COLOMBIA POTENCIA DE LA VIDA

Gobierno del Cambio

INFORME FINAL AUDITORIA AL MSPI VIGENCIA 2024 PROCESO GTI

OFICINA DE CONTROL INTERNO

Junio 2025

UNGRD
Unidad Nacional para la Gestión del Riesgo de Desastres

Sistema Nacional de Gestión del Riesgo de Desastres

CONTENIDO

1. Objetivo

Verificar el cumplimiento de los lineamientos establecidos en el Modelo de Seguridad y Privacidad de la Información (MSPI) a cargo del Grupo de Tecnología de la Información (GTI) de la UNGRD y su operación con eficiencia y eficacia, evaluando también la definición de los posibles riesgos que puedan presentarse durante la gestión y aplicación del MSPI.

2. Alcance

La auditoría inició con la evaluación por muestreo de los controles de seguridad verificando cada uno de los dominios establecidos en la norma NTC: ISO/IEC 27001:2013, los cuales tratan los objetivos de control del Modelo y su efectividad, los procedimientos implementados en el proceso que aplica al área auditada, el tratamiento de los riesgos detectados de seguridad de la información y la matriz de riesgos en la vigencia 2024.

3. Metodología

La metodología que se aplicó para la evaluación del modelo, se basó en consultas, análisis de datos, observación, inspección, revisión y confirmación de información, además, de otras técnicas de auditoría aceptadas:

- Revisión plan de mejoramiento - informe de auditoría al Sistema de Gestión en Seguridad de la Información (SGSG) - ISO/IEC 27001:2013 de agosto 2023
- Verificación de la aplicabilidad de la normativa vigente y evaluación de los controles, las pruebas y evidencias a auditar del MSPI. Definición de la muestra a revisar.
- Solicitud de información, recolección de datos, listas de chequeo, revisión documental, de controles en el MSPI, revisión de indicadores y de riesgos de seguridad de la información.
- Realización de mesas de trabajo con el proceso.
- Definición y estructuración de hallazgos y recomendaciones.
- Informe preliminar y final; fortalezas, hallazgos, recomendaciones y conclusiones. De acuerdo a los factibles hallazgos encontrados, se definiría un plan de mejoramiento al proceso.

4. Marco Legal

La Oficina de Control Interno - OCI, en cumplimiento de las funciones establecidas en la Ley 87 de 1993, efectuó una evaluación y seguimiento por muestreo al MSPI, atendiendo lo dispuesto en la siguiente normativa:

- Decreto 4147 de 2011, Por el cual se crea la Unidad Nacional para la Gestión del Riesgo de Desastres, se establece su objeto y estructura
- Ley 1581 de 2012, “Por la cual se dictan disposiciones generales para la protección de datos personales”.

- Ley 1712 de 2014, Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional
- Norma ISO: IEC 27001:2013
- MSPI de MINTIC.
- Plan de Seguridad y Privacidad 2024
- Plan de tratamiento de Riesgos SI 2024
- Matriz Gestión Riesgo de Seguridad de la Información RG-1101-GTI-04_9
- Manual de políticas de Seguridad de la información (M-1101-GTI-01)
- Manual del Sistema de Seguridad y Privacidad de la información (M-1101-GTI-03_3)
- Procedimientos asociados para dar cumplimiento al MSPI.

5. Desarrollo del Informe

De acuerdo a la metodología mencionada, el equipo auditor realizó una revisión detallada de todos los dominios establecidos en el autodiagnóstico del MSPI de MinTIC, con base a la cual seleccionó la muestra a auditar y solicitó al proceso las evidencias correspondientes.

Se realizaron 2 mesas de trabajo con GTI, verificaciones in situ, revisión de indicadores de gestión y la matriz de riesgos de seguridad de la información.

Se evidenció por muestreo del 43%, de un total de 119 controles que el proceso auditado atiende la mayoría de los controles referenciados en el Anexo A de las normas ISO/IEC 27001:2013, con base a las pruebas alineadas con esos controles y con las respectivas evidencias que están definidas en el autodiagnóstico del MSPI de la entidad.

Finalmente, terminado el ejercicio auditor, se detectaron 5 hallazgos y se generaron recomendaciones importantes con el propósito de apoyar la mejora continua en el área auditada.

5.1 Resultados del Ejercicio Auditor

5.1.1 Revisión plan de mejoramiento vigencia 2023

Se revisó en la plataforma NeoGestión el Plan de Mejoramiento resultado del informe de la auditoría al SGSI ISO/IEC 27001:2013 de agosto 2023, evidenciando el tratamiento adecuado y cierre de 5 no conformidades como *Eficaz*.

Se revisó la no conformidad pendiente registrada en NeoGestión bajo la acción correctiva 289 de GTI, donde fue evaluada como *No Eficaz*, pero en noviembre 2023, desde la OCI se evalúa como *Eficaz*, una vez revisadas las aclaraciones que presentó el proceso, dando alcance a lo registrado en NeoGestión.

5.1.2 Hallazgos

El equipo auditor evidenció 5 hallazgos, los cuales se especifican a continuación:

5.1.2.1 Debilidad en la designación en el CIGD del Oficial de Seguridad de la Información de la entidad de una contratista vinculada al Grupo TI de la UNGRD, situación motivada por ese proceso, desatendiendo el criterio normativo en cuanto a la instancia o área jerárquica a la cual debe vincularse, exponiendo a la entidad a llamados de atención de entes de control.

En ese contexto, la vinculación del Oficial de Seguridad y su nombramiento debe estar a cargo de la Alta Dirección de la entidad o de un área estratégica y no de GTI para conservar su independencia en el ejercicio de sus funciones u obligaciones. En el Acta No 1 del 15 de marzo de 20232, Numeral 2 .2 Oficial de Seguridad de la Información, GTI manifiesta que *"el rol de Oficial de Seguridad de la Información debe ser nombrado por la Alta Dirección en cumplimiento a lo requerido en la norma ISO: IEC 27001:2013 que establece el Sistema de Gestión de Seguridad de la Información SGSI".*

Mencionado lo anterior, se evidenció que la Oficial de Seguridad de la entidad, Ing. Silvia Ribero, estuvo vinculada hasta principios de abril 2025 al Grupo TI, (contrato 9677-PPAL001-374-2024, CDP 240861 solicitado por GTI e informes mensuales de ejecución del contrato). También se evidenció que, en el Comité Institucional de Gestión y Desempeño, Acta No 1 del 15 de marzo de 2023, se aprobó, la designación de la contratista Silvia Ribero como Oficial de Seguridad de la Información de la UNGRD, atendiendo lo mencionado por el Grupo de TI en el sentido que la contratista Ribero contaba con el perfil requerido para ejercer ese rol.

En definitiva, no se tuvo en cuenta la norma para definir y proponer el nombramiento del Oficial de Seguridad de la Información ante el CIGD; el *Estándar ISO/IEC 27001:2013*, *Anexo A, Numeral A.6.1.1 Roles y responsabilidades para la seguridad de información, Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información* y el Documento Maestro de Seguridad y Privacidad de la información, MSPI, MinTIC de 2021, Numeral 07 Planificación, 7.2 Liderazgo, 7.2.3 Roles y responsabilidades, "*(…) el responsable de la seguridad y privacidad de la información deberá depender de un área estratégica que no sea la Oficina o Dirección de Tecnología (se recomienda el despacho de nominador), (…).*

La entidad aplica la herramienta de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI) de MinTIc, *"instrumento que permite a las entidades públicas evaluar su nivel de madurez en la implementación del Modelo, identificando fortalezas y áreas de mejora. Este proceso ayuda a las entidades a cumplir con estándares nacionales e internacionales de seguridad y privacidad, como la ISO/IEC 27001, y a fomentar una cultura de mejora continua".*

Respuesta del Proceso:

El acta No. 1 del Comité Institucional de Gestión y Desempeño (CIGD) del 15-mar-2023 dejó constancia de que la Alta Dirección —no el Grupo TI— aprobó la designación de la Ing. Silvia Ribero como OSI, en concordancia con la ISO 27001. Ese documento demuestra que el nombramiento provino de la instancia estratégica que rige la entidad y, por tanto, se salvaguarda la independencia funcional que exige el MSPI 2021 (numeral 7.2.3, el responsable de seguridad debe depender de un área estratégica distinta a TI). El hecho de que el contrato laboral se tramite a través de GTI es meramente administrativo y presupuestal que no altera la línea de reporte: las responsabilidades del OSI —incluida la obligación de rendir cuentas directamente al CIGD— están descritas en el Manual SGSI, capítulo 6.3.1.1 y son ejercidas ante el Comité.

No obstante, lo anterior, es de resaltarse que el contrato de la Ing, Sylvia Ribero como OSI terminó el día 1 de abril del 2025 y como acción de mejora inmediata al recibo del resultado de la auditoria que nos ocupa, se procederá con el cambio de supervisor de los contratos que se suscriban en adelante con el mismo objeto para que esta quede en cabeza de una dependencia diferente al grupo de GTI.

Respuesta OCI:

Se reitera que la Oficial de Seguridad de la entidad, Ing. Silvia Ribero, estuvo vinculada hasta principios de abril 2025 al Grupo TI, (contrato 9677-PPAL001-374-2024, CDP 240861 solicitado por GTI e informes mensuales de ejecución del contrato). En *los informe de supervisión de contratos y/o convenios (Proceso: GTI)* del contrato de la Ing. Ribero figuraron como supervisores diferentes miembros del Grupo TI, lo anterior demuestra que la OSI, quien fue nombrada como tal por el CIGD en marzo de 2023, estaba vinculada y *dependía* directamente de ese grupo de trabajo de la entidad, situación que desatiende el Documento Maestro de Seguridad y Privacidad de la información, MSPI, MinTIC de 2021, Numeral 07 Planificación, 7.2 Liderazgo, 7.2.3 Roles y responsabilidades, "*(…) el responsable de la seguridad y privacidad de la información deberá depender de un área estratégica que no sea la Oficina o Dirección de Tecnología (se recomienda el despacho de nominador), (…).*

En ese sentido, el proceso responde que *"como acción de mejora inmediata al recibo del resultado de la auditoria que nos ocupa, se procederá con el cambio de supervisor de los contratos que se suscriban en adelante con el mismo objeto para que esta quede en cabeza de una dependencia diferente al grupo de GTI"*, lo que corrobora lo mencionado y evidenciado por el grupo auditor.

Conforme a todo lo anterior, el hallazgo se mantiene en el infirme final de la auditoría.

5.1.2.2 *Inobservancia de las funciones u obligaciones del Oficial de Seguridad de la Información de la entidad establecidas en el Manual del Sistema de Gestión de Seguridad de la Información, por no reportar directamente el desempeño del SGSI al CIGD en la vigencia 2024.*

El ejercicio auditor, no evidenció en la documentación allegada por el proceso, contrato 9677-PPAL001-374-2024 e informes mensuales de ejecución del contrato de la Ing. Silvia Ribero, ninguna presentación de informe de gestión de este oficial con relación al desempeño del SGSI en la vigencia 2024 ante el CIGD, en ese sentido, en las actas del segundo, tercer y cuarto CIGD del 11 de octubre 2024, 14 y 28 de enero 2025, los informes de GTI fueron presentados por su Coordinadora u otro miembro de GTI.

Es de anotar, que se pudo verificar *en el informe No. 6 de supervisión del contrato del 1 de febrero 2025* de la contratista mencionada, que "*elaboró el Plan de Seguridad y Privacidad de la Información 2025 y el Plan de Tratamiento de Riesgos 2025 para aprobación del Comité de Gestión y Desempeño*", pero su presentación y aprobación ante el 4to Comité de la vigencia 2024, realizado el 28 de enero de 2025, la hizo un contratista de GTI.

Es claro y se reitera, que la coordinación de GTI y/o algunos integrantes de ese proceso, dan cuentan sobre el estado, avance y gestión de la seguridad de la información en la entidad al CIGD, tal como se evidencia en algunas actas de sus reuniones en la vigencia 2024. El ejercicio auditor hace énfasis y se refiere solamente a las responsabilidades que le competen al Oficial de Seguridad de la información ante el CIGD de acuerdo al Manual del Sistema de Gestión de Seguridad de la Información (M-1101-GTI-03_3).

"*La administración, monitoreo y coordinación permanentemente de la seguridad de la Información, apoyar la definición de acciones que permitan identificar las vulnerabilidades en la infraestructura y asegurar la adecuada gestión de los incidentes de seguridad de la información en la Entidad*", entre otras, son funciones y responsabilidades del Oficial de Seguridad de la Información, que están definidas en el *Manual del Sistema de Gestión de Seguridad de la información de la Unidad*, temas especializados que directamente deben ser informados y presentados ante el CIGD por la persona idónea que fue designada por ese Comité como Oficial.

En ese contexto y de acuerdo al *Manual del Sistema de Gestión de Seguridad de la Información (M-1101-GTI-03_3 aprobado el 19 de septiembre de 2023), Numeral 6.3 Responsabilidades del oficial de seguridad de la información, 6.3.1.1. Oficial de Seguridad de la Información o quien haga sus veces debe* "*informar al Comité Institucional de Gestión y Desempeño, el desempeño del Sistema de Gestión de Seguridad de la Información en la Entidad".*

Respuesta del proceso:

Para subsanar y fortalecer esta función se adelantarán las siguientes acciones:

1. En los CIGD al agendarse en el orden del día temas relacionados con el MSPI, serán presentados por el OSI.

Respuesta OCI:

De acuerdo a la respuesta del proceso, el hallazgo se sostiene en el informe final de la auditoría.

5.1.2.3 Adecuar el Manual de Política de Seguridad de la Información de la entidad, a causa de la falta de completitud y precisión del alcance y contenido de la Política sobre el Uso de Controles Criptográficos, lo que podría conllevar a llamados de atención de entes de control externos.

La Política sobre Controles Criptográficos de la entidad definida en el *Manual de Política de Seguridad de la Información,* determina que, *"Los computadores portátiles que pertenezcan y estén autorizados para salir de la entidad deben contar con una herramienta de cifrado, con el fin de proteger la información almacenada en los discos duros de estos equipos, salvaguardando así la confidencialidad de la información almacenada (…) Se realiza la configuración de una herramienta de cifrado seleccionando la partición del disco que se quiere cifrar y donde se almacenaran los archivos a resguardar".*

El ejercicio auditor evidenció, con un listado de la vigencia 2024, que están asignados 8 portátiles de propiedad de la entidad a funcionarios/contratistas que trabajan de manera remota.

COMPUTADORES PORTÁTILES ASIGNADOS VIGENCIA 2024						
Placa d e inventario	Responsable	Elemento	Marca	Modelo	Serial	Dependencia
F000755	DIEGO ANDRES LOZANO OSORIO	PORTATIL	DELL	N4110	NO APLICA	SALA DE RADIOS
F004581	CARMEN ADRIANA ALARCON MUÃ'OZ	COMPUTADOR PORTATIL	ACER	ASPIRE E14	16E5A7600	GRUPO DE CONTRATACION
F004595	OLGA LUCIA MONTOYA TOVAR	COMPUTADOR PORTATIL	ACER	ASPIRE E14	EC37600	GRUPO DE APOYO ADMINISTRATIVO
F004603	OLGA LUCIA MONTOYA TOVAR	COMPUTADOR PORTATIL	ACER	ASPIRE E14	F987600	GRUPO DE APOYO ADMINISTRATIVO
F005307	MARIA PAOLA DE SALVADOR TATIS	COMPUTADOR PORTATIL	LENOVO	80SX		GRUPO DE APOYO ADMINISTRATIVO
F036753	JESUS ANTONIO ESLAVA BOTELLO	COMPUTADOR PORTATIL	ACER	A315-59-50KP FHD	NXK65AL00J320070983400	GESTIÓN BIENES MUEBLES E INMUEBLES
U002693	ANGELA CALDERON PALACIOS	PORTATIL	HEWLETT PACKARD	PROBOOK 450 G4	5CD7306QG7	GRUPO DE APOYO ADMINISTRATIVO
U002737	DANIEL FELIPE GONZALEZ PALACIO	PORTATIL	APPLE	A1707	C02X30N0HTD8	OFICINA ASESORA DE COMUNICACIONES

Documento Excel, equipos portátiles asignados a personal de la entidad, vigencia 2024, fuente Grupo de Apoyo Administrativo

El equipo auditor realizo 4 visitas en las instalaciones de la Unidad a los funcionarios/contratistas que tienen en uso esos portátiles y evidenció que a ninguno se le ha aplicado una herramienta para cifrar o encriptar la información de la entidad que ellos gestionan pero que han cumplido con mantener en reserva la documentación institucional que tienen a cargo de acuerdo a lo indicado y determinado por GTI para trabajar desde las casas.

Es importante mencionar que aun así que la política en cuestión define que se debe encriptar la información que gestionan los contratistas/funcionarios que tienen asignados activos de la entidad (portátiles) para el trabajo remoto, también es cierto que no todo el personal gestiona el mismo nivel de confidencialidad y de información reservada que aplica en la entidad, en ese sentido, el contenido de esa política de encriptación de información, está muy abierto y se fija para todos los portátiles que están en uso fuera de la Unidad, por tanto, es evidente que carece de *completitud y precisión,* lo cual implica que se debe definir

o determinar si se les encripta o no la información que gestiona ese personal, de acuerdo a la confidencialidad e información reservada asignada laboralmente y en sus contratos.

Es de anotar, que el equipo auditor realizó una reunión el día 25 de junio de 2025 con el proceso auditado, donde se trató y analizó la política en cuestión, concluyendo que se debe dar más consistencia en su contenido.

Considerando lo anterior, se evidencia una debilidad en el Manual *de Política de Seguridad de la Información de la entidad (M-1101-GTI-01 aprobado el 8 de noviembre de 2023), Numeral, 5.7 Política sobre el uso de Controles Criptográficos,* que adopta y da alcance al *Anexo A de la normatividad ISO/IEC 27001:2013, Control A 10.1.1 Política sobre el uso de controles criptográficos, Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.*

Respuesta del proceso:

Para subsanar se adelantarán las siguientes acciones:

1. Se procederá a actualizar la Política de Controles Criptográficos incorporando el alcance preciso y criterios de aplicación

Respuesta OCI:

Dada la respuesta del proceso, el hallazgo se mantiene en el informe final de la auditoría.

Condiciones de área, Cuarto Eléctrico (CE) - Edificio G4.

5.1.2.4 Fallas en las condiciones de seguridad física en el CE por dejar elementos no permitidos en ese recinto y dejar el Patch Panel del CCTV abierto continuamente, exponiendo al cuarto a factibles hechos o situaciones inesperadas que podrían presentarse y afectar el normal funcionamiento de ese espacio técnico, incumpliendo las normas ISO/IEC 27001:2013 y los requisitos regulados por el Grupo de Apoyo.

El ejercicio auditor pudo constatar, con grabaciones del CCTV de la vigencia 2024, fallas que pueden afectar el buen funcionamiento del cuarto eléctrico:

Descuido en la seguridad del CE, al evidenciarse en la visita in situ, cajas de cartón a bajo de las cajas metálicas eléctricas, elementos que no pertenecen ni deben estar en ese espacio que es exclusivo para dispositivos y acometidas eléctrica, que pueden presentar algún peligro, ocupan espacio y pueden impedir la adecuada circulación del personal de mantenimiento y supervisión de esos equipos eléctricos.

También se evidenció que el Patch Panel del CCTV permanece abierto y expuesto, a personas no permitidas en ese recinto distintas a los técnicos de mantenimiento y personal de la entidad con autorización de entrada a ese cuarto, situación que podría permitir la

manipulación indebida de los switchs de ese panel y del computador, afectando el CCTV, tal como se muestra en las siguientes imágenes y en los videos alojados en el Drive: https://drive.google.com/drive/folders/1i25XPKUMO95zjQmdCAilUd7Lw837U1Xs?usp=drive_link

Imágenes No 1 de video, cajas y pach panel CCTV de Vigilancia abierto en el CE 2do piso G4, noviembre 2024 que trasgreden la seguridad y la normatividad, fuente grabaciones del CCTV

Imagen No 2, de video, cajas y pach panel del CCTV de Vigilancia abierto en el CE 2do piso G4, diciembre 2024 que no atienden la seguridad y la normatividad, fuente grabaciones del CCTV

Lo anterior, incumple *el Procedimiento de Control de Acceso Físico, PR-1603-SA-05, Numeral 4.2. 7. Ingreso áreas seguras,* que dan alcance a las normas *ISO/IEC 27001:2013, el Anexo A*, *Literal A.11.11, "Perímetro de seguridad física, Control: Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información"*.

Finalmente, el *Formato Registro Ingreso a Cuarto Eléctrico - FR-1603-SA-23*, en el apartado de otras obligaciones, se exige que *"se deben sacar todas las cajas y desechos antes de salir de las instalaciones. El cuarto eléctrico debe mantenerse limpio y ordenado en todo momento".*

Respuesta del proceso:

Para subsanar se adelantarán las siguientes acciones:

1. Lista de verificación quincenal basada en el Formato FR-1603-SA-23 que ya exige mantener el recinto limpio y retirar desechos; la checklist debe firmarse.

2. Armario o rack permanezca cerrado para el patch-panel CCTV con llave custodios:

Coordinador de vigilancia, operador de medios tecnológicos, piso 2 G4; aplicar etiqueta “No manipular- solo personal autorizado".

Respuesta de OCI:

Según respuesta del proceso, el hallazgo se mantiene en el informe final de la auditoría.

Condiciones de área en el Data Center - Edificio G4.

5.1.2.5 Fallas en las condiciones de seguridad física en el Data Center, exponiéndola a riesgos de factibles hechos o situaciones inesperadas que podrían afectar el normal funcionamiento de ese espacio tecnológico, incumpliendo las normas ISO/IEC 27001:2013 y exigencias fijadas en las políticas de seguridad de la información establecidas en la entidad.

El ejercicio auditor evidenció en la visita in situ elementos no permitidos encima de las UPS del DC que podrían afectar su funcionamiento u ocasionar eventos inesperados, módulo o Patch Panel abierto, cajas metálicas eléctricas no aseguradas y puerta de entrada al DC sin ajustar adecuadamente, permitiendo factible manipulación indebida de personal no autorizado y poniendo en riesgo el adecuado funcionamiento de los equipos de comunicación y de cómputo, tal como se muestra en las siguientes imágenes y en los videos alojados en el Drive:

https://drive.google.com/drive/folders/1i25XPKUMO95zjQmdCAilUd7Lw837U1Xs?usp=drive_link

Imagen No 3, de video, cargadores electrónicos y cables encima de la UPS en el CE, 2do piso G4, noviembre 2024 que violan la seguridad y la normatividad, fuente grabaciones del CCTV

Imagen No 4, de video, cargadores electrónicos, cables y maletín encima de la UPS en el CE, 2do piso G4, diciembre 2024 que no atienden la seguridad y la normatividad, fuente grabaciones del CCTV

La falta de un total control de seguridad física por parte del personal a cargo de GTI, podría ocasionar alteraciones o trastornos en el funcionamiento adecuado del Data Center.

Lo anterior, incumple las normas *ISO/IEC 27001:2013, el Anexo A*, *Literal A.11.2, Equipos A, 11.2.1 Ubicación y protección de los equipos, Control: "Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado"*.

También, el *"Manual de Políticas de Seguridad de la Información – M-1101-GTI-01",* el cual adopta las normas mencionadas, que establece en el numeral *"5.17. Política de Acceso al Centro de Datos",* el apartado *"Finalización de Labores - Se deben sacar todas las cajas y desechos antes de salir de las instalaciones. El Centro de Datos debe mantenerse limpio y ordenado en todo momento.", "La UNGRD se reserva el derecho de remover y descartar cualquier basura o desechos dejados en él".*

Finalmente, *el Procedimiento de trabajo en áreas seguras, PR-1101-GTI-13_01, Condiciones Generales del Procedimiento,* el apartado*, "Se deben retirar los residuos del proceso de instalaciones propias, realizadas por personal de la misma unidad o por algún tercero".*

Respuesta del proceso:

Para subsanar se adelantarán las siguientes acciones:

Etiquetado de activos y racks ligado al inventario de TI; cualquier equipo fuera de inventario genera alerta y no podrá permanecer en el DC más de 24 h.

Capacitación y sensibilización al personal responsable de dar acceso al DC.

Respuesta de OCI:

Conforme a la respuesta del proceso, el hallazgo se mantiene en el informe final de la auditoría.

6. Riesgos Identificados

Los posibles riesgos identificados con relación al hallazgo formulado en la vigencia 2024, son los siguientes:

- Sin informes del Oficial y sin su participación en el CIGD se podría ver afectado la toma de decisiones del Comité en materia de seguridad de la información. Se pueden ignorar aspectos críticos de seguridad, afectando probablemente la confidencialidad, integridad y disponibilidad de la información.
- Sin la participación del Oficial de Seguridad en los CIGD, probablemente no podría comunicar oportunamente riesgos o brechas relevantes que deben ser tratados por la alta dirección.
- Se incrementaría la probabilidad de incidentes de seguridad no gestionados o mal respondidos.
- El CIGD busca articular todos los sistemas de gestión (calidad, seguridad de la información, control interno, etc.). Si el Oficial de Seguridad no participa activamente en ese Comité, probablemente, se pierde, la posibilidad de sinergias y acciones coordinadas en lo que compete al SGSI.
- El Oficial de Seguridad es el líder de todo el ciclo de PHVA del MSPI, sin la información y comunicación de él al Comité, podrían presentarse vacíos en ese ciclo.
- La falta de la correcta aplicación de la Política sobre el uso de Controles Criptográficos podría conllevar a desviaciones en la conservación de la confidencialidad e información reservada de la entidad.
- Llamados de atención de entes de control externos.

Cuarto eléctrico.

- Sin atender totalmente las condiciones de seguridad física en el CE, pueden presentarse situaciones apremiantes que podrían afectar el normal funcionamiento de este recinto técnico.

- Sin la protección pertinente del Patch Panel del CCTV, se expone a riesgos de manipulación indebida de los switchs por personas no autorizadas, que afectarían el normal funcionamiento de este sistema de VV.
- Llamados de atención de entes de control externos.

Data Center.

- La falta de un control completo de las condiciones de seguridad física del DC por parte del personal a cargo de GTI, podría ocasionar alteraciones o trastornos en el funcionamiento adecuado de este espacio tecnológico.
- Llamados de atención de entes de control externos.

7. Conclusiones

- De acuerdo a la muestra de auditoría seleccionada, el proceso auditado gestiona de manera adecuada la mayoría de los controles establecidos en las normas ISO/IEC 27001:2013, Autodiagnóstico MSPI

- Los riesgos detectados durante el ejercicio auditor se deben tratar para mitigar o evitar su materialización.

- El proceso auditado debe tratar los hallazgos evidenciados por el equipo auditor a través de un plan de mejoramiento.

8. Recomendaciones

- Vincular o nombrar al Oficial de Seguridad de la Información desde la Alta Dirección de la entidad o de un área estratégica dando alcance a la normatividad ISO/IEC 27001:2013 (A.6.1.1) y de acuerdo al Documento Maestro de Seguridad y Privacidad de la información, MSPI, MinTIC de 2021.

- Aplicar el *Manual del Sistema de Gestión de Seguridad de la Información (M-1101-GTI-03_3)* con relación a las competencias del Oficial de Seguridad de la Información ante el CIGD como líder del ciclo de PHVA del MSPI.

- Garantizar la gobernanza efectiva de la seguridad de la información con la participación activa del Oficial de Seguridad de la Información en el CIGD para agregar valor en el cumplimiento de la mejora continua que exige el MSPI.

- Ajustar el Manual de Política de Seguridad de la Información de la entidad, para precisar mejor la Política sobre el uso de Controles Criptográficos y así dar

cumplimiento al Anexo A de la normatividad ISO/IEC 27001:2013 y no dejar vacíos en esa política con relación a la aplicación de la confidencialidad e información reservada de la entidad.

- Cumplir con la normatividad para garantizar las adecuadas condiciones físicas de seguridad tanto del Cuarto Eléctrico como del Data Center y la protección de los equipos eléctricos y electrónicos.

OTRAS RECOMENDACIONES – AUTODIAGNOSTICO MSPI

- Realizar y coordinar con GTH inducciones/capacitaciones a los colaboradores de la entidad donde se socialicen las políticas de seguridad de la información que se encuentran en el Manual de Políticas de Seguridad y Privacidad de la Información, tal como, quedó en el acta No. 2 de la mesa de trabajo con el proceso auditado.

- Cumplir con las pruebas o actividades alineadas a los controles del Anexo A de las normas ISO/IEC 27001:2013 y solución de brechas del autodiagnóstico MSPI, es decir, del avance logrado por el proceso que fue verificado por el ejercicio auditor en la vigencia 2024, los ítems que se encuentran con calificación entre 20 y 80% en la Tabla de Escala de Valoración de Controles del MSPI.

- Estimar la posibilidad legal, que el Oficial de Seguridad de la Información haga parte del CIGD. Es claro que la conformación del Comité de la Unidad da alcance al *Decreto 1083 de 2015 y al Decreto 1499 de 2017, "Artículo 2.2.22.3.8, Comités Institucionales de Gestión y Desempeño,* y también a la *Resolución No. 1324 del 22 de diciembre de 2023,* expedida por la UNGRD, *"por medio del cual se reglamenta el Modelo Integrado de Planeación y Gestión (MIPG) y estableció formalmente la conformación del Comité Institucional de Gestión y Desempeño, en cumplimiento de la normativa nacional",* pero en ese mismo artículo establece que, el CIGD estará integrado, " (…) en el nivel descentralizado, por los subdirectores generales o administrativos o los secretarios generales o quienes hagan su veces, e integrado por los servidores públicos del nivel directivo o asesor que designe el representante legal de cada entidad".

  Por otra parte, el *Documento Maestro de Seguridad y Privacidad de la información, MSPI, MinTIC de 2021*, Numeral 07 Planificación, 7.2 Liderazgo, 7.2.3 Roles y responsabilidades, "(…) el responsable de la seguridad y privacidad de la información (…) de igual manera la persona designada deberá ser incluida como miembro del comité de gestión institucional con voz y voto y en el comité de control interno con voz".

Cuarto Eléctrico Vigencia 2025.

Es importante, que el proceso auditado estime estas recomendaciones, debido a que se están presentando desde la vigencia 2024.

- Garantizar las condiciones de seguridad física del CE y la protección de las cajas metálicas eléctricas (no están bajo llave), lo que podría ocasionar factibles riesgos de manipulación y alteración de estas por personal no autorizado, exponiendo este cuarto a probables situaciones inesperadas que podrían afectar su funcionamiento y la alimentación de potencia del Data Center.

- Evitar elementos no permitidos en el CE y no dejar el Patch Panel del CCTV abierto, exponiendo al cuarto a situaciones inesperadas que podrían afectar el normal funcionamiento de ese espacio técnico. Velar por las condiciones de seguridad física en el CE, tal como se observa en las imágenes.

Imágenes No. 5, elementos del CE 2do piso G4 que podrían afectar su seguridad, fuente propia, CE

Imágenes No. 6, pach panels abiertos en el CE 2do piso G4 vigencia 2025 que podrían afectar la seguridad del CCTV, fuente propia, CE

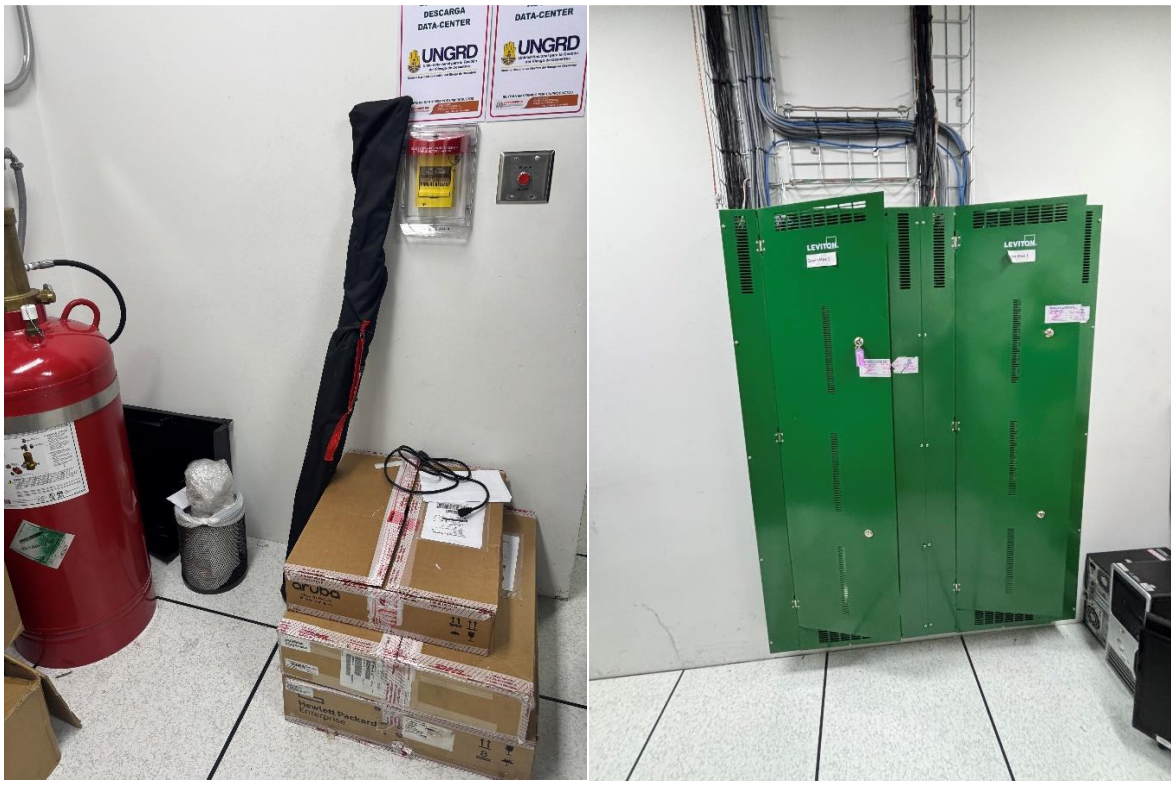
- Mantener asegurada la puerta metálica de entrada al CE en el 2do piso, G4. El equipo auditor en compañía del funcionario/contratista del Grupo Administrativo que atendió la visita de auditoría, evidencio que estaba abierta, lo que podría facilitar el acceso a personas no autorizadas, situación que pondría en riesgo la seguridad del CE.

Data Center, vigencia 2025.

De igual forma, es conveniente, que el proceso auditado estime estas recomendaciones, debido a que se están presentando desde la vigencia 2024.

- Velar por las condiciones de seguridad del cuarto de procesamiento de datos y equipos de comunicación. Se evidencian, cajas de cartón, sillas, equipos de cómputos, pantallas y otros materiales en el DC, elementos y equipos que no pertenecen ni deben estar en el centro de comunicaciones, ocupan espacio, afectando el desplazamiento del personal técnico autorizado y poniendo en riesgo la seguridad del DC.

- Proteger las cajas eléctricas del DC (no están bajo llave), situación que puede ocasionar riesgos de manipulación y alteración de estas cajas por personal no autorizado,

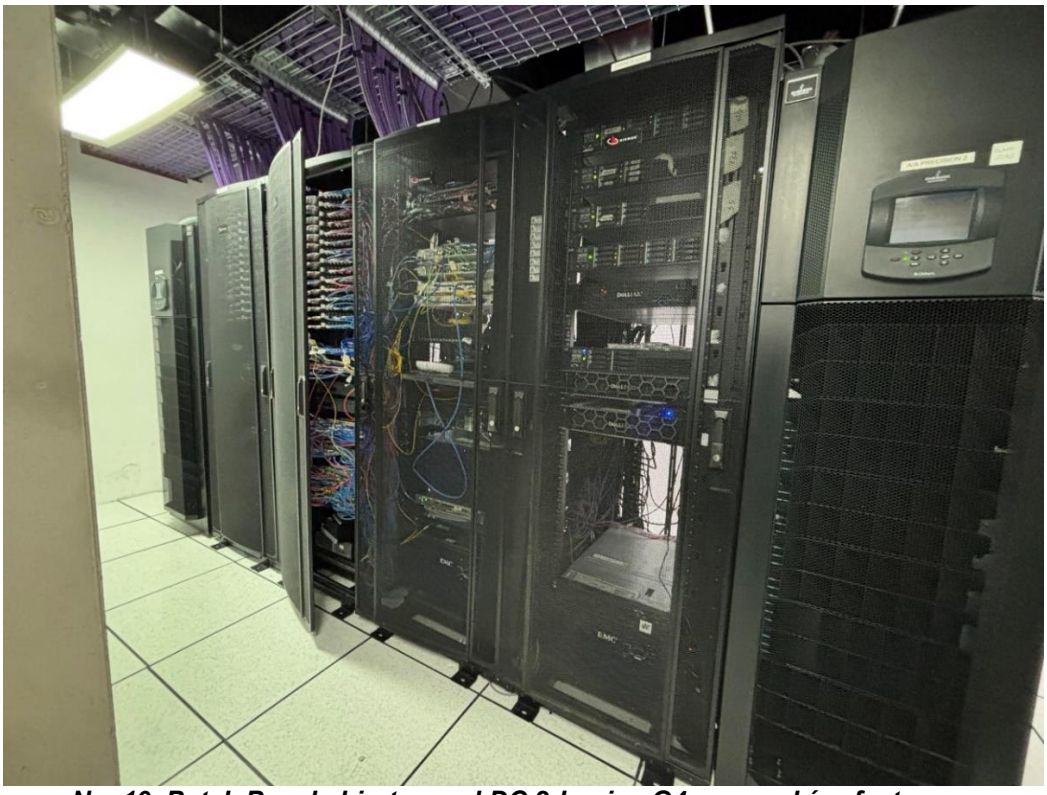


Imágenes No. 7, elementos y cajas metálicas eléctricas abiertas en el DC 2do piso G4 que trasgreden su seguridad, fuente propia, DC

Imágenes No. 8, otros elementos y equipos de cómputo en el piso en el DC 2do piso G4 que pueden afectar su seguridad y normal operación, fuente propia, DC

Imagen No. 9 cajas de cartón el cuarto de comunicaciones del 5to piso G4, fuente propia

- Mantener bajo llave los patch panel del Data Center, para evitar riesgos de manipulación y alteración de los switchs, por personal no autorizado.



Imágenes No. 10, Patch Panel abierto en el DC 2do piso G4 que podría afectar su seguridad, fuente propia, DC.

Finalmente es indispensable, mantener asegurada la puerta metálica de entrada al DC en el 2do piso, G4. El equipo auditor evidencio que estaba abierta el día de la visita de auditoría al CE, con el acompañamiento del encargado del Grupo Administrativo. Durante la visita programada de auditoría de la OCI con GTI, ya se evidenció que estaba cerrada. Esa puerta de seguridad debe permanecer continuamente cerrada, independientemente de lo que se esté gestionando de soporte o actualización de su sistema biométrico, de lo contrario, podría facilitar el acceso a personas no autorizadas, situación que pondría en riesgo la seguridad del DC.

9. Papeles de Trabajo

Los papeles de trabajo utilizados durante el ejercicio auditor reposan en el servidor dispuesto para la OCI y son los soportes del equipo auditor con base a los cuales se generaron los resultados de la auditoría.

10. Plan de Mejoramiento

Agradecemos la atención prestada y esperamos contar con su disposición para la socialización de este informe a los líderes de los procesos que fueron objeto de esta

auditoría, evaluación o seguimiento para que dentro de sus facultades analicen las observaciones presentadas y las causas identificadas, estudien la viabilidad de adoptar las recomendaciones propuestas por la Oficina de Control Interno y presenten el correspondiente Plan de Mejoramiento con el fin de corregir las situaciones presentadas en este informe y prevenir posibles desviaciones y materialización de riesgos, dentro de los cinco (5) días hábiles siguientes a la recepción del informe.

Dicho plan de mejoramiento debe ser informado por el Líder del proceso al jefe de la Oficina de Control Interno para programar su verificación en el mes siguiente de su reporte. Así mismo, que estas acciones de mejora sean incluidas en el SIPLAG.

Cordialmente,

OSCAR SALAMANCA
Jefe Oficina de Control Interno (E)

Elaboró: **Juan Gutiérrez G Líder de auditoría** .
Andrés Quiroga Apoyo a la Auditoría

Leandro Sánchez Apoyo a la Auditoría
Contratistas OCI

Revisó: ***Adriana Botero Líder Estratégico***
Contratistas OCI