INFORME FINAL DE LA AUDITORÍA INTERNA AL PROCESO GESTIÓN DE TECNOLOGÍA DE LA INFORMACIÓN

Noviembre 2021

ALCALDÍA MAYOR DE BOGOTÁ D.C.

BOGOTÁ

TABLA DE CONTENIDO

INDICE DE TABLAS

TABLA DE ILUSTRACIONES

INFORME FINAL DE AUDITORÍA INTERNA DE AL PROCESO DE GESTIÓN DE TECNOLOGÍA DE LA INFORMACIÓN.

Fecha de Ejecución: del 19 de septiembre al 16 de noviembre de 2021

1. OBJETIVO

Evaluar los controles generales del Procesos de Gestión de Tecnologías de Información con el fin de verificar la implementación de las buenas prácticas de gestión TIC alineadas a los objetivos estratégicos del Instituto e identificar y verificar las actividades a evaluar tomando como base los criterios de auditoría definidos, mediante la inspección implementación y existencia documentada y divulgada de las políticas, estándares y procedimientos, diseñados para proporcionar confianza en relación a los objetivos de la función TIC y de esta manera se logren alcanzar con el uso eficiente de los recursos disponibles y que los eventos no deseados se corrijan y prevean, oportunamente.

2. ALCANCE

Se realizó la revisión de controles generales al Proceso de Gestión de Tecnologías de Información del IDPAC alineados a:

- Planeación y administración de los recursos informáticos
- Seguridad física
- Administración de recursos de TI
- Desarrollo y adquisición de software aplicativo
- Administración de datos y seguridad lógica

Lo anterior con corte a octubre de 2021.

3. CRITERIOS

La presente auditoría corresponde a una evaluación de la existencia documentada e implementada de controles generales en los dominios relacionados en el alcance, para lo cual el auditor usa como referente el cumplimiento de algunos lineamientos de buenas prácticas de los estándares, ISO 27001:2013, Manual de Gobierno Digital 2018 y el marco de referencia de Arquitectura Empresarial para la Gestión de Tecnologías de la Información del Estado Colombiano.

Así mismo dentro de la referencia interna se tuvo en cuenta:

- ✓ Caracterización del Proceso de Gestión de Tecnología de la Información IDPAC-GTI-CA-01 Versión del 30/11/2020
- ✓ Política de seguridad de la Información, - IDPAC-GTI-OT-04 Versión 2 del 23/03/2021

- ✓ Plan estratégico de las tecnologías de la Información y las Comunicaciones – PETI - IDPAC-GTI-PL-02 Versión 1 -23/03/2021
- ✓ Plan Estratégico Institucional PEI 2020-2024
- ✓ Decreto 415 de 2016 Ministerio TIC
- ✓ Resolución interna 116 de 2017 del IDPAC
- ✓ Guía metodológica de formulación, medición, seguimiento y evaluación de gestión de indicadores del IDPAC
- ✓ Formato Registro Ingreso al centro de cómputo IDPAC-GTI-FT-16
- ✓ Plan Nacional de Desarrollo 2018-2022. "Pacto por Colombia, Pacto por la Equidad
- ✓ Decreto 1078 de 2015
- ✓ Ley 1523 de 2012
- ✓ Guía No 2 de la elaboración de la Política de Seguridad de la Información del Ministerio de Tecnologías de la Información

4. METODOLOGÍA

Para el desarrollo de la auditoría 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 del IDPAC, solicitando al Proceso de Gestión de Tecnología de la Información las evidencias correspondientes a través de correos electrónicos. De igual forma se realizaron mesas de trabajo con el Proceso con el fin de aclarar inquietudes sobre los aspectos evaluados y se solicitaron los soportes que evidenciaran la ejecución de los temas indagados.

5. PRESENTACIÓN DE RESULTADOS

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

- ✓ Observaciones: Corresponden a los aspectos negativos (debilidades) identificadas para el Proceso de Gestión de Tecnologías de Información.

- ✓ Oportunidades de mejora: Corresponde a la existencia de un cumplimiento, pero a pesar de ello se determina, bajo criterios objetivos, que existe un margen de mejora para optimizar más una actividad, tarea o Proceso concreto

- ✓ Riesgos Asociados: Corresponde a las situaciones donde existe la posibilidad de sufrir un daño o ser vulnerable con la posible materialización de la oportunidad de mejora identificada

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

6. DESARROLLO DE LA AUDITORÍA

6.1 Planeación y administración de los recursos informáticos

6.1.1 Fortalezas componente de Planeación y Administración de Recursos Informáticos:

- ✓ El PETI (Plan Estratégico de Tecnología de la Información) se encuentra debidamente alineado al PEI (Plan Estratégico Institucional) a través del proyecto de inversión 7714 "Fortalecimiento de la capacidad tecnológica y administrativa del Instituto Distrital de la Participación y Acción Comunal - IDPAC. Bogotá" y bajo el objetivo estratégico de fortalecer la capacidad institucional, potencializar el desarrollo del talento humano, promoviendo Procesos de innovación en la gestión y el uso de nuevas tecnologías para dar respuesta eficiente, efectiva y eficaz a las demandas sociales de participación.

- ✓ Se generan informes de gestión anuales en los cuales se presentan los avances de los diferentes proyectos del Instituto, entre ellos el 7714 para el cual en el Informe de gestión 2020 (diciembre 2020), se contemplan elementos relevantes de Gobierno Digital alineados con el cumplimiento MIPG (Modelo Integrado de Planeación y Gestión) y declara como reto el "Implementar una estrategia para fortalecer y modernizar la capacidad tecnológica del sector de gobierno".

- ✓ Acorde al esquema de estructura organizacional de TI se evidencia en la actualidad una mayor centralización de contratistas y proveedores en la gestión de servicios TIC, bajo responsabilidad de profesional Líder del Proceso de Gestión TIC.

- ✓ Compromiso por parte de los contratistas del Proceso pese a la naturaleza de su contrato. Este compromiso se evidencia no solo en la ejecución del objeto contratado sino en el interés por adquirir conocimiento que pueda ser de valor agregado para la entidad

6.1.2 Aspectos susceptibles de mejora al componente de Planeación y Administración de Recursos Informáticos:

6.1.2.1 Dirección u Oficina de tecnología de la Información y las comunicaciones

Acorde con las sesiones de trabajo realizadas con los responsables del Proceso de Gestión de Tecnología de la Información y a la revisión de la documentación divulgada Sistema Integrado de Gestión – SIG Participo, especialmente al PETI (Plan Estratégico de Tecnología de la Información) se pudo evidenciar que el IDPAC no 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.

Riesgos asociados

El no tener una Dirección u Oficina de Tecnología de la Información y las Comunicaciones limita 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. Al no contar con un presupuesto propio el Proceso, es susceptible de ser redireccionado a otras adquisiciones

Observación No. 1.

El Proceso de Gestión de Tecnología de la Información, incumple con lo definido en el decreto 415 de 2016, artículo 2.2.35.4., establece que cuando la entidad cuente con su estructura con una dependencia encargada de accionar la estrategia de las tecnologías y sistemas de la Información y las comunicaciones, hará parte del comité directivo y dependería del nominador y/o representante legal de la misma

Recomendación No. 1.

Evaluar la viabilidad o no, y dejar evidencia documental de esto, en cuanto a la creación de una Dirección u Oficina de Tecnología de la Información y las Comunicaciones, cuyo responsable haga parte del Comité Directivo y cuyo propósito este orientado al cumplimiento de los 16 Objetivos del fortalecimiento institucional del artículo 2.2.35.3 del decreto 415 de 2016.

6.1.2.2 Comité de seguridad de la Información

Acorde con las sesiones de trabajo realizadas con los responsables del Proceso de Gestión de Tecnología de la Información y a la revisión de la documentación divulgada en el Sistema Integrado de Gestión – SIG Participo a nivel de Gobierno TI y la estrategia de seguridad de la información, se procedió a validar el estado y acciones realizadas por parte del Comité de Seguridad, solicitando las tres (3) actas de las más recientes reuniones del comité para el periodo 2021, donde no se logro tener evidenciar alguna en ese momento.

En la reunión de cierre de la auditoria llevada a cabo el 22 de noviembre de 2021, el Proceso indico que los temas relacionados con este comité se trataban en sesiones del comité de Gestión y Desempeño por lo cual se solicito por parte del auditor la remisión, a más tardar el día 23 de noviembre de 2021, de las actas de las sesiones de Comité de Gestión y Desempeño de 2021 en las cuales se hubiesen tratado aspectos del Comité de Seguridad de la información, no obstante a la fecha de emisión del presente informe el Proceso no se allego la documentación solicitada.

Riesgos asociados

El hecho de no reunirse el Comité de Seguridad de la Información de forma periódica limita a la entidad a revisar los diagnósticos del estado de la seguridad de la Información del IDPAC, así mismo no habría coordinación para dirigir acciones específicas que ayuden a proveer un ambiente seguro y estable de los recursos de Información que sea consistente con las metas y objetivos del IDPAC.

Observación No. 2.

El Proceso de Gestión de Tecnología de la Información, si bien tiene establecido un Comité de Seguridad de la Información bajo resolución interna 116 de 2017 del IDPAC incumple con lo definido en el artículo 6 que establece que el Comité de Seguridad de la Información deberá reunirse, de manera ordinaria cuatro (4) veces al año, con previa convocatoria del secretario técnico del comité.

Recomendación No. 2.

- ✓ Evaluar la posibilidad de fortalecer los lineamientos y funciones definidas del Comité de Seguridad de la Información de tal manera que sea un referente de la organización para toma de decisiones que ayuden a proveer un ambiente seguro.

- ✓ Adelantar las acciones necesarias que conduzcan a que se realicen las reuniones del Comité de seguridad de la Información acorde a la periodicidad definida en la resolución interna 116 de 2017, documentando las respectivas actas.

6.1.2.3 PETI (Plan Estratégico de Tecnología de la Información)

En indagación al link de transparencia de la página web IDPAC el 14 de octubre de 2021, se logra evidenciar que el PETI (Plan Estratégico de Tecnología de la Información) se encuentra desactualizado dado que se hace referencia a la versión 17-12-2019 y no es acorde con la vigencia de la administración actual.

Es importante mencionar que la entidad si cuenta con dicho documento formalizado, no obstante, solo se ha divulgado como primera versión a través del Sistema Integrado de Gestión – SIG.

En la reunión de cierre de la auditoria llevada a cabo el 22 de noviembre de 2021, el Proceso manifestó que este documento si había sido publicado (actualizado) de manera oportuna, por lo cual se solicito allegar la evidencia correspondiente; mediante correo electrónico recibido el 23 de noviembre el Proceso únicamente remitió el link donde se encuentra publicado el documento, una vez verificado se pudo establecer que la solicitud de actualización (publicación) del documento fue realizada a las 20:35 horas del 14 de octubre de 2021, es decir posterior a la verificación y requerimiento efectuados por el auditor.

Riesgo asociado

El hecho que los integrantes de las instituciones y comunidad en general desconozcan Información estratégica y obligatoria de las entidades limita a dar garantía sobre el conocimiento, transparencia y confianza sobre la gestión y aplicabilidad de los planes a desarrollar por la entidad.

Observación No. 3.

El Proceso de Gestión de Tecnología de la Información incumple con lo definido con la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional bajo el articulo 11 apartado C, hace mención a publicar la Información obligatoria y de manera proactiva, para aquellos documentos o procedimiento que se siguen para tomar decisiones en las diferentes áreas.

Recomendación No. 3.

- ✓ Adelantar las acciones necesarias para mantener actualizada la Información del Proceso (en particular el Plan Estratégico de Tecnología de la Información (PETI)) en el link de transparencia de la página Web del IDPAC.

- ✓ Evaluar la posibilidad de fortalecer las capacidades y procedimientos internos del Proceso para cumplir con la ley y brindar Información de mayor calidad.

6.1.2.4 Indicadores del Proceso de Gestión de Tecnologías de la Información.

Acorde con la revisión realizada el 14 de octubre de 2021 a los tres (3) indicadores del Proceso de Gestión de Tecnologías de Información, definidos en su caracterización y que son gestionados a través el Sistema de Información SIG Participo, se pudo evidenciar que en la actualidad no se ha reportado ningún indicador para el periodo del 2021 acorde a las frecuencias definidas (mensual o trimestral), por lo cual se desconoce el estado de la gestión de los indicadores mencionados a continuación:

- Servicios disponibles
- Soporte realizado
- Requerimientos de desarrollo realizados

Riesgo asociado

Una inadecuada gestión de indicadores se presta para una incorrecta medición de objetivos y metas del Proceso, así como toma de decisiones equivocadas y limitantes para analizar comportamiento a lo largo del tiempo.

Observación No. 4.

El Proceso de Gestión de Tecnología de la Información incumple lo definido en la "Guía metodológica de formulación, medición, seguimiento y evaluación de gestión de indicadores del IDPAC", en particular con lo relacionado a las políticas operativas para la administración de indicadores que establecen:

- *La medición y seguimiento de los indicadores se efectuará de acuerdo con lo establecido en la Hoja de reporte por Proceso de las prácticas del Sistema Integrado de Gestión*

- *Los resultados de los indicadores y su análisis, serán remitidos a la Oficina Asesora de Planeación, en los instrumentos y en las condiciones establecidas por esta dependencia, para ser publicados en la página web de la Entidad.*

Recomendación No. 4

Tomar medidas encaminadas a cumplir de manera completa y oportuna con el reporte de Información en el Sistema de Información SIG Participo, en particular a lo concerniente a los indicadores del Proceso.

6.2 Seguridad Física

6.2.1 Fortalezas componente de Seguridad Física:

- ✓ Los servidores, equipos de comunicación y demás elementos críticos se encuentran resguardados en el Centro de Cómputo con el respectivo control de acceso que permite limitar el ingreso exclusivamente a los funcionarios autorizados del Proceso de Gestión de Tecnología de la Información.

- ✓ El centro de cómputo cuenta con elementos de seguridad física tanto de detección como mitigación en caso de alguna eventualidad o contingencia tales como sistema detección y aspersión para incendios, sistema de refrigeración con su respectivo control de temperatura.

- ✓ Se lleva un registro de control y monitoreo por parte de los responsables del Proceso de Gestión de Tecnología de la Información, sobre el acceso de personal externo al ingreso del Centro de Cómputo.

6.2.2 Aspectos susceptibles de mejora al componente de Seguridad Física:

6.2.2.1 Centro de Cómputo Principal

Acorde a la visita a realizada al centro de cómputo principal del IDPAC el 22 de octubre de 2021 en compañía de un funcionario responsable del Proceso de Gestión de Tecnología de la Información, se realizó una inspección tanto a nivel físico como ambiental del espacio mencionado, evidenciando las siguientes situaciones susceptibles de mejora:

Riesgo asociado

El estado actual y los hechos mencionados a continuación aumentan la probabilidad de pérdida de Información y no operación del negocio debido a daños que afecten la disponibilidad de los recursos tecnológicos por condiciones ambientales, eléctricas y locativas no adecuadas.

Al tener la mala distribución y no contar tener etiquetados la totalidad de los cables en los racks cual dificultaría la identificación de fallas en los puntos y disminuye los tiempos de atención.

Cómo parte de la visita realizada se logra evidenciar la existencia de material inflamable como cajas de cartón, cables de red sueltos, equipos de cómputo sin usar, documentación en papel suelto, bolsas plásticas.

Ilustración 1 Material Inflamable en el Centro De Cómputo

Fuente: Evidencia Oficina de Control Interno

Observación No. 5.

El Proceso de Gestión de Tecnología de la Información incumple con lo expuesto en el "Formato Registro Ingreso al centro de cómputo IDPAC-GTI-FT-16 del 03/05/2018 donde señala que dentro de los "Elementos que no se pueden ingresar" esta "*Explosivos, elementos o sustancias inflamables o corrosivas*. por su parte en "Otras Obligaciones" establece *retirar los desechos y cajas vacías antes de salir del edificio.*

Recomendación No. 5.

- ✓ Establecer acciones tendientes a garantizar que las medidas físicas y ambientales sean adecuadas, mediante la ejecución adecuada de los procedimientos y protocolos establecidos.

- ✓ Evaluar la viabilidad de fortalecer el procedimiento de ingreso al Centro de Cómputo cumplimiento lo estipulado en el Formato Registro Ingreso al centro de cómputo IDPAC-GTI-FT-16.

- Cómo parte de la visita realizada se logra evidenciar una distribución de cables de rack desorganizada, donde no sé logra identificar o clasificar cables de red o de electricidad, llevando esta situación a un alto de riesgo ante una contingencia.

Ilustración 2 Deficiente organización de cables del rack de Centro de Cómputo

Fuente: Evidencia Oficina de Control Interno

Observación No. 6.

El Proceso de Gestión de Tecnología de la Información incumple con lo expuesto en el "Formato Registro Ingreso al centro de cómputo IDPAC-GTI-FT-16 del 03/05/2018 donde señala en "Otras Obligaciones" Al finalizar cualquier trabajo en el Centro de Cómputo, deberá asegurarse que los cables estén bien instalados y ordenados, dentro de sus gabinetes, así como asegurarse que todas las puertas de los racks estén bien cerradas al igual que la puerta de acceso.

Recomendación No. 6

- ✓ Ver la viabilidad de adelantar un plan de etiquetado y generación de diagrama en todos los closets de comunicaciones (Racks) del centro de cómputo para permitir la fácil ubicación y rápida identificación de equipos y puntos de red.

- ✓ Ver la viabilidad, de proveer en todos los closets los organizadores de cables y organizarlos con el fin de agilizar la identificación y ubicación de cualquier falla. Adecuar o proveer espacios en los racks para que todos los equipos queden ubicados y con las protecciones adecuadas en los centros de cómputo.

Oportunidad de mejora No. 1.

Se cuenta con un extintor en el exterior del Centro de Cómputo principal de manera señalizada y con carga vigente, sin embargo, su ubicación actual no es la adecuada dado que esta junto una fotocopiadora que limitaría su retiro de manera ágil ante un evento imprevisto que genere una emergencia.

Ilustración 3 Ubicación del extintor externo al Centro de Cómputo

Fuente: Evidencia Oficina de Control Interno

- Recomendación Oportunidad de mejora No. 1.

  - ✓ Adelantar acciones que propendan por que la ubicación y en general los elementos para uso de emergencia, sean de fácil acceso y se encuentren en perfecto estado para su uso.

Oportunidad de mejora No.2.

Aunque existe un procedimiento formal de administración del centro de cómputo, este se encuentra enfocado a tareas de contingencia y monitoreo de equipo, diarios o mensuales, sin embargo, dicho documento no ha sido actualizado desde el 2018, y no contempla aspectos de gestión de acceso físico a las instalaciones, controles ambientales, etc.

Recomendación Oportunidad de mejora No.2.

Evaluar la viabilidad:

- ✓ Actualizar el procedimiento del Centro de Cómputo que establezca los controles físicos y ambientales donde se incluya aspectos relacionados a:
  - ❖ Controles de acceso físico (Cerradura, biométrico) a la ubicación.
  - ❖ Personal autorizado para el acceso a las ubicaciones donde residen los servidores.
  - ❖ Listado de controles ambientales mínimos del centro de cómputo.
  - ❖ Cronograma de mantenimiento para los dispositivos de control ambiental

6.3 Administración de Recursos TI

6.3.1 Fortalezas componente de Administración de Recursos TI:

- ✓ Los PC 's y servidores se mantienen correctamente actualizados de acuerdo con las demandas de crecimiento de la plataforma TI.

- ✓ El responsable del MSPI ya adelanto el catálogo de servicios tecnológicos "Catalogo Servicios TIC.xls" que constituye la base para establecer las matrices de cargos vs servicios para determinar la gestión de accesos del dominio 9 del GLPI asegurando que los privilegios se asignan de acuerdo a las funciones del colaborador.

- ✓ Se cuenta con la herramienta de mesa de servicio GLPI para la que se han liberado funcionalidades necesarias para hacer una gestión efectiva de mesa de servicio y solo es preciso configurarlas en la herramienta.

- ✓ La gestión de la mesa de servicio se encuentra correctamente implementada en GLPI de acuerdo a buenas prácticas. Se gestionan adecuadamente las solicitudes a través de esta mesa, los incidentes y requerimientos de los usuarios. Al servicio se ingresa únicamente desde la intranet.

6.3.2 Aspectos susceptibles de mejora al componente de Administración de Recursos TI:

6.3.2.1 Plan de Continuidad de Negocio

Acorde con las sesiones de trabajo realizadas con los responsables del Proceso de Gestión de Tecnología de la Información y al revisar la documentación divulgada en el Sistema Integrado de Gestión – herramienta SIG Participo, se pudo evidenciar que el Proceso no cuenta en la actualidad con un Plan de Continuidad de Servicios que permita definir la hoja de ruta ante una eventualidad de contingencia o controles y herramientas que brinden un análisis proyectivo de capacidad que permita establecer acciones y/o adquisiciones para asegurar la continuidad de operaciones bajo el mejor uso de recursos.
Si bien se menciona por parte de los responsables del Proceso que el Plan de Continuidad de Servicios como un instrumento en elaboración, para el mes de octubre de 2021 dicho plan no se ha formalizado, aprobado ni divulgado.

Riesgo asociado
La ausencia de un plan de continuidad de servicio limita al Proceso y a la entidad en conocer el paso a paso de cómo reaccionar ante una eventualidad que afecto los recursos tecnológicos, donde podría quedar expuesta la pérdida total de datos, interrupción del servicio, mala reputación.

Observación No. 7.
El Proceso de Gestión de Tecnología de la Información incumple las siguientes normativas relacionados al plan de riesgos y continuidad de servicios.

- ✓ Ley 1955 de 2018, por el cual se expide el Plan Nacional de Desarrollo 2018-2022. "Pacto por Colombia, Pacto por la Equidad", bajo el artículo 147. Transformación Digital Pública. Las entidades estatales del orden nacional en todos los escenarios la transformación digital deberá aplicar y aprovechar de estándares, modelos, normas y herramientas que permitan la adecuada gestión de riesgos de seguridad digital, para generar confianza en los Procesos de las entidades públicas y garantizar la protección de datos personales.

- ✓ Decreto 1078 de 2015. "TÍTULO 17 lineamientos generales en el uso y operación de los servicios ciudadanos digitales. ARTÍCULO 2.2.17.5.6. Seguridad de la Información y Seguridad Digital. Los actores que traten Información en el marco del presente título deberán contar con una estrategia de seguridad y privacidad de la Información, seguridad digital y continuidad de la prestación del servicio. en la cual, deberán hacer periódicamente una evaluación del riesgo de seguridad digital. que incluya una identificación de las mejoras a implementar en su Sistema de Administración del Riesgo Operativo.

- ✓ Ley 1523 de 2012, Por la cual se adopta la política nacional de gestión del riesgo de desastres y se establece el Sistema Nacional de Gestión del Riesgo de Desastres. Artículo 2°. De la responsabilidad. La gestión del riesgo es responsabilidad de todas las autoridades y de los habitantes del territorio colombiano. En cumplimiento de esta responsabilidad, las entidades públicas, privadas y comunitarias desarrollarán y ejecutarán los Procesos de gestión del riesgo, entiéndase: conocimiento del riesgo, reducción del riesgo y manejo de desastres, en el marco de sus competencias, su ámbito de actuación y su jurisdicción, como componentes del Sistema Nacional de Gestión del Riesgo de Desastres.

Recomendación No. 7.

- ✓ Adelantar las acciones necesarias para que se adopte e implemente el Plan de Continuidad de Servicio y recuperación de la entidad de manera articulada con la gestión de riesgos de la entidad.

- ✓ El plan debe incluir las estrategias de contingencia y de recuperación por cada activo crítico y bajo criterios de tiempos máximos de salida de operación de los Procesos de la entidad, debe tener responsables y protocolos de pruebas y de actuar.

- ✓ Una vez adelantado el Plan de Continuidad de Servicios, ejecutar las pruebas integrales al Plan y documentar los 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.

6.3.2.2 Copias de Respaldo y Restauración

Oportunidad de Mejora No.3.

Acorde con las sesiones de trabajo realizadas con los responsables del Proceso de Gestión de Tecnología de la Información y a la revisión de la documentación divulgada Sistema Integrado de Gestión, se pudo evidenciar que el Proceso no cuenta en la actualidad con un procedimiento formal y en detalle de los lineamientos para la ejecución de las copias respaldos y restauraciones de las mismas. De la misma manera, no evidencia la existencia de un procedimiento y lineamientos que contemplen las pruebas de restauración periódica, con el fin de verificar la calidad y disponibilidad de la Información almacenada en ellos.

Cabe que mencionar, que el Proceso de copias de respaldo se ejecuta con la frecuencia que establece las buenas prácticas, adicionalmente dentro de la política de seguridad de la Información existe un apartado de lineamiento de copias de respaldo, pero hace mención en términos generales.

El Proceso de Gestión de tecnología de la Información, requiere fortalecer con lo definido en los siguientes marcos de referencias que soportan el Manual de Gobierno Digital 2018:

- ✓ El marco de referencia de Arquitectura Empresarial para la Gestión de Tecnologías de la Información del Estado colombiano que indica en el lineamiento LI.ST.13 Respaldo y recuperación de los Servicios tecnológicos : *La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe contar con mecanismos de respaldo para los servicios tecnológicos críticos de la entidad así como con un Proceso periódico de respaldo de la configuración y de la Información almacenada en la infraestructura tecnológica, incluyendo la Información clave de las estaciones de trabajo de los funcionarios de la entidad. . Este Proceso debe ser probado periódicamente y debe permitir la recuperación íntegra de los Servicios Tecnológicos*.

- ✓ El Marco de referencia ISO 27001_2013 según lo indica el control A.12.3.1 Respaldo de Información, se deben hacer copias de respaldo de Información, software, imágenes de los sistemas y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas

Recomendación Oportunidad de Mejora No. 3.

- ✓ Evaluar la posibilidad, de establecer y formalizar el procedimiento de realización y recuperación de copias de respaldo, incluyendo aspectos tales como:

  - ❖ Tipos de copias de respaldo realizados
  - ❖ Frecuencia de ejecución de copias de respaldo y pruebas de restauración
  - ❖ Medios de almacenamiento
  - ❖ Actividades de realización y restauración de copias de respaldo
  - ❖ Responsables.

- ✓ Evaluar la viabilidad de realizar restauraciones periódicas a la Información de las copias de respaldo para garantizar la disponibilidad y calidad de la Información, asegurándose igualmente la trazabilidad y documentación de dichas pruebas de restauración.

6.4 Desarrollo y Adquisición de Software Aplicativo

6.4.1 Fortalezas componente de Desarrollo y Adquisición de Software Aplicativo:

- ✓ El Proceso ha adelantado la elaboración del procedimiento "IDPAC-GTI-PR-21- Desarrollo-y-Mantenimiento-de-Software" y los siguientes formatos como avance de la documentación del dominio 14 del MSPI.

6.4.2 Aspectos susceptibles de mejora al componente de Desarrollo y Adquisición de Software Aplicativo:

6.4.2.1 Adquisiciones Tecnológicas

Acorde con las sesiones de trabajo realizadas con los responsables del Proceso de Gestión de Tecnología de la Información y a la revisión de la documentación divulgada en el Sistema Integrado de Gestión – herramienta SIG-Participo, se pudo evidenciar que el Proceso no cuenta en la actualidad con un procedimiento formal de adquisiciones tecnológicas que incluya un formato de evaluación de criterios de viabilidad relacionados con: estandarización, evolución, capacidad de integración, mantenimiento, desempeño, apropiación del conocimiento, riesgo tecnológico, seguridad de la Información y sostenibilidad futura.
Es importante enmarcar, 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 mitiguen el riesgo de desequilibrio costo/beneficio.

Si bien se menciona por parte de los responsables del Proceso que la Política de Adquisición de Elementos Tecnológicos como un instrumento en elaboración, para el mes de octubre de 2021 dicho plan no se ha formalizado, aprobado ni divulgado.

Riesgo asociado

El no contar con asesoría por parte del Proceso de Gestión de Tecnología en adquisiciones tecnologías hacia otras áreas de la entidad, podría generar un desequilibrio costo/beneficio frente la adquisición tecnológica llevando a no generar valor estratégico para la entidad.
La ausencia de controles adecuados para la evaluación de adquisiciones tecnológicas podría exponer a la entidad en aspectos legales inciertos si se filtran datos confidenciales (es decir, recursos humanos) o también si se presentan incidentes, interrupciones, obsolescencia y reProcesos.

Observación No. 8
El Proceso de Gestión de tecnología de la Información, incumple con lo definido en el siguiente marco de referencias que soportan la política y Manual de Gobierno Digital 2018:

- ✓ El marco de referencia de Arquitectura Empresarial para la Gestión de Tecnologías de la Información del Estado colombiano que especifica en los siguientes lineamentos:

  - ❖ LI.GO.07 Criterios de adopción y de compra de TI *-La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir los criterios y metodologías que direccionen la toma de decisiones de inversión en Tecnologías de la Información (TI), buscando el beneficio económico y de servicio de la institución.*

- LI.GO.08 Retorno de la inversión de TI - La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe establecer la relación costo-beneficio y justificar la inversión de los proyectos de TI mediante casos de negocio e indicadores financieros

- LI.GO.09 Liderazgo de proyectos de TI - La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe liderar la planeación, ejecución y seguimiento a los proyectos de TI. En aquellos casos en que los proyectos estratégicos de la institución incluyan componentes de TI y sean liderados por otras áreas, la dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, deberá supervisar el trabajo sobre el componente de TI conforme con los lineamientos de la Arquitectura Empresarial de la institución.

Recomendación No. 8

- ✓ Evaluar la posibilidad definir mecanismos para la racionalización de recursos invertidos en proyectos de tecnología, para garantizar su pleno uso, respaldos, garantías y mantenimientos durante su periodo de operación.

- ✓ Evaluar la posibilidad de establecer mecanismos de control de seguimiento a los Procesos de adquisición y desarrollo de tecnología para el ejercicio de Gobierno de TI, que permita avanzar en la maduración de proyectos tecnológicos para hacerlos más eficientes y eficaces.

- ✓ Evaluar la posibilidad de involucrar todas las subdirecciones, oficinas, áreas y Procesos que involucren en el ejercicio de sus competencias la compra de tecnología, proyectos de desarrollo tecnológico, innovación o desarrollo de aplicativos de software.

6.5 Administración de datos y seguridad lógica

6.5.1 Fortalezas componente de Administración de Datos y Seguridad Lógica:

- ✓ El IDPAC cuenta con elementos de protección de red tales como firewalls "Check Point" que brinda protección perimetral y el antivirus "Kaspersky Security Center", que provee protección a los equipos de usuarios y servidores.

- ✓ El firewall se encuentra correctamente configurado para detectar y bloquear las amenazas externas y para controlar el ancho de banda.

- ✓ Se tienen definidas y configuradas correctamente las interfaces, objetos y rutas de red, también están configuradas reglas, control de aplicaciones y filtros de contenido de Internet filtros y controles de navegación por grupos de usuarios con o sin permisos, la siguiente imagen evidencia el control de accesos y servicios de red permitidos y bloqueados correspondientes al mes de octubre de 2021.

- ✓ El IDPAC cuenta con un controlador de dominio Windows en el cual está configurado el directorio activo y se tienen creadas correctamente unidades organizativas por cada área funcional.

- ✓ Se tienen bien configuradas las políticas de auditoria para el acceso a objetos, cambio de políticas y de privilegios de auditoría.

- ✓ El antivirus está debidamente configurado en los PC´s para evitar su desactivación sin ingreso de contraseña de administrador o la suministrada por el Proceso de Gestión de TI.

- ✓ El sistema no permite la instalación de aplicativos sin la contraseña de usuario administrador al igual que detener los servicios o cambiar la configuración de políticas del equipo.

6.5.2 Aspectos susceptibles de mejora al componente de Administración de Datos y Seguridad Lógica:

6.5.2.1 Procedimiento Gestión de acceso a la VPN (Virtual Private Network)

Acorde con las sesiones de trabajo realizadas con los responsables del Proceso de Gestión de Tecnología de la Información y a la revisión de la documentación divulgada Sistema Integrado de Gestión – SIG Participo, se pudo establecer que en la actualidad no se cuenta con un procedimiento o política de gestión de acceso a VPN o Teletrabajo, aprobada y divulgada que definida los controles el acceso para los usuarios que requieran acceder a los servicios y recursos de la red de datos institucional.

Sin embargo, es relevante mencionar que actualmente el Proceso de Gestión de Tecnología de la Información, gestiona un Proceso interno no formalizado (no se encuentra documentado en el Sistema Integrado de Gestión) para los accesos a VPN a los funcionarios de la entidad acorde a las disposiciones de contingencia por la brindadas por la Alcaldía de Bogotá y la Dirección del IDPAC con motivo de la Pandemia COVID-19.

Riesgo Asociado

Estar a expuesto a vulnerabilidades de red o acceso no autorizados de usuarios, comprometiendo la seguridad de la Información al no tener unos lineamientos, hoja de ruta o controles que permitan asegurar el entorno y recursos tecnológicos sobre las conexiones externas a partir de malas prácticas

Observación No. 9

El Proceso de Gestión de tecnología de la Información, no se encuentra totalmente alineado con lo definido en los siguientes marcos de referencias que soportan el Manual de Gobierno Digital 2018:

- ✓ El Marco de referencia ISO 27001_2013 según lo indica el control A.6.2.2 Teletrabajo, Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la Información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.

Recomendación No. 9

- ✓ Ver la viabilidad de diseñar, formalizar y divulgar una política o procedimiento de gestión de acceso a la VPN o en su debido caso actualizar el Proceso de Gestión de Accesos, que permita garantizar la Información cuando se acceda remotamente a los recursos de la entidad, tanto por personal interno como externo, definiendo las condiciones y restricciones, procedimientos y mecanismos operativos necesarios para permitir el acceso remoto con seguridad. Se sugiere que esta política tenga en cuenta y defina aspectos como:

  - ❖ Herramientas de comunicaciones seguras para el acceso remoto
  - ❖ Concientización de los teletrabajadores sobre la necesidad y proteger sus contraseñas de acceso
  - ❖ Compromiso de los empleados de no realizar actividades ilícitas
  - ❖ Cada conexión debe ser registrada para asegurar la trazabilidad en caso de un incidente
  - ❖ Lista de servicios, redes, sistemas de Información que pueden ser accedido remotamente por personal que realiza acceso remoto o teletrabajo
  - ❖ Inventario de acceso remotos que se han otorgado identificando la persona que tiene dicho acceso y motivo por el cual se otorgó.

6.5.2.2 Gestión de acceso a la VPN (Virtual Private Network)

Oportunidad de Mejora No. 4

Con el objetivo de validar el control de acceso que tiene implementado al Proceso para los accesos a VPN, se seleccionó una muestra de cinco (5) casos de usuarios activos que ingresaron en el 2021, evidenciándose que para un (1) usuario, no se cuenta con la evidencia y soportes de solicitud, autorización y justificación de la asignación del acceso. Para los cuatro (4) usuarios restantes fue suministrado los respectivos soportes que asegura la debida trazabilidad definida en el control que se diseñó de manera interna por parte del Proceso de Gestión de Tecnología de la Información.

Tabla 1 Usuario que no cuenta con soportes de solicitud y autorización para acceso a la VPN

Nombre Completo	Usuario	Tipo de Vinculación	Dependencia	Fecha de ingreso al IDPAC	Usuario responsable de la creación
Eduardo Gomez Polo	Egomez	Planta	Secretaría General - Sistemas	19/05/2021	Soporte

Fuente: Oficina de Control Interno

El hecho de no tener una adecuada gestión de accesos a la VPN a usuarios podría generar accesos no autorizados a Información y recursos tecnológicos del IDPAC impactando la integridad, confidencialidad y disponibilidad de la Información.

Oportunidad de Mejora No. 4

Establecer medidas de control para los accesos a la VPN, complementados estos con acciones orientadas a:

- ✓ La necesidad de contar con una solicitud y aprobación de manera explícita, bien sea física o digital. La aprobación debe ser brindada por una persona con el suficiente grado de autoridad sobre el Proceso.

- ✓ Esta evidencia debe almacenarse en un sitio centralizado con el fin de poder acceder a ella cuando sea necesario.

- ✓ Capacitar y socializar este procedimiento sobre el personal designado para ello identificando un responsable principal y respaldo.

- ✓ Revisar y asegurar que todos los usuarios que tengan activo el acceso a VPN ya sean que sigan laborando o se han vinculado de la entidad se encuentren acorde a los lineamientos definidas por la dirección, talento humano y del Proceso Gestión de Tecnología de la Información, de lo contrario proceder a deshabilitar este permiso de acceso.

6.5.2.3 Concientización y sensibilización

Oportunidad de Mejora No. 5

Acorde a las sesiones de trabajo y entendimiento realizadas con los responsables del Proceso de Gestión de Tecnologías de la Información y a la revisión de la documentación divulgada en el Sistema Integrado de Gestión – herramienta SIG-Participo, se logró identificar, que en la actualidad aunque se han desarrollado actividades orientadas a la concientización enfocada a los usuarios finales sobre actividades de teletrabajo o en su defecto a las buenas prácticas de seguridad de la Información, no se tiene definida e implementada de manera formal una estrategia o campaña.

.

Recomendación Oportunidad de Mejora No. 5

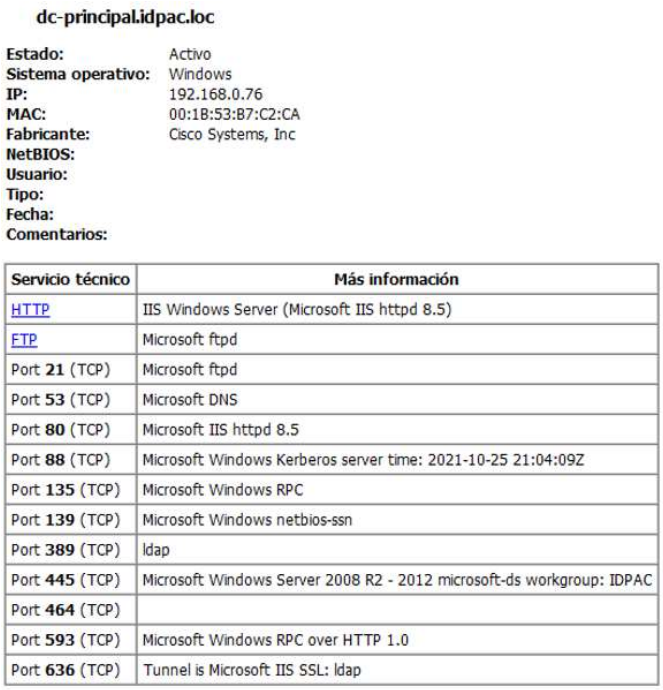
Implementar un programa de comunicación y sensibilización de seguridad de la Información de manera formal y transversal con las áreas interesadas para los usuarios finales, con el fin de incentivar las buenas prácticas para el buen uso de la Información, acceso remoto, actividades de teletrabajo, uso de los recursos tecnológicos, entro otros, a partir de estrategias como Tics de tecnología vía mail, protector de pantalla, fondos de pantalla, concursos, medios audiovisuales., etc. , e incluirlas en el plan de capacitación institucional.

6.5.2.4 Configuración Puertos de Red

Oportunidad de Mejora No. 6

Acorde a un análisis de vulnerabilidad realizado desde herramienta de escáner de red por el auditor a la red de IDPAC se logró evidenciar que el servidor del Controlador de Dominio Windows tiene habilitado once (11) puertos de red y acorde a las vulnerabilidades identificadas en las industria y buenas prácticas, cuatro (4) de estos puertos son recurrentes para realizar ataques por parte de las ciberdelincuentes y no sé tiene controlado desde los recursos de seguridad del Proceso.

Ilustración 4 Puertos de red abiertos en el Servidor del Controlador de Dominio Windows



dc-principal.idpac.loc

Estado: Activo
Sistema operativo: Windows
IP: 192.168.0.76
MAC: 00:1B:53:B7:C2:CA
Fabricante: Cisco Systems, Inc
NetBIOS:
Usuario:
Tipo:
Fecha:
Comentarios:

Servicio técnico	Más información
HTTP	IIS Windows Server (Microsoft IIS httpd 8.5)
FTP	Microsoft ftpd
Port **21** (TCP)	Microsoft ftpd
Port **53** (TCP)	Microsoft DNS
Port **80** (TCP)	Microsoft IIS httpd 8.5
Port **88** (TCP)	Microsoft Windows Kerberos server time: 2021-10-25 21:04:09Z
Port **135** (TCP)	Microsoft Windows RPC
Port **139** (TCP)	Microsoft Windows netbios-ssn
Port **389** (TCP)	ldap
Port **445** (TCP)	Microsoft Windows Server 2008 R2 - 2012 microsoft-ds workgroup: IDPAC
Port **464** (TCP)	
Port **593** (TCP)	Microsoft Windows RPC over HTTP 1.0
Port **636** (TCP)	Tunnel is Microsoft IIS SSL: ldap

Fuente: Evidencia Oficina de Control Interno desde la herramienta Advanced Port Scanner

Tabla 2 Detalle de puertos abiertos vulnerables

Puerto	Función	Descripción de las vulnerabilidades
21	FTP es un protocolo de Internet que permite a las computadoras dentro de la red intercambiar archivos de forma masiva	Un puerto FTP inseguro que aloja un servidor FTP es una gran falla de seguridad. Muchos servidores FTP tienen vulnerabilidades que pueden permitir la autenticación anónima, el movimiento lateral dentro de la red, el acceso a técnicas de escalada de privilegios y,

Puerto	Función	Descripción de las vulnerabilidades
		debido a que muchos servidores FTP pueden controlarse mediante scripts, un medio para implementar scripts entre sitios. Los programas de malware como Dark FTP, Ramen y WinCrash han hecho uso de puertos y servicios FTP inseguros.
80	Este puerto es el que se usa para la navegación web de forma no segura HTTP.	Es vulnerable a un ataque de denegación de servicio (DoS) al enviar spam de encabezados HTTP incompletos, bloqueando efectivamente el acceso al dashboard. La vulnerabilidad afectaría a últimas versiones de Apache HTTP Server y ha sido catalogada con una severidad Alta
139	Los puertos NetBIOS son utilizados por el intercambio de archivos y aplicaciones de uso compartido de impresoras	Los ciberdelincuentes conocen este camino y con regularidad tratan de entrar en un servidor de archivos a través de este puerto. para llevar a cabo, denegación de Servicio (DoS), ataque de Fuerza Bruta, Punto de Acceso
445	Protocolo de red de capa de aplicación que se utiliza principalmente para compartir archivos, compartir impresoras y compartir puertos serie.	Las buenas prácticas de ciberseguridad hacen mención de que el puerto 445 tiene fallas graves y, por lo tanto, es vulnerable a ataques de ciberdelincuentes. El software malintencionado también puede infiltrarse en él, por lo que normalmente se recomienda desactivarlo. Sin embargo, también evitará que comparta archivos e impresoras, por lo que es posible que deba permitir que el puerto del firewall interno utilice dichos servicios para compartir.

Fuente: Evidencia Oficina de Control Interno

Recomendación Oportunidad de Mejora No. 6

- ✓ Evaluar la viabilidad técnica de cerrar o blindar los puertos de red mencionados, teniendo en cuenta que estos puertos son recurrentes para realizar ataques de los ciberdelincuentes.

- ✓ Evaluar la posibilidad de establecer las revisiones constantes de los recursos y los mecanismos de seguridad para poder minimizar los riesgos y vulnerabilidades encontradas, realizar pruebas de penetración en la red (Penetration Testing), con ello se evaluarán nuevos riesgos y la opción de tomar medidas de contrarresten posibles fallas en los sistemas de seguridad.

- ✓ Velar por el cumplimento de políticas de seguridad, realizando revisiones constantes a los equipos activos que presenten el servicio de conectividad inalámbrica (Switch capa 2 y 3, puntos de acceso) Revisar los constantes parches de seguridad de los servidores que presten servicios de DHCP y DNS, para mitigar ataques de fuerza bruta o consulta de cache.

- ✓ Evaluar la viabilidad técnica de aplicar el filtrado para mantener esta Información fuera de la red y eliminar cualquier opción que no esté en uso.

6.5.2.5 Seguridad de páginas Web de la entidad

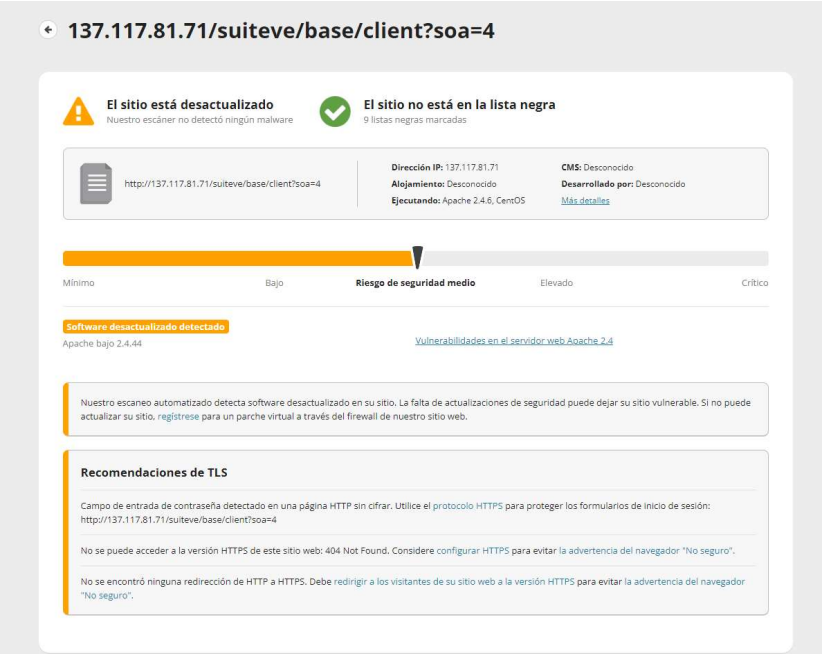
Cómo parte de a un análisis básico de vulnerabilidades realizado el 14 de octubre de 2021 a través de herramienta de escaneo de seguridad Web sobre algunos de los sitios web de IDPAC a, se lograron identificar las siguientes debilidades:

SIG PARTICIPO – http:/137.117.81.71/suiteve

El sitio se encuentra en riesgo medio de seguridad, debido principalmente a que el servidor se encuentra desactualizado, y puede ser aprovechada alguna de las vulnerabilidades conocidas de esta versión y a su vez el certificado de seguridad no es válido.

A continuación, se presenta el resumen del análisis:

Ilustración 5 Análisis de seguridad sobre el sitio Web SIG PARTICIPO

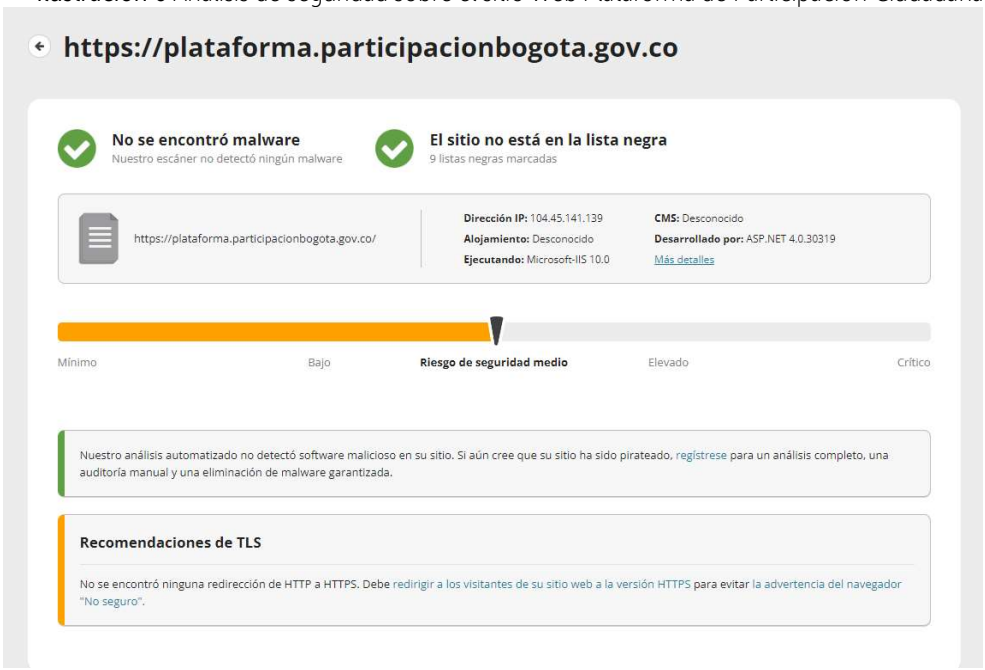


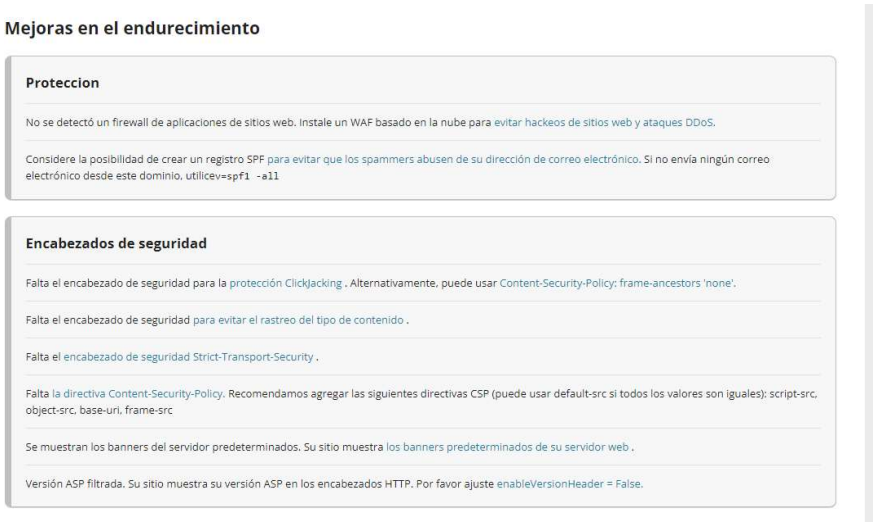
Fuente: Evidencia Oficina de Control Interno desde la página Sucuri Site Check

Plataforma de Participación Ciudadana: https://plataforma.participacionbogota.gov.co/

El sitio se encuentra en riesgo medio de seguridad debido principalmente a que el certificado de seguridad no es válido.

Ilustración 6 Análisis de seguridad sobre el sitio Web Plataforma de Participación Ciudadana





Fuente: Evidencia Oficina de Control Interno desde la página Sucuri Site Check

Riesgo asociado

La ausencia de un certificado SSL, permite a los ciberdelincuentes pueden acceder a toda la Información confidencial de un sitio web. Esto puede provocar la filtración de datos personales o confidenciales de la entidad. En la actualidad, los ciberdelincuentes pueden reconocer fácilmente los sitios vulnerables y causar interrupciones que pueden ser catastróficas para la operación.

Observación No. 10

El Proceso de Gestión de tecnología de la Información, incumple con lo definido en la resolución MinTIC 1519 de 2020, Anexo 3 Condiciones mínimas técnicas y de seguridad digital, apartado 3.2 Condiciones de Seguridad Digital, donde las entidades deberán implementar controles en el desarrollo de sitios web y aplicaciones como:

- ✓ *Ejecutar monitoreos de seguridad sobre las páginas web que contemple, entre otras, las siguientes acciones: escaneo de archivos infectados, escaneo de vulnerabilidades, análisis de patrones para detectar acciones sospechosas, verificación contra listas negras, monitoreo del tráfico para detectar ataques de denegación de servicios.*

- ✓ *Garantizar conexiones seguras a través de uso de certificados, SSL (HTTPS para la confianza de usuarios) y cifrado en la estructura de las peticiones para portales transaccionales, para evitar la manipulación de parámetros en las peticiones. (adicional al cifrado SSL), También deben habilitar las cabeceras de seguridad, entre otras las siguientes: Content-Security-Policy (CSP), X-Content-Type-Options, X-Frame-Options, X-XSS-Protection, StrictTransport-Security (HSTS), Public-Key-Pins (HPKP) Referrer-Policy, FeaturePolicy.*

Recomendación No. 10

- ✓ Atender las vulnerabilidades encontradas de los portales SIG Participo y la Plataforma de Participación Ciudadana de manera inmediata, así mismo aplicar las Condiciones mínimas técnicas y de seguridad digital del Anexo 3 de la resolución MinTIC 1519 de 2020.

- ✓ Establecer las revisiones constantes a TODOS los sitios web de la entidad para poder minimizar los riesgos y vulnerabilidades encontradas, con ello se evaluarán nuevos riesgos y la opción de tomar medidas de contrarresten posibles fallas en los recursos tecnológicos de la entidad.

6.5.2.6 Estándar de parámetros contraseña para los sistemas de Información

Acorde a las sesiones de trabajo realizadas a nivel de entendimiento con los responsables del Proceso de Gestión de Tecnología de la Información y al revisar la documentación divulgada en el Sistema Integrado de Gestión "SIG-Participo", se evidencia que no existe un estándar de configuración de contraseñas que permita definir dicha configuración a los sistemas de Información del IDPAC.

Cabe mencionar que, aunque se tiene una política de seguridad de la Información, este documento solo hace mención en términos generales la importancia de una contraseña segura y los controles de acceso, más no indica en detalle o el estándar de contraseña definido por el Proceso de Gestión de Tecnología de la Información.

Riesgo asociado

Esta situación aumenta la probabilidad de incumplir normas básicas sobre administración de sistemas, que podrían comprometer la integridad, confidencialidad o disponibilidad de la Información y acceso no autorizado a la Información, entre otras.

Observación No. 11

El Proceso de Gestión de Tecnología de la Información, no se encuentra totalmente alineado con la Guía No 2 de la elaboración de la Política de Seguridad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones, donde indica que la sección 9.3 de Gestión de acceso. Sección 3 **Gestión de Contraseñas,** establece que: *la política debe definir los lineamientos mínimos en cuanto a calidad que deben tener las contraseñas para ser utilizadas como mecanismo de autenticación en los accesos a la red, aplicaciones y/o sistemas de Información de la entidad, así mismo debe indicar a los funcionarios, contratistas y/o terceros los parámetros mínimos para que una contraseña sea considera como fuerte, gestión de cambio de contraseña, debe determinar que los accesos a la red, las aplicaciones y sistemas de Información deben requerir un usuario (ID) y una contraseña fuerte para que realice la correspondiente autenticación y acceso a la Información de forma segura.*

Recomendación No. 11

Desarrollar las acciones necesarias con el fin de definir un estándar de contraseñas dentro la política de seguridad de la Información, que aplique de manera transversal a los sistemas de Información y se contemple los siguientes parámetros acorde a las mejores prácticas de seguridad de contraseñas:

- Longitud mínima y máxima de caracteres de la contraseña
- Nivel de complejidad de la contraseña
- Tiempo de vigencia de la contraseña
- Intentos fallidos antes de que bloquee la contraseña
- Historial de contraseña

6.5.2.7 Parámetros de contraseña al Controlador de Dominio Windows

Oportunidad de Mejora No. 7

Acorde a la prueba de seguridad realizada el 22 de octubre de 2021, con el administrador del Controlador de Dominio (herramienta que permite gestionar y controlar el acceso a la sesión de usuario de los equipos de cómputo y correo electrónico) sobre la evaluación las políticas de contraseñas se identificaron lo siguiente:

✓ De ocho (8) parámetros de contraseñas evaluados al Controlador de Dominio Windows, uno (1) no se encuentra alineado a las mejores prácticas de la industria y seguridad de la Información, los siete (7) parámetros restantes se encuentran configurados correctamente.

Tabla 3 Parámetros de contraseña del controlador de Dominio no alineadas a las buenas prácticas

Parámetro	Descripción	Valor configurado	Estándar definido IDPAC	Valor Buenas Prácticas
PasswordHistorySize	El número de contraseñas que se requieren antes de volver a utilizar una contraseña	2 contraseñas	N/A	24 contraseñas

Fuente: Oficina de Control Interno

Una inadecuada configuración en la reutilización de contraseñas es una preocupación importante en cualquier organización. Muchos usuarios desean reutilizar la misma contraseña para su cuenta durante un período de tiempo prolongado. Cuanto más tiempo se use la misma contraseña para una cuenta en particular, mayor será la posibilidad de que un atacante pueda determinar la contraseña a través de ataques de fuerza bruta.

Y acorde a las mejores prácticas brindadas por Microsoft para la configuración de un controlador de dominio, define lo siguiente:

- ✓ PasswordHistorySize: *Especificar un número bajo para hacer cumplir el historial de contraseñas permite a los usuarios continuamente la misma cantidad pequeña de contraseñas repetidamente, por lo cual establezca exigir historial de contraseñas en 24. Esto ayudará a mitigar las vulnerabilidades causadas por la reutilización de contraseñas.*

Recomendación Oportunidad de Mejora No. 7

Evaluar la posibilidad de configurar los parámetros de contraseña acorde con las mejores prácticas de Microsoft. En caso de ser necesario, y de manera particular actualizar la política de seguridad de la Información o el estándar de contraseña con los parámetros de contraseñas definidos para cada sistema de Información.

6.5.2.8 Usuarios con altos privilegios en el Controlador de Dominio Windows

Acorde a la prueba de seguridad realizada el 22 de octubre con el administrador del controlador de dominio (*herramienta que permite gestionar y controlar el acceso a la sesión de usuario de los equipos de cómputo y correo electrónico*) sobre las cuentas de usuario con altos privilegios se puedo evidenciar que se tienen definidos seis (6) usuarios al grupo de administradores, de los cuales en validación con el responsable de dicha herramienta tecnológica, hace mención que solo un (1) usuario llamado "Adminidpac" no requiere tener dicho privilegio.

Así mismo se evidencia que el usuario llamado "Administrador" no ha sido renombrado y por su parte identifica que no se ha realizado cambio de contraseña para este super usuario hace más de siete (7) meses, dado que tiene una configuración para realizar el cambio de contraseña de manera manual

Tabla 4 Estado de usuarios Administrador Controlador de Domino

Usuario	¿Renombrado?	¿Último cambio de contraseña?
Administrador	No	11/03/2021

Fuente: Oficina de Control Interno

Riesgo asociado

Una inadecuada configuración del usuario administrador aumenta la probabilidad de que si un atacante conoce el nombre del usuario administrador aumenta sus chances de hacer efectivo un ataque, así mismo el no realizar un cambio periódico de contraseña a un usuario con altos privilegios aumenta la probabilidad de accesos no autorizados a la plataforma tecnológica debido a que esta contraseña puede ser identificada o compartida con el paso del tiempo, impactando la integridad, disponibilidad y la confidencialidad de la Información que almacena el servidor.

Observación No. 12

El Proceso de Gestión de Tecnología de la Información a nivel de los usuarios con privilegios no se encuentra alineado a las consideraciones de las mejores prácticas brindadas por Microsoft para la configuración de un controlador de dominio, donde define lo siguiente:

- ✓ *La cuenta de administrador existe en todas las versiones de Windows. Por lo cual, si cambia el nombre de esta cuenta, es un poco más difícil para las personas no autorizadas adivinar esta combinación de nombre de usuario y contraseña con privilegios, así mismo asegúrese de restringir su uso y de cambiar la contraseña con regularidad.*

Así mismo el Proceso de Gestión de Tecnología de la Información, incumple con lo definido en marco de referencias que soportan el Manual de Gobierno Digital 2018:

- ✓ El Marco de referencia ISO 27001_2013 según lo indica el control A.9.2.5 Revisión de los derechos de acceso de usuarios, donde estable que *los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares*

Recomendación No. 12

- ✓ Evaluar la posibilidad de renombrar la cuenta de administrador bajo un nombre no asociado al termino "Administrador".

- ✓ Evaluar la viabilidad técnica de aplicar al usuario anteriormente mencionado el parámetro para la expiración de contraseñas (PswdExpires=Yes), con el fin de que dichos usuarios cumplan con la política de expiración definida. En caso tal de no ser posible una configuración adecuada del parámetro, evaluar la posibilidad de realizar un cambio periódico manual de contraseña, máximo de 6 meses sobre la cuenta de usuario identificada.

- ✓ Evaluar la posibilidad técnica de retirar los privilegios de administrador al usuario **Adminidpac** en caso que no se requiere que tenga dichos privilegios.

6.5.2.9 Seguridad base de datos SQL que soporta el sistema de Información SIG Participo

Oportunidad de Mejora No. 8

Acorde a la revisión de seguridad realizada a la base de datos SQL que soporta el sistema de Información SIG Participo, se identificaron las siguientes oportunidades de mejora:

- La versión actual de la base SQL que soporta SIG Participo, no corresponde a la última versión o Service Pack ofrecida por el proveedor Microsoft.

Tabla 5 Estado de la versión de la base datos SQL - SIG Participo

Versión actual	Última Versión	Fin de Soporte del proveedor
Microsoft SQL Server Server 2012 (11.0.2100.60)	Microsoft SQL Server 2012 (11.0.7001.0 SP4)	Hasta 12 de julio de 2022

Fuente: Evidencia Oficina de Control Interno

Sin embargo, es importante mencionar que la base de datos del sistema SIGPARTIPO cuenta con soporte por parte del proveedor en el caso que se requiera actualizar o presente fallas.

- Se evidencia que el usuario SA el cual es creado por defecto por la base de datos en su instalación y que cuenta con los mayores privilegios, se encuentra activo y no tiene definida una contraseña

  Nota: *Cabe mencionar que la administración del sistema de Información "SIG Participo" es gestionada por un tercero llamado Pensemos y el responsable del contrato es la Oficina Asesora de Planeación. Sin embargo, al ser un recurso tecnológico que gestiona Información crítica y confidencial de la entidad, es fundamental por parte de los expertos de la entidad, en este caso el Proceso de Gestión de Tecnología de la Información, salvaguardar o brindar el entorno tecnológico del sistema de Información mencionado.*

El hecho de no tener actualizada la base de datos SQL, existe la probabilidad de que sean explotadas vulnerabilidades de seguridad de la base de datos, las cuales podrían llegar a tener un fuerte impacto en la confidencialidad, disponibilidad e integridad de la Información de la compañía,

Así mismo una inadecuada gestión del usuario privilegiado SA, en las bases de datos incrementa la probabilidad de accesos no autorizados a los datos críticos de la entidad causando posible pérdida de integridad, disponibilidad y confidencialidad de la Información.

Por eso acorde a las mejores prácticas brindadas por Microsoft para la seguridad la base de datos SQL Server en relación a los usuarios por defecto y versión hace relación a lo siguiente:

- ✓ *La cuenta SA es una cuenta de SQL Server muy conocida y, a menudo, está dirigida por usuarios malintencionados. No habilite la cuenta SA a menos que su aplicación lo requiera. Es importante que utilice una contraseña segura para iniciar sesión en SA.*

- ✓ *Microsoft recomienda una instalación proactiva y continua de las actualizaciones acumulativas de Service Pack de las bases de datos SQL Server 2012 a medida que estén disponibles dado que contienen valor añadido respecto a las revisiones. Esto incluye actualizaciones de compatibilidad, manejabilidad y confiabilidad.*

Recomendación Oportunidad de Mejora No. 8

- ✓ Evaluar la posibilidad de actualizar la versión la base de datos Microsoft SQL Server 2012 R2, a una versión más reciente, la cual permita aprovechar el soporte vigente por parte del proveedor. Adicionalmente, se recomienda realizar una revisión periódica sobre las notificaciones emitidas por el proveedor, con el fin de tomar acciones de manera oportuna.

- ✓ Evaluar la viabilidad técnica de deshabilitar el usuario SA, o en caso no ser posible evaluar la posibilidad de definir una contraseña de inicio para el usuario en mención definiendo un control periódico de cambios de contraseña debido al riesgo que representan y conforme a lo que recomiendan las buenas prácticas.

7. CONCLUSIONES

Una vez auditado el Proceso de Gestión de Tecnología de la Información, a partir de la evaluación de los controles generales y la verificación sobre la implementación de las buenas prácticas de gestión TIC, se concluye que el Proceso, cumple con los objetivos de apoyo a la entidad y se han fortalecidos los controles de seguridad perimetral, software, acceso de la infraestructura tecnológica y gestión a nivel de gobierno TI.

No obstante lo anterior, se identifican aspectos susceptibles de mejora evidenciando una ejecución parcial sobre los componentes evaluados en esta auditoría, identificando observaciones y oportunidades de mejora de cumplimiento en aspectos tales como: creación de la Dirección u Oficina de Tecnología de la Información y las Comunicaciones, gestión de indicadores, actualización de documentación, estandarización de actividades, controles ambientales sobre el centro de cómputo principal del IDPAC, campañas de concientización, adquisición tecnológica, seguridad lógica sobre la infraestructura tecnológicas y páginas Web .Adicionalmente en la práctica el Proceso realiza diversas actividades que permiten controlar o asegurar riesgo identificados, pero no siempre se generan los registros de trazabilidad.

Finalmente, cabe resaltar la disposición por parte de los funcionarios y contratistas del Proceso de Gestión de Tecnología de la Información para atender las solicitudes realizadas por la Oficina de Control Interno, así como su conocimiento sobre los aspectos evaluados. En el cuerpo del presente informe se encuentran detallados los análisis realizados, y se consignan las observaciones y recomendaciones documentadas en procura de la mejora continua de la gestión institucional.

8. DIFICULTADES DURANTE LA AUDITORÍA

No se presentaron dificultades durante la ejecución del trabajo de auditoría.

Aprobado: 24/11/2021

Elaboró y verificó

Andrés Rojas Prada

Andrés Rojas Prada
Contratista Oficina Control Interno

Revisó y aprobó:

Pablo Salguero Lizarazo
Jefe de la Oficina de Control Interno