INFORME FINAL
AUDITORÍA DE VERIFICACIÓN AL CUMPLIMIENTO Y MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN EL SGC

Fecha del Informe: 2024-12-30
Nombre Auditor: Andrés Mauricio Cruz Vargas
No. Informe: OCI-35-2024

1. OBJETIVO Y ALCANCE.

Evaluar el nivel de cumplimiento, implementación y madurez del Modelo de Seguridad y Privacidad de la Información del SGC, con el fin de identificar las fortalezas, debilidades y áreas de mejora.

Como alcance comprenderá, la revisión de la documentación que hace parte del Sistema Gestión de Calidad ISOLUCION del SGC, normatividad interna y externa pertinente, orientadas a la planificación, implementación, seguimiento, evaluación y mejora continua del Modelo de Seguridad y Privacidad de la Información del SGC desde el periodo de 2023 a la fecha.

2. CRITERIOS DE AUDITORÍA / SEGUIMIENTO.

- Decreto 1008 de 2018 “Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".
- Resolución 500 de 2021 "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital".
- Resolución 1519 de 2020, “Por la cual 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”.
- Ley 1581 de 2012, “Establece las disposiciones generales para la protección de datos personales”.
- Ley 1474 de 2011 “Enfoca en la prevención, investigación y sanción de actos de corrupción”.
- CONPES 3995 de 2020 Política Nacional de confianza y seguridad Digital
- Norma ISO/IEC 27001:2013 - Norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información.
- Política General de Seguridad de la Información del SGC (DG-GGC-012)
- Manual de Normas y Políticas de Seguridad Informática (MO-TEC-001)
- Manual de Políticas Específicas de Gestión de Seguridad de la Información, Protección de Datos Personales (MO-GGCGSI-001)

- Procedimientos, manuales, guías, directrices, lineamientos, estándares, instructivos relacionados con seguridad de la información, el modelo de seguridad y privacidad de la información de MinTic y Gobierno en Línea.

Vale la pena mencionar que, concluida la elaboración del informe Preliminar, resultante del presente informe, el mismo fue emitido al Grupo de Trabajo Plataforma y Tecnologías de la Información y a la Dirección Técnica Gestión de Información, mediante radicado No. SGC-3-2024-007306 de fecha 20 de diciembre de 2024, con el fin de conocer los comentarios que consideraran respecto a su contenido. Frente a esa comunicación, el 27 de diciembre de 2024 se recibió radicado No. SGC-3-2024-007408 de la Dirección Técnica Gestión de Información, con la cual dieron a conocer los comentarios al Informe Preliminar, comentarios que fueron tenidos en cuenta para la elaboración del presente Informe Final, en lo que se consideró pertinente.

3. METODOLOGÍA

La Oficina de Control Interno mediante comunicación interna SGC-3-2024-005906 del 08 de noviembre del presente año, solicitud a la Dirección Técnica de Gestión de Información, la información siguiente:

- Resolución que indique quien es el líder, oficial y/o responsable de seguridad de la información, con funciones asignadas.
- Plan de continuidad del SGC.
- Plan de recuperación de desastres tecnológicos
- Indicadores y métricas de seguridad de la información definidos.
- Declaración de aplicabilidad – SoA
- Metodología y Planes de tratamientos de Riesgos
- Indicadores de gestión del MSPI definidos, revisados y aprobados por la alta Dirección.
- Modelo de Seguridad y Privacidad de la Información y Autodiagnóstico – MSPI del SGC.
- Documento con el resultado de la herramienta de la encuesta de diagnóstico de seguridad y privacidad de la información, revisado, aprobado y aceptado por la alta dirección
- Inventario de activos de información del SGC.

Esta solicitud fue respondida por medio de una carpeta en un drive, el día 18 de noviembre de 2024. Posterior a la revisión documental, esta Oficina realizó la programación con el profesional a cargo del seguimiento e implementación del MSPI.

4. ANALISIS

La revisión de las evidencias y documentación observada se llevó a cabo a través de una muestra selectiva de auditoría aplicada a registros y soportes, con el fin de evaluar el grado de avance en relación con los controles asociados a la implementación del Sistema

de Gestión de Seguridad de la Información en la entidad, basado en la norma ISO 27001:2013 y el MSPI del MINTIC.

En este sentido, se planteó la siguiente escala de evaluación para la interpretación de los resultados evidenciados por esta Oficina:

ESTADO	DESCRIPCIÓN
Cumple Satisfactoriamente	El control está completamente implementado, gestionado y cumple con los requisitos establecidos por la norma. Está debidamente documentado, es conocido por todos los involucrados y se aplica de manera efectiva dentro del SGSI.
Cumple parcialmente	El control se está cumpliendo de manera parcial, aunque no de acuerdo a lo solicitado por la norma. Se están realizando acciones similares, pero no exactamente como se requiere, puede que no esté documentado, o que no esté completamente gestionado, aunque haya una definición inicial.
No Cumple	El control no está implementado, no existe o no se está ejecutando conforme a lo establecido por la norma.
No Aplica	El control no es aplicable a la entidad. En el campo de evidencia, debe indicarse la justificación que explique por qué no se aplica.

A continuación, se presentan los resultados obtenidos, desglosados por dominio y control:

Dominio / Control	# ISO	Control	VALORACIÓN OCI
DOMINIO	**5**	**POLITICA DE LA SEGURIDAD DE LA INFORMACION**	
Control	5.1.1	Documento de la política de seguridad y privacidad de la Información	Cumple parcialmente
	5.1.2	Revisión de las políticas para la seguridad de la información	
La entidad dispone de una Política de Seguridad y Privacidad de la Información de fecha 2022, la cual ha sido publicada en la página web de la entidad y socializada internamente por medio del Sistema de Gestión ISOLUCION. **Observación No. 1 – Control 5.1.2:** Conforme con lo expuesto por esta Oficina, no se constató una revisión periódica a las políticas de seguridad de la información, conforme lo indica la norma "*Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas*". **Fortaleza No. 1:** Conforme la documentación evidenciada, esta Oficina resalta el compromiso por parte de la Dirección Técnica de Gestión de Información, en relación a la formalización de la Política de Seguridad y Privacidad de la Información de la entidad, mediante la emisión de una Resolución, ya que la política adquiere un carácter oficial y vinculante dentro de la entidad, lo que refuerza el compromiso de la alta dirección y los responsables de la seguridad de la información.			
DOMINIO	**6**	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION**	
Control	6.1.1	Roles y responsabilidades para la seguridad de la información	No cumple
	6.1.2	Separación de deberes / tareas	

Dominio / Control	# ISO	Control	VALORACIÓN OCI
	6.1.4	Contacto con grupos de interés especiales	Cumple satisfactoriamente
	6.1.5	Seguridad de la información en la gestión de proyectos	
	6.2.1	Política para dispositivos móviles	No Aplica
	6.2.2	Teletrabajo	Cumple satisfactoriamente

No Conformidad No. 1 – Control 6.1.1: Designación del rol Oficial de Seguridad de la Información
Conforme con la Matriz de Roles y Responsabilidades, actualmente el SGC no cuenta con un responsable formal de la seguridad de la información (OSI) conforme se establece en el ítem 6.5 "Cumplimiento de la política", la cual indica: "*La Alta Dirección garantizará que el personal del SGC, directamente relacionado con el establecimiento, implementación y mejora continua del Sistema Integrado de Gestión de Seguridad de la Información, cuente con las competencias, formación y capacitación necesarias para desempeñar las funciones y responsabilidades asignadas en dicho sistema, con el fin de asegurar el cumplimiento de sus objetivos*". Por otra parte, tampoco se cuenta con un Oficial de Protección de Datos Personales (OPDP).

Por otra parte:

- No contar con un (OSI) designado, la responsabilidad de asumir y gestionar los **riesgos relacionados con la seguridad de la información** recae en la Alta Dirección de la entidad. Esto está respaldado por los principios de la norma ISO/IEC 27001 y las mejores prácticas de gobernanza, que asignan la responsabilidad última del sistema de gestión a los niveles más altos de liderazgo.
- Conforme la norma ISO/IEC 27001, la alta dirección debe demostrar liderazgo y compromiso con la seguridad de la información. Esto incluye la asignación de **recursos, roles y responsabilidades**, así como la aceptación de los riesgos hasta que se designen responsables específicos.
- La Alta Dirección tienen la obligación de **proteger los activos de información**, cumplir con la normativa aplicable (como la Ley 1581 de 2012 en Colombia o el MSPI del MinTIC) y salvaguardar la reputación y continuidad del negocio.

Recomendación OCI No. 1 – Control 6.1.1: Se **recomienda** a la Alta Dirección de la entidad designar formalmente el rol del Oficial de Seguridad de la Información (OSI) con el fin de cumplir con lo establecido en el ítem 6.5 "Cumplimiento de la política", así como con los lineamientos de la norma ISO/IEC 27001 y el Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC y por otra parte, el rol de Oficial de Seguridad de la Información (OSI) debe ubicarse fuera de la Gerencia de Tecnología, con el propósito de garantizar su independencia y autonomía, lo que le permitirá cumplir de manera efectiva con la responsabilidad de alcanzar los objetivos establecidos en materia de seguridad de la información.

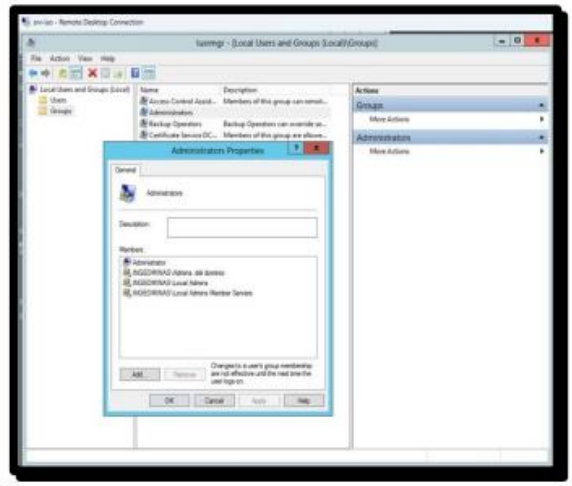
No Conformidad No. 2 – Control 6.1.2: Definición de Matriz de Roles y Perfiles
Actualmente el SGC, no cuenta con una Matriz de Roles y Perfiles que permita definir, gestionar y controlar los accesos de los usuarios a los sistemas de información. La ausencia de esta herramienta representa un riesgo significativo para la seguridad de la información, ya que no se garantiza la segregación de funciones, el principio de mínimo privilegio ni el acceso adecuado

Dominio / Control	# ISO	Control	VALORACIÓN OCI

según las responsabilidades asignadas.

> **Recomendación No. 2 – Control 6.1.2:** Esta Oficina **recomienda** diseñar e implementar una Matriz de Roles y Perfiles que permita gestionar los accesos a sistemas, datos y recursos, garantizando la seguridad de la información y el cumplimiento normativo. Por otra parte, evaluar periódicamente los roles y perfiles evitando que no se tengan conflictos con los privilegios otorgados.

La Dirección Técnica Gestión de Información indicó respecto a la **No Conformidad No. 2 – Control 6.1.2: Definición de Matriz de Roles y Perfiles,** lo siguiente: "*Durante la prueba de recorrido se evidenció que, aunque no se cuenta con una Matriz de Roles y Perfiles formalmente definida, el control se cumple parcialmente. Esto se debe a que los administradores no emplean sus usuarios normales para acceder a los servidores, sino que utilizan un perfil específico para cada servicio que administran*."



En consecuencia la Oficina de Control Interno indica que, aunque la Dirección Técnica de Gestión de Información mencionó que los administradores utilizan perfiles específicos para cada servicio, esto no elimina los riesgos asociados ni sustituye la necesidad de un mecanismo formal que:

- Documente y gestione claramente los accesos y privilegios.
- Asegure la trazabilidad y el principio de mínimo privilegio
- Garantice la segregación de funciones y el cumplimiento normativo.

Por lo anterior, la Oficina de Control Interno **MANTIENE** la No Conformidad, ya que la ausencia de una **Matriz de Roles y Perfiles** formalizada representa un riesgo significativo para la seguridad de la información y el cumplimiento de los estándares regulatorios. Si bien el uso de perfiles específicos por parte de los administradores constituye un avance parcial, este no sustituye la necesidad de un control formal y debidamente documentado.

La implementación de las recomendaciones propuestas no solo permitirá subsanar esta no conformidad, sino que también fortalecerá la gestión de accesos y la seguridad de la entidad.

Dominio / Control	# ISO	Control	VALORACIÓN OCI

Observación No. 2 – Control 6.2.1: Según la Declaración de Aplicabilidad (versión 2018) y el Manual de Políticas Específicas de Gestión de Seguridad de la Información (versión 2020), se establece la aplicabilidad de la Política para dispositivos móviles. Sin embargo, la Dirección Técnica de Gestión de Información, indico que dicha política no resulta aplicable, ya que la entidad no cuenta con dispositivos móviles dentro de su infraestructura tecnológica.

Observación No. 3 – Control 6.2.2: Según la Declaración de Aplicabilidad (versión 2018), se establece la aplicabilidad de la Política para el Teletrabajo. Sin embargo, el Manual de Políticas Específicas de Gestión de Seguridad de la Información (versión 2020) no establece una política descrita para tal fin.

DOMINIO	**7**	**SEGURIDAD DE LOS RECURSOS HUMANOS**	
Control	7.1.1	Selección e investigación de antecedentes	Cumple satisfactoriamente
	7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	
	7.2.3	Proceso Disciplinario	

El SGC ha implementado controles adecuados en cuanto a la selección e investigación de antecedentes (7.1.1), la toma de conciencia y formación en seguridad de la información (7.2.2), y el proceso disciplinario relacionado con violaciones a las políticas de seguridad de la información (7.2.3). Estas acciones reflejan buenas prácticas de seguridad de la información en la entidad, así como un enfoque claro sobre la capacitación y las consecuencias por el incumplimiento de las políticas internas. Sin embargo, es importante asegurar que estos procesos se mantengan actualizados y sean consistentes con las normativas y mejores prácticas para garantizar su efectividad.

Fortaleza No. 2: La principal fortaleza de la entidad radica en la existencia de un Plan de concienciación y sensibilización definido, orientado a la adopción de buenas prácticas de seguridad de la información, así como en el establecimiento de un proceso disciplinario claro para tratar violaciones a las políticas de seguridad. Además, el proceso de selección de personal incluye verificaciones de antecedentes con diversas entidades relevantes (Contraloría, Procuraduría, Policía), lo que ayuda a mitigar riesgos asociados al personal que ingresa a la entidad.

DOMINIO	**8**	**GESTION DE ACTIVOS**	
Control	8.1.1	Inventario de activos	Cumple parcialmente
	8.1.2	Propiedad de los activos	
	8.1.3	Uso aceptable de los activos	
	8.2.2	Etiquetado de la Información	

Observación No. 4 – Gestión de Activos: El SGC en lo que respecta al **inventario de activos** (8.1.1) y la **propiedad de los activos** (8.1.2), están programados para concluir el levantamiento de activos el 17 de diciembre de 2024. Por otra parte, la **política de uso aceptable de los activos** está implementada y se siguen los lineamientos en la gestión de la información clasificada y reservada. Sin embargo, se requiere asegurar la efectividad de la implementación de estos controles y realizar una revisión constante para garantizar el cumplimiento total dentro de los plazos establecidos.

Dominio / Control	# ISO	Control	VALORACIÓN OCI
DOMINIO	**9**	**CONTROL DE ACCESO**	
Control	9.1.1	Política de control de acceso	Cumple parcialmente
	9.2.1	Registro y cancelación del registro de usuarios	
	9.2.2	Suministro de acceso a usuario	
	9.2.3	Gestión de derechos de acceso privilegiado	Cumple satisfactoriamente
	9.2.5	Revisión de los derechos de acceso de usuarios	Cumple parcialmente
	9.4.3	Sistema de Gestión de Contraseñas	
	9.4.5	Control de acceso a códigos fuente de programas	Cumple satisfactoriamente

No Conformidad No. 3 – Control 9.1.1 Gestión de usuarios genéricos
Se identificó el uso de un usuario genérico denominado **ADMIN** para el acceso a la herramienta "**OCS Inventory**" y el usuario **ADMINISTRADOR** para el acceso al servidor ARGIS7. Esto contraviene lo establecido en el Manual de Políticas Específicas de Gestión de Seguridad de la Información, que dispone: "*Los administradores de las aplicaciones, sistemas operativos y plataformas deben asegurar que los recursos sean operados y administrados en condiciones controladas, por medio de la asignación de usuarios personalizados y la asignación de roles y privilegios de administración, los super usuarios genéricos (en cualquier plataforma ejemplo sys, system, root, admin, administrador, sa, etc.) no deberán ser utilizados en las tareas del día a día, sino solo en ocasiones de contingencia*"

> **Recomendación No. 3 – Control 9.1.1:** Esta Oficina **recomienda** deshabilitar el usuario genérico ADMIN en la herramienta "OCS Inventory" y sustituirlo por cuentas de usuario personalizadas, asignadas a cada administrador con base en sus roles y responsabilidades.

Observación No. 5 – Control 9.1.1: Según el procedimiento de **Gestión de Acceso a Usuarios**, no se identifica una Matriz base por cargo, y no existe una Matriz de roles y perfiles (relacionado con el No Conformidad No. 2 – Control 6.1.2: Definición de Matriz de Roles y Perfiles). Esto impacta directamente en la capacidad de la entidad para gestionar y controlar de manera adecuada los accesos, ya que no se cuenta con una referencia estructurada que defina los permisos necesarios para cada función o cargo dentro de la entidad.

Por tal motivo, el procedimiento de **Gestión de Acceso a Usuarios** no se encuentra actualizado a la fecha de la presente auditoría, lo que podría generar riesgos asociados a accesos inadecuados o conflictos con los principios de mínimo privilegio y segregación de funciones. Finalmente, se reitera la **recomendación No. 2 – Control 6.1.2**

Observación No. 6 – Control 9.2.1 y 9.2.2: En el Directorio Activo, se identificaron cuentas con una nomenclatura diferente (ma-bg) asignadas a la unidad organizativa (OU) correspondiente a la mesa de servicio. Sin embargo, al realizar la validación del inventario de usuarios, con el propósito de constatar la asignación de dichas cuentas, no se encontró evidencia documental que permita identificar claramente a quién pertenecen.

Observación No. 7 – Control 9.2.5: Conforme el No Conformidad No. 3 – Control 9.1.1 Gestión

Dominio / Control	# ISO	Control	VALORACIÓN OCI
de usuarios genéricos, esta Oficina constató que no se están realizando actividades relacionadas con el monitoreo periódico en la revisión de los derechos de acceso a los usuarios. **Observación No. 8 – Control 9.4.3:** Según el procedimiento de Gestión de Accesos a Usuarios, no se identifican lineamientos dirigidos a salvaguardar la Confidencialidad, Integridad de las contraseñas (Gestor de Contraseñas, Calidad de la contraseña, etc)			
DOMINIO	**10**	**CRIPTOGRAFIA**	
Control	10.1.1	Política sobre el uso de controles criptográficos	Cumple parcialmente
	10.1.2	Gestión de llaves	**No cumple**
No Conformidad No. 4 – Control 10.1.1 y 10.1.2: Procedimiento Gestión de Llaves En el Manual de Políticas Específicas de Gestión de Seguridad de la Información (versión 2020) se encuentra documentada la Política sobre el uso de Controles Criptográficos. Sin embargo, esta carece de información detallada en los siguientes puntos: • No se especifican procedimientos claros sobre la evaluación periódica y la actualización de las herramientas criptográficas utilizadas. • No se establecen lineamientos para la selección de algoritmos robustos, como AES-256 o RSA-2048, ni los escenarios específicos en los que deben emplearse. • No se incluyen parámetros para identificar y eliminar algoritmos considerados inseguros (por ejemplo, DES o MD5), comprometiendo la confidencialidad, integridad y autenticidad de la información cifrada. **Recomendación No. 4 – Control 10.1.2:** Esta Oficina **recomienda** establecer un procedimiento formal y documentado que detalle el ciclo de vida completo de las llaves criptográficas, incluyendo su generación, distribución, almacenamiento, uso, renovación, revocación y destrucción. Incluir en la política directrices claras para la selección de algoritmos robustos como AES-256, RSA-2048 o superiores, especificando los casos de uso en los que se deben implementar según los estándares internacionales actuales. Identificar algoritmos considerados obsoletos (por ejemplo, DES, MD5) y definir una política para su eliminación progresiva o inmediata según el nivel de riesgo que representen.			
DOMINIO	**11**	**SEGURIDAD FISICA**	
Control	11.1.1	Perímetro de seguridad física	Cumple satisfactoriamente
	11.1.2	Controles físicos de entrada	
	11.1.3	Seguridad de oficinas, recintos e instalaciones	
	11.1.4	Protección contra amenazas externas y ambientales	
	11.1.5	Trabajo en áreas seguras	
	11.1.6	Áreas de despacho y carga	No Aplica
	11.2.2	Servicios de suministro	Cumple satisfactoriamente
	11.2.3	Seguridad del cableado	
	11.2.8	Equipos de usuario desatendido	

Dominio / Control	# ISO	Control	VALORACIÓN OCI
	11.2.9	Política de escritorio limpio y pantalla limpia	No Cumple

Fortaleza No. 3: (i) Las instalaciones críticas están claramente delimitadas, permitiendo priorizar su protección. (ii) implementación de extintores, alarmas y detectores contribuye a la seguridad física de las instalaciones. (iii) Control y coordinación de accesos para personal autorizado y visitantes garantizan una gestión estructurada del ingreso. (iv) La portería equipada con detector de metales agrega un nivel básico de control. (v) Se tiene implementada una política de bloqueo automático a los 5 minutos de inactividad.

No Conformidad No. 5 – Control 11.2.9: Escritorio y pantalla limpia de información
En el Manual de Políticas Específicas de Gestión 'de Seguridad de la Información (versión 2020) está documentada la **Política de escritorio limpio y pantalla limpia**, establece *"…el Grupo de Tecnologías de Información debe aplicar políticas a los equipos para restringir el almacenamiento de información en el escritorio de los equipos de cómputo suministrados por el SGC…*". Sin embargo, durante una sesión virtual realizada el 11 de diciembre de 2024, esta Oficina constató que, en la práctica, se está almacenando información no solo en los escritorios de los equipos, sino también en la carpeta de "Descargas". Además, desde esa ubicación se intentaba acceder a la información relacionada con la presente auditoría. Esto sugiere que los repositorios institucionales, que cuentan con mecanismos de seguridad como copias de seguridad, no están siendo utilizados adecuadamente.

Recomendación No. 5 – Control 11.2.9: Esta Oficina **recomienda** reforzar la política de escritorio limpio y pantalla limpia mediante la implementación de controles técnicos que restrinjan el almacenamiento de información en ubicaciones no autorizadas, como el escritorio y la carpeta de "Descargas, Mis Documentos, etc". Asimismo, se debe reforzar el uso de los **repositorios institucionales** que cuenten con mecanismos de seguridad adecuados, como copias de seguridad, entre otros. Adicionalmente, se sugiere continuar realizando sesiones de sensibilización y capacitación periódicas para todos los usuarios sobre la importancia de seguir estas políticas, y establecer procedimientos de auditoría para verificar el cumplimiento de las mismas.

DOMINIO	12	SEGURIDAD DE LAS OPERACIONES	
Control	12.1.2	Gestión de cambios	Cumple satisfactoriamente
	12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Cumple parcialmente
	12.2.1	Controles contra códigos maliciosos	Cumple satisfactoriamente
	12.3.1	Respaldo de Información	
	12.4.1	Registro de eventos	
	12.4.4	Sincronización de relojes	Cumple parcialmente
	12.5.1	Instalación de software en sistemas operativos	Cumple satisfactoriamente
	12.6.2	Restricciones sobre la instalación de software	

Fortalezas No. 4: (i) Implementación de controles eficaces para prevenir malware, asegurando la integridad y confidencialidad de los sistemas. (ii) Proceso de respaldo de datos, garantizando la disponibilidad y recuperación ante desastres. (iii) Proceso controlado para instalar software autorizado, minimizando riesgos de vulnerabilidades. (iv) Restricciones sobre instalaciones no autorizadas, asegurando el cumplimiento de las políticas y reduciendo riesgos de seguridad.

Dominio / Control	# ISO	Control	VALORACIÓN OCI

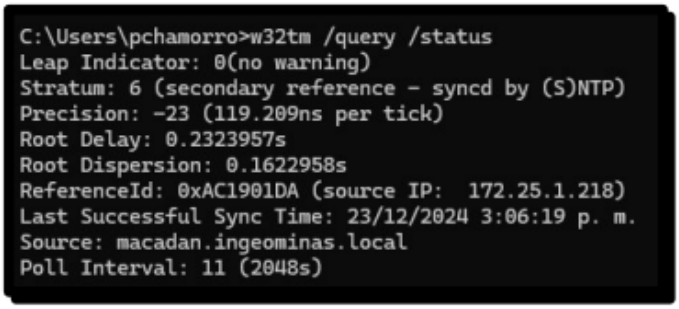
Observación No. 9 – Control 12.1.4: Se observó que se han creado ambientes productivos y de desarrollo para algunos servicios. Sin embargo, esta práctica no se está llevando a cabo de manera consistente, ya que el licenciamiento disponible es limitado. En algunos casos, el servidor de pruebas se utiliza también como servidor de producción, lo que puede generar riesgos operativos y de seguridad al no separar adecuadamente los entornos.

Observación No 10 –Control 12.4.4: Sincronización de Relojes

En el Manual de Políticas Específicas de Gestión de Seguridad de la Información (versión 2020) se encuentra documentada la Política de Registro de Eventos, establece "El Grupo de Tecnologías de Información debe implementar la sincronización de relojes de los sistemas de información a un único servidor NTP (Network Time Protocol)". Sin embargo, según la relatoría proporcionada por el administrador del Directorio Activo, se indicó que el servidor NTP se encontraba fuera de servicio debido a una falla operativa. Como resultado, se optó por utilizar los servidores DNS de Google como fuente alternativa de sincronización, lo que podría generar riesgos en términos de control y seguridad.

> **Recomendación No. 6 – Control 12.4.4:** Esta Oficina **recomienda** restablecer el servicio del servidor NTP interno como fuente principal de sincronización de los relojes de los sistemas de información, conforme a la política de Registro de Eventos del Manual de Políticas Específicas de Gestión de Seguridad de la Información (versión 2020).

En relación con el Informe Preliminar de esta auditoría, la Dirección Técnica Gestión de Información indicó: "*Todos los computadores de usuarios, servidores Windows que se encuentren integrados al dominio del Directorio Activo mantienen sincronizados sus relojes. A nivel de servidores Linux se habilitará un servidor NTP propio del SGC para que tomen la sincronización del reloj de esa fuente.*



Se puede ejecutar ese comando en cualquier computador o servidor windows: w32tm /query /status ahí muestra Source IP"

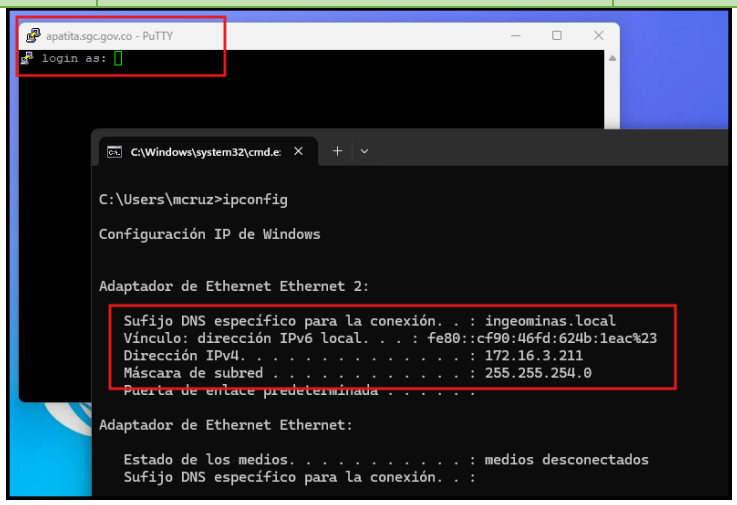
Con base en la revisión realizada por esta Oficina, aunque los computadores de usuarios y servidores Windows sincronizan sus relojes mediante el Directorio Activo, y la Dirección Técnica Gestión de Información ha indicado que se habilitará un servidor NTP propio para los sistemas Linux, el servidor NTP interno principal continúa fuera de servicio. Como medida temporal, se están utilizando los servidores DNS de Google como fuente de sincronización, lo que implica riesgos en términos de control y seguridad.

Dominio / Control	# ISO	Control	VALORACIÓN OCI
La Oficina de Control Interno **CAMBIÓ** la **No Conformidad** registrada en el Informe Preliminar, por la **Observación (No. 10)** con la **recomendación** expuesta, considerando que se están tomando medidas correctivas para mitigar los riesgos asociados a la sincronización de relojes y garantizar el cumplimiento de las políticas de seguridad de la información.			
DOMINIO	**13**	**SEGURIDAD DE LAS COMUNICACIONES**	
Control	13.1.1	Controles de redes	Cumple parcialmente
	13.1.2	Seguridad de los servicios de red	
	13.1.3	Separación de las redes	
	13.2.1	Políticas y procedimientos de transferencia de información	Cumple satisfactoriamente
	13.2.3	Mensajería electrónica	
	13.2.4	Acuerdos de confidencialidad o de no divulgación	

No Conformidad No. 7 – Control 13.1.1, 13.1.2 y 13.1.3: Controles de seguridad en redes
En el Manual de Políticas Específicas de Gestión de Seguridad de la Información (versión 2020) se encuentra documentada la **Política de Gestión de la Seguridad en las Redes**, la cual establece que "*El SGC, a través del Grupo designado, únicamente proporcionará a los funcionarios, contratistas y proveedores acceso a los servicios para los que específicamente se les haya autorizado, controlando las conexiones de red y los equipos o servicios de red que deben estar definidos según los roles y perfiles aprobados por el SGC.*" No obstante, durante una sesión virtual realizada el 11 de diciembre de 2024, esta Oficina constató que, aunque se está realizando la segregación de redes mediante VLANs para las sedes de Bogotá, sin embargo, se encuentra pendiente la migración de los usuarios a dicha VLAN para la sede de Cali.

Por otra parte, se identificó una brecha en la **aplicación de controles de seguridad**, ya que es posible acceder al switch core mediante una conexión VPN de usuarios. Esto indica que no existen restricciones de acceso adecuadas entre las VLANs, poniendo en riesgo la segregación y el control de accesos internos. Es fundamental que los recursos de administración solo sean accesibles desde VLANs de administración específicas para garantizar una mayor seguridad y control.

Dominio / Control	# ISO	Control	VALORACIÓN OCI



Recomendación No. 7 – Control 13.1.1, 13.1.2 y 13.1.3: Esta Oficina **recomienda** revisar y actualizar la configuración de VLANs para asegurar que cada grupo de usuarios tenga acceso solo a los recursos autorizados, conforme a sus roles y perfiles. Además, debe implementarse un control estricto que impida el acceso no autorizado a dispositivos críticos de la red, como los switches core, a través de la VPN, estableciendo restricciones entre VLANs y utilizando herramientas de segmentación más estrictas.

En relación con el Informe Preliminar de esta auditoría, la Dirección Técnica Gestión de Información indicó: "*Para las No Conformidades mencionadas, indicamos que no estamos de acuerdo, y damos las siguientes aclaraciones:*

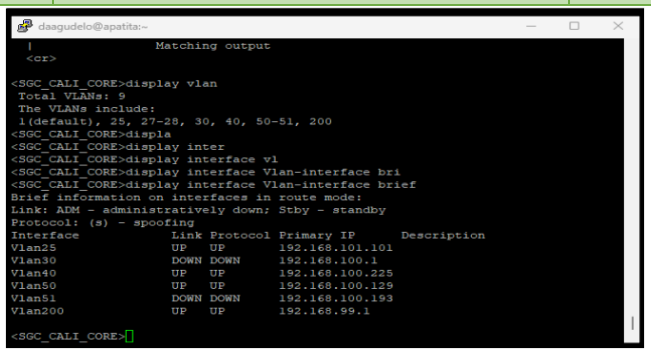
"no se ha identificado una desagregación adecuada de redes para los usuarios en la sede de Cali":

El SGC tiene definida en todas las sedes, la segmentación de red a través de VLAN, incluida la sede CALI. Esta segmentación es igual en todas, cuyos principales segmentos de red son:

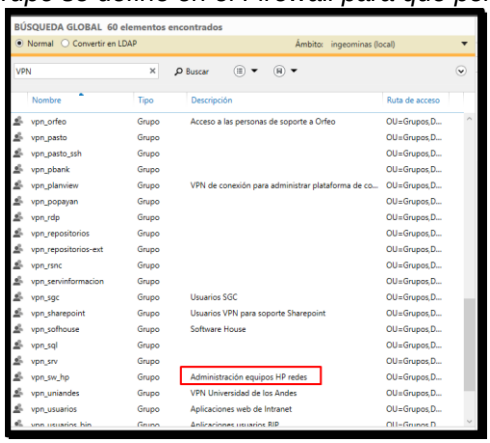
- *Servidores en la VLAN 25*
- *Usuarios en la VLAN 30*
- *WiFi en la VLAN 50*
- *Impresoras en la VLAN 200*

Recalcamos que en la sede Cali existen y funcionan las mismas VLAN que en las demás ciudades; sin embargo y únicamente en esta sede, es necesario realizar la migración de unos usuarios a la VLAN respectiva, que debe ser realizada localmente en coordinación con los usuarios.

Dominio / Control	# ISO	Control	VALORACIÓN OCI



***"se identificó una brecha en la aplicación de controles de seguridad, ya que es posible acceder al switch core mediante una conexión VPN autenticada"**:*
Es normal que se pueda acceder a los switch core utilizando la VPN y esto sucede en cualquier entidad o compañía, de lo contrario debería existir personal las 24 horas en sitio para realizar cualquier actividad de soporte, mantenimiento o configuración. Este usuario que se conecta a los switch core es el administrador de la red. Para este acceso se han creado en Directorio Activo grupos de usuarios de VPN para cada caso de uso (entre ellos el de acceso a switches como se
muestra en la gráfica) y el grupo se define en el Firewall para que permita la conectividad.



Una vez conectado a la VPN, el acceso a los equipos de red (switch core, switches,entre otros) se realiza por autenticación de login y contraseña, que son distintas a la de la VPN y donde el acceso es por medio de protocolo cifrado, normalmente SSH. Es decir, además de la seguridad de la VPN, también se utiliza la seguridad de otro protocolo para ingresar a los switch core y el único fin de este usuario es administrar las reglas y segmentos de red, donde no tiene acceso a ningún otro dispositivo que no sea de switch. Esto es bien distinto a los usuarios que acceden a la VLAN permitida (grupo vpn_sgc) para realizar sus labores normales".

Con base en lo anterior, esta Oficina **ACOGE** el planteamiento presentando por la Dirección Técnica de Gestión de Información "*no se ha identificado una desagregación adecuada de redes para los usuarios en la sede de Cali*" y **MANTIENE** el segundo planteamiento "*se identificó una brecha en la aplicación de controles de seguridad, ya que es posible acceder al switch core mediante una conexión VPN autenticada*", toda vez que lo planteando por esta Oficina,

Dominio / Control	# ISO	Control	VALORACIÓN OCI
evidencia que es posible acceder desde la VPN de usuarios al switch core, conforme se demostró en la imagen. En consecuencia, la Oficina de Control Interno **REPLANTEÓ** la No Conformidad expuesta en el presente informe final.			
DOMINIO	**14**	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**	
Control	14.1.1	Análisis y especificación de requisitos de seguridad de la información	Cumple satisfactoriamente
	14.2.1	Política de desarrollo seguro	
	14.2.5	Principios de construcción de sistemas seguros	
	14.2.8	Pruebas de seguridad de sistemas	
	14.3.1	Protección de datos de prueba	
DOMINIO	**15**	**RELACIONES CON LOS PROVEEDORES**	
Control	15.1	Seguridad de la información en las relaciones con los proveedores	No cumple
	15.2	Gestión de la prestación de servicios de proveedores	Cumple satisfactoriamente
No Conformidad No. 8 – Control 15.1: Análisis de riesgos con proveedores En el Manual de Políticas Específicas de Gestión de Seguridad de la Información (versión 2020) se encuentra documentada la Política de Relación con los Proveedores, establece que "*El SGC a través del grupo designado debe dar a conocer las políticas de SGSI y de protección de datos personales, y debe formalizar los acuerdos con los proveedores antes del inicio de las actividades. El jefe inmediato o supervisor de contrato apoyado por el Responsable de Seguridad de Información realizará* ***análisis de riesgo de seguridad*** *para establecer los* ***criterios de acceso a los activos de información*** *a los cuales tiene acceso terceras partes y definir los planes o acciones de tratamiento para* ***prevenir la materialización de los riesgos*** *identificados.*" Sin embargo, conforme la sesión realizada el día 11 de diciembre, está actividad no se esta llevando a cabo por ninguno de los dos responsables. **Recomendación 8 – Control 15.1:** Esta Oficina **recomienda** establecer un plan de acción para garantizar la implementación efectiva de la Política de Relación con los Proveedores, que incluya la realización de análisis de riesgos de seguridad de la información por las partes interesadas. Este plan debe incluir la documentación y formalización de los acuerdos, la difusión de las políticas de SGSI y de protección de datos personales, así como la definición y aplicación de medidas de tratamiento para mitigar los riesgos identificados, asegurando la protección de los activos de información.			
DOMINIO	**16**	**GESTION DE INCIDENTES DE SEGURIDAD**	
Control	16.1.1	Responsabilidades y procedimientos	Cumple parcialmente
	16.1.2	Reporte de eventos de seguridad de la información	
	16.1.3	Reporte de debilidades de seguridad de la información	
	16.1.4	Evaluación de eventos de seguridad de	

Dominio / Control	# ISO	Control	VALORACIÓN OCI
		la información y decisiones sobre ellos	
	16.1.5	Respuesta a incidentes de seguridad de la información	
	16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	
	16.1.7	Recolección de evidencia	

Observación No. 11: Conforme a la evidencia remitida, esta Oficina constató que se han implementado controles perimetrales, como un WAF (Web Application Firewall) y un SIEM (Security Information and Event Management), los cuales permiten detectar, monitorear y responder a posibles amenazas de manera efectiva, fortaleciendo la seguridad de los sistemas y la protección de la información del SGC. A la fecha de la presente auditoría no se cuenta con la formalización del procedimiento **GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y DATOS PERSONALES**, el cual abarca los controles del presente dominio.

DOMINIO	17	CONTINUIDAD	
Control	17.1.1	Planificación de la continuidad de la seguridad de la información	Cumple satisfactoriamente
	17.1.2	Implementación de la continuidad de la seguridad de la información	
	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	Cumple parcialmente
	17.2.1	Disponibilidad de instalaciones de procesamiento de información	

Observación No. 12 – Control 17.1.3: Si bien se identificó que se ejecutó un programa de prueba durante la presente auditoría, se constató que, a la fecha de la misma, no se dispone de un informe oficial que documente los resultados obtenidos de la evaluación de continuidad. La ausencia de este informe impide evaluar de manera adecuada la efectividad de las pruebas realizadas y el nivel de preparación de la entidad ante posibles incidentes que afecten la continuidad de sus operaciones.

Observación No. 13 – Control 17.2.1: Conforme con lo manifestado por la Dirección Técnica de Gestión de Información, se constató que el datacenter alterno (CDA) no cuenta con una conexión redundante de internet. Esta falta de redundancia podría generar riesgos en términos de disponibilidad y continuidad de los servicios en caso de que la conexión principal se vea afectada, lo cual podría impactar negativamente en la operatividad de la entidad.

DOMINIO	18	CUMPLIMIENTO	
Control	18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales.	Cumple parcialmente
	18.1.3	Protección de registros.	
	18.1.4	Protección de los datos y privacidad de la información relacionada con los datos personales.	
	18.2.1	Revisión independiente de la seguridad de la información	
	18.2.2	Cumplimiento con las políticas y normas	

Dominio / Control	# ISO	Control	VALORACIÓN OCI
		de seguridad.	

Observación No. 14 – Control 18.1.1: Actualmente se identifica el normograma en la sección de Transparencia de la página web de la entidad, sin embargo, no se identifica requisitos legales, reglamentarios que apliquen a la entidad en materia de Protección de Datos Personales.

Observación No. 15 – Control 18.1.3: Conforme la sesión realizada el día 11 de diciembre del presente año, la Dirección Técnica de Gestión de Información expreso que a la fecha de la presente auditoria no se ha oficializado o actualizada la tabla de retención documental. Su ultima actualización radica en el año 2019 y es la versión que se encuentra publicada. No obstante, al corte de la presente auditoria, se cuenta con una versión aprobada y esta a la espera de su implementación.

Observación No. 16 – Control 18.1.4: La entidad cuenta con la Política de Protección de Datos Personales, sin embargo, no se tiene un rol de Oficial de Protección de Datos Personales (OPDP). La ausencia de este rol dificulta la supervisión efectiva y la gestión de las políticas relacionadas con la protección de datos personales, lo que podría exponer a la entidad a riesgos legales, operacionales y reputacionales asociados a un manejo inadecuado de dicha información.

Observación No. 17 – Control 18.2.1 y 18.2.2: Durante el período 2023, no se llevaron a cabo revisiones independientes de seguridad de la información por parte de la Oficina de Control Interno, lo que limita la capacidad de la entidad para evaluar de manera objetiva y detallada la efectividad de los controles de seguridad implementados. No obstante, en el marco de la presente auditoria se comprendió el periodo 2023-2024.

5. CONCLUSIONES

Dominio 5 - Política de Seguridad de la Información: La entidad cuenta con una política actualizada, pero no se revisa periódicamente. Se recomienda realizar una revisión continua.

Dominio 6 - Organización de la Seguridad de la Información: Falta un Oficial de Seguridad de la Información (OSI) y una matriz de roles y perfiles. Se recomienda asignar un OSI y formalizar políticas para dispositivos móviles y teletrabajo.

Dominio 7 - Seguridad de los Recursos Humanos: Se han implementado controles adecuados en selección, formación y disciplina, pero deben mantenerse actualizados conforme a las normativas vigentes.

Dominio 8 - Gestión de Activos: Se está avanzando en la gestión de activos, pero es necesario garantizar la efectividad de los controles y revisiones periódicas.

Dominio 9 - Control de Acceso: Se identificaron usuarios genéricos y falta de una matriz actualizada. Se recomienda deshabilitar cuentas genéricas, actualizar la matriz de roles y realizar revisiones periódicas.

Dominio 10 - Criptografía: La política de criptografía necesita ser actualizada y no incluye procedimientos detallados ni criterios claros para la selección de algoritmos seguros. Se recomienda implementar procedimientos de gestión de llaves criptográficas.

Dominio 11 - Seguridad Física: Se implementan controles adecuados, pero hay deficiencias en la política de escritorio limpio y almacenamiento adecuado de información. Se recomienda reforzar esta política y realizar auditorías periódicas.

Dominio 12 - Seguridad de las Operaciones: La separación de ambientes y la gestión de NTP son áreas de mejora. Se recomienda asegurar la correcta separación de ambientes y restablecer el servidor NTP interno.

Dominio 13 - Seguridad de las Comunicaciones: Hay deficiencias en la asignación de usuarios de la sede Cali y acceso no autorizado a dispositivos críticos. Se recomienda revisar la configuración de VLANs y reforzar los controles de acceso.

Dominio 14 - Adquisición, Desarrollo y Mantenimiento de Sistemas: El manual de desarrollo no ha sido actualizado desde 2016. Se recomienda incluir una política de desarrollo seguro y actualización de los procedimientos.

Dominio 15 - Relaciones con los Proveedores: No se están realizando análisis de riesgos con proveedores. Se recomienda establecer un plan de acción para implementar esta política de forma efectiva.

Dominio 16 - Gestión de Incidentes de Seguridad: Falta formalizar el procedimiento de gestión de incidentes. Se recomienda documentar y formalizar este procedimiento para una respuesta organizada.

Dominio 17 - Continuidad: Se identificaron deficiencias en la documentación de pruebas de continuidad y en la falta de redundancia en el datacenter alterno. Se recomienda generar informes de pruebas y mejorar la infraestructura de continuidad.

Dominio 18 - Cumplimiento: Hay áreas críticas como la falta de especificación de requisitos legales de protección de datos personales, una tabla de retención desactualizada, la ausencia de un OPDP, y falta de revisiones independientes de seguridad. Se recomienda mejorar el cumplimiento de normativas y realizar revisiones de seguridad periódicas.

Finalmente, se presenta un cuadro resumen que sintetiza las No Conformidades, observaciones y fortalezas para facilitar su comprensión; se resalta que sobre las No Conformidades es necesario definir un plan de mejoramiento en la plantilla que será suministrada dentro del radicado del presente informe final:

RESUMEN		
CLASIFICACÍON	**Cant.**	**% Part. /**

DEL SITUACIONES EVIDENCIADAS		Tipo de Situación
No Conformidad	8	22.2%
Observaciones	17	47.2%
Fortalezas	4	11.1%
Recomendaciones	7	19.4%
Total	**36**	**100%**

Firmas:

Auditor que ejecutó la auditoria: Andrés Mauricio Cruz Vargas
Contratista Oficina de Control Interno

Revisó y aprobó: Erika Marcela Huari Mateus
Jefe Oficina de Control Interno