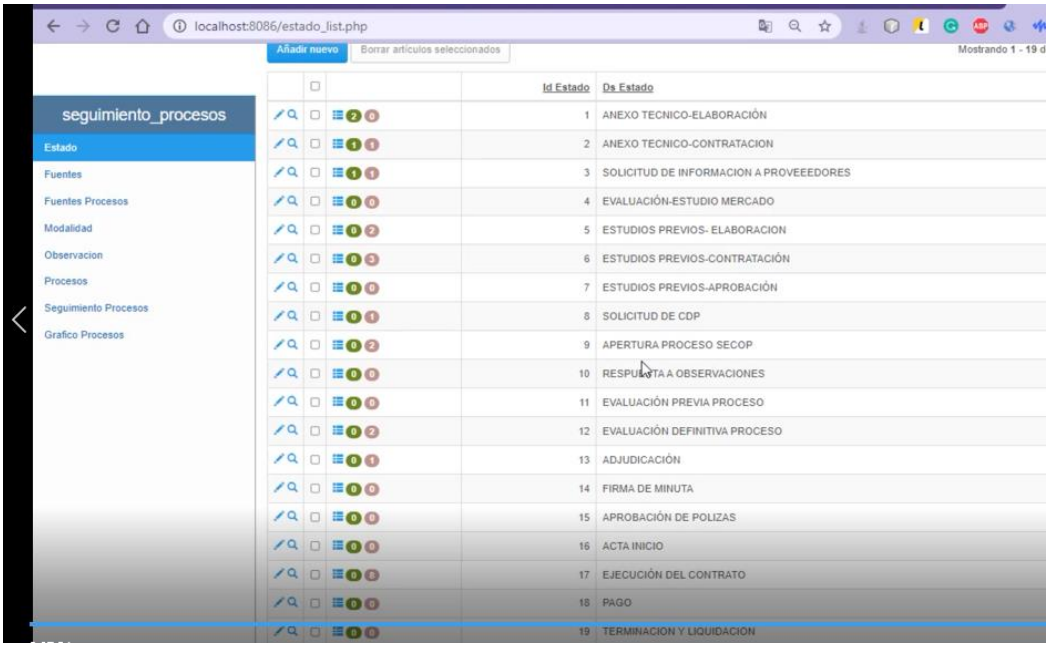
👉 A la fecha no se cuenta con una metodología de Gestión de Proyectos, documentada, formalizada e implementada, que incluya las fases de planeación, gestión de recursos y adquisiciones, implementación, criterios de aceptación de entregables e indicadores, gestión del riesgo y retrospectiva, con el realizar el balance de alcance, tiempos, costos y satisfacción, para garantizar equilibrio entre valor agregado e inversión TIC y realimentar el ciclo PHVA. Sin embargo, se está adelantando una iniciativa en PHP para gestionar las actividades del equipo TIC, inicialmente relacionadas con la gestión de adquisiciones, que puede ser mejorada para atender el seguimiento a proyectos.

Vale aclarar que la metodología borrador que se está adelantando esta más orientada al ciclo de desarrollo en metodologías agiles, no a gestión de proyectos tecnológicos en general, los proyectos de desarrollo solo son un tipo de proyecto y el ciclo de fabrica es aprovechable para articular la fase de ejecución de ese tipo de proyectos.

La herramienta permite registrar actividades y bitácora de acciones con respecto a cada una de ellas, tiene elementos valiosos y puede ser evolucionado para gestionar proyectos aprovechando que la Secretaría de la Mujer tiene fabrica interna:

- En primera instancia se deben parametrizar los estados que son propios de un proyecto (inicio, planeación, ejecución y cierre, particularizando la fase de ejecución de acuerdo a la naturaleza del proyecto ejemplo: análisis, diseño, desarrollo, pruebas, despliegue), ya que hasta el momento solo se han incluido aquellos inherentes a procesos de contratación. Vale aclarar que los estados incluidos, son propios de la fase de inicio cuando un proyecto este articulado con una adquisición. Un proyecto puede tener más de una adquisición.

Grafica 3



- En el registro del proceso al equipararlo a un proyecto, se debe agregar la fecha fin planeada del proyecto.
- Para equiparar las observaciones a las actividades de planeación, deben incluir fecha inicio y final de cada actividad, fecha de finalización real de la actividad (para cálculo de desviaciones de cumplimiento), % de avance y el responsable asignado con nombre propio para determinar equilibrio entre capacidad instalada y esfuerzo asignado. Puede usarse una base de 8 horas diarias para construir alertas de sobre asignación.

Imagen 4

- Se requiere tener niveles jerárquicos para las actividades, con el fin de agrupar en fases o equipos paralelos.

Imagen 5

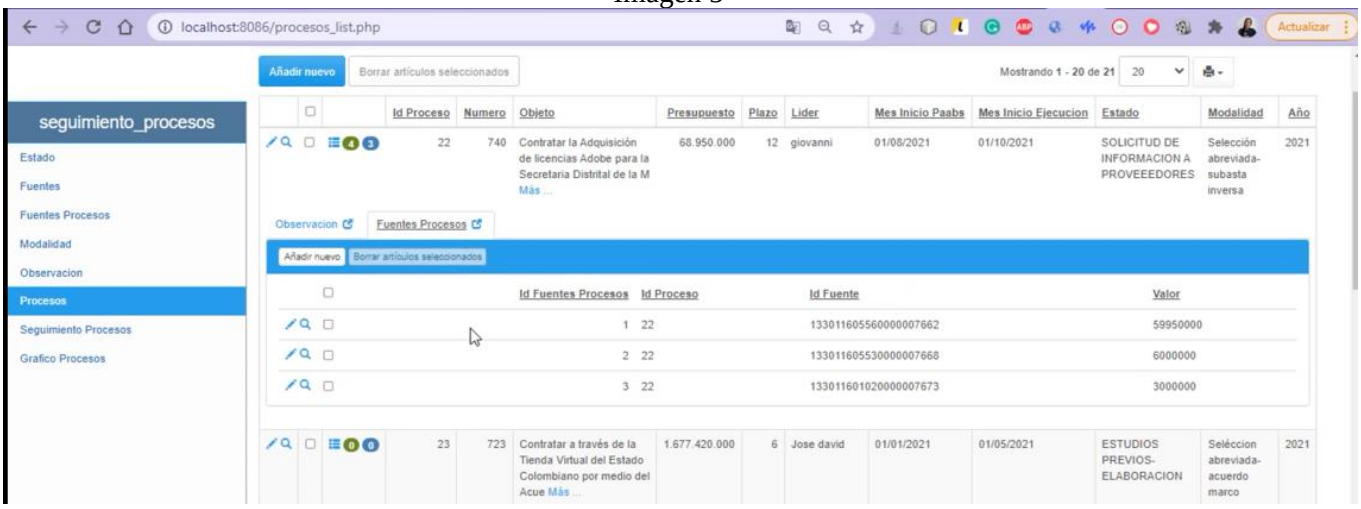
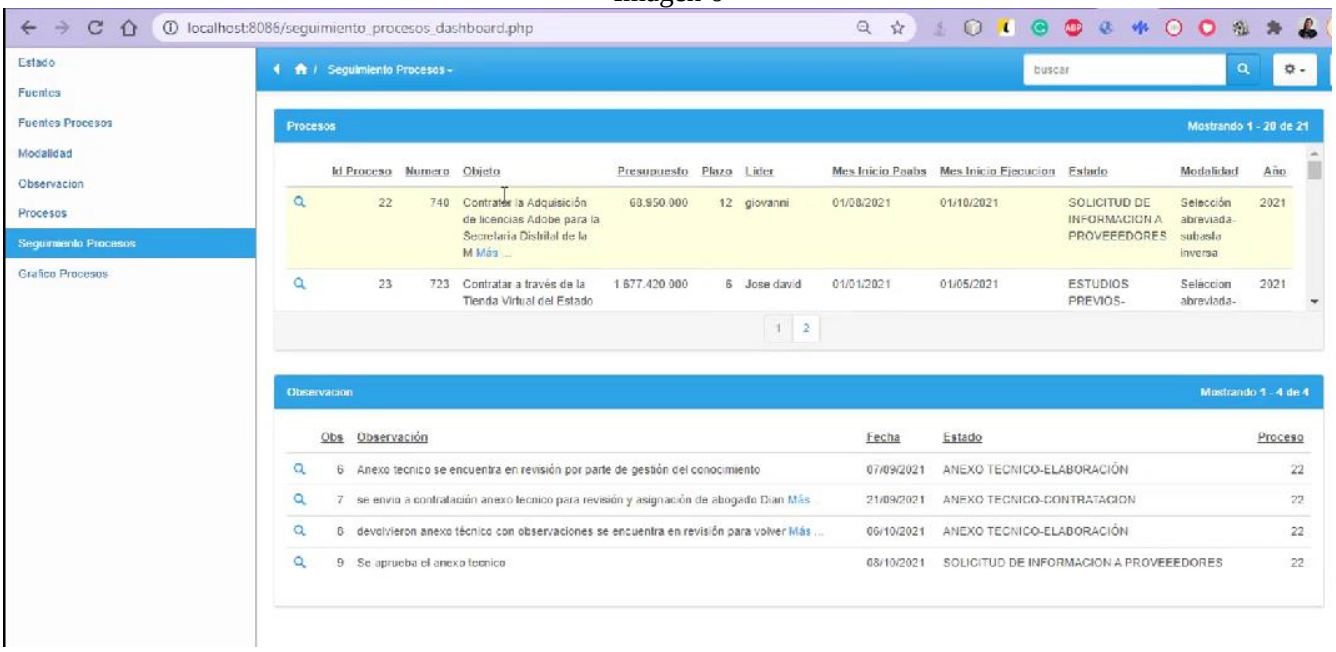


Imagen 6



👉 A nivel de seguimiento del PETI, se lleva el tablero de control Seguimiento PETI 2021, en el cual se registra seguimiento cualitativo y cuantitativo de los avances a través de entrevistas con los responsables, quienes emiten un cálculo perceptivo de avance, pero no es resultado de un indicador SPI sobre un cronograma de trabajo del proyecto.

En este seguimiento se encuentran entre otros los elementos de infraestructura, sistemas de información, soporte, formación y capacitación, que podrían relacionarse con el proyecto PETI "**Modernización infraestructura tecnológica** ", pero en términos generales se observa que el tablero de seguimiento no tiene

fechas objetivo para identificar desviaciones en el cumplimiento de las actividades, lo cual también impide tener un punto de contraste para verificar desviaciones dé % de avance.

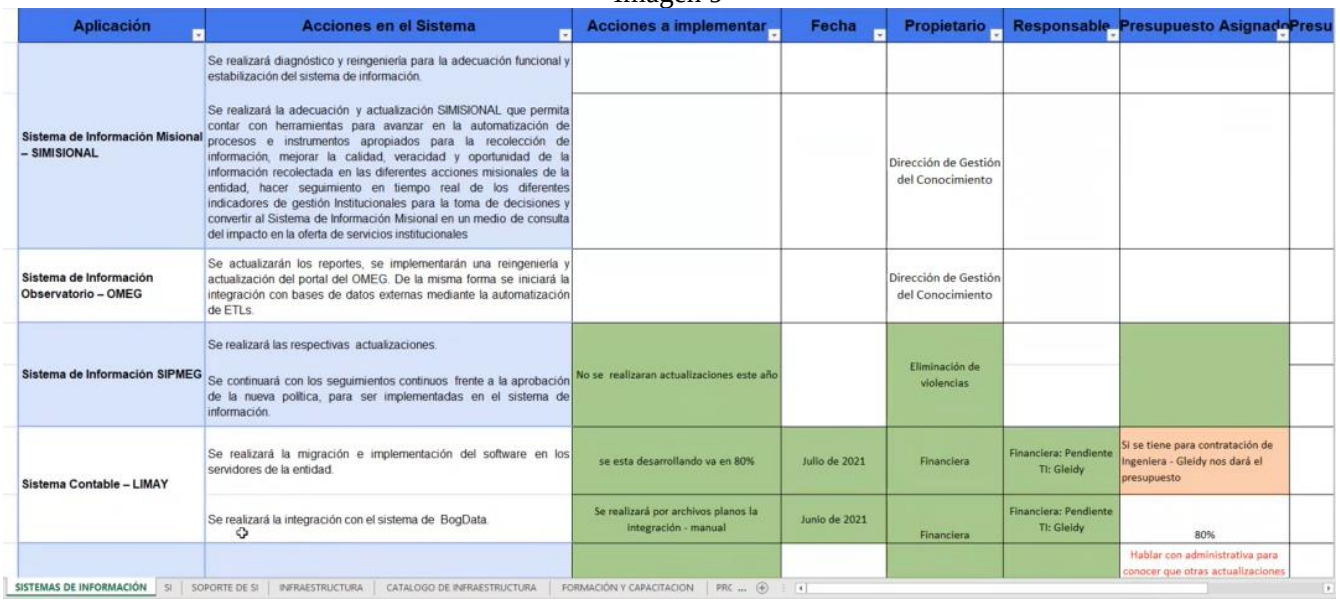
Imagen 7

ID servicios de infraestructura	Servicio de infraestructura	Oportunidad de Mejora	Acción de mejora	Avances	Fecha	Responsables
ST.SI.01	Servicio de nube	Ampliar Instancias, servidores de aplicativos y respaldos de información.	Ampliar en servidores oracle	100%		TI - Gleidy
		Ampliar Instancias, servidores de aplicativos y respaldos de información.	Ampliar en servidores Microsoft azure	Pendiente		Gestión del Conocimiento
ST.SI.02	Servicio de Redes	Renovar la licencia de Lacnic para IPv6 y renovar la infraestructura de comunicaciones	Contrato con ETB - ADICIÓN POR 2 MESES	Solicitud a proveedores y justificación - 20%	Junio de 2021	TI - Miguel
ST.SI.03	Servicio de seguridad	Adquirir una solución de Seguridad Perimetral, DLP y Respaldos.	Realizar contratación	se encuentra en estudios previos - 30%	Agosto de 2021	TI - Miguel
ST.SI.04	Servicio de servidores	Ampliar el sistema de hiperconvergencia.	Contratar la ampliación	Se encuentra en proceso de contratación 20%	Septiembre de 2021	TI - Miguel
ST.SI.05	Servicio de almacenamiento	Adquirir una solución SAN de mayor capacidad.	Se implemento	100%		
ST.SI.06	Servicio de telefonia	Ampliar la cobertura del servicio telefónico.	Se implemento	Se da atención a los requerimeintos de los nuevos proyectos 100%		
ST.SI.07	Servicio de respaldo eléctrico y aire acondicionado	Renovar UPS y sistema de aire acondicionado.	Proyección a 2023			
ST.SI.08	Servicio de Periféricos	Renovar el parque computacional de la entidad.		Pendiente de decisión de Jefas para adquisición de nuevos computadores		

Imagen 8

Actividad	Grado de madurez	Descripción hallazgo u oportunidad de mejora	Acción de mejora	Fecha	Responsables	Presupuesto Asignado	Presupuesto Ejecutado
Soporte de aplicaciones nivel 1	Implementado	El procedimiento existente no cumplía con todas las actividades requeridas, por esta razón se modificó y se creó el procedimiento GT-PR-12 GESTIÓN DE SOPORTE A USUARIOS E INCIDENTES TIC	OK				
Soporte de aplicaciones nivel 2	Implementado	El procedimiento existente no cumplía con todas las actividades requeridas, por esta razón se modificó y se creó el procedimiento GT-PR-12 GESTIÓN DE SOPORTE A USUARIOS E INCIDENTES TIC	OK				
Soporte de aplicaciones nivel 3	Implementado	El procedimiento existente no cumplía con todas las actividades requeridas, por esta razón se modificó y se creó el procedimiento GT-PR-12 GESTIÓN DE SOPORTE A USUARIOS E INCIDENTES TIC	OK				

Imagen 9



Aplicación	Acciones en el Sistema	Acciones a implementar	Fecha	Propietario	Responsable	Presupuesto Asignado	Presu
Sistema de Información Misional – SIMISIONAL	Se realizará diagnóstico y reingeniería para la adecuación funcional y estabilización del sistema de información. Se realizará la adecuación y actualización SIMISIONAL que permita contar con herramientas para avanzar en la automatización de procesos e instrumentos apropiados para la recolección de información, mejorar la calidad, veracidad y oportunidad de la información recolectada en las diferentes acciones misionales de la entidad, hacer seguimiento en tiempo real de los diferentes indicadores de gestión Institucionales para la toma de decisiones y convertir al Sistema de Información Misional en un medio de consulta del impacto en la oferta de servicios institucionales			Dirección de Gestión del Conocimiento			
Sistema de Información Observatorio – OMEG	Se actualizarán los reportes, se implementarán una reingeniería y actualización del portal del OMEG. De la misma forma se iniciará la integración con bases de datos externas mediante la automatización de ETLs.			Dirección de Gestión del Conocimiento			
Sistema de Información SIPMEG	Se realizará las respectivas actualizaciones. Se continuará con los seguimientos continuos frente a la aprobación de la nueva política, para ser implementadas en el sistema de información.	No se realizaran actualizaciones este año		Eliminación de violencias			
Sistema Contable – LIMAY	Se realizará la migración e implementación del software en los servidores de la entidad.	se esta desarrollando va en 80%	Julio de 2021	Financiera	Financiera: Pendiente TI: Gleidy	Si se tiene para contratación de Ingeniera - Gleidy nos dará el presupuesto	
	Se realizará la integración con el sistema de BogData	Se realizará por archivos planos la integración - manual	Junio de 2021	Financiera	Financiera: Pendiente TI: Gleidy	80%	
						Hablar con administrativa para conocer que otras actualizaciones	

SISTEMAS DE INFORMACIÓN | SI | SOPORTE DE SI | INFRAESTRUCTURA | CATALOGO DE INFRAESTRUCTURA | FORMACIÓN Y CAPACITACION | PRC ...

Imagen 10

Grado de madurez	Descripción hallazgo u oportunidad de mejora	Acción de mejora	Fecha	Responsables	avances	Presupuesto Asignado	Presupuesto
medio	Demoras que se presentan en la implementación y migración de las actualizaciones de hardware, software, gestores de base de datos y comunicaciones.	Definición del cronograma de mantenimiento a los Sistemas de Información.		TI	100%		
medio	Demoras en la identificación de las causas de los defectos del software	Presentar el plan de auditorías periódicas que determinen el correcto funcionamiento. - Se debe corregir actividad	Pendiente por definir por TI - 18 de mayo	TI - Ruben - Giovanny	0%		
medio	No se cuenta con un plan de rollback en caso de que la actualización impacte negativamente el comportamiento del sistema	Elaborar e implementar el plan de rollback. - **Se debe revisar si se deja o se cambia**	Pendiente por definir por TI - 18 de mayo	TI - Ruben - Giovanny	0%		

SISTEMAS DE INFORMACIÓN | SI | SOPORTE DE SI | INFRAESTRUCTURA | CATALOGO DE INFRAESTRUCTURA | FORMACIÓN Y CAPACITACION | PRC ...

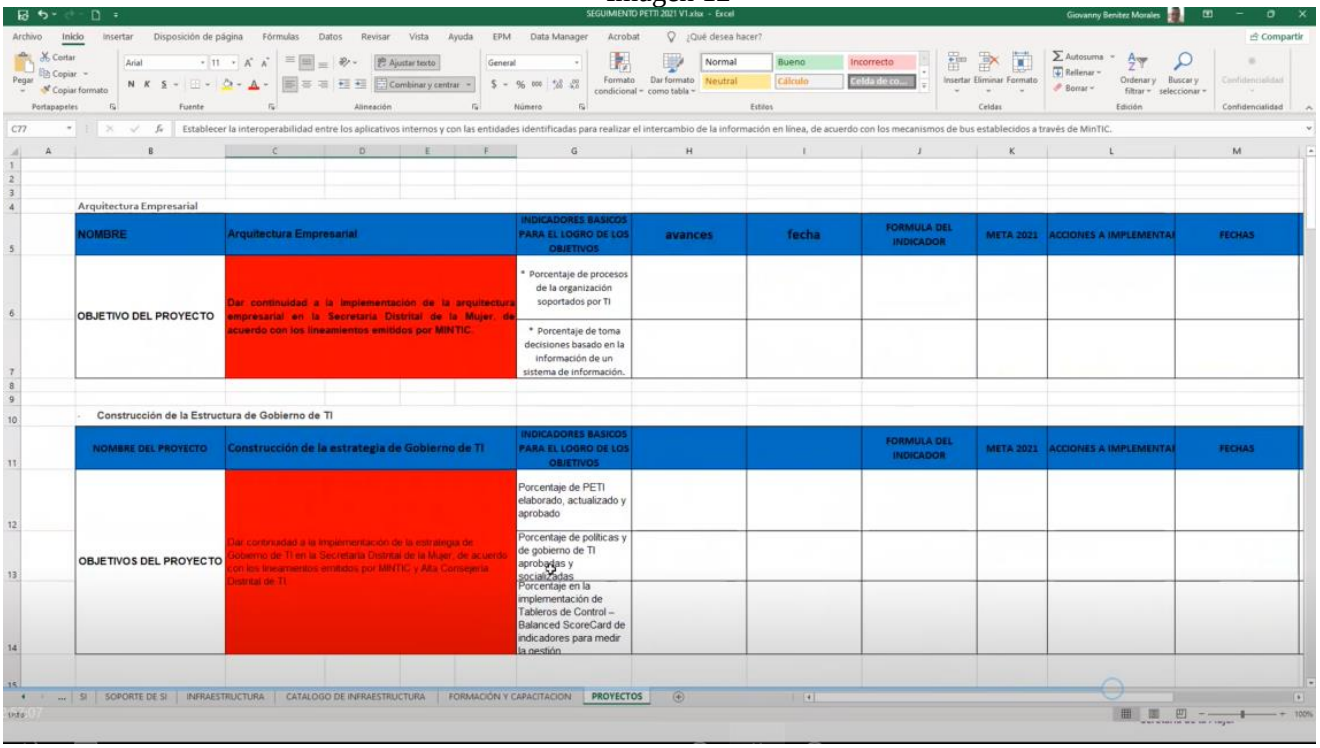
Imagen 11

IT12	Servidor DNS	Instalar una nueva versión del sistema operativo	100% ya se desarrollo		IT-MIGUEL			
IT13	Servidor VPN	Adquirir una solución perimetral	30%		IT-MIGUEL			
IT14	Servidor NTP	Instalar una nueva versión del sistema operativo	100% - 2021	2022	IT-MIGUEL			
IT15	Sistema de archivos	Instalar una nueva versión del sistema operativo		2022	IT-MIGUEL			
IT16	Repositorio de certificados de seguridad	Adquirir y configurar los certificados	Contratar certificados - servicio- se encuentra en contratación radicado - 70%	Junio de 2021	TI - GIOVANNY			
IT017	Software de monitoreo de servidores	Adquirir una herramienta de monitoreo	Se inicia en agosto	Noviembre de 2021	TI - Miguel			seguimiento septiembre
IT018	Software de monitoreo de red	Adquirir una herramienta de monitoreo	Se inicia en agosto	Noviembre de 2021	TI - Miguel			seguimiento septiembre
IT019	Framework de programación	Definir un Framework de programación transversal a la entidad	Se inicia en agosto	Diciembre de 2021	TI - laura			laura (agosto)
IT020	Software de ofimática	Instalar la última versión de ofimática	Ok se realizo proceso microsoft - 100%		IT-MIGUEL			
IT021	Servidor correo electrónico	Ampliar la capacidad de cuentas de correo	Ok se realizo proceso microsoft - 100%		IT-MIGUEL			
IT022	Switch	Renovar la infraestructura de red	Estan definiendo presupuesto, esta en anexo técnico	PENDIENTE	IT-MIGUEL			
IT023	Software de georreferenciación	Renovar el licenciamiento		PENDIENTE	Gestión del Conocimiento			
IT024	Ubicación física de Datacenter	Mejorar los sistemas de acceso y seguridad del centro de datos		2022	IT-MIGUEL			
IT025	Computador personal	Renovar el parque computacional	DEFINIR PRESUPUESTO Y CANTIDADES	PENDIENTE	IT-Juan david			
IT026	Software de monitoreo de Bases de datos	Adquirir una herramienta de monitoreo	Contratar herramienta , se encuentra en elaboración de estudios previos - estudio de mercado - 20%	Julio de 2021	TI - Giovanni			pendiente de revision de jerson
IT027	Respaldos (Backup)	Adquirir una solución de backup	Contratar solución - se realizó cotización y se tiene anexo técnico - pendiente presupuesto -	Septiembre de 2021	TI - Miguel			seguimiento agosto

SISTEMAS DE INFORMACIÓN | SI | SOPORTE DE SI | INFRAESTRUCTURA | CATALOGO DE INFRAESTRUCTURA | FORMACIÓN Y CAPACITACION | PRC ...

El documento incluye una hoja para seguimiento a los proyectos del PETI pero no se observa avance registrado:

Imagen 12



Arquitectura Empresarial

NOMBRE	Arquitectura Empresarial	INDICADORES BASICOS PARA EL LOGRO DE LOS OBJETIVOS	avances	fecha	FORMULA DEL INDICADOR	META 2021	ACCIONES A IMPLEMENTAI	FECHAS
OBJETIVO DEL PROYECTO	Dar continuidad a la implementación de la arquitectura empresarial en la Secretaria Distrital de la Mujer, de acuerdo con los lineamientos emitidos por MINTIC.	* Porcentaje de procesos de la organización soportados por TI						
		* Porcentaje de toma decisiones basado en la información de un sistema de información.						

Construcción de la Estructura de Gobierno de TI

NOMBRE DEL PROYECTO	Construcción de la estrategia de Gobierno de TI	INDICADORES BASICOS PARA EL LOGRO DE LOS OBJETIVOS			FORMULA DEL INDICADOR	META 2021	ACCIONES A IMPLEMENTAI	FECHAS
OBJETIVOS DEL PROYECTO	Dar continuidad a la implementacion de la estrategia de Gobierno de TI en la Secretaria Distrital de la Mujer, de acuerdo con los lineamientos emitidos por MINTIC y Alta Consejeria Distrital de TI	Porcentaje de PETI elaborado, actualizado y aprobado						
		Porcentaje de politicas y de gobierno de TI aprobadas y socializadas						
		Porcentaje en la implementación de Tableros de Control – Balanced ScoreCard de indicadores para medir la gestión						

SI | SOPORTE DE SI | INFRAESTRUCTURA | CATALOGO DE INFRAESTRUCTURA | FORMACIÓN Y CAPACITACION | PROYECTOS

El seguimiento a actividades del proceso de Gestión TIC se llevan en el Plan de acción 2021, Seguimiento a Plan operativo anual III Trimestre 2021 y Plan Operativo del proceso de Gestión TIC. Para cada actividad se realizan reportes trimestrales de avance. En términos generales las acciones están orientadas al mantenimiento y operación de la plataforma tecnológica y al cumplimiento de acciones en el marco de MIPG, pero las actividades no coinciden con los proyectos declarados en el PETI, se puede intuir que corresponden al proyecto "**Modernización infraestructura tecnológica**".

- Avanzar en la implementación de las Dimensión Gestión con valores para el Resultado en la Política de Gobierno Digital y Seguridad Digital - MIPG.
- Adquirir el licenciamiento para los productos y/o servicios a cargo de gestión tecnológica.
- Suministrar e implementar los servicios tecnológicos que requiera la SDMujer
- Atender los requerimientos tecnológicos que requiera las diferentes áreas de la entidad
- Ejecutar el plan de mantenimiento preventivo y correctivo a la infraestructura tecnológica de la SDMujer
- Soportar y actualizar a los sistemas de información y aplicativos de la entidad a cargo de gestión tecnológica
- Servicios de Información: Identificar y construir de los aplicativos requeridos por la Entidad para la automatización de los procesos.

En el documento *Plan mejora agosto 2021 Gob digital final.xls* se lleva el seguimiento a las recomendaciones de FURAG para la implementación de Gobierno Digital y Seguridad Digital, el documento tiene actividades, fechas objetivo y responsables. Pero los avances presentados en el documento suministrado a la auditoría no coinciden con el reportado en el documento *0. POA_SEGUIMIENTO III TRIMETRE_2021_SDMUJER*.xlsx que presenta un cumplimiento del 100% esperado para cada trimestre, pese a que, si bien hay avances importantes, no se ha cumplido a cabalidad con todos los requisitos. En este caso es importante que la planeación señale cuales son los requisitos que se tiene viabilidad de cubrir en cada vigencia para de esta manera alinear alcance y avance entre las dos herramientas.

Imagen 13

INDICADOR	FORMULA DEL INDICADOR	MAGNITUD / UNIDAD DE MEDIDA	TIPO DE INDICADOR	MEDIOS DE VERIFICACIÓN	PROGRAMACIÓN (Trimestral)					AVANCE DE EJECUCIÓN				
					TRIM I	TRIM II	TRIM III	TRIM IV	TOTAL	TIMR I	TRIM II	TRIM III	TRIM IV	TOTAL
Porcentaje cumplimiento Dimensión Gestión con valores para el Resultado en la Política de Gobierno Digital - MIPG.	(Porcentaje de cumplimiento Gobierno Digital / Porcentaje de cumplimiento esperado)*100%	100%	Gestión	Plan Estratégico de Tecnologías de la Información - PETI actualizado y Tablero Digital (Cada trimestre se calcula el indicador y se multiplica por 25%) Cumplimiento esperado: 80%	25%	25%	25%	25%	100%	25%	25%	25%		
Porcentaje cumplimiento Dimensión Gestión con valores para el Resultado en la Política de Seguridad Digital - MIPG.	(Porcentaje de cumplimiento Seguridad Digital / Porcentaje de cumplimiento esperado)*100%	100%	Gestión	Instrumento de evaluación del Modelo de Seguridad y Privacidad - MSPI. (Cada trimestre se calcula el indicador y se multiplica por 25%) Cumplimiento esperado 85%	25%	25%	25%	25%	100%	25%	25%	25%		

En cuanto a indicadores de gestión y de seguridad informática, el área manifiesta no tener avance, sin embargo, se identificaron los siguientes documentos en los que se declara el uso de indicadores, pero no se aporta evidencia de la fuente del cálculo periódico.

- *0. POA_SEGUIMIENTO III TRIMETRE_2021_SDMUJER.*xlsx: presenta indicadores de cumplimiento de metas del Plan de acción que en términos generales se

Tabla 4 Observaciones a los indicadores

INDICADOR	FORMULA DEL INDICADOR	OBSERVACION
Porcentaje cumplimiento Dimensión Gestión con valores para el Resultado en la Política de Gobierno Digital - MIPG.	(Porcentaje de cumplimiento Gobierno Digital / Porcentaje de cumplimiento esperado) *100%	No se suministra evidencia de la fuente del cálculo. El archivo de seguimiento FURAG no coincide con los valores reportados
Porcentaje cumplimiento Dimensión Gestión con valores para el Resultado en la Política de Seguridad Digital - MIPG.	(Porcentaje de cumplimiento Seguridad Digital / Porcentaje de cumplimiento esperado) *100%	
Licenciamiento de la Sdmujer	(No. de licencias adquiridas / No. de licencias instaladas) * 100%	No se aporta evidencia de la fuente de cálculo, el documento suministrado *Inventario de Información de Aplicaciones.xlsx* no tiene esta información. Los datos pueden ser tomados de la herramienta de mesa de ayuda GLPI El indicador esta formulado de manera invertida entre numerador y denominador
Servicios tecnológicos implementados	(No. de servicios implementados / No. de servicios priorizados) *100	Aunque no se aporta evidencia de fuente de cálculo, el área tiene debidamente organizados los servicios tecnológicos, lo cual facilita su medición
Requerimientos de soportes tecnológicos	(No. de requerimientos de soporte tecnológico, atendidos / No. de requerimientos de soporte tecnológico solicitados) * 100%	Se calcula con la mesa de servicio GLPI La fórmula del indicador no mide cumplimiento en los ANS establecidos, por lo tanto, no mide efectividad, únicamente la atención.
Plan de mantenimiento infraestructura tecnológica	Porcentaje de ejecución del plan de mantenimiento/100%	El documento suministrado *Inventario de Información de Aplicaciones.xlsx* incluye los cronogramas de mantenimientos que pueden ser la fuente de cálculo
Sistemas de información y aplicativos soportados y actualizados.	(No. de actualizaciones realizadas / No. de actualizaciones requeridas) X 100%	Aunque no se aporta evidencia de fuente de cálculo, el área tiene debidamente organizados los sistemas de información, lo cual facilita su medición. Sin embargo, es una debilidad el hecho de que no todos los sistemas de información están soportados y actualizados por la OAP y por lo tanto se genera un conflicto de responsabilidad sobre la medición del indicador.
Sistemas de información y aplicativos desarrollados	(No. de requerimientos de desarrollo atendidos / No. de requerimientos de desarrollo solicitados) X 100%	En primera instancia no se aporta evidencia de la existencia de pilas de producto para desarrollo de software que permita medir el estatus general por requerimientos, de igual manera, es una debilidad el hecho de que no todos los sistemas de información están soportados y actualizados por la OAP y por lo tanto se genera un conflicto de responsabilidad sobre la medición del indicador

6.1.2. ESTRUCTURA ORGANIZACIONAL Y GOBIERNO DE TI

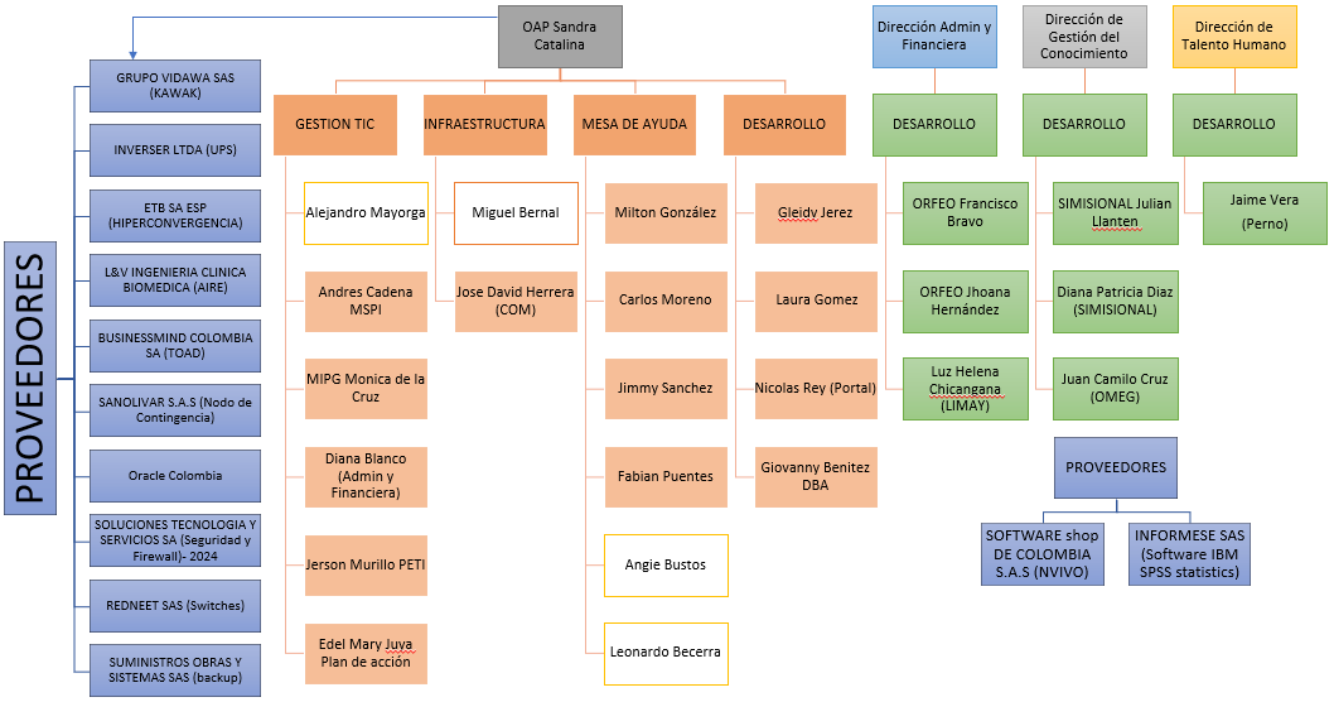
6.1.2.1. FORTALEZAS Y OPORTUNIDADES DE MEJORA

La estructura organizacional corresponde al siguiente esquema, donde se evidencia la segregación de Funciones de los recursos de TI en modalidad de funcionarios, contratistas y proveedores.

Guía de Color:

Proveedores
Contratistas OAP
Contratistas Otras áreas
Funcionarios

Imagen 14 Estructura de Gobierno TI



Fuente: Elaboración propia basada en el SECOP II

👉 Se observa que existen tanto contratistas como proveedores cuya supervisión del contrato se encuentra a cargo de las direcciones: Administrativa y Financiera, Gestión del Conocimiento y talento Humano, pese a que corresponden a servicios tecnológicos de desarrollo y de adquisición de activos de información, esta situación dificulta la optimización de recursos para el logro de los objetivos de la entidad en fortalecimiento tecnológico, incrementa la dependencia de conocimiento de terceros e incrementa el riesgo de pérdida de integridad y estandarización de la plataforma tecnológica que redunda en dificultades de escalamiento y mantenimiento futuro.

👉 No se cuenta con una Dirección u Oficina de tecnología de la información y las comunicaciones como lo establece el Decreto 415 de 2016, cuyo propósito es que las entidades aporten en la construcción de un Estado más eficiente y transparente gracias a la gestión estratégica TIC y dejen atrás la concepción de la función tecnológica como soporte y no como habilitador para el desarrollo de las estrategias institucionales y sectoriales. Esto, dificulta el logro de los objetivos de un Gobierno TI a saber: inversión estratégica de TIC, toma de decisiones centralizada, gestión integral de proyectos, apropiación del conocimiento TIC, aplicabilidad efectiva del ciclo PHVA y sostenibilidad de la plataforma tecnológica a mediano y largo plazo.

👉 No se cuenta con el Rol de "Oficial de Seguridad de la Información" asignado a un colaborador de la entidad que no esté subordinado al líder o jefe del Proceso de gestión tecnológica para aportar objetividad al ejercicio de verificaciones internas de la efectividad de los controles implementados en respuesta a los 14 dominios MSPI.

👉 Los interlocutores de la OAP manifiestan que perciben bajo reconocimiento al proceso de gestión tecnológica como área estratégica de la entidad, en lugar de un área de soporte y operación de la plataforma tecnológica.

Vale señalar que en las percepciones de mejora del instrumento PETI sesión 6 las áreas manifiestan que "*Generar estrategias de posicionamiento de TI al interior de la organización que le permita tener alianzas con las áreas misionales y sea área indispensable para generar las mejoras en estas áreas*"

👉 Las decisiones tecnológicas no están completamente centralizadas en la gestión TIC, de tal manera que se evalúe los impactos de cualquier decisión de inversión, adquisición o modernización tecnológica en la entidad. Si bien las áreas tienen la capacidad de gestionar adquisiciones que satisfagan requerimientos puntuales, es necesaria la intervención de expertos técnicos para que las adquisiciones garanticen el costo/beneficio y cumplan con criterios de estandarización, evolución, capacidad de integración, mantenimiento, desempeño, apropiación del conocimiento, riesgo tecnológico, seguridad de la información y sostenibilidad futura.

👉 De la situación anterior se deriva que el proceso de Gestión Tecnológica no lleva control y seguimiento sobre los proyectos liderados por otras áreas que corresponden a proyectos tecnológicos y por ende deberían tener el aval y participación de liderazgo por parte de tecnología, dado que es el área con la competencia para determinar el direccionamiento estratégico de la entidad, con el fin de garantizar si estandarización, compatibilidad, escalamiento y sostenibilidad autónoma.

👍 A nivel de Gobierno se cuenta con el Comité de enlace MIPG, lo cual es relevante para garantizar que se de integración entre las políticas de Gobierno Digital y Seguridad Digital con las demás políticas del MIPG. El seguimiento al PETI se realiza en el Comité Institucional de Gestión y Desempeño, donde también se tratan los planes y avances de la Política de Gobierno Digital y de implementación del MSPI.

👍 Dentro de los contratistas de la OAP se cuenta con conocimiento en el sistema integrado de gestión, lo cual facilita la articulación 9001 con 27001 en el marco de integración MSPI.

👉 No se cuenta con un comité, mesa de sistemas de información o cualquier otra instancia donde se discutan y prioricen los requisitos de las áreas en materia de adquisiciones o cambios al dominio de sistemas de información o al dominio servicios tecnológicos. Esto con el fin de determinar prioridades en la implementación de requerimientos de sistemas de información, como estrategia para optimizar la capacidad instalada del equipo de desarrollo de software y/o de los recursos para adquirir desarrollo por encargo a terceros. La priorización de requerimientos hace parte de las metodologías de referencia para el desarrollo de

software o sistemas de información del Dominio Sistemas de Información del Manual de Gobierno Digital. También es recomendado por Mintic en el instrumento "Mejores prácticas para la transformación de las entidades del Estado en el desarrollo de Sistemas de Información".

Vale anotar que los interlocutores de la OAP están adelantando una metodología de desarrollo de software con enfoque scrum, que por definición "exige" la estimación y priorización de los requerimientos particionados en historias de usuario, para establecer cuantos desarrollos son viables de atender en un Sprint según las horas disponibles del equipo de desarrollo y que es viable de paralelizar según la priorización y dependencias.

En cuanto a los controles establecidos en los contratos con proveedores y contratistas de servicios tecnológicos (muestra de tres contratos) se emiten las siguientes validaciones con respecto a la incorporación de elementos de control para gobernanza y gestión de seguridad con terceros y se concluye:

- Están correctamente incluidos los acuerdos de confidencialidad con terceros
- Están correctamente gestionadas las condiciones de propiedad intelectual y formalidad de uso a favor de la Secretaria de la Mujer en caso de software comercial, al igual que la cesión de derechos patrimoniales a favor de la entidad en caso de desarrollo por encargo.

- En los contratos SOFTWARE shop DE COLOMBIA S.A.S, Oracle y los 3 contratistas de desarrollo. No se incluyen ANS pese a que el objeto incluye soporte y/ o desarrollo de software susceptible de requerir soporte luego de la puesta en operación. Vale aclarar que los contratistas de desarrollo se crean correctamente en GLPI como agentes de soporte. Los demás contratos incluyen correctamente los ANS
- En los contratos ETB SA ESP, INFORMESE SAS, Oracle y los 3 contratistas de desarrollo. No se incluye trasferencia de conocimiento lo cual aplica por el objeto del contrato que incluye conocimiento especifico en su ejecución. Los demás contratos incluyen correctamente trasferencia de conocimiento suficiente.
- En los contratos GRUPO VIDAWA SAS, SOFTWARE shop DE COLOMBIA S.A.S no se incluyen condiciones de seguridad de la información como lo establece el dominio 15 de MSPI y los 3 contratistas de desarrollo si bien incluyen condiciones generales de seguridad de la información, no incluyen condiciones de "aplicar" procedimientos de desarrollo seguro en los productos construidos. Los demás contratos incluyen correctamente seguridad de la información.
- Ninguno de los contratos que incluyen la posibilidad de desarrollo de software hace alusión al obligatorio cumplimiento de la metodología de desarrollo de software en lo que compete a la naturaleza de su contrato que en el caso de software por encargo a personas naturales o jurídicas es pleno y para software comercial es concertado con el proveedor según condiciones de propiedad intelectual. Vale aclarar que, aunque no existe una metodología definitiva si existen y se aplican instrumentos del ciclo de fábrica.

En la siguiente tabla se marcan resaltado los casos de mejora para futuras contrataciones.

Tabla 5 Observaciones contratos

N° Contrato	Nombre Empresa	Fecha Inicio	Fecha Finalización contrato /servicio	Objeto Contractual	Acuerdo Conf	ANS	Trasferencia de conocimiento	Requisitos de seguridad	Metodología de desarrollo	PI	Cesión / Licencia	Observaciones Auditoría
CO1.PCCNTR. 2553222	GRUPO VIDAWA SAS	1/06/2021	31/05/2022	Contratar la renovación del soporte técnico actualización y mantenimiento del software KAWAK de la Secretaría Distrital de la Mujer	SÍ	Max 24 horas	SI 10 personas	NO	NO	SÍ	N/A	N/A
CO1.PCCNTR. 2574719	INVERSER LTDA - INVERSIONES Y SERVICIOS	23/06/2021	31/12/2021 6 meses tras firma o hasta agotar recursos	Prestar el servicio de mantenimiento preventivo y correctivo para equipos UPS de nivel central y las sedes de la Secretaría Distrital de la Mujer.	SÍ	NO	NO	NO	NO	N/A	N/A	N/A
CO1.PCCNTR. 2605767	SOFTWARE shop DE COLOMBIA S.A.S	25/06/2021	24/07/2021 12 meses tras firma	Adquisición del software NVIVO para la Secretaria Distrital de la Mujer	SÍ	NO	SI 10 horas	NO	NO	SI	6.B.3. Entregar el documento expedido por el fabricante donde se indique la adquisición de la licencia de los derechos de uso del software NVivo a nombre de la Secretaría con vigencia de un año, dando cumplimiento a las normas	N/A

N° Contrato	Nombre Empresa	Fecha Inicio	Fecha Finalización contrato /servicio	Objeto Contractual	Acuerdo Conf	ANS	Trasferencia de conocimiento	Requisitos de seguridad	Metodología de desarrollo	PI	Cesión / Licencia	Observaciones Auditoría
											de derechos de autor.	
CO1.PCCNTR. 2625070	Empresa de Telecomunicaciones de Bogota ETB SA ESP	1/07/2021	28/02/2022	Suministrar los servicios integrados de comunicaciones convergentes que requiera la Secretaría Distrital de la Mujer.	SÍ	SÍ. 5.9 en Anexo Técnico	NO	SÍ. Cláusula 8, par 2.	NO	N/A	N/A	N/A
CO1.PCCNTR. 2646225	L&V INGENIERIA CLINICA BIOMEDICA	13/07/2021	31/12/2021	Prestar el servicio de mantenimiento preventivo y correctivo para Aire Acondicionado para Nivel Central de la Secretaría Distrital de la Mujer	SÍ	NO	NO	NO	NO	N/A	N/A	N/A
CO1.PCCNTR. 2875253	BUSINESSMIND COLOMBIA SA	29/09/2021	28/09/2022 Soporte 12 meses tras implementación	Adquirir Licencias TOAD para la administración de bases de datos de la Secretaría Distrital de la Mujer.	SÍ	SÍ. 6 en Anexo Técnico	SI 10 horas	SÍ. Cláusula 20, par 2.	NO	SI	7.1.2. Entregar la licencia adquirida a perpetuidad al igual que el documento mediante el cual se otorguen los derechos a uso de las mismas a nombre de la Secretaría Distrital de la Mujer	No se encontraron documentos del contratista para verificar capacidad de licenciamiento
CO1.PCCNTR. 2949800	SANOLIVAR S.A.S	29/10/2021	20/12/2021 Soporte 3 años a partir de puesta en funcionamiento	Adquirir un nodo de contingencia para el sistema de hiperconvergencia existente en la Secretaría	SÍ	SÍ. 6 en Anexo Técnico	Documentar configuraciones; Capacitación 8 horas	SÍ. Cláusula 9, par 3.	NO	NO	C.5. Documentos de suscripción y licenciamiento	No es recomendable incluir 3 regímenes distintos de confidencialidad. No se encuentra registro de propiedad

N° Contrato	Nombre Empresa	Fecha Inicio	Fecha Finalización contrato /servicio	Objeto Contractual	Acuerdo Conf	ANS	Trasferencia de conocimiento	Requisitos de seguridad	Metodología de desarrollo	PI	Cesión / Licencia	Observaciones Auditoría
				Distrital de la Mujer							de la solución ofertada.	intelectual en documentos del contratista a pesar de que existe obligación de licenciamiento.
CO1.PCCNTR. 2958445	Oracle Colombia LTDA	5/11/2021	4/01/2022 Soporte hasta 9/ago/2022	Contratar la renovación del servicio de soporte mantenimiento y actualizaciones de las licencias Oracle de la Secretaría Distrital de la Mujer.	SÍ	NO	NO	NO	NO	SI	SI. Cláusula 3B y 6B3	N/A
CO1.PCCNTR. 2969666	SOLUCIONES TECNOLOGIA Y SERVICIOS SA	8/11/2021	31/12/2021 Licencia, sorporte y garantía 3 años	Adquirir e implementar una solución de seguridad perimetral para la Secretaría Distrital de la Mujer	SÍ	SÍ. 6 en Anexo Técnico	(2) funcionarios en administración, monitoreo y resolución de problemas de las plataformas Mínimo 40 horas.	SÍ. Cláusula 10, par 2.	NO	SI	SI	N/A
CO1.PCCNTR. 3059900	REDNEET SAS	1/12/2021	20/12/2021 Licencia, actualizaciones y garantía hasta por 3 años tras firma	Contratar la adquisición de Switches para fortalecer la infraestructura de comunicaciones de la Secretaría Distrital de la Mujer	SÍ	SÍ. Punto 7, Anexo Técnico	(2) funcionarios en administración, monitoreo y resolución de problemas de las plataformas Mínimo 40 horas.	SÍ, Cláusula 9, par 2.	NO	SI	SI	N/A
CO1.PCCNTR. 3064824	SUMINISTROS OBRAS Y SISTEMAS SAS	30/11/2021	20/12/2021 Licenciamiento y garantía 3 años tras recepción de la solución	Adquirir e implementar una solución física de backup para la Secretaría Distrital de la Mujer	SÍ	SÍ. Punto 6, Anexo Técnico	(2) funcionarios en administración, monitoreo y resolución de problemas de las plataformas Mínimo 40 horas.	SÍ. Cláusula 9, par 2.	NO	SI	SI	N/A

N° Contrato	Nombre Empresa	Fecha Inicio	Fecha Finalización contrato /servicio	Objeto Contractual	Acuerdo Conf	ANS	Trasferencia de conocimiento	Requisitos de seguridad	Metodología de desarrollo	PI	Cesión / Licencia	Observaciones Auditoría
CO1.PCCNTR. 3069215	INFORMESE SAS	1/12/2021	31/12/2021 Soporte 12 meses tras Acta de Inicio	Adquirir licenciamiento y contratar la actualización del Sofware IBM SPSS statistics con plan anual de mantenimiento	SÍ	Max 24 horas	NO	SÍ. Cláusula 8, par 2.	NO	SI	SI	N/A
CO1.PCCNTR. 2170606		27/01/2021	31/12/2021	Prestar servicios profesionales para realizar el soporte técnico análisis diseño y desarrollo de funcionalidades del Sistema de Gestión Documental ORFEO	SÍ	NO	NO	SÍ pero no en desarrollo	NO	N/A	SI	N/A
CO1.PCCNTR .2238657		10/02/2021	31/12/2021	Prestar servicios profesionales a la Dirección de Gestión del Conocimiento en la actualización soporte y adecuado funcionamiento del Sistema de Información Misional - SIMISIONAL - y los aplicativos que requiera la dependencia.	SÍ	NO	NO	SÍ pero no en desarrollo	NO	N/A	SI	No existe obligación de transferencia de conocimiento ni de metodología de desarrollo, pero existe obligación de apoyo a gestión del conocimiento
CO1.PCCNTR. 2270404		18/02/2021	31/12/2021	Prestar servicios profesionales en la Dirección de Talento Humano desarrollando actividades concernientes con la actualización soporte técnico y	SÍ	NO	NO	SÍ pero no en desarrollo	NO	N/A	SI	N/A

N° Contrato	Nombre Empresa	Fecha Inicio	Fecha Finalización contrato /servicio	Objeto Contractual	Acuerdo Conf	ANS	Trasferencia de conocimiento	Requisitos de seguridad	Metodología de desarrollo	PI	Cesión / Licencia	Observaciones Auditoría
				funcional del Sistema de Información de Personal y Nómina (PERNO) o del software implementado para registrar la información de personal y nómina de la Ent								

6.2. IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

6.2.1. IMPLEMENTACION DEL MSPI

6.2.1.1. FORTALEZAS Y OPORTUNIDADES DE MEJORA

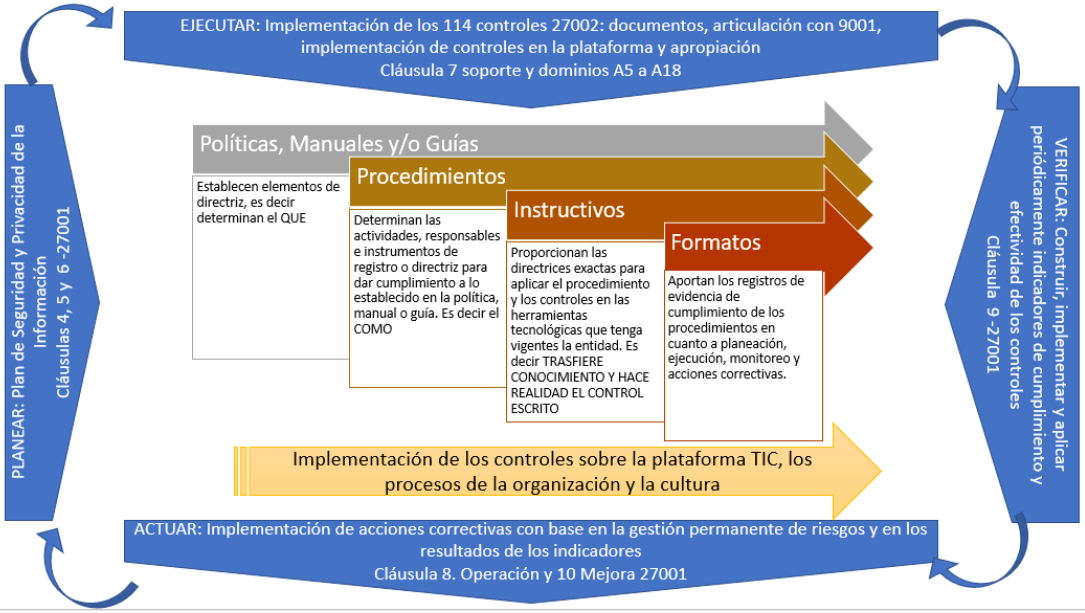
El modelo de seguridad y privacidad de la información cuyos lineamientos establecen las directrices para la implementación del habilitador trasversal de Seguridad de la información de la Política de Gobierno Digital, busca la implementación de los lineamientos de seguridad de la información en todos sus procesos, servicios tecnológicos, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad y disponibilidad y privacidad de los datos, mediante la aplicación de un proceso de gestión efectiva del riesgo.

Este habilitador tiene como resultado el Sistema de Gestión de Seguridad de la Información, basado en la norma ISO 27001:2013 y que debe estar articulado con el Sistema de Gestión Integral de la entidad, pero también implica la configuración tecnología de los controles en la plataforma de servicios tecnológicos y un proceso de concientización y sensibilización que garanticen la apropiación de la seguridad como un componente de la cultura organizacional.

De igual manera, su implementación total se considera finalizada cuando se han construido e implementado todos los componentes que hacen efectivo un sistema de gestión en el ciclo PHVA.

Así las cosas, si bien la OAP ha avanzado en la construcción de elementos documentales y ha avanzado en la configuración de controles y componentes de sensibilización, solo se puede considerar finalizado cuando se cumplen los elementos del siguiente esquema, con base en el cual se emiten las observaciones de este capítulo.

Imagen 15 Estrategia de implementación MSPI



Fuente: Elaboración propia basada en ISO27001:2013

- Mediante RESOLUCIÓN No. 407 de 2019 "*…se actualizó y se adopta la Política de Seguridad de la Información de la Secretaría Distrital de la Mujer y se deroga la Resolución 061 de 2014*", la cual referencia correctamente al MANUAL DE POLÍTICAS ESPECIFICAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN y establece su obligatorio cumplimiento.

- De igual manera se ha construido el GT-MA-3 - MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN - V3, como documentos base del MSPI. Su articulación es correcta con respecto a la norma ISO 27701:2013 y su anexo A 27002. La aplicación de los criterios y lineamientos establecidos en dicho manual se relacionan en el presente informe y así mismo, las debilidades en materia de controles implementados se relacionan en el numeral 6.2.2.

A continuación, se relaciona la verificación general de instrumentos en cumplimiento MSPI

6.2.1.2. 5. LIDERAZGO. CLAUSULA 27001:2013

- En el GT-MA-3 - MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN - V3, se ha incluido la asignación de roles y responsabilidades de manera correcta y el órgano de liderazgo en el Comité Institucional de Gestión y Desempeño – Alta Dirección.

6.2.1.3. 4. Contexto de la organización. CLAUSULA 27001:2013

- Se ha adelantado la Declaración de Aplicabilidad (*Declaración de Aplicabilidad Final.xlx*) en la cual la entidad ha declarado el 100% de aplicabilidad de los 114 controles del Anexo A 27002:2013. En términos generales, si bien los instrumentos a continuación relacionados y en especial los manuales GT-MA-3 - MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN - V3 y el GT-MA-1 - MANUAL GESTIÓN TECNOLÓGICA - V3, tienen definidas correctamente las políticas, en la práctica no se cumplen a cabalidad. En el numeral de este informe 6.2.2. PRACTICAS DE CONFIABILIDAD, INTEGRIDAD Y SEGURIDAD DE LA INFORMACION se emiten las debilidades en materia de controles configurados en la plataforma para la seguridad informática.

Tabla 6 Observaciones sobre el SOA MSPI

DOMINIO ISO 27002:2013 MSPI	OBSERVACIONES DE LA AUDITORIA
A.5 Políticas de seguridad de la información	Se referencia correctamente al GT-MA-3 - MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN - V3 y la POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN No se hace alusión a las auditorías internas adelantadas por la Oficina de Control interno, que de acuerdo al manual de seguridad hacen parte de su responsabilidad. SEC-PR-1 - FORMULACIÓN Y SEGUIMIENTO DEL PLAN ANUAL DE AUDITORÍA V5 y SEC-PR-5 SEGUIMIENTO PLAN DE MEJORAMIENTO - V6.
A.6 Organización de la seguridad de la información	Los roles y responsabilidades están correctamente declarados en el GT-MA-3 - MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN - V3 El manual no incluye la lista de contactos con autoridades y grupos de interés, solo lo menciona de manera general, pero ya se está finalizando la construcción del documento con los datos puntuales

DOMINIO ISO 27002:2013 MSPI	OBSERVACIONES DE LA AUDITORIA
	que dan cumplimiento al objetivo de control y que incluye correctamente los datos de contactos y enlaces. 👉 Con respecto a la Seguridad de la información en la gestión de proyectos, la declaración de aplicabilidad hace alusión a las minutas de contrato y el GT-MA-3 - MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN - V3, establece que "Los proyectos que adelante o desarrolle inhouse la Entidad, contemplar la gestión de los riesgos de seguridad asociados a la información del proyecto, lo cual incluye una identificación de los riesgos y la definición de la forma como serán gestionados." Sin embargo, en los siguientes contratos tomados como muestra de colaboradores a cargo de proyectos de desarrollo Inhouse no se mencionan ni la gestión ni los riesgos de seguridad de la información. - Contrato 026-2021 Laura Estefania Gomez Muñoz: contratista a cargo del proyecto icops - Contrato 024-2021 Gleidy Jeniffer Jerez Mayorga: contratista a cargo de proyectos de desarrollo inhouse En todo caso ni la política de seguridad ni el manual establece de manera explícita las políticas de seguridad en la gestión de proyectos conforme a la norma ISO 27001:2013. 👉 Con respecto a la política y medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles, si bien el manual GT-MA-3 incluye los lineamientos, estos no están implementados en la práctica y solo están orientados a dispositivos institucionales pese a que desde dispositivos personales se puede acceder a servicios Tic tales como el correo, con respecto al cual el proceso anuncia que está implementando un control de seguridad por PIN y doble factor , pero al momento de la auditoría no estaba completamente implementado. 👉 Con respecto a la política y medidas que apoyen la seguridad para proteger la información a la que se accede, procesa o almacena en los sitios de teletrabajo, el manual GT-MA-3 - MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN - V3 en su numeral 8.1 establece lineamientos de seguridad, pero no se relaciona evidencia de su aplicación, en especial lo relacionado con que los equipos estén previamente configurados por gestión tecnológica, el control de antivirus, instalaciones peligrosas", no exige que los equipos de cómputo desde los que se conectan los usuarios, sean equipos seguros, ya que no se obliga la ejecución de un análisis de vulnerabilidades y su respectiva corrección.
A.7 Seguridad de los recursos humanos	👉 Se referencia al procedimiento GTH-PR-2 - SELECCIÓN Y VINCULACIÓN DE PERSONAL - V2, el cual es válido como instrumento para dar cumplimento al control de seguridad antes del empleo, pero no es suficiente ya que solo se refiere a funcionarios y no a contratistas. No se incluye la referencia al instrumento de vinculación de contratistas y las medidas para revisión de antecedentes. 👉 La declaración de aplicabilidad no se hace referencia al GT-MA-1 - MANUAL GESTIÓN TECNOLÓGICA - V3, numeral 3.4, mediante el cual se establecen algunos lineamientos para la gestión de los permisos de usuario a servicios tecnológicos. 👉 El manual GT-MA-1 solo hace referencia al alta de accesos a correo institucional y sistemas de información asociados al Directorio activo, pese a que varios sistemas tales como SIM misional y Si capital no están integrados a LDAP. Vale aclarar que en la práctica la gestión TIC si gestiona a través de GLPI los accesos a todos los servicios tecnológicos, pero el documento no lo incluye de esta manera. 👉 El manual GT-MA-1 no incluye las modificaciones de accesos por cambio de rol, o bajas

DOMINIO ISO 27002:2013 MSPI	OBSERVACIONES DE LA AUDITORIA
	temporales por vacaciones, suspensiones o incapacidades. En la inspección de la mesa de servicio y entrevista con la colaboradora del área de talento humano, se pudo observar que no siempre se informa a Gestión TIC sobre estos eventos para que se proceda a suspender temporalmente los privilegios. El manual GT-MA-1 no incluye los lineamientos de seguridad en la baja permanente de privilegios a los servicios tecnológicos. En la práctica se realizan por demanda. Se cuenta con un formato de entrega de equipo y un formato de paz y salvo al finalizar la relación contractual, de igual manera el manual GT-MA-1 hace referencia al backup de la información a la baja de privilegios. Sin embargo, estos formatos no se referencian en la declaración de aplicabilidad. Se encuentran correctamente incluidas las cláusulas relacionadas con seguridad de la información en los contratos delos colaboradores (CONFIDENCIALIDAD: CONFIDENCIALIDAD, SEGURIDAD DE LA INFORMACIÓN Y TRATAMIENTO DE DATOS PERSONALES), sin embargo debe ser especifico en el caso de accesos privilegiados del personal de tecnología. Los contratos incluyen correctamente acuerdos de confidencialidad. Se hace correcta referencia a los procesos disciplinarios GDIS-PR-1 - DISCIPLINARIO VERBAL - V1 y GDIS-PR-2 - DISCIPLINARIO ORDINARIO - V2 Se cuenta con el formato GT-FO-8 - ACUERDO DE CONFIDENCIALIDAD - V1, sin embargo, no se menciona en la declaración de aplicabilidad y no hay certeza de su aplicación. En el caso del contrato de la auditora, el formato no se exigió. Se revisaron como muestra los contratos: de compraventa Nº 660 de 2021 con SOFTWARE SHOP DE COLOMBIA SAS y de renovación, actualización, mantenimiento y soporte Técnico N° 618 de 2021, con GRUPO VIDAWA S.A.S. Entre los documentos de estos contratos no se incluye el acuerdo de manera independiente, solo se referencia el asunto en la Clausula Octava del contrato. Se hace referencia al “Plan Capacitaciones Seguridad Digital” el cual esta correctamente estructurado y se encuentra en actualización, además el Plan Institucional de Formación y Capacitación incluye la referencia a la Socialización de la política de seguridad de la información y protección de datos y los usuarios entrevistados tienen recordación de capacitaciones y campañas. La política de seguridad está debidamente socializada y se adelantan campañas con apoyo de Talento humano.
A.8 Gestión de activos	Se hace correcta referencia al manual GD-PR-2 - ACTIVOS DE INFORMACION - V1que incluye correctamente los tipos de activos: hardware, software, información, servicios y bases de datos personales. De igual manera incluye correctamente los lineamientos de los objetivos de control 8.1 y 8.2 del MSPI referentes a la responsabilidad y clasificación de la información. Se cuenta con el formato GA-FO-28 para la entrega de los activos de los equipos de cómputo, el cual se esta diligenciando recientemente. Pero solo incluye los activos tipo hardware, puede mejorarse agregando los elementos de software instalado y accesos a servicios tecnológicos y sistemas de información, como evidencia de la entrega formal del alta y punto de referencia para modificaciones y bajas. Se hace referencia al formato GD-FO-8 - INVENTARIO DE ACTIVOS DE INFORMACION - V2, que en cuanto a estructura es correcto, pero a la fecha no ha sido diligenciado en su totalidad para los activos hardware, software, información, servicios y bases de datos personales,

DOMINIO ISO 27002:2013 MSPI	OBSERVACIONES DE LA AUDITORIA
	únicamente se suministró a la auditoria una matriz de activos documentales de la oficina asesora jurídica. Vale aclarar que el inventario de activos de información es un requisito obligado de la implementación MSPI y es la base para el tratamiento de riesgos. Aunque la política lo menciona, en la práctica no están limitados los accesos a medios removibles tales como USB. La auditora realizó la inspección en 4 equipos. Vale aclarar que el control de limitar el uso de USB no es solo por fuga de información, sino porque es un medio para trasmisión de virus, modificación del usuarios administradores locales y ejecución de programas portables potencialmente peligrosos.
A.9 Control de acceso	En cuanto a cumplimiento documental, se relaciona el documento GT-MA-3 - MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN - V3, que referencia lineamientos de acceso para telefonía, internet y altas de usuarios a Dominio, sin embargo, en el numeral 6.2. se evidencian las debilidades de seguridad de accesos identificadas por el auditor que contradicen lo establecido. A su vez el documento relacionado GT-PR-12 - GESTIÓN DE SOPORTE A USUARIOS E INCIDENTES TIC - V1, corresponde al procedimiento de mesa de ayuda, y los requisitos de altas, bajas y modificaciones están siendo articulados con la herramienta de mesa de servicio. No se hace entrega ni se relacionan los instrumentos de gestión de accesos privilegiados a personal que tiene acceso a servicios tecnológicos a modo de administrador, soporte, desarrollo y/o implementación. El auditor evidencio la existencia de 20 cuentas de usuarios de dominio con privilegios de administrador entre las cuales hay 7 no nombradas. Los detalles se presentan en el numeral 6.2.2 A nivel de control de acceso a sistemas y aplicaciones, la política está declarada de manera general en el GT-MA-3, pero no se recibió evidencia de la existencia de los procedimientos técnicos o instructivos técnicos para cada servicio tecnológico y gestión de accesos a archivos fuentes, que mitiguen el riesgo de dependencia de conocimiento frente a una ausencia temporal o permanente del responsable de la administración y configuración de herramientas para la gestión de seguridad y acceso. No se menciona al GT-MA-1 MANUAL GESTIÓN TECNOLÓGICA, el cual incluye elementos relacionados con la gestión de accesos. Si bien el manual GT-MA-01 se incluyen lineamientos para gestión de contraseñas seguras y cambio periódico, estos no corresponden fielmente a las directivas de dominio (ejemplo cambio periódico de 92 días según manual y de 180 en directivas) En todo caso, los usuarios entrevistados manifiestan que en virtualidad no recuerdan que les haya sido solicitado cambio de contraseña obligatorio. No se pidió cambio de contraseña al inicio de sesión por primera vez a la auditora. En el numeral 6.2.2 se relacionan accesos no autorizados originados en esta fuga de control.
A.10 Criptografía	Si bien el GT-MA-3 - MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN - V3, incluye lineamientos de seguridad para criptografía, no se aporta evidencia de un procedimiento de gestión de llaves criptográficas para los elementos mencionados en el manual. El manual señala que para los dispositivos móviles se utiliza encriptación con BitLocker, pero no se hace referencia a la custodia de las claves criptográficas generadas.
A.11 Seguridad física y del entorno	Solo se menciona al GT-MA-3 - MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN - V3, el cual únicamente referencia acceso a instalaciones, pero no controles específicos de seguridad para el centro de cómputo y su etiquetado, puntos de red

DOMINIO ISO 27002:2013 MSPI	OBSERVACIONES DE LA AUDITORIA
	desatendidos y el retiro e ingreso de equipos portátiles. En la visita se evidencio el uso del formato GT-FO-13 - REGISTRO DE INGRESO AL CENTRO DE COMPUTO - V2, pero no está relacionado en la SOA. No se relaciona el PLAN DE EMERGENCIA Y CONTINGENCIAS DE LA SECRETARIA DISTRITAL DE LA MUJER que incluye elementos de seguridad física - Protección contra las amenazas externas y ambientales. La auditora ingreso y retiro un equipo portátil sin que se solicitara registro alguno. Los detalles se relacionan en el numeral 6.2.2 de este informe. No se relaciona el manual GT-MA-1 MANUAL GESTIÓN TECNOLÓGICA, el cual incluye elementos relacionados con la seguridad física. No se hace referencia al contrato con INVERSER LTDA - INVERSIONES Y SERVICIOS en cumplimiento a Seguridad en el suministro. No se incluyen instructivos para el mantenimiento de equipos de cómputo que incluya condiciones de seguridad tales como restricciones de ODBC, conexión a wifi, limitantes de panel de control entre otros. Se cuenta con el documento LINEAMIENTO ALISTAMIENTO EQUIPOS DE COMPUTO que incluye algunos elementos, pero no se relaciona en la declaración de aplicabilidad. Se incluyen correctamente los lineamientos de Equipo de usuario desatendido y Política de escritorio limpio y pantalla limpia
A.12 Seguridad de las Operaciones	Con respecto al control de código malicioso se observa que en la práctica no hay restricciones en cuanto a navegación en sitios potencialmente peligrosos, descargas, uso de Web WhatsApp, juegos etc. En el numeral 6.2.2. se presentan evidencias. Pese a que el manual de seguridad en su numeral 8.5. POLÍTICA ACCESO A INTERNET lo prohíbe. El proceso de Gestión TIC manifiesta que no le ha sido permitido implementar las medidas por parte de las áreas. Se encuentra correctamente configurada la protección de *endpoints*: *Microsoft 365 Defender* para los equipos de red. A nivel de instrumentos documentales, el dominio se encuentra desarrollado de manera muy general en el GT-MA-3 - MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN - V3, y los documentos relacionados con los procedimientos para la gestión de operaciones no dan cumplimiento cabal al dominio A12, toda vez que este dominio se refiere a aquellos procedimientos necesarios para operar, mantener, monitorear y evolucionar los servicios tecnológicos de la entidad. Vale aclarar que este dominio es el de mayor envergadura desde el punto de vista de la documentación del MSPI dado que su propósito es documentar el conocimiento para la operación y continuidad de los servicios TIC sin dependencia de conocimiento de los operadores actuales. Los siguientes son algunos de los procedimientos que no están construidos y que son requeridos por MSPI: Procedimiento de gestión de cambios en plataforma tecnológica. Se incluye el GT-PR-17 - IMPLEMENTACIÓN Y MANTENIMIENTO DE SOLUCIONES DE INFORMACIÓN - V1, pero está relacionado de manera equivocada ya que corresponde al dominio A.14 Adquisición, desarrollo y mantenimiento de sistemas. También se relaciona el GT-PR-15 - IMPLEMENTACIÓN DE SOLUCIONES Y SERVICIOS DE TECNOLOGÍA - V1, que da cubrimiento parcial para el caso de adquisiciones en atención a requerimientos de la entidad, pero

DOMINIO ISO 27002:2013 MSPI	OBSERVACIONES DE LA AUDITORIA
	no incluye los cambios de emergencia y la planeación de capacidad para identificar requerimientos de cambio necesarios para la continuidad sin detrimento de eficiencia del procesamiento de datos y o almacenamiento de información. Procedimiento de gestión de ambientes. Su propósito es reducir riesgos asociados a la realización de cambios no autorizados o accesos no autorizados al entorno productivo en los sistemas de información activos en la infraestructura de la entidad, mediante la separación, gestión de seguridad, creación, monitoreo, aprovisionamiento y baja de los entornos de desarrollo, pruebas y productivo. No solo no está construido el procedimiento explicito, sino que los desarrolladores tienen acceso a los tres ambientes y el formato RFC con que se cuenta es insuficiente para dar autonomía a infraestructura de hacer un despliegue de manera autónoma. Procedimientos de registro, monitoreo y medición de capacidad y desempeño. No está documentado, pero vale aclarar que si se realizan inspecciones de monitoreo. Procedimiento de registro y seguimiento de eventos de sistemas de Información y comunicaciones. No está documentado, pero vale aclarar que si se realizan inspecciones de eventos. Los siguientes procedimientos están correctamente relacionados al dominio A12.:GT-PR-12 - GESTIÓN DE SOPORTE A USUARIOS E INCIDENTES TIC - V1, GT-PR-16 - GESTIÓN DE SOLUCIONES Y SERVICIOS - V1 No se incluye la referencia a instructivos de operación necesarios para la implementación del dominio A12, toda vez que son los instrumentos que garantizan la autonomía de la entidad en la gestión de las herramientas tecnológicas que administran configuran y gestionan la operación d ellos servicios TIC. En cuanto al respaldo de la información el GT-MA-3 - MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN - V3, incluye las políticas generales, pero hace alusión a el documento ADMINISTRACIÓN DE BACKUPS Y RESTAURACIÓN DE LA INFORMACIÓN, que no se encontró en lucha. A su vez el documento GT-MA-1 MANUAL GESTIÓN TECNOLÓGICA incluye en mayor detalle los lineamientos para los procesos de respaldo de la información. No se hace referencia a formatos de planeación de backups (ya sean manuales o automáticos de la consola) y formatos de pruebas de restauración aleatoria y periódica. Vale aclarar que, si se han realizado pruebas de restauración y monitoreo de backup, y existe el procedimiento GT-PR-04 ADMINISTRACION DE BACKPS Y RESTAURACION DE LA INFORMACIÓN, y condiciones correctamente establecidas en el manual de gestión tecnológica (3.10) pero la declaración no los referencia.
A.13 Seguridad de las comunicaciones	La topología de red está debidamente documentada al igual que los esquemas de red, pero no se hace referencia a ellos en la declaración de aplicabilidad. Se aportan a la auditoria los diagramas físicos de red, lógico de red y de servidores. El GT-MA-3 - MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN - V3, incluye las políticas generales, pero no se relacionan procedimientos y/o instructivos de: o Aseguramiento de equipos de red, inventario de todos los equipos de red activos y los registros de monitoreo y medición de la capacidad para todos los canales de comunicación, Controles de red para interconexiones mediante WLAN, controles de red para uso de equipos móviles corporativos y/o bajo la modalidad BYOD y teletrabajo (controles no políticas), Segregación de las redes organizacionales y trasferencia de información.

DOMINIO ISO 27002:2013 MSPI	OBSERVACIONES DE LA AUDITORIA
	Se identificaron algunas debilidades de seguridad en elementos de protección de red que se muestran en el numeral 6.2.2
A.14 Adquisición, desarrollo y mantenimiento de sistemas	Únicamente se relacionan los documentos GT-MA-3 - MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN - V3, GT-PR-16 - GESTIÓN DE SOLUCIONES Y SERVICIOS - V1, GT-PR-17 - IMPLEMENTACIÓN Y MANTENIMIENTO DE SOLUCIONES DE INFORMACIÓN - V1 y GT-MA-4 - MANUAL DE DESARROLLO O MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN - V1, pero no el conjunto de instrumentos construidos para la gestión de Desarrollo de software. Con respecto al control de cambios en sistemas de información se cuenta con algunos instrumentos aplicados en el ciclo de fabrica que aplican como registro del control, sin embargo, están orientados a desarrollo interno y no se incluyen elementos de cambio en software comercial. No se encuentra evidencia de procedimientos específicos de seguridad en el desarrollo de software para las tres modalidades: Adquisición de software comercial, Desarrollo por encargo con terceros y desarrollo inhouse, que contemple: ○ seguridad del entorno de desarrollo; ○ seguridad del ciclo de vida del desarrollo de software: ○ seguridad en la metodología de desarrollo de software; ○ pautas de codificación segura del lenguaje que se utiliza; ○ requisitos de seguridad en la fase de diseño; ○ verificación de seguridad dentro de los hitos del proyecto; ○ repositorios seguros; ○ seguridad en el control de la versión; ○ conocimiento de seguridad de aplicación necesario; ○ capacidad de los desarrolladores de evitar, encontrar y solucionar la vulnerabilidad. Las observaciones especificas se incluyen en el numeral 6.5
A.15 Relaciones con los proveedores	Solo se relaciona el GT-MA-3 - MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN - V3, que expone las políticas de manera muy general sin hacer alusión a los instrumentos con que ya cuenta la entidad para gestionar los terceros. No han sido desarrolladas en detalle las políticas de seguridad antes, durante y después de la relación con el tercero a través de documentos reguladores para: ✓ Gestión de accesos a sistemas, aplicaciones e instalaciones x terceros ✓ Tratamiento de riesgos en contratos con terceros ✓ Gestión de ANS de proveedores TIC ✓ Criterios de aceptación en contratos con proveedores TIC ✓ Monitoreo de acciones y gestión de incidentes en el marco de contratos con terceros En la revisión de contratos adelantada por el auditor se exponen algunas debilidades (ver 6.1.2) El documento GT-PR-15 IMPLEMENTACIÓN DE SOLUCIONES Y SERVICIOS DE TECNOLOGÍA es aplicable, pero no está relacionado en la declaración.

DOMINIO ISO 27002:2013 MSPI	OBSERVACIONES DE LA AUDITORIA
A.16 Gestión de incidentes de seguridad de la información	El GT-MA-3 - MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN - V3, expone las políticas de manera muy general, y el procedimiento GT-PR-12 - GESTIÓN DE SOPORTE A USUARIOS E INCIDENTES TIC - V1, no trata de manera explícita los incidentes se seguridad. En la mesa de ayuda no hay una categoría para estos casos. No se relacionan los procedimientos de cómo actuar frente a un incidente de seguridad, su relación con la materialización de riesgos conocidos o la inclusión por riesgo desconocido como insumo para la actualización del tratamiento de riesgos de seguridad de la información.
A.17 Aspectos de seguridad de la información de la gestión de continuidad de negocio	El GT-MA-3 - MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN - V3, expone las políticas de manera muy general, y el procedimiento GT-PR-13 - ADMINISTRACIÓN DEL PLAN DE CONTINUIDAD - V1, describe los pasos para construir un Plan de Continuidad, pero sin alusión a la relación entre los activos críticos, los riesgos aceptados y los planes de contingencia, igualmente no referencia claramente la aplicación de análisis BIA para la construcción del plan. En la práctica se cuenta con solución de hiperconvergencia que aporta contingencia para los servidores. No se incluye ninguna referencia en la declaración
A.18 Cumplimiento	Tanto el GT-MA-3 - MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN - V3, como las minutas de contratos con personas naturales y jurídicas se menciona correcta y explícitamente la cesión de derechos patrimoniales y/o las condiciones de propiedad intelectual según el caso. Se tomaron como muestra: ✓ De compraventa Nº 660 de 2021 con SOFTWARE SHOP DE COLOMBIA SAS ✓ De renovación, actualización, mantenimiento y soporte Técnico N° 618 de 2021, con GRUPO VIDAWA S.A.S. ✓ Contrato 026-2021 Laura Estefanía Gomez Muñoz: contratista a cargo del proyecto Icops ✓ Contrato 024-2021 Gleidy Jennifer Jerez Mayorga: contratista a cargo de proyectos de desarrollo inhouse. No se relaciona la Política de tratamiento de datos personales con la que cuenta la entidad. La Oficina de Control interno ha cumplido con su rol de verificación establecido en el Manual de Seguridad Digital, con la ejecución de la presente auditoría que incluye el seguimiento al MSPI.

6.2.1.4. 6. Planificación. CLAUSULA 27001:2013

Las Acciones para tratar riesgos y oportunidades se analizan y emiten observaciones en el numeral 6.3

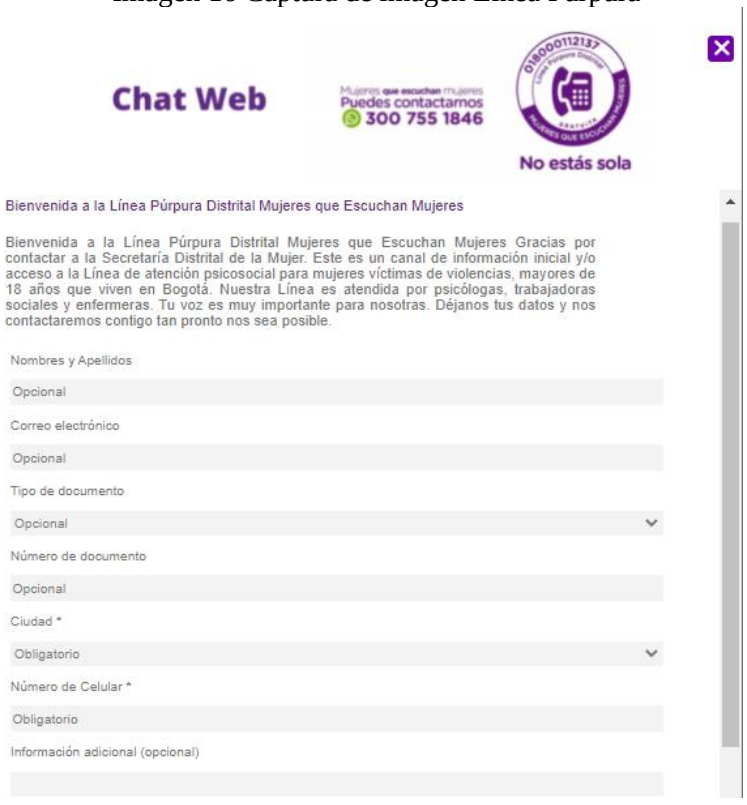
Se cuenta con el **Plan de Seguridad y Privacidad de la Información** vigencia 2021, que relaciona las siguientes actividades a ejecutar en el año 2021, sobre las que se emiten observaciones:

El plan incluye las actividades de alto nivel para atender en la vigencia 2021, pero no se cuenta con un instrumento de planeación detallada por actividades con fechas puntuales de entrega, responsables y seguimiento detallado de % de avance. Algunas actividades se relacionan en el documento "*Plan mejora agosto 2021 Gob digital final*", pero no se relacionan % de avance o desviación. Para la implementación MSPI la planeación detallada es relevante dada la envergadura de la implementación de los 114 controles aceptados en la Declaración de aplicabilidad y que su implementación incluye por lo menos los siguientes componentes:

- ✓ El MSPI como habilitador tiene como resultado el Sistema de Gestión de Seguridad de la Información, basado en la norma ISO 27001:2013 y que debe estar articulado con el Sistema de Gestión Integral de la entidad en sus elementos comunes tal como riesgos, medición, seguridad en recursos humanos y gestión de terceros entre otros.
- ✓ Construcción de los instrumentos (manuales, guías, procedimientos, formatos e instructivos), que demuestren la implementación documentada de los 114 controles del MSPI.
- ✓ Implementación y configuración tecnológica de los controles en la plataforma de servicios tecnológicos
- ✓ Un proceso de concientización y sensibilización que garanticen la apropiación de la seguridad como un componente de la cultura organizacional articulado con el dominio de uso y apropiación del MRAE
- ✓ Construcción de indicadores que permutan medir la efectividad de los controles implementados y el nivel de cumplimiento por parte de los actores involucrados, como herramienta para identificar elementos de mejora y actualización continuas.

👉 Como evidencia de la actividad "Actualización y aprobación de la Política de Privacidad y Datos Personales" programada para su elaboración y publicación el 31 de marzo y 30 de abril de 2021 respectivamente, se aporta el documento en actualización "10. Política de privacidad y tratamiento de datos personales Secretaría de la Mujer VF", el cual se encuentra correctamente estructurado, pero no hace referencia a un protocolo de anonimización de datos personales, y no se encuentra relacionada en formularios de captura de información tal como la línea purpura. Vale aclarar que la nueva política no ha sido publicada.

Imagen 16 Captura de imagen Línea Purpura



👍 Como evidencia de la actividad de "*Actualización de la metodología de Activos de Información*", programada para marzo 31 de 2021, se presenta el documento GDC-PR-02 ACTIVOS DE INFORMACION, que corresponde a la metodología, la cual incluye correctamente los tipos de activos: hardware, software, información, servicios y bases de datos personales. De igual manera incluye correctamente los lineamientos de los objetivos de control 8.1 y 8.2 del MSPI referentes a la responsabilidad y clasificación de la información.

👉 Como evidencia de la actividad "*Actualización de Activos de Información*" programada para julio de 2021, se aporta el documento "2021 - MATRIZ INVENTARIO ACTIVOS DE INFORMACIÓN_JURIDICA.xlsx" el cual no contiene el inventario total de activos de información, únicamente contiene documentos de la oficina asesora Jurídica. A su vez, en las publicaciones de la entidad solo se encontró el documento MATRIZ ACTIVOS DE INFORMACION_2019, que únicamente incluye activos documentales, pero no tecnológicos.

👉 Pese a que el GT-MA-3 - MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN - V3 contempla aplicación de controles criptográficos para activos de información catalogados como críticos, no se ha incluido en el levantamiento de activos con las áreas la identificación de documentos reservados que son objeto de trasporte y que por lo tanto son candidatos para aplicar controles criptográficos antes de su transporte y/o almacenamiento.

👉 No tienen contemplado en el levantamiento de activos tipo "información" aquellos generados en el proceso de gestión tecnológica, tales como documentos de arquitectura de sistemas de información, documentos de infraestructura o del proceso de desarrollo de software entre otros, que pueden resultar de carácter reservado y en algunos casos hasta aportar información que facilite un ataque de seguridad.

👎 No se cuenta con una versión final de inventario de activos de información actualizada que incluya los activos totales de hardware, software, archivos digitales, conjuntos de datos, servicios tecnológicos y sistemas de información y se haya determinado para ellos:

- ✓ Nivel de criticidad del activo TIC en función del valor para el negocio y el impacto de la materialización de una amenaza sobre su operación.
- ✓ Los requisitos de integración de conjuntos de datos.
- ✓ Información confidencial en tránsito interno y con terceros.
- ✓ Archivos y datos confidenciales que deben ser objeto de controles criptográficos y/o anonimización de bases de datos.
- ✓ Levantamiento del Inventario de sistemas de información y aplicativos que incluyan tanto software adquirido como herramientas de uso libre autorizadas.
- ✓ Articulación de activos críticos con la gestión de riesgos.

👍 En cuanto al manejo de los activos tipo "Información" orientado a las áreas, el diseño de la matriz es correcto e incluye preguntas tipo que facilitan la clasificación de los atributos de confidencialidad, integridad y disponibilidad que facilitan la clasificación de criticidad del activo de información.

Como evidencia de la actividad de Revisión procedimientos, guías, manuales y controles de la norma ISO 270001:2013 seguridad de la información se hace entrega a la auditoría del archivo "*Instrumento_Evaluacion_MSPI-JUNIO 2021*" el cual relaciona los instrumentos construidos y las evidencias de implementación de los controles MSPI. Sobre este documento se observa.

Imagen 17

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	88	100	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	88	100	OPTIMIZADO
A.9	CONTROL DE ACCESO	96	100	OPTIMIZADO
A.10	CRIPTOGRAFÍA	60	100	EFECTIVO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	81	100	OPTIMIZADO
A.12	SEGURIDAD DE LAS OPERACIONES	62	100	GESTIONADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	72	100	GESTIONADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	73	100	GESTIONADO
A.15	RELACIONES CON LOS PROVEEDORES	90	100	OPTIMIZADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	74	100	GESTIONADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	70	100	GESTIONADO
A.18	CUMPLIMIENTO	83.5	100	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		81	100	OPTIMIZADO

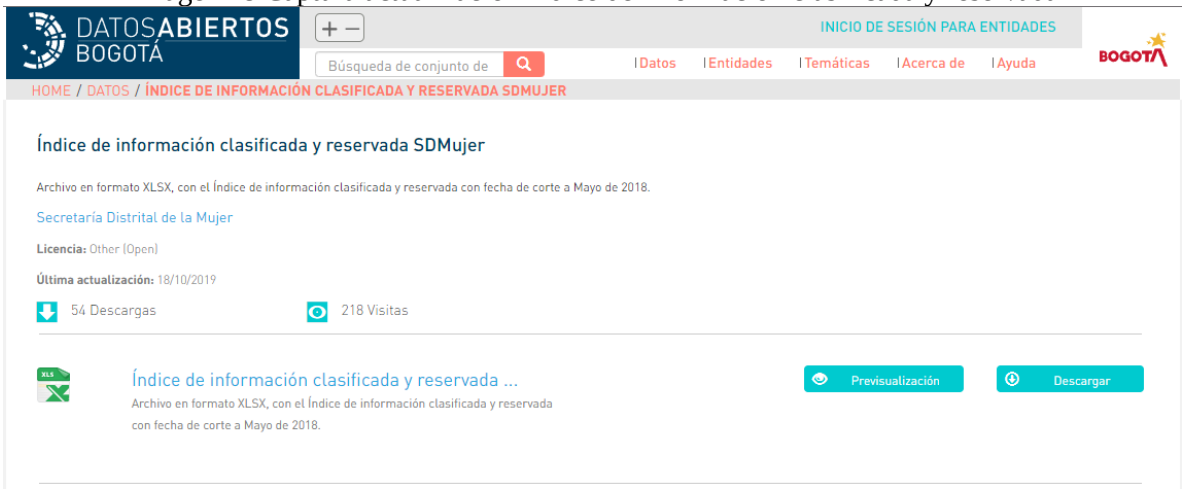
El 81% de avance reportado ponderado por cada uno de los 14 dominios no es consecuente con las evidencias relacionadas en el instrumento, que únicamente referencian instrumentos documentales, pero no incluye evidencias de cumplimiento del ciclo PHVA con respecto a:

- Evidencia de implementación de los controles en la plataforma tecnológica, con formatos e instructivos que hacen parte de la implementación – HACER
- Evidencia de diseño y aplicación de herramientas de monitoreo y medición del cumplimiento de procedimientos y efectividad de los controles – VERIFICAR
- Evidencia de acciones correctivas o de mejora derivadas de los resultados de la medición periódica – ACTUAR

Es de anotar que el ciclo PHVA, es parte inherente de las implementaciones basadas en normas ISO y hacen parte integral del instrumento de evaluación de MINTIC

En cuanto a la actividad de publicación del índice de información clasificada y reservada, programada para el 30de septiembre de 2021, se evidencia que la última actualización es del 18/10/2019.

Imagen 18 Captura actualización índice de información clasificada y reservada



Como evidencia de las actividades de Actualización, Ejecución del plan de sensibilización, se adelantan

campañas y eventos donde se realiza correctamente el proceso de sensibilización. A modo de ejemplo, el próximo 15 de diciembre hay un evento con base en un phishing controlado de octubre de 2021.

Imagen 19 Ejemplo 1 de correo electrónico con tips de seguridad

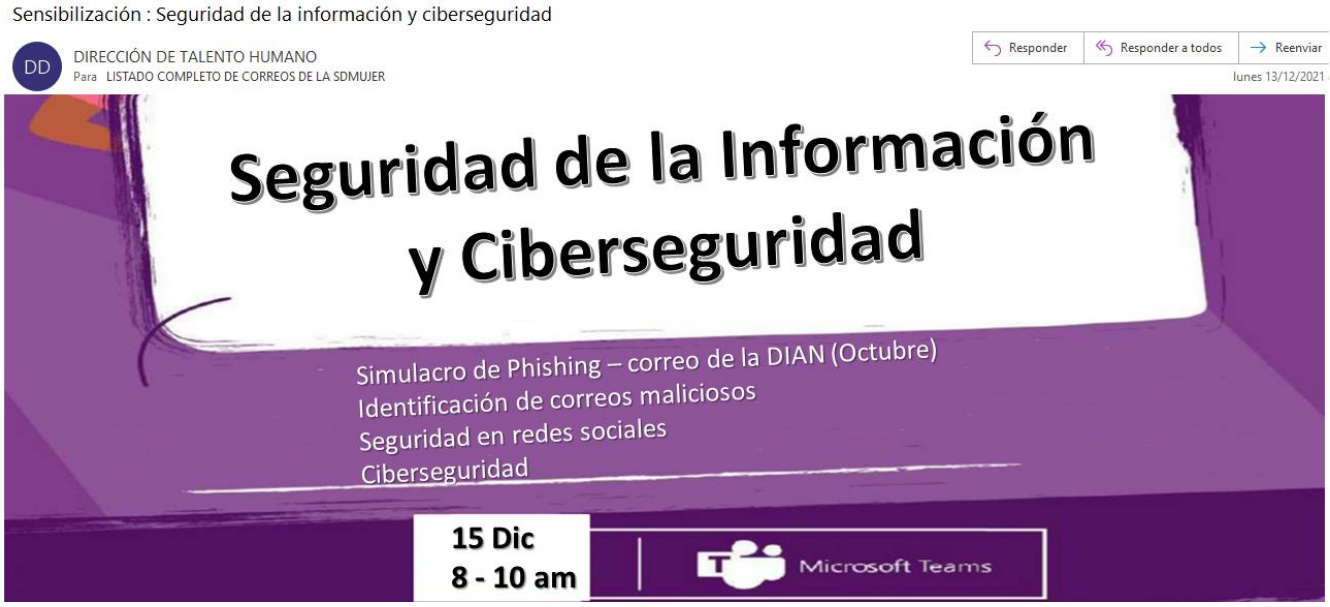


Imagen 20 Ejemplo 2 de correo con tips de seguridad

6.2.1.5. Evaluación y desempeño. Clausula 9 27001:2013

Como evidencia de la actividad de Definir Indicadores del Sistema de Gestión de Seguridad de la Información, programada para 2021, se hace entrega a la auditoría del archivo "INDICADORES DE GESTIÓN DE SEGURIDAD" el cual incluye 11 indicadores que en su gran mayoría corresponden a una actividad más que a un indicador toda vez que no están construidos como una fórmula que permita establecer un resultado frente a un valor de meta. Tampoco se presentó evidencia de su cálculo periódico y fuente de datos de cada indicador. A continuación, se muestra un ejemplo de indicadores correctamente formulados para el dominio A14 MSPI:

Imagen 21 Ejemplo de indicadores dominio 14 MSPI

Sección	Dominio, objetivos de control y Controles	NOMBRE DEL INDICADOR	DEFINICIÓN DEL INDICADOR	TIPO DE INDICADOR	PERIODICIDAD DE CALCULO	FUENTE DE INFORMACION	INTERPRETACION DEL INDICADOR	FORMULA PARA EL CALCULO	UNIDAD DEL INDICADOR
A.14.2	**Objetivo de Control: Seguridad en los procesos de desarrollo y de soporte**								
A.14.2.1	Política de desarrollo seguro								
A.14.2.5	Principios de construcción de los sistemas seguros	Seguridad en Sistemas de Información	Porcentaje de Sistemas de Información que cumplen las políticas de seguridad	Proceso	Por demanda	P-SIS-017 Principios de ingeniería de sistemas seguros	Porcentaje de Sistemas de Información que cumplen las políticas de seguridad	=% de SI que cumplen las políticas de seguridad/ N° total de sistemas de información en uso	Porcentaje
A.14.2.6	Ambiente de desarrollo seguro								
A.14.2.2 **A.14.2.3** **A.14.2.4**	Procedimientos de control de cambios en sistemas Revisión técnica de las aplicaciones después de cambios en la plataforma de operación Restricciones en los cambios a los paquetes de software	Cumplimiento en cambios	Desviación fechas de entrega de desarrollos de software	Resultado	mensual	Herramienta de gestión de desarrollo de software	Desviación fechas de entrega de desarrollos de software	= N° de cambios entregados en la fecha acordada / N° total de cambios del mes	Porcentaje
		Productividad en cambios	# Desarrollos terminados/ # Desarrollos Planeados	Resultado	mensual	Herramienta de gestión de desarrollo de software	# Desarrollos terminados/ # Desarrollos Planeados	= Promedio de diferencia entre el esfuerzo real y el esfuerzo planeado por mes	valor
		Documentación de cambios a SI	Numero de cambios documentados	Proceso	semestral	P-SIS-016 Procedimiento de cambios a sistemas de Información	Numero de cambios documentados	= Cambios que cumplen procedimiento/ Total de cambios del semestre	Porcentaje
A.14.2.7	Desarrollo contratado externamente	Calidad cambios de terceros	# Desarrollos terminados a satisfacción/ # Desarrollos Planeados con terceros	Resultado	Por demanda	Contrato P-SIS-018 Procedimiento de Pruebas a los sistemas	Calidad cambios de terceros	= N° Desarrollos con 0 defectos / Total de desarrollos de cada tercero	Porcentaje
		Cumplimiento cambios de terceros	Estadística de cumplimiento de criterios de aceptación de entregables por cada proveedor	Resultado	Por demanda	Contrato R-SIS-027, R-SIS-028	Cumplimiento cambios de terceros	= N° Entregables cumplen los criterios / Total de entregables de cada tercero	Porcentaje
A.14.2.8	Pruebas de seguridad de sistemas								
A.14.2.9	Pruebas de aceptación de sistemas	Calidad cambios Internos	Cumplimiento de los niveles de tolerancia en defectos de software por desarrollador y por criticidad de defectos	Resultado	mensual	Herramienta de gestión de desarrollo de software	calidad en el desarrollo de software	= N° defectos del sprint por desarrollador/ # defectos tolerables por criticidad	Porcentaje

Fuente: Elaboración propia

Vale aclarar que los indicadores del MSPI van más allá del cumplimiento de actividades, toda vez que su propósito es "medir" no solo el avance en la implementación sino el nivel de efectividad de los controles establecidos.

6.2.2. PRACTICAS DE CONFIABILIDAD, INTEGRIDAD Y SEGURIDAD DE LA INFORMACION

6.2.2.1. FORTALEZAS Y OPORTUNIDADES DE MEJORA

6.2.2.1.1. ELEMENTOS DE PROTECCIÓN DE RED

La Secretaría cuenta con los siguientes esquemas: esquema de red local (LAN) y esquema de red WAN, de acuerdo con el Plan Estratégico de Tecnologías de la Información de TI - PETI 2020-2024 de la Oficina asesora de planeación sobre el cual se emiten observaciones:

Imagen 22

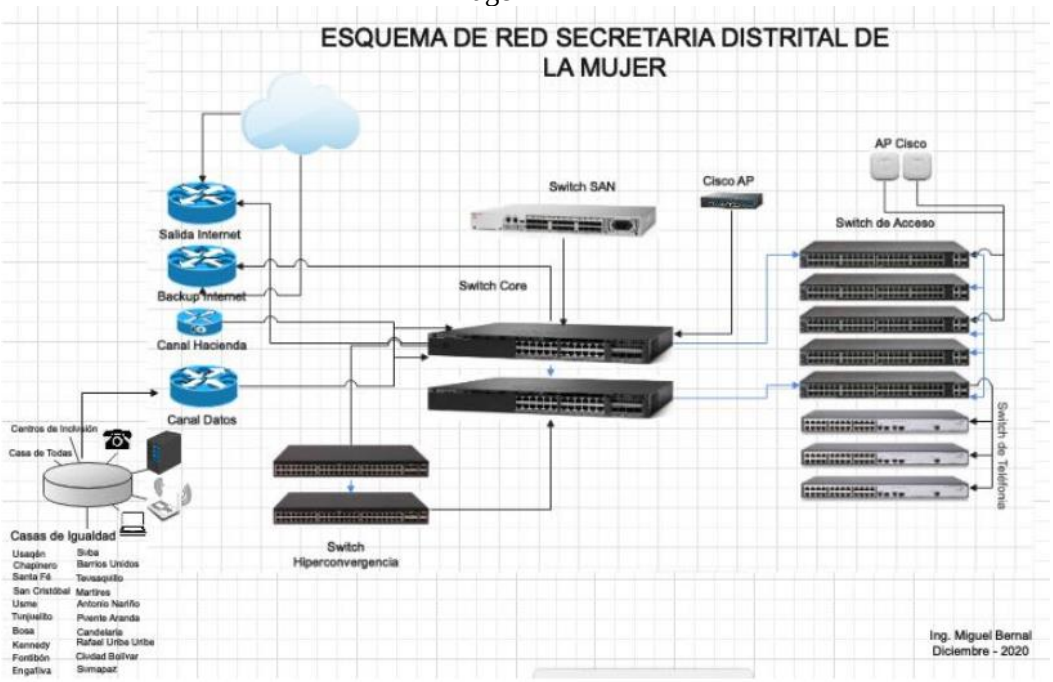
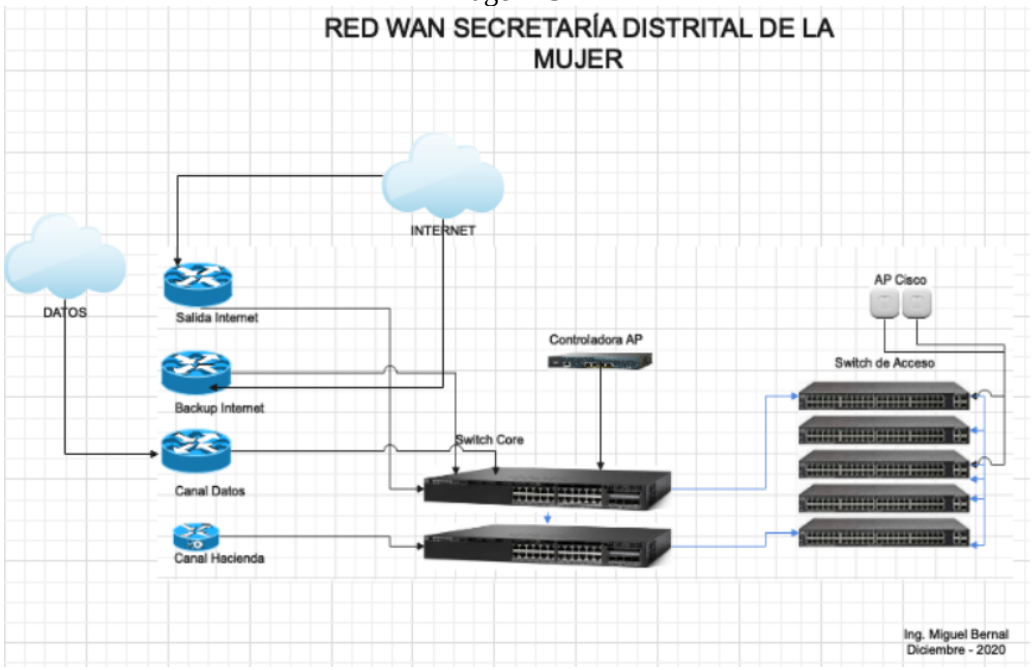


Imagen 23



👉 Es importante tener en cuenta que estos esquemas sirven para visualizar de forma general la infraestructura y pueden ser utilizados para la documentación pública, sin embargo, se debe contar con una versión "reservada" de estos esquemas para la OAP en la cual se relacionen y se puedan identificar detalladamente los rangos de direcciones IpV4 y las equivalencias de IPv6, tanto de servidores como de los segmentos de red configurados

(incluyendo los de WIFI). Además, que permita identificar los equipos de DHCP y DNS, y elementos de contingencia, entre otros. El objetivo de este diagrama es permitir a actuales y nuevos funcionarios del área, a proveedores y a contratistas, conocer en un único documento la disposición y arquitectura de la infraestructura TIC de la entidad, que sirva como para disminuir la dependencia de conocimiento de los encargados de la administración y mantenimiento de la infraestructura de TI.


Como se puede observar en los esquemas de red, no se cuenta con equipos de protección para la seguridad perimetral (Firewall), que permitan controlar de forma adecuada el tráfico entre la red pública - internet y la red local (LAN) de la Secretaría, por tanto, no se cuenta tampoco, con un sistema de detección de intrusos, de escaneo de capas de red, de controles de navegación de internet, entre otros sistemas de monitoreo centralizados incluidos en los firewalls. Al no contar con estos equipos la entidad se encuentra expuesta a sufrir ataques externos. Vale aclarara que en el marco del contrato con SOLUCIONES TECNOLOGIA Y SERVICIOS SA suscrito el 29 de octubre del 2021 se ha adquirido una solución de seguridad perimetral, pero al momento de la auditoria no estaba implementada.


La OAP ya suscribió el contrato de compraventa No. 877 de 2021 celebrado entre La Secretaría Distrital de la Mujer y Soluciones Tecnología y Servicios S.A. para la adquisición e implementación de la solución de seguridad perimetral de la entidad, en el cual se establecieron de forma adecuada en su anexo técnico las especificaciones y características necesarias para la solución, se incluyen correctamente las actividades de análisis de vulnerabilidades antes y después de la implementación y las sesiones de transferencia de conocimiento.


Con respecto a la implementación del protocolo IPv6 en atención a los lineamientos emitidos por MINTIC mediante Resolución 2710 del 2017, la OAP ejecutó el contrato para la adquisición e implementación de rango de direccionamiento IPv6 en modalidad de doble pila de protocolos (Dual Stack), en el cual se realizaron de forma adecuada las acciones necesarias para su implementación.


Los accesos remotos por red privada virtual (VPN), se configuran directamente en el enrutador (Router) del proveedor de acceso a internet (ETB) mediante peticiones vía correo electrónico. El proveedor es el encargado de habilitar estás conexiones configurando listas de control de acceso (ACL's) por usuario en el enrutador y permitiendo el acceso externo a la red local, únicamente a las direcciones IP necesarias para su trabajo y por puertos específicos, como se observa en la siguiente imagen (configuración router) para los usuarios ADIAZ, DDIAZ y FBRAVO:

Si bien esta configuración cumple con su objetivo, no es la mejor práctica, ya que no permite tener autonomía en la generación de las mismas, y debido a no contar con un firewall, no se pueden tener un control y monitoreo adecuado sobre estas conexiones, tampoco se pueden configurar restricciones, filtros y condiciones adicionales para garantizar que las conexiones sean seguras y que los equipos desde los que se conectan estos usuarios cumplan con las condiciones de seguridad necesaria.

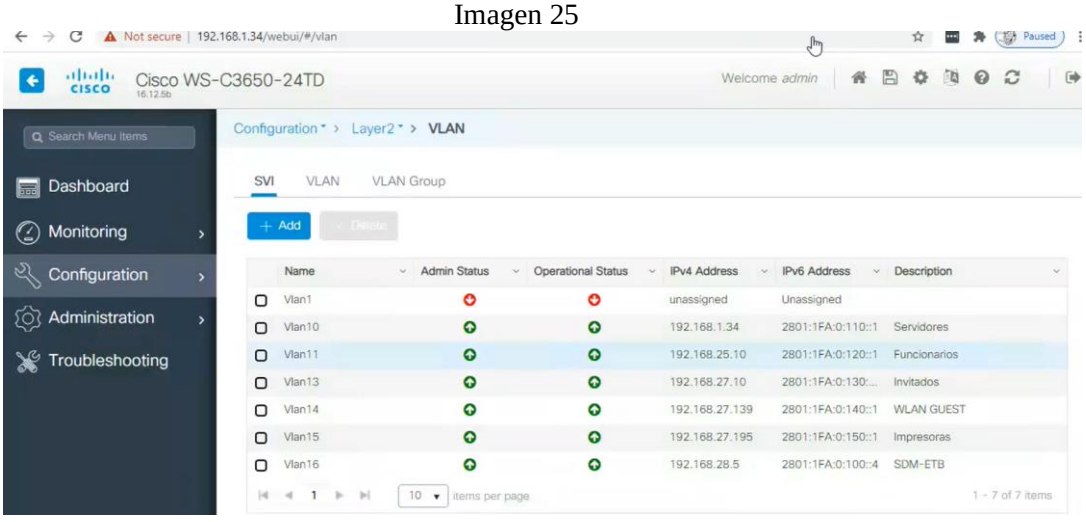
Imagen 24

```
ip ssh authentication-retries 2
ip ssh port 2222 rotary 1
ip ssh version 2
!
!
ip access-list extended ACL_ADIAZ
 permit ip host 192.168.1.23 192.169.8.0 0.0.0.255
 permit ip host 192.168.1.73 192.169.8.0 0.0.0.255
ip access-list extended ACL_DBSYSTEM
 permit ip host 192.168.1.9 192.169.14.0 0.0.0.255
ip access-list extended ACL_DDIAZ
 permit ip host 192.168.1.43 192.169.20.0 0.0.0.255
 permit ip host 192.168.1.22 192.169.20.0 0.0.0.255
 permit ip host 192.168.1.41 192.169.20.0 0.0.0.255
 permit ip host 192.168.1.23 192.169.20.0 0.0.0.255
 permit ip host 192.168.1.42 192.169.20.0 0.0.0.255
 permit ip host 192.168.1.70 192.169.20.0 0.0.0.255
 permit ip host 192.168.1.25 192.169.20.0 0.0.0.255
 permit ip host 192.168.1.74 192.169.20.0 0.0.0.255
 permit ip host 192.168.1.40 192.169.20.0 0.0.0.255
 permit ip host 192.168.1.75 192.169.20.0 0.0.0.255
 permit ip host 192.168.1.73 192.169.20.0 0.0.0.255
ip access-list extended ACL_FBRAVO
 permit ip host 192.168.1.18 192.169.12.0 0.0.0.255
 permit ip host 192.168.1.20 192.169.12.0 0.0.0.255
 permit ip host 192.168.1.25 192.169.12.0 0.0.0.255
 permit ip host 192.168.1.10 192.169.12.0 0.0.0.255
```

👉 Se cuenta con una hoja de Excel: *"Usuarios VPN.xlsx"*, en la cual se lleva el control de los usuarios que tiene acceso por VPN a la red local de la Secretaría, a que equipos y servicios se les permite este acceso. Se tienen relacionados 12 usuarios activos y 2 deshabilitados, 1 usuarios de la Dirección Administrativa y Financiera, 5 de la Oficina Asesora de Planeación – Gestión tecnológica, y 6 de la Dirección de Gestión del Conocimiento. Al no tener aún el firewall esta práctica es alternativa, pero al ser manual pueden presentarse errores de actualización o de digitación que no se reflejen necesariamente en la configuración actual en el enrutador del proveedor. Esto se resuelve con la implementación del firewall.

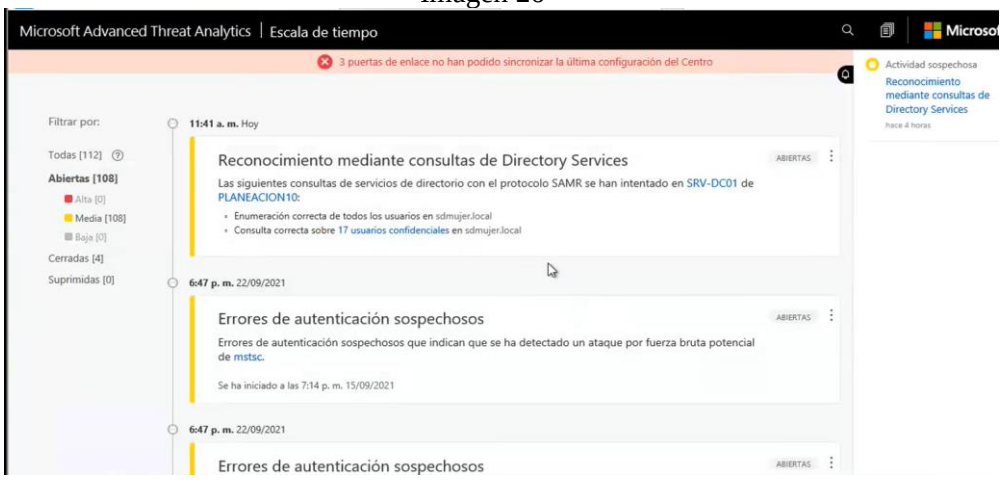
👎 Si bien, la red local (LAN) de la Secretaría se encuentra segmentada en VLAN's, y se tiene configurado un segmento para la red inalámbrica (192.168.27.x) y otro para servidores (192.168.1.x), como se muestra en la siguiente imagen, estos segmentos no se encuentran correctamente configurados para restringir escaneos de un segmento de red a otro, como se muestra en las evidencias de las pruebas de seguridad internas realizada y registradas en el numeral 6.2.2.1.2 de este documento. Cabe anotar que el auditor uso el acceso inalámbrico que se habilito en su equipo portátil.

Imagen 25



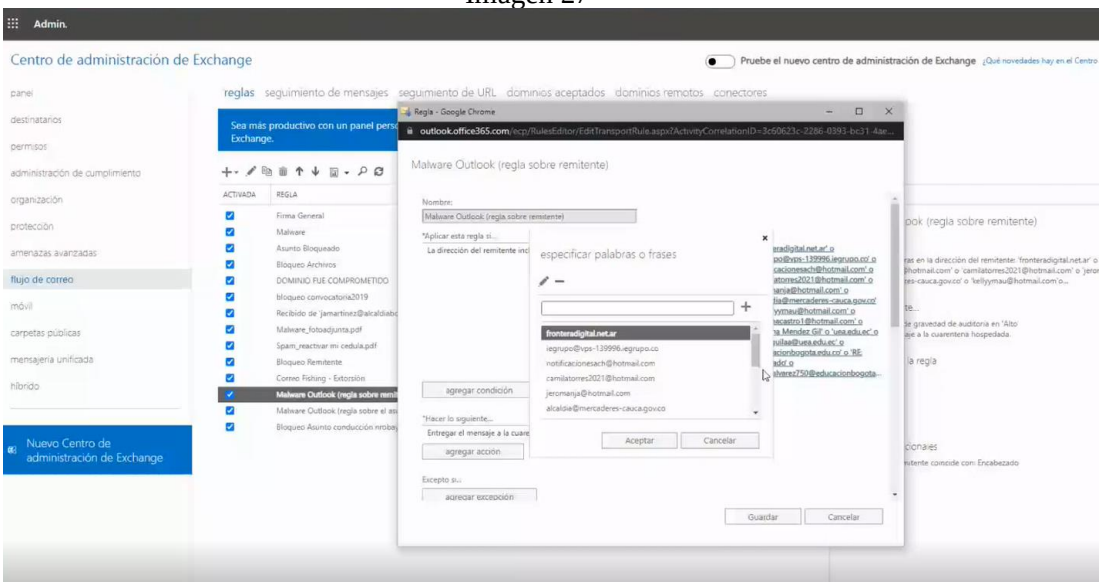
Se encuentra implementada la herramienta Microsoft Advanced Threat Analytics (ATA), que sirve para monitorear y detectar comportamientos sospechosos de los usuarios que acceden a la red (Windows), para prevenir y detectar posibles ataques a la infraestructura, en esta herramienta se puede hacer seguimiento a los usuarios del dominio de Windows y perfilar su comportamiento, en la imagen se muestra la escala de tiempo de actividades sospechosas:

Imagen 26



Se encuentran correctamente configuradas las protecciones para spam, phishing y software malicioso para los correos entrantes a la Entidad y se controla de forma adecuada desde la consola del centro de administración de Exchange las notificaciones de incidentes de seguridad que reporta el equipo de respuesta a incidentes de seguridad informática – CSIRT creando reglas y filtros para los correos entrantes y salientes para bloquearlos, como se ve en la siguiente imagen:

Imagen 27



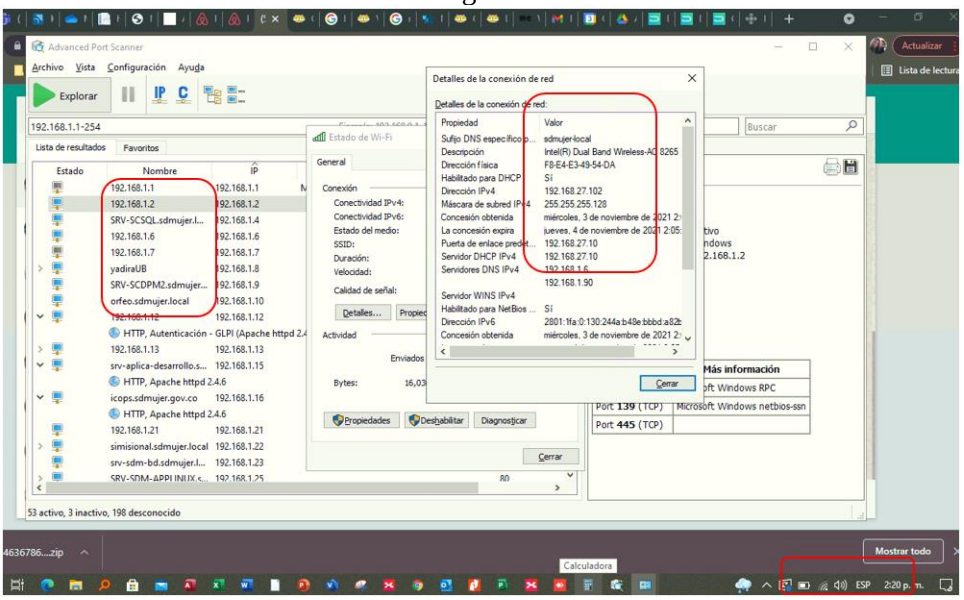
La configuración de red y de la asignación automática de direcciones (DHCP) no tiene configuradas restricciones para evitar la conexión de equipos con direcciones de tarjetas de red (Mac Address) no autorizadas, ya que asigna direcciones IP automáticas en los segmentos de red a cualquier equipo que se conecte, lo cual permitió al auditor conectar su equipo personal a un punto de red y obtener información para realizar posibles ataques aprovechando la configuración de su tarjeta de red como equipo de red local y los programas instalados en su equipo, lo cual se evidencia en las pruebas realizadas (6.2.2.1.2).

En los equipos de funcionarios que tiene tarjeta de red física e inalámbrica no se tienen restricciones para que se conecten únicamente a redes controladas y seguras, un funcionario podría conectarse a la red de datos de su celular y así evadir los controles que se implementen para la navegación por internet en la red local y comprometer la seguridad del equipo.

6.2.2.1.2. PRUEBAS DE SEGURIDAD INTERNAS

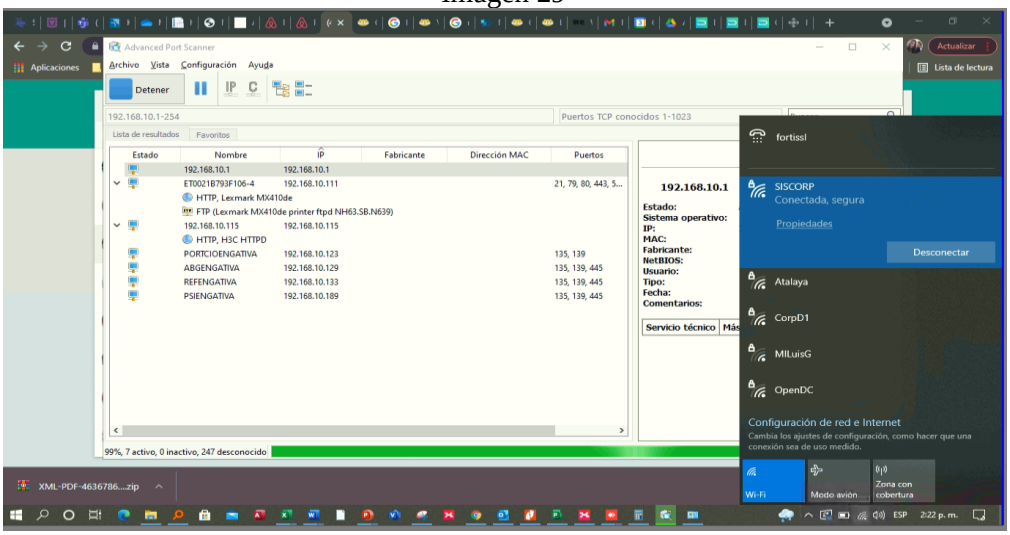
En las pruebas de seguridad realizadas por el auditor se evidencia que es posible realizar escaneos y búsqueda de objetivos desde cualquier segmento de red hacia cualquiera de los otros segmentos, incluyendo el de servidores, tal como se observa en las siguientes imágenes en donde, estando el equipo del auditor conectado al segmento de la VLAN inalámbrica, el auditor pudo escanear la VLAN de los servidores (segmento 192.168.1.x), y de todos los otros segmento de la red de la Secretaría, enumerando los puertos abiertos, sistemas y recursos de cada equipo, servidores y equipos de la red local, esta información es utilizada por los atacantes para planificar diferentes ataques, como de fuerza bruta para descubrir contraseñas, identificar recursos sin protección, ataques de captura de paquetes de red, etc., que no serían detectados, ni bloqueados al no tener una protección en la seguridad perimetral adecuada:

Imagen 28



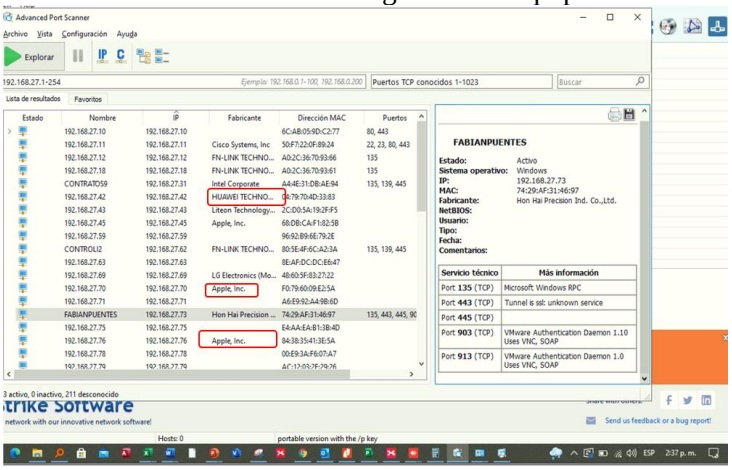
En la imagen se evidencia el escaneo hacia otros segmentos desde la red inalámbrica, caso CIOENGATIVA que están en el segmento 192.168.10.x, esto arroja información de las asignaciones a cada casa de igualdad (puertos abiertos y posibles recursos para explotarlos):

Imagen 29



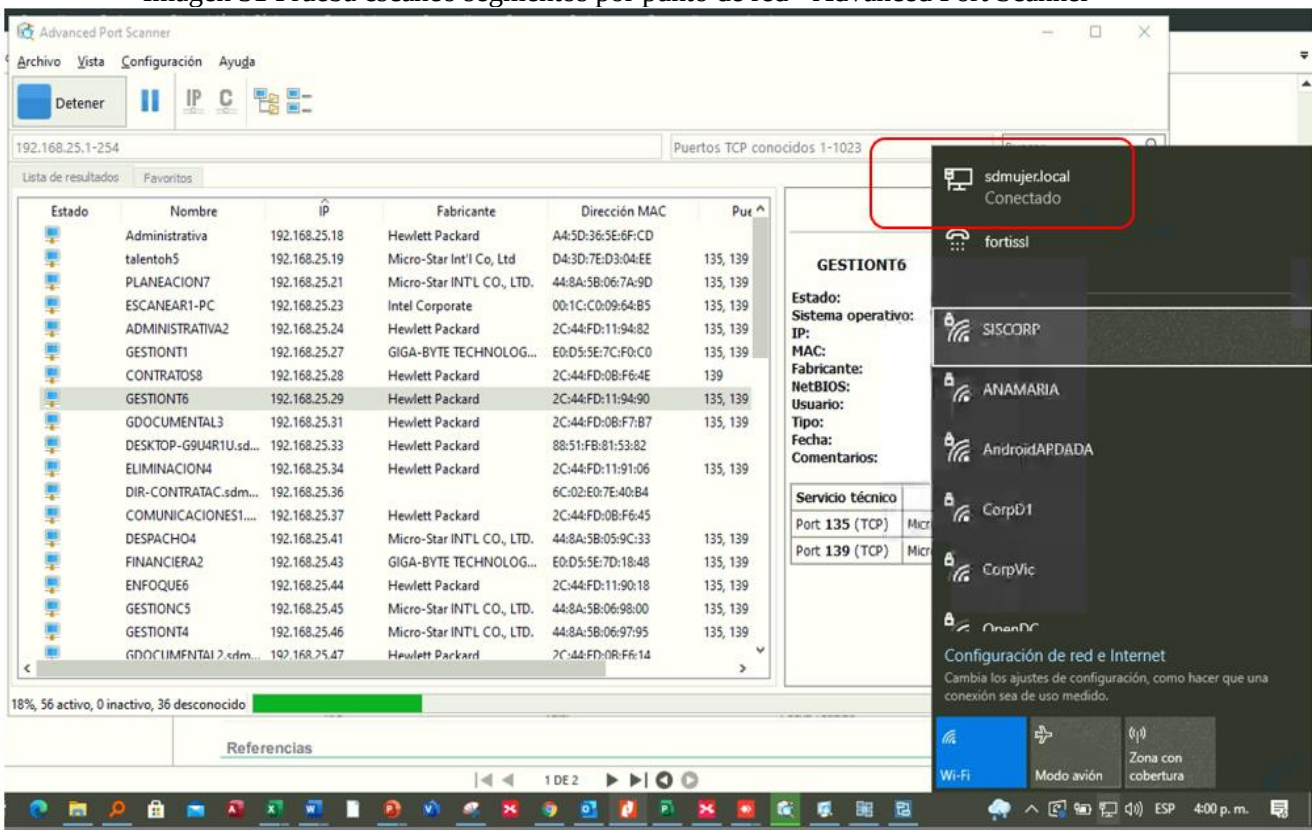
También se puede evidenciar la coexistencia de equipo asignados a funcionarios con celulares conectados a la red inalámbrica, estos celulares al no ser equipos controlados, ni con garantías de seguridad adecuada, exponen a la red local a posibles ataques por malware o virus instalados en estos equipos. En la imagen se muestran equipos móviles Apple y Huawei conectados en el mismo segmento de los equipos de usuarios: CONTRATOS9, CONTROLI2 y el equipo de FABIAN PUENTES, su enumeración de puertos abiertos y de las direcciones MAC de los dispositivos. La red inalámbrica debe estar aparte y más si voy a permitir conectarse a la red desde celulares, dado que actualmente existen herramientas de scaneo y explotación de vulnerabilidades para celulares:

Imagen 30 Prueba celulares conectados al mismo segmento de equipos - Advanced Port Scanner



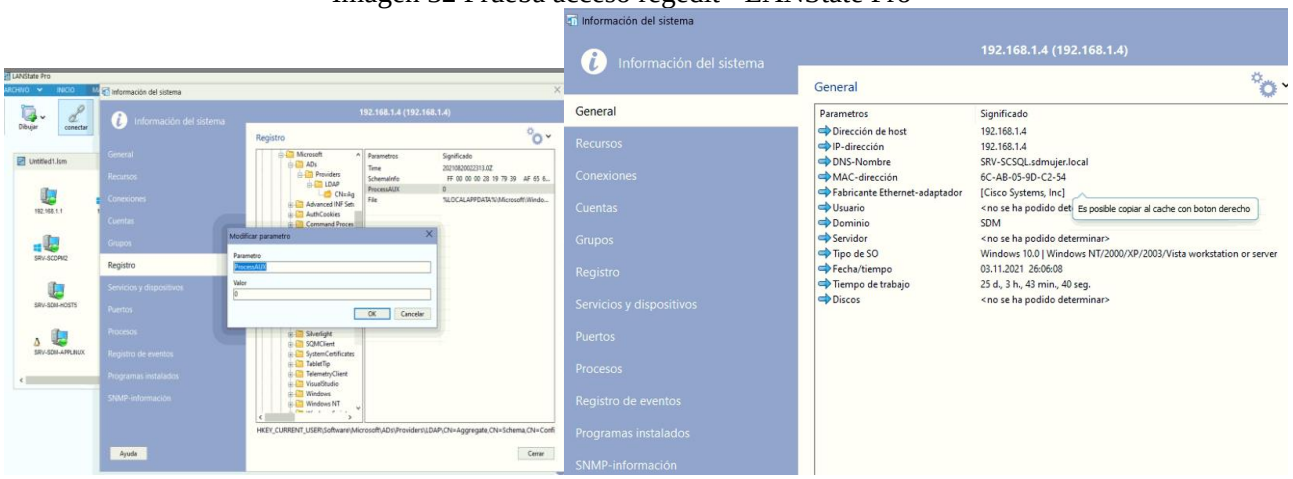
En las pruebas de seguridad sobre puntos no atendidos de red, es decir aquellos puntos a los cuales un invitado o un posible atacante con su propio cable, pueda conectar su equipo y tener acceso a la red, se evidencia que no se tiene un control adecuado sobre estos puntos, ya que al conectar el equipo portátil del auditor, automáticamente se le asigno una dirección IP dentro del segmento de red de funcionarios de la Secretaría, y por lo descrito en los puntos anteriores tener acceso a los otros segmentos, incluyendo al de servidores. La principal amenaza en esta debilidad es que un equipo que se conecte de esta manera puede tener instalado software utilizado por los atacantes (Hackers) para realizar capturas de paquetes de red (snnifers), identificación de vulnerabilidades y/o malware entre otros, para ejecutar ataques a la infraestructura. En la siguiente imagen se puede ver, el escaneo de red realizado por el auditor desde su portátil conectado a un punto de red de la entidad y acceso al dominio: ***sdmujer.local***, identificando los equipos, puertos, direcciones de tarjeta de red y recursos de los mismos:

Imagen 31 Prueba escaneo segmentos por punto de red - Advanced Port Scanner



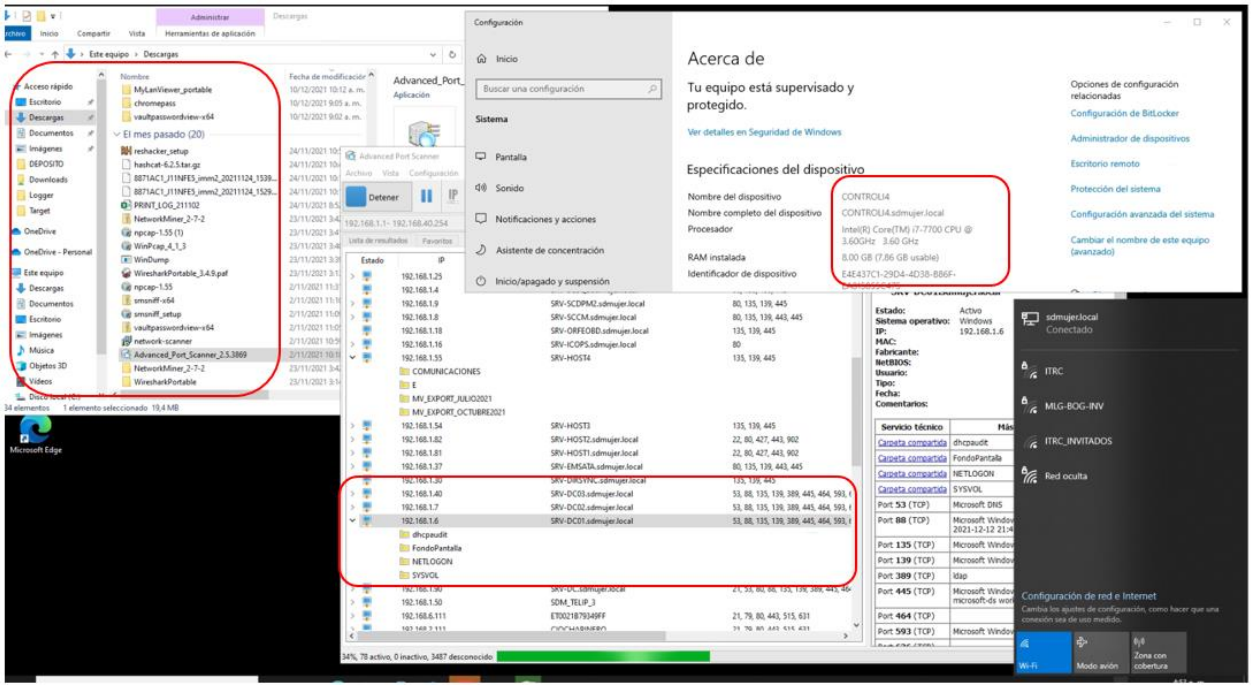
En la siguiente imagen se muestra la ejecución de un software (LANState Pro) de descubrimiento de recurso, usuarios, acceso al registro de equipos, enumeración de usuarios, entre otros, instalado en el equipo del auditor, con el cual logro obtener acceso al registro de Windows (Regedit) del servidor 192.168.1.4 (SRV-SCSQL.sdmujer.local), enumerar los recursos de cada equipo y/o servidor para encontrar posibles recursos sin la debida protección:

Imagen 32 Prueba acceso regedit - LANState Pro



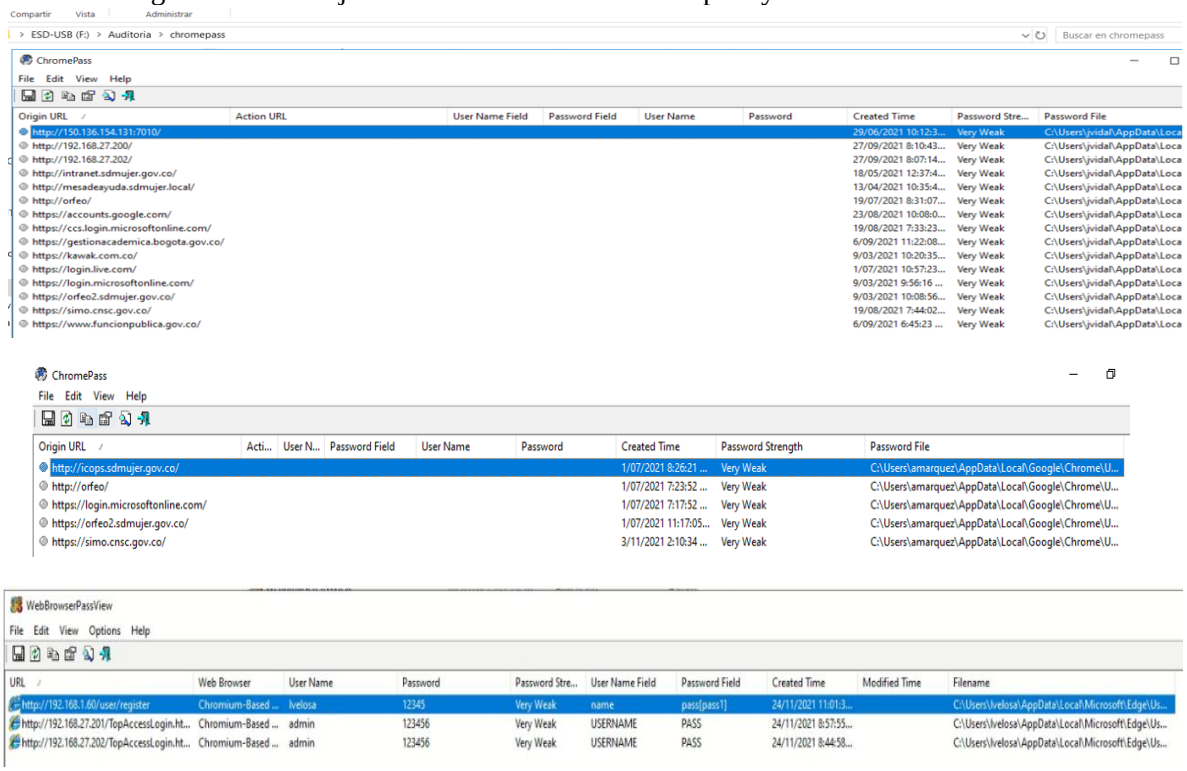
En las pruebas de seguridad realizadas en los equipos de funcionarios, y en el asignado al auditor, también se encontraron las debilidades ya mencionadas en cuanto al escaneo de VLAN's, al descubrimiento de recursos, puertos. Estas pruebas se realizaron debido a que no existe restricción de descargas de archivos ejecutables y/o portables, de esta forma el auditor logro descargar varios programas portables que al ejecutarse permiten realizar este tipo de escaneos, como se evidencia en la siguiente imagen:

Imagen 33 Prueba Descarga de software portable y peligroso en equipo asignado al auditor



Cabe anotar que si bien en los equipos de usuarios, existe la restricción de instalación de software por parte de los usuarios sin privilegios administrativos, y que algunas herramientas portables no se pudieron ejecutar, varias se lograron ejecutar sin ningún problema como se evidencia en las siguientes imágenes, que muestran la ejecución de herramientas portables para el descubrimiento de contraseñas (Chromepass y WebBrowserPassview) desde la USB del auditor en los equipos de funcionarios: CONTROLI5, DIR-CINTERNO y CONTROLI4:

Imagen 34 Prueba ejecuciones desde USB Chromepass y WebBrowserPassview

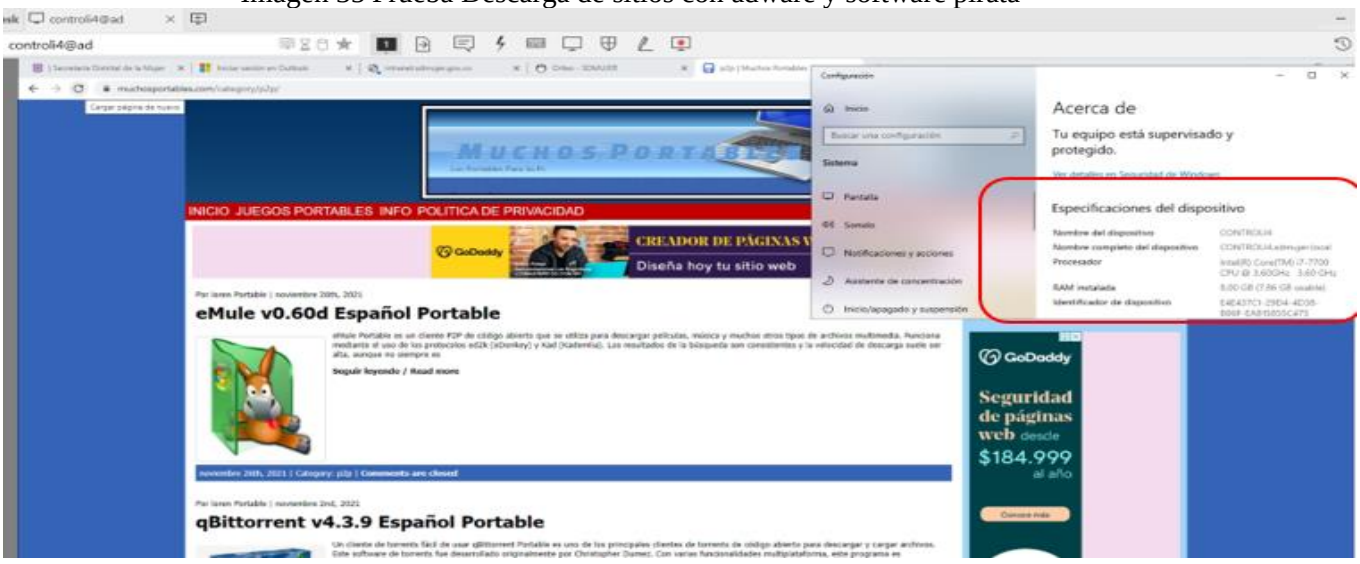


En la última imagen se puede ver que se permite guardar contraseñas planas en los navegadores, caso 192.168.27.201 – impresora con usuario Admin y contraseña: 123456.

También se evidencia que los controles de navegación en internet no están implementados de forma adecuada o en su totalidad, ya que en el equipo asignado para la auditoria se logró descargar software considerado como pirata o peligroso, además de navegar sobre sitios con software malicioso publicitario (adware: lanza ventanas emergentes para lograr la descarga), sitios de juegos en línea, de citas en línea y de contenido pornográfico, como se aprecia en las siguientes imágenes:

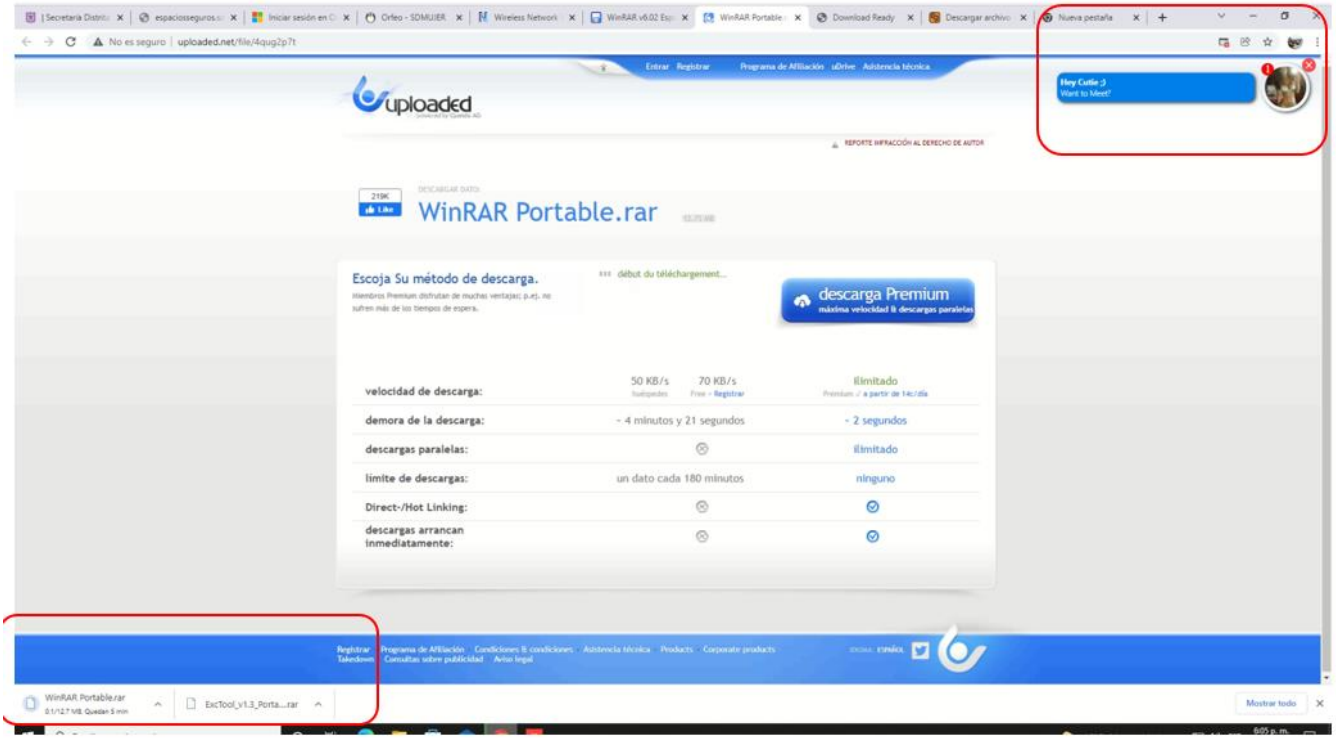
Descarga de archivos portables para descarga de software pirata (ejemplo eMule y qBittorrent para descargar películas piratas y otro tipo de software):

Imagen 35 Prueba Descarga de sitios con adware y software pirata



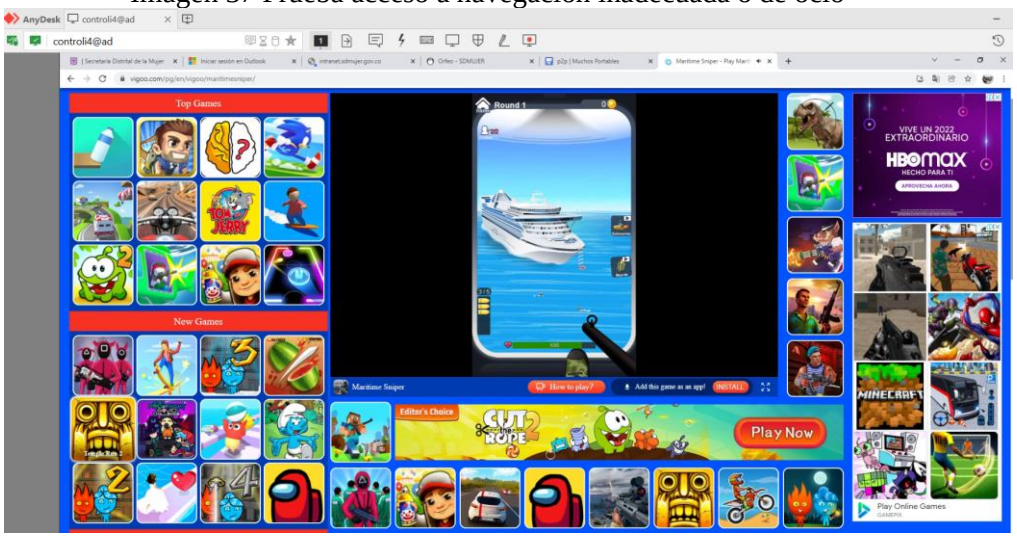
Descarga de sitios con adware y software pirata:

Imagen 36 Prueba Descarga de software pirata



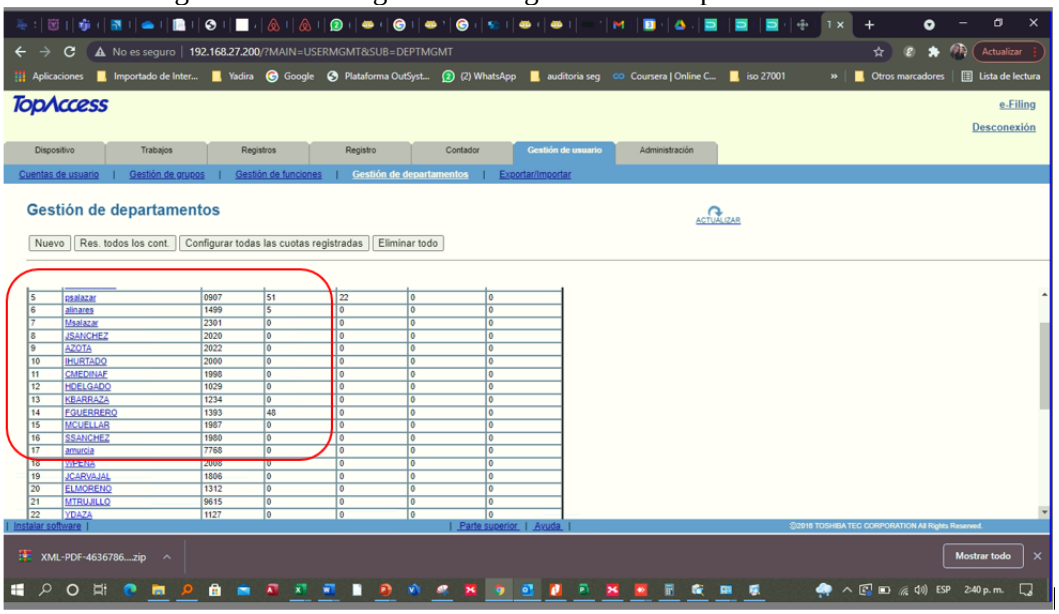
Sitios de Juego on line:

Imagen 37 Prueba acceso a navegación inadecuada o de ocio



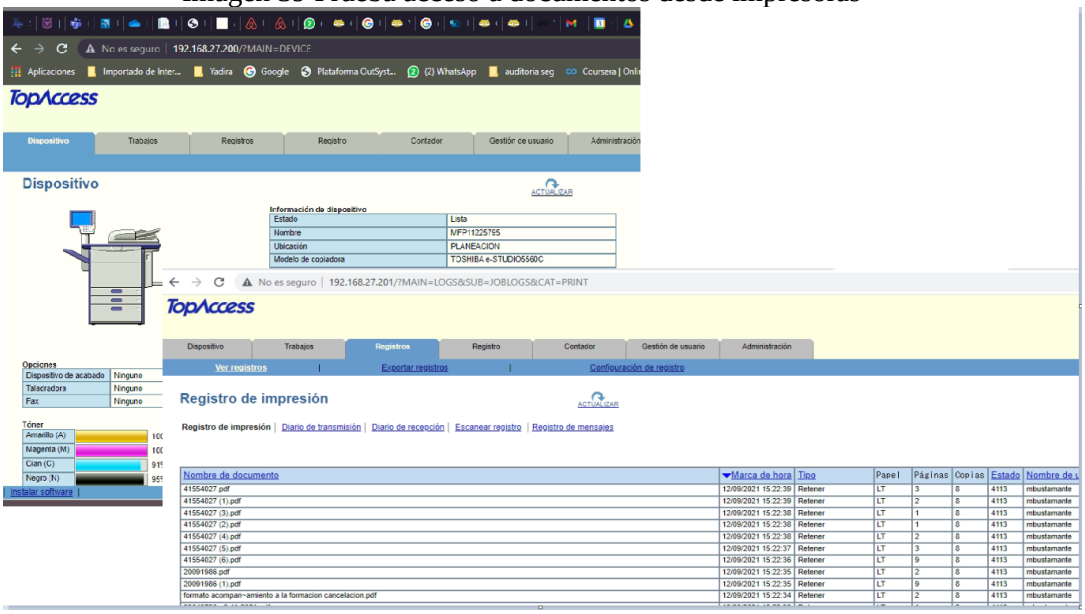
Debido al análisis anterior el auditor logro detectar vulnerabilidades e ingresar a varios elementos activos de red y recursos sin protección. En las siguientes imágenes se evidencia el ingreso del auditor a la configuración de impresoras de red, las cuales aún están con el usuario y contraseña de fabrica: *Usuario: Admin* y *contraseña:123456*, estos accesos a configuraciones de impresoras permiten a los atacantes crear y conocer pin de usuarios, manipular información o adjuntar scripts para capturar las impresiones y enviarlas a correos personales del atacante:

Imagen 38 Prueba ingreso a configuración de impresoras de red



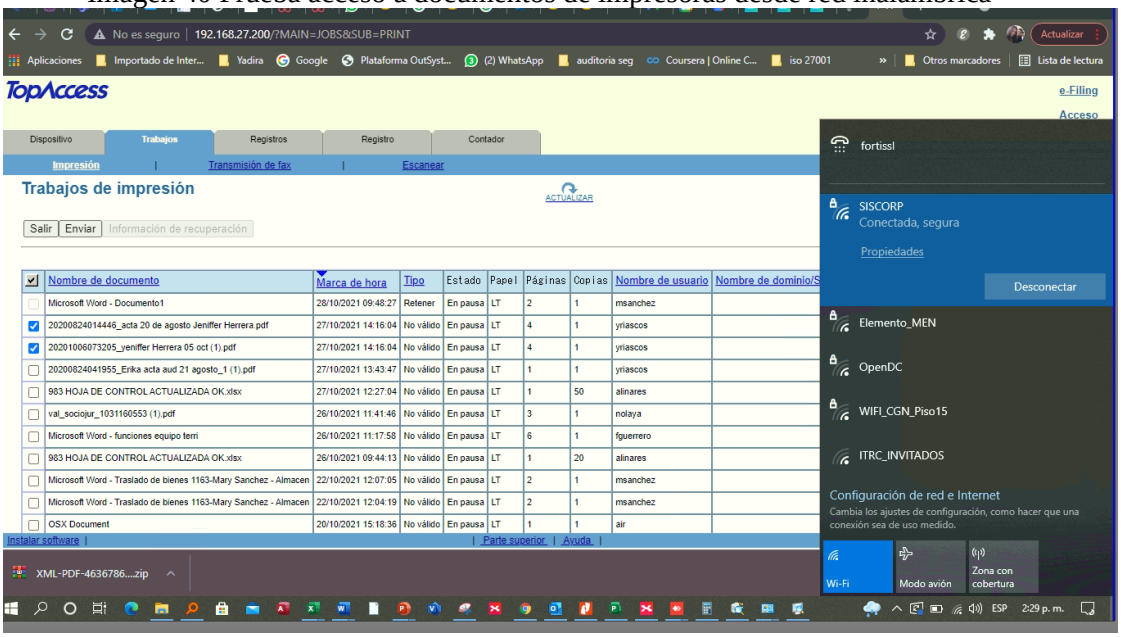
En las imágenes se muestran solo dos de las impresoras capturadas, pero en las pruebas todas las impresoras Toshiba estaban con esta vulnerabilidad. Vale aclarar que en la configuración de la impresora se pueden implantar scripts para direccionar documentos a correos.

Imagen 39 Prueba acceso a documentos desde impresoras



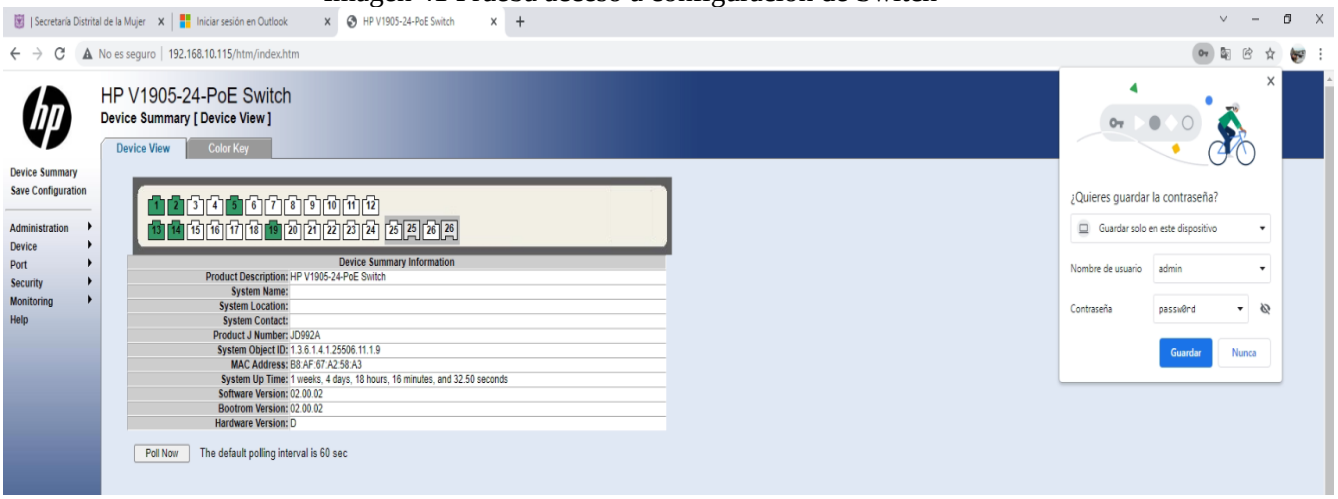
En la siguiente imagen se observa que también se puede hacer conectado desde la inalámbrica.

Imagen 40 Prueba acceso a documentos de impresoras desde red inalámbrica



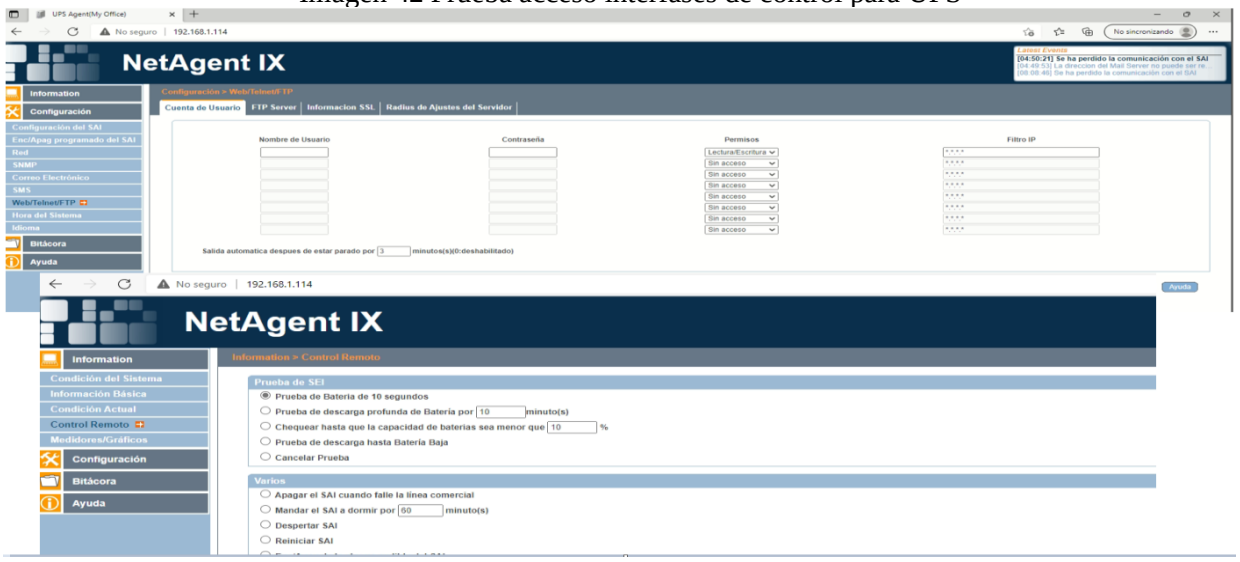
Se encontraron elementos activos de red como switches con el usuario y contraseña de fábrica. En la siguiente imagen se muestra como el auditor tuvo acceso a la configuración del switch (192.168.10.115) de la CIO Engativá con el usuario: *admin* y contraseña: *passw0rd*, un atacante podría aprovechar esta vulnerabilidad para configurar accesos no permitidos a la red o para modificar interfaces y habilitar puertos para mantener estos accesos y de ahí escalar a otro tipo de ataques que comprometan la infraestructura de TI de la Secretaría.

Imagen 41 Prueba acceso a configuración de Switch



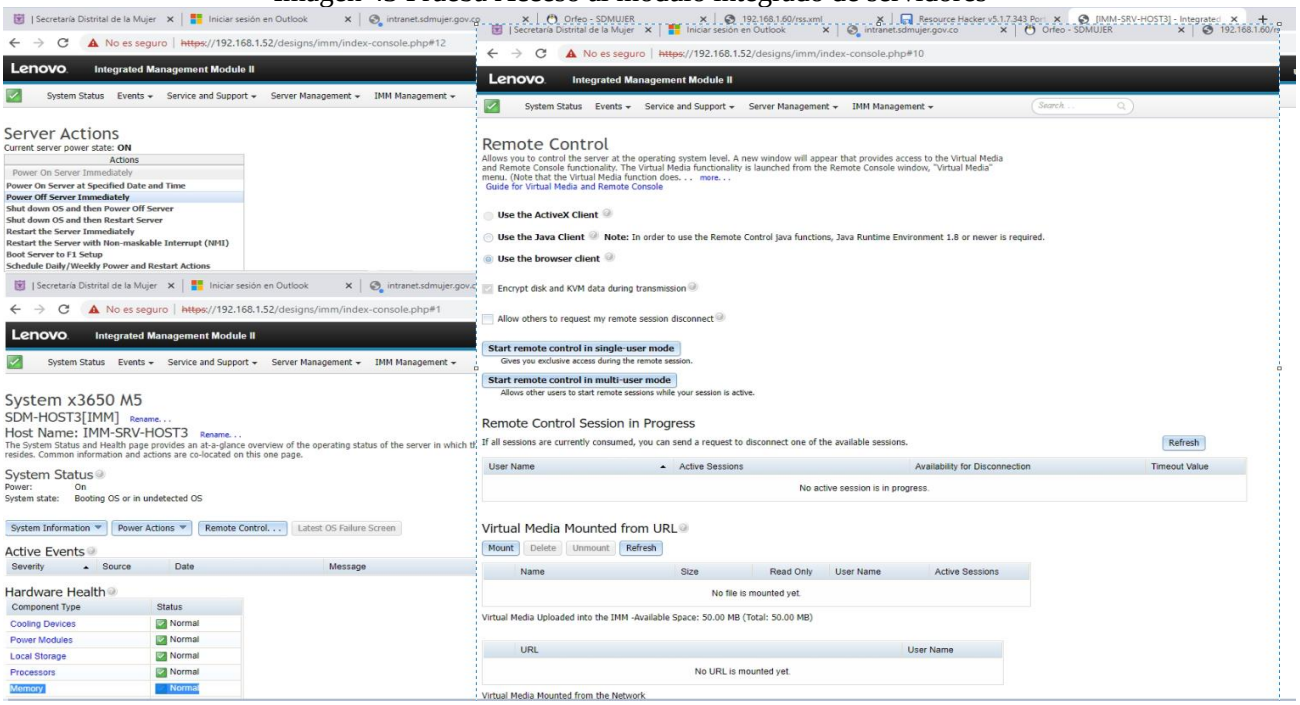
También se encontraron sin protección de usuario y contraseña las interfaces de control para la UPS – SAI, como se muestra en la imagen, a través de lo cual podría apagarse o mandar el SAI a dormir. Como tiene ftp server se podría subir scripts:

Imagen 42 Prueba acceso interfases de control para UPS



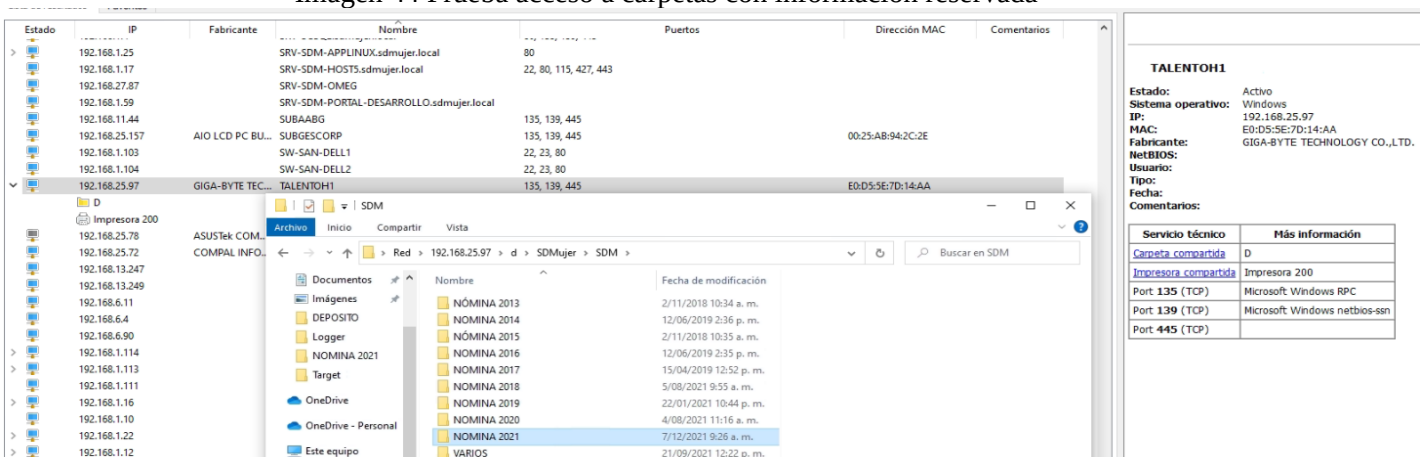
La consola de IBM / Lenovo IMM (Módulo de gestión integrado de servidores), se encuentra con la configuración de usuario (USERID) y contraseña por defecto (PASSW0RD), un atacante podría tener control sobre estos servidores y ejecutar ataques de diferentes tipos, como denegación de servicios ya que puede apagar remotamente el módulo de los servidores, cargas líneas de ejecución de comandos (scripts) entre otros, como se ve en la siguiente imagen:

Imagen 43 Prueba Acceso al módulo integrado de servidores



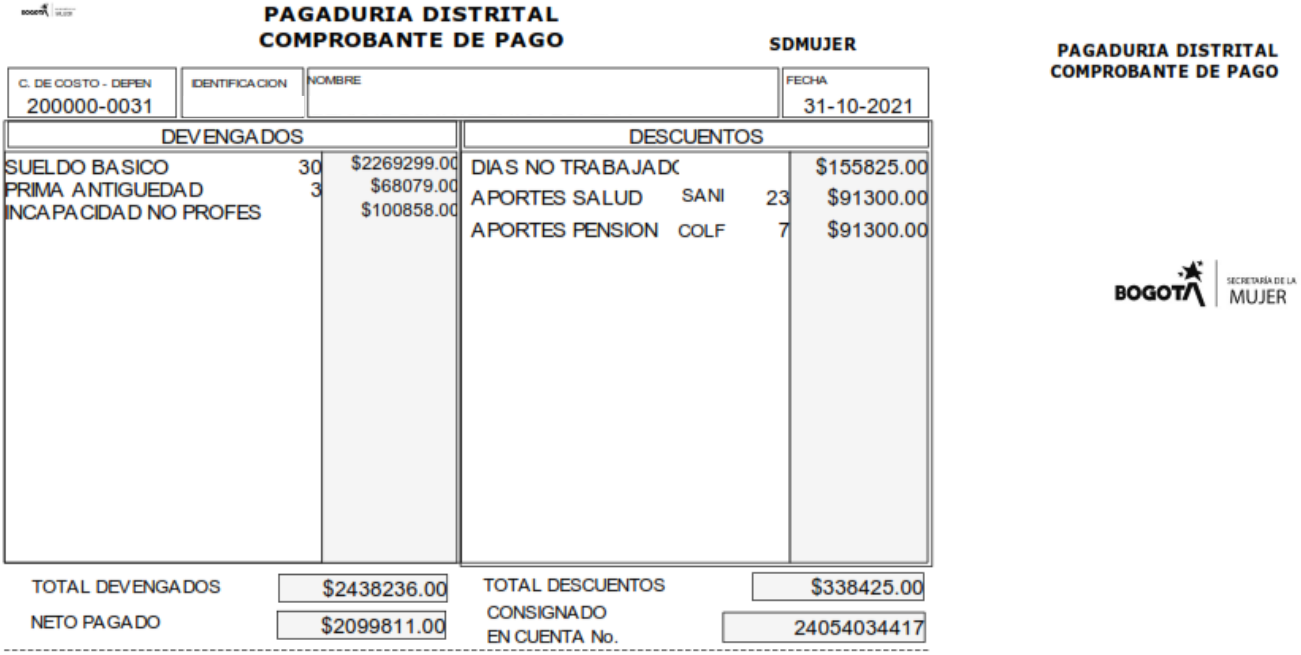
Se encontraron varios recursos o carpetas compartidas sin la debida protección, el auditor capturo varios documentos, imágenes de discos duros de servidores, backups de usuarios, archivos planos y desprendibles de nómina entre otros, como se puede ver en las siguientes imágenes, cabe anotar que un atacante podría utilizar esta información para fraudes monetarios en el caso de los archivos planos de nómina, además de tener información financiera de los funcionarios, en la siguiente imagen se muestra la unidad “d:\” del equipo:TALENTOH1, que se encuentra compartida sin protección en la red y que contiene la información de las nóminas:

Imagen 44 Prueba acceso a carpetas con información reservada



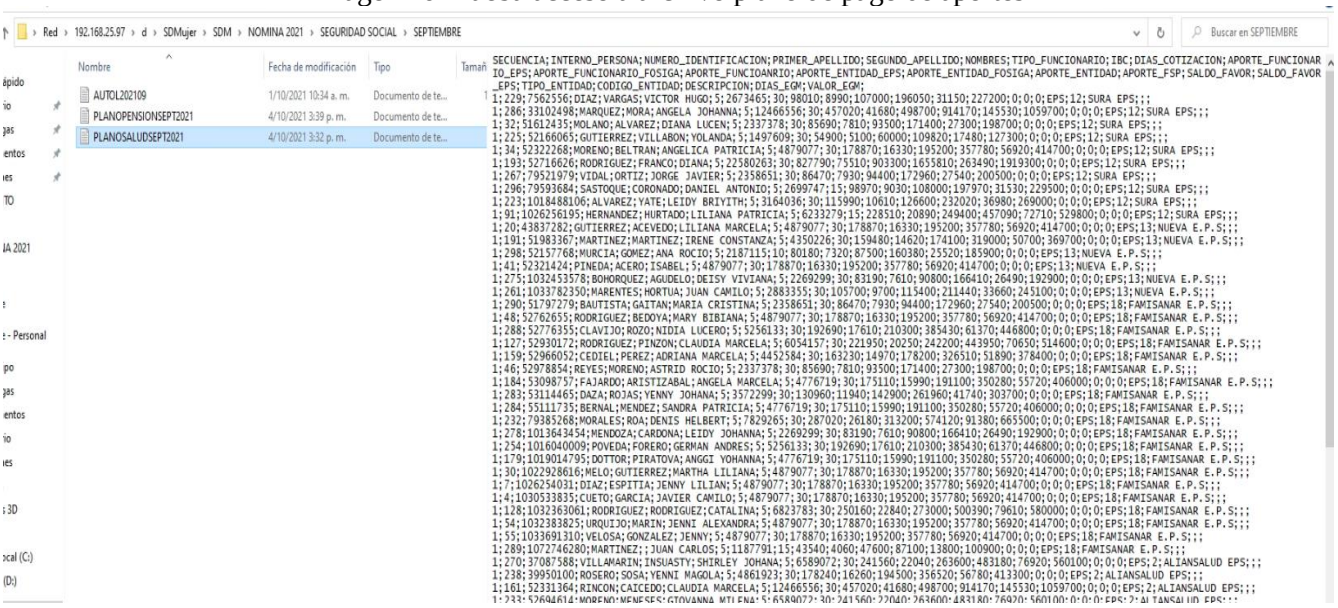
- Evidencia desprendibles de nómina:

Imagen 45 Prueba acceso a desprendibles de nomina



-Evidencia Archivo plano de aportes – sept 2021, modificables:

Imagen 46 Prueba acceso a archivo plano de pago de aportes



-Evidencia Certificados de ingresos y retenciones de funcionarios:

Imagen 47 Prueba acceso a certificados de ingresos y retenciones funcionarios

REPUBLICA DE COLOMBIA
DIAN

Certificado de Ingresos y Retenciones para Personas Naturales Empleados Año Gravable 2020

220

4. Número de Formulario

Retenedor

5. Número de Identificación Tributaria (NIT): 899999061 — 6. DV. 7. Primer apellido 8.Segundo apellido 9.Primer Nombre 10. Otros nombres

11 Razon Social: SECRETARIA DISTRITAL DE LA MUJER

Empleado

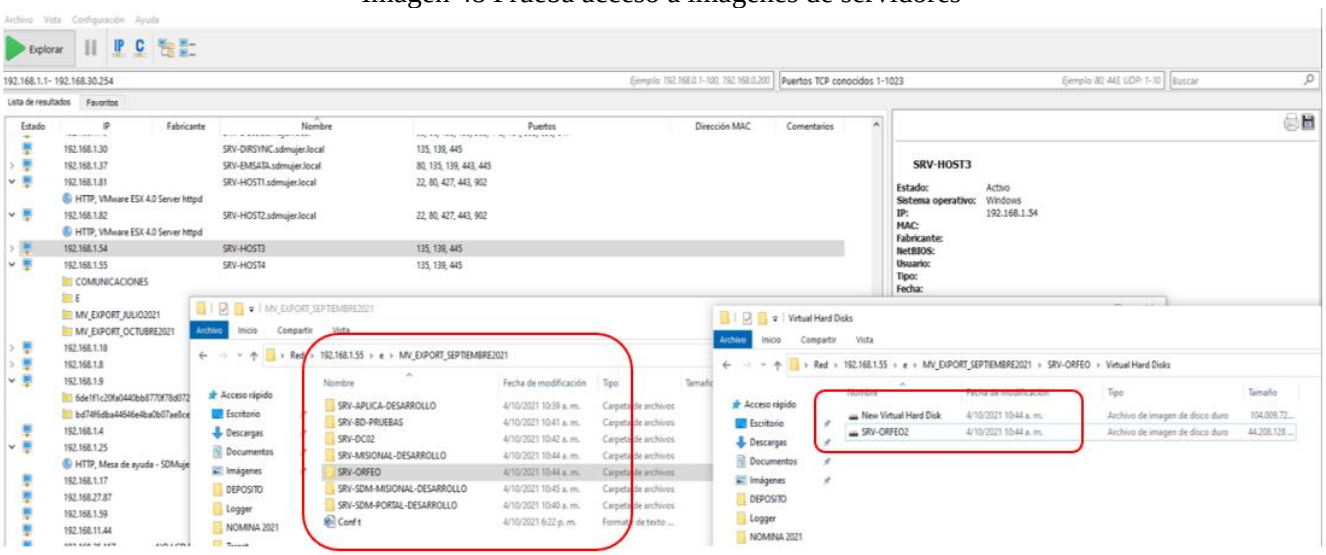
24.Tipo de documento: CC | 25. Número de identificación: | Apellidos y nombres: 26 Primer Apellido 27. Segundo Apellido 28.Primer nombre 29:Otros nombres

Periodo de la Certificación 30. DE:	2020-01-01	31. A:	2020-12-31	32. Fecha de expedicion	33. Lugar donde se practicó la retención	34. Cód. Dpto	35. Cód. Ciudad Municipio
				2021-03-08	BOGOTA D.C.	11	001

Concepto de los Ingresos		Valor
Pagos por salarios o emonumentos eclesiásticos	36	78,380,000
Pagos realizados con bonos electronicos o de papel de servicio.cheques.tarietas.vales.etc.	37	0
Pagos por Honorarios	38	0
Pagos por servicios	39	0
Pagos por Comisiones	40	0
Pagos por Prestaciones sociales	41	15,342,000
Pagos por Viaticos	42	0
Pagos por gastos de representación	43	0
Pagos por compensaciones por el trabajo asociado cooperativo	44	0
Otros Pagos	45	1,871,000
Cesantías e intereses de cesantías efectivamente pagadas en el período	46	7,381,000
Pensiones de jubilación, vejez o invalidez	47	0
Total de ingresos brutos (Sume casillas 36 a 47)	48	101,103,000
Concepto de los aportes		**Valor**
Aportes obligatorios por salud a cargo del trabajador	49	3,133,000
Aportes obligatorios a fondos de pensiones y solidaridad pensional a cargo del trabajador	50	3,360,000
Cotizaciones voluntarias al régimen de ahorro individual con solidaridad -RAIS	51	0
Aportes voluntarios al impuesto solidario por COVID 19	52	0
Aportes voluntarios a fondos de pensiones voluntarias	53	0
Aportes a cuentas AFC	54	0

-Evidencia de archivos de imágenes de discos duros de servidores sin protección, lo cuales pueden ser copiados y transferidos a equipos de usuario para vulnerarlos e instalarlos y así obtener acceso a la información:

Imagen 48 Prueba acceso a imágenes de servidores

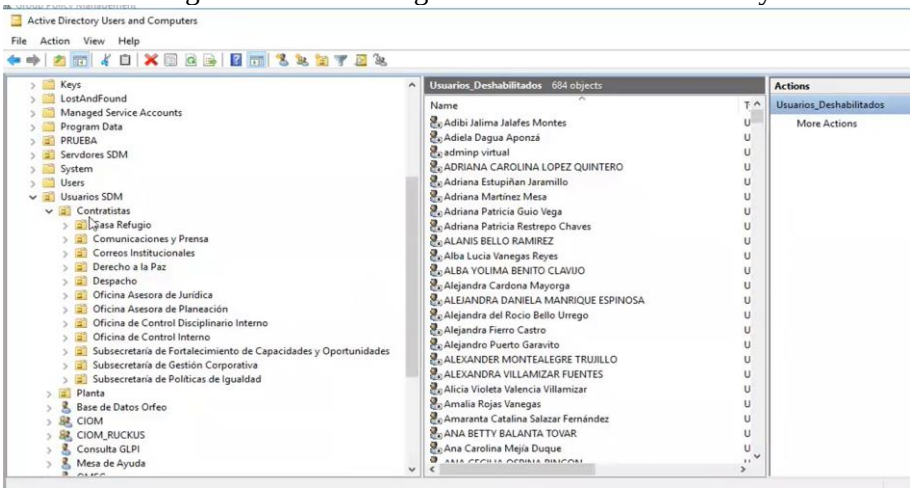


Vale aclarar que la presente auditoría no contempla ataques de penetración, ni es una auditoria de hacking ético, por lo tanto, las vulnerabilidades encontradas no pueden considerarse como las únicas existentes.

6.2.2.1.3. GESTIÓN DE ACCESOS

La Secretaría de la mujer cuenta con un controlador de dominio bajo Windows en el cual está configurado el directorio activo, en el cual se tienen creadas correctamente unidades organizativas por funcionarios contratistas y de planta ubicados en su área funcional, como se puede ver en la siguiente imagen:

Imagen 49 Unidades organizativas – Active Directory



La solicitud de creación de los usuarios a cargo de sistemas se hace por mesa de ayuda y/o por correos electrónicos. El área crea el usuario de dominio y configura el correo y los accesos solicitados, asignándole una contraseña temporal y marcando la opción de cambio obligatorio de contraseña al siguiente inicio de sesión.

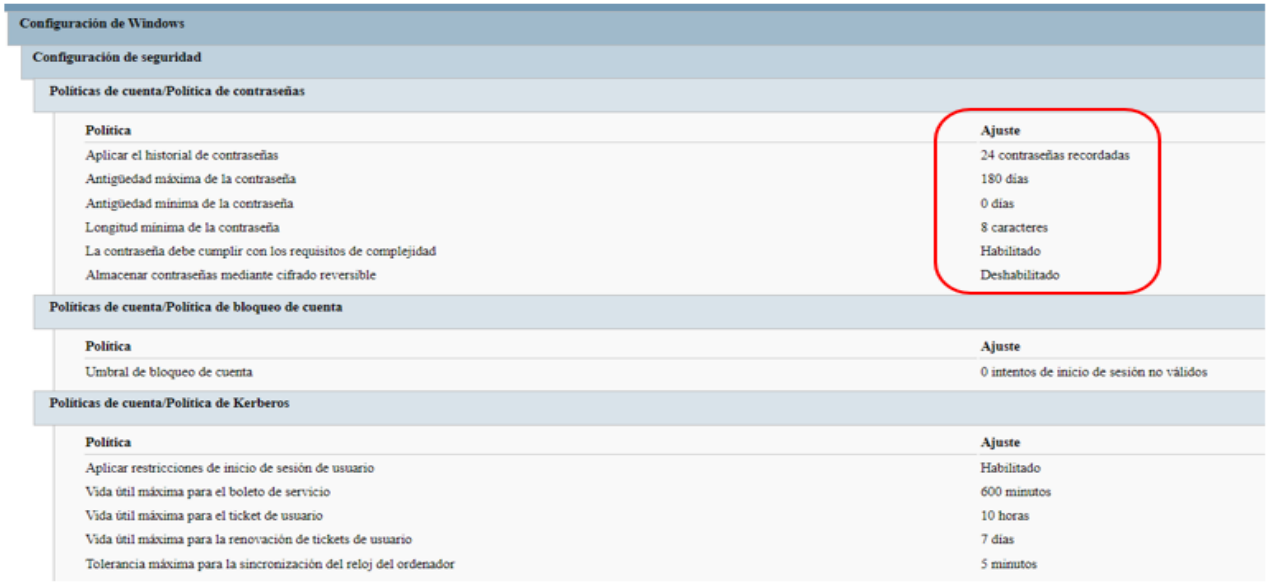
Imagen 50 Ejemplo clave explicita en mesa de ayuda

Cuando un usuario se retira, se deshabilita su cuenta en el dominio y se traslada de manera adecuada a la unidad organizativa: usuarios deshabilitados.

Los aplicativos Intranet, Icops, mesa de ayuda (GLPI), Orfeo, Correo y office 365 están integrados por LDAP (protocolo ligero de acceso al directorio), es decir que utilizan el mismo usuario y contraseña, del asignado a dominio y por ende no es necesario crear usuarios para cada aplicativo, así mismo heredan las políticas de seguridad definidas en el dominio.

En la configuración de seguridad de las políticas de dominio de Windows, se tienen configuradas las directivas de cuenta/contraseña con longitud mínima de 8 caracteres, vigencia de 180 días, 24 contraseñas recordadas, se exige complejidad y se tiene configuradas correctamente las directivas de Kerberos. La vigencia de contraseña a 180 días es muy alta y expone a los usuarios a ataques de fuerza bruta para suplantaciones y accesos no autorizados, lo recomendado es mínimo 90 días, se informa por parte del proceso que esta directiva se modificó a 180 días debido a la pandemia covid-19, lo cual no tiene sentido, ya que es bien sabido que los ataques informáticos aumentaron durante la pandemia y lo correcto es reforzar las medidas de seguridad. La siguiente imagen muestra la configuración de las directivas en el controlador de dominio:

Imagen 51 Directivas de contraseñas – Active Directory



Configuración de Windows

Configuración de seguridad

Políticas de cuenta/Política de contraseñas

Política	Ajuste
Aplicar el historial de contraseñas	24 contraseñas recordadas
Antigüedad máxima de la contraseña	180 días
Antigüedad mínima de la contraseña	0 días
Longitud mínima de la contraseña	8 caracteres
La contraseña debe cumplir con los requisitos de complejidad	Habilitado
Almacenar contraseñas mediante cifrado reversible	Deshabilitado

Políticas de cuenta/Política de bloqueo de cuenta

Política	Ajuste
Umbral de bloqueo de cuenta	0 intentos de inicio de sesión no válidos

Políticas de cuenta/Política de Kerberos

Política	Ajuste
Aplicar restricciones de inicio de sesión de usuario	Habilitado
Vida útil máxima para el boleto de servicio	600 minutos
Vida útil máxima para el ticket de usuario	10 horas
Vida útil máxima para la renovación de tickets de usuario	7 días
Tolerancia máxima para la sincronización del reloj del ordenador	5 minutos

👉 No se tiene configurado el umbral de bloqueo de cuenta por intentos de inicio de sesión fallidos, lo normal son tres intentos, lo cual debe incluirse como control de seguridad contra intentos de acceso no autorizado, ya que esto permitiría ataques de fuerza bruta por diccionario.

👍 Se tienen correctamente configuradas las políticas de auditoría de acceso de usuarios para permitir revisar los accesos exitosos o fallidos en el dominio:

Imagen 52 Directivas de auditoría – Active Directory

Políticas locales/Política de auditoría

Política	Ajuste
Eventos de inicio de sesión de cuentas de auditoría	Éxito, fracaso
Eventos de inicio de sesión de auditoría	Éxito, fracaso
Auditar el acceso a objetos	Éxito, fracaso
Auditar eventos del sistema	Éxito, fracaso

👎 Si bien se tiene configurada la vigencia de contraseña en el dominio a 180 días, en las entrevistas con usuarios y en la ejecución de la herramienta de descubrimiento de usuarios LANState Pro, la cual revela la fecha del último cambio de contraseña, el auditor pudo evidenciar que no se solicita este cambio. Hay usuarios que no cambian contraseña desde hace más de un año y en las entrevistas manifiestan que desde el inicio de la pandemia no se acuerdan de haber modificado la contraseña. En la imagen se muestra el listado que logra generar el auditor con las últimas fechas de modificación de contraseña, el listado completo de usuarios del dominio se entrega en el archivo adjunto a este informe: *"usuarios sdmujer dominio.xls"*: (se marcan algunos casos pero se presentan más)

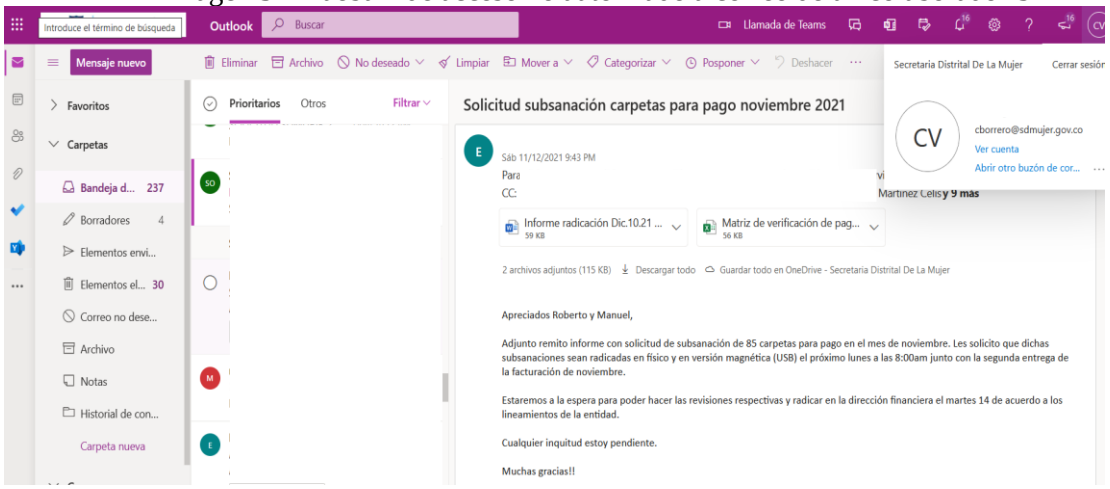
Imagen 53

usuario	nombre	descripcion	privilegios	tipo cuenta	ultima modificacion Contraseña	ultima sesion
mocampo		PROFESIONAL	Usuario	Usuario global	26/07/2018 11:47:14 a. m.	9/10/2018 6:00:51 p. m.
eguaqueta		Profesional	Usuario	Usuario global	2/08/2021 2:41:35 p. m.	9/08/2021 9:26:29 a. m.
ciocandelaria1			Usuario	Usuario global	6/06/2018 8:45:43 a. m.	9/08/2018 4:05:53 p. m.
AdminADMT		Cuenta de Admin de la Herramienta de Migracion ADMT	Administrador	Usuario global	11/10/2017 3:16:52 p. m.	9/07/2021 4:22:22 p. m.
ciokennedy4			Usuario	Usuario global	9/06/2018 11:02:18 a. m.	9/07/2018 10:37:57 a. m.
ciousme2			Usuario	Usuario global	9/05/2018 9:29:29 a. m.	9/05/2018 9:29:20 a. m.
ciochapinero1			Usuario	Usuario global	9/04/2018 12:08:04 p. m.	9/04/2018 12:07:50 p. m.
rhernandez		Directora de Enfoque Diferencial	Usuario	Usuario global	10/02/2020 8:46:00 a. m.	9/03/2020 10:36:46 a. m.
dasastoque		Profesional Especializado	Usuario	Usuario global	1/10/2021 3:05:30 p. m.	8/10/2021 3:11:13 p. m.
jfresneda		AUXILIAR ADMINISTRATIVO CODIGO 407 GRADO 18	Usuario	Usuario global	16/05/2019 3:49:40 p. m.	8/08/2019 5:33:07 p. m.
msiachica		Profesional Universitaria	Usuario	Usuario global	27/02/2020 7:27:00 a. m.	8/06/2020 3:59:48 p. m.
plibreros		Auxiliar Administrativa	Usuario	Usuario global	11/02/2020 1:54:21 p. m.	8/06/2020 10:23:33 a. m.
redex		Empresa de Mensajeria	Usuario	Usuario global	10/06/2020 8:38:31 a. m.	8/05/2021 1:59:16 a. m.
jbermudez		SUBSECRETARIA DE FORTALECIMIENTO DE CAPACIDAD	Usuario	Usuario global	26/01/2018 9:30:48 a. m.	8/02/2018 3:24:57 p. m.
lnorato		Profesional Especializada	Usuario	Usuario global	16/03/2020 3:38:01 p. m.	7/10/2020 7:09:23 p. m.
cioengativa		CIO Engativa	Usuario	Usuario global	8/09/2021 1:45:25 p. m.	7/09/2021 5:15:24 p. m.
dmejia		ASESORA DE DESPACHO	Usuario	Usuario global	27/08/2018 12:38:35 p. m.	7/09/2018 10:51:40 a. m.
ciousme		CIO Usme	Usuario	Usuario global	1/03/2021 3:22:26 p. m.	7/07/2021 4:35:14 p. m.
jwbonilla		Profesional Universitaria	Usuario	Usuario global	17/02/2020 9:06:11 a. m.	7/07/2021 2:26:45 p. m.
prueba1			Usuario	Usuario global	29/10/2020 5:30:12 p. m.	7/07/2020 1:38:55 p. m.
ctodas5			Usuario	Usuario global	7/03/2018 8:52:26 a. m.	7/03/2018 10:59:59 a. m.
dsastoque			Usuario	Usuario global	8/01/2019 1:46:35 p. m.	7/02/2019 5:06:50 p. m.
smparra		PROFESIONAL UNIVERSITARIO	Usuario	Usuario global	6/02/2019 9:08:22 a. m.	7/02/2019 3:46:23 p. m.
cpening		SUBSECRETARIA DE GESTION CORPORATIVA	Usuario	Usuario global	14/12/2017 3:26:16 p. m.	7/02/2018 4:32:33 p. m.
cvelez		SECRETARIA DE DESPACHO	Usuario	Usuario global	9/01/2018 11:52:58 a. m.	7/02/2018 4:21:34 p. m.
noviedo		Asesora Despacho	Usuario	Usuario global	13/03/2020 4:36:04 p. m.	6/10/2021 12:08:02 p. m.
corporativa		Profesional	Usuario	Usuario global	22/01/2020 4:37:42 p. m.	6/09/2021 3:29:49 p. m.
lmarin		AUXILIAR ADMINISTRATIVA	Usuario	Usuario global	5/08/2019 8:18:05 a. m.	6/09/2019 4:47:46 p. m.
jbarrera		Profesional Universitaria	Usuario	Usuario global	4/02/2021 3:15:16 p. m.	6/03/2021 8:35:01 a. m.
jmonroy		Profesional Universitario	Usuario	Usuario global	10/03/2021 4:48:16 p. m.	6/02/2021 6:50:27 p. m.
dbuitrago		PROFESIONAL UNIVERSITARIA	Usuario	Usuario global	29/01/2019 9:51:22 a. m.	5/12/2018 8:29:12 a. m.
dmurillo		Profesional Universitaria	Usuario	Usuario global	20/10/2020 1:47:28 p. m.	5/11/2020 12:47:03 p. m.
dolarte		Subsecretaria de Gestion Corporativa	Usuario	Usuario global	6/10/2021 4:52:00 p. m.	5/10/2021 3:25:30 p. m.

Se evidencia que a los nuevos usuarios no se les está exigiendo el cambio de contraseña obligatorio al inicio de la primera sesión, al obtener la lista anterior y al conocer la metodología de asignación de contraseñas a usuarios; es decir se entrega la cuenta y contraseña *Estado.2021* por correo (la misma entregada al usuario del auditor), se realizaron pruebas de acceso, con esta misma contraseña para usuarios ingresados en los últimos meses (septiembre y octubre del 2021), el auditor logro acceso a las cuentas de correo de los usuarios: dquinones@sdmujer.gov.co, aternera@sdmujer.gov.co y cborrero@sdmujer.gov.co. Con esta debilidad un atacante podría realizar suplantaciones de usuarios, obtener información confidencial entre otros. En las imágenes siguientes se evidencian estos accesos desde el equipo del auditor:

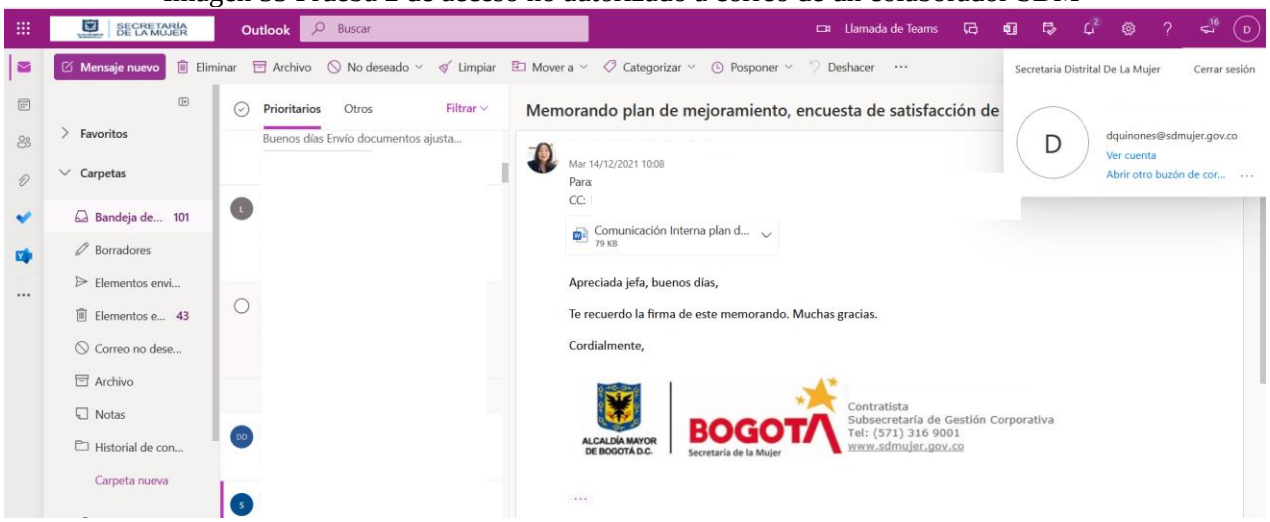
- Evidencia Ingreso al Correo de Servidora de la SDM

Imagen 54 Prueba 1 de acceso no autorizado a correo de un colaborador SDM



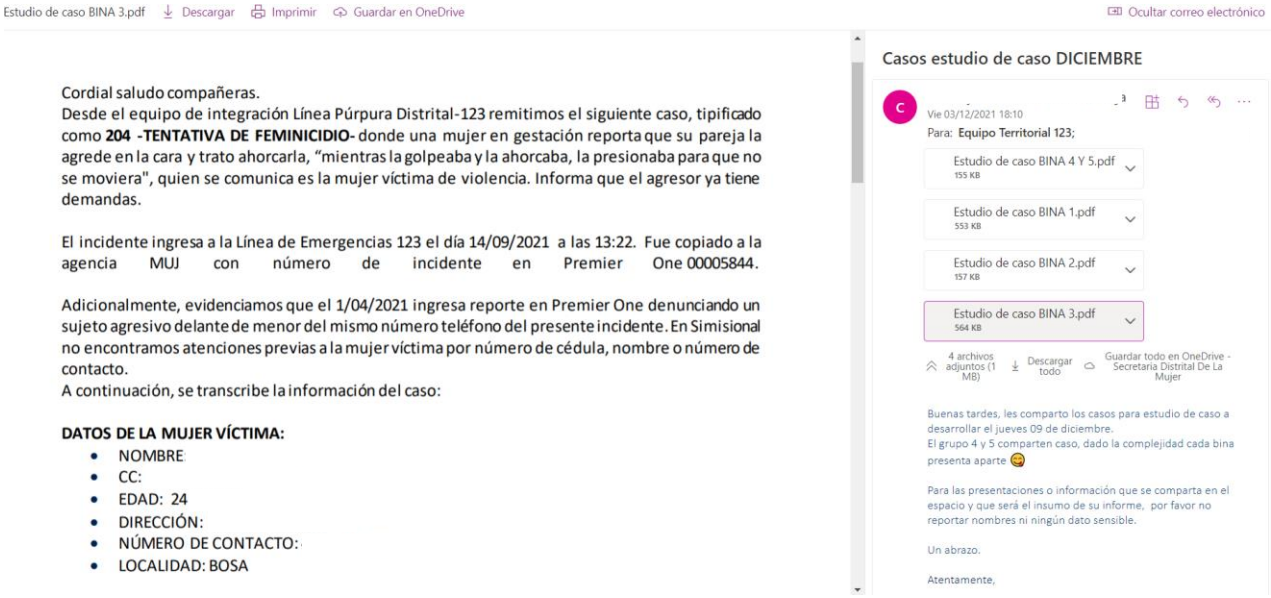
- Evidencia Ingreso al Correo de Servidora de la SDM

Imagen 55 Prueba 2 de acceso no autorizado a correo de un colaborador SDM



- Evidencia Ingreso al Correo con información confidencial de tentativa de feminicidio:

Imagen 56 Prueba de acceso no autorizado a información confidencial tentativa feminicidio



De lo anterior se evidencia también que no se tiene correctamente configurada la verificación de doble factor para accesos a los correos electrónicos desde de equipos nuevos o desconocidos, lo que permito al auditor ingresar a esas cuentas sin ninguna restricción.

En cuanto a la gestión de usuarios administradores de dominio se observa que 19 usuarios tienen privilegios de administrador, incluyendo el área de soporte del proceso de gestión tecnológica, lo que no es recomendable ya que incrementa el riesgo de ataques y no permite segregar responsabilidades de accesos privilegiados como lo indica MSPI (9.2.3). Adicionalmente existen 6 usuarios administradores "no nombrados" ***AdminADMT***, ***emsata***, *etc*., que no corresponde a una persona en particular, estos se crean para la ejecución de algunos servicios, la amenaza es que este tipo de usuarios son a los que más ataques de fuerza bruta dirigen los hackers, principalmente debido a que normalmente no se les cambia contraseña periódicamente para no alterar el servicio ya que al no pertenecer a un usuario fijo, no se notaria que el usuario está siendo usado por otra persona. Esto se evidencia en la siguiente imagen, en la lista de usuarios que el auditor logro tomar del servidor de dominio:

Imagen 57 Muestra de usuarios administradores no requeridos – Active Directory

usuario	nombre	descripcion	privilegios	tipo cuenta	ultima modificacion Contraseñ	ultima sesion	e	sesiones abiertas
AdminADMT		Cuenta de Admin de la Herramienta de	Administrador	Usuario global	11/10/2017 3:16:52 p. m.	9/07/2021 4:22:22 p. m.	0	104
SCDPMAdmin			Administrador	Usuario global	23/04/2018 2:30:49 p. m.	31/10/2021 3:20:22 p. m	0	1947
mgonzalez		Contratista	Administrador	Usuario global	18/08/2020 3:14:22 p. m.	3/11/2021 3:19:45 p. m.	0	4944
Administrator		Built-in account for administering the c	Administrador	Usuario global	27/08/2020 11:51:58 a. m.	3/11/2021 3:10:20 p. m.	5	6235
evillarraga		Usuario para perno, no deshabilitar gle	Administrador	Usuario global	10/03/2020 10:18:22 a. m.	3/11/2021 12:05:03 p. m	0	1405
print		Usuario Corporativo	Administrador	Print operator	14/10/2021 10:20:03 a. m.	3/11/2021 11:31:12 a. m	0	214
dblanco		Contratista	Administrador	Usuario global	2/09/2021 3:23:52 p. m.	3/11/2021 11:01:12 a. m.	0	4803
fpuentes		Contratista	Administrador	Usuario global	24/08/2021 1:32:21 p. m.	29/10/2021 10:13:35 a. r	0	248
acadena		Contratista	Administrador	Usuario global	14/09/2020 3:36:37 p. m.	28/10/2021 3:47:11 p. m	0	2176
lbecerra		Tecnico Administrativo	Administrador	Usuario global	3/12/2020 8:47:00 p. m.	27/10/2021 12:31:49 p. r	0	516
emsata			Administrador	Usuario global	10/02/2020 12:50:15 p. m.	2/11/2021 9:19:53 p. m.	0	1325
mbernal		Profesional Especializado	Administrador	Usuario global	27/08/2020 4:35:41 p. m.	2/11/2021 6:32:05 p. m.	0	54155
jherrera		Contratista	Administrador	Usuario global	26/03/2021 12:09:55 p. m.	2/11/2021 4:47:56 p. m.	0	371
cmoreno		Contratista	Administrador	Usuario global	23/10/2020 9:46:36 a. m.	2/11/2021 4:23:01 p. m.	0	5810
SCCMADMIN			Administrador	Usuario global	30/04/2018 12:36:35 p. m.	2/11/2021 4:06:18 p. m.	0	25703
jgleidy		Contratista	Administrador	Usuario global	25/08/2020 9:56:00 a. m.	2/11/2021 3:03:52 p. m.	0	564
SCCMCP			Administrador	Usuario global	28/11/2017 4:31:18 p. m.	2/11/2021 10:21:12 a. m	0	13728
jsanchez		Contratista	Administrador	Usuario global	9/03/2021 9:49:20 a. m.	2/11/2021 10:04:36 a. m	0	3357
AdminAADC			Administrador	Usuario global	22/12/2017 2:28:34 p. m.	14/05/2018 12:00:34 p. r	0	209

Si bien el grupo de soporte y los contratistas y funcionarios de gestión tecnológica, deben tener privilegios especiales para poder realizar su labor sobre todos los equipos de la infraestructura, es riesgoso mantenerlos como administradores de dominio, debido a que tendrían permisos completos de acceso a todo el dominio sdmujer, al tener estos privilegios en caso de algún error o problema que se presente no sería posible determinar responsabilidades. En el grupo de políticas de Windows existen una gran variedad de permisos a configurar para que se puedan realizar funciones especiales sin necesidad de ser administrador del dominio. La justificación dada para que el equipo de soporte tenga permisos de administrador es que ellos se encargan de unir los equipos al dominio, para esto existe una directiva que permite asignar usuarios para esta función sin necesidad de ser administradores:

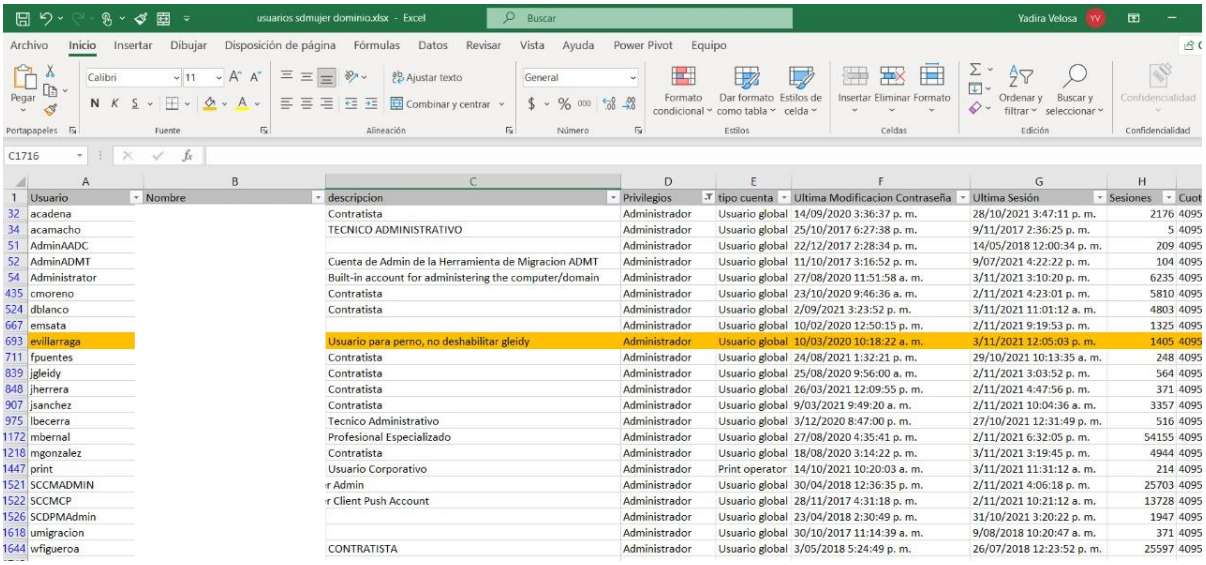
Imagen 58 Ejemplo de alternativas de asignación de accesos privilegiados – Active Directory

Directivas locales/Asignación de derechos de usuario
Directiva
Agregar estaciones de trabajo al dominio

En el listado de usuarios administradores se evidencia la dependencia de una cuenta de usuario: ***evillarraga***, para el funcionamiento de Software de la Secretaría de Hacienda para registrar la nómina de las entidades del Distrito – Perno, que corresponde a la contratista Ester Ligia Villarraga que fue contratada en el 2019 para

apoyar técnicamente en la implementación de este Sistema y ya no tiene contrato vigente, más allá de que existe una cuenta de un contratista que ya no trabaja con la secretaría, el hecho de que no se puede eliminar la cuenta evidencia una mala práctica en la implementación del software, ya que implica que pueden haber datos de conexión explícitos ("quemados") y por ende comprometer la seguridad del sistema y no se podría eliminar el usuario porque dejaría de funcionar correctamente e implicaría una modificación en su implementación.

Imagen 59 Muestra de usuarios administradores no requeridos – listado de usuarios suministrado por el proceso auditado

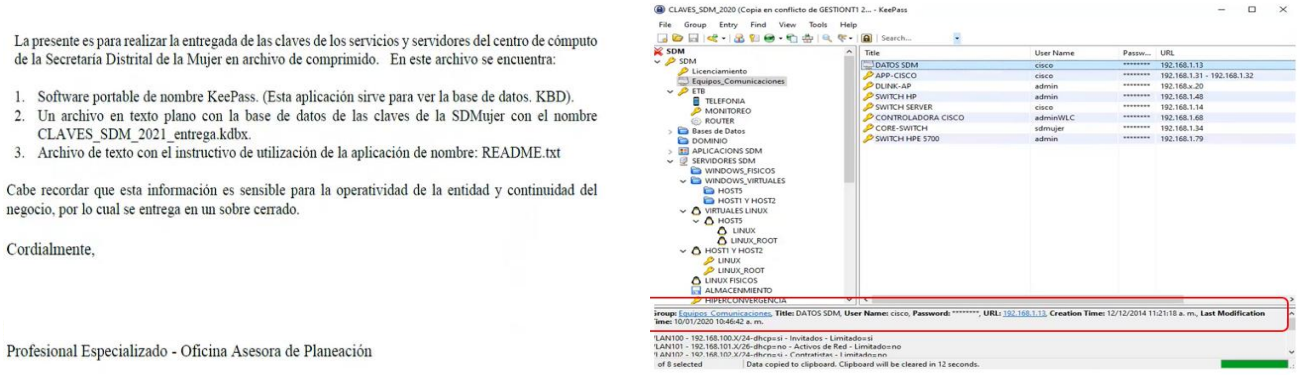


usuarios sdmujer dominio.xlsx - Excel — Yadira Velosa

	Usuario	Nombre	descripcion	Privilegios	tipo cuenta	Ultima Modificacion Contraseña	Ultima Sesión	Sesiones	Cuot
32	acadena		Contratista	Administrador	Usuario global	14/09/2020 3:36:37 p. m.	28/10/2021 3:47:11 p. m.	2176	4095
34	acamacho		TECNICO ADMINISTRATIVO	Administrador	Usuario global	25/10/2017 6:27:38 p. m.	9/11/2017 2:36:25 p. m.	5	4095
51	AdminAADC			Administrador	Usuario global	22/12/2017 2:28:34 p. m.	14/05/2018 12:00:34 p. m.	209	4095
52	AdminADMT		Cuenta de Admin de la Herramienta de Migracion ADMT	Administrador	Usuario global	11/10/2017 3:16:52 p. m.	9/07/2021 4:22:22 p. m.	104	4095
54	Administrator		Built-in account for administering the computer/domain	Administrador	Usuario global	27/08/2020 11:51:58 a. m.	3/11/2021 3:10:20 p. m.	6235	4095
435	cmoreno		Contratista	Administrador	Usuario global	23/10/2020 9:46:36 a. m.	2/11/2021 4:23:01 p. m.	5810	4095
524	dblanco		Contratista	Administrador	Usuario global	2/09/2021 3:23:52 p. m.	3/11/2021 11:01:12 a. m.	4803	4095
667	emsata			Administrador	Usuario global	10/02/2020 12:50:15 p. m.	2/11/2021 9:19:53 p. m.	1325	4095
693	evillarraga		Usuario para perno, no deshabilitar gleidy	Administrador	Usuario global	10/03/2020 10:18:22 a. m.	3/11/2021 12:05:03 p. m.	1405	4095
711	fpuentes		Contratista	Administrador	Usuario global	24/08/2021 1:32:21 p. m.	29/10/2021 10:13:35 a. m.	248	4095
839	jgleidy		Contratista	Administrador	Usuario global	25/08/2020 9:56:00 a. m.	2/11/2021 3:03:52 p. m.	564	4095
848	jherrera		Contratista	Administrador	Usuario global	26/03/2021 12:09:55 p. m.	2/11/2021 4:47:56 p. m.	371	4095
907	jsanchez		Contratista	Administrador	Usuario global	9/03/2021 9:49:20 a. m.	2/11/2021 10:04:36 a. m.	3357	4095
975	lbecerra		Tecnico Administrativo	Administrador	Usuario global	3/12/2020 8:47:00 p. m.	27/10/2021 12:31:49 p. m.	516	4095
1172	mbernal		Profesional Especializado	Administrador	Usuario global	27/08/2020 4:35:41 p. m.	2/11/2021 6:32:05 p. m.	54155	4095
1218	mgonzalez		Contratista	Administrador	Usuario global	18/08/2020 3:14:22 p. m.	3/11/2021 3:19:45 p. m.	4944	4095
1447	print		Usuario Corporativo	Administrador	Print operator	14/10/2021 10:20:03 a. m.	3/11/2021 11:31:12 a. m.	214	4095
1521	SCCMADMIN		r Admin	Administrador	Usuario global	30/04/2018 12:36:35 p. m.	2/11/2021 4:06:18 p. m.	25703	4095
1522	SCCMCP		r Client Push Account	Administrador	Usuario global	28/11/2017 4:31:18 p. m.	2/11/2021 10:21:12 a. m.	13728	4095
1526	SCDPMAdmin			Administrador	Usuario global	23/04/2018 2:30:49 p. m.	31/10/2021 3:20:22 p. m.	1947	4095
1618	umigracion			Administrador	Usuario global	30/10/2017 11:14:39 a. m.	9/08/2018 10:20:47 a. m.	371	4095
1644	wfigueroa		CONTRATISTA	Administrador	Usuario global	3/05/2018 5:24:49 p. m.	26/07/2018 12:23:52 p. m.	25597	4095

Se está utilizando la herramienta gratuita *KeePass* como gestor de contraseñas y cuya principal finalidad es permitir tener una base de datos segura y offline para la custodia de las contraseñas de los diferentes servidores, sistemas, bases de datos y equipos. La maneja el encargado de la infraestructura de TI y se entrega a la directora de la OAP con su debida protección y contraseña en un cd para su almacenamiento como contingencia:

Imagen 60 Uso KeePass



La presente es para realizar la entregada de las claves de los servicios y servidores del centro de cómputo de la Secretaría Distrital de la Mujer en archivo de comprimido. En este archivo se encuentra:

1. Software portable de nombre KeePass. (Esta aplicación sirve para ver la base de datos. KBD).
2. Un archivo en texto plano con la base de datos de las claves de la SDMujer con el nombre CLAVES_SDM_2021_entrega.kdbx.
3. Archivo de texto con el instructivo de utilización de la aplicación de nombre: README.txt

Cabe recordar que esta información es sensible para la operatividad de la entidad y continuidad del negocio, por lo cual se entrega en un sobre cerrado.

Cordialmente,

Profesional Especializado - Oficina Asesora de Planeación

CLAVES_SDM_2020 (Copia en conflicto de GESTION1 2... - KeePass

SDM
- Licenciamiento
- Equipos_Comunicaciones
- ETB
  - TELEFONIA
  - MONITOREO
  - ROUTER
- Bases de Datos
- DOMINIO
- APLICACIONS SDM
- SERVIDORES SDM
  - WINDOWS_FISICOS
  - WINDOWS_VIRTUALES
    - HOST5
    - HOST1 Y HOST2
  - VIRTUALES LINUX
    - HOST5
      - LINUX
      - LINUX_ROOT
    - HOST1 Y HOST2
      - LINUX
      - LINUX_ROOT
  - LINUX FISICOS
  - ALMACENMIENTO
  - HIPERCONVERGENCIA

Title	User Name	Passw...	URL
DATOS SDM	cisco	********	192.168.1.13
APP-CISCO	cisco	********	192.168.1.31 - 192.168.1.32
DLINK-AP	admin	********	192.168.x.20
SWITCH HP	admin	********	192.168.1.48
SWITCH SERVER	cisco	********	192.168.1.14
CONTROLADORA CISCO	adminWLC	********	192.168.1.68
CORE-SWITCH	sdmujer	********	192.168.1.34
SWITCH HPE 5700	admin	********	192.168.1.79

Group: Equipos_Comunicaciones, Title: DATOS SDM, User Name: cisco, Password: ********, URL: 192.168.1.13, Creation Time: 12/12/2014 11:21:18 a. m., Last Modification Time: 10/01/2020 10:46:42 a. m.

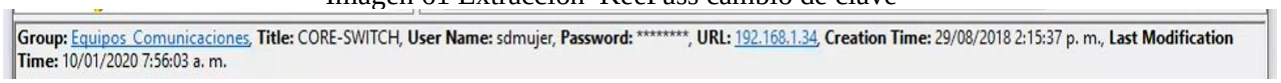
LAN100 - 192.168.100.X/24- dhcp=si - Invitados - Limitado=si
LAN101 - 192.168.101.X/26- dhcp=no - Activos de Red - Limitado=no
LAN107 - 167.168.107.X/24- dhcp=si - Contratistas - Limitado=no

of 8 selected | Data copied to clipboard. Clipboard will be cleared in 12 seconds.

Como se aprecia en el recuadro rojo de la imagen anterior, se evidencia que la última vez que se cambió la contraseña del equipo seleccionado es el 10 de enero del 2020, lo cual va en contra de la política de seguridad

de cambio de contraseña periódico que debería cumplirse con mayor detalle en las contraseñas administrativas. Durante las sesiones en el uso de esta herramienta se pudo ver que estos casos son repetitivos:

Imagen 61 Extracción KeePass cambio de clave

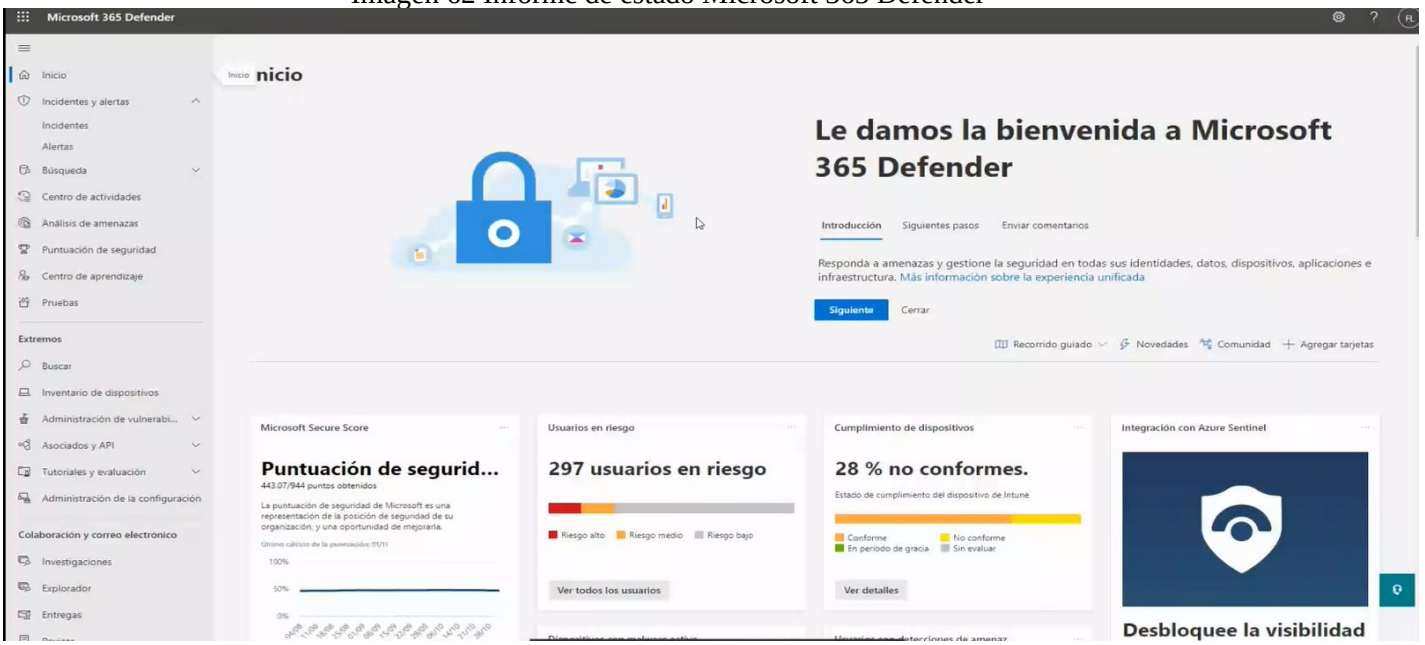


No existen procedimientos documentados y aplicados de cambio periódico de contraseñas de usuarios administradores, de las bases de datos, de los administradores locales de los equipos de usuario, de administradores de elementos activos de red, etc., lo cual al no tener aún el firewall en funcionamiento aumenta la exposición al riesgo de sufrir ataques por suplantación de identidad. Vale aclarar que la política incluida en el GT-MA-3 - MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN - V3 no remplaza el procedimiento.

6.2.2.1.4. SEGURIDAD DE PC's Y DOCUMENTOS

En cuanto a la seguridad de los equipos de usuarios final se cuenta con la solución para protección de *endpoints*: *Microsoft 365 Defender*, se controla y monitorea el estado de las protecciones y actualizaciones de las firmas de antivirus en los computadores desde la consola administrativa de la solución y del Microsoft System Center para la configuración en servidores y otros equipos y definición de políticas de escaneo, entre otros. En la inspección de la configuración del antivirus realizada durante la auditoria se evidencia que se tiene configuradas adecuadamente las reglas y políticas para el control de virus, malware y spam, en las imágenes se muestra el informe de estado:

Imagen 62 Informe de estado Microsoft 365 Defender

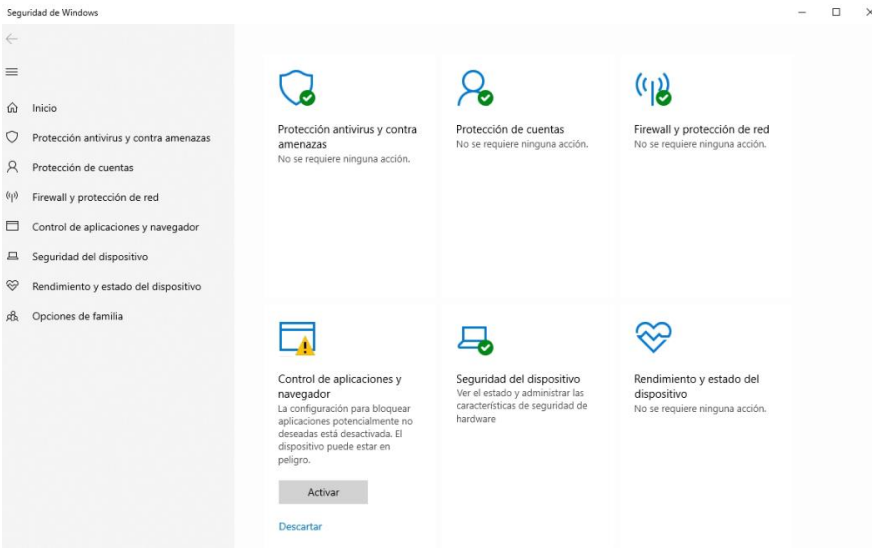


👉 Como se puede apreciar en la consola del 365 Defender, 297 usuarios se encuentran en riesgo y la puntuación de seguridad es menor del 50% (443.07/944), valor que es muy bajo y que indica que hay varias oportunidades de mejora para subir esa puntuación, estas herramientas emiten las recomendaciones para remediar los casos:

Imagen 63 Puntuación de seguridad Microsoft 365 Defender

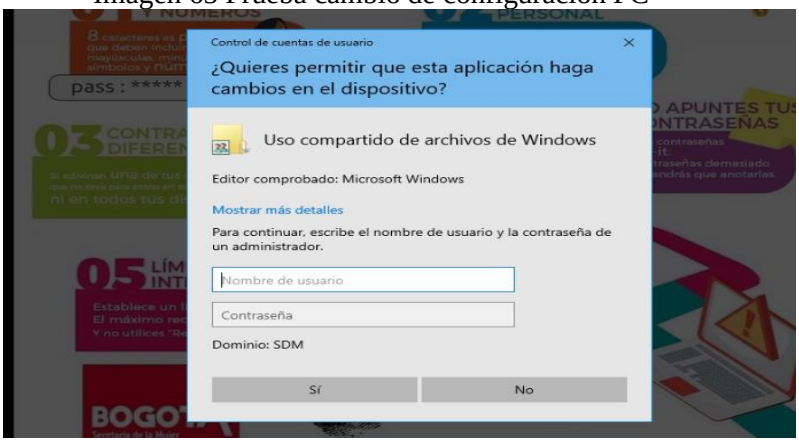
👉 En las pruebas realizadas por la auditoria, se evidencia que el cliente de antivirus Windows defender en los equipos que se inspeccionaron esta correctamente configurado y en funcionamiento, no permite desactivar las protecciones, detecta de forma adecuado archivos infectados y no es posible excluirlos de la cuarentena o del análisis de virus. Sin embargo, no se tiene habilitado el control de aplicaciones y del navegador, lo que permitió al auditor descargar y usar herramientas portables consideradas como peligrosas, como se evidencio en el numeral 6.2.2.1 pruebas internas en este documento:

Imagen 64 Control de aplicaciones y navegador Microsoft 365 Defender



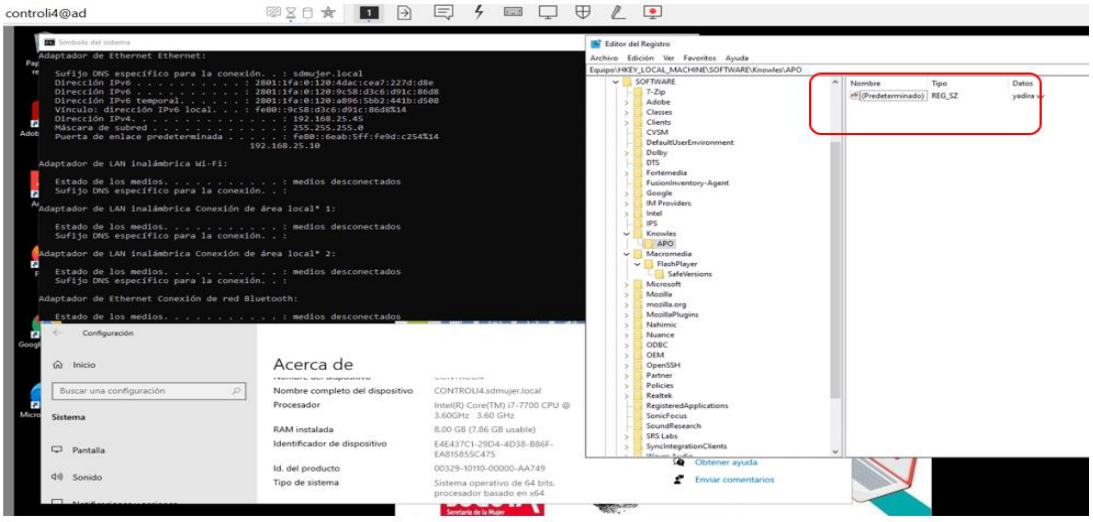
En los PC's se tiene correctamente restringidas a usuarios administradores las opciones, de instalar o desinstalar software, de crear o modificar usuarios, activar la detención de redes, compartir carpetas o archivos, eliminar archivos del sistema.

Imagen 65 Prueba cambio de configuración PC



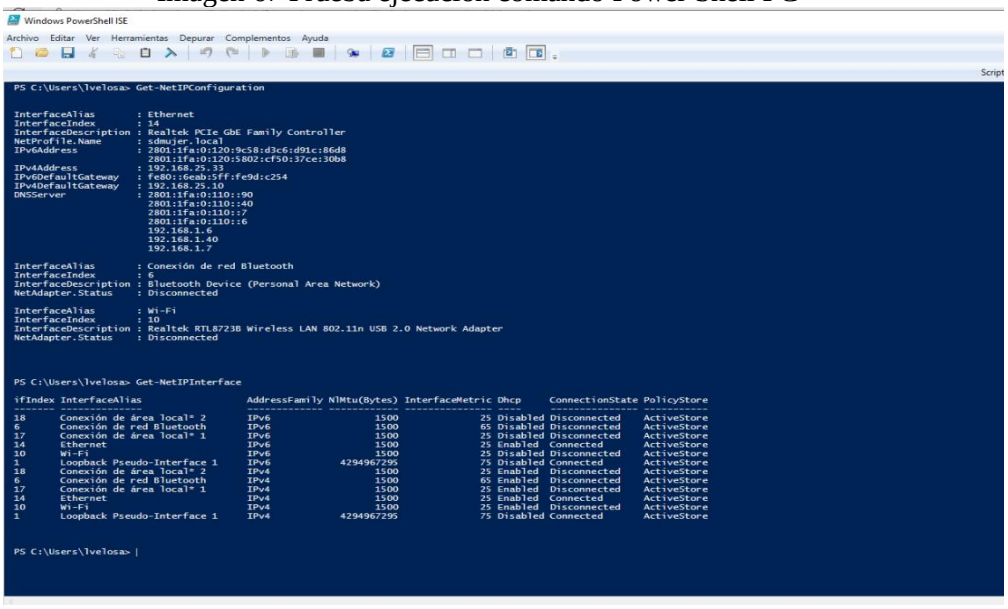
No se encuentran deshabilitados los accesos al panel de control, a herramientas administrativas, a visualizar la configuración de red y de tarjetas, generador de conexiones ODBC, a la ejecución de comandos (CMD), la edición del registro de Windows y al PowerShell de Windows. Es importante tener en cuenta que, al tener acceso al PowerShell, al cmd, o al editor de registro de los equipos, permite ejecutar scripts (fragmentos de código) de descubrimientos o ingresar comandos para activar software espía o malicioso. En la siguiente imagen se muestra el acceso al REGEDIT con la creación de una llave (*yadira vv- recuadro rojo*) como evidencia de cambio por parte del auditor en el registro de Windows, y la ejecución de comandos desde el símbolo del sistema: ***cmd*** en el equipo controli4. Esto se realizó con el propósito de mostrar que, si pueden hacerse modificaciones, por ejemplo, un virus malicioso en el RunOnce.

Imagen 66 Prueba acceso a regedit y creación de llave



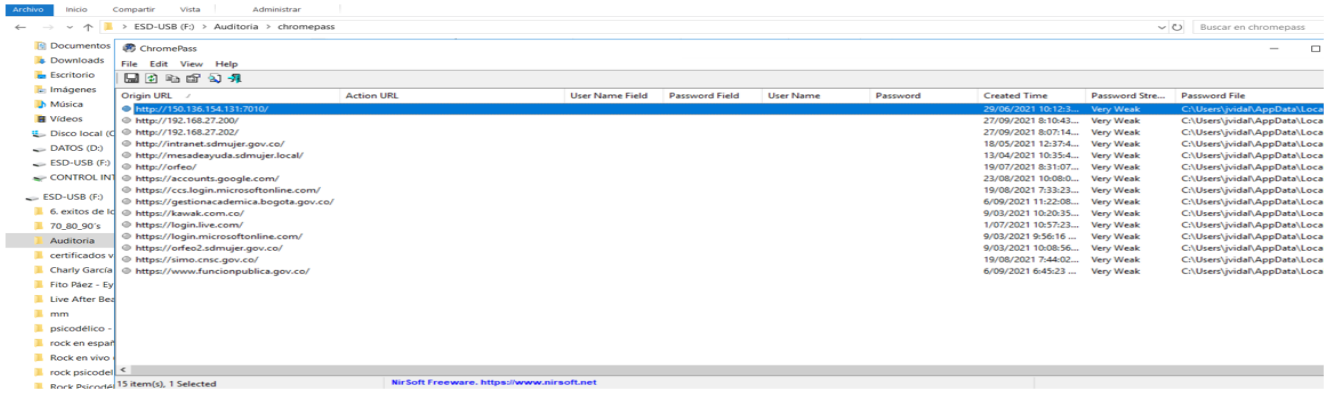
Evidencia de ejecución de comandos desde el PowerShell de Windows desde el equipo asignado a la auditoria:

Imagen 67 Prueba ejecución comando Power Shell PC



No se tienen restricciones sobre el uso de unidades de almacenamiento externas y/o extraíbles, lo que permitió al auditor la ejecución de herramientas de descubrimiento de usuarios y contraseñas planas. El auditor logro ejecutar el *chromepass* y el *WebBrowserpassView* en los equipos de control interno.

Imagen 68 Prueba ejecución chromepass



Al tener los medios de almacenamiento extraíbles habilitados, la principal amenaza no es la fuga de información confidencial es la difusión de virus, o ejecución de pruebas de penetración desde las mismas. Con dispositivos USB Booteables es posible para un atacante no experto o usuario, activar o crear usuarios administradores locales en menos 3 minutos y así obtener acceso total al equipo evadiendo todas las protecciones implementadas, incluyendo la instalación de software y deshabilitar la protección del antivirus.

No existen restricciones a descargas de archivos ejecutables (*.exe, .com, .bat,* etc), ni la restricción a ejecución de aplicaciones portables, debido a esto el auditor pudo realizar los descubrimientos y vulnerabilidades mencionadas en las pruebas internas con herramientas portables como: "***Advanced Port Scanner***", "***Advanced Lan scanner***".

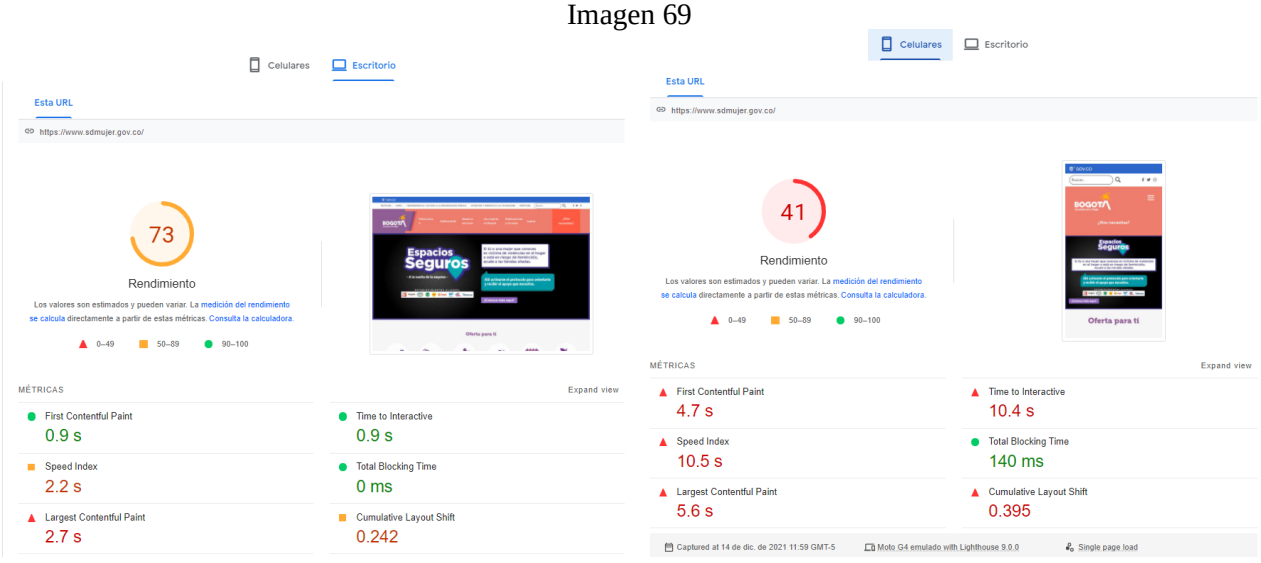
6.2.2.1.5. PRUEBAS DE SEGURIDAD EXTERNAS

El auditor realizo pruebas de rendimiento sobre los portales web de la Secretaria, en las pruebas de rendimiento se obtiene una puntuación calculada a partir de las métricas web esenciales, basadas únicamente en las mejores practica de desarrollo web, no en análisis de las características de los servidores en los que están alojados los portales, del período de 28 días de recolección más reciente de Google Analytics, realizando un análisis detallado y emitiendo recomendaciones de mejora, gracias a la carga de los portales en un entorno simulado. Los siguientes son los resultados de estas pruebas:

RESULTADOS DE PORTAL WEB – https://www.sdmujer.gov.co

El portal web obtiene una puntuación de rendimiento medio entre 68/100 a 73/100 para equipos de escritorio y bajo para celulares 41/100 como se ve en las siguientes imágenes, debido principalmente a no tener habilitada la compresión de texto, a tener código de JavaScript no utilizado, entre otros, que se encuentran detallados en el reporte generado por la herramienta adjunto a este informe, es importante tener en cuenta que los valores en estas pruebas son dinámicos y varían dependiendo del momento de ejecutarse y del contenido del portal, sin embargo, la auditoria ejecutó varias veces las pruebas obteniendo valores similares en todas, y las mismas oportunidades de mejoras, que sirve como guía para elevar el rendimiento del portal.

Imagen 69



El diagnóstico y las oportunidades de mejora del rendimiento para el portal se muestran en las siguientes imágenes y están detalladas en el documento adjunto, o que pueden ser consultadas por los encargados de los portales al

ejecutar la herramienta en línea (PageSpeed Insights). En las pruebas se evaluaron varios enlaces del portal obteniendo puntajes similares, y las mismas oportunidades de mejora y de diagnóstico:

Imagen 70

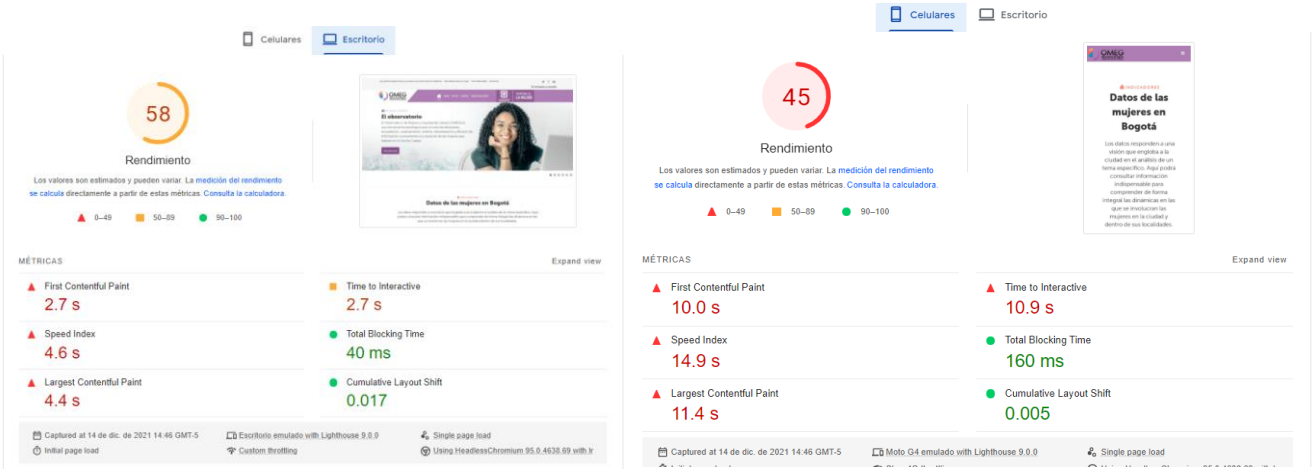
Para los otros sitios web analizados solo presentamos el resumen del análisis, las oportunidades de mejora y diagnósticos se adjuntan al informe.

RESULTADOS – http://omeg.sdmujer.gov.co

El portal web Observatorio de Mujeres y Equidad de Género, obtiene una puntuación de rendimiento medio 58 sobre 100 para equipos de escritorio y bajo 45 sobre 100 para dispositivos móviles, principalmente debido al uso

de contenido JavaScript que no se usa y a el uso de recursos que bloquean el renderizado, como se ve en las siguientes imágenes:

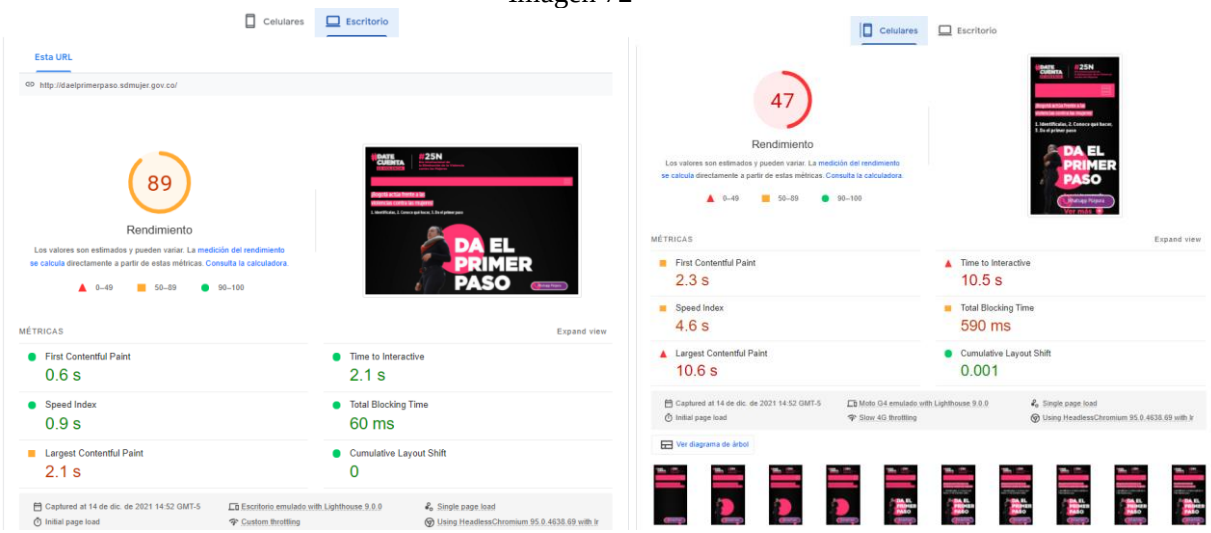
Imagen 71



RESULTADOS – http://daelprimerpaso.sdmujer.gov.co/

El micrositio “Da el primer paso”, obtiene una puntuación de rendimiento medio 89 sobre 100 para equipos de escritorio y bajo 47 sobre 100 para dispositivos móviles, principalmente debido al uso de contenido JavaScript que no se usa y a el uso de recursos que bloquean el renderizado, como se ve en las siguientes imágenes:

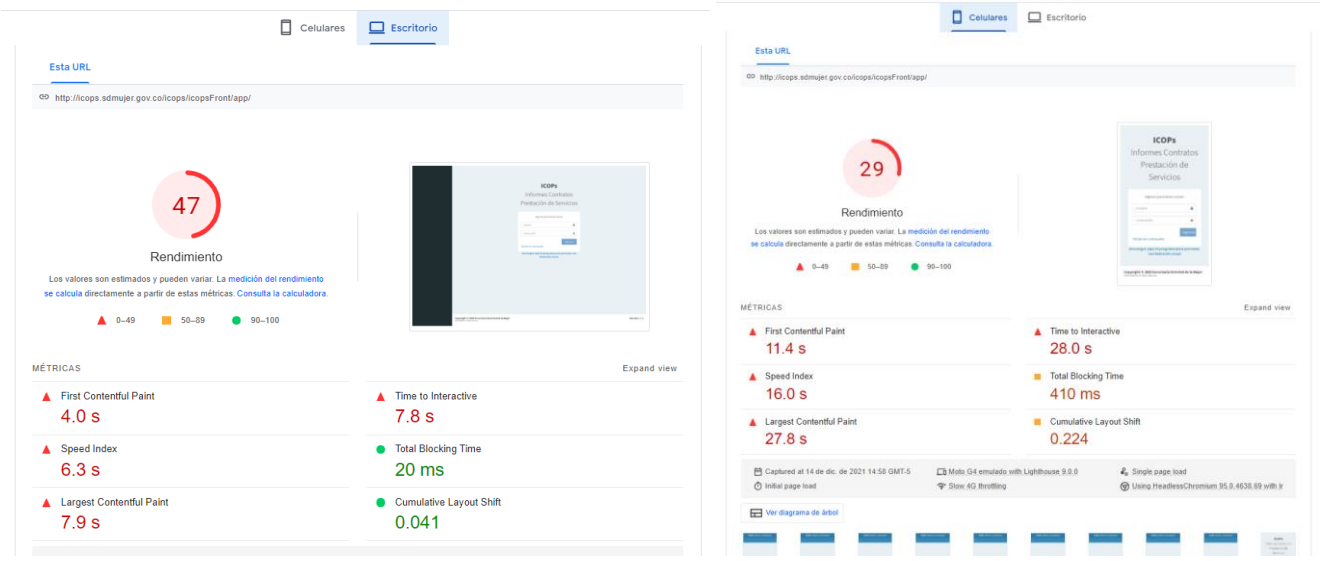
Imagen 72



RESULTADOS – http://icops.sdmujer.gov.co/

La app Icops obtiene una puntuación de rendimiento bajo 47 sobre 100 para equipos de escritorio y bajo 29 sobre 100 para dispositivos móviles, debido al uso de recursos que bloquean el renderizado y al no uso de compresión de texto, como se ve en las siguientes imágenes:

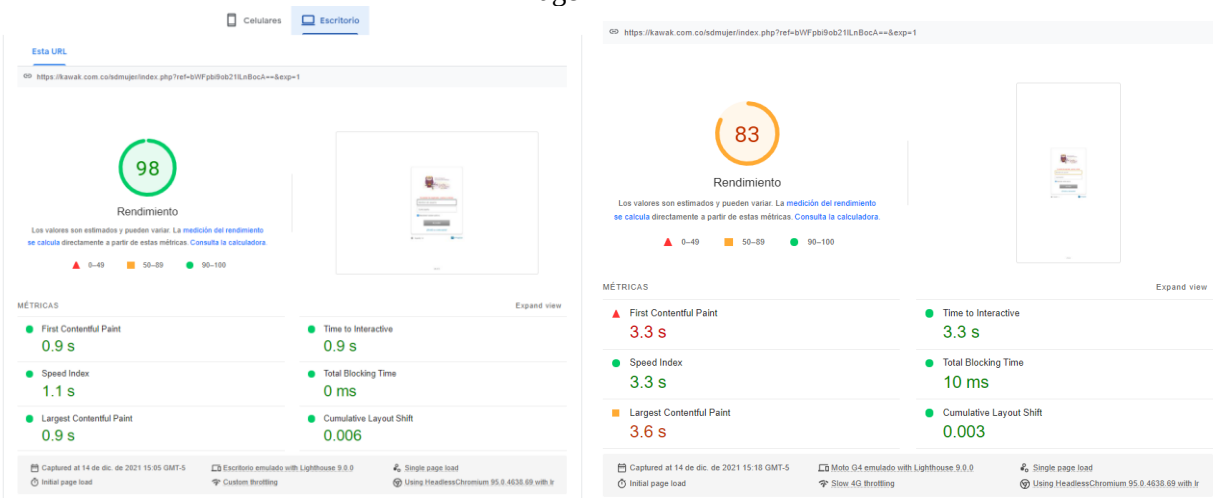
Imagen 73



RESULTADOS – https://kawak.com.co/sdmujer/main/home.php/

El aplicativo web Kawak obtiene una puntuación de rendimiento alto 98 sobre 100 para equipos de escritorio y medio 83 sobre 100 para celulares:

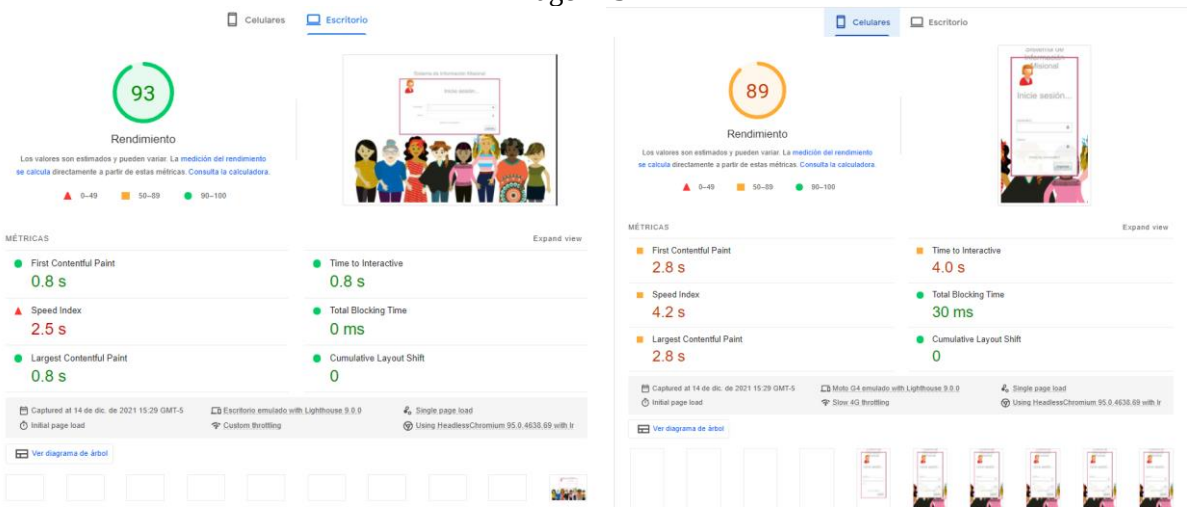
Imagen 74



RESULTADOS – http://simisional.sdmujer.gov.co/

El aplicativo web SIMISIONAL obtiene una puntuación de rendimiento alto 93 sobre 100 para equipos de escritorio y medio 89 sobre 100 para celulares, lo cual se debe a no utilizar tantos elementos visuales:

Imagen 75

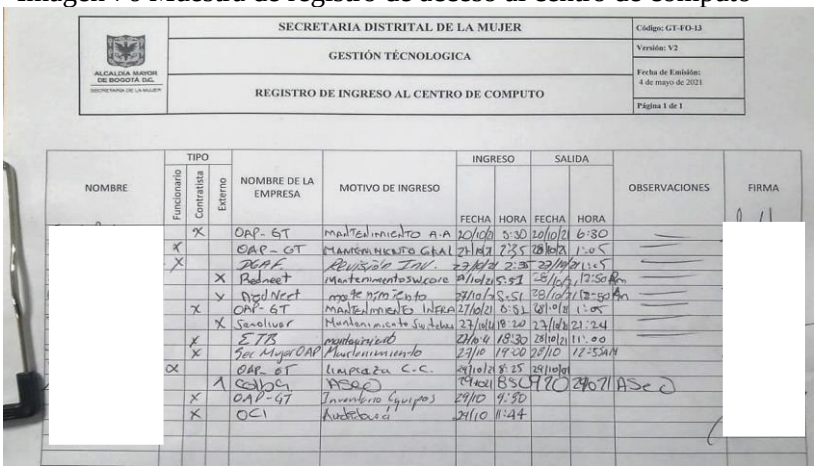


6.2.3. SEGURIDAD FÍSICA (CENTRO DE CÓMPUTO Y OFICINAS)

6.2.3.1. FORTALEZAS Y OPORTUNIDADES DE MEJORA

Los servidores, equipos de comunicación y demás elementos críticos se encuentran resguardados en centros de cómputo de cada sede con control de acceso por llave que solo la tiene el equipo de encargado de administrar la infraestructura tecnológica. Se cuenta con un formato de control de acceso al centro de cómputo, en el cual se registra correctamente además del nombre y la firma, el motivo, la hora de ingreso y de salida:

Imagen 76 Muestra de registro de acceso al centro de computo

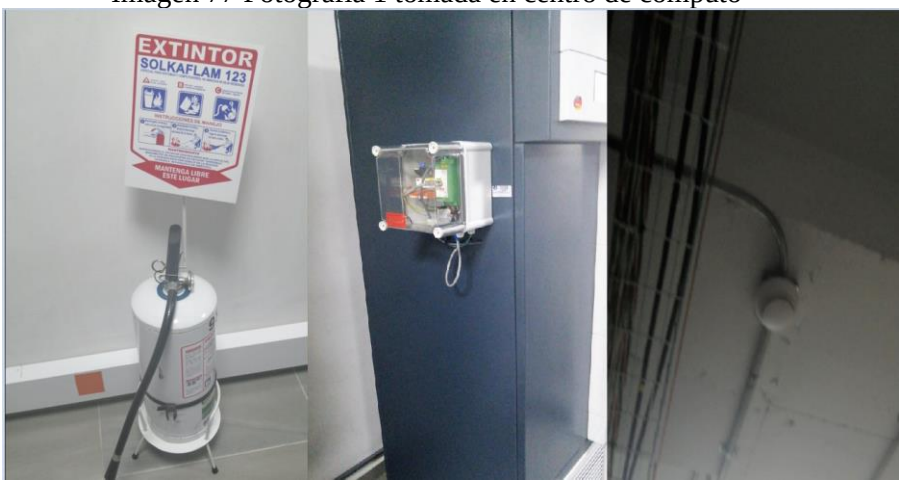


SECRETARIA DISTRITAL DE LA MUJER | Código: GT-FO-13
GESTIÓN TÉCNOLOGICA | Versión: V2
REGISTRO DE INGRESO AL CENTRO DE COMPUTO | Fecha de Emisión: 4 de mayo de 2021 | Página 1 de 1

NOMBRE	TIPO: Funcionario	TIPO: Contratista	TIPO: Externo	NOMBRE DE LA EMPRESA	MOTIVO DE INGRESO	INGRESO FECHA	INGRESO HORA	SALIDA FECHA	SALIDA HORA	OBSERVACIONES	FIRMA
		X		OAP- GT	MANTENIMIENTO A.A	20/10/21	5:30	20/10/21	6:30		
X				OAP - GT	MANTENIMIENTO GRAL	21/10/21	2:35	21/10/21	1:05		
X				OAP	Revisión Inv.	27/10/21	2:35	27/10/21	1:05		
			X	Redneet	mantenimiento switche	27/10/21	5:51	28/10/21	12:50 Am		
		X		Redneet	mantenimiento	27/10/21	5:51	28/10/21	12:50 Am		
		X		OAP- GT	MANTENIMIENTO INFRA	27/10/21	6:51	28/10/21	1:05		
		X		Sanoliver	Mantenimiento Switches	27/10/21	19:20	27/10/21	21:24		
		X		ETB	mantenimiento	27/10/21	18:30	28/10/21	11:00		
		X		Sec Mujer OAP	Mantenimiento	27/10	19:00	28/10	12:53AM		
X				OAP- GT	LIMPIEZA C.C.	28/10/21	8:25	29/10/21			
		1		OAP	ASEO	29/10/21	8:50	29/10/21	ASEO		
		X		OAP- GT	Inventario Equipos	29/10	9:50				
		X		OCI	Auditoria	29/10	11:44				

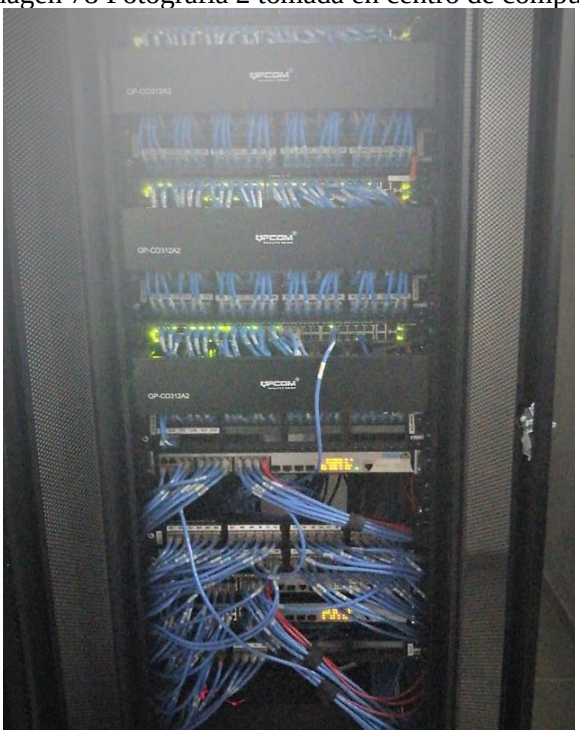
👍 El centro de cómputo tiene instalados correctamente elementos de seguridad física como detección de incendios, refrigeración, control de temperatura y extintor en el centro de cómputo:

Imagen 77 Fotografía 1 tomada en centro de computo



👍 Se cuenta con canaletas adecuadas para red eléctrica, de voz y de datos, el cableado estructurado es de categoría 6ª, se tienen 222 puntos de datos y 60 puntos de voz, con sus respectivas etiquetas en los racks de comunicaciones:

Imagen 78 Fotografía 2 tomada en centro de computo



👉 No se cuenta con diagramas en los closets de comunicaciones del centro de cómputo que permita identificar

rápidamente los elementos, equipos y ubicaciones de puntos en los racks.

👍 Se cuenta con protecciones eléctricas adecuadas, la UPS tiene una autonomía de 1 hora y se cuenta con una planta eléctrica que se activa automáticamente a los 30 segundos del fallo eléctrico:

Imagen 79 Fotografía 3 tomada en centro de computo

👎 Todo invitado debería registrarse en la entrada de las oficinas y dar el serial del portátil que ingresa, sin embargo, en las visitas realizadas a las instalaciones por el auditor no se lleva este control ni al ingreso, ni a la salida, lo cual permitiría hurtar o retira equipos sin autorización y no da cumplimiento al dominio 11 MSPI.

👎 No se cuenta con un procedimiento documentado de apagado seguro de los equipos de comunicaciones y/o de servidores del centro de cómputo, este procedimiento evita daños físicos en los equipos por fallos eléctricos inesperados, en caso de que falle la planta eléctrica y el tiempo de autonomía de la UPS se cumpla o falle ambas protecciones.

6.3. PLAN DE ADMINISTRACIÓN DE RIESGOS Y CONTINGENCIAS

6.3.1. ADMINISTRACION DE RIESGOS

6.3.1.1. FORTALEZAS Y OPORTUNIDADES DE MEJORA

👍 La entidad cuenta con la "*Política de Administración del Riesgo",* que describe de manera muy general la aceptación de riesgos de seguridad digital.

👉 A su vez el documento DE-PR-11 ADMINISTRACION DEL RIESGO, escribe de manera general el procedimiento para su identificación, valoración y tratamiento, sin hacer ninguna precisión en los riesgos TIC ni los Riesgos de seguridad y privacidad de la información y su administración de manera alineada con la implementación del MSPI, activos de información y especialmente en la implementación de controles de ISO 27002:2013 para controlar los riesgos de seguridad de la información.

👉 A nivel de Planeación existe el "Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información" vigencia 2021 que establece la relación entre los activos de información y los riesgos de seguridad y privacidad de la información, lo cual es consistente con MSPI, pero en la práctica no se han levantado los activos de información tecnológico y por ende no hay un análisis de riesgos articulado con activos.

👉 El plan adolece de actividades a desarrollar en la vigencia 2021 para la identificación y tratamiento de riesgos de SPI tales como: actualización de la metodología de gestión de riesgos, la identificación de activos críticos, la identificación de riesgos para esos activos, su valoración, el establecimiento de estrategias para mitigarlos, evitarlos transferirlos o aceptarlos y finalmente la construcción de planes de contingencia y continuidad para los riesgos aceptados y el permanente seguimiento "medible" y evidenciado de la efectividad de los controles para su tratamiento. Vale aclarar que algunas de estas actividades están en el Plan de Seguridad y privacidad de la información que se extrae a continuación, pero solo la actualización metodológica está programada para una fecha inferior al inicio de la auditoría. A la fecha la actividad no está finalizada.

Imagen 80 Extracción Plan de Seguridad y Privacidad de la Información

4.1	Actualizar y ajustar la metodología de riesgos de seguridad de la información	Política, manual o guía de riesgos de seguridad de la información	15 Febrero	30 Abril
4.2	Identificación y análisis de riesgos de seguridad de la información	Matriz de riesgos de seguridad de la información	02 Agosto	30 Noviembre
4.3	Comunicación de riesgos de seguridad de la información	Acta	03 Diciembre	17 Diciembre
4.4	Plan de tratamiento de riesgos de seguridad de la información	Matriz de riesgos de seguridad de la información – Acta o documento de plan de tratamiento	01 Octubre	30 Noviembre
4.5	Seguimiento y revisión de riesgos de seguridad de la información	Acta	Marzo 2022	Abril 2022

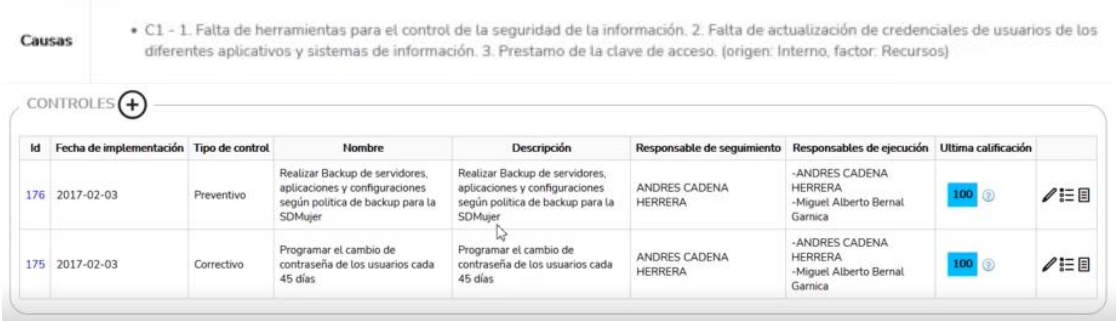
👉 A nivel de registro oficial se utiliza la herramienta kawak, en la cual se tienen registrados tres riesgos para el Proceso de Gestión Tecnológica, que no dan cubrimiento a la totalidad de los riesgos tecnológicos de manera alineada con la implementación MSPI, que establece la relación entre los riegos, los activos de información y los controles de la norma ISO 27002:2013. Para los riesgos y acciones contempladas se emiten algunas observaciones:

Imagen 81 Observaciones al tratamiento de riesgos

<table>
<tr><th>RIESGO</th><th>OBSERVACIONES AUDITORÍA</th></tr>
<tr><td>Caídas de Red (comunicaciones, internet y sistemas)</td><td>
Causas • C1 - 1. Daño de Equipos de comunicaciones. 2. Daño del Sistema de alimentación interrumpida (UPS). 3. El no pago de los servicios. 4. Errores humanos. (origen: Interno, factor: Recursos)
Efectos • 1. Retrasos y dificultades en las labores de las servidoras y servidores de la Entidad. 2. Incumplimientos de las obligaciones de la entidad. 3. Inicio de procesos disciplinarios internos y externos 4. Pérdida de información.
CONTROLES ⊕
<table>
<tr><th>Id</th><th>Fecha de implementación</th><th>Tipo de control</th><th>Nombre</th><th>Descripción</th><th>Responsable de seguimiento</th><th>Responsables de ejecución</th></tr>
<tr><td>165</td><td>2017-02-03</td><td>Preventivo</td><td>Establecer control de acceso al centro de cómputo</td><td>Establecer control de acceso al centro de cómputo.</td><td>ANDRES CADENA HERRERA</td><td>-Miguel Alberto Bernal Garnica</td></tr>
<tr><td>163</td><td>2017-02-03</td><td>Preventivo</td><td>Realizar la programación de mantenimiento correctivo y preventivo servidores y equipos de comunicaciones.</td><td>Programación de mantenimiento correctivo y preventivo servidores y equipos de comunicaciones.</td><td>ANDRES CADENA HERRERA</td><td>-ANDRES CADENA HERRERA
-Miguel Alberto Bernal Garnica</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>RIESGO</th><th>OBSERVACIONES AUDITORÍA</th></tr>
<tr><td></td><td>El riesgo y sus controles están correctamente declarados y se llevan las evidencias en la herramienta
 
EVALUACIÓN - CONTROL DE RIESGO
Histórico de evaluaciones
<table>
<tr><th>Fecha evaluación</th><th>Resultado por variable</th><th>Resultado total</th><th>Archivos adjuntos</th></tr>
<tr><td>2021-08-27 16:31:46</td><td>- Posee una herramienta para ejercer el control. (H) = 15
- Existen manuales instructivos o procedimientos para el manejo de la herramienta (D) = 15
- En el tiempo que lleva la herramienta ha demostrado ser efectiva. (T) = 30
- Están definidos los responsables de la ejecución del control y del seguimiento. (R) = 15
- La frecuencia de la ejecución del control y seguimiento es adecuada. (F) = 25</td><td>100</td><td>entrada datacenter 23dic2020 - 13agos2021.pdf</td></tr>
<tr><td>2021-09-03 21:39:13</td><td>- Posee una herramienta para ejercer el control. (H) = 0
- Existen manuales instructivos o procedimientos para el manejo de la herramienta (D) = 15
- En el tiempo que lleva la herramienta ha demostrado ser efectiva. (T) = 30
- Están definidos los responsables de la ejecución del control y del seguimiento. (R) = 15
- La frecuencia de la ejecución del control y seguimiento es adecuada. (F) = 25</td><td>85</td><td>1 Caidas de red.zip</td></tr>
</table>

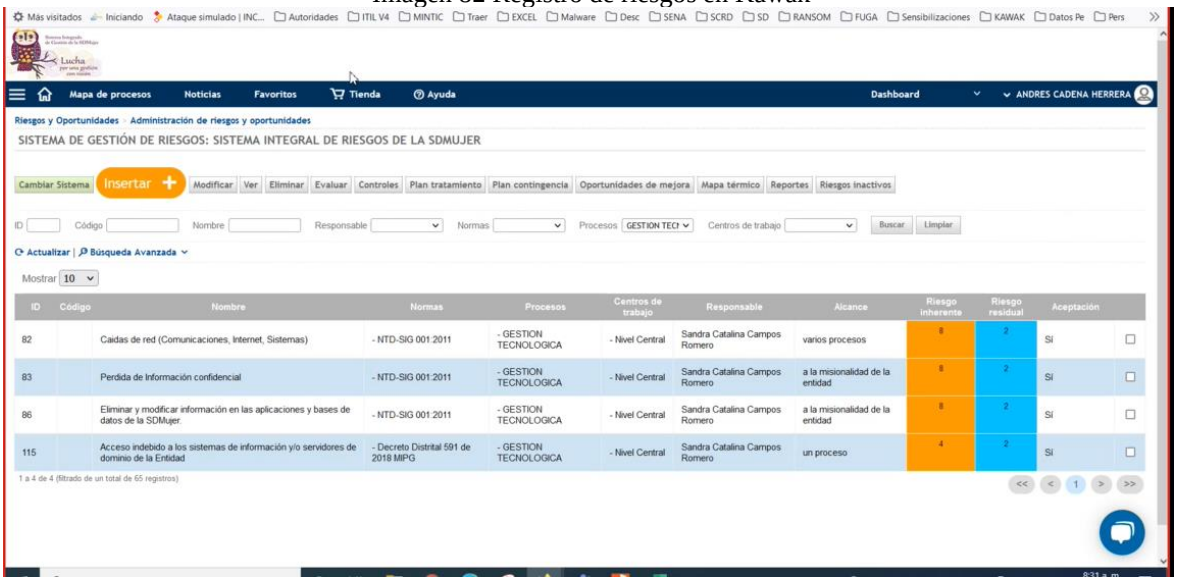
Se maneja correctamente el registro de acceso al centro de computo
Se evidencian los mantenimientos a los servidores y equipos de comunicaciones de manera articulada con el PLAN DE MANTENIMIENTO PREVENTIVO A EQUIPOS INFORMATICOS y los programas o cronogramas de mantenimientos.
Se evidencian los mantenimientos a sistemas de información junto con el Plan y los cronogramas.</td></tr>
<tr><td>Perdida de Información confidencial</td><td> 
Causas
• C1 - 1. Caída de servidores, 2. Manipulación de la información. 3. Falta de backup (respaldo externo) 4. Préstamo de usuarios y contraseñas. 5. Falta de seguridad Perimetral. (origen: Interno, factor: Recursos)
Efectos
• 1. Retrasos y dificultades en las labores de las servidoras y servidores de la Entidad. 2. Reportes erróneos.
• 1. Duplicidad de la información. 2. Bajos niveles de seguridad en la información. 3. Retrasos en el procesamiento de datos por la necesidad de verificar y depurar la información.
<table>
<tr><th>Id</th><th>Fecha de implementación</th><th>Tipo de control</th><th>Nombre</th><th>Descripción</th><th>Responsable de seguimiento</th><th>Responsables de ejecución</th><th>Ultima calificación</th><th></th></tr>
<tr><td>248</td><td>2018-02-26</td><td>Preventivo</td><td>Monitorear las amenazas que puedan vulnerar los equipos de cómputo, así como la información de la entidad</td><td>Monitorear las amenazas que puedan vulnerar los equipos de cómputo, así como la información de la entidad</td><td>ANDRES CADENA HERRERA</td><td>-Miguel Alberto Bernal Garnica</td><td>100</td><td></td></tr>
<tr><td>168</td><td>2017-02-03</td><td>Preventivo</td><td>Socializar la política de seguridad de la SDMujer</td><td>Socializar la política de seguridad de la SDMujer</td><td>ANDRES CADENA HERRERA</td><td>-ANDRES CADENA HERRERA</td><td>100</td><td></td></tr>
<tr><td>167</td><td>2017-02-03</td><td>Preventivo</td><td>Realizar Backup de servidores, aplicaciones y configuraciones según política de backup para la SDMujer</td><td>Realizar Backup de servidores, aplicaciones y configuraciones según política de backup para la SDMujer</td><td>ANDRES CADENA HERRERA</td><td>-Gleidy Jeniffer Jerez Mayorga
-Miguel Alberto Bernal Garnica
-GIOVANNY BENITEZ MORALES</td><td>100</td><td></td></tr>
<tr><td>166</td><td>2017-02-03</td><td>Preventivo</td><td>Realizar la programación de mantenimiento correctivo y preventivo servidores y equipos de comunicaciones.</td><td>Realizar la programación de mantenimiento correctivo y preventivo servidores y equipos de comunicaciones.</td><td>ANDRES CADENA HERRERA</td><td>-Miguel Alberto Bernal Garnica</td><td>100</td><td></td></tr>
</table>

Se presenta evidencia del monitoreo de amenazas
Se presenta evidencia de la socialización de políticas de seguridad
Se presenta evidencia de los backups de imágenes, bases de datos, servidores.</td></tr>
<tr><td>Eliminar y modificar información en las aplicaciones y bases de datos de la SDMujer</td><td> 
Causas
• C1 - 1. Falta de herramientas para el control de la seguridad de la información. 2. Falta de actualización de credenciales de usuarios de los diferentes aplicativos y sistemas de información. 3. Prestamo de la clave de acceso. (origen: Interno, factor: Recursos)
CONTROLES
<table>
<tr><th>Id</th><th>Fecha de implementación</th><th>Tipo de control</th><th>Nombre</th><th>Descripción</th><th>Responsable de seguimiento</th><th>Responsables de ejecución</th><th>Ultima calificación</th><th></th></tr>
<tr><td>176</td><td>2017-02-03</td><td>Preventivo</td><td>Realizar Backup de servidores, aplicaciones y configuraciones según política de backup para la SDMujer</td><td>Realizar Backup de servidores, aplicaciones y configuraciones según política de backup para la SDMujer</td><td>ANDRES CADENA HERRERA</td><td>-ANDRES CADENA HERRERA
-Miguel Alberto Bernal Garnica</td><td>100</td><td></td></tr>
<tr><td>175</td><td>2017-02-03</td><td>Correctivo</td><td>Programar el cambio de contraseña de los usuarios cada 45 días</td><td>Programar el cambio de contraseña de los usuarios cada 45 días</td><td>ANDRES CADENA HERRERA</td><td>-ANDRES CADENA HERRERA
-Miguel Alberto Bernal Garnica</td><td>100</td><td></td></tr>
</table>

Se presenta evidencia de los backups de servidores y aplicaciones</td></tr>
</table>

RIESGO	OBSERVACIONES AUDITORÍA
	El cambio de contraseña no es consistente, el control dice 45 días, la política dice 92, las directivas 180 y en la práctica no se solicita cambio de contraseña, en el numeral 6.2.2. se evidencian accesos del auditor por debilidades en cambio de contraseña.
Acceso indebido a los sistemas de información y/o servidores de dominio de la entidad	**Causas** • C1 - Debilidades en la implementación de controles de acceso. (origen: Interno, factor: Recursos) • C2 - Intereses particulares de servidoras(es) públicos y/o contratistas (origen: Interno, factor: Cultura) • C3 - Presiones indebidas u ofrecimiento de dádivas por parte de terceros (origen: Interno, factor: Cultura) CONTROLES (+) Id | Fecha de implementación | Tipo de control | Nombre | Descripción | Responsable de seguimiento | Responsables de ejecución | Ultima calificación 275 | 2019-01-25 | Preventivo | Establecer control de acceso al centro de computo | Establecer control de acceso al centro de computo | ANDRES CADENA HERRERA | -ANDRES CADENA HERRERA | 100 274 | 2019-01-25 | Preventivo | Programar el cambio de contraseña de los usuarios cada 45 días | Programar el cambio de contraseña de los usuarios cada 45 días | ANDRES CADENA HERRERA | -ANDRES CADENA HERRERA | 100 Se presentan las mismas evidencias anteriores

Imagen 82 Registro de riesgos en Kawak



A nivel de seguimiento se hace cuatrimestralmente el seguimiento a los riesgos TIC y de Seguridad.

6.3.2. PLAN DE CONTINUIDAD

6.3.2.1. FORTALEZAS Y OPORTUNIDADES DE MEJORA

La entidad cuenta con un sistema de hiperconvergencia que permite brindar continuidad y disponibilidad de los servicios y aplicaciones que se prestan desde el centro de datos principal, donde está alojado el sistema

misional, la administración de la red, infraestructura de servidores Windows y Linux, el sistema de gestión documental, aplicaciones cliente servidor y aplicativos webs entre otros. De igual manera se ha adquirido un nodo de contingencia para el sistema de hiperconvergencia existente en la Secretaría Distrital de la Mujer.

👎 Se cuenta con el procedimiento: GT-PR-13 Administración del Plan de Continuidad del Negocio TIC, en el que se especifica los pasos para crear y mantener el plan de continuidad de la entidad, sin embargo, el plan de continuidad de la Entidad aún no ha sido creado.

👎 No se ha adelantado un Análisis de Impacto al Negocio BIA como primer paso de la implementación del Plan de Continuidad una vez seleccionados los riesgos extremos asumidos, con el fin de identificar los activos o servicios tecnológicos críticos, y los posibles impactos que se tendrían si éstos no se encuentran disponibles y en correcto funcionamiento:

- Estimar los tiempos de contingencia y recuperación de los procesos esenciales a su operación normal después que ha ocurrido el incidente invalidante, de acuerdo a la tolerancia de la entidad para operar sin el servicio TIC.
- Los puntos de recuperación de los datos y condiciones de registro alterno durante contingencia

👉 Las copias de respaldo de los servidores virtuales, la hiperconvergencia y las protecciones eléctricas del centro de cómputo, son las únicas herramientas de contingencia con la que cuenta la entidad para garantizar la continuidad de la operación, lo que expone a la Entidad a no tener la capacidad de respuesta en los tiempos máximos BIA y es insuficiente para cumplir con una correcta gestión de continuidad, además no se ha articulado con el PLAN DE EMERGENCIA Y CONTINGENCIAS DE LA SECRETARIA DISTRITAL DE LA MUJER, en el sentido de contingencia por daño parcial o total del centro de cómputo.

👉 Se observa que el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, no incluye la relación entre el tratamiento de riesgos de activos críticos y los planes de continuidad, teniendo en cuenta la correlación entre activos críticos – riesgos aceptados y planes de contingencia y continuidad.

6.3.3. PROCEDIMIENTOS DE BACKUP Y RECUPERACIÓN

6.3.3.1. FORTALEZAS Y OPORTUNIDADES DE MEJORA

👍 En el manual de gestión tecnológica en el numeral 3.10 Administración de backup y recuperación de la información, se define correctamente la política y estrategia de copias de seguridad de la Entidad, en este numeral se detalla de forma adecuada la identificación de la información que será objeto de realización de copias de seguridad, su periodicidad, tiempos de retención, tipo de backups a realizar y responsables de su ejecución.

👍 La información a la cual se le realizan copias de respaldo según el manual es:

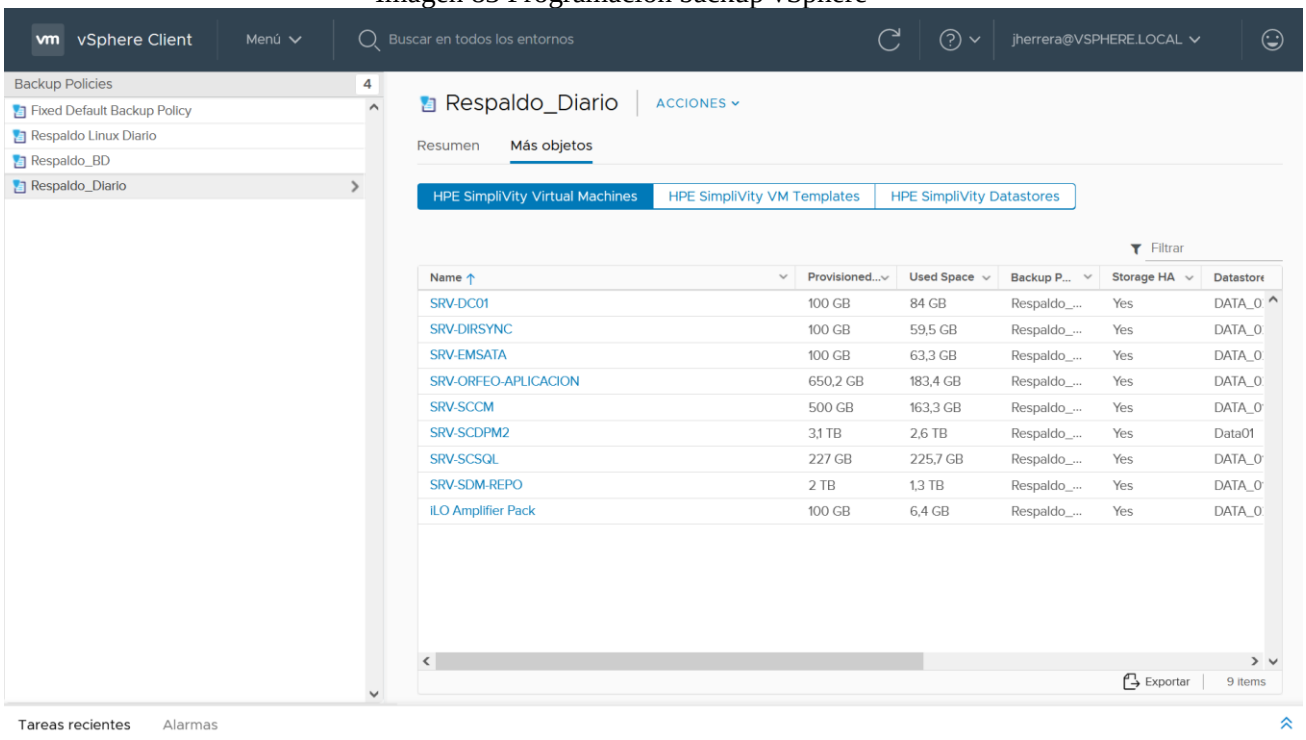
- ✓ Información de bases de datos (Oracle, SQL, Mysql, Maria-DB, Postgres)
- ✓ FileSystem: Datos almacenados en las particiones lógicas de los servidores.
- ✓ Respaldo de imágenes virtuales de sistemas operativos Windows Server.
- ✓ Respaldo de imágenes virtuales de sistemas operativos Linux.
- ✓ Respaldo de Aplicaciones misionales (Simisional, Lucha, Sofía, etc.)
- ✓ Respaldo de Moodle.
- ✓ Respaldo de Aplicativos Web (Pagina- Intranet).

- ✓ Respaldo de aplicaciones en la nube.
- ✓ Respaldo de recursos compartidos en un servidor de repositorio de información.
- ✓ Equipos de Comunicaciones.
- ✓ Log de eventos.
- ✓ Respaldo de Buzones de correo electrónico.

Se definen correctamente tareas de restauración aleatoria mensuales para verificar la integridad de la información respaldada.

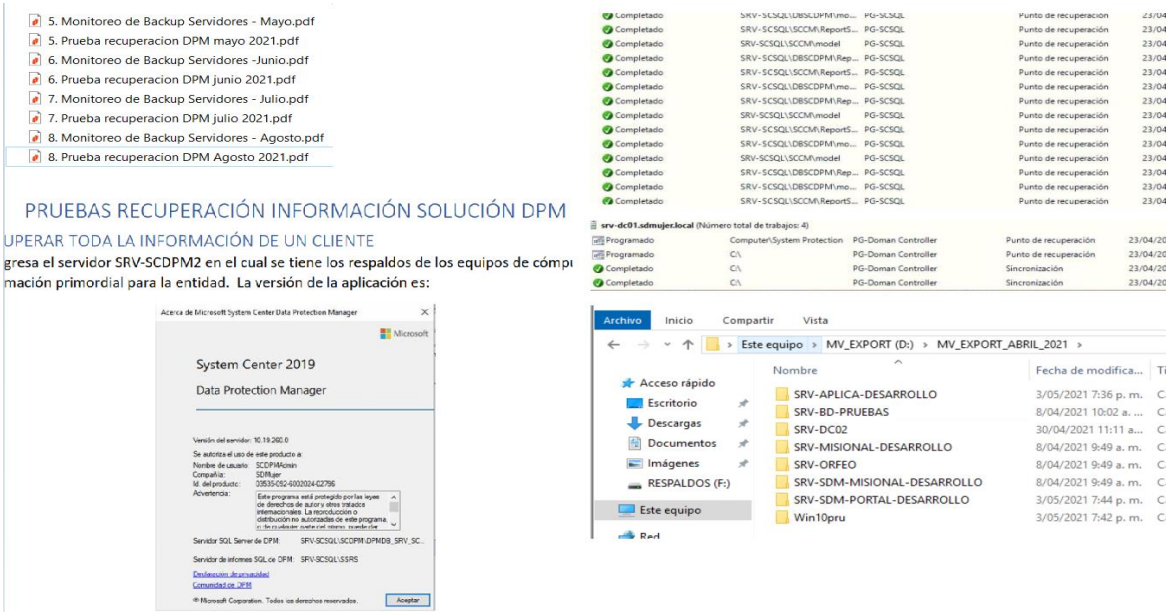
Las copias de los servidores virtualizados se tienen programadas de forma adecuada en la consola vSphere y se realizan revisiones de su correcto funcionamiento:

Imagen 83 Programación backup vSphere



Se realiza y documenta correctamente el monitoreo de los backups de los servidores y las pruebas de recuperación de información desde el Data Protección Manager, en donde se puede validar que se realizan respaldos a los servidores y en las pruebas de restauración se elige mensualmente una restauración aleatoria de alguno de los equipos protegidos:

Imagen 84 Evidencias de recuperación



Fuente: Información suministrada por el proceso auditado

👉 De acuerdo a lo descrito en la administración de backups y recuperación, las ubicaciones finales de los respaldos realizados son unidades de almacenamiento (SAN) dentro de la entidad, no se describe, ni especifica las ubicaciones de los respaldos fuera de la entidad o en la nube como contingencia en caso de desastres totales en el centro de cómputo o en las oficinas principales. Vale aclarar que en el anexo técnico de la adquisición e implementación de la nueva solución de backups se contempla este punto, se debe validar su cumplimento.

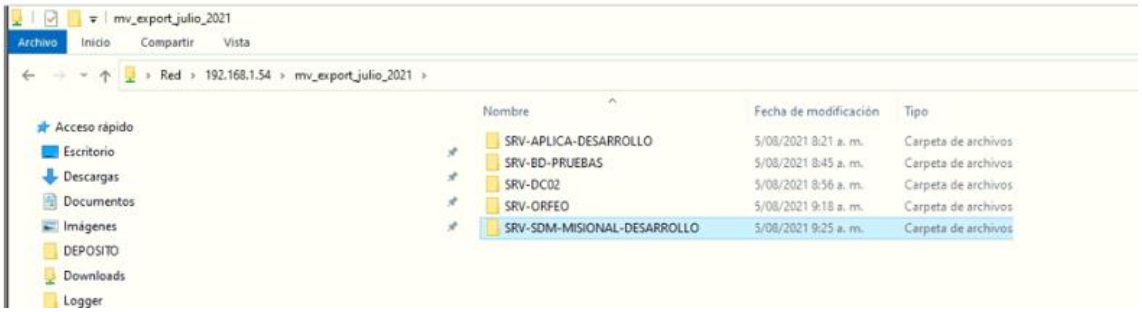
👍 Ya se adelantó la contratación de una solución de backups (contrato 936 de 2021), que permita administrar y controlar todos los respaldos desde una única plataforma y que cuente con todas las funcionalidades necesaria para tener una estrategia de copias de seguridad actualizada y con las mejores prácticas, en el anexo técnico de este contrato se encuentran correctamente detallas las características y especificaciones necesarias para la solución y se contempla de forma adecuado los respaldos de servidores físicos e integración con soluciones de antivirus y motores de bases de datos.

👉 Si bien en el numeral Administración de backup y recuperación de la información se determinan las frecuencias, tipos de backups y retención de las copias de seguridad, no se cuenta con un único formato del **Plan de Backups** que permita identificar de forma detallada, y en un único documento toda la información respaldada, la frecuencia, retención, detalle de las ubicaciones intermedias y finales, ubicación de logs, permisos de acceso y de seguridad de todos los backups generados en la Entidad. Esto además de generar dependencia de las herramientas utilizada para programar y realizar las copias, podría generar retrasos en las restauraciones en caso de contingencia y genera dependencia de conocimiento de los encargados del proceso.

👎 Se debe revisar la seguridad de acceso a los respaldos de servidores generados, y su disposición final debe estar correctamente protegida a accesos o copias no autorizadas de estos respaldos. En las pruebas realizadas

por la auditoria se encontraron recursos compartidos (servidor 192.169.1.54 mv_export_julio_2022) sin protección con copias de seguridad de los servidores virtuales y que el auditor logro copiar a su equipo.

Imagen 85 Prueba de copia de archivos de backup servidores al equipo del auditor



6.4. IMPLEMENTACIÓN DE ACCESIBILIDAD WEB - NTC 5854

6.4.1. FORTALEZAS Y OPORTUNIDADES DE MEJORA

A partir de la resolución 1519 de 2020, se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.

La Ley Estatutaria 1712 del 6 de marzo de 2014 consagró el Derecho de Acceso a la Información Pública como un derecho fundamental que tienen todas las personas para conocer de la existencia y acceder a la información pública en posesión o bajo control de los sujetos obligados, en su artículo 3o, contempla el desarrollo del principio de la calidad de la información, y determina que la información pública debe ser procesable en formatos accesibles. Por dicho motivo, en la mencionada resolución, se definen las directrices de accesibilidad web, conforme lo dispone el artículo 2.1.1.2.2.2 del Decreto 1081 del 2015. ÚLTIMA FECHA DE ACTUALIZACIÓN: 13 DE OCTUBRE DE 2021 "Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República.

Atendiendo dicha resolución 1519 ARTÍCULO 3o. DIRECTRICES DE ACCESIBILIDAD WEB. a partir del 1 de enero del 2022, la entidad deberá dar cumplimiento a los estándares AA de la Guía de Accesibilidad de Contenidos Web (Web Content Accesibillity Guidelines - WCAG) en la versión 2.1, expedida por el World Web Consortium (W3C).

- Así las cosas, la Secretaria de la Mujer, atiende los lineamientos de accesibilidad de que trata la normativa y en cumplimiento de accesibilidad en medios electrónicos para población en situación de discapacidad, con el fin que sus medios de comunicación electrónica dispuestos para divulgar la información cumplan con las directrices de accesibilidad que dicte el Ministerio de Tecnologías de la Información y las Comunicaciones a través de los lineamientos que se determinen en la Estrategia de Gobierno en línea.

- La entidad ha contratado y asignado a un profesional dedicado a cumplir con esta labor, lo cual resulta no solo responsable con su compromiso, sino efectivo para lograr la meta establecida.

👍 Se observa que el profesional asignado tiene profundo conocimiento de la norma técnica 5854 y sus 4 principios: Principio 1 – Perceptible, Principio 2 – Operable, Principio 3 – Comprensible y Principio 4 – Robusto.

👉 Es de anotar que, si bien el cumplimiento de la norma en gran medida se establece a partir del etiquetado del lenguaje para que las herramientas de los usuarios discapacitados funcionen, otro componente necesario es que también los contenidos cumplan con los requisitos de accesibilidad, lo cual esta bajo la responsabilidad de los generadores de contenidos al interior de la entidad o proveedores y no solo del proceso de gestión tecnológica. El interlocutor manifiesta que no todos los contenidos cumplen con estos requisitos. El plan de cambio, talleres y apropiación debería estar en cabeza de comunicaciones.

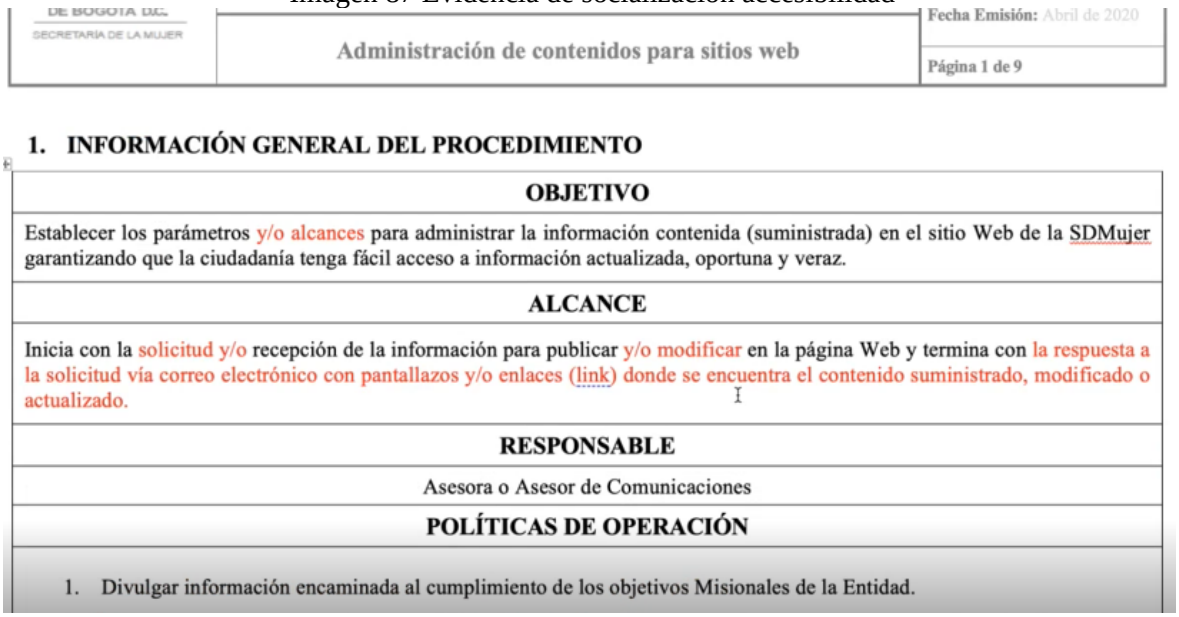
👍 El ejercicio se inició en febrero de 2021, dando prioridad a la publicación de la nueva página principal de la SDM, y posteriormente el establecimiento de la robustez del código bajo una estrategia de ajuste ágil, para esto se adelantó un diagnóstico de los 50 criterios, documentado correctamente en el instrumento "WCAG21 R65.xlsx" donde el contratista asignado ha llevado registro para cada criterio del estado de cumplimiento, las evidencias y observaciones y recomendaciones

👉 El ejercicio se ha adelantado sin un plan de trabajo formal que involucre a los demás responsables de generación de contenidos, con el fin de garantizar que la implementación de cobertura a todos medios de comunicación electrónica dispuestos para divulgar la información. Si bien se compartieron algunos lineamientos y directrices, no se hizo un plan formal con talleres para garantizar el compromiso y llevar seguimiento al cumplimiento de las directrices. Vale aclarar que el contratista a cargo ha adelantado la actualización del procedimiento de administración de contenidos en página web que fue socializado con apoyo de comunicaciones, además de generar directrices, procedimiento de piezas gráficas y material comunicativo, además de un ejercicio de arquitectura de información para plantear el portal.

Sin embargo, los resultados deben escalarse para que el liderazgo en gestión del cambio se de a más alto nivel para garantizar sostenibilidad a futuro y eliminar las malas prácticas dado que es un proceso dinámico que no se resuelve con una implementación puntual.

Imagen 86 Correo evidencia de socialización accesibilidad

Imagen 87 Evidencia de socialización accesibilidad



DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER | Administración de contenidos para sitios web | Fecha Emisión: Abril de 2020 | Página 1 de 9

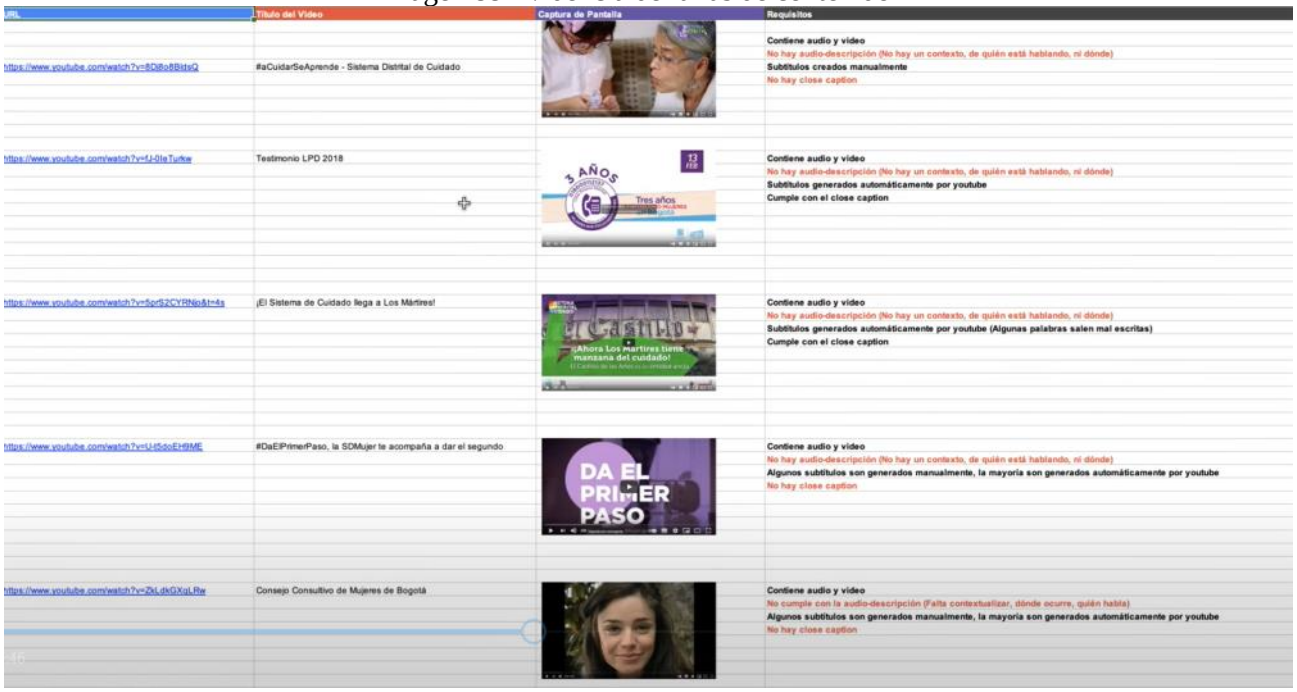
1. INFORMACIÓN GENERAL DEL PROCEDIMIENTO

OBJETIVO
Establecer los parámetros y/o alcances para administrar la información contenida (suministrada) en el sitio Web de la SDMujer garantizando que la ciudadanía tenga fácil acceso a información actualizada, oportuna y veraz.
ALCANCE
Inicia con la solicitud y/o recepción de la información para publicar y/o modificar en la página Web y termina con la respuesta a la solicitud vía correo electrónico con pantallazos y/o enlaces (link) donde se encuentra el contenido suministrado, modificado o actualizado.
RESPONSABLE
Asesora o Asesor de Comunicaciones
POLÍTICAS DE OPERACIÓN
1. Divulgar información encaminada al cumplimiento de los objetivos Misionales de la Entidad.

Fuente: Documento aportado por el proceso auditado

👉 En relación al no cumplimiento en los contenidos, tal es el caso del criterio AA 1.2.5 audio descripción para todos los videos, frente al cual se registra que no se cumple por razones de contenido. Vale aclarar que hay varios criterios señalados en la misma situación.

Imagen 88 Evidencia de fallas de contenido



	Título del Video	Captura de Pantalla	Requisitos
https://www.youtube.com/watch?v=8D8o8BtdsQ	#aCuidarSeAprende - Sistema Distrital de Cuidado		Contiene audio y video No hay audio-descripción (No hay un contexto, de quién está hablando, ni dónde) Subtítulos creados manualmente No hay close caption
https://www.youtube.com/watch?v=tJ-0IeTurkw	Testimonio LPD 2018		Contiene audio y video No hay audio-descripción (No hay un contexto, de quién está hablando, ni dónde) Subtítulos generados automáticamente por youtube Cumple con el close caption
https://www.youtube.com/watch?v=5prS2CYRNio&t=4s	¡El Sistema de Cuidado llega a Los Mártires!		Contiene audio y video No hay audio-descripción (No hay un contexto, de quién está hablando, ni dónde) Subtítulos generados automáticamente por youtube (Algunas palabras salen mal escritas) Cumple con el close caption
https://www.youtube.com/watch?v=tJ-t5ooEH9ME	#DaElPrimerPaso, la SDMujer te acompaña a dar el segundo		Contiene audio y video No hay audio-descripción (No hay un contexto, de quién está hablando, ni dónde) Algunos subtítulos son generados manualmente, la mayoría son generados automáticamente por youtube No hay close caption
https://www.youtube.com/watch?v=ZkLdkGXqLRw	Consejo Consultivo de Mujeres de Bogotá		Contiene audio y video No cumple con la audio-descripción (Falta contextualizar, dónde ocurre, quién habla) Algunos subtítulos son generados manualmente, la mayoría son generados automáticamente por youtube No hay close caption

Fuente: Documento aportado por el proceso auditado

Al momento de la auditoría el contratista presenta un 86% de cumplimiento y el 14% restante es viable de resolver 3 por parte del contratista a cargo de la implementación y 4 relacionados con contenidos, 3 de ellos por videos antiguos sobre los que las áreas deben decidir la continuidad de su publicación.

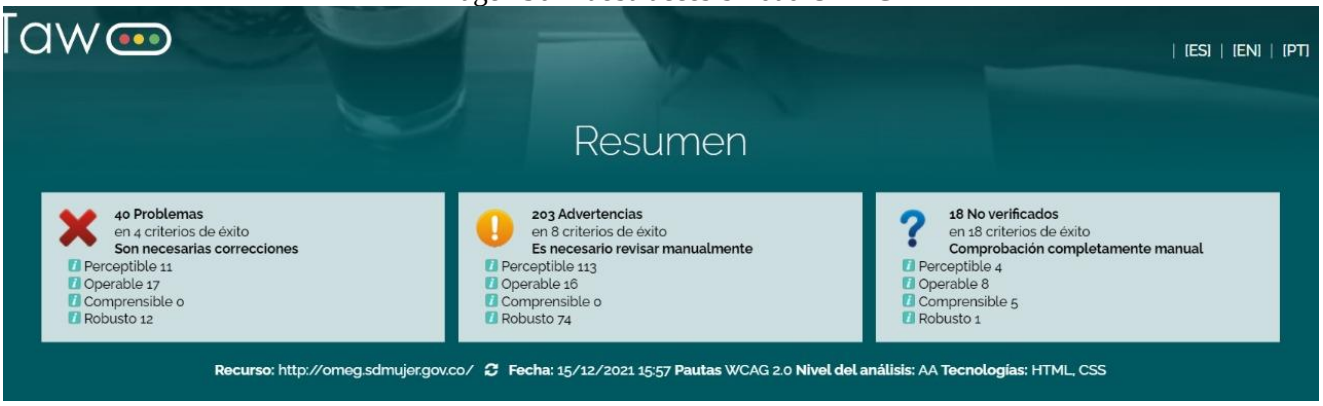
Imagen 89 Evidencia de avance accesibilidad

¿Cumple?	¿Evidencia?
3	6%
4	8%
43	86%
50	100%

Fuente: Documento aportado por el proceso auditado

👉 El alcance logrado se ha enfocado a los desarrollos en Drupal del portal de la SDM, por lo tanto, es importante adelantar un diagnóstico de otros sitios o subsitios que pudieron ser objeto de cumplimiento y que están a cargo de otras áreas, ejemplo el Observatorio de Mujeres y Equidad de Género, sobre el cual el auditor ejecuto pruebas de cumplimiento con la herramienta TAWDIS, que fue creada por la Fundación CTIC en España teniendo como referencia técnica las pautas de accesibilidad al contenido web (WCAG 2.0) del W3C que en Colombia fue homologada con la norma NTC 5854 Accesibilidad a páginas web y que Mintic considera una opción válida (ver https://www.gobiernodigital.gov.co/623/articles-74967_recurso_14.pdf), en los resultados de la herramienta se corrobora lo señalado con respecto a la necesidad de hacer extensivo el ejercicio a otros sitios en cumplimiento de la citada norma.

Imagen 90 Prueba accesibilidad OMEG



6.5. DESARROLLO Y ADQUISICIÓN DE SOFTWARE APLICATIVO

6.5.1. FORTALEZAS Y OPORTUNIDADES DE MEJORA

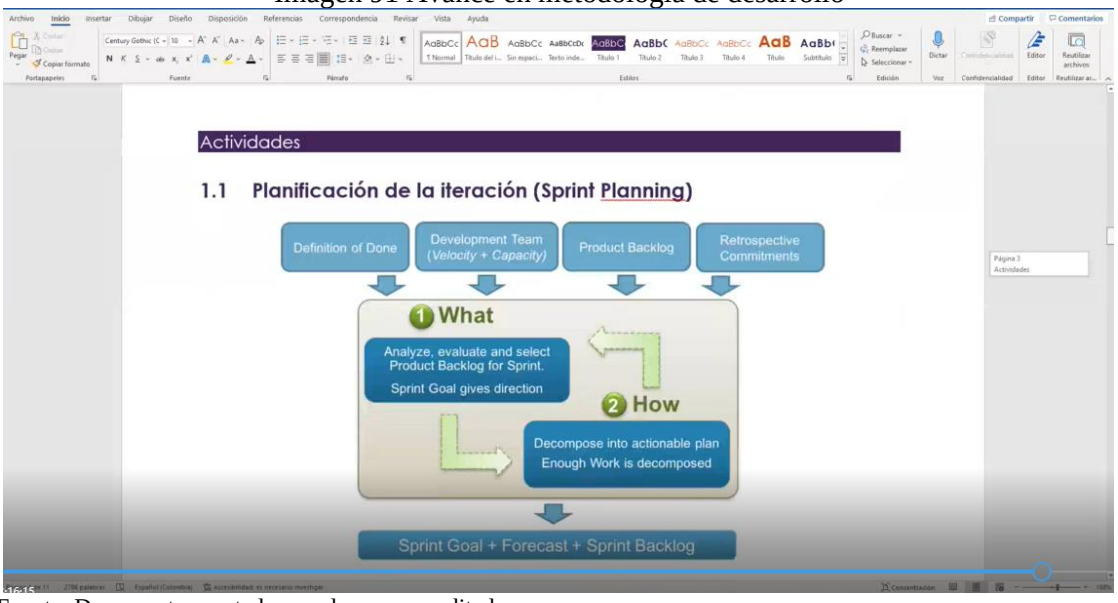
👍 El área cuenta con un catálogo de sistemas de información "*Inventario de Información de Aplicacione.xlsxs*" como lo determina el dominio de sistemas de información del Marco de Referencia de Arquitectura Empresarial, pero puede ser mejorado adicionando los atributos:

- Servidor de contingencia

- Si es propio o con terceros
- Si está amparado en un contrato de soporte
- Versión
- Si es fuente de datos abiertos

El equipo de desarrollo está en proceso de estructuración de una metodología de desarrollo de software orientada a scrum, lo cual es la mejor estratega para la entidad dado de su misionalidad no es hacer software, es un equipo reducido de desarrollo y es una metodología que tiene menor carga documental. Sin embargo, solo es efectiva si se respetan las reglas de scrum para desarrollo ágil y la gestión controlada de cambios para garantizan la entrega de componentes de software en los tiempos estimados, con un mínimo de defectos y sin reapertura por obviedades de especificación y diseño.

Imagen 91 Avance en metodología de desarrollo



Fuente: Documento aportado por el proceso auditado

Se cuenta con instrumentos procedimentales para la gestión de desarrollo de software que aportan una base importante, pero pueden ser mejorados en el marco de la nueva metodología en construcción

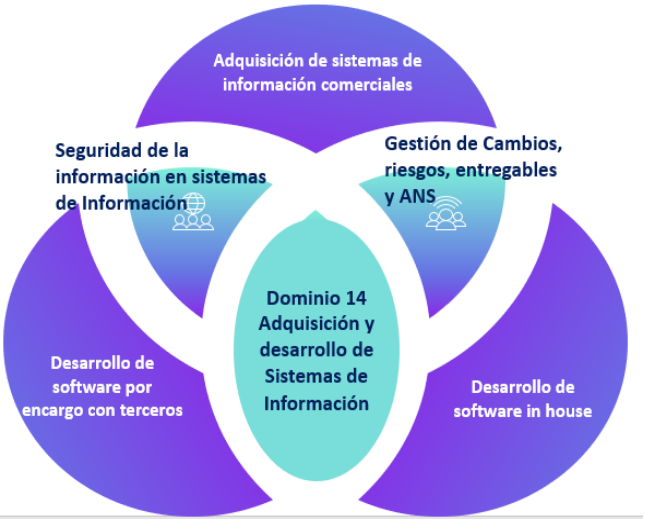
- GT-FO-24 - DEFINICIÓN DEL PROYECTO DE SOFTWARE - V1: el formato es correcto como Especificación del Requerimiento del proyecto en general
- GT-FO-19 - PILA DE PRODUCTO DE SOFTWARE - V1: es mas un formato de declaración de historias de usuario que puede ser un anexo a cada elemento de una pila de producto, ya que una pila es un listado centralizado de requerimientos de todas las áreas sobre todos los sistemas información, caracterizado, priorizado y con estimaciones de esfuerzo para determinar su inclusión en iteraciones o Sprints. La mejor practica es usar una herramienta tipo trello o jira.
- GT-FO-22 - PERSISTENCIA DE DATOS DE SOFTWARE - V2: el formato es correcto, pero puede ser mejorado con análisis de impactos por merge con otros desarrollos sobre el mismo modelo de datos. Vale aclarar que, aunque se controle el versionamiento por GitLab, este documento es valioso para control integrado de cambios e insumos para actualización de documentos de arquitectura general

por solución.

- GT-FO-26 - SOLICITUD DE CAMBIOS - RFC - V1: es suficientemente detallado para garantizar que el equipo de infraestructura tenga autonomía para un despliegue, tiene minutograma y rollback. Es importante anotar que el RFC tiene dos propósitos: pasar el desarrollo a producción y probar que los componentes para despliegue sean correctos. Se complementa con el GT-FO-20 - PASO A PRODUCCIÓN DE SOFTWARE - V2
- GT-FO-25 - MATRIZ DE PRUEBAS DE SOFTWARE - V1: es correcta, sin embargo, es recomendable usar una herramienta para registrar los defectos con el fin de llevar indicadores de calidad en desarrollo de software.
- GT-FO-23 - MANUAL DE USUARIO DE SOFTWARE - V1: es correcto, se puede mejorar con inclusión de casos de soporte comunes para autogestión.
- GT-FO-21 - MANUAL TÉCNICO DESARROLLO SOFTWARE - V2: ver la posibilidad de unificarlo con GT-FO-22 - PERSISTENCIA DE DATOS DE SOFTWARE - V2. y orientarlo más a documento de arquitectura de la solución.

A nivel de los lineamientos del MSPI para el dominio 14, los instrumentos creados a la fecha no dan cobertura total a los 3 escenarios en los cuales se da la adquisición y desarrollo de software aplicativo:

Imagen 92 Alcance dominio 14 MSPI



Fuente: elaboración propia con base en ISO 27001:2013

- ✓ El primer caso corresponde a Adquisición de Sistemas de Información Comerciales, Para este caso deben desarrollarse criterios mínimos de RFP (Request for Proposal), tipo lista de chequeo base para la selección que incluya de manera ponderada criterios; funcionales, técnicos, referencias, relación futura, legal, de seguridad y económica.
- ✓ El segundo caso corresponde al desarrollo de software por encargo a terceros, como es el caso de requerimientos adicionales sobre los sistemas existentes, para lo cual deben establecerse criterios de aceptación de entregables y cumplimiento de la metodología de desarrollo con trasferencia de conocimiento.
- ✓ El tercer caso corresponde al Desarrollo In House. Para lo cual se debe implementar una metodología de desarrollo.

6.6. SERVICIOS A USUARIOS TIC

6.6.1. INVENTARIOS Y MANTENIMIENTO DE HARDWARE Y SOFTWARE

6.6.1.1. FORTALEZAS Y OPORTUNIDADES DE MEJORA

En cuanto al mantenimiento de hardware se cuenta con el plan de mantenimiento preventivo a equipos informáticos 2021, en el cual se detallan y definen de forma adecuada las políticas alcance beneficios y las acciones a realizar en los mantenimientos:

Imagen 93 Evidencia plan mantenimiento equipos

PLAN DE MANTENIMIENTO PREVENTIVO A EQUIPOS INFORMÁTICOS 2021

Teniendo en cuenta que el objetivo del proceso de Gestión Tecnológica es desarrollar, implementar, mantener y gestionar la plataforma tecnológica existente en la Secretaría Distrital de la Mujer y asesorar la adquisición e implementación de nuevas tecnologías de información y comunicaciones que brinden soluciones eficaces a las necesidades de los procesos misionales y administrativos de la Secretaría Distrital de la Mujer y servicios a la comunidad en general Así mismo, el objetivo del procedimiento de mantenimiento preventivo a equipos informáticos es el de asegurar que los equipos informáticos de la entidad operen en óptimas condiciones con el propósito de garantizar el normal desarrollo de las actividades de la comunidad misional y administrativa, y en aras del mejoramiento continuo, se hace necesario elaborar e implementar del Plan anual de mantenimiento preventivo a los equipos informáticos.

Fuente: Documento aportado por el proceso auditado

Se cuenta con el procedimiento GT-PR-17 IMPLEMENTACIÓN Y MANTENIMIENTO DE SOLUCIONES DE INFORMACIÓN y el manual GT-MA-4 MANUAL DE DESARROLLO O MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.doc en los cuales se definen de forma adecuada los lineamientos y política s relacionadas con los mantenimientos a los sistemas de información

Se cuenta con cronogramas de mantenimientos preventivos para los diferentes equipos y para los sistemas de información, con sus respectivos formatos de checklist por sistema de información en donde se detalla y registran las actividades a realizar en cada mantenimiento.

Imagen 94 Evidencia programación mantenimiento SI

PROGRAMACIÓN DE MANTENIMIENTOS SISTEMAS DE INFORMACIÓN 2021								
			II SEMESTRE 2021					
			TIPO DE MANTENIMIENTO					
ITEM	Aplicativo	RESPONSABLE	PREVENTIVO	CORRECTIVO	Fecha de Inicio	Fecha Terminación	Hora	Realizado (Si/NO)
1	Aplicativo de Correspondencia	Grupos Sistemas de Información	X		20/08/2021	21/08/2021	10:00 p. m.	SI
2	icop.sdmujer.gov.co	Grupos Sistemas de Información	X		1/07/2021	1/07/2021	10:00 p. m.	SI
3	orfeo.sdmujer.gov.co	Grupos Sistemas de Información	X		20/08/2021	21/08/2021	10:00 p. m.	SI
4	Bogdata	Secretaria de Hacienda	X		11/08/2021	11/08/2021	14:00	SI
5	inventarios	Grupos Sistemas de Información	X		20/08/2021	21/08/2021	10:00 p. m.	SI
6	SIPMEG - Aplicación	Grupos Sistemas de Información	X		20/08/2021	21/08/2021	10:00 p. m.	SI
7	acosos.sdmujer.gov.co	Grupos Sistemas de Información	X		20/08/2021	21/08/2021	10:00 p. m.	SI
8	violeta.sdmujer.gov.co	Grupos Sistemas de Información	X		20/08/2021	21/08/2021	10:00 p. m.	SI
9	cursos	Ing de Gestión del Conocimiento	X		N/A	N/A	N/A	N/A
10	sofiapp.sdmujer.local	Grupos Sistemas de Información	X		20/08/2021	21/08/2021	10:00 p. m.	SI
11	Sistema de Infromacion Misional Producción -Aplicación	Ing de Gestión del Conocimiento	X		N/A	N/A	N/A	N/A
12	Sistema de Infromacion Misional Desarrollo - Aplicación	Ing de Gestión del Conocimiento	X		N/A	N/A	N/A	N/A

Fuente: Documento aportado por el proceso auditado

Imagen 95 Evidencia registro mantenimiento equipos

	SECRETARÍA DISTRITAL DE LA MUJER	Código:
	GESTIÓN TECNOLÓGICA	Versión:
	CHECK LIST MANTENIMIENTOS DE SISTEMAS DE INFORMACIÓN	Fecha de Emisión:
		Página 1

DEPENDENCIA:	Oficina Asesora de Planeación
PROCESO:	Gestión Tecnológica
Objetivo:	Plan de trabajo para realizar el proceso de mentenimientos de Sistemas de Información de la Entidad.
Aplicativo	ICOPS - SIS ICÓN RADICACIÓN DE INFORMES DE CONTRATISTAS
Participantes:	Laura Estefania Gómez Gleidy Jeréz Giovanny Benitez

INFORMACIÓN GENERAL			
Servidor Infraestructura	192.168.1.16	Motor de base de datos	ORACLE 12
Tipo Servidor	Apache 2.4.6	Dependencia o Area que utiliza	Administrativa y financiera
Lenguaje Programación	PHP Version 7.3	Administrador	Contratos- Financiera- Gestión Tecnológica
Servidor de base de datos	192.168.1.23		
Observaciones	Aplicativo en producción para el registro y control de los informes de actividades de los contratistas de la Secretaría Distrrital de la Mujer.		

ACTIVIDAD	ESTADO INICIAL	OBSERVACIONES	ESTADO FINAL	Check de Verficación		
				Actualizado	Verificado	Fecha
SISTEMA OPERATIVO						
Versionamiento	LINUX CENTOS 7 de 64		CentOS-7-2020.12.14-0		x	6/08/2021
Memoria	4 GB		24 GB		x	6/08/2021
Procesador	2 procesador Virtualización		2 Procesadores		x	6/08/2021
Sistema de Seguridad	N/A		Firewall		x	6/08/2021
MOTOR DE BASE DE DATOS						

Fuente: Documento aportado por el proceso auditado

- Evidencia programación anual de mantenimiento:

Imagen 96 Evidencia programación anual mantenimientos

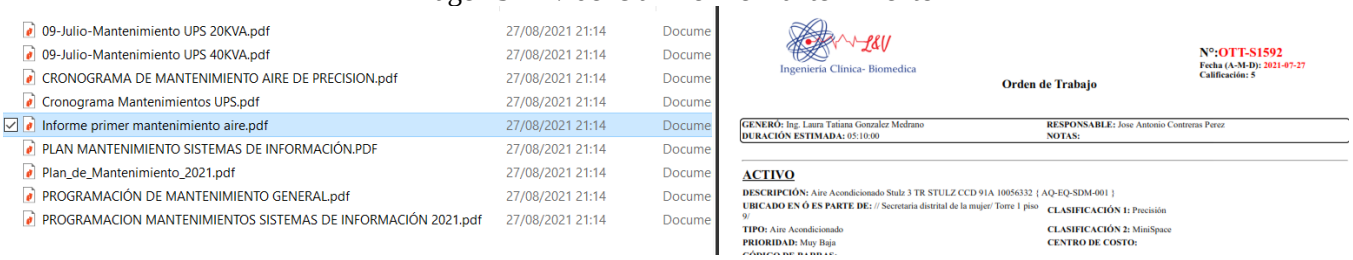
PROGRAMACION ANUAL MANTENIMIENTOS - CALENDARIO DE ACTIVIDADES 2021

ELEMENTOS	DESCRIPCION	PERSONAL	PREVENTIVO	CORRECTIVO	FECHA												
					SEGUNDO TRIMESTRE			REALIZADO SI/NO	TERCER TRIMESTRE			REALIZADO	CUARTO TRIMESTRE			REALIZADO SI/NO	RESPONSABLE
					F. INICIO	TERMINACIÓ	HORA		F. INICIO	F. TERMINACI	HORA		F. INICIO	TERMINACIÓ	HORA		
SERVIDORES	4 Equipos marca HP	Ing. de Infraestructura	X		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	20/10/2021				
	1 Equipo Marca lenovo	Ing. de Infraestructura	X		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	20/10/2021				
	2 Equipo Marca lenovo	Ing. de Infraestructura	X		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	20/10/2021				
	2 Equipos Maarca HP - Hiperconvergencia	Sanolivar	X		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	21/10/2021				
	1 Almacenamiento	Redcomputo	X		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	22/10/2021				
EQUIPOS DE COMUNICACIONES																	
SWITCH	5 Switch Marca CISCO	Ing. de Infraestructura	X		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	20/10/2021				
	3 Switch Marca HP	Ing. de Infraestructura	X		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	20/10/2021				
	1 switch F.O. Marca	Ing. de Infraestructura	X		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	20/10/2021				
	2 Switch HP - Sistema de Hiperconvergencia Simplivity	Sanolivar	X		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	21/10/2021				
	w switch Cisco - CoreSwitch	Redneet	X		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	20/10/2021				
ROUTER	CISCO 4400 SERIES	Ing. de Infraestructura	X		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	20/10/2021				
ROUTER	CISCO - 800 SERIES	Proveedor	X		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A					
ROUTER	CISCO - 3900 SERIES	Proveedor	X		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A					
ROUTER	CISCO - 2900 SERIES	Proveedor	X		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A					
ROUTER	CISCO - 3900 SERIES	Proveedor	X		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A					
DEMARCADOR	RAISECOM - rax700	Proveedor	X		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A					
DEMARCADOR	RAISECOM - rax700	Proveedor	X		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A					
ROUTER - DEMARCADOR	CIO USAQUÉN	Proveedor	X		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A					
ROUTER - DEMARCADOR	CIO CHAPINERO	Proveedor	X		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A					
ROUTER - DEMARCADOR	CIO SANTA FE	Proveedor	X		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A					
ROUTER - DEMARCADOR	CIO LA CANDELARIA	Proveedor	X		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A					
ROUTER - DEMARCADOR	CIO SAN CRISTÓBAL	Proveedor	X														
ROUTER - DEMARCADOR	CIO USME	Proveedor	X		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A					
ROUTER - DEMARCADOR	CIO TUNJUELITO	Proveedor	X		N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A					

Fuente: Documento aportado por el proceso auditado

Se generan y almacena informes con las acciones, resultados y observaciones de cada uno de los mantenimientos realizados y se les realiza el seguimiento adecuado:

Imagen 97 Evidencia informe mantenimiento



Fuente: Documento aportado por el proceso auditado

👉 Si bien la gestión de los mantenimientos es adecuada, no se registran los programas de mantenimiento preventivo, sus resultados y observación en la herramienta de mesa de ayuda GLPI para relacionarlo con cada equipo, software o sistema de información, para que esta información pueda ser integrada en un solo instrumento y facilitar el control de activos de información, genera reportes estadísticos e indicadores desde la herramienta.

👉 En cuanto a los inventarios de hardware y software se llevan de forma manual en libros de Excel, aunque ya se tiene implementado el agente de inventarios de hardware y software automatizados en el GLPI, basado en escaneo a la infraestructura, y que garantiza mantener actualizados estos inventarios para así poder controlar la gestión de licencias y detección de Software no licenciado o no autorizado, la presencia o ausencia de hardware, y genera mayor confiabilidad en la información de los mismos, no se ha formalizado la utilización de estos inventarios como los oficiales de la entidad.

Imagen 98 Inventario equipos

B14 | Gestor de Encuestas

SECRETARIA DISTRITAL DE LA MUJER
CATALOGO DE SOFTWARE UTILIZADO

Software utilizado Sdmujer	Descripción	Clasificación
Anydesk	Software para escritorio remoto. Mesa de ayuda	Sofware libre
Wampserver	Simulador de Servidor de aplicaciones	Sofware libre
Php Versión 5.4 a la 7.8	leguaje Programación	Sofware libre
Mysql	base datos	Software libre
mariaDB	Base de datos	Software libre
Mobaxterm	software para manejo de maquinas virtuales por SSH	Software libre
Drupal 9	Gestor de contenidos pagina web	Software libre
Jumgla	Gestor de contenidos Intranet	Software libre
Limesurvey	Gestor de Encuestas	Software libre
Glpi	Software para la gestión de la mesa de ayuda	Software libre
Weblogic	Servidor de aplicaciones Oracle para PERNO y Limay	Software libre
Forms	Servidor de aplicaciones Oracle para PERNO y Limay	Licencia Adquirida
Report	Servidor de aplicaciones Oracle para PERNO y Limay	Licencia Adquirida
Oracle	Base de datos 10.0 local y nube 12 a 18	Licencia Adquirida
Vpn Sisco	acceso a la vpn	Software libre
Gilab	Versionador de aplicaciones	Software libre
Nerbeans	Herramienta para construcción de aplicaciones	Software libre
Notepad++	gestor de archivos de texto avanzado	Software libre
Suite Adobe Creative Cloud	Aplicaciones para diseño y publicaciones	Licencia Adquirida
Adobe Sing	Aplicativo para firma digital	Licencia Adquirida
Office 365	Aplicaciones de Windows	Licencia Adquirida
Moodle	Aplicativo para las capacitaciones	Software libre
SPSS	software para estadísticas	Licencia Adquirida
Argies	Sistema para georeferenciar	Licencia Adquirida
Licencias de power BI	Suite de BI de Microsoft (Gestión del conocimiento)	Licencia Adquirida
SqlDeveloper	gestor de base de datos	Software libre
PhpMyadmin	Aplicativo de acceso base de datos	Software libre

INVENTARIO APLICACIONES | Sofware utilizado | Cronograma de mantenimiento | Mto servidor Apl. Web | Mto ICOPS

Fuente: Documento aportado por el proceso auditado

👉 En los inventarios entregados a la auditoria, no se relaciona la cantidad de instalaciones de software, ni se detallan en que equipos se encuentra instalado, tampoco las características de equipos, ni sus hojas de vida.

👍 Durante la visita de auditoria se pudo comprobar que el proceso de instalación de los agentes para el control de inventarios automatizados en los pc 's inspeccionados se está adelantando de manera correcta.

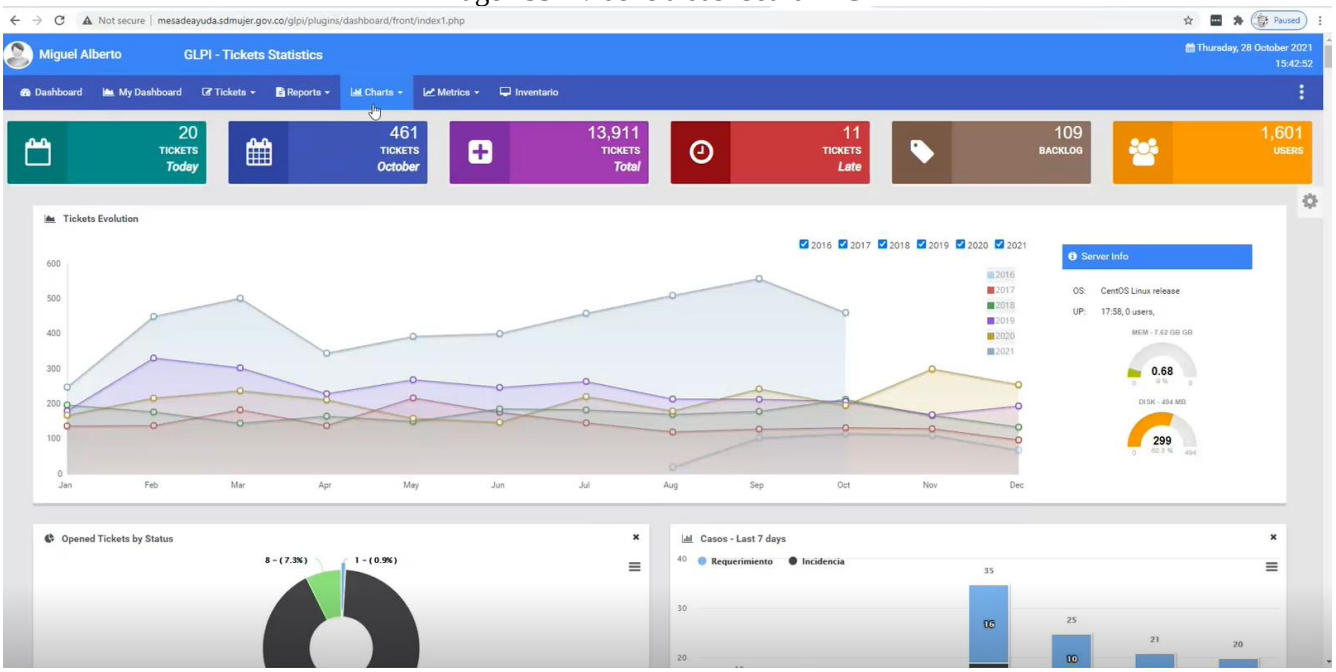
👉 Dentro de las funcionalidades del GLPI se permite llevar seguimiento a la presencia y/o ausencia de software y hardware, la gestión de activos y configuraciones, gestión de cambio y conocimiento, hoja de vida de los equipos con su respectiva relación de software instalado, que aún no se han implementado totalmente en la entidad y se constituyen como la mejor practica para el control de inventarios de hardware y software.

6.6.2. MESA DE SERVICIO

6.6.2.1. FORTALEZAS Y OPORTUNIDADES DE MEJORA

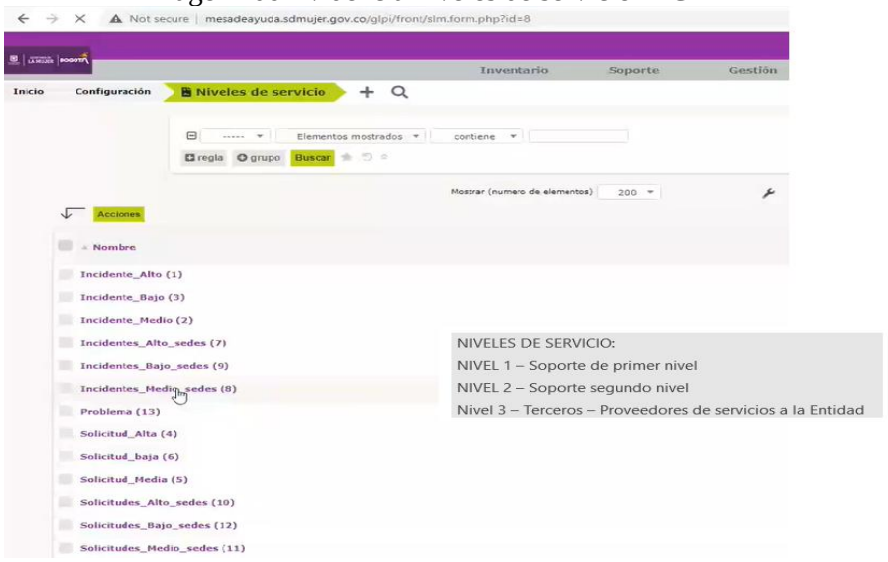
👍 La gestión de la mesa de servicio se encuentra correctamente implementada en el software GLPI de acuerdo con buenas prácticas y se gestionan adecuadamente a través de esta herramienta los incidentes y requerimientos de los usuarios, se tramitan las ordenes de servicio y se asignan los agentes de atención a cada caso:

Imagen 99 Evidencia dashboard – GLPI



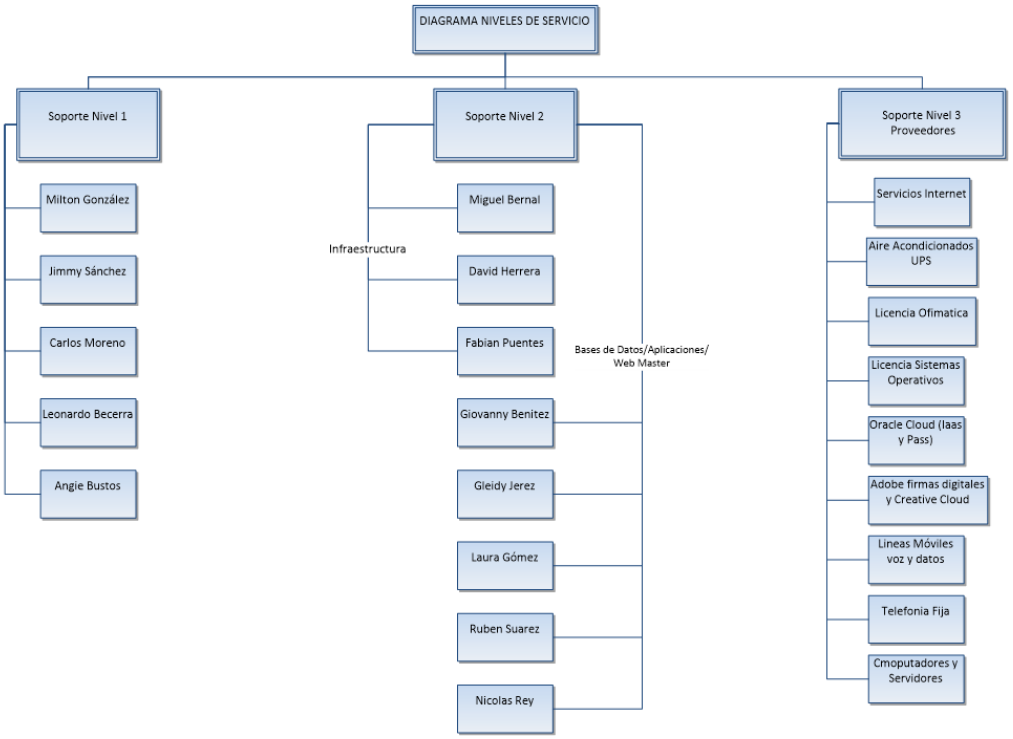
👍 Se encuentran correctamente configuradas en la herramienta de mesa de ayuda, la categorización de servicios y los acuerdos de niveles de servicio - ANS, además se eleboró el documento en borrador: "NIVELES DE SERVICIO SECRETARÍA DISTRITAL DE LA MUJER" en donde se describen de forma adecuada los tres niveles de servicio que tiene el proceso de Gestión tecnológica:

Imagen 100 Evidencia niveles de servicio – GLPI



En ese documento se encuentra correctamente definido el diagrama de los niveles de servicios y sus responsables, y su configuración esta implementada en los perfiles de usuarios y definición de roles en la herramienta de mesa de ayuda GLPI:

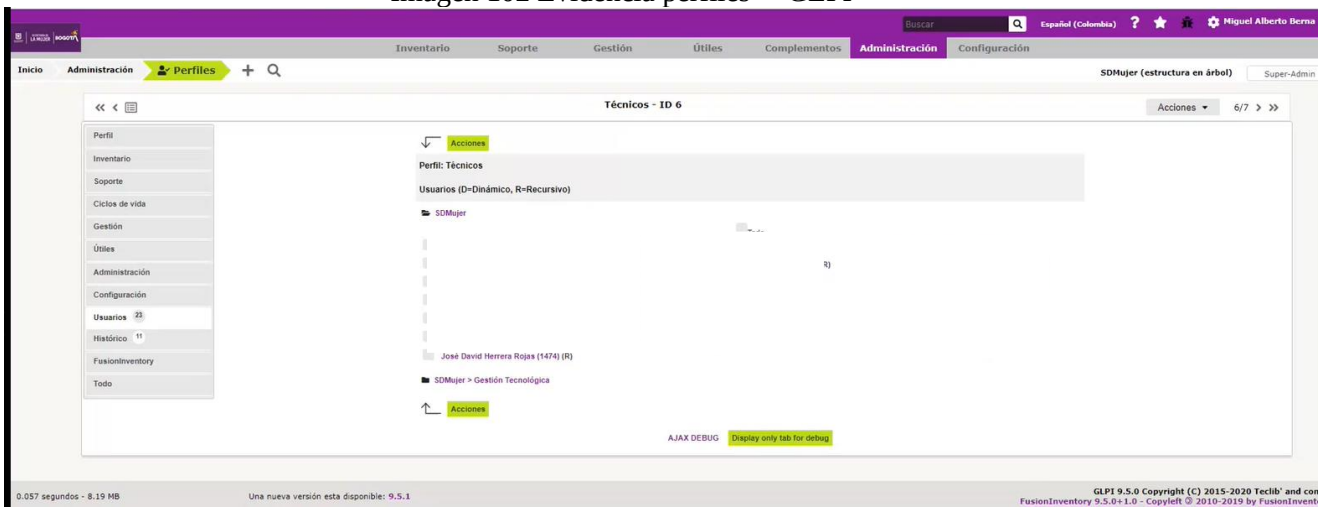
Imagen 101 Evidencia responsables de soporte



Fuente: Documento aportado por el proceso auditado

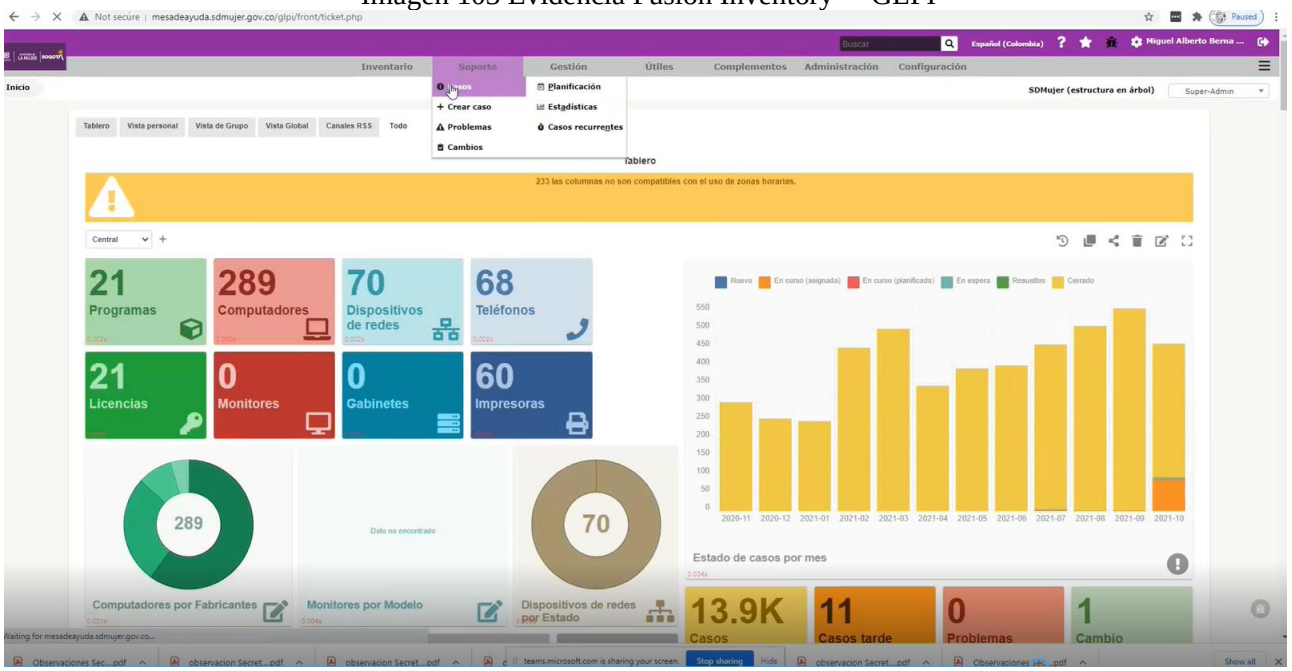
Evidencia Configuración de perfiles de técnicos en GLPI

Imagen 102 Evidencia perfiles – GLPI



Si bien se tiene implementado el agente de inventarios de hardware y software automatizados en el GLPI: *Fusion Inventory*, al momento de la auditoria aún se encontraba en proceso de pruebas, y de entendimiento por parte de los encargados de la administración de la herramienta de mesa de ayuda.

Imagen 103 Evidencia Fusion Inventory – GLPI



- No se ha definido un procedimiento de generación de informes periódicos del GLPI que sirvan como indicadores para medir la efectividad en la atención y prestación de servicios del Área de TI. Se denota que los colaboradores del proceso, encargados de la administración de la herramienta están en proceso de conocimiento y aprendizaje de las diferentes funcionalidades ofrecidas por la herramienta.

- Si bien se tienen definidas encuestas para medir el nivel de satisfacción de los usuarios en la resolución de los incidentes, se evidencia resistencia de los usuarios a diligenciarlas y por tanto los reportes de niveles de satisfacción que se generan en la herramienta no son del todo confiables.

- Si bien la herramienta de mesa de ayuda se encuentra implementada, funcionalidades como el control de licenciamiento de software, inventarios de software y hardware automatizados, gestión de cambios, control de incidentes de seguridad, definición de plantillas por tipo de incidente o requerimientos de desarrollo, gestión de conocimiento y auto soporte, entre otros, no se han configurado. Por lo cual se debe elaborar un plan de implementación de esas características para aprovechar todas sus funcionalidades que sirva para mejorar, simplificar y centralizar toda la gestión de servicio de TI.

7. CONCLUSIONES

7.1. FORTALEZAS

La auditoría arrojó los siguientes resultados satisfactorios:

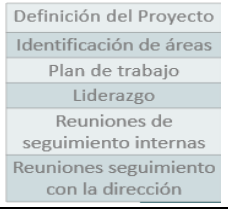
- El proceso de Gestión de Tecnologías de Información ha estructurado y presentado para la vigencia 2021 el Plan Estratégico de Tecnologías de la Información, el cual refleja el interés del proceso por dar cumplimiento a los lineamientos el Marco de Referencia de Arquitectura Empresarial en adelante MRAE, para la Gestión de TI del Estado colombiano y a la Guía 6 para la estructuración del PETI dispuesta por Mintic y constituye un documento de base que puede ser fortalecido para que se establezca como guía estratégica para el mantenimiento y mejoramiento de la función tecnológica alineada a los objetivos estratégicos institucionales y garantizando la seguridad de la información de la entidad.
- Aunque son susceptibles de mejora, la OAP realizó la actualización y publicación de los Planes: Plan estratégico de Tecnologías de la Información y las Comunicaciones -PETI, Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y el Plan de Seguridad y Privacidad de la Información, como parte integral del Plan de Acción institucional, conforme al Decreto 612 de 2018, por lo cual, se espera que estén articulados con los demás planes de la entidad y en especial con sus objetivos institucionales.
- Otro elemento favorable es la inclusión del Modelo de Seguridad y Privacidad de la Información - MSPI en la planeación del sistema integrado de gestión, lo cual facilita la articulación del Sistema de Gestión de Calidad con el Sistema de Gestión de Seguridad de la Información.
- Se destaca la gestión realizada el funcionario asignado al MSPI, en la construcción del Sistema de Gestión de Seguridad de la Información, la integración de las áreas de negocio en el proceso y las acciones en materia de campañas de sensibilización en las políticas de seguridad de la información, las cuales han generado recordación en los usuarios
- El equipo humano que atiende el proceso de Gestión de Tecnologías de Información ha estructurado y presentado instrumentos en aras de llevar control de la gestión, buscar mejorar los servicios tecnológicos y avanzar en la implementación del Modelo Integrado de Planeación y Gestión, en adelante MIPG. Tal es el

caso de instrumentos de ciclo de fábrica, Manuales de Operación, instrumentos MSPI y elementos de sensibilización y gestión del conocimiento dirigidos a la adopción de buenas prácticas.

- Se cuenta con un equipo de funcionarios, contratistas y proveedores con un alto nivel de compromiso y competencias distintas para abordar de manera integral la mejora en la función TIC.
- En seguridad lógica se destaca la existencia configurada de soluciones EndPoint para la protección de los equipos de usuario, así como el uso de herramientas robustas de monitoreo a las acciones de los usuarios del dominio, lo que permite actuar de manera preventiva.
- La Secretaria de la Mujer, atiende los lineamientos de accesibilidad de que trata la resolución 1519 de 2020 y en cumplimiento de accesibilidad en medios electrónicos para población en situación de discapacidad, con el fin que sus medios de comunicación electrónica dispuestos para divulgar la información cumplan con las directrices de accesibilidad que dicte el Ministerio de Tecnologías de la Información y las Comunicaciones a través de los lineamientos que se determinen en la Estrategia de Gobierno en línea. La entidad ha contratado y asignado a un profesional dedicado a cumplir con esta labor, lo cual resulta no solo responsable con su compromiso, sino efectivo para lograr la meta establecida
- Se lleva un control adecuado de mantenimientos tanto al hardware (Pc´s, servidores y equipos de comunicaciones) como a software base y aplicativo, lo que disminuye los riesgos asociados a fallas en activos de información.
- A pesar de contar con pocas herramientas de contingencia se ha optimizado el uso de las soluciones de hiperconvergencia y de backup para lograr un modelo aceptable de continuidad, que con las nuevas adquisiciones podrá evolucionar a un modelo robusto.
- Se evidencia la estructuración de un modelo de servicio satisfactorio con la herramienta GLPI, con la cual se han implementado un número importante de funcionalidades, que si bien no son todas las disponibles, el equipo de tecnología demuestra interés en estudiar más a fondo para aprovechar las potencialidades no implementadas.
- Se han implementado algunos elementos de protección y gestión de la plataforma tecnológica que si bien deben ser mejorados ofrecen un nivel aceptable de protección sobre los activos de información.
- Los usuarios de los servicios TIC tienen una percepción positiva sobre el servicio prestado por el proceso de Gestión de Tecnologías de Información.
- Se tiene control en las estrategias de copias de seguridad que protegen la información generada por la entidad y que permiten asegurar su recuperación de diferentes fuentes de respaldo en caso de siniestros o contingencias.

7.2. OPORTUNIDADES DE MEJORA

A continuación, se enuncian las oportunidades de mejora principales encontradas a lo largo de la auditoria, con el ánimo de identificar mejoras potenciales que el área o proceso *de Gestión Tecnológica* podría tener en cuenta para su autoevaluación y por ende para la formulación de acciones de mejoramiento, sin embargo dada la importancia de las oportunidades de mejora para garantizar la seguridad de la plataforma tecnológica y el cumplimiento de la política de gobierno digital, se requiere la formulación de un plan de mejoramiento que abarque todas las oportunidades de mejora relacionadas en el presente informe.

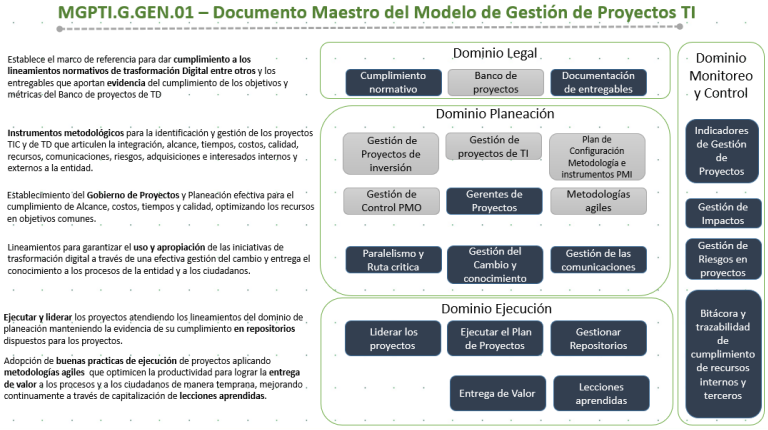
N°	OPORTUNIDAD Y/O RECOMENDACIÓN	Numeral Del Informe	Proceso Responsable
1	Dar continuidad a la aplicación de la Guía 6 de Mintic para la construcción del PETI actualización 2022, con el ánimo de construir un documento articulador del direccionamiento estratégico de la entidad en materia de tecnología. Mejorar los siguientes aspectos: ✓ Diligenciar completamente las plantillas del instrumento, dado que los registros de algunas son insumo formulado para plantillas posteriores. Analizar en especial la relación entre sesión 3 y sesión 5. ✓ Mejorar el diligenciamiento del análisis DOFA aportado por el proceso de Gestión TIC enfocado en la plataforma tecnológica, los recursos humanos TIC y las capacidades TIC de la entidad en relación con la capacidad de ofrecer continuidad y desempeño aceptable para soportar los requisitos externos, requisitos de la entidad, proyectos propios TIC y oportunidades de innovación enfocadas en el Conpes 3975 de Trasformación Digital e Inteligencia Artificial. ✓ Incluir como debilidad el hecho de que todas las adquisiciones, cambios y liderazgo en tecnología no estén centralizados en el proceso de Gestión Tecnológica, dado su impacto en el equilibrio entre la inversión tecnológica y el valor agregado para la entidad además de exponer al riesgo de pérdida de control sobre terceros y fuga de conocimiento. ✓ Actualizar la estructuración del PETI 2022 contemplando las modificaciones del MAE.G.GEN.01 Documento Maestro de Arquitectura Empresarial versión del 31 de octubre de 2019. ✓ Incluir como insumo para el PETI 2022 el seguimiento al cumplimiento de la hoja de ruta de proyectos vigencia anterior, lecciones aprendidas y medición por indicadores como componentes de mejora continua resultado de la retrospectiva.	6.1.1	Gestión Tecnológica
2	Garantizar la construcción de planeas tácticos para todos los proyectos de PETI, en el primer bimestre de la vigencia, bajo la premisa de que su inclusión en el PETI es declaración de su viabilidad con respecto al alcance establecido. De ser posible crear un frente de Gestión de Proyectos que articule la planeación y gestión de los proyectos del PETI de manera articulada con los demás stakeholders, con 6 elementos rectores para su planeación, liderazgo y seguimiento:  	6.1.1	Gestión Tecnológica
3	Adelantar la metodología de gestión de proyectos atendiendo las directrices de los siguientes referentes para el estado colombiano. A continuación, se incluyen algunos resúmenes de lineamientos aplicables: **REFERENTES:** • Marco de la Transformación Digital para el Estado Colombiano V1. 07/20 – MTDEC Se articula al paso iv) ejecutar la ruta e implementar proyectos de transformación digital, priorizados de acuerdo al valor para la ciudadanía y la misionalidad, Establece el marco para la construcción del **Gobierno de Proyectos**, con 6 elementos rectores para su planeación, liderazgo y seguimiento	6.1.1	Gestión Tecnológica

N°	OPORTUNIDAD Y/O RECOMENDACIÓN	Numeral Del Informe	Proceso Responsable

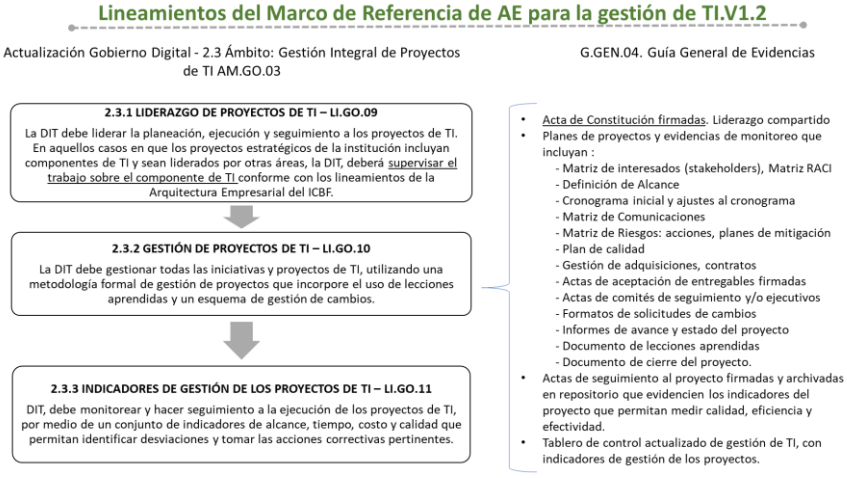
- MAE.G.GEN.01 – Documento Maestro del Modelo de Arquitectura Empresarial V1 10/19

Los proyectos priorizados en la hoja de ruta que resulten de los ejercicios de Arquitectura Empresarial son un insumo al momento de actualizar el PETI, son objeto de estrategia de uso y apropiación y deben ser justificados para su inversión.

- Documento Maestro del Modelo de Gestión de Proyectos TI MGPTI.G.GEN.01 – V1 10/19



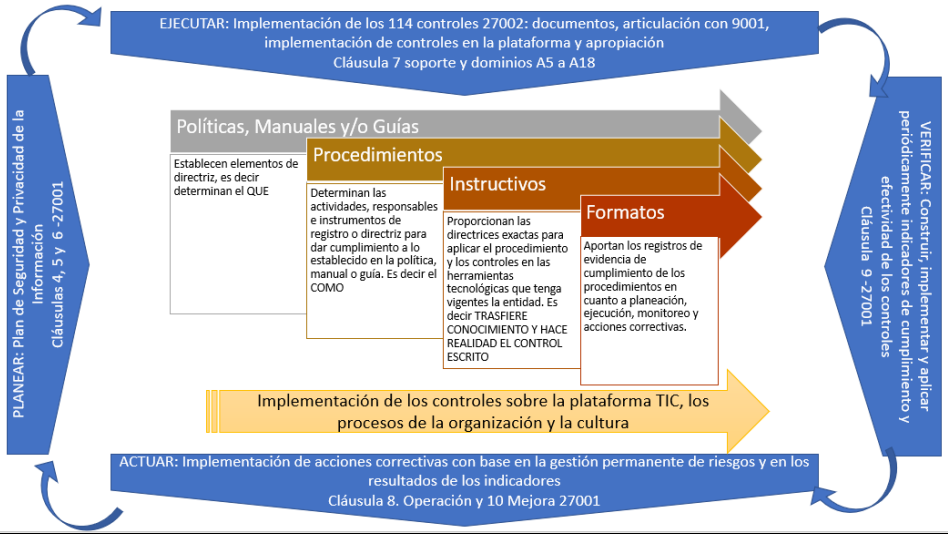
- Lineamientos del Marco de Referencia de AE para la gestión de TI.V1.2 -10/2019 - Act GD



N°	OPORTUNIDAD Y/O RECOMENDACIÓN	Numeral Del Informe	Proceso Responsable
4	Con relación a los Planes de acción y cronogramas para Control acciones y/o proyectos se recomienda: ✓ Establecer las fechas y responsables con base en un análisis de estimación de esfuerzo por tareas versus la capacidad de trabajo instalada. Esto con el fin de identificar necesidades de recurso humano, establecer fechas viables de cumplimiento y ponderar las actividades de acuerdo con el esfuerzo requerido. ✓ Antes del cálculo de capacidad disponible deben sustraerse los tiempos requeridos por cada recurso para la atención de funciones de rutina. ✓ Incluir actividades No rutinarias que requieren acompañamiento de recursos del área ✓ Asignar tareas de manera individual con el fin de medir cumplimiento y productividad por recurso. ✓ Priorizar las tareas de acuerdo con: - Prioridad 1: requisitos regulatorios o normativos - Prioridad 2: de valor agregado para los procesos misionales - Prioridad 3: de valor agregado para el desempeño o seguridad de la plataforma tecnológica (DOFA) - Prioridad 4: atender innovación TIC - Prioridad 5: de valor agregado para los procesos de apoyo ✓ Establecer criterios de aceptación de los entregables para garantizar que el resultado obtenido realmente cumple con la mejor práctica y lo incluido en los documentos se ve reflejado en la implementación sobre procesos y plataforma tecnológica ✓ Calcular los avances de acuerdo al nivel de cumplimiento de los entregables con los criterios establecidos y con las fechas establecidas. Si es posible hacer revisión de pares.	6.1.1	Gestión Tecnológica
5	Continuar la implementación del sistema para gestión de procesos en PHP acondicionándolo para que pueda ser aplicable a la gestión de proyectos de tecnología. ✓ En primera instancia se deben parametrizar los estados que son propios de un proyecto (inicio, planeación, ejecución y cierre, particularizando la fase de ejecución de acuerdo a la naturaleza del proyecto ejemplo: análisis, diseño, desarrollo, pruebas, despliegue), ya que hasta el momento solo se han incluido aquellos inherentes a procesos de contratación. Vale aclarar que los estados incluidos, son propios de la fase de inicio cuando un proyecto este articulado con una adquisición. Un proyecto puede tener más de una adquisición. ✓ En el registro del proceso al equipararlo a un proyecto, se debe agregar la fecha fin planeada del proyecto. ✓ Para equiparar las observaciones a las actividades de planeación, deben incluir fecha inicio y final de cada actividad, fecha de finalización real de la actividad (para cálculo de desviaciones de cumplimiento), % de avance y el responsable asignado con nombre propio para determinar equilibrio entre capacidad instalada y esfuerzo asignado. Puede usarse una base de 8 horas diarias para construir alertas de sobre asignación. ✓ Se requiere tener niveles jerárquicos para las actividades, con el fin de agrupar en fases o equipos paralelos.	6.1.1	Gestión Tecnológica
6	En la planeación táctica garantizar que exista correlación entre los resultados del instrumento de la Guía 6 Mintic, los proyectos de hoja de ruta, y los planes detallados de actividades del proyecto. Establecer para los proyectos en el marco MIPG alcances detallados para cada vigencia con el fin de ser consecuente con los instrumentos de autodiagnóstico de Gobierno Digital, Seguridad Digital y MSPI. Para los proyectos que impliquen desarrollo de software con fabrica interna o externa, generar trazabilidad con la pila de producto o de requerimientos de cada proyecto.	6.1.1	Gestión Tecnológica
7	Optimizar la declaración de indicadores de gestión construyendo la ficha de cada indicador donde se especifique la fuente de cálculo con el fin de corroborar el resultado del indicador con la medición real.	6.1.1	Gestión Tecnológica

N°	OPORTUNIDAD Y/O RECOMENDACIÓN	Numeral Del Informe	Proceso Responsable
	Para los indicadores calculados sobre actividades cumplidas con respecto a actividades planeadas, utilizar en lo posible como fuente el desarrollo que se está adelantando en PHP. Para el indicador de cumplimiento en el servicio de soporte, usar los registros de GLPI que han sido atendidos en los tiempos de los ANS internos y de terceros previamente configurados en GLPI.		
8	Trasferir formalmente la supervisión de los contratos de servicios tecnológicos a la gestión de TI, con el fin de: ✓ Garantizar que los entregables a cargo de los contratistas cumplen con los criterios de aceptación y los procesos de trasferencia de conocimiento técnico se hagan a lo largo de la prestación del servicio. ✓ Mitigar el riesgo de pérdida de integridad y estandarización de la plataforma tecnológica que redunda en dificultades de escalamiento y mantenimiento futuro. ✓ El logro de los objetivos de un Gobierno TI a saber: inversión estratégica de TIC, toma de decisiones centralizada, gestión integral de proyectos, apropiación del conocimiento TIC, aplicabilidad efectiva del ciclo PHVA y sostenibilidad de la plataforma tecnológica a mediano y largo plazo. ✓ Posicionar a TI de manera estratégica para lograr la visión de la entidad. ✓ Que las adquisiciones garanticen el costo/beneficio y cumplan con criterios de estandarización, evolución, capacidad de integración, mantenimiento, desempeño, apropiación del conocimiento, riesgo tecnológico, seguridad de la información y sostenibilidad futura. ✓ Centralizar la gestión integrada de proyectos TIC.	6.1.2	Gestión Tecnológica
9	De ser posible asignar un oficial de seguridad no subordinado a la OAP, o que en su lugar Control Interno ejecute la auditoría independiente de que habla el dominio 18 de MSPI y la cláusula principal 9 en cuanto a la medición de la efectividad de los controles de seguridad a partir de indicadores.	6.1.2	Gestión Tecnológica
10	Adelantar una identificación de los conocimientos específicos del recurso humano de la función TIC (funcionarios y contratistas) que deben ser trasferidos, el par de contingencia y que documentos de procedimientos e instructivos deben incorporarse a la transferencia. Formalizar un Plan de Transferencia de Conocimiento, que haciendo uso de un número de horas a la semana por colaborador se ejecute: ✓ La elaboración de los instructivos y procedimientos (que aún no existan) correspondientes al conocimiento a trasferir. ✓ Capacitación incluyendo incidentes y recuperaciones para el colaborador identificado como contingencia. ✓ Elaborar un plan de rotación de funciones temporal, entre colaboradores principales y de contingencia. ✓ Evaluar resultados Este ejercicio puede incorporarse a la documentación de Plan de continuidad de negocio y al desarrollo del dominio 17 (continuidad) del Modelo de Seguridad y Privacidad de la Información (MSPI) ya que el personal con conocimientos específicos es objeto de tratamiento de riesgos por ausencia temporal o permanente.	6.1.2	Gestión Tecnológica
11	Una vez construida y socializada la metodología de desarrollo de software, incorporar en el órgano que corresponda una mesa de sistemas de información donde se priorice con las áreas los requerimientos que han entrado a la pila de producto, con base en criterios de urgencia y valor, como instrumento para planear el desarrollo por iteraciones y evitar al máximo el impacto de inclusiones de requerimientos no planeados, equilibrar cargas de trabajo entre los recursos de área, adelantar transferencia de	6.1.2	Gestión Tecnológica

N°	OPORTUNIDAD Y/O RECOMENDACIÓN	Numeral Del Informe	Proceso Responsable
	conocimiento entre los miembros de equipo de desarrollo y obtener indicadores de cumplimiento, calidad y productividad de fábrica.		
12	De ser posible, incluir en los contratos, cláusulas para: ✓ Trasferir conocimiento ✓ Criterios de aceptación de entregables; documentos, servicios y productos ✓ Especificaciones de la documentación técnica mínima a entregar en desarrollo de software y la metodología que debe ser aplicada ✓ Obligaciones relacionadas con la seguridad de la información en desarrollo de software. ✓ Condiciones de soporte sobre el producto y ANS durante la vigencia del contrato	6.1.2	Gestión Tecnológica
13	Garantizar para próximas contrataciones con proveedores las condiciones de trasferencia, ANS, aplicación de la metodología de desarrollo y condiciones de seguridad según el objeto del contrato.	6.1.2	Gestión Tecnológica
14	Establecer como política de seguridad del MSPI dominio 15 la inclusión de criterios de aceptación, políticas de gestión de cambios y requisitos de seguridad en los contratos con terceros. Establecer instrumentos de seguimiento y control a las obligaciones de los contratos y en especial a las relacionadas con seguridad de la información. Estas políticas y procedimientos deben incluir el control de proveedores TIC centralizado en el proceso de Gestión de TI, no en las áreas. Complementar las condiciones de formalidad de uso en software comercial, incluyendo en los estudios previos la prohibición de ceder los derechos patrimoniales del sistema a terceros durante la vigencia del contrato y un tiempo adicional que deberá ser determinado de acuerdo al impacto que pueda causar para la entidad no contar con los servicios se soporte y mantenimiento del sistema. Solicitar los derechos de propiedad intelectual sobre el producto.	6.1.2	Gestión Tecnológica
15	Para los contratos que incluyan soporte o alta disponibilidad incluir siempre ANS y llevar herramientas de control de cumplimiento preferiblemente GLPI. Incluir en las categorías de GLPI los incidentes y requerimientos a sistemas de información, crear los proveedores como agentes de soporte e iniciar la práctica de registrar los incidentes en la mesa de ayuda con el debido registro de tiempos de respuesta y solución (resuelto). Integrar a GLPI los GLPI Plugin's que permitan aprovechar las funcionalidades liberadas para la herramienta tanto de registro como de control y generación de reportes estadísticos (Dashboard). De ser posible incluir en la FORMA DE PAGO de los estudios previos sanciones relacionadas con el incumplimiento de los ANS durante el periodo que corresponde a cada pago.	6.1.2	Gestión Tecnológica
16	Para el caso de herramientas de seguridad informática o de plataformas tecnológicas de conocimiento especializado, fortalecer las condiciones de trasferencia de conocimiento en los contratos de los proveedores para garantizar el máximo aprovechamiento de la herramienta y disminuir la dependencia de conocimiento del proveedor.	6.1.2	Gestión Tecnológica
17	Evaluar las brechas reales de implementación del MSPI en el marco del ciclo PHVA para establecer las actividades y esfuerzo requerido para completar su implementación en 4 frentes paralelos y actualizar el **Plan de Seguridad y Privacidad de la Información** vigencia 2022 a las metas viables junto con la planeación o cronogramas detallados:	6.2.1	Gestión Tecnológica

N°	OPORTUNIDAD Y/O RECOMENDACIÓN	Numeral Del Informe	Proceso Responsable
	• Levantamiento y planeación de los documentos comunes en el sistema integrado de gestión y la planeación de la salida escalonada de documentos de acuerdo al avance en implementación, especialmente para los dominios 6, 7, 11 y 15. • Escalar la toma de decisiones sobre los controles a implementar en la realidad sobre la plataforma tecnológica • La elaboración del marco documental de políticas, procedimientos, instructivos y formatos en la declaración de aplicabilidad. Tener en cuenta que la implementación de los dominios no se realiza por orden de la norma, sino de acuerdo a los esfuerzos de su implementación, sensibilización y puesta en operación real. • Actualizar el programa de concientización, educación y capacitación sobre la 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. • Implementación de los controles de seguridad de la información en la plataforma TIC que sean consecuentes con lo que está declarado en los documentos de políticas, guías y manuales. • Establecer la métrica de efectividad de los controles establecidos • Implementar el plan de mejora continua y actualización anual y por cambios en la plataforma o servicios TIC Se recomienda adelantar una inspección de análisis de vulnerabilidades antes de la planeación para determinar criticidad y prioridad y nuevamente una vez finalizada la implementación para verificar su eficacia. 		
18	Ajustar la declaración de aplicabilidad y el instrumento MSPI de Mintic, incluyendo los instrumentos con que cuenta el área y que no están declarados, identificar cuales requieren actualización o articulación con documentos correlacionados. Documentar controles que en la práctica se están llevando correctamente pero no se han formalizado.	6.2.1	Gestión Tecnológica
19	En el marco de la implementación del MSPI actualizar el inventario de activos de información incluyendo los demás activos establecidos en el Manual GD-PR-2 - ACTIVOS DE INFORMACION - V1 de la entidad y en todo caso los lineamientos ISO 27001. Aprovechar la información adelantada en el PETI, en los instrumentos de la Guía 6 del PETI, el Inventario de Información de Aplicaciones y los reportes GLPI, que contienen información valiosa de insumo. Identificar documentos sensibles en transito que requieran ser encriptados. Levantamiento de activos tipo “información” generados en el proceso de gestión tecnológica, tales como documentos de arquitectura de sistemas de información, documentos de infraestructura o del proceso de desarrollo de software entre otros, que pueden resultar de carácter reservado.	6.2.1	Gestión Tecnológica
20	En la siguiente actualización del instrumento de evaluación MSPI, relacionar como evidencias los documentos evolucionados para cada control de MSPI y registrar el avance teniendo en cuenta que la implementación 100%	6.2.1	Gestión Tecnológica

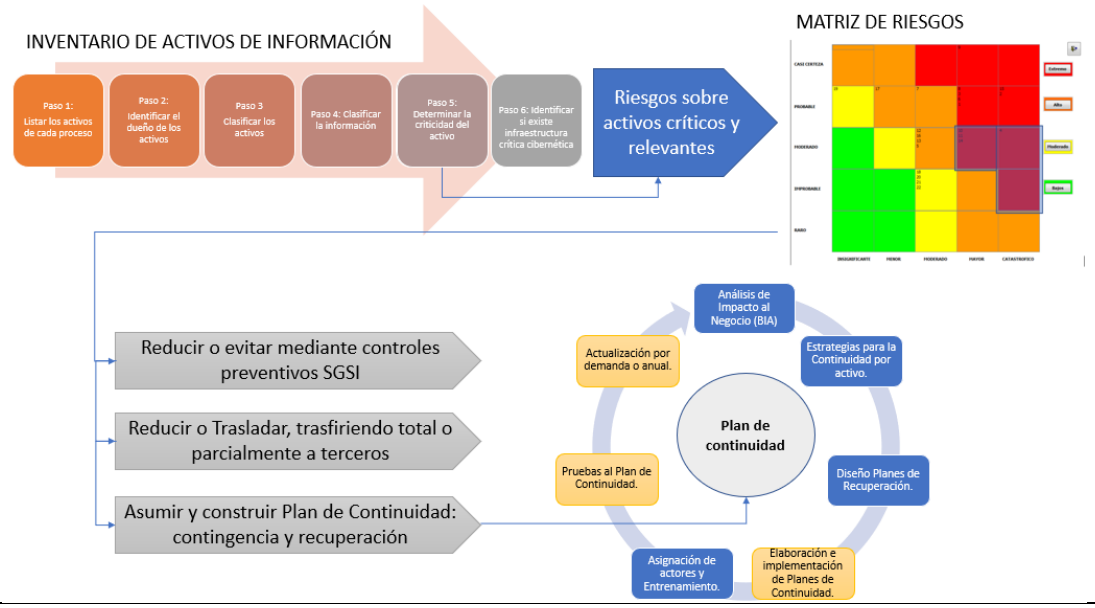
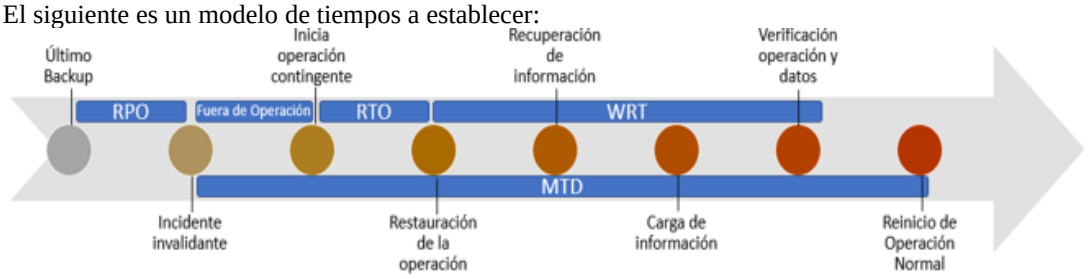
<table>
<tr><th>N°</th><th>OPORTUNIDAD Y/O RECOMENDACIÓN</th><th>Numeral Del Informe</th><th>Proceso Responsable</th></tr>
<tr><td></td><td>de cada componente incluye: Planear, elaborar los instrumentos, implementar los controles, sensibilizar, evaluar efectividad y mejorar.

Evolucionar los documentos existentes y garantizar que están articulados con la realidad de los controles aprobados para ser implementados.</td><td></td><td></td></tr>
<tr><td>21</td><td>Construir los procedimientos e instructivos de los dominios 12 y13 que mitiguen el riesgo de dependencia de conocimiento frente a una ausencia temporal o permanente del responsable de la administración y configuración de herramientas para la gestión de seguridad y acceso.

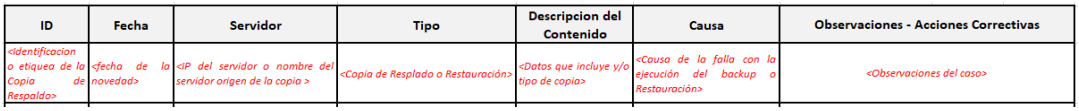
Diagnosticar, ajustar y documentar la gestión de accesos privilegiados.</td><td>6.2.1</td><td>Gestión Tecnológica</td></tr>
<tr><td>22</td><td>En las políticas de seguridad en la Gestión de proyectos, incluir las siguientes condiciones de seguridad:
• Si hay activos críticos involucrados en el proyecto
• Si hay información o datos confidencias al que puedan acceder terceros
• Riesgos de seguridad asociados al proyecto
• Condiciones de propiedad intelectual
• Responsabilidad por incidentes de seguridad de terceros.
En caso de proyectos de adquisición o desarrollo de sistemas de información establecer formalmente los criterios de aceptación en materia de seguridad.</td><td>6.2.1</td><td>Gestión Tecnológica</td></tr>
<tr><td>23</td><td>Antes de publicar la nueva Política de Privacidad y Datos Personales, incluir el protocolo de anonimización y al publicarla incluir el link en todos los accesos web que impliquen algún tipo de entrega de información por parte de un ciudadano</td><td>6.2.1</td><td>Gestión Tecnológica</td></tr>
<tr><td>24</td><td>Al levantar el inventario de los instrumentos faltantes, tener en cuenta que, la seguridad digital es parte integral de los dominios de Arquitectura TI, por lo tanto, existen elementos comunes que permiten a la entidad avanzar con los mismos esfuerzos en los dos sentidos, La siguiente tabla muestra elementos de cruce entre MSPI y la construcción de los dominios del PETI que puede servir de guía:
<table>
<tr><td>CLAUSULAS Y DOMINIOS MSPI</td><td>Fases PETI
DOMINIOS MRAE</td><td>FASE 1
Estrategia</td><td>FASE 2
Gobierno TI</td><td>FASE 3
Información</td><td>FASE 3
Servicios TIC</td><td>FASE 3
Sistemas de Inf.</td><td>FASE 4
Uso y apropiación</td></tr>
<tr><td colspan="2">4.Contexto de La Organización</td><td>X</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2">5.Liderazgo</td><td>X</td><td>X</td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2">6. Planificación</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2">7. Soporte</td><td></td><td></td><td></td><td></td><td></td><td>x</td></tr>
<tr><td colspan="2">8. Operación</td><td></td><td></td><td></td><td>X</td><td></td><td></td></tr>
<tr><td colspan="2">9. Evaluación y Desempeño</td><td></td><td>x</td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2">10. Mejora</td><td></td><td>x</td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2">A5. Política De Seguridad</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2">A6 Aspectos Organizativos</td><td></td><td>x</td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2">A7 Recursos Humanos</td><td></td><td></td><td></td><td></td><td></td><td>x</td></tr>
<tr><td colspan="2">A8 Gestión de Activos</td><td></td><td>x</td><td>X</td><td>X</td><td>X</td><td></td></tr>
<tr><td colspan="2">A9 Gestión de Accesos</td><td></td><td></td><td></td><td>X</td><td></td><td></td></tr>
<tr><td colspan="2">A10 Criptografía</td><td></td><td></td><td>X</td><td></td><td></td><td></td></tr>
<tr><td colspan="2">A11 Seguridad Física</td><td></td><td></td><td></td><td>X</td><td></td><td></td></tr>
<tr><td colspan="2">A12 Gestión Operacional</td><td></td><td></td><td></td><td>X</td><td></td><td></td></tr>
<tr><td colspan="2">A13 Comunicaciones</td><td></td><td></td><td></td><td>X</td><td></td><td></td></tr>
<tr><td colspan="2">A14 Desarrollo y Adquisición de Software Aplicativo</td><td></td><td></td><td></td><td></td><td>x</td><td></td></tr>
<tr><td colspan="2">A15 gestión de Terceros</td><td></td><td>x</td><td></td><td></td><td></td><td></td></tr>
</table>
</td><td>6.2.1</td><td>Gestión Tecnológica</td></tr>
</table>

N°	OPORTUNIDAD Y/O RECOMENDACIÓN	Numeral Del Informe	Proceso Responsable
	A16 Incidentes de Seguridad: X A17 Gestión de Continuidad: X A18 Cumplimiento: x, X		
25	Una vez implementados los controles MSPI y los instrumentos definir métricas o indicadores de efectividad. Ver ejemplo en oportunidades de mejora.	6.2.1	Gestión Tecnológica
26	Configurar correctamente las VLAN´s para evitar que se realicen escaneos a direcciones IP diferentes a la del segmento en la que se encuentra configurado cada equipo. Crear un segmento especial únicamente para los servidores.	6.2.2.	Gestión Tecnológica
27	Adelantar la implementación de la solución de seguridad perimetral contratado, al terminarla se deben realizar las pruebas necesarias para garantizar que las VLAN's se encuentren correctamente configuradas y que las debilidades relacionadas en este informe se hayan remediado. Garantizar que se creen los instructivos necesarios para la administración, monitoreo de la solución.	6.2.2.	Gestión Tecnológica
28	Crear el esquema de red detallado, completo y actualizado de acuerdo a las observaciones dadas en el presente informe, en este deben especificarse claramente los elementos de red, su ubicación, las VLAN's, equivalencias de IPv4 – Ipv6, Wifi, etc.	6.2.2.	Gestión Tecnológica
29	Elaborar instructivos de la configuración y operación del routers y swtichs, además de un procedimiento para el cambio periódico de las claves de administrador para el Dominio, Routers y Firewalls.	6.2.2.	Gestión Tecnológica
30	Configurar las políticas del nuevo firewall y las políticas de dominio para impedir descargas de archivos ejecutables o de instalación. La restricción se debe generar independientemente del cargo del usuario. Todo archivo ejecutable que se requiera debe ser autorizado por la OAP.	6.2.2.	Gestión Tecnológica
31	Para la Wifi se recomienda usar una puerta de enlace servidor DHCP, DNS y WINS diferente a los utilizados por la red corporativa. De ser posible enmascarar la dirección IP de las Wifi para que aparezca en un segmento diferente a la red corporativa.	6.2.2.	Gestión Tecnológica
32	Configurar la red y el DHCP para restringir la conexión alámbrica al dominio solo a equipos cuya dirección de tarjeta de red (Mac Address) este registrada en la lista autorizada o con un equipo unido al dominio *sdmujer. Local*	6.2.2.	Gestión Tecnológica
33	Restringir en todos los equipos de escritorio y portátiles el acceso al panel de control y en especial al centro de redes y recursos compartidos. Restringir de igual manera la ejecución de comandos desde el símbolo del sistema de Windows (CMD), REGEDIT y del PowerShell en los equipos de usuario. Igualmente configurar los navegadores para impedir el almacenamiento de contraseñas en texto plano. Impedir en todos los equipos la creación de conexiones ODBC.	6.2.2.	Gestión Tecnológica
34	Configurar correctamente todos los clientes del antivirus para que no permita ejecución y descargue de archivos ejecutables considerados como peligrosos.	6.2.2.	Gestión Tecnológica
35	Por ningún motivo exponer información de claves de acceso en archivos sin encriptación ni en correos y/o documentos físicos sin custodia.	6.2.2.	Gestión Tecnológica
36	Configurar todas las directivas de seguridad del dominio de acuerdo con las recomendaciones de Microsoft para entornos corporativos, en especial la vigencia de contraseña a máximo 90 días. Habilitar bloqueo de cuentas por intentos fallidos. Validar que esté funcionando correctamente.	6.2.2.	Gestión Tecnológica
37	Implementar la obligatoriedad de cambio de contraseña al inicio de primera sesión tanto para el dominio como para el correo y sistemas de información, ya que esta debilidad puede ser aprovechada para suplantaciones de identidad o acceso a información confidencial, no solo por atacantes externos, sino internos.	6.2.2.	Gestión Tecnológica
38	Implementar los niveles de acceso a la navegación en internet en la nueva solución de seguridad perimetral, con el fin de garantizar que todos los usuarios tengan privilegios acordes con las funciones de su cargo. No es recomendable que en las oficinas se ingrese a correos personales, redes sociales personales, etc.	6.2.2.	Gestión Tecnológica

N°	OPORTUNIDAD Y/O RECOMENDACIÓN	Numeral Del Informe	Proceso Responsable
39	Generar un procedimiento de revisión periódica de los informes generados por las consolas del endpoint y del nuevo firewall, tomar acciones correctivas frente a estas alertas y documentarlas.	6.2.2.	Gestión Tecnológica
40	Realizar un procedimiento de revisión y cambio periódico de las contraseñas de los equipos activos de red tales como: Switches, impresoras, NAS routers y asegurar que en ningún equipo quede con la contraseña de fábrica.	6.2.2.	Gestión Tecnológica
41	Asegurar que en las configuraciones del nuevo Firewall y del antivirus se detecte y bloquee automáticamente todo tipo de trafico de envenenamiento ARP, para evitar el uso de sniffers no autorizado.	6.2.2.	Gestión Tecnológica
42	Instalar una herramienta que escanee periódicamente los recursos compartidos en la red e identifique cuales se encuentran sin protección y configurar las debidas restricciones de acceso.	6.2.2.	Gestión Tecnológica
43	Generar una revisión de los usuarios administradores de domino y dejar como máximo 2 usuarios, el resto se deben perfilar de acuerdo a las funciones de cada uno, los usuarios de soporte no necesitan ser administradores de dominio para ejecutar sus funciones. Para usuarios administradores no nombrados que usan algunos servicios de red, se debe garantizar el cambio periódico de contraseña y su respectivo monitoreo. Solucionar la dependencia del usuario: ***evillarraga*** para el correcto funcionamiento de Perno	6.2.2.	Gestión Tecnológica
44	Configurar en la solución de *enpoint*, la opción de control de dispositivos para deshabilitar todos los dispositivos extraíbles como unidad de CD, USB, bluetooth, celulares, etc. y solo permitir aquellos que sean aprobados para su uso dependiendo del usuario con privilegios que lo necesite para las funciones de su cargo. El uso de CD o USB 's de arranque permite violar la seguridad de cualquier equipo, ya que podría cambiarse la contraseña de administrador local de los mismos.	6.2.2.	Gestión Tecnológica
45	En la implementación de la solución de seguridad perimetral asegurar que se configure la sincronización Firewall – Endpoints, para proteger correctamente todo el tráfico interno de la red local, y así poder detectar y bloquear automáticamente cualquier anomalía o ataque interno desde los equipos y/o elementos de red.	6.2.2.	Gestión Tecnológica
46	Cambiar todas las contraseñas de cualquier servicio o recurso expuesto sobre la red y ocultarlos para que no sea posible su visualización por parte de cualquier usuario sin autenticación en dominio.	6.2.2.	Gestión Tecnológica
47	Implementar medidas automáticas o manuales para el cambio periódico de contraseña en todos los servicios Tic y sistemas de información atendiendo el dominio 9 de MSPI. De ser posible usar la solución de contraseña de administrador local" (LAPS) para la administración de contraseñas de cuentas locales de equipos unidos al dominio	6.2.2.	Gestión Tecnológica
48	En el marco de la construcción del inventario de activos de información, identificar equipos de cómputo que almacenan de manera local información de carácter confidencial e implementar medidas de seguridad que impidan su acceso por alguien distinto al responsable del equipo.	6.2.2.	Gestión Tecnológica
49	Atender y evaluar las oportunidades de mejora para el rendimiento de los portales y aplicaciones web relacionados en los reportes de rendimiento web.	6.2.2.	Gestión Tecnológica
50	Se debe adelantar la generación de un diagrama de distribución de puntos, equipos y elementos activos de red en los closets de cableado para facilitar la rápida identificación y referenciación de puntos y equipos al personal de soporte y/o contratistas en caso de contingencia y como transferencia de conocimiento.	6.2.3	Gestión Tecnológica
51	Adelantar un procedimiento de apagado seguro de los equipos de comunicaciones y/o de servidores del centro de cómputo en caso de contingencia eléctrica.	6.2.3	Gestión Tecnológica
52	Fortalecer el control de ingreso y salida de equipos en las oficinas y realizar verificaciones y auditorias para el cumplimiento de esta norma de seguridad, con los vigilantes.	6.2.3	Gestión Tecnológica
53	Adelantar el proceso de generación del plan de continuidad de la entidad, tomando como referencia las guías: 10 - Continuidad de Negocio y 11 - Análisis de Impacto de Negocio emitidas por Mintic para la implementación del MSPI, al no contar este plan implementado, la Entidad se puede exponer a perdidas por tiempos de inactividad en caso de contingencias o desastres.	6.3	Gestión Tecnológica

N°	OPORTUNIDAD Y/O RECOMENDACIÓN	Numeral Del Informe	Proceso Responsable
54	Complementar la identificación de riesgos de seguridad y tecnológicos de manera articulada con los activos de información y los objetivos de control de MSPI, incluir la relación entre el tratamiento de riesgos y los planes de continuidad, teniendo en cuenta la correlación entre activos – riesgos y planes de contingencia y continuidad. La siguiente imagen presenta un ejemplo de correlación:  	6.3	Gestión Tecnológica
55	Adelantar el Análisis de Impacto al Negocio BIA para establecer los tiempos, los protocolos de contingencia y recuperación y las estrategias de fidelidad de la data entre ambientes. Articular con el Plan de continuidad de acuerdo con los resultados del BIA. El siguiente es un modelo de tiempos a establecer:  		
56	Generar un Plan de contingencias y de recuperación de desastres que incluya como mínimo: • Todos los activos de información críticos. • Los acuerdos ANS alcanzados con los responsables de procesos. • Incluir respaldo de elementos de configuración de la plataforma TIC que permitan ya sea contar con ambientes replica o agilizar los tiempos de puesta en operación de la contingencia. Ajustar las actividades y planes de contingencia específicos conforme a los acuerdos alcanzados con el negocio.	6.3	Gestión Tecnológica
57	Luego de construido el plan de continuidad adelantar las pruebas integrales al mismo y documentar los protocolos y resultados, contemplar los lineamientos de ISO 27002:2013 en el control 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	6.3	Gestión Tecnológica

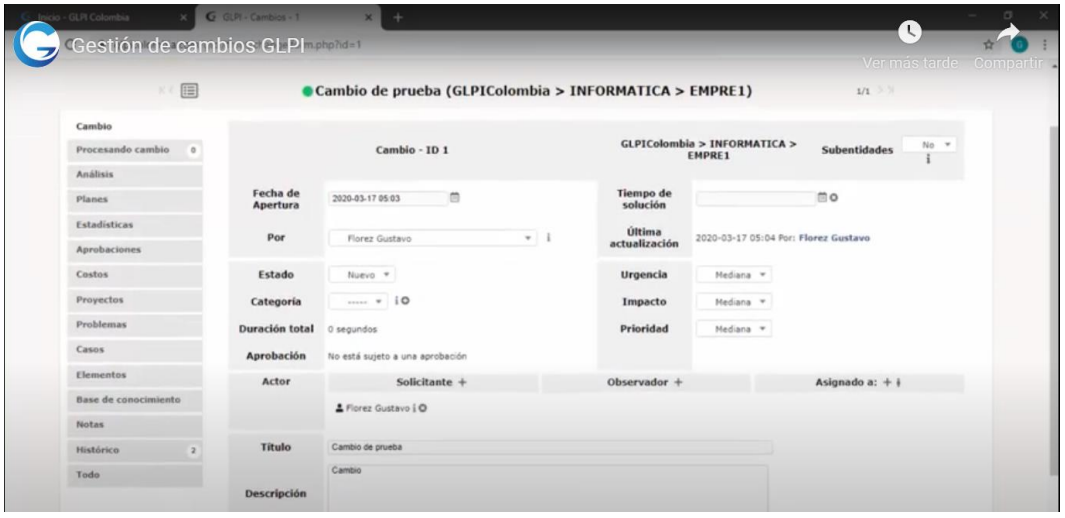
<table>
<tr><th>N°</th><th>OPORTUNIDAD Y/O RECOMENDACIÓN</th><th>Numeral Del Informe</th><th>Proceso Responsable</th></tr>
<tr><td>58</td><td>Adelantar la implementación de la nueva solución de backups garantizando que se generen los procedimientos, guías e instructivos de su administración y correcto funcionamiento. Verificar que se implementen en la herramienta reportes automatizados que sirvan como documentación para el seguimiento y el control de los respaldos y pruebas de restauración.</td><td>6.3</td><td>Gestión Tecnológica</td></tr>
<tr><td>59</td><td>Verificar que en la nueva solución de copias de seguridad se incluya la programación de copias de respaldo el Backup de los archivos de configuración de los sistemas manejadores de bases de datos (RDBMS), Backup de las bases de datos, las imágenes de los servidores físicos, configuraciones de switches, el nuevo firewall, routers, y en general de todas las configuraciones de los elementos activos de red y su ubicación final en almacenamientos en la nube.</td><td>6.3</td><td>Gestión Tecnológica</td></tr>
<tr><td>60</td><td>Generar un formato del plan de copias de seguridad que permita identificar de forma detallada y en un único documento la información respaldada, la frecuencia, retención, ubicaciones intermedias y finales, ubicación de logs, permisos de acceso y de seguridad de todos los backups generados en la Entidad y que no dependa de la solución adquirida para los backups, incluir un formato de novedades de procesos y de restauraciones aleatorias en cumplimiento del objetivo de control 12.3 del MSPI
A continuación, se presenta un ejemplo de estos formatos:
-Formato Plan de Backups:
 
<table>
<tr><th>N°</th><th>Información a respaldar</th><th>Detalles del respaldo</th><th>Responsable</th><th>Herramienta utilizada</th><th>Frecuencia/ Hora de Ejecución</th><th>Retención Inicial</th><th>Medio Inicial/ruta</th><th>Retención Final</th><th>Medio final/ruta</th><th>ubicación custodia alterna</th><th>Evidencia de ejecución</th><th>Evidencia de No Conformidad y acción correctiva</th><th>Evidencia de prueba restauración</th><th>Procedimiento relacionado</th></tr>
<tr><td>replicación</td><td>Indique el tipo de información a respaldar de acuerdo a lo establecido en DG-GER-015</td><td>Explique el propósito del respaldo y en que consiste</td><td>Funcionario responsable de ejecución, verificación, acciones correctivas y pruebas</td><td>herramienta de backup utilizada</td><td>Frecuencia de ejecución acordada con los propietarios de la información cuando aplique</td><td>tiempo de retención en el primer medio de backup</td><td>ruta y/o media donde se almacena el primer backup</td><td>Tiempo de Retención cuando se lleva a custodia alterna</td><td>ruta y/o Media de Retención cuando se lleva a custodia alterna</td><td>Ubicación fuera de las instalaciones</td><td>en que archivos y ubicación se almacenan los logs de la ejecución</td><td>en que archivos y ubicación se almacenan las evidencias de acciones correctivas frente a logs fallidos o errores en pruebas de restauración</td><td>fecha y evidencia de las pruebas de restauración periódicas y aleatorias</td><td>Nombre del procedimiento SIG relacionado</td></tr>
<tr><td>1</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>2</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>3</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

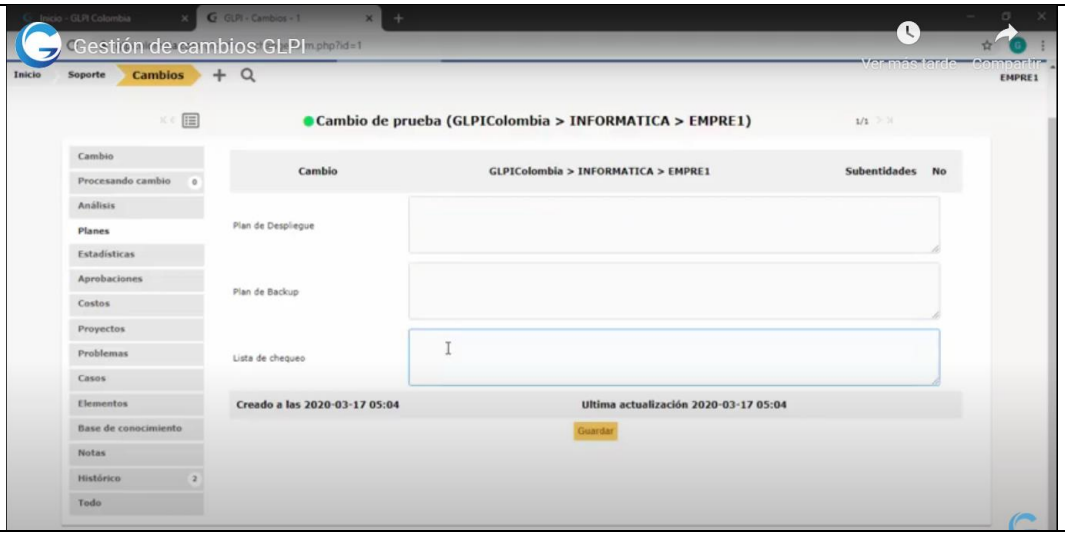
-Formato Registro de novedades de Backups:
 
<table>
<tr><th>ID</th><th>Fecha</th><th>Servidor</th><th>Tipo</th><th>Descripcion del Contenido</th><th>Causa</th><th>Observaciones - Acciones Correctivas</th></tr>
<tr><td><identificacion o etiquea de la Copia de Respaldo></td><td><fecha de la novedad></td><td><IP del servidor o nombre del servidor origen de la copia ></td><td><Copia de Resplado o Restauración></td><td><Datos que incluye y/o tipo de copia></td><td><Causa de la falla con la ejecución del backup o Restauración></td><td><Observaciones del caso></td></tr>
</table></td><td>6.3</td><td>Gestión Tecnológica</td></tr>
<tr><td>61</td><td>Asegurar que todas las copias de seguridad generadas y almacenadas en ubicaciones compartidas de la red local tenga los permisos de acceso únicamente a funcionarios o contratistas del proceso de gestión tecnológica.</td><td>6.3</td><td>Gestión Tecnológica</td></tr>
<tr><td>62</td><td>En el marco de la implementación del MSPI actualizar la identificación de la matriz de riesgos de acuerdo con los activos de información y depurar las acciones y controles reportados de acuerdo con las configuraciones de dichos controles en la plataforma TIC.
Incluir evidencia de la implementación y eficacia de los controles.

Continuar la identificación de riesgos y asociación con los controles de MSPI dando cobertura a los demás objetivos de control de la norma.

En el marco de la implementación del MSPI unificar el procedimiento DE-PR-11 ADMINISTRACION DEL RIESGO para todo el sistema integrado de gestión, agregando si es necesario lo que corresponda a la particularidad de identificación y tratamiento de riesgos de manera alineada con los activos de información de la entidad.</td><td>6.3</td><td>Gestión Tecnológica</td></tr>
</table>

N°	OPORTUNIDAD Y/O RECOMENDACIÓN	Numeral Del Informe	Proceso Responsable
	Se recomienda adelantar el ejercicio de identificación de riesgos de seguridad de la información orientado a activos críticos que en caso de materialización de amenazas afectan la continuidad de la operación y/o la disponibilidad, integridad y resguardo de la información. Tener en cuenta que los riesgos deben contemplar también los diferentes aspectos de la gestión TIC para garantizar que los controles de la norma han sido incorporados en los riesgos. Tal es el caso de los riesgos relacionados con la relación con terceros que no necesariamente se originan en activos tecnológicos, sino en debilidades contractuales o de control.		
63	Adelantar un plan de sensibilización y gestión de cambio para el cumplimiento sostenible de la resolución 1519 de 2020 que incluya: ✓ Socialización de los resultados a la alta dirección por parte del contratista a cargo, que incluya no solo los avances logrados sino su percepción de las estrategias a seguir para dar continuidad al cumplimiento. ✓ Establecer un equipo de representantes de las áreas que sean agentes de cambio de construcción de contenido, para realizar la planeación de talleres de sensibilización y transferencia de conocimiento para incorporar la norma en todos los contenidos que se generen a futuro. ✓ Establecer responsables de la revisión periódica del cumplimiento.	6.4	Gestión Tecnológica
64	Incorporar al documento de "METODOLOGIA PARA EL DESARROLLO DE SOFTWARE" las características de Scrum y de ser posible implementar una herramienta para su gestión que incluya: • Tablero de requerimientos de alto nivel codificados y segmentados en historias de usuario • Cronogramas de desarrollo a nivel de actividad por historias de usuario. • Asignaciones individuales de tareas • Asignación de pesos y fechas de entrega con base en una técnica de cálculo de esfuerzo de desarrollo Incorporar metodologías de estimación de esfuerzo, para los desarrollos de software: Una técnica practica para grupos pequeños de desarrollo es la estimación por transacciones en unidad de medida horas (mesa de trabajo con los desarrolladores para asignar esfuerzo en horas a cada tipo de objeto de construcción como resultado del promedio de juicio de experto), esta técnica permite establecer el máximo aprovechamiento de las inversiones realizadas por la entidad en recursos asignados al desarrollo de software, además de aportar elementos de juicio para documentar cronogramas de desarrollo con menor riesgo de atrasos. Gestionar de manera rígida los cambios. Alinear la metodología para cumplir de manera paralela con MSPI: **14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.** 14.1 Requisitos de seguridad de los sistemas de información. 14.1.1 Análisis y especificación de los requisitos de seguridad. 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas. 14.1.3 Protección de las transacciones por redes telemáticas. 14.2 Seguridad en los procesos de desarrollo y soporte. 14.2.1 Política de desarrollo seguro de software. 14.2.2 Procedimientos de control de cambios en los sistemas. 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo. 14.2.4 Restricciones a los cambios en los paquetes de software. 14.2.6 Seguridad en entornos de desarrollo. 14.2.7 Externalización del desarrollo de software.	6.5	Gestión Tecnológica

N°	OPORTUNIDAD Y/O RECOMENDACIÓN	Numeral Del Informe	Proceso Responsable
	14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas. 14.2.9 Pruebas de aceptación. 14.3 Datos de prueba. 14.3.1 Protección de los datos utilizados en pruebas.		
65	En GLPI incluir los requerimientos de desarrollo como una tipología de solicitud, registrar las historias de usuario de cada requerimiento, asignar responsable y usar la funcionalidad de documentos anexos para llevar la base documental de cada desarrollo. Usar la funcionalidad de gestión de cambios. Las siguientes imágenes orienten sobre la funcionalidad de RFC en GLPI que permite llevar la trazabilidad de los cambios de desarrollo y asociar tanto actividades como documentos, planes y procesos de aprobación. De igual manera asociar incidentes sobre los desarrollos desplegados.  	6.5	Gestión Tecnológica

N°	OPORTUNIDAD Y/O RECOMENDACIÓN	Numeral Del Informe	Proceso Responsable
			
66	Con base en los registros de mesa de ayuda y los cronogramas de control, diseñar nuevos indicadores de Cumplimiento (desviaciones entre fechas reales y planeadas), productividad (menores retrabajos por especificación, diseño y construcción), calidad (conteo de defectos, número de pasadas de testing y desempeño del producto final) y/o eficiencia (logro de objetivos sin desviación de recursos)	6.5	Gestión Tecnológica
67	Dar instrucción de obligatorio cumplimiento del procedimiento establecido en cuanto al diligenciamiento de los formatos del ciclo de desarrollo de software y su almacenamiento en las carpetas dispuestas para este fin.	6.5	Gestión Tecnológica
68	Incluir en los sets de prueba, casos de pruebas no funcionales cuando el desarrollo implique procesamiento de altos volúmenes de datos o alta concurrencia de usuarios. Aplicar no funcionales cuando son desarrollos de cara a la ciudadanía Dar trazabilidad entre los requerimientos, las historias de usuario, casos de prueba y los defectos mediante codificación jerárquica, con el fin de establecer indicadores de calidad sobre el desarrollo.	6.5	Gestión Tecnológica
69	Se debe generar un procedimiento de generación de informes periódicos del GLPI que sirvan como indicadores para medir la efectividad en la atención y prestación de servicios del proceso de gestión tecnológica.	6.6	Gestión Tecnológica
70	Para que se aproveche toda la funcionalidad de la herramienta se debe adelantar un plan para implementar y configurar todas las funcionalidades como los inventarios de software y hardware automatizados, gestión de cambios, control de incidentes de seguridad, definición de plantillas por tipo de incidente o requerimientos, gestión de conocimiento y auto soporte.	6.6	Gestión Tecnológica
71	Publicar manuales, instructivos, formatos y procedimientos en la funcionalidad de Gestión de conocimientos del GLPI y capacitar a los usuarios de su uso. Se debe mantener una constante actualización de la documentación publicada para evolucionar a la autogestión de incidentes por parte d ellos usuarios.	6.6	Gestión Tecnológica
72	Terminar la implementación de agente *fusión inventory* en los equipos de usuarios que permita generar el inventario de software y hardware automáticos y actualizado con información centralizada y permita la obtención de información histórica y estadística de equipos.	6.6	Gestión Tecnológica
73	Luego de concluir con implementación del agente de inventarios automatizados, habilitar el control de licenciamiento de software en el GLPI, el seguimiento a la presencia y/o ausencia de software y hardware, la gestión de activos y configuraciones, hoja de vida de los equipos con su respectiva relación de software instalado, generar un procedimiento y manual de este control.	6.6	Gestión Tecnológica

N°	OPORTUNIDAD Y/O RECOMENDACIÓN	Numeral Del Informe	Proceso Responsable
74	Incluir el registro del cronograma de mantenimientos preventivos y el resultado de los mismos en la herramienta de mesa de ayuda con evidencias de las acciones realizadas	6.6	Gestión Tecnológica

7.1. HALLAZGOS

Tema o Palabras Clave		Numeral del Informe	CONDICIÓN	CRITERIO	CAUSA	EFECTO	Proceso Responsable	ID LUCHA (reincidencia)
1.	NA	NA	NA	NA	NA	NA	NA	NA

ORIGINAL FIRMADO
ANGELA JOHANNA MARQUEZ MORA
JEFA DE CONTROL INTERNO