UNIDAD DE SERVICIOS PENITENCIARIOS Y CARCELARIOS - USPEC

Informe Auditoría ISO 27001 y Modelo de Seguridad y privacidad de la información MSPI

BOGOTÁ D.C., AGOSTO 2026

VERSIÓN 1.0

USPEC

TABLA DE CONTENIDO

Contenido

1. DATOS GENERALES 2
2. OBJETIVO DE LA AUDITORÍA.....3
3. ALCANCE DE LA AUDITORÍA.....3
4. DECLARATORIA 3
5. CRITERIOS DE AUDITORÍA.....4
6. METODOLOGÍA Y DESARROLLO DE LA AUDITORÍA 5
6.1 Limitaciones de Auditoría (Si aplica) 37
6.2 Siglas usadas (Si aplica) 38
6.3 Riesgos del proceso e identificados por el auditor 38
6.4 Seguimiento plan de mejoramiento (Si aplica) 40
7. FORTALEZAS.....40
8. RECOMENDACIONES 40
9. CONCLUSIONES 42
10. AUTORIZACIÓN PARA COMUNICAR ESTE INFORME: 43
11. EVIDENCIAS FOTOGRÁFICAS (cuando aplique) Evidencia 44

1. DATOS GENERALES

Proceso(s) /Actividad (es) Auditado (s)	Gestión de Tecnologías de la Información y Sistema de Gestión de seguridad de la Información (SGSI). Gestión del talento Humano y Gestión contractual. Gestión de recursos físicos y suministros y Gestión de infraestructura.
Líder(es) de Proceso:	Mayra Agudelo- Seguridad de la Información. Imelda Muñoz- Oficina Tecnologías de la Información. Alejandro Montero- Coordinación de grupo administrativo. Jully Bustos
Cargo:	Oficial Seguridad de la Información Directora de la Oficina de Tecnologías de la Información (OTEC). Coordinador de grupo administrativo. Profesional Universitario.
Auditor Líder:	Walter Raúl Niño Pérez
Cargo:	Contratista Oficina control Interno
Auditores Acompañantes:	

Fecha de Apertura Auditoria	Fecha de cierre de la Auditoría
02 / 03 / 26	14 / 07 / 26

2. OBJETIVO DE LA AUDITORÍA

Evaluar el nivel de madurez, gobernanza y eficacia del Sistema de Gestión de Seguridad de la Información (SGSI), identificando brechas críticas frente a los requisitos de la norma ISO/IEC 27001:2022 que puedan constituir No Conformidades Mayores en un proceso de certificación, e identificar el grado de implementación y madurez del Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC, mediante la valoración de sus componentes estratégicos, tácticos y operativos, con el fin de generar recomendaciones para el fortalecimiento de la seguridad y privacidad de la información.

3. ALCANCE DE LA AUDITORÍA

Evaluar el diseño, implementación, operación y eficacia del Sistema de Gestión de Seguridad de la Información (SGSI) de la USPEC, verificando su alineación con los requisitos de la Norma ISO/IEC 27001:2022 y las buenas prácticas establecidas en la ISO/IEC 27002:2022, incluyendo el liderazgo de la Alta Dirección, la gobernanza del sistema, la gestión de riesgos de seguridad de la información, la gestión de activos, los controles de acceso lógico y físico, la gestión de vulnerabilidades, la continuidad de los servicios tecnológicos, la protección de la información institucional y el cumplimiento de los controles del Anexo A aplicables al alcance definido.

De manera complementaria, la auditoría incorpora la evaluación del grado de implementación y madurez del Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), mediante la verificación de los componentes de planificación, operación, evaluación del desempeño y mejoramiento continuo, así como de los mecanismos de gestión del riesgo, gobierno de la seguridad digital, respuesta a incidentes, continuidad del negocio y cumplimiento de la Política de Gobierno Digital, en aquellos aspectos que guardan relación con el Sistema de Gestión de Seguridad de la Información.

4. DECLARATORIA

- Esta auditoría fue realizada con base en la consecución y análisis de diferentes muestras aleatorias, seleccionadas por los auditores encargados de llevar a cabo el trabajo de aseguramiento.

  Una consecuencia de lo anterior, es la presencia del riesgo de muestreo; es decir, el riesgo de que la conclusión basada en la muestra analizada, no coincida con la conclusión a que se habría llegado en caso de haber evaluado todos los elementos que componen la población; sin embargo, la muestra genera una alerta frente a los resultados obtenidos.

- Es responsabilidad de cada líder de proceso el suministro y contenido de la información base del análisis del proceso de aseguramiento. La responsabilidad de la Oficina de Control Interno se circunscribe a producir un informe contentivo de los resultados de la auditoría ejecutada; las pruebas, procedimientos y análisis de la auditoría se practican de acuerdo con las normas legales vigentes de auditoría y las políticas y procedimientos formulados para el proceso de Evaluación de la Gestión Institucional /Oficina de Control Interno que se encuentran incluidos en el Sistema de Gestión Integrado de la Unidad.
- En caso, de que en el desarrollo de la auditoría se detecten asuntos no contemplados en el alcance y en los criterios de la misma, la Oficina de Control Interno tiene la obligación y el deber de informar a través del presente informe los hechos que puedan perjudicar el funcionamiento de la administración pública, de acuerdo con lo establecido en el numeral 26 del Artículo 38 de la Ley 1952 de 2019, el cual determina los deberes de los servidores públicos; de igual forma, el Artículo 231 del Decreto-Ley 019 de 2012, en el que se estipula que el Jefe de la Oficina de Control Interno "sin perjuicio de las demás obligaciones legales, deberá reportar a los organismos de control los posibles actos de corrupción e irregularidades que haya encontrado en ejercicio de sus funciones".

  Así mismo, el literal c) del Artículo 2.2.21.4.9 del Decreto 648 de 2017 "informes", señala que "Los jefes de Control Interno o quienes haga sus veces deberán presentar los informes que se relacionan a continuación: … c. sobre actos de corrupción, directiva presidencial 01 de 2015, o aquella que la modifique, adicione o sustituya…".

  Complementariamente, el Artículo 67 del Código de Procedimiento Penal, señala que el servidor público que conozca de la comisión de un delito que deba investigarse de oficio, iniciará sin tardanza la investigación si tuviere competencia para ello; en caso contrario, pondrá inmediatamente el hecho en conocimiento ante la entidad competente.

5. CRITERIOS DE AUDITORÍA

Para el desarrollo del presente ejercicio de auditoría, se establecen como puntos de referencia, marcos de buena práctica y parámetros de control, las normas de carácter legal (externas), la regulación sectorial y los documentos de gestión interna de la entidad que se enlistan a continuación, así como todas aquellas disposiciones concordantes, coincidentes y complementarias vigentes:

- **ISO/IEC 27001:2022:** *Sistemas de gestión de la seguridad de la información — Requisitos.* (Aplica para las Cláusulas 4 a 10 de la norma: Contexto, Liderazgo, Planificación, Soporte, Operación, Evaluación del Desempeño y Mejora).

- **ISO/IEC 27002:2022:** *Controles de seguridad de la información.* (Aplica para fundamentar las buenas prácticas de implementación de los 93 controles del

Anexo A, agrupados en las 4 dimensiones: *Organizacionales, Personal, Físicos y Tecnológicos*).

- **ISO/IEC 27007:2020 / ISO 19011:2018:** *Directrices para la auditoría de sistemas de gestión.* (Representan el criterio metodológico del auditor para la planificación, ejecución y redacción del informe).

- Leyes Estatales/Nacionales de Protección de Datos Personales (Habeas Data): Normativa legal vigente aplicable al tratamiento, custodia y confidencialidad de datos personales por parte de la entidad. Ley 1581 de 2012.

- Política General de Seguridad de la Información: Marco estratégico aprobado por la Alta Dirección para la protección de los activos de información. Resolución número 000008 del 9/1/2025- TI-MA-005_V1_Manual de Políticas de Seguridad de Información_copia_controlada.

- Manual y Metodología de Gestión de Riesgos Corporativos / TI: Directrices institucionales para la identificación, análisis, evaluación y tratamiento de riesgos. -GE-PO-001 Política de Administración de Riesgos

- Procedimiento de Vinculación, Movilidad Interna y Desvinculación de Personal: Manuales y flujos de trabajo del área de Gestión Humana que regulan el ingreso, cambio de rol, trámite de Paz y Salvo y retiro de colaboradores.

- Política de Uso Aceptable de Activos de Información: Reglas internas que establecen las responsabilidades de los funcionarios respecto al hardware, software y accesos asignados. -TI-MA-002 Manual de Clasificación de Activos

6. METODOLOGÍA Y DESARROLLO DE LA AUDITORÍA

Para la evaluación del Sistema de Gestión de Seguridad de la Información (SGSI) y los controles aplicables (Anexo A ISO 27001), se empleó una metodología basada en un enfoque mixto de verificación, dividida en dos modalidades complementarias: revisión documental (escritorio) y verificación en sitio (campo).

Como parte del desarrollo de la auditoría, **se incorporó la evaluación de los principales componentes del Modelo de Seguridad y Privacidad de la Información (MSPI) definido por el Ministerio TIC**, con el propósito de verificar el nivel de implementación y madurez de los controles institucionales relacionados con la gestión de la seguridad digital y su articulación con el Sistema de Gestión de Seguridad de la Información (SGSI).

Para tal efecto, se evaluaron evidencias correspondientes a las cuatro fases del modelo (Planificación, Operación, Evaluación del Desempeño y Mejoramiento

Continuo), verificando aspectos relacionados con la gestión de riesgos de seguridad de la información, inventario y clasificación de activos, gestión de incidentes, continuidad del negocio, copias de seguridad, monitoreo de eventos de seguridad, gestión de accesos, capacitación y sensibilización, evaluación de controles, auditorías internas, revisión por la dirección y acciones de mejora, entre otros elementos que soportan la implementación del SGSI.

Los controles de ISO 27001 donde se integra el MSPI permitió evaluar los siguientes controles y cláusulas de ISO 27001:

Componente MSPI	ISO 27001:2022	Controles Anexo A relacionados
Contexto y planificación	Cláusulas 4 y 6	Gestión del riesgo
Liderazgo	Cláusula 5	Gobierno del SGSI
Gestión de activos	Cláusula 8	A.5.9 a A.5.13
Gestión de riesgos	Cláusula 6	A.5.7, A.5.8
Gestión de accesos	Cláusula 8	A.5.15 a A.5.18
Concienciación	Cláusula 7	A.6.3
Seguridad física	Anexo A	Controles serie A.7
Seguridad tecnológica	Anexo A	Controles serie A.8
Gestión de incidentes	Cláusula 8	A.5.24 a A.5.28
Continuidad del negocio	Cláusulas 8 y 9	A.5.29 y A.5.30
Monitoreo y auditoría	Cláusula 9	A.8.15, A.8.16
Auditoría interna	Cláusula 9.2	ISO 19011 e ISO 27007
Revisión por la dirección	Cláusula 9.3	Gobierno del SGSI
Acciones correctivas	Cláusula 10	Mejora continua

La definición de la revisión se realizó con base en la serie de preguntas establecidas para cada control de la norma, como se evidencia en este documento:

https://docs.google.com/spreadsheets/d/1yw0JYpdqGBofy7nQkVhOOLY3kJCY26pv/edit?usp=sharing&ouid=116814403603928865905&rtpof=true&sd=true

Hallazgo 1:

Debilidades en los controles de seguridad física y restricción de acceso en las puertas de emergencia.

Condición:

Durante la inspección física realizada a las instalaciones de la entidad, se constató que las puertas de evacuación y emergencia ubicadas en los pisos 12 y 13, carecen

de controles físicos de restricción de acceso desde el exterior. Se observó que permanecen sin pasadores unidireccionales, no cuentan con alarmas por apertura prolongada y se encuentran ubicadas en puntos ciegos que no son cubiertos por las cámaras del circuito cerrado de televisión (CCTV), permitiendo el libre ingreso de personas sin pasar por los filtros de la recepción principal.

Evidencia hallazgo 1

Criterio:

ISO/IEC 27001:2022 — Anexo A — Control 7.4 (Seguridad física perimetral): El control establece textualmente que:

"Los perímetros de seguridad física se deben definir y utilizar para proteger las áreas que contienen información y otros activos asociados." Complementado por el Control

7.5 (Seguridad de los accesos físicos), el cual dictamina textualmente que: "Las áreas de acceso físico se deben proteger mediante controles de acceso y puntos de entrada apropiados."

Causa:

Priorización exclusiva de los lineamientos del edificio, sin haber diseñado e instalado una solución de ingeniería que integre diferentes requerimientos (como barras antipánico electromecánicas conectadas al sistema de incendios e intrusión).

Posibles consecuencias:

Intrusión no autorizada de terceros directamente a las áreas operativas o de custodia de infraestructura tecnológica de la organización (ej. cuartos técnicos o de servidores). Esto incrementa el riesgo de hurto físico de activos informáticos, manipulación malintencionada del hardware institucional o sabotaje perimetral de los servicios críticos, anulando la efectividad de los controles de la entrada principal de la entidad.

Hallazgo 2:

Ausencia de controles de acceso físico y falta de registros de trazabilidad en el depósito de planos históricos. (No Conformidad mayor)

Condición:

Durante la inspección física realizada a las áreas de archivo y custodia de la entidad, se constató la ausencia de controles físicos de acceso y la inexistencia de registros

de ingreso en el cuarto de planos históricos. El área evaluada carece de cerraduras restringidas (biométricas o por tarjeta de proximidad), permaneciendo vulnerable o accesible para personal no autorizado. Asimismo, se verificó que no se lleva una bitácora o libro de control (físico o digital) que permita registrar la fecha, hora, nombre del funcionario y motivo de consulta de los planos, así como tampoco se evidenciaron sistemas de monitoreo por circuito cerrado de televisión (CCTV) en dicho depósito.

Evidencia Hallazgo #2

Criterio:

ISO/IEC 27001:2022 — Anexo A — Control 7.1 (Perímetros de seguridad física): El control establece textualmente que:
Los perímetros de seguridad física se deben definir y utilizar para proteger las áreas que contienen información y otros activos asociados. Las directrices indican que la organización debe identificar sus áreas sensibles y colocar barreras físicas perimetrales sólidas para protegerlas del acceso no autorizado

ISO/IEC 27001:2022 — Anexo A — Control 7.2 (Seguridad del ingreso físico): El control establece textualmente que**:**

Las áreas seguras se deben proteger mediante controles de ingreso apropiados para garantizar que solo el personal autorizado tenga acceso. La norma exige de forma explícita que las fechas y horas de ingreso de los visitantes y del personal deben ser registradas y auditadas para mantener la trazabilidad del perímetro protegido.

ISO/IEC 27001:2022 — Anexo A — Control 7.5 (Seguridad de los accesos físicos): El control establece textualmente que:

Las áreas de acceso físico se deben proteger mediante controles de acceso y puntos de entrada apropiados. Las directrices especifican que se deben otorgar derechos de acceso solo a las personas autorizadas, y que los puntos de entrada y salida de las áreas donde se almacena información sensible deben ser registrados mediante una pista de auditoría (logs o bitácoras).

ISO/IEC 27001:2022 — Anexo A — Control 7.10 (Medios de almacenamiento): El control establece textualmente que:

Los medios de almacenamiento se deben gestionar a lo largo de su ciclo de vida de recopilación, procesamiento, almacenamiento, transporte, entrega y destrucción, de acuerdo con la clasificación de la información y los requisitos de almacenamiento de la organización. (Aplica para planos físicos en papel, microfilmes o cartografía original en custodia).

Causa:

Subestimación del valor de la información en soporte físico. La organización ha enfocado sus esfuerzos de seguridad en los activos digitales, descuidando el ciclo de vida, inventario y protección de los activos físicos históricos y de infraestructura.

Posibles consecuencias:

- Pérdida o Deterioro de Propiedad Intelectual: Riesgo de hurto, sustracción, pérdida o daño físico de planos únicos e históricos debido al libre tránsito de personas por el área, generando un detrimento en la memoria institucional de la entidad.

- Espionaje o Sabotaje de Infraestructura: Al no tener un registro de quién consulta los planos, personal malintencionado podría revisar u obtener copias de los diseños arquitectónicos, redes lógicas, sistemas de seguridad o rutas eléctricas de la entidad, facilitando la planificación de ataques lógicos o físicos contra las instalaciones.

- Pérdida de Trazabilidad: Imposibilidad de realizar una investigación forense o identificar responsabilidades administrativas ante la desaparición o alteración de un plano confidencial, al no existir una pista de auditoría física de quién ingresó al cuarto de custodia.

Hallazgo 3:

Inexistencia de un proceso de depuración y gestión periódica de cuentas de usuario inactivas en las plataformas tecnológicas de la entidad. (No Conformidad Mayor)

Condición:

Se identificó que la entidad no realiza un proceso de depuración, deshabilitación o eliminación periódica de cuentas de usuario que se encuentran inactivas o sin uso en el Directorio Activo y en los sistemas de información misionales. Tras una revisión por muestreo, se detectaron cuentas asociadas a personal externo, contratistas y exempleados que siguen siendo identificadas por la entidad y que tienen vigencia de hace mucho tiempo.

Evidencia hallazgo # 3

Criterio:

ISO/IEC 27001:2022 — Anexo A — Control 8.13 (Gestión de derechos de acceso): El control establece textualmente que:

Los derechos de acceso a la información y otros activos asociados se deben revisar a intervalos periódicos o ante cambios significativos." Las directrices especifican que las cuentas inactivas deben ser deshabilitadas o eliminadas de manera oportuna para evitar su explotación indebida.

Causa:

Inexistencia de un procedimiento formal y automatizado para el aprovisionamiento y des aprovisionamiento de usuarios (ciclo de vida de la identidad). El área de TI opera de manera reactiva, ejecutando las bajas de cuentas únicamente cuando recibe una solicitud explícita por correo electrónico de Gestión Humana o de los jefes inmediatos, omitiendo la realización de auditorías de cuentas y revisiones de acceso rutinarias o programadas sobre la base total de usuarios.

Posibles consecuencias:

- Acceso Remoto No Autorizado: Exposición crítica de la red corporativa frente a conexiones externas no autorizadas si un excolaborador utiliza sus credenciales históricas (o si estas son comprometidas mediante ataques de fuerza bruta) para ingresar a los aplicativos de la entidad desde internet.

- Vulneración de la Trazabilidad y No Repudio: Si una cuenta inactiva o huérfana es utilizada para cometer un fraude, alteración de datos o fuga de información, las bitácoras (logs) registrarán el nombre del exempleado, imposibilitando la identificación del verdadero atacante técnico y viciando la validez legal de las pistas de auditoría.

- Puerta de Entrada para Malware: Las cuentas inactivas suelen carecer de políticas actualizadas de cambio de contraseña o doble factor de autenticación (MFA), lo que las convierte en el blanco preferido de los ciberdelincuentes para establecer persistencia dentro de la infraestructura tecnológica de la entidad.

Hallazgo 4:

Falta de Actualización y Revisión de Documentos Clave del SGSI. Un Sistema de Gestión de Seguridad de la Información cuyos documentos clave (políticas, manuales, análisis de riesgos) están desactualizados se convierte en un sistema "de papel". (No Conformidad Mayor)

Condición:

Se evidenció la falta de actualización, revisión periódica y formalización de los documentos estratégicos y operativos clave del Sistema de Gestión de Seguridad de la Información (SGSI) de la entidad. Al revisar el repositorio documental del SGSI, se identificó que políticas críticas (tales como el manual de Políticas de Seguridad de

la Información, la Política de Control de Accesos y el Manual de Gestión de Incidentes) presentan fechas de última revisión superiores a los plazos establecidos internamente, carecen de firmas de aprobación por parte de la Alta Dirección y no contemplan los cambios tecnológicos e institucionales recientes de la organización.

Evidencia hallazgo #4

Criterio:

- **ISO/IEC 27001:2022 — Anexo A — Control 5.1 (Políticas para la seguridad de la información):** El control establece textualmente que:

  La política de seguridad de la información y las políticas específicas del tema se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su idoneidad, adecuación y eficacia continuas."

- **ISO/IEC 27001:2022 — Anexo A — Control 5.36 (Cumplimiento de políticas y normas de seguridad):** El control establece textualmente que:

  El cumplimiento de la política de seguridad de la información de la organización, las políticas específicas del tema, las normas y las operaciones se deben revisar periódicamente. Las directrices exigen que los administradores verifiquen que los procesos cumplan con las políticas y que estas mantengan su vigencia legal y operativa.

- **ISO/IEC 27001:2022 — Numeral 7.5.2 (Creación y actualización):** La norma establece textualmente que al crear y actualizar la información documentada, la organización debe asegurarse de que lo siguiente sea apropiado:

  c) La revisión y aprobación con respecto a la idoneidad y adecuación."

- **ISO/IEC 27001:2022 — Numeral 7.5.3 (Control de la información documentada):** Establece textualmente que la información documentada requerida por el SGSI se debe controlar para asegurarse de que:

  a) Esté disponible y sea idónea para su uso, dónde y cuándo se necesite; y b) Esté protegida adecuadamente". Para el control de la información documentada, la organización debe abordar actividades como el almacenamiento, preservación, control de cambios, revisión e idoneidad.

Causa:

Ausencia de una cultura de gobernanza documental y de un cronograma automatizado de revisiones obligatorias por parte del Oficial de Seguridad de la Información (CISO) o el Comité de Seguridad. El proceso de actualización se ejecuta de manera reactiva ante incidentes o auditorías externas, y no como parte de un ciclo proactivo de mejora continua, sumado a la falta de asignación de tiempos formales para que los dueños de procesos revisen sus respectivas guías y procedimientos.

Posibles consecuencias:

- Inoperatividad e Ineficacia de Controles: El personal operativo podría estar ejecutando sus labores con base en directrices obsoletas que no responden a la arquitectura tecnológica actual de la entidad, lo que genera fallas de control y errores de configuración en los sistemas.

- Desalineación frente a Nuevas Amenazas: Al no actualizar los documentos clave, se omiten controles para mitigar amenazas tecnológicas emergentes (como riesgos asociados al uso de Inteligencia Artificial, computación en la nube o teletrabajo), dejando desprotegido el entorno digital de la organización.

- Pérdida de Respaldo Legal e Institucional: Si las políticas generales no cuentan con la firma de aprobación de la Alta Dirección vigente, carecen de validez legal vinculante para exigir su cumplimiento obligatorio ante los colaboradores o para aplicar sanciones disciplinarias en caso de infracciones.

Hallazgo 5:

Acceso de terceros no autorizado, sin trazabilidad ni supervisión técnica al Controlador de Dominio principal. (No Conformidad Mayor)

Condición:

Se detectó el acceso no autorizado, no registrado y sin supervisión técnica por parte de un proveedor externo (tercero) al Controlador de Dominio principal de la entidad. Durante las pruebas de auditoría al proceso de restablecimiento de contraseña, se constató que el personal del tercero ejecutó labores de mantenimiento y modificaciones de configuración directamente sobre el Directorio Activo utilizando credenciales de nivel Administrador de Dominio (Admin), sin contar con una solicitud formal aprobada, sin la presencia física o remota de un supervisor del área de TI de la entidad, y sin que se activara un mecanismo de grabación de sesión o acompañamiento para validar las acciones realizadas.

Evidencia Hallazgo #5

Criterio:

- **ISO/IEC 27001:2022 — Anexo A — Control 5.21 (Seguridad de la**

información en las relaciones con proveedores): El control establece textualmente que:

Se deben definir e implementar procesos y procedimientos de seguridad de la información para mitigar los riesgos asociados con el acceso de los proveedores a los activos de la organización.

- **ISO/IEC 27001:2022 — Anexo A — Control 8.12 (Privilegios de acceso especiales):** El control establece textualmente que:

  La asignación y el uso de privilegios de acceso especiales se deben restringir y controlar estrictamente. Las directrices indican que los accesos con máximos privilegios por parte de terceros deben ser autorizados caso por caso, ser temporales y estar bajo supervisión directa.

- **ISO/IEC 27001:2022 — Anexo A — Control 8.18 (Uso de programas de utilidad con privilegios):** El control establece textualmente que:

  El uso de programas de utilidad que puedan tener la capacidad de anular los controles del sistema y de la aplicación se debe restringir y controlar estrictamente. (Aplica para herramientas de administración global del Controlador de Dominio).

Causa:

Ausencia de un procedimiento riguroso para la gestión de accesos remotos o locales de terceros proveedores, sumado a la falta de herramientas de monitoreo en tiempo real (como soluciones PAM - Privileged Access Management) o bitácoras de auditoría automatizadas que alerten sobre la elevación y uso de privilegios críticos por personal externo.

Posibles consecuencias:

- Pérdida Total de Confidencialidad e Integridad de las Credenciales: Un tercero sin supervisión tiene la capacidad técnica de extraer la base de datos de contraseñas de toda la entidad, crear usuarios administradores ocultos ("puertas traseras"), o modificar las políticas de grupo (GPO) para debilitar la seguridad de todas las estaciones de trabajo.
- Riesgo de Interrupción Catastrófica: Cualquier error humano o configuración errónea accidental ejecutada por el tercero en el Controlador de Dominio puede derribar la autenticación de toda la organización, impidiendo que los funcionarios inicien sesión, accedan al correo o utilicen los aplicativos del negocio, paralizando la operación por completo.
- Anulación del Principio de Responsabilidad y No Repudio: Al permitir que un externo use cuentas genéricas de administrador o ingrese sin supervisión ni grabación de video de su sesión, la entidad no puede atribuir legal ni administrativamente la responsabilidad en caso de un sabotaje, fuga de datos

o alteración malintencionada de la red

Hallazgo 6:

Inexistencia de matrices de roles y perfiles para la asignación formal de accesos y privilegios en la infraestructura tecnológica. (No Conformidad Mayor)

Condición:

Se identificó mediante entrevistas y verificación en sitio, la ausencia de Matrices de Roles y Responsabilidades (Matrices de Accesos / RBAC) formalizadas y actualizadas para regular la asignación de permisos, perfiles y privilegios en los sistemas de información institucionales, bases de datos y en el Directorio Activo de la entidad. Las autorizaciones de acceso se realizan bajo criterios subjetivos u órdenes verbales/escritas sin un estándar técnico preconcebido, propiciando que los usuarios acumulen privilegios que no corresponden estrictamente a sus funciones actuales o que exceden las necesidades reales de su cargo: adicionalmente no se evidenciaron perfiles estándar por cargo, criterios documentados para la asignación y revocación de privilegios, ni un mecanismo formal para la revisión periódica de los accesos otorgados a los usuarios.

Evidencia hallazgo # 6:

Criterio:

- **ISO/IEC 27001:2022 — Anexo A — Control 5.15 (Control de acceso):** El control establece textualmente que:

  Las reglas para controlar el acceso físico y lógico a la información y otros activos asociados se deben definir e implementar de acuerdo con las necesidades del negocio y de la seguridad de la información. Las directrices señalan que las reglas de control de acceso deben considerar los requisitos de los roles de los usuarios (need-to-know).

- **ISO/IEC 27001:2022 — Anexo A — Control 8.11 (Aprovisionamiento de acceso):** El control establece textualmente que:

  La asignación y revocación de los derechos de acceso se deben realizar de acuerdo con la política de control de acceso de la organización, incluyendo perfiles de usuario estándar para categorías de roles comunes.

Causa:

Falta de una estrategia de Gobernanza de Identidades y Accesos (IAM) coordinada entre el área de Talento Humano (propietaria de los perfiles de puesto) y el área de TI (ejecutora técnica). No se ha definido un proyecto formal para el levantamiento de un modelo de Control de Acceso Basado en Roles (RBAC).

Posibles consecuencias:

- Violación del Principio de Segregación de Funciones: Al no existir una matriz que limite los roles, un mismo usuario podría quedar habilitado en el sistema para ejecutar acciones incompatibles entre sí, tales como registrar un proveedor y autorizar su pago, o crear un usuario y auto-aprobarse permisos, facilitando la ejecución de fraudes internos sin control cruzado.
- Privilegios Acumulativos: Cuando los colaboradores cambian de área o ascienden, el área de TI les asigna los nuevos accesos pero omite remover los anteriores por falta de una matriz de referencia, generando usuarios con excesivo poder lógico dentro de las plataformas de la entidad.
- Inviabilidad de Auditorías de Accesos: Control Interno no cuenta con un parámetro objetivo ("el deber ser") para contrastar si los permisos actuales de un funcionario son correctos o abusivos, viciando la efectividad de las revisiones de seguridad periódicas.

Hallazgo 7:

Deficiencias en el seguimiento, monitoreo y supervisión periódica de la seguridad de la información en la gestión de proveedores externos. (No Conformidad Mayor)

Condición:

Se evidenció a través de entrevistas y verificación de informes mensuales de seguimiento a la ejecución del contrato, la ausencia de un proceso periódico de seguimiento, monitoreo y supervisión a la *gestión de seguridad de la información* ejercida por los proveedores externos (terceros) por parte de las áreas propietarias del servicio (supervisores de contrato) y del área de Seguridad de la Información. Al revisar en campo el seguimiento contractual de los proveedores clave del último período, no se hallaron evidencias documentales de la realización de auditorías revisión de certificaciones o evidencias relacionadas con la seguridad de la información durante la ejecución contractual.

En la revisión de los expedientes contractuales y de la documentación suministrada por las áreas responsables no se evidenciaron registros que demostraran la ejecución periódica de actividades tales como:

- Revisiones de cumplimiento de los controles de seguridad definidos contractualmente;
- Evaluaciones periódicas de riesgos asociados a terceros;

- Seguimiento a incidentes de seguridad que involucren al proveedor;
- verificación de la vigencia de compromisos de confidencialidad cuando corresponda;
- Revisión de certificaciones o evidencias relacionadas con la seguridad de lainformación durante la ejecución contractual.

Lo anterior evidencia la inexistencia de un mecanismo formal de supervisión continua de los riesgos asociados a terceros.

Evidencia hallazgo 7

Criterio:

- **ISO/IEC 27001:2022 — Anexo A — Control 5.21 (Gestión de la seguridad de la información en las relaciones con proveedores):** El control establece textualmente que:

  Se deben definir e implementar procesos y procedimientos de seguridad de la información para mitigar los riesgos asociados con el acceso de los proveedores a los activos de la organización.

- **ISO/IEC 27001:2022 — Anexo A — Control 5.22 (Monitoreo y revisión de servicios de proveedores):** El control establece textualmente que:

  La organización debe monitorear, revisar y auditar periódicamente la prestación de servicios de los proveedores para garantizar que se cumplan las políticas y los requisitos de seguridad de la información." Las directrices señalan que se deben revisar de forma recurrente los informes de servicio, los registros de incidentes y las evaluaciones de vulnerabilidades realizadas por o sobre los terceros.

Causa:

Inexistencia de un procedimiento formal de Supervisión de Riesgo de Terceros que asigne responsabilidades explícitas a los supervisores de contrato. Las áreas de la entidad perciben la gestión de proveedores como un trámite administrativo que concluye con la firma del contrato y el informe de facturación mensual, mientras que el área de Seguridad de la Información no cuenta con un cronograma formal de auditorías o listas de chequeo periódico aplicables a la base de contratistas activos.

Posibles consecuencias:

- Transferencia Involuntaria de Riesgos No Controlados: La entidad queda expuesta de forma ciega a las vulnerabilidades, malas prácticas o brechas de

seguridad que sufra el proveedor en sus propios entornos, perdiendo la capacidad de reaccionar preventivamente antes de que ocurra un incidente que impacte a la organización.

- Incumplimiento Inadvertido de Niveles de Servicio (SLA) y Acuerdos de Confidencialidad: Imposibilidad de validar si el tercero está cumpliendo con la encriptación de datos, la gestión de parches en los sistemas arrendados o las copias de seguridad prometidas en el contrato, dejando a la entidad en un estado de indefensión técnica.
- Incapacidad de Exigencia Legal: Si ocurre un incidente originado en la infraestructura del proveedor, la entidad no podrá justificar la debida diligencia ante entes de control o reguladores al no contar con un expediente de supervisión y monitoreo continuo.

Hallazgo 8:

Inexistencia de un procedimiento formal para la modificación y revocación oportuna de privilegios de acceso en procesos de movilidad interna. (No Conformidad Menor)

Condición:

Se identificó la falta de un procedimiento formal para la modificación, ajuste y revocación oportuna de los derechos de acceso lógico de los colaboradores cuando son objeto de movilidad interna (traslados de dependencia, promociones o cambios de funciones). Como resultado del muestreo efectuado sobre usuarios con movilidad interna, se verificó que algunos funcionarios que fueron trasladados de áreas operativas a áreas administrativas conservaban activos perfiles, roles y permisos de acceso —incluidos permisos de escritura sobre carpetas compartidas y aplicativos— correspondientes a sus funciones anteriores, sin evidenciarse una revisión formal de la pertinencia de dichos privilegios.

Evidencia hallazgo #8

Criterio:

- **ISO/IEC 27001:2022 — Anexo A — Control 5.18 (Gestión de derechos de acceso):** El control establece textualmente que**:**

- "Los derechos de acceso a la información y otros activos asociados se deben revisar a intervalos periódicos o ante cambios significativos, tales como un cambio de empleo o de rol." Las directrices de la norma especifican de forma explícita que: "Los derechos de acceso para una persona que cambia de rol dentro de la organización deben ser modificados o revocados en función del nuevo rol."

- **ISO/IEC 27001:2022 — Anexo A — Control 8.11 (Aprovisionamiento**

de acceso): El control establece textualmente que**:**
bajo el principio de necesidad de conocer).

Causa:

Inexistencia de un procedimiento formalizado para la gestión de movimientos internos coordinado entre Talento Humano y TI. Actualmente, el proceso de onboarding (ingreso) y offboarding (retiro) está parcialmente mapeado, pero se omiten las directrices de control para los cambios de rol dentro de la misma entidad, delegando la responsabilidad en el usuario o en la memoria del jefe anterior.

Posibles consecuencias:

- Acumulación excesiva de privilegios, donde un usuario de larga trayectoria termina poseyendo accesos a casi toda la infraestructura de la entidad sin requerirlos para su función actual.

- Ruptura de la Segregación de Funciones Inter-área: Un funcionario trasladado de un área operativa hacia un área de auditoría, pagos o control interno, podría mantener la capacidad técnica de ejecutar o modificar transacciones que ahora le corresponde supervisar, anulando el control cruzado institucional.

- Contaminación de las Pistas de Auditoría (Audit Trails): En caso de un incidente de seguridad en la dependencia anterior, la presencia de accesos vigentes de ex-integrantes dificulta el análisis forense y la imputación de responsabilidades, al existir usuarios "extraños" a la operación actual con acceso legítimo desde el punto de vista del sistema.

Hallazgo 9:

Ausencia de un plan periódico de pruebas y verificación de integridad para la recuperación de copias de seguridad. (No Conformidad Mayor)

Condición:

Se constató la ausencia de un plan periódico de pruebas de restauración y verificación de la integridad de las copias de seguridad (backups) de las bases de datos, aplicaciones centrales e infraestructura de la entidad. Aunque la organización ejecuta rutinas automatizadas de respaldo diario, el área de Tecnología de la Información no realiza ejercicios simulados ni mantiene evidencias documentales (bitácoras o actas de prueba) que certifiquen que la información contenida en los medios de almacenamiento de respaldo sea 100% legible, consistente y operable en caso de requerirse una recuperación ante desastres.

Evidencia hallazgo #9

Criterio:

- **ISO/IEC 27001:2022 — Anexo A — Control 8.14 (Copia de seguridad de la información):** El control establece textualmente que:

  "Se deben mantener y probar regularmente copias de seguridad de la información, el software y las imágenes del sistema de acuerdo con la política de copia de seguridad acordada."
  Las directrices de la norma especifican de forma explícita que las pruebas de restauración no solo deben verificar la capacidad de recuperar los datos, sino también la integridad y el tiempo necesario para completar la restauración, alineándose con los objetivos de tiempo de recuperación (RTO) del negocio.

Causa:
Falta de inclusión de las pruebas de recuperación dentro de la carga operativa rutinaria de TI, la ausencia de un entorno de pruebas (Sandboxing o ambiente de pruebas) dedicado a la restauración y falta de un plan o calendario formalizado de pruebas de restauración de datos. No se ha establecido un procedimiento institucional que defina la planificación, ejecución, documentación y seguimiento de pruebas periódicas de restauración de copias de seguridad, incluyendo responsables, frecuencia, criterios de aceptación y tratamiento de resultados.

Posibles consecuencias:

- Incapacidad de Recuperación ante Incidentes de Ransomware o Desastres: En caso de un cifrado masivo de servidores o una falla catastrófica de hardware, la entidad corre el riesgo de descubrir que los archivos de respaldo estaban corruptos, incompletos o inaccesibles (por ejemplo, por pérdida de la clave de cifrado del backup), resultando en la pérdida irrecuperable de la información institucional.

- Superación del Tiempo Máximo de Interrupción Tolerable (RTO): Al no haber ensayado el proceso de restauración previamente, el tiempo real necesario para levantar los sistemas en una emergencia puede tomar días o semanas en lugar de horas, paralizando la prestación de servicios públicos/corporativos y desbordando las metas del Plan de Continuidad del Negocio (BCP).

- Incertidumbre sobre la Integridad de los Datos: Riesgo de restaurar copias de seguridad que contengan inconsistencias lógicas en las bases de datos (pérdida de relaciones de tablas, transacciones a medias), lo que corrompería la información operativa del negocio al intentar reanudar servicios.

Hallazgo 10:

Inexistencia de un Plan de Continuidad del Negocio (BCP), Análisis de Impacto (BIA) y esquemas de contingencia operativa (No Conformidad Mayor).

Condición:

Se identificó la inexistencia de un Plan de Continuidad del Negocio (BCP - Business Continuity Plan) formalizado, probado y actualizado, así como la falta de planes de contingencia operativos y un Análisis de Impacto en el Negocio (BIA - Business Impact Analysis) en la entidad. Ante la ocurrencia de un evento disruptivo mayor (ej. ciberataque masivo, caída prolongada del centro de cómputo, indisponibilidad de proveedores críticos o desastres naturales), la organización no cuenta con estrategias preestablecidas, sitios alternos de operación, procedimientos de trabajo en contingencia manual ni tiempos máximos tolerables de interrupción (RTO / RPO) definidos para garantizar la continuidad de sus funciones misionales. Igualmente, no se evidenciaron documentos correspondientes al Análisis de Impacto al Negocio (BIA), definición de Objetivos de Tiempo de Recuperación (RTO), Objetivos de Punto de Recuperación (RPO), estrategias de continuidad, procedimientos de operación en contingencia ni evidencias de pruebas periódicas del plan.

Evidencia hallazgo # 10

Criterio:

- **ISO/IEC 27001:2022 — Anexo A — Control 5.29 (Continuidad de la seguridad de la información):** El control establece textualmente que:

  "La organización debe planificar, implementar, mantener y probar la continuidad de la seguridad de la información durante un evento de disrupción o crisis."

- **ISO/IEC 27001:2022 — Anexo A — Control 5.30 (Preparación de las TIC para la continuidad del negocio): El control establece textualmente que:**

  "La preparación de las TIC se debe planificar, implementar, mantener y probar periódicamente sobre la base de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC." Las directrices exigen la definición explicita del Recovery Time Objective (RTO) y Recovery Point Objective (RPO) para los procesos y sistemas críticos.

Causa:

Ausencia de una visión de gestión integral de riesgos de desastre y resiliencia organizacional por parte de la Alta Dirección y las áreas líderes de proceso. Se ha delegado erróneamente la responsabilidad de la continuidad de forma exclusiva en el área de TI (asumiendo que los backups son suficientes), omitiendo la necesidad de estructurar un plan estratégico que involucre el componente operativo, logístico, administrativo y legal de toda la entidad.

La entidad no ha definido ni implementado un proceso institucional para la gestión de continuidad del negocio que establezca responsabilidades, metodologías y recursos para el análisis de impacto, la definición de estrategias de continuidad y la ejecución periódica de pruebas

Posibles consecuencias:

- Parálisis Operativa Prolongada e Indefinida: Ante un incidente de gran magnitud, la entidad carecerá de un "hoja de ruta" sobre cómo operar en contingencia, lo que resultará en el cierre indefinido de trámites, servicios o líneas de negocio, afectando directamente la misión institucional.

- Toma de Decisiones Improvisadas y Caóticas en Crisis: La falta de roles, comités de crisis y canales de comunicación previamente asignados propiciará un escenario de descoordinación interna, donde los líderes responderán bajo criterios empíricos, incrementando las pérdidas operativas y el riesgo reputacional.

- Pérdida Incalculable de Datos e Información Operativa: Al no tener calculados formalmente los Objetivos de Punto de Recuperación (RPO), la reconstrucción de la información perdida durante una caída del sistema puede requerir reprocesar semanas o meses de datos operativos, con el consiguiente margen de error y costo operativo.

Hallazgo 11:

Uso de credenciales compartidas y cuentas genéricas para el acceso a sistemas de información institucionales (No Conformidad Mayor).

Condición:

Durante la auditoría se evidenció el uso de credenciales compartidas para el acceso a sistemas de información institucionales. En las pruebas efectuadas sobre el Sistema de Información "Humano" se verificó que varios funcionarios utilizaban una misma cuenta de usuario para acceder al aplicativo, compartiendo las credenciales de autenticación entre diferentes personas.

Esta situación impide identificar de manera individual al responsable de las operaciones ejecutadas en el sistema y compromete la trazabilidad de las

actividades realizadas.

Evidencia hallazgo #11

Criterio:

- **ISO/IEC 27001:2022 — Anexo A — Control 8.5 (Autenticación segura):** El control establece textualmente que:

  "Las tecnologías y procedimientos de autenticación segura se deben implementar en función de las restricciones de control de acceso y los requisitos del negocio." Prohíbe expresamente el uso compartido de credenciales que anule la capacidad de auditar accesos individuales.

- **ISO/IEC 27001:2022 — Anexo A — Control 5.16 (Gestión de identidades).** El control establece textualmente que:

  "El ciclo de vida completo de las identidades se debe gestionar mediante la organización."

- **ISO/IEC 27001:2022 — Anexo A — Control 5.17 (Información de autenticación).** El control establece textualmente que:

  "La asignación y gestión de la información de autenticación se debe controlar mediante un proceso de gestión formal, incluyendo el asesoramiento al personal sobre el manejo adecuado de la información de autenticación."

- **ISO/IEC 27001:2022 — Anexo A — Control 5.18 (Derechos de acceso).** El control establece textualmente que:

  "Los derechos de acceso a la información y a otros recursos asociados se deben aprovisionar, revisar, modificar y eliminar de acuerdo con la política de control de acceso específica de la organización."

Causa:

Ausencia de lineamientos institucionales efectivos para garantizar el uso exclusivo de credenciales individuales, así como debilidades en la administración de cuentas de usuario y en los mecanismos de supervisión del cumplimiento de la política de control de acceso

Posibles consecuencias:

- Destrucción Total del No Repudio y de las Pistas de Auditoría (*Audit Trails*): En

caso de presentarse una alteración maliciosa de datos, un borrado de registros financieros o una transacción fraudulenta, las bitácoras (*logs*) del sistema registrarán únicamente la cuenta genérica o compartida. Esto imposibilita vincular la falta a una persona física específica, anulando cualquier proceso disciplinario o legal por falta de prueba directa.

- Exposición Masiva por Fuga de Credenciales: Cuando una contraseña es compartida entre varias personas, el riesgo de que sea interceptada, filtrada o utilizada fuera del horario laboral aumenta exponencialmente. Además, si un funcionario renuncia o es despedido, conserva la contraseña activa para ingresar remotamente, a menos que se cambie la clave de forma inmediata para todos los demás usuarios (lo cual raras veces ocurre).

- Imposibilidad de Asignación Diferenciada de Roles: El uso de una cuenta común impide limitar los permisos según el perfil de cada persona, otorgando a todos los usuarios de esa cuenta el nivel máximo de privilegios del grupo.

Hallazgo 12:

Ausencia de procedimientos formalizados para el control de acceso físico a áreas seguras e infraestructura crítica. (No Conformidad Menor)

Condición:

Se evidenció la ausencia de procedimientos documentados, formalizados y aprobados que regulen el control de acceso físico a las sedes de la entidad y, de manera crítica, a las áreas aseguradas de procesamiento de información (Centro de Cómputo/Data Center, cuartos de cableado y archivo central de documentos). Si bien existen controles físicos perimetrales (como lectores de tarjetas y lectores biométricos), el personal del grupo administrativo y los administradores de TI operan basándose en el conocimiento informal, sin directrices claras sobre la autorización, registro y revocación de accesos físicos para empleados, contratistas y visitantes, sin contar con:

- Listas de autorización previa para zonas restringidas.
- Protocolos estandarizados para el registro y control de ingreso/salida de activos tecnológicos.
- Bitácoras obligatorias de registro de visitantes con nivel de detalle adecuado (sin verificación de documento de identidad ni motivo de la visita).

Evidencia hallazgo 12

Criterio:

- **ISO/IEC 27001:2022 — Anexo A — Control 7.1 (Perímetros de**

seguridad física): El control establece textualmente que:

"Se deben definir e implementar perímetros de seguridad física para proteger las áreas que contienen información y otros activos asociados."

- **ISO/IEC 27001:2022 — Anexo A — Control 7.2 (Entrada física):** El control establece textualmente que:

  "Las áreas aseguradas se deben proteger mediante controles de entrada adecuados para garantizar que solo se permita el acceso al personal autorizado." Las directrices exigen que los accesos físicos estén regulados por procedimientos claros que incluyan la identificación obligatoria, registro en bitácoras y la delimitación de autorización según el rol del visitante.

- **ISO/IEC 27001:2022 — Anexo A — Control 7.4 (Monitoreo de la seguridad física):** El control establece textualmente que:

  "Las instalaciones se deben monitorear continuamente para detectar accesos físicos no autorizados."

- **ISO/IEC 27001:2022 — Anexo A — Control 7.3 (Protección de oficinas, salas e instalaciones)** El control establece textualmente que: "Se deben diseñar e implementar medidas de seguridad física para oficinas, salas e instalaciones."

Causa:

Falta de gobernanza en seguridad física y una dependencia excesiva en la memoria institucional o procesos verbales. No se ha priorizado la documentación de los controles operativos de las áreas seguras dentro del Sistema de Gestión de Seguridad de la Información (SGSI).

Posibles consecuencias:

- Exposición Directa de la Infraestructura Crítica: Personas ajenas a la operación técnica pueden ingresar a áreas sensibles (servidores, redes, archivos físicos) por falta de un protocolo de validación previo, abriendo la puerta a actos de sabotaje, robo o desconexión accidental de equipos.

- Incapacidad de Trazabilidad e Investigación Forense: Ante la pérdida de un equipo, la manipulación no autorizada de un servidor o la extracción no autorizada de documentación física, la entidad no cuenta con bitácoras confiables ni registros auditables que permitan identificar quién estuvo presente en el lugar y momento del incidente.

- Riesgo de Introducción de Dispositivos Maliciosos: Sin un control físico estricto, cualquier visitante o contratista no supervisado puede conectar hardware malicioso (como keyloggers físicos o sniffers de red) directamente a los conmutadores (switches) o servidores institucionales.

Hallazgo 13:

Deficiencias en el control y trazabilidad del ingreso y salida de activos tecnológicos en las instalaciones de la entidad. (No Conformidad Menor).

Condición:

Se evidenció la ausencia de un mecanismo formalizado de control, autorización y registro sobre el flujo de ingreso y salida de dispositivos tecnológicos (computadores portátiles, servidores, discos duros externos, componentes de red y medios de almacenamiento extraíbles) en las sedes de la entidad. Durante las pruebas de recorrido e inspección en los puestos de control de seguridad física, se constató que el personal administrativo no exige paz y salvos, pases de salida firmados ni realiza la verificación física de los números de serie de los activos que son extraídos o ingresados por funcionarios, contratistas o proveedores de mantenimiento.

Durante la auditoría se evidenció que la entidad no dispone de un procedimiento formal para la autorización, registro y verificación del ingreso y salida de activos tecnológicos de sus instalaciones.

En los recorridos realizados a los puestos de control se observó que, para la extracción o ingreso de equipos tecnológicos por parte de funcionarios, contratistas y proveedores, no se aplicaban controles documentados tales como la validación de autorizaciones de salida, la verificación de números de serie o la existencia de registros que permitieran la trazabilidad del movimiento de dichos activos.

Evidencia hallazgo # 13

Criterio:

- **ISO/IEC 27001:2022 — Anexo A — Control 7.9 (Seguridad de los activos fuera de las instalaciones):** El control establece textualmente que:

  "Se deben proteger los activos fuera de las instalaciones, teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización." Las directrices especifican que la extracción de activos tecnológicos debe contar con la autorización previa del responsable del activo y mantenerse un registro estricto de su movimiento.

- **ISO/IEC 27001:2022 — Anexo A — Control 7.10 (Medios de almacenamiento):** El control establece textualmente que:

"Los medios de almacenamiento se deben gestionar de acuerdo con la clasificación de la información y los requisitos de manejo de la organización, desde su adquisición, uso, transporte y eliminación."

Causa:

Falta de alineación y procedimientos operativos conjuntos entre el área de Seguridad Física (grupo administrativo) y la Dirección de TI/Seguridad de la Información. No se han definido políticas perimetrales que restrinjan la introducción de hardware ajeno o la extracción de propiedad de la entidad. Se carece de un procedimiento estandarizado de " Salida de Activos" y de un sistema de etiquetado/inventario unificado que permita al personal encargado validar en tiempo real si un equipo portátil o servidor tiene autorización legal para salir de la sede.

Posibles consecuencias:

- Pérdida Inadvertida de Patrimonio (Hurto de Activos): Riesgo de sustracción o pérdida de equipos portátiles, periféricos o componentes de cómputo sin que la entidad pueda identificar de inmediato el activo faltante ni la persona responsable de su extracción.

- Fuga de Información Confidencial por Extracción de Dispositivos: Dispositivos o discos duros que salen de las instalaciones sin cifrar pueden ser perdidos, robados o vendidos, dejando expuesta información clasificada, bases de datos de ciudadanos o propiedad intelectual.

- Introducción de Dispositivos Infectados a la Red Corporativa: Permite que funcionarios o terceros ingresen e interconecten computadores personales (BYOD) o dispositivos de red no autorizados ni auditados por TI, los cuales pueden contener malware, spyware o configuraciones que vulneren el perímetro de ciberseguridad.

Hallazgo 14:

Deficiencias en los procedimientos para la destrucción segura de documentos físicos que contienen información sensible. (No Conformidad Menor).

Condición:

Se identificó la ausencia de un procedimiento formalizado, regulado y supervisado para la destrucción e inactivación segura de documentos físicos que contienen información confidencial, reservada o datos personales.

Durante la auditoría se evidenció que la entidad no dispone de un procedimiento documentado que establezca los controles para la destrucción segura de documentos físicos que contienen información clasificada, reservada o datos personales.

Asimismo, durante los recorridos efectuados y la revisión documental no se evidenciaron lineamientos sobre los métodos autorizados de destrucción, registros de eliminación, responsables del proceso ni mecanismos de supervisión para garantizar la disposición segura de este tipo de documentos.

Evidencia hallazgo #14

Criterio:

- **ISO/IEC 27001:2022 — Anexo A — Control 7.14 (Reutilización o eliminación segura de dispositivos):** El control establece textualmente que:

  "Los elementos que contengan medios de almacenamiento se deben verificar para garantizar que los datos sensibles y el software licenciado se hayan eliminado o sobrescrito de forma segura antes de su eliminación o reutilización." Las directrices de la norma extienden este principio a la destrucción de soportes físicos impresos que contengan información clasificada, exigiendo métodos de destrucción (como trituración de corte cruzado o incineración) que impidan la reconstrucción del documento.

- **ISO/IEC 27001:2022 — Anexo A — Control 5.12 (Clasificación de la información):** El control establece textualmente que:

  "La información se debe clasificar de acuerdo con las necesidades de seguridad de la información de la organización..." Las directrices especifican que la eliminación de la información debe corresponder con su nivel de clasificación y sensibilidad legal.

- **ISO/IEC 27001:2022 — Anexo A — Control 5.10 (Uso aceptable de la información y otros activos asociados).** El control establece textualmente que:

  "Se deben identificar, documentar e implementar reglas para el uso aceptable y los procedimientos de manejo de la información y otros activos asociados."

- **ISO/IEC 27001:2022 — Anexo A — Control 7.10 (Almacenamiento de medios).** El control establece textualmente que:

  "Los medios de almacenamiento se deben gestionar de acuerdo con el esquema de clasificación de la organización y sus requisitos de manejo.

Causa:

No se han definido ni documentado procedimientos institucionales que regulen la destrucción segura de documentos físicos con información sensible, estableciendo responsabilidades, métodos autorizados, controles y mecanismos de supervisión.

Posibles consecuencias:

- Exposición a Fuga de Información por "Dumpster Diving": Riesgo inminente de que terceros, personal de aseo, recolectores de basura o competidores obtengan acceso a documentos institucionales confidenciales arrojados a la basura sin triturar, permitiendo la extracción de datos estratégicos, financieros o personales.

- Incumplimiento de la Ley de Protección de Datos Personales: Vulneración del principio de seguridad y confidencialidad exigido por las leyes de protección de datos, al no garantizar la destrucción irreversible de formularios, carpetas o documentos que contengan datos de ciudadanos o colaboradores.

- Anulación de los Esfuerzos de Ciberseguridad: Incoherencia en el esquema de control interno, donde la entidad gasta recursos protegiendo la versión digital de un documento mediante cifrado y contraseñas, pero permite que la copia física impresa del mismo documento sea desechada libremente en el cesto de basura del escritorio

Hallazgo 15:

Deficiencias en la administración, revisión y monitoreo de los sistemas de control de acceso biométrico a áreas críticas. (No Conformidad Menor).

Condición:

Se constató la ausencia de un proceso de verificación, calibración periódica y auditoría a los sistemas de control de acceso biométrico instalados en las puertas de ingreso a los pisos correspondientes (12 y 13) y zonas de acceso restringido (Centro de Cómputo/Data Center, cuartos de cableado y archivo). Mediante pruebas de auditoría física y revisión de configuraciones, se identificó que:

- No se realizan pruebas técnicas periódicas.
- Las bases de datos locales (templates biométricos almacenados en la memoria de los lectores independientes) no son auditadas ni conciliadas de forma rutinaria contra la base general de personal activo, permitiendo que registros biométricos de personal no autorizado permanezcan habilitados en los dispositivos físicos de lectura.

- No existe un protocolo de revisión técnica de los registros de eventos (logs de acceso biométrico) para detectar intentos fallidos recurrentes o manipulación de los lectores.

- A pesar de que exista una revisión por parte del proveedor (FAMOC), la entidad debe asegurar o establecer un procedimiento de revisión periódica, con el fin de verificar que todos los datos almacenados en los dispositivos biométricos, sean íntegros, confiables y estén siempre disponibles.

Evidencia hallazgo #15

Criterio:

- **ISO/IEC 27001:2022 — Anexo A — Control 7.2 (Entrada física):** El control establece textualmente que:

  "Las áreas aseguradas se deben proteger mediante controles de entrada adecuados para garantizar que solo se permita el acceso al personal autorizado." Las directrices especifican que la tecnología utilizada para el control de entrada (incluyendo la biometría) debe someterse a mantenimiento, pruebas de funcionamiento y revisiones periódicas de los permisos concedidos.

  ISO/IEC 27001:2022 — Anexo A — Control 7.4 (Monitoreo de la seguridad física): El control establece textualmente que:

  "Las instalaciones se deben monitorear continuamente para detectar accesos físicos no autorizados." (Exige la revisión activa de los registros de alerta y la calibración de los dispositivos de detección).

  ISO/IEC 27001:2022 — Anexo A — Control 8.13 (Gestión de derechos de acceso): Exige que la revisión y revocación de accesos se extienda a todos los repositorios físicos y lógicos, incluyendo la memoria de los dispositivos biométricos.

Causa:

No se ha definido un procedimiento institucional que establezca las actividades, responsables, frecuencia y mecanismos para la revisión periódica, conciliación y supervisión de los sistemas de control de acceso biométrico, dependiendo principalmente de las actividades de mantenimiento realizadas por el proveedor del servicio.

Posibles consecuencias:

- Ingreso No Autorizado por Fallas de Sensibilidad o Plantillas Huérfanas: Ex-

empleados, contratistas retirados o terceros malintencionados podrían superar los controles de ingreso físico si su huella o rostro continúa enrolado en la memoria interna del lector, o si la falta de calibración del sensor permite la lectura con un margen de tolerancia erróneo (Falso Acepto).

- Vulnerabilidad a Técnicas de Suplantación (Biometric Spoofing): La falta de actualización de firmware o ajuste en los sensores biométricos impide la detección de prueba de vida (liveness detection), permitiendo que el sistema pueda ser evadido con réplicas sintéticas o imágenes de alta resolución.

- Corrupción de las Pistas de Auditoría de Entrada Física: La descalibración en la hora/fecha de los lectores o la presencia de usuarios genéricos registrados en los dispositivos biométricos invalida el valor probatorio de los registros de ingreso ante la investigación de un siniestro, robo o sabotaje interno.

Hallazgo 16:

Deficiencias en las condiciones de orden, almacenamiento y protección física de activos tecnológicos en áreas críticas. (No Conformidad Menor).

Condición:

Durante el recorrido efectuado en las áreas destinadas al almacenamiento y soporte de infraestructura tecnológica, se evidenciaron condiciones inadecuadas de orden y almacenamiento que pueden afectar la protección física de los activos de información. En particular, se observó:

- Acumulación de cajas de cartón, sillas, mobiliario en desuso, material de embalaje y otros elementos ajenos a la operación tecnológica.
- Presencia de alimentos y bebidas en áreas destinadas al almacenamiento y manipulación de equipos tecnológicos.
- Bloqueo parcial del acceso a tableros eléctricos, extintores y rutas de evacuación debido al almacenamiento improvisado de activos y materiales tecnológicos.
- Almacenamiento de activos tecnológicos sin una delimitación física o clasificación que facilite su identificación y control.

Evidencia hallazgo 16

Criterio:

- **ISO/IEC 27001:2022 — Anexo A — Control 7.6 (Trabajo en áreas aseguradas):** El control establece textualmente que:

"Se deben diseñar e implementar medidas de seguridad para las áreas de trabajo en instalaciones aseguradas." Las directrices de la norma exigen que las áreas destinadas al mantenimiento y soporte de tecnología mantengan condiciones de orden, limpieza y restricciones de acceso que eviten daños accidentales o la manipulación no autorizada de activos.

- **ISO/IEC 27001:2022 — Anexo A — Control 7.1 (Perímetros de seguridad física):** Establece que los activos deben protegerse contra amenazas ambientales o riesgos físicos derivados de un entorno inadecuado.

- **ISO/IEC 27001:2022 — Anexo A — Control 7.7 (Escritorio y pantalla limpios):** Exige que los soportes físicos de información y medios de almacenamiento se encuentren protegidos contra accesos visivos o físicos no autorizados cuando no están en uso.

- **ISO/IEC 27001:2022 — Anexo A — Control 7.3 (Protección de oficinas, habitaciones e instalaciones):**El control establece textualmente que: "Se deben diseñar e implementar medidas de seguridad para oficinas, salas e instalaciones con el fin de proteger la información y otros activos asociados contra el acceso físico no autorizado, los daños y las interferencias."

Causa:

Ausencia de una política de "escritorio limpio y pantalla limpia" extensiva a las áreas de TI, falta de un proceso de depuración periódica de activos obsoletos, falta de asignación de un espacio exclusivo para el almacenamiento de basura tecnológica o material de embalaje y falta de auditorías internas periódicas de seguridad física e higiene industrial por parte del área de Servicios Generales y SST.

Posibles consecuencias:

- Incremento Crítico del Riesgo de Incendio: La acumulación masiva de material combustible (cartón y plásticos) junto a enchufes sobrecargados, multitomas y equipos electrónicos en prueba genera una carga de fuego elevada que facilita la ignición y propagación rápida de un incendio en el piso 13.

- Deterioro y Daño Accidental de Activos Institucionales: Riesgo de caídas, golpes o descargas electrostáticas (ESD) sobre repuestos nuevos o equipos de cómputo de la entidad en proceso de configuración, derivando en pérdidas financieras por averías provocadas por el entorno.

- Incapacidad de Trazabilidad y Pérdida de Repuestos: El desorden físico dificulta la realización de inventarios rápidos de componentes, facilitando el extravío o el hurto hormiga de partes internas de hardware (memorias RAM, discos duros, tarjetas de red) por falta de un control de stock delimitado.

Hallazgo 17:

Deficiencias en la implementación de controles de filtrado y restricción de navegación web. (No Conformidad Mayor).

Condición:

Se constató que la organización permite la navegación a páginas web catalogadas como prohibidas, de alto riesgo o no relacionadas con la operación del negocio (tales como sitios de correos electrónicos personales, almacenamiento en la nube no autorizado, redes sociales y páginas de descarga de software ilegal) a diferentes usuarios de la entidad. Durante las pruebas en sitio, se comprobó que el firewall perimetral o la solución de filtrado web (Proxy/DNS) no estaba aplicando políticas restrictivas homogéneas ni basadas en perfiles de puesto.

Evidencia hallazgo 17

Criterio:

- **ISO/IEC 27001:2022 — Anexo A — Control 8.23 (Filtrado web):** El control establece textualmente que:

  "El acceso a sitios web externos se debe gestionar para reducir la exposición de la organización a contenido malicioso." Las directrices especifican la obligación de restringir el acceso a categorías de sitios web no autorizados o de alto riesgo, utilizar motores de reputación en tiempo real y aplicar políticas adaptadas al nivel de riesgo de la información.

- **ISO/IEC 27001:2022 — Anexo A — Control 8.7 (Protección contra código malicioso):** Exige la implementación de controles defensivos (incluido el filtrado de navegación) para prevenir y detectar la descarga no autorizada de código malicioso.

- **ISO/IEC 27001:2022 — Anexo A — Control 8.12 (Prevención de fuga de datos):** Exige aplicar medidas para evitar la transmisión no autorizada de datos sensibles fuera de la organización a través de canales web desprotegidos.

- **ISO/IEC 27001:2022 — Anexo A — Control 5.10 (Uso aceptable de la información y otros activos asociados):**El control establece textualmente que:

  "Se deben identificar, documentar e implementar reglas para el uso aceptable y los procedimientos para el manejo de la información y otros

activos asociados."

Causa:

Falta de una política formal de uso aceptable de activos de información y debilidades en la configuración y actualización de las listas de categorías en las herramientas de seguridad perimetral. No se ha definido una matriz de perfiles de navegación que restrinja el acceso según las necesidades del rol del usuario.

Posibles consecuencias:

- Compromiso masivo por Ransomware o Phishing: La navegación libre facilita que un usuario sea engañado mediante vectores de ingeniería social (click en enlaces malintencionados o descarga de adjuntos en sitios clonados), derivando en la ejecución de código malicioso que puede cifrar servidores institucionales o secuestrar credenciales de dominio.

- Exfiltración de Información Institucional (Fuga de Datos): La posibilidad de subir libremente bases de datos, expedientes o código fuente a repositorios en la nube personales no auditado (Shadow IT), eludiendo los controles de prevención de pérdida de datos.

- Saturación del Ancho de Banda e Ineficiencia Operativa: Consumo excesivo de los recursos de red por streaming de video, descargas de archivos pesados o contenido recreativo en horario laboral, degradando el rendimiento de las aplicaciones críticas del negocio.

Hallazgo 18:

Inconsistencia entre los parámetros de autenticación implementados y el Procedimiento de Gestión de Accesos e Identidades. (No Conformidad Menor).

Condición:

Se evidenció que las configuraciones lógicas de complejidad de contraseñas implementadas en el Directorio Activo y en los sistemas misionales no coinciden con los lineamientos descritos en el Procedimiento de Gestión de Accesos e Identidades. Mientras que el documento formal exige una longitud mínima de 12 caracteres, uso de caracteres especiales y cambio obligatorio cada 90 días, la verificación técnica in situ demostró que el sistema permite contraseñas de 8 caracteres y cambio obligatorio de 60 días.

Evidencia hallazgo #18

Criterio:

- **ISO/IEC 27001:2022 — Anexo A — Control 5.1 (Políticas para la seguridad de la información):** El control establece que:

  "Las políticas de seguridad de la información y las políticas específicas del tema se deben definir, aprobar por la dirección, publicar, comunicar y revisar periódicamente." Las directrices exigen que las políticas aprobadas sean de obligatorio cumplimiento y se traduzcan en configuraciones técnicas reales**.**

- **ISO/IEC 27001:2022 — Anexo A — Control 5.36 (Conformidad con las políticas y estándares de seguridad):** El control establece textualmente que:

  "El cumplimiento de las políticas de seguridad de la información, los estándares específicos del tema y otros requisitos de seguridad de la organización se debe revisar periódicamente."

- **ISO/IEC 27001:2022 — Anexo A — Control 8.5 (Autenticación segura):** Exige que los sistemas de gestión de contraseñas impongan la fortaleza de la clave de acuerdo con los requisitos del negocio y la política de control de acceso.

Causa:

Falta de mecanismos de auditoría técnica continúa (Compliance Auditing) e integración entre el Oficial de Seguridad de la Información (CISO) y el área de Administración de Infraestructura/Redes. Tras la aprobación del documento de políticas por la Alta Dirección, el área técnica no tradujo ni aplicó dichos lineamientos en las políticas de grupo (GPO) o en las tablas de configuración de las bases de datos de los aplicativos, o bien modificó las configuraciones a solicitud de usuarios para evitar bloqueos continuos, sin actualizar la documentación ni solicitar una excepción formal.

Posibles consecuencias:

- Vulnerabilidad Inminente a Ataques de Fuerza Bruta y Password Spraying: La permisión técnica de contraseñas cortas y simples sin política de bloqueo de cuenta efectiva facilita que ciberdelincuentes puedan adivinar o violentar credenciales mediante herramientas automatizadas en cuestión de minutos o pocas horas.

- Falsa Sensación de Seguridad e Ineficacia de la Gobernanza del SGSI: La Alta Dirección y el Comité de Control Interno asumen que la entidad está protegida basándose en los documentos aprobados, cuando en la práctica operativa la infraestructura expone niveles de seguridad inferiores e inaceptables.

- Inobservancia Legal en Revisiones Externas y Certificaciones: Invalida el cumplimiento formal en auditorías de entes de control o de certificación ISO 27001, ya que el auditor externo valida la efectividad del control en la práctica (evidencia técnica) y no solo el papel firmado.

Hallazgo 19:

Deficiencias en la trazabilidad y formalización de la gestión de solicitudes e incidentes de la Mesa de Ayuda de TI. (No Conformidad Menor).

Condición:

Se identificó la ausencia de trazabilidad e formalización en la atención de solicitudes de servicio, requerimientos técnicos e incidentes por parte de la Mesa de Ayuda de TI. Durante las pruebas de recorrido y la revisión de evidencias de atención al usuario, se constató que:

- Los casos registrados carecen de campos obligatorios para documentar la autorización explícita del líder del área solicitante, la evidencia del cierre conforme por parte del usuario y la categorización del tipo de incidente o requerimiento o la disponibilidad de la información de los tickets puestos en la mesa de ayuda, no están disponibles para todos los técnicos de la mesa.

Evidencia hallazgo 19

Criterio:

- **ISO/IEC 27001:2022 — Anexo A — Control 5.24 (Gestión de incidentes de seguridad de la información):** El control establece que:

  "La organización debe planificar y preparar la gestión de incidentes de seguridad de la información definiendo, estableciendo y comunicando procesos, roles y responsabilidades." Las directrices exigen registrar, clasificar, priorizar y monitorear el ciclo de vida completo de cada caso hasta su cierre formal.

- **ISO/IEC 27001:2022 — Anexo A — Control 5.18 (Derechos de acceso**): Exige que el aprovisionamiento o modificación de derechos de acceso se realice mediante un proceso formal de autorización documentado y auditable.

- **ISO/IEC 27001:2022 — Anexo A — Control 8.16 (Monitoreo de actividades):** Exige la generación y conservación de registros de eventos (logs y bitácoras) sobre las operaciones de cambio y soporte en los sistemas.

- **ISO/IEC 27001:2022 — Anexo A — Control 5.37 (Procedimientos**

operativos documentados): El control establece textualmente que: "Los procedimientos operativos para las instalaciones de procesamiento de información se deben documentar y poner a disposición del personal que los necesite.

Causa:

Falta de una directriz institucional que declare la Mesa de Ayuda como el único canal oficial de atención de TI, sumada a la ausencia de un flujo de trabajo (workflow) automatizado que exija aprobaciones digitales antes de asignar un ticket a los técnicos. Asimismo, persiste una cultura organizacional orientada a la "atención inmediata informal" sobre el cumplimiento de los controles de seguridad y registro.

Posibles consecuencias:

- Otorgamiento de Accesos y Cambios No Autorizados: El procesamiento de solicitudes informales permite que técnicos de soporte otorguen privilegios, creen cuentas o modifiquen configuraciones a petición directa de usuarios que no cuentan con la autoridad o el visto bueno de sus jefes inmediatos.

- Incapacidad de Control, Métricas y SLA: La entidad no puede medir objetivamente el nivel de servicio de TI, los tiempos de respuesta, los tipos de incidentes recurrentes ni la carga de trabajo real del equipo de soporte, impidiendo la toma de decisiones basada en datos.

- Destrucción del No Repudio en Operaciones de Soporte: En caso de que una intervención técnica genere la pérdida de archivos, la corrupción de una base de datos o una interrupción del servicio, no existe registro de quién solicitó la tarea, quién la autorizó ni qué acciones técnicas específicas realizó el ingeniero de soporte.

Resumen de Madurez del Sistema de Gestión de Seguridad de la Información (SGSI)

La evaluación del estado actual del Sistema de Gestión de Seguridad de la Información (SGSI) se ha llevado a cabo mediante la integración de los requisitos y controles de la norma ISO/IEC 27001 evaluados a través de la metodología CMMI (Capability Maturity Model Integration). Este enfoque permite medir no solo la existencia formal de políticas y mecanismos de control, sino también el grado de institucionalización, optimización y capacidad predictiva de los procesos en cada uno de los dominios evaluados.

El modelo de madurez CMMI clasifica el nivel de desempeño de los dominios en una escala progresiva:

- Nivel 1 (Inicial): Procesos impredecibles, reactivos y dependientes de esfuerzos individuales.

- Nivel 2 (Gestionado): Procesos planificados, ejecutados, medidos y controlados a nivel de proyectos básicos.
- Nivel 3 (Definido): Procesos estandarizados, documentados y consolidados a nivel organizacional.
- Nivel 4 (Cuantitativamente Gestionado): Procesos controlados mediante métricas y objetivos cuantitativos de rendimiento.
- Nivel 5 (En Optimización): Procesos enfocados en la mejora continua y la adaptación proactiva a nuevas amenazas.

A continuación, se presenta el análisis consolidado del nivel de madurez alcanzado en cada dominio del estándar, destacando las fortalezas operativas y las áreas clave de oportunidad para la evolución de la postura de seguridad de la organización.

Componentes	Madurez
Controles Organizacionales	2,10
Controles de personas	2,50
Controles físicos	2,00
Controles tecnológicos	2,00
Promedio	2,09

Lo anterior indica que la entidad se encuentra en un estado de madurez: Gestionado, 2.09 de 5, equivalente al 41.8%.

Durante la ejecución de la auditoría del Sistema de Gestión de Seguridad de la Información (SGSI) basada en la norma ISO/IEC 27001:2022, se consideraron como insumo fundamental los riesgos identificados y gestionados bajo el Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC. La revisión contempló la validación de la metodología aplicada para la identificación, análisis, evaluación y tratamiento de riesgos, así como la verificación de la efectividad de los controles implementados para mitigar los escenarios de riesgo identificados. Asimismo, se evaluó la coherencia entre los riesgos documentados, los planes de tratamiento definidos y los controles establecidos en el SGSI, con el propósito de determinar su alineación con los requisitos de la norma ISO 27001, el contexto organizacional y los objetivos de seguridad y privacidad de la información. Este ejercicio permitió identificar oportunidades de mejora relacionadas con la gestión de riesgos, fortalecer la toma de decisiones basada en riesgo y validar el nivel de madurez alcanzado por la organización en la implementación del MSPI.

6.1 Limitaciones de Auditoría (Si aplica)

N/A

6.2 Siglas usadas (Si aplica)

- ISO/IEC: International Organization for Standardization / International Electrotechnical Commission — Organismo internacional que emite el estándar de gestión de seguridad de la información ISO/IEC 27001:2022.
- SGSI / ISMS: Sistema de Gestión de Seguridad de la Información (Information Security Management System) — Conjunto de políticas, procesos y controles para gestionar los riesgos de información en la entidad.
- NTP: Network Time Protocol — Protocolo de red destinado a la sincronización de los relojes de los sistemas informáticos.
- TI: Tecnologías de la Información.
- RBAC: Role-Based Access Control — Control de acceso basado en roles o perfiles.
- MFA: Multi-Factor Authentication — Autenticación de Múltiples Factores.
- BCP: Business Continuity Plan — Plan de Continuidad del Negocio.
- GPO: Group Policy Object — Objetos de Directiva de Grupo (configuraciones centralizadas aplicadas en un entorno de Directorio Activo de Microsoft).
- SLA: Service Level Agreement — Acuerdo de Nivel de Servicio (tiempos de respuesta y solución acordados para la atención de casos).
- DNS: Domain Name System — Sistema de Nombres de Dominio (asocia nombres de sitios web con sus direcciones IP).
- SSL / TLS: Secure Sockets Layer / Transport Layer Security — Protocolos criptográficos que proporcionan comunicaciones seguras sobre una red (tráfico cifrado HTTPS).
- BYOD: Bring Your Own Device — Tendencia de permitir que los empleados traigan sus propios dispositivos personales a la red de la organización.
- UPS: Uninterruptible Power Supply — Sistema de Alimentación Ininterrumpida (baterías de respaldo eléctrico).

6.3 Riesgos del proceso e identificados por el auditor

- Riesgo de Degradación de la Seguridad durante la Contingencia: El riesgo de que, al intentar improvisar soluciones para reactivar la operación rápidamente, se omitan los controles de seguridad lógicos y físicos (ej. uso de redes no seguras, elevación indeseada de privilegios o salto de firmas de aprobación), exponiendo los datos a ataques o fugas.
- Riesgo de Sabotaje Físico y Caída de Servicios: El riesgo de la interrupción deliberada o accidental de la operación lógica debido a la manipulación física imprevista de cables, unidades de energía (UPS) o servidores por parte de personal no autorizado
- Riesgo de Intrusión y Acceso Físico Directo a Infraestructura Crítica: La falta de controles de ingeniería y CCTV en las puertas de emergencia materializa el riesgo de que un atacante físico acceda a los switches, cableado estructurado o servidores principales de la entidad de forma directa.

- Riesgo de Pérdida de Confidencialidad por Espionaje de Infraestructura: Al no existir barreras en el ingreso (A.7.1 y A.7.2), se materializa el riesgo de que personal no autorizado o contratistas externos visualicen, fotografíen o sustraigan copias de los planos de los centros de reclusión a nivel nacional y sistemas de seguridad física, exponiendo planos tácticos que detallan las vulnerabilidades arquitectónicas de la organización.
- Riesgo de Pérdida de Integridad por Alteración Documental: Riesgo de modificación, tachadura o daño deliberado o accidental en la cartografía e información histórica original durante consultas sin supervisión ni trazabilidad, invalidando la fidelidad de la información técnica disponible para futuras obras o auditorías.
- Riesgo de Intrusión y Secuestro de Información (Ransomware): El riesgo de que un actor de amenaza tome el control de una cuenta inactiva que aún posea privilegios elevados en la red, utilizándola como pivote para desplegar código malicioso, cifrar servidores institucionales o extraer bases de datos críticas de la entidad.
- Riesgo de Modificación No Autorizada de Datos: Posibilidad de alteración de registros financieros, operativos o de control mediante el uso de credenciales huérfanas que no fueron revocadas tras la salida de sus titulares.
- Riesgo de Gestión Inadecuada de Incidentes: Al mantener desactualizado el manual de incidentes, el equipo técnico mitigará los ataques bajo criterios empíricos y no estandarizados, elevando el riesgo de interrupciones prolongadas del servicio o destrucción accidental de evidencia digital durante la contención de una brecha.
- Riesgo de Aplicación de Controles Obsoletos: El riesgo de invertir recursos y esfuerzos en asegurar plataformas o perímetros que ya no son críticos para el negocio, mientras que los nuevos activos digitales quedan desprovistos de directrices de blindaje técnico.
- Riesgo de Compromiso Total de la Red (Dominio Comprometido): El riesgo inminente de que el tercero, de forma malintencionada o por verse infectado en su propio equipo, introduzca ransomware directamente en el Controlador de Dominio, permitiendo el cifrado masivo y simultáneo de todos los servidores y computadores conectados a la red institucional.
- Riesgo de Ex filtración de Información Confidencial: Al controlar el DC, el tercero puede otorgarse a sí mismo permisos de acceso a cualquier carpeta compartida, bases de datos o correos de la Alta Dirección, materializando la fuga de información sensible.
- Riesgo de Fuga de Datos en Infraestructura de Terceros: Riesgo de filtración de información confidencial o datos personales almacenados en la nube o bases de datos gestionadas por el proveedor, derivado de fallas de configuración del tercero que no fueron detectadas ni exigidas a corregir por la entidad a tiempo.
- Riesgo de Ex filtración de Información Sensible: El riesgo de que un colaborador trasladado continúe accediendo, descargando o compartiendo documentación confidencial de su área anterior (por ejemplo, estrategias comerciales, presupuestos, nóminas o datos personales) por curiosidad o mala

fe, aprovechando que conserva los permisos de red activos.

- Riesgo de Destrucción Definitiva del Patrimonio Digital (Pérdida Total de Datos): El riesgo crítico de enfrentar la pérdida irremediable de registros históricos, financieros o del núcleo del negocio debido a que las copias de seguridad almacenadas no fueron funcionales al momento de ser requeridas.
- Riesgo de Brecha de Datos por Pérdida de Portátiles / Discos: El riesgo inminente de filtración masiva de información institucional o sensible si un equipo extraído sin cifrado ni control de salida es extraviado o robado en tránsito.

6.4 Seguimiento plan de mejoramiento (Si aplica)

7. FORTALEZAS

En el proceso de auditoría, fueron detectadas las siguientes fortalezas:

1. La organización cuenta con un sistema de monitoreo ambiental continuo en las instalaciones críticas (cuarto de comunicaciones / centro de cómputo), enfocado en la medición permanente de temperatura y humedad, así como en la detección temprana de humo.
2. Arquitectura de Red Segregada: Segmentación efectiva de la red interna mediante VLANs, separando el tráfico administrativo, el de servidores críticos y el de acceso a internet de visitantes.
3. Implementación de diferentes controles de seguridad (biometría, CCTV y control de presencia) monitorear el acceso al Data Center/Centro de Cómputo principal.
4. Transparencia y Disponibilidad de Evidencia: Disposición proactiva del equipo de TI y los custodios de procesos para facilitar el acceso a la documentación, bitácoras (*logs*) y configuraciones requeridas.

8. RECOMENDACIONES

1. Desarrollo del Análisis de Impacto en el Negocio (BIA): Realizar un estudio formal para identificar los procesos misionales de la entidad, los activos de TI que los soportan y definir formalmente los RTO (Tiempo Máximo Tolerable de Caída) y RPO (Pérdida Máxima Tolerable de Datos) para cada uno.
2. Ejecución de Simulacros y Pruebas de Continuidad (Mínimo Anuales): Someter el BCP a pruebas de escritorio (Tabletop exercises) y simulacros reales de interrupción para validar la efectividad de las rutas de contingencia y medir los tiempos de respuesta del personal ante emergencias reales.
3. Procedimiento y Cronograma Anual de Pruebas de Restauración: Formalizar un procedimiento que obligue a realizar pruebas de restauración aleatorias mensuales para sistemas críticos y semestrales/anuales para la totalidad de la infraestructura de TI.
4. Formalización del Protocolo de Verificación e Informe de Pruebas: Documentar

cada ejercicio de simulación en un acta técnica que incluya:

- Sistema probado.
- Fecha de la copia utilizada.
- Tiempo real que tomó la restauración (RTO medido).
- Verificación de consistencia de los datos por parte del Líder de Proceso / Propietario de la Información.
- Firma de conformidad de TI y del Oficial de Seguridad de la Información.

5. Política y control de cuentas: Formalizar una directriz institucional que prohíba el uso de credenciales compartidas para operar aplicativos, correo, red o sistemas de información. Todo acceso debe asociarse a un usuario individual, identificable y trazable. Las cuentas genéricas, técnicas o de servicio solo podrán mantenerse de manera excepcional, debidamente justificadas, inventariadas y asignadas a un responsable o custodio nominal específico, garantizando control de uso, custodia de credenciales, revisión periódica, registros de auditoría, privilegios mínimos y eliminación progresiva de cuentas compartidas.
6. Implementación de Bitácoras Estandarizadas de Acceso: Diseñar un registro obligatorio (físico o digital en recepción y Data Center) que capture: Nombre completo, identificación, empresa, motivo de la visita, funcionario que autoriza, hora de entrada/salida y firma.
7. Procedimiento Formal y Formato de "Salida de Activos Tecnológicos": Implementar un formato obligatorio (físico o digital en la Intranet) firmado por el Jefe de Activos, el Líder de TI y el funcionario responsable, donde se especifique: Serial del equipo, marca, motivo de salida, destino, fecha estimada de retorno y si el disco duro cuenta con cifrado activo.
8. Implementación de Flujos de Aprobación (Workflows) en la Plataforma: Configurar la herramienta de ticketing para que las solicitudes relativas a accesos, carpetas, correos o licencias requieran la aprobación digital obligatoria del Jefe Inmediato o Custodio de la Información antes de ser asignadas a un técnico.
9. Cierre Formal y Encuesta de Satisfacción/Conformidad: Implementar que ningún ticket sea marcado como "Resuelto" sin la confirmación explícita del usuario solicitante y la documentación en la plataforma de las actividades técnicas realizadas para su solución.
10. Alineación Técnica de las GPO del Active Directory: Ajustar y desplegar las directrices de grupo (Group Policy Objects) en el Directorio Activo para que reflejen de forma idéntica o superior lo exigido en el procedimiento.
11. Implementación de una política de uso y protección física para infraestructura crítica: Definir un estándar operativo de almacenamiento y orden para los cuartos de comunicaciones que restrinja su uso únicamente a activos tecnológicos en operación. Se recomienda establecer un calendario de auditorías físicas periódicas y formalizar el protocolo de disposición/baja de insumos y desechos, asegurando la eliminación inmediata de empaques o material inflamable que comprometan la seguridad del área.
12. Procedimiento de Auditoría y Depuración de información de Lectores

Biométricos: Establecer por directriz técnica la extracción e inspección de la base de usuarios almacenada en cada terminal biométrica, asegurando el borrado inmediato de los registros que no correspondan a personal activo de la entidad. Este procedimiento se debe realizar de acuerdo con el análisis de riesgos establecido por la entidad, criticidad de los activos y necesidades del negocio.

13. Implementación de trazabilidad bidireccional en el control de acceso a áreas críticas:
    - Configurar e implementar mecanismos de control de acceso físico que permitan el registro automatizado tanto del ingreso como de la salida (in/out reader) en el Datacenter, áreas de tecnología y demás zonas de procesamiento sensible.
    - Esta medida garantizará la trazabilidad completa, la generación de bitácoras precisas de permanencia en tiempo real y la prevención de vulnerabilidades de seguridad física como el anti-passback o la evasión de registros.
14. Procedimiento Formal de Destrucción Segura de Documentos: Redactar y socializar un protocolo que establezca qué tipo de documentos deben ser triturados de forma inmediata en las áreas y cuáles deben ser custodiados en contenedores sellados para su destrucción masiva programada.
15. Análisis de los mapas de riesgos y los controles: Se recomienda el Proceso de Tecnología junto a la Oficina Asesora de Planeación, en su calidad de segunda línea de defensa, en articulación con los demás procesos, efectúen un análisis integral de la materialización de los riesgos evidenciados durante la auditoría, contrastando los hechos identificados con los riesgos actualmente registrados en la matriz del proceso de Gestión Contractual e identificando, adicionalmente, aquellos eventos que se materializaron sin haber sido previamente reconocidos, valorados o tratados. Este ejercicio deberá orientarse a determinar las causas que permitieron su ocurrencia, evaluar la suficiencia y efectividad de los controles existentes, identificar brechas en la gestión preventiva y, cuando corresponda, actualizar la matriz de riesgos incorporando nuevos eventos, causas, consecuencias, controles, responsables e indicadores de seguimiento, con el propósito de fortalecer la estructura institucional de administración del riesgo, reducir la probabilidad de recurrencia de las situaciones observadas y asegurar que los controles diseñados respondan efectivamente a los riesgos asociados a la planeación, ejecución, supervisión, modificación y cierre de la gestión contractual.

9. CONCLUSIONES

1. Los controles del Anexo A de la norma ISO 27001 presentan un nivel de madurez inferior al objetivo institucional. Si bien la entidad opera en un nivel "gestionado", al contar con un marco documental de políticas y estándares, la falta de actualización normativa y la escasa socialización con las partes interesadas limitan la efectividad operativa del sistema de gestión de seguridad de la información.

2. El monitoreo sobre la gestión de terceros presenta deficiencias en materia de Seguridad de la Información. Aunque la entidad realiza el seguimiento a la ejecución de los contratos, existe un vacío en la planificación y verificación

periódica de los lineamientos de seguridad exigidos a los proveedores críticos, lo que expone a la organización a riesgos no evaluados en la cadena de suministro.

3. Se concluye que el SGSI carece del nivel de gobernanza requerido. Si bien existen áreas y roles asignados para su operación, la falta de compromiso y disposición de la alta dirección compromete la efectividad del sistema, omitiendo el principio fundamental de liderazgo exigido para el logro de los objetivos de seguridad.
4. No se realizan ejecuciones periódicas de análisis de pruebas de seguridad tipo escaneo de vulnerabilidades ni pentesting, lo cual aumenta el riesgo de infecciones de virus, apertura de puertas traseras sin identificar, Keyloggers implementados y configurados para extracción de información de manera ilegal y compromisos serios de seguridad de la información para la entidad.
5. La entidad no cuenta con un Plan de Recuperación ante Desastres (DRP) formalizado, probado ni documentado. Esta falencia limita el cumplimiento de los estándares de continuidad del negocio y seguridad de la información, dejando a la organización expuesta a un alto impacto operativo, financiero y reputacional en caso de fallas graves en los sistemas de información.
6. La entidad presenta debilidades en la gestión de la seguridad de la información debido a la desactualización o inexistencia de un proceso formalizado para la identificación, reporte y atención de incidentes. Esta deficiencia limita la capacidad de respuesta oportuna ante amenazas, incrementa el tiempo de exposición a vulnerabilidades y dificulta el aprendizaje institucional para prevenir eventos futuros.
7. La gestión de accesos lógicos no garantiza una adecuada segregación de funciones ante los cambios de responsabilidad interna. La falta de alineación entre el área de Talento Humano y Tecnologías de la Información impide la actualización oportuna de perfiles y credenciales, permitiendo que colaboradores mantengan privilegios de roles anteriores y comprometiendo la confidencialidad e integridad de los sistemas de información.
8. Se evidencia una debilidad estructural en la gestión documental de la entidad, caracterizada por la falta de estandarización, control de versiones y políticas de retención o disposición final de la información. Esta deficiencia dificulta la trazabilidad de los procesos, genera dispersión de datos sensibles en medios físicos y digitales, e incrementa el riesgo de pérdida, alteración o divulgación no autorizada de documentos institucionales.

10. AUTORIZACIÓN PARA COMUNICAR ESTE INFORME:

En cumplimiento del parágrafo 1° del Artículo 2.2.21.4.7 del Decreto 648 de 2017 "Relación administrativa y estratégica del Jefe de Control Interno o quien haga sus veces", el presente informe tendrá como destinatario principal al representante legal de la Entidad y al líder del proceso auditado. A través del Comité Institucional de Coordinación de Control Interno, se dará a conocer los resultados de las auditorías a los miembros de esta instancia.

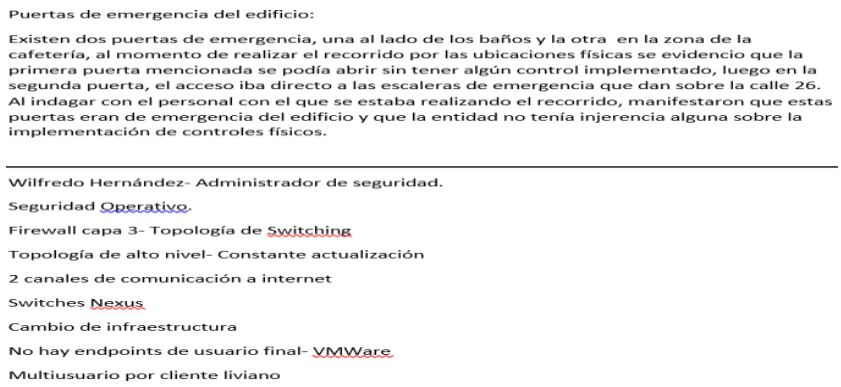
Así mismo y en cumplimiento de la Ley 1712 de 2014, este informe se publicará en la

página web de la Entidad - Ley de Transparencia.

Nombre completo	Responsabilidad	Firma
Nombre: Walter Raúl Niño Pérez Cargo: Contratista-Oficina Control Interno (OCI)	Auditor Líder	Walter Raúl Niño Pérez CC. 1.014.205.150

11. EVIDENCIAS FOTOGRÁFICAS (cuando aplique) Evidencia

Hallazgo 1: Debilidades en los controles de seguridad física y restricción de acceso en las puertas de emergencia.



Puertas de emergencia del edificio:

Existen dos puertas de emergencia, una al lado de los baños y la otra en la zona de la cafetería, al momento de realizar el recorrido por las ubicaciones físicas se evidencio que la primera puerta mencionada se podía abrir sin tener algún control implementado, luego en la segunda puerta, el acceso iba directo a las escaleras de emergencia que dan sobre la calle 26. Al indagar con el personal con el que se estaba realizando el recorrido, manifestaron que estas puertas eran de emergencia del edificio y que la entidad no tenía injerencia alguna sobre la implementación de controles físicos.

Wilfredo Hernández- Administrador de seguridad.

Seguridad Operativo.

Firewall capa 3- Topología de Switching

Topología de alto nivel- Constante actualización

2 canales de comunicación a internet

Switches Nexus

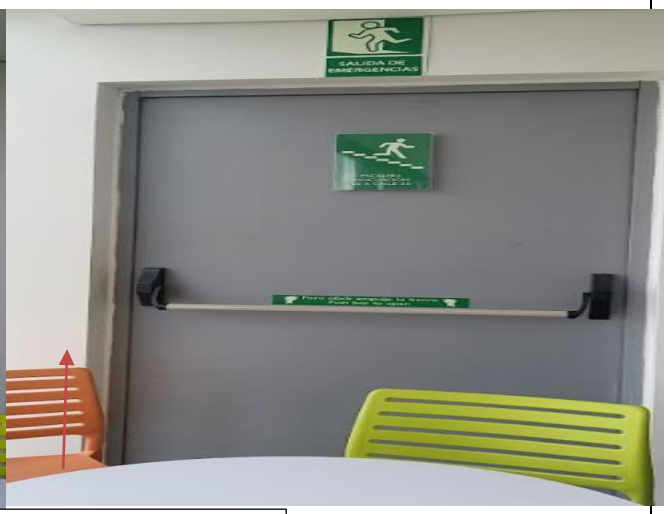
Cambio de infraestructura

No hay endpoints de usuario final- VMWare

Multiusuario por cliente liviano

A través de las notas identificadas en la auditoría, se observa que no existen controles de acceso físico en las puertas de emergencia de edificio.

Escalera de Emergencia al lado delos baños piso 12



Escalera de Emergencia cocina piso 12

Evidencia hallazgo 2: Ausencia de controles de acceso físico y falta de registros de trazabilidad en el depósito de planos históricos. (No Conformidad mayor)

Acceso físico a cuarto de Planimetría Piso 13

2.1

Planos e información institucional sin control alguno

2.2

Los planos están en una zona considerada de alto riesgo, ya que si se presenta un incendio este puede afectar los canales de comunicación.

2.3

Evidencia hallazgo 3: Inexistencia de un proceso de depuración y gestión periódica de cuentas de usuario inactivas en las plataformas tecnológicas de la entidad. (No Conformidad Mayor).

Gestión de usuarios:

Administrativo

Gestión administrativa.

Solicitud de creación de usuarios.

Matriz compartida con administrativa

No hay una depuración de usuarios inactivos dentro de la entidad.

Mergy Estefani Esterling Parra-> usuaria desactivada

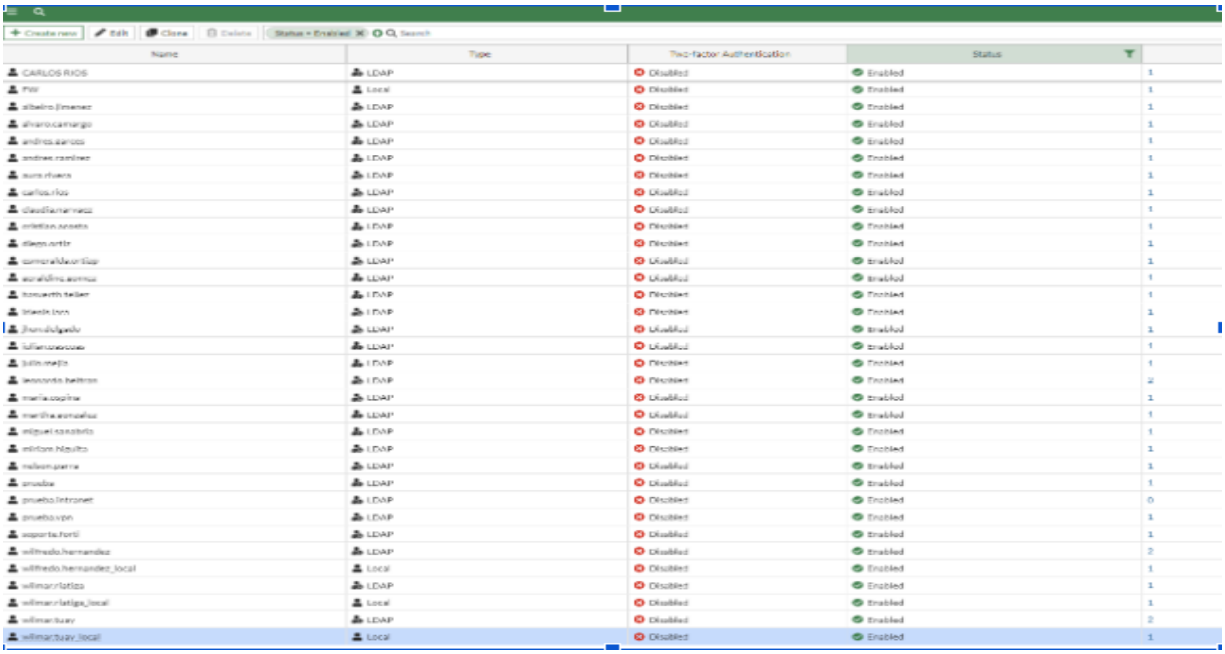
Se cambia la contraseña una vez se le haya entregado el usuario al funcionario.

Documentado política de copias de respaldo.

"Oscar Julián Cobos" se retiró de la entidad el día 3 de junio y solicita prorroga del acceso a la información

Existe información de copias de seguridad desde el año 2013 que puede ser accedida en el servidor de copias de seguridad. Adicionalmente se están guardando copias de seguridad del correo electrónico en el mismo espacio.

Se evidencia a través de la recopilación de notas en visita en campo, que existen usuarios muy antiguos que aunque se encuentren deshabilitados, aún son reconocidos por la entidad. Adicionalmente se levantó acta con fecha del 10 de junio 2026 con Mayra Oficial de seguridad.
Usuarios Activos en Firewall para acceso a VPN-SSL de FortiClient asociados al DC (LDAP).



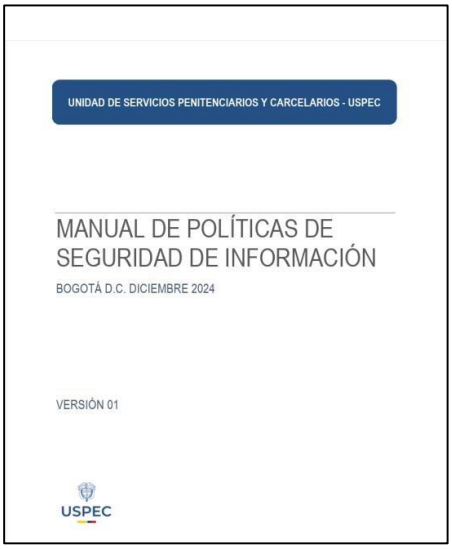
Evidencia hallazgo 4: Falta de Actualización y Revisión de Documentos Clave del SGSI. Un Sistema de Gestión de Seguridad de la Información cuyos documentos clave (políticas, manuales, análisis de riesgos) están desactualizados se convierte en un sistema "de papel". (No Conformidad Mayor)

USPEC	MANUAL DE POLÍTICAS DE SEGURIDAD DE INFORMACIÓN	**Código**: TI-MA-003 **Versión**: 01 **Vigencia**: 17/12/2024

RESUMEN DE CAMBIOS

Versión	Fecha	Numerales	Descripción de la modificación
01	17/12/2024	Todos	Se crea el documento y se aprueba en el Comité Institucional de Gestión y Desempeño, según acta N. 232 del 11 de diciembre de 2024

RESPONSABILIDAD Y AUTORIDAD		
Elaboró / Actualizó:	**Revisó:**	**Aprobó:**
Nombre: Daniel Muñoz Alvarado	Nombre: Álvaro Camargo Barbosa	Nombre: Imelda Muñoz Mancipe
Cargo: Oficial de Seguridad de Información	Cargo: Analista de Sistemas	Cargo: Jefe Oficina de Tecnología
Dependencia: Dirección General	Dependencia: Oficina de Tecnología	Dependencia: Oficina de Tecnología
	Nombre: Wilfredo Hernández Estupiñán	
	Cargo: Profesional Universitario	
	Dependencia: Oficina de Tecnología	
	Nombre: Sebastián Espinel	
	Cargo: Profesional Especializado	
	Nombre: Mayra Alexandra Agudelo Carvajal	
	Cargo: Profesional Especializado	
	Dependencia: Oficina de Tecnología	



A través de la revisión documental se puede evidenciar que la fecha de revisión del manual de políticas de Seguridad de Información tiene como fecha diciembre 2024.

Dentro del control de cambios del manual de políticas de seguridad, no se evidencia por lo menos una revisión anual.

Evidencia hallazgo 5: Acceso de terceros no autorizado, sin trazabilidad ni supervisión técnica al Controlador de Dominio principal. (No Conformidad Mayor)

Los ingenieros Carlos y Alvaro tienen la funcionalidad de activar, modificar, bloquear e inhabilitar usuarios.

Los ingenieros Wilfredo y Wilmar Ricardo solamente pueden consultar.

Los Ingenieros de mesa de ayuda solo atienden ticket para desbloquear usuario.

Existe un riesgo sobre fuga de información de los accesos que tienen los ingenieros de mesa de ayuda al controlador de dominio.

No hay matrices de roles y responsabilidades que definan los permisos y privilegios establecidos por cada uno de los funcionarios de la organización.

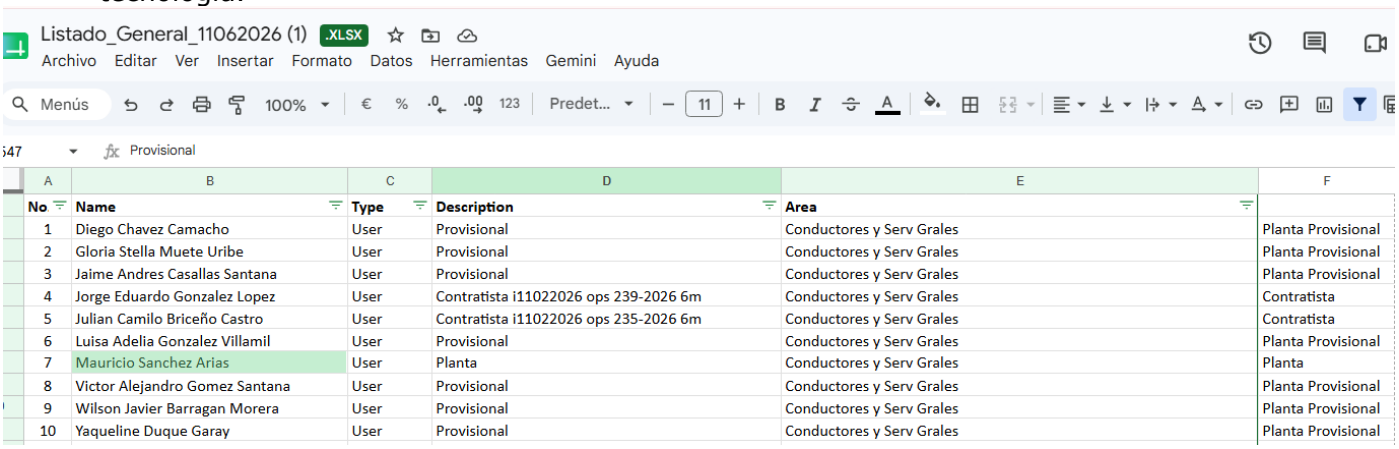
Miguel Rodríguez- Coordinador de la mesa de servicios.

Tercerizado- Aldesarrollo.

ITCM- Registro de solicitudes.

Correo debe venir del líder o el jefe del área

Se puede evidenciar a través de las notas apuntadas en sitio, que usuarios de la mesa de ayuda, pueden realizar acciones administrativas sin tener control alguno o supervisión del área de tecnología.



Listado_General_11062026 (1) .XLSX

Archivo Editar Ver Insertar Formato Datos Herramientas Gemini Ayuda

Menús 100% € % .0 .00 123 Predet... 11 B I

547 fx Provisional

	A	B	C	D	E	F
	No	Name	Type	Description	Area	
1	1	Diego Chavez Camacho	User	Provisional	Conductores y Serv Grales	Planta Provisional
2	2	Gloria Stella Muete Uribe	User	Provisional	Conductores y Serv Grales	Planta Provisional
3	3	Jaime Andres Casallas Santana	User	Provisional	Conductores y Serv Grales	Planta Provisional
4	4	Jorge Eduardo Gonzalez Lopez	User	Contratista i11022026 ops 239-2026 6m	Conductores y Serv Grales	Contratista
5	5	Julian Camilo Briceño Castro	User	Contratista i11022026 ops 235-2026 6m	Conductores y Serv Grales	Contratista
6	6	Luisa Adelia Gonzalez Villamil	User	Provisional	Conductores y Serv Grales	Planta Provisional
7	7	Mauricio Sanchez Arias	User	Planta	Conductores y Serv Grales	Planta
8	8	Victor Alejandro Gomez Santana	User	Provisional	Conductores y Serv Grales	Planta Provisional
9	9	Wilson Javier Barragan Morera	User	Provisional	Conductores y Serv Grales	Planta Provisional
10	10	Yaqueline Duque Garay	User	Provisional	Conductores y Serv Grales	Planta Provisional

Evidencia hallazgo 6: Inexistencia de matrices de roles y perfiles para la asignación formal de accesos y privilegios en la infraestructura tecnológica. (No Conformidad Mayor)

Existe información de copias de seguridad desde el año 2013 que puede ser accedida en el servidor de copias de seguridad. Adicionalmente se están guardando copias de seguridad del correo electrónico en el mismo espacio.

Gestión de contraseñas:

Cambio de contraseñas

Guia de contraseñas seguras. Esta cargado en el Drive.

Adolfo Romero> No presenta paz y Salvo

Jeimmy Lorena Martinez-> Validación de software de gestión humana.

Gestión Contractual- > Carlos Pérez

Grupo Administración de personal

Existe un riesgo sobre fuga de información de los accesos que tienen los ingenieros de mesa de ayuda al controlador de dominio.

No hay matrices de roles y responsabilidades que definan los permisos y privilegios establecidos por cada uno de los funcionarios de la organización.

Existen paz y salvos que no tienen las firmas completas de todas las áreas por las cuales debería pasar el usuario una vez finalice su contrato laboral.

Checklist de todos los usuarios activos, inhabilitados de la entidad.

Usuarios definidos en establecimientos. Entrega de usuario y elementos de tecnología.

Actualización del documento: Gestión de acceso a usuarios Tercer trimestre.

616 personas en total en la USPEC.

Luis Alejandro Gonzalez: fecha de retiro: 4 de mayo.

Se inhabilito el 4 de mayo 2026

Se tiene el paz y salvo

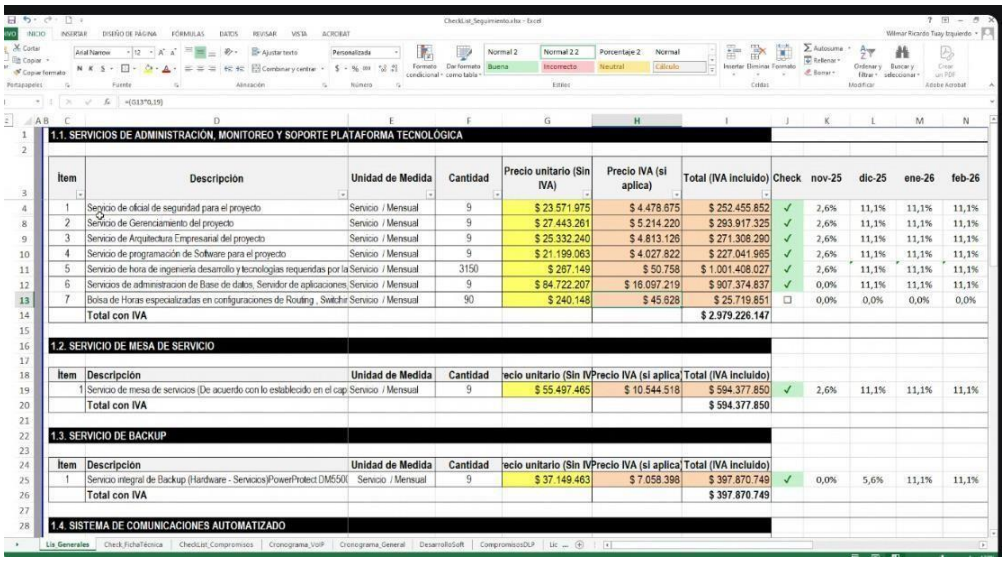
Mediante la visita en sitio al área de tecnología, se revisó si existía matriz de roles basado en las responsabilidades de cada usuario.

Estado de Implementación ISO 27001

Sección	Controles Anexo A	Requerimientos ISO 27001	Preguntas	Respuesta
	5.34 Privacidad y protección de datos (PII)		sus requisitos (legales, reglamentarios, contractuales)?	
4.2 (b)	6.2 Términos y condiciones del empleo	Determinar los requerimientos y oblicaciones relevantes de seguridad de la información		
4,3		**Determinación del alcance del SGSI**		
4,3	5.9 Inventario de activos 8.22 Segregación de redes 7.1 Perímetros físicos	Determinar y documentar el alcande del SGSI	¿Está el alcance documentado, considerando límites, interfaces y dependencias? Relacionar el documento correspondiente.	El alcance se encuentra documentado dentro de la Política de seguridad y privacidad de información
4,4		**SGSI**		
4,4	5.37 Procedimientos operativos 8.16 Monitoreo de actividades 8.32 Gestión de cambios 5.35 Revisión independiente	Establecer, implementar, mantener y mejorar de forma continua el SGSI acorde al estandar		
5		**Liderazgo**		
5,1		**Liderazgo y compromiso**		
5,1	5.4 Responsabilidades de la dirección 5.37 Procedimientos operativos. 8.6 Gestión de capacidad	La administración debe demostrart liderazgo y compromiso por el SGSI	¿Demuestra la alta dirección liderazgo mediante la política, objetivos e integración en procesos?	El liderazgo se puede evidenciar a través de la política de seguridad y privacidad de información, a través de la cual se definen roles y responsabilidades. Adicionalmente de forma semestral se presenta ante el Comité Directivo el estado del SGSI.

Evidencia hallazgo 7: Deficiencias en el seguimiento, monitoreo y supervisión periódica de la seguridad de la información en la gestión de proveedores externos. (No Conformidad Mayor).

7.1



1.1. SERVICIOS DE ADMINISTRACIÓN, MONITOREO Y SOPORTE PLATAFORMA TECNOLÓGICA

Ítem	Descripción	Unidad de Medida	Cantidad	Precio unitario (Sin IVA)	Precio IVA (si aplica)	Total (IVA incluido)	Check	nov-25	dic-25	ene-26	feb-26
1	Servicio de oficial de seguridad para el proyecto	Servicio / Mensual	9	$ 23.571.975	$ 4.478.675	$ 252.455.852	✓	2,6%	11,1%	11,1%	11,1%
2	Servicio de Gerenciamiento del proyecto	Servicio / Mensual	9	$ 27.443.261	$ 5.214.220	$ 293.917.325	✓	2,6%	11,1%	11,1%	11,1%
3	Servicio de Arquitectura Empresarial del proyecto	Servicio / Mensual	9	$ 25.332.240	$ 4.813.126	$ 271.308.290	✓	2,6%	11,1%	11,1%	11,1%
4	Servicio de programación de Software para el proyecto	Servicio / Mensual	9	$ 21.199.063	$ 4.027.822	$ 227.041.965	✓	2,6%	11,1%	11,1%	11,1%
5	Servicio de hora de ingeniería desarrollo y tecnologías requeridas por la	Servicio / Mensual	3150	$ 267.149	$ 50.758	$ 1.001.408.027	✓	2,6%	11,1%	11,1%	11,1%
6	Servicios de administracion de Base de datos, Servidor de aplicaciones	Servicio / Mensual	9	$ 84.722.207	$ 16.097.219	$ 907.374.837	✓	0,0%	11,1%	11,1%	11,1%
7	Bolsa de Horas especializadas en configuraciones de Routing , Switchir	Servicio / Mensual	90	$ 240.148	$ 45.628	$ 25.719.851	☐	0,0%	0,0%	0,0%	0,0%
	Total con IVA					$ 2.979.226.147					

1.2. SERVICIO DE MESA DE SERVICIO

Ítem	Descripción	Unidad de Medida	Cantidad	ecio unitario (Sin IV	Precio IVA (si aplica	Total (IVA incluido)					
1	Servicio de mesa de servicios (De acuerdo con lo establecido en el cap	Servicio / Mensual	9	$ 55.497.465	$ 10.544.518	$ 594.377.850	✓	2,6%	11,1%	11,1%	11,1%
	Total con IVA					$ 594.377.850					

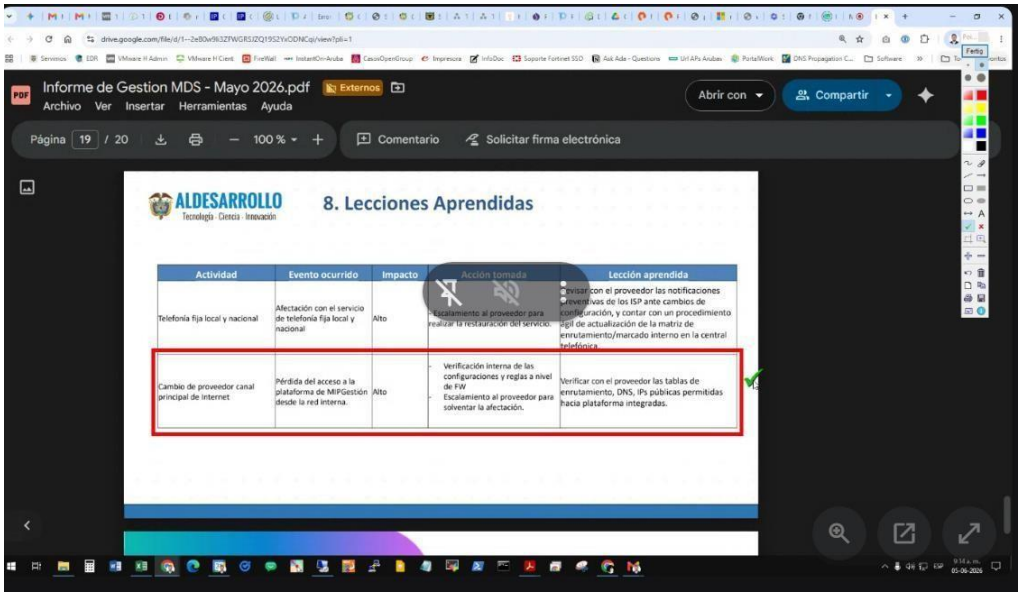
1.3. SERVICIO DE BACKUP

Ítem	Descripción	Unidad de Medida	Cantidad	ecio unitario (Sin IV	Precio IVA (si aplica	Total (IVA incluido)					
1	Servicio integral de Backup (Hardware - Servicios)PowerProtect DM5500	Servicio / Mensual	9	$ 37.149.463	$ 7.058.398	$ 397.870.749	✓	0,0%	5,6%	11,1%	11,1%
	Total con IVA					$ 397.870.749					

1.4. SISTEMA DE COMUNICACIONES AUTOMATIZADO

Se evidencia que el área de tecnología realiza un seguimiento a los servicios contratados de monitoreo y soporte de infraestructura tecnológica.

7.2



El proveedor de la mesa de ayuda "ALDESARROLLO", envía a la USPEC un informe de gestión del servicio (seguimiento a la ejecución del contrato), más no un seguimiento de los lineamientos de seguridad que debe cumplir el proveedor.

Evidencia hallazgo 8: Inexistencia de un procedimiento formal para la modificación y revocación oportuna de privilegios de acceso en procesos de movilidad interna. (No Conformidad Menor)

El envio de correo electrónico referente a las solicitudes de extracción de información es manejado por cada uno de los integrantes de la mesa de ayuda.

No existe una trazabilidad de las acciones mediante el software de la mesa de ayuda.
Traslado: A través de un oficio y/o resolución.

No se esta realizando la revocación de los accesos a la información de los usuarios que cambian entre dependencias.

Responsable: Supervisor de contrato.

- **Usuario Practicante**: se debe adjuntar copia del contrato.
  Responsable: Tutor.

5.3 LINEAMIENTOS ADICIONALES

Ante el evento de desvinculación de un usuario, éste debe gestionar personalmente la entrega de los accesos asignados de acuerdo a lo requerido en el formato TI-FO-053 Paz y Salvo, para el caso de la desvinculación de un directivo o jefe, este puede delegar a un funcionario de su dependencia para realizar el trámite de entrega de cuentas.

Los usuarios creados para los contratistas y practicantes, son creados y parametrizados de acuerdo al tiempo de vinculación con la Entidad, esto siempre y cuando el sistema lo permita. Una vez terminada la fecha de vinculación, los accesos quedan automáticamente inhabilitados. Si se llega a presentar alguna novedad en la contratación, como renovación del contrato, terminación anticipada o cualquier otra, la Dirección de Gestión Contractual o el supervisor de contrato o tutor(a) en el caso de los practicantes, deben informar estas novedades a los administradores funcionales para que se restablezcan o inhabiliten definitivamente los accesos.

En caso que se requiera obtener información de una cuenta de usuario, que se encuentre ausente de forma temporal o definitiva, únicamente podrá ser solicitado por su jefe inmediato o supervisor de contrato a través de correo electrónico dirigido al Jefe o Directivo responsable del activo. En el caso de jefes o directivos también pueden solicitar la información de la persona a la que reemplacen.

En el caso de traslados de personal de una dependencia a otra, se lleva a cabo la eliminación de la información alojada en el servidor de archivos del cargo anterior, según lo establecido en la Política TI-PO-010 de Generación y Restauración de Copias de Respaldo.

Cualquier omisión o incumplimiento a los lineamientos contemplados en el presente procedimiento será considerada una falta a los protocolos de seguridad de información y se procederá de acuerdo a lo establecido en la Política de Seguridad, Privacidad de Información y Seguridad Digital de la USPEC.

A través de entrevistas en sitio, se evidenció que no hay revocación de accesos a la información de los usuarios que son promovidos internamente. Sustentado en acta del 10 de junio 2026.

Evidencia hallazgo 9: Ausencia de un plan periódico de pruebas y verificación de integridad para la recuperación de copias de seguridad. (No Conformidad Mayor)

Hasta el 2024 se estaba realizando el plan de pruebas de restauración de BackUps.

No se esta realizando las pruebas de restauración.

No hay un plan de continuidad de negocio.

Se van a empezar a definir los BIAS con cada una de las áreas.

Inventario de activos

RTOs y RPOs desactualizados (2020-2021)

2021 ultima actualización.

De acuerdo con la revisión en sitio, se verificó a través de entrevistas el control de pruebas de restauración de backups.

Evidencia hallazgo 10: Inexistencia de un Plan de Continuidad del Negocio (BCP), Análisis de Impacto (BIA) y esquemas de contingencia operativa (No Conformidad Mayor).

Hasta el 2024 se estaba realizando el plan de pruebas de restauración de BackUps.

No se esta realizando las pruebas de restauración.

No hay un plan de continuidad de negocio.

Se van a empezar a definir los BIAS con cada una de las áreas.

Inventario de activos

RTOs y RPOs desactualizados (2020-2021)

2021 ultima actualización.

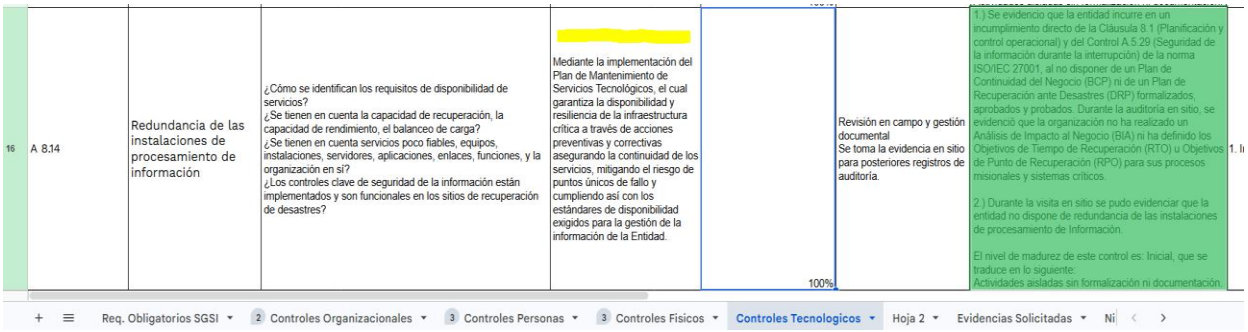
Servicios en la nube.

Critico: humano Nube

Gestión documental: nube.

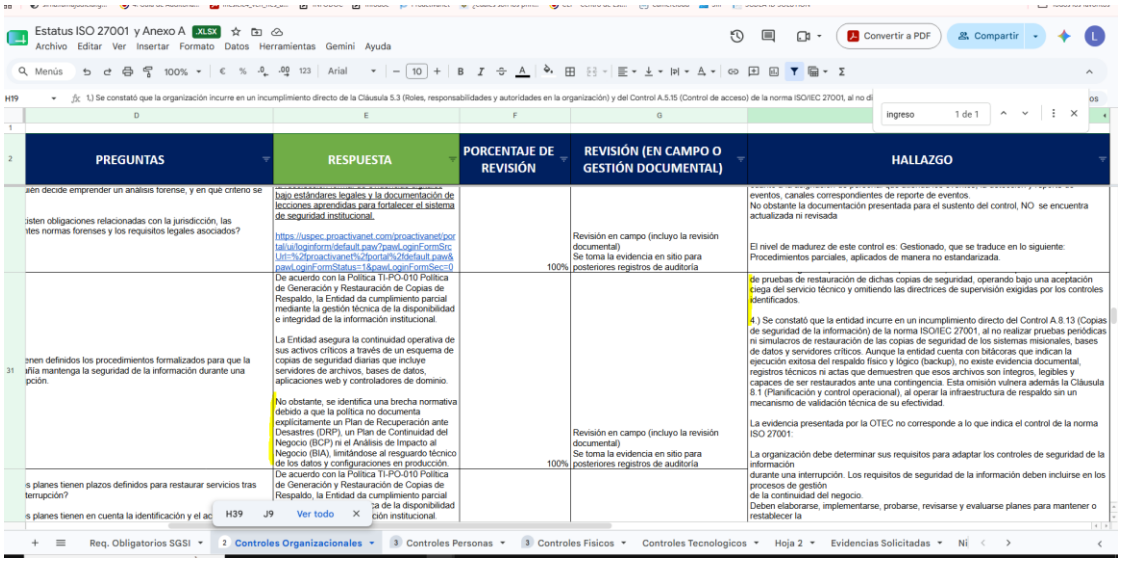
Sistema misional en la nube.

De acuerdo con la revisión en sitio, se verificó a través de entrevistas el control de pruebas de restauración de backups.



16	A 8.14	Redundancia de las instalaciones de procesamiento de información	¿Cómo se identifican los requisitos de disponibilidad de servicios? ¿Se tienen en cuenta la capacidad de recuperación, la capacidad de rendimiento, el balanceo de carga? ¿Se tienen en cuenta servicios poco fiables, equipos, instalaciones, servidores, aplicaciones, enlaces, funciones, y la organización en sí? ¿Los controles clave de seguridad de la información están implementados y son funcionales en los sitios de recuperación de desastres?	[redacted] Mediante la implementación del Plan de Mantenimiento de Servicios Tecnológicos, el cual garantiza la disponibilidad y resiliencia de la infraestructura crítica a través de acciones preventivas y correctivas asegurando la continuidad de los servicios, mitigando el riesgo de puntos únicos de fallo y cumpliendo así con los estándares de disponibilidad exigidos para la gestión de la información de la Entidad.	100%	Revisión en campo y gestión documental Se toma la evidencia en sitio para posteriores registros de auditoría.	1.) Se evidencio que la entidad incurre en un incumplimiento directo de la Cláusula 8.1 (Planificación y control operacional) y del Control A.5.29 (Seguridad de la información durante la interrupción) de la norma ISO/IEC 27001, al no disponer de un Plan de Continuidad del Negocio (BCP) ni de un Plan de Recuperación ante Desastres (DRP) formalizados, aprobados y probados. Durante la auditoría en sitio, se evidenció que la organización no ha realizado un Análisis de Impacto al Negocio (BIA) ni ha definido los Objetivos de Tiempo de Recuperación (RTO) u Objetivos de Punto de Recuperación (RPO) para sus procesos misionales y sistemas críticos. 2.) Durante la visita en sitio se pudo evidenciar que la entidad no dispone de redundancia de las instalaciones de procesamiento de Información. El nivel de madurez de este control es: Inicial, que se traduce en lo siguiente: Actividades aisladas sin formalización ni documentación.	1. In

Req. Obligatorios SGSI | 2 Controles Organizacionales | 3 Controles Personas | 3 Controles Físicos | Controles Tecnologicos | Hoja 2 | Evidencias Solicitadas | Ni



Estatus ISO 27001 y Anexo A .XLSX

Archivo Editar Ver Insertar Formato Datos Herramientas Gemini Ayuda

Convertir a PDF | Compartir

	PREGUNTAS	RESPUESTA	PORCENTAJE DE REVISIÓN	REVISIÓN (EN CAMPO O GESTIÓN DOCUMENTAL)	HALLAZGO
	uién decide emprender un análisis forense, y en qué criterio se	bajo estándares legales y la documentación de lecciones aprendidas para fortalecer el sistema de seguridad institucional. https://uspec.proactivanet.com/proactivanet/portal/ui/loginform/default.paw?pawLoginFormSrcUrl=%2fproactivanet%2fportal%2fdefault.paw&pawLoginFormStatus=1&pawLoginFormSec=0	100%	Revisión en campo (incluyo la revisión documental) Se toma la evidencia en sitio para posteriores registros de auditoría	eventos, canales correspondientes de reporte de eventos. No obstante la documentación presentada para el sustento del control, NO se encuentra actualizada ni revisada El nivel de madurez de este control es: Gestionado, que se traduce en lo siguiente: Procedimientos parciales, aplicados de manera no estandarizada.
	isten obligaciones relacionadas con la jurisdicción, las ntes normas forenses y los requisitos legales asociados?				
31	enen definidos los procedimientos formalizados para que la iñila mantenga la seguridad de la información durante una pción.	De acuerdo con la Política TI-PO-010 Política de Generación y Restauración de Copias de Respaldo, la Entidad da cumplimiento parcial mediante la gestión técnica de la disponibilidad e integridad de la información institucional. La Entidad asegura la continuidad operativa de sus activos críticos a través de un esquema de copias de seguridad diarias que incluye servidores de archivos, bases de datos, aplicaciones web y controladores de dominio. No obstante, se identifica una brecha normativa debido a que la política no documenta explícitamente un Plan de Recuperación ante Desastres (DRP), un Plan de Continuidad del Negocio (BCP) ni el Análisis de Impacto al Negocio (BIA), limitándose al resguardo técnico de los datos y configuraciones en producción.	100%	Revisión en campo (incluyo la revisión documental) Se toma la evidencia en sitio para posteriores registros de auditoría	de pruebas de restauración de dichas copias de seguridad, operando bajo una aceptación ciega del servicio técnico y omitiendo las directrices de supervisión exigidas por los controles identificados. 4.) Se constató que la entidad incurre en un incumplimiento directo del Control A.8.13 (Copias de seguridad de la información) de la norma ISO/IEC 27001, al no realizar pruebas periódicas ni simulacros de restauración de las copias de seguridad de los sistemas misionales, bases de datos y servidores críticos. Aunque la entidad cuenta con bitácoras que indican la ejecución exitosa del respaldo físico y lógico (backup), no existe evidencia documental, registros técnicos ni actas que demuestren que esos archivos son íntegros, legibles y capaces de ser restaurados ante una contingencia. Esta omisión vulnera además la Cláusula 8.1 (Planificación y control operacional), al operar la infraestructura de respaldo sin un mecanismo de validación técnica de su efectividad. La evidencia presentada por la OTEC no corresponde a lo que indica el control de la norma ISO 27001: La organización debe determinar sus requisitos para adaptar los controles de seguridad de la información durante una interrupción. Los requisitos de seguridad de la información deben incluirse en los procesos de gestión de la continuidad del negocio. Deben elaborarse, implementarse, probarse, revisarse y evaluarse planes para mantener o restablecer la
	s planes tienen plazos definidos para restaurar servicios tras terrupción?	De acuerdo con la Política TI-PO-010 Política de Generación y Restauración de Copias de Respaldo, la Entidad da cumplimiento parcial			
	s planes tienen en cuenta la identificación y el ac	ción institucional.			

H39 J9 Ver todo

Req. Obligatorios SGSI | 2 Controles Organizacionales | 3 Controles Personas | 3 Controles Físicos | Controles Tecnologicos | Hoja 2 | Evidencias Solicitadas | Ni

Evidencia hallazgo 11: Uso de credenciales compartidas y cuentas genéricas para el acceso a sistemas de información institucionales (No Conformidad Mayor).

Sistema Humano

Dora Astrid Escobar- Profesional Universitario.

Diana Carolina-Nomina- Liquidación de nómina.

Recepción del insumo de la nómina a través de diferentes maneras:

Física y correo electrónico (novedades en la nómina). Mensuales Periodicidad recurrente.

Correo electrónico: nomina@uspec.gov.co

Clave compartida del correo electrónico de la unidad de nómina. **Riesgo de fuga de información.**

Incapacidades y fondo nacional de correo.

Auxiliar y líder técnico.

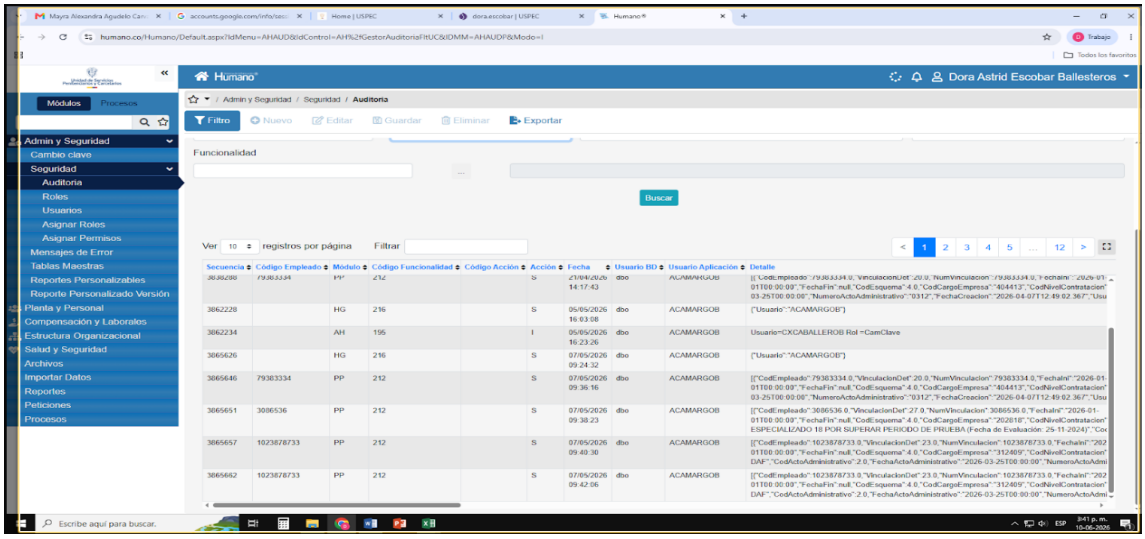
Humano-> aplicativo (soporte lógico) acceso a diferentes módulos de acuerdo con los permisos otorgados.

Administrador Yeimmy Lorena Martínez.

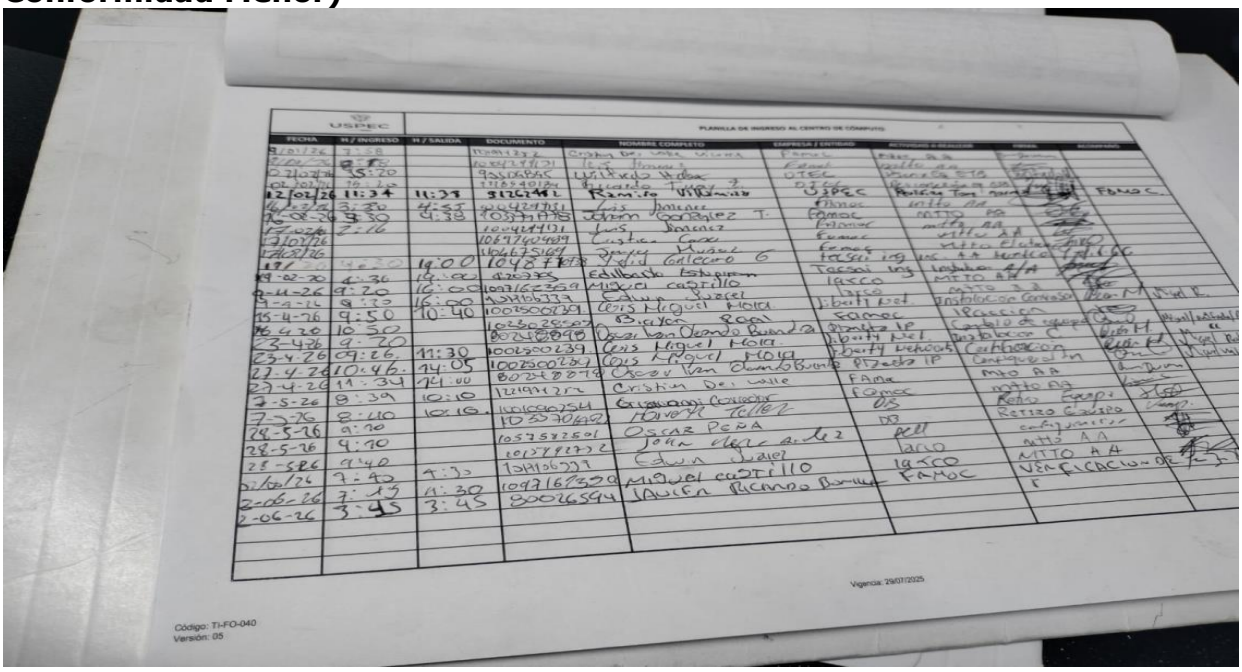
Contabilidad y tesorería. July Bustos e Isabel Cristina Díaz

Capacitación a nivel de la aplicación. Cambio de contraseña a la primera vez que ingresa a la plataforma. July Bustos puede ser administradora la aplicación.

A través de la revisión en sitio se evidenció que existe el riesgo de compartir las credenciales de acceso al correo electrónico de nómina.



Evidencia hallazgo 12: Ausencia de procedimientos formalizados para el control de acceso físico a áreas seguras e infraestructura crítica. (No Conformidad Menor)



Bitácora del acceso al Datacenter. Se puede observar que hay campos que no están diligenciados y que puede ser una causal de que no se pueda realizar una trazabilidad completa de las acciones realizadas de los usuarios que acceden al Datacenter

Evidencia hallazgo 13: Deficiencias en el control y trazabilidad del ingreso y salida de activos tecnológicos en las instalaciones de la entidad. (No Conformidad Menor).

Acceso ilimitado

Zonas donde hay control restritivo: gestión documental, oficina de tecnología, Datacenter.

Ingreso de visitantes a través de correo electrónico.

Se envía un nuevo correo indicando la prolongación de la estadía del visitante.

7/24 disponibilidad para el acceso físico.

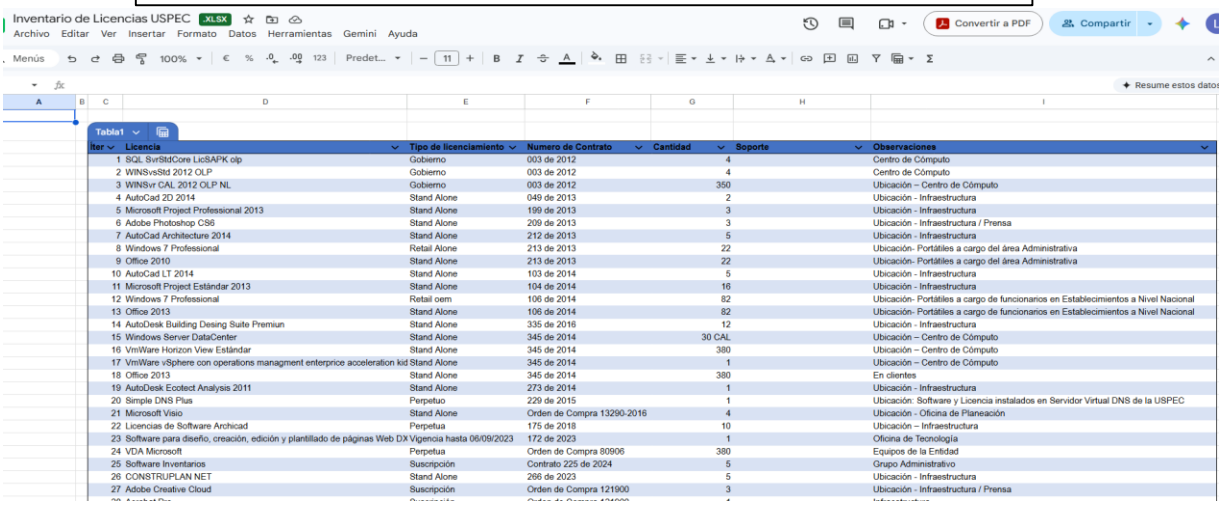
No hay limitación para el acceso a las oficinas de la entidad.

Se esta actualizando el documento correspondiente al procedimiento de áreas seguras.

Mes de junio.

No se esta llevando control sobre dispositivos tecnológicos.

No hay una inspección de maletas. Levantamiento de acta



Iter	Licencia	Tipo de licenciamiento	Numero de Contrato	Cantidad	Soporte	Observaciones
1	SQL SvrStdCore LicSAPK olp	Gobierno	003 de 2012	4		Centro de Cómputo
2	WINSvsStd 2012 OLP	Gobierno	003 de 2012	4		Centro de Cómputo
3	WINSvr CAL 2012 OLP NL	Gobierno	003 de 2012	350		Ubicación – Centro de Cómputo
4	AutoCad 2D 2014	Stand Alone	049 de 2013	2		Ubicación - Infraestructura
5	Microsoft Project Professional 2013	Stand Alone	199 de 2013	3		Ubicación - Infraestructura
6	Adobe Photoshop CS6	Stand Alone	209 de 2013	3		Ubicación - Infraestructura / Prensa
7	AutoCad Architecture 2014	Stand Alone	212 de 2013	5		Ubicación - Infraestructura
8	Windows 7 Professional	Retail Alone	213 de 2013	22		Ubicación- Portátiles a cargo del área Administrativa
9	Office 2010	Stand Alone	213 de 2013	22		Ubicación- Portátiles a cargo del área Administrativa
10	AutoCad LT 2014	Stand Alone	103 de 2014	5		Ubicación - Infraestructura
11	Microsoft Project Estándar 2013	Stand Alone	104 de 2014	16		Ubicación - Infraestructura
12	Windows 7 Professional	Retail oem	106 de 2014	82		Ubicación- Portátiles a cargo de funcionarios en Establecimientos a Nivel Nacional
13	Office 2013	Stand Alone	106 de 2014	82		Ubicación- Portátiles a cargo de funcionarios en Establecimientos a Nivel Nacional
14	AutoDesk Building Desing Suite Premiun	Stand Alone	335 de 2016	12		Ubicación - Infraestructura
15	Windows Server DataCenter	Stand Alone	345 de 2014	30 CAL		Ubicación – Centro de Cómputo
16	VmWare Horizon View Estándar	Stand Alone	345 de 2014	380		Ubicación – Centro de Cómputo
17	VmWare vSphere con operations managment enterprice acceleration kid	Stand Alone	345 de 2014	1		Ubicación – Centro de Cómputo
18	Office 2013	Stand Alone	345 de 2014	380		En clientes
19	AutoDesk Ecotect Analysis 2011	Stand Alone	273 de 2014	1		Ubicación - Infraestructura
20	Simple DNS Plus	Perpetuo	229 de 2015	1		Ubicación- Software y Licencia instalados en Servidor Virtual DNS de la USPEC
21	Microsoft Visio	Stand Alone	Orden de Compra 13290-2016	4		Ubicación - Oficina de Planeación
22	Licencias de Software Archicad	Perpetua	175 de 2018	10		Ubicación – Infraestructura
23	Software para diseño, creación, edición y plantillado de páginas Web DX	Vigencia hasta 06/09/2023	172 de 2023	1		Oficina de Tecnología
24	VDA Microsoft	Perpetua	Orden de Compra 80906	380		Equipos de la Entidad
25	Software Inventarios	Suscripción	Contrato 225 de 2024	5		Grupo Administrativo
26	CONSTRUPLAN NET	Stand Alone	266 de 2023	5		Ubicación - Infraestructura
27	Adobe Creative Cloud	Suscripción	Orden de Compra 121900	3		Ubicación - Infraestructura / Prensa

A través de revisión en sitio y por medio de entrevistas, se evidencia que no existe un protocolo y/o procedimiento de revisión sobre los dispositivos tecnológicos.

Evidencia hallazgo 14: Deficiencias en los procedimientos para la destrucción

segura de documentos físicos que contienen información sensible. (No Conformidad Menor).

Tarjetas físicas: entidad administra las tarjetas.

Activación de la tarjeta para cada una de las ubicaciones.

Formato de vigencia de las tarjetas. Nombre: Asignación de perfiles de acceso en tarjetas magnéticas.

Existe un inventario de las tarjetas entregadas a los funcionarios de la entidad. Queda pendiente el inventario. Histórico de las tarjetas de acceso cuando han sido registrados a más de un servidor (funcionarios directos y contratistas)

Proceso de carnetización: paz y salvo. Proceso de destrucción del carne corporativo.

Destrucción del carne. Una persona que administre la destrucción.

No quedan registros de la destrucción.

No hay un seguimiento de la destrucción del carne físico. Levantamiento de acta (evidencia)

Grupo administrativo se hace la solicitud de manejo, gestión y soporte de las tarjetas (segregación de funciones) La persona que maneja las tarjetas no puede ser la misma que las destruye.

A través de entrevistas en sitio se evidencio que no existe un procedimiento para la destrucción física de documentos

Evidencia hallazgo 15: Deficiencias en la administración, revisión y monitoreo de los sistemas de control de acceso biométrico a áreas críticas. (No Conformidad Menor).

Registro de usuarios.

Proveedor gestiona directamente el manejo del dispositivo

Control manager.

No han tenido la necesidad de solicitar un registro de logs.

Personas desvinculadas

Pendiente: Informe del ejercicio de Ingenieria Social

Biométrico: registro mensual

No existe un procedimiento formal que permita identificar el paso a paso de la revisión de los elementos de físicos de acceso a cada una de las áreas definidas por la entidad, no por el simple hecho de que exista una revisión por parte del proveedor, al entidad se desligue por completo de hacer sus propias validaciones.

40 usuarios por biométrico. Por áreas.

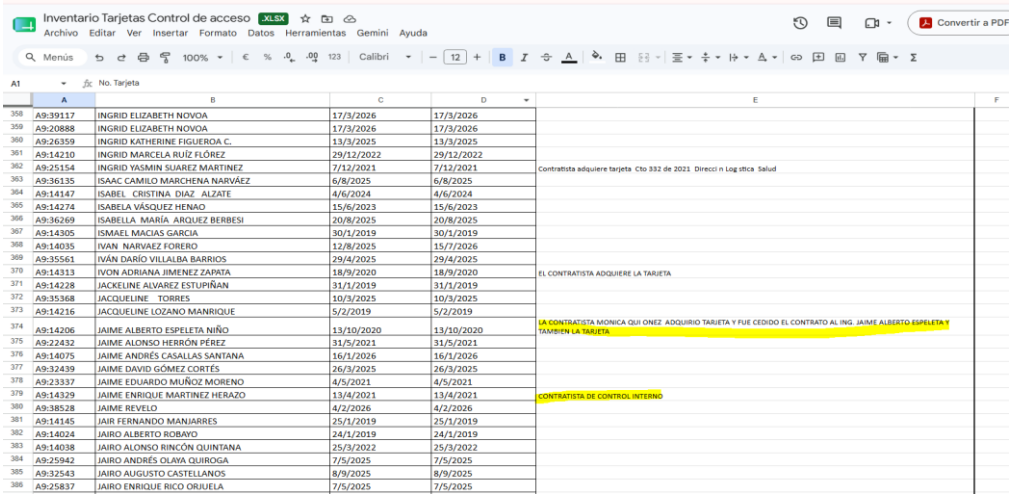
Pendiente: revisión mensual del biométrico de los últimos tres meses.

CCTV: Gestión compartida con administración.

Autorización para ingresar al aplicativo para realizar revisión de cámaras.

Tiempo almacenado: llenado de disco duro. 2 meses Aprox.

Notas tomadas en sitio referente al proceso de revisión de logs de los sistemas Biométricos.



Inventario Tarjetas Control de acceso .XLSX

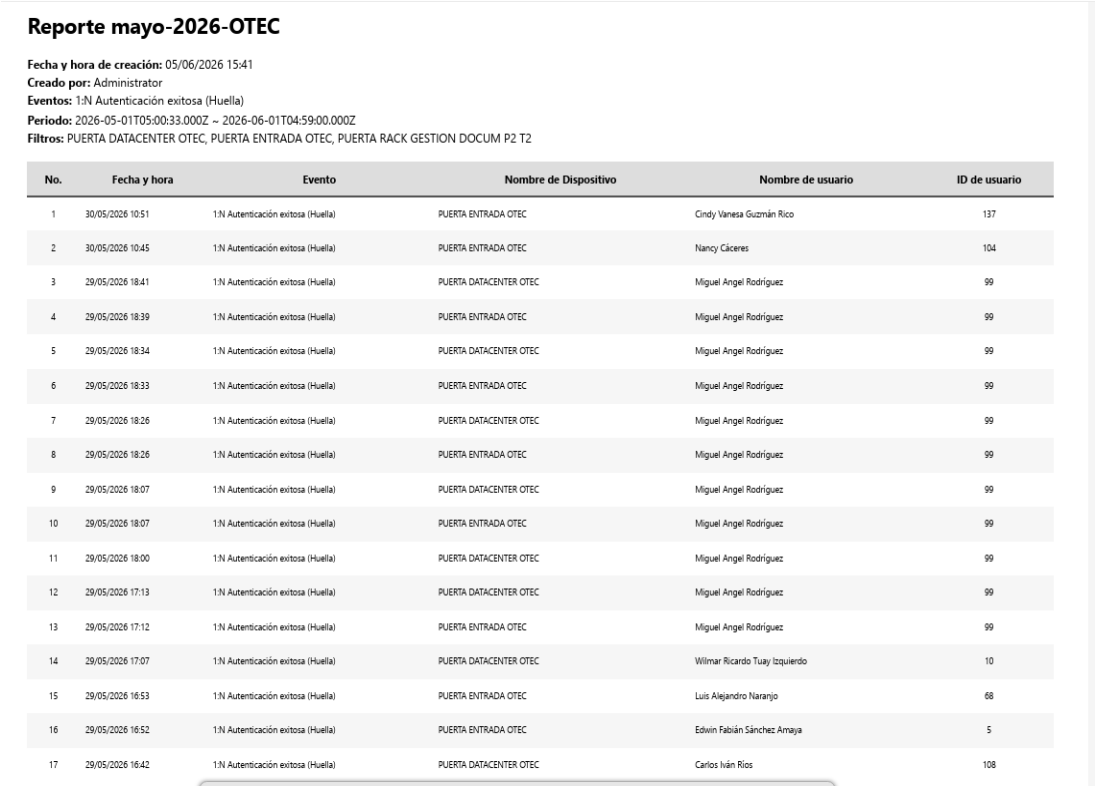
Archivo Editar Ver Insertar Formato Datos Herramientas Gemini Ayuda

Convertir a PDF

Menús 100% Calibri 12

A1 No. Tarjeta

	A	B	C	D	E	F
358	A9:39117	INGRID ELIZABETH NOVOA	17/3/2026	17/3/2026		
359	A9:20888	INGRID ELIZABETH NOVOA	17/3/2026	17/3/2026		
360	A9:26359	INGRID KATHERINE FIGUEROA C.	13/3/2025	13/3/2025		
361	A9:14210	INGRID MARCELA RUÍZ FLÓREZ	29/12/2022	29/12/2022		
362	A9:25154	INGRID YASMIN SUAREZ MARTINEZ	7/12/2021	7/12/2021	Contratista adquiere tarjeta Cto 332 de 2021 Direcci n Log stica Salud	
363	A9:36135	ISAAC CAMILO MARCHENA NARVÁEZ	6/8/2025	6/8/2025		
364	A9:14147	ISABEL CRISTINA DIAZ ALZATE	4/6/2024	4/6/2024		
365	A9:14274	ISABELA VÁSQUEZ HENAO	15/6/2023	15/6/2023		
366	A9:36269	ISABELLA MARÍA ARQUEZ BERBESI	20/8/2025	20/8/2025		
367	A9:14305	ISMAEL MACIAS GARCIA	30/1/2019	30/1/2019		
368	A9:14035	IVAN NARVAEZ FORERO	12/8/2025	15/7/2026		
369	A9:35561	IVÁN DARÍO VILLALBA BARRIOS	29/4/2025	29/4/2025		
370	A9:14313	IVON ADRIANA JIMENEZ ZAPATA	18/9/2020	18/9/2020	EL CONTRATISTA ADQUIERE LA TARJETA	
371	A9:14228	JACKELINE ALVAREZ ESTUPIÑAN	31/1/2019	31/1/2019		
372	A9:35368	JACQUELINE TORRES	10/3/2025	10/3/2025		
373	A9:14216	JACQUELINE LOZANO MANRIQUE	5/2/2019	5/2/2019		
374	A9:14206	JAIME ALBERTO ESPELETA NIÑO	13/10/2020	13/10/2020	LA CONTRATISTA MONICA QUI ONEZ ADQUIRIO TARJETA Y FUE CEDIDO EL CONTRATO AL ING. JAIME ALBERTO ESPELETA Y TAMBIEN LA TARJETA	
375	A9:22432	JAIME ALONSO HERRÓN PÉREZ	31/5/2021	31/5/2021		
376	A9:14075	JAIME ANDRÉS CASALLAS SANTANA	16/1/2026	16/1/2026		
377	A9:32439	JAIME DAVID GÓMEZ CORTÉS	26/3/2025	26/3/2025		
378	A9:23337	JAIME EDUARDO MUÑOZ MORENO	4/5/2021	4/5/2021		
379	A9:14329	JAIME ENRIQUE MARTINEZ HERAZO	13/4/2021	13/4/2021	CONTRATISTA DE CONTROL INTERNO	
380	A9:38528	JAIME REVELO	4/2/2026	4/2/2026		
381	A9:14145	JAIR FERNANDO MANJARRES	25/1/2019	25/1/2019		
382	A9:14024	JAIRO ALBERTO ROBAYO	24/1/2019	24/1/2019		
383	A9:14038	JAIRO ALONSO RINCÓN QUINTANA	25/3/2022	25/3/2022		
384	A9:25942	JAIRO ANDRÉS OLAYA QUIROGA	7/5/2025	7/5/2025		
385	A9:32543	JAIRO AUGUSTO CASTELLANOS	8/9/2025	8/9/2025		
386	A9:25837	JAIRO ENRIQUE RICO ORJUELA	7/5/2025	7/5/2025		



Reporte mayo-2026-OTEC

Fecha y hora de creación: 05/06/2026 15:41
Creado por: Administrator
Eventos: 1:N Autenticación exitosa (Huella)
Periodo: 2026-05-01T05:00:33.000Z ~ 2026-06-01T04:59:00.000Z
Filtros: PUERTA DATACENTER OTEC, PUERTA ENTRADA OTEC, PUERTA RACK GESTION DOCUM P2 T2

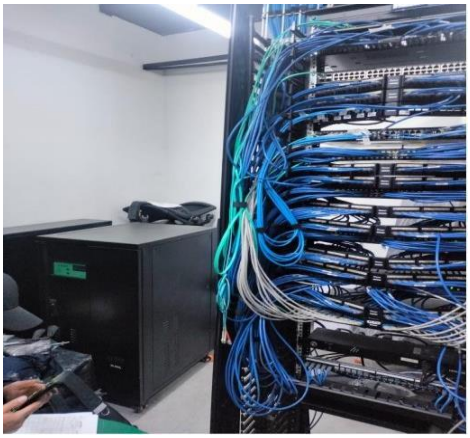
No.	Fecha y hora	Evento	Nombre de Dispositivo	Nombre de usuario	ID de usuario
1	30/05/2026 10:51	1:N Autenticación exitosa (Huella)	PUERTA ENTRADA OTEC	Cindy Vanesa Guzmán Rico	137
2	30/05/2026 10:45	1:N Autenticación exitosa (Huella)	PUERTA ENTRADA OTEC	Nancy Cáceres	104
3	29/05/2026 18:41	1:N Autenticación exitosa (Huella)	PUERTA DATACENTER OTEC	Miguel Angel Rodríguez	99
4	29/05/2026 18:39	1:N Autenticación exitosa (Huella)	PUERTA ENTRADA OTEC	Miguel Angel Rodríguez	99
5	29/05/2026 18:34	1:N Autenticación exitosa (Huella)	PUERTA DATACENTER OTEC	Miguel Angel Rodríguez	99
6	29/05/2026 18:33	1:N Autenticación exitosa (Huella)	PUERTA ENTRADA OTEC	Miguel Angel Rodríguez	99
7	29/05/2026 18:26	1:N Autenticación exitosa (Huella)	PUERTA DATACENTER OTEC	Miguel Angel Rodríguez	99
8	29/05/2026 18:26	1:N Autenticación exitosa (Huella)	PUERTA ENTRADA OTEC	Miguel Angel Rodríguez	99
9	29/05/2026 18:07	1:N Autenticación exitosa (Huella)	PUERTA DATACENTER OTEC	Miguel Angel Rodríguez	99
10	29/05/2026 18:07	1:N Autenticación exitosa (Huella)	PUERTA ENTRADA OTEC	Miguel Angel Rodríguez	99
11	29/05/2026 18:00	1:N Autenticación exitosa (Huella)	PUERTA DATACENTER OTEC	Miguel Angel Rodríguez	99
12	29/05/2026 17:13	1:N Autenticación exitosa (Huella)	PUERTA DATACENTER OTEC	Miguel Angel Rodríguez	99
13	29/05/2026 17:12	1:N Autenticación exitosa (Huella)	PUERTA ENTRADA OTEC	Miguel Angel Rodríguez	99
14	29/05/2026 17:07	1:N Autenticación exitosa (Huella)	PUERTA DATACENTER OTEC	Wilmar Ricardo Tuay Izquierdo	10
15	29/05/2026 16:53	1:N Autenticación exitosa (Huella)	PUERTA ENTRADA OTEC	Luis Alejandro Naranjo	68
16	29/05/2026 16:52	1:N Autenticación exitosa (Huella)	PUERTA ENTRADA OTEC	Edwin Fabián Sánchez Amaya	5
17	29/05/2026 16:42	1:N Autenticación exitosa (Huella)	PUERTA DATACENTER OTEC	Carlos Iván Ríos	108

Evidencia hallazgo 16: Deficiencias en las condiciones de orden, almacenamiento y protección física de activos tecnológicos en áreas críticas. (No Conformidad Menor).

16.1

Cajas apiladas en el área de Datacenter, bloqueando el acceso a los tableros de emergencia.

16.2



Sillas apiladas en el cuarto técnico del piso 13.

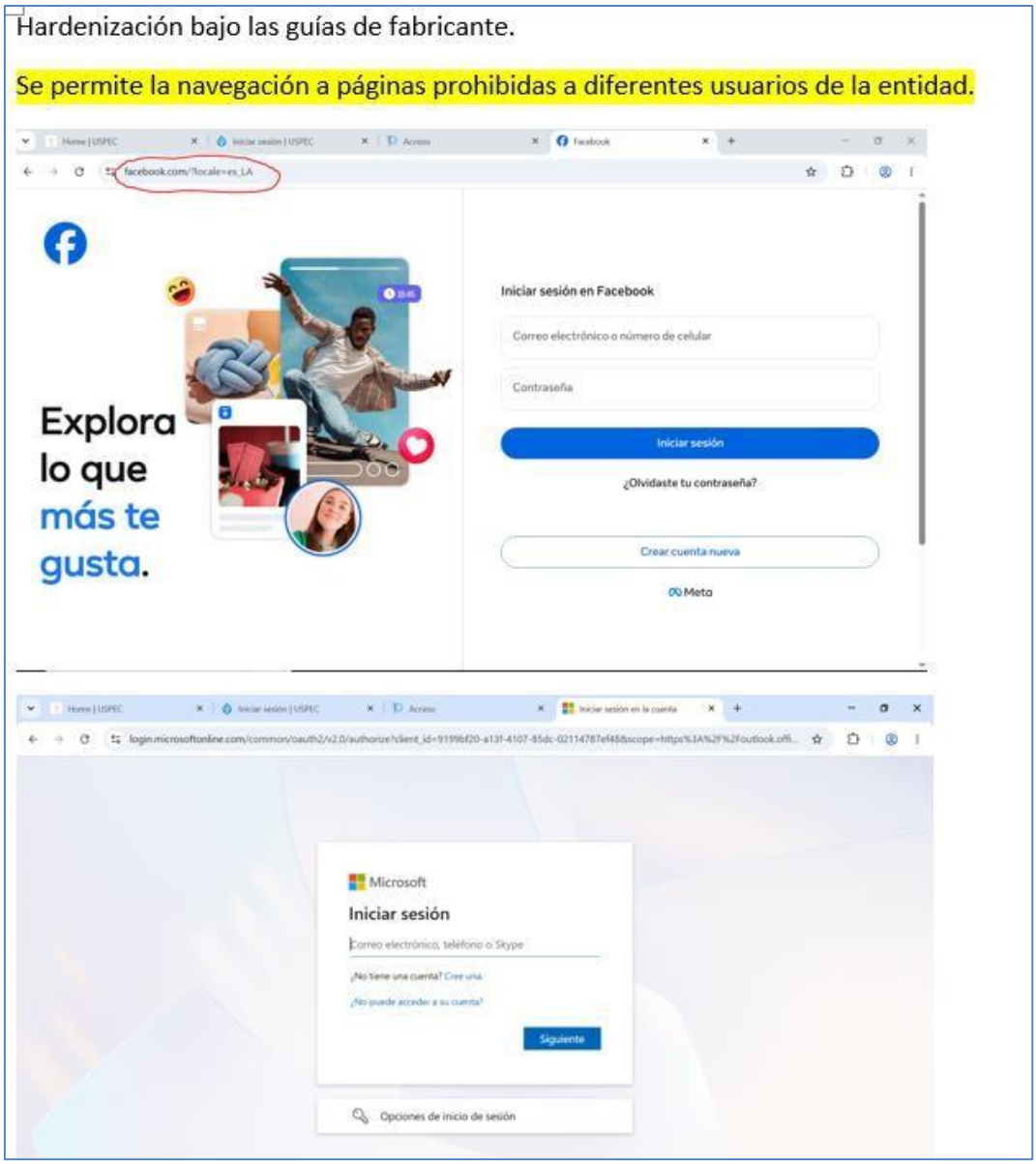
16.3

"Botellón de agua" sobre el rack de comunicaciones, el cual NO corresponde a la función definida por la entidad.

16.4

Mas sillas apiladas en el cuarto técnico del piso 13.

Evidencia hallazgo 17: Deficiencias en la implementación de controles de filtrado y restricción de navegación web. (No Conformidad Mayor).



Evidencia hallazgo 18: Inconsistencia entre los parámetros de autenticación implementados y el Procedimiento de Gestión de Accesos e Identidades. (No Conformidad Menor).

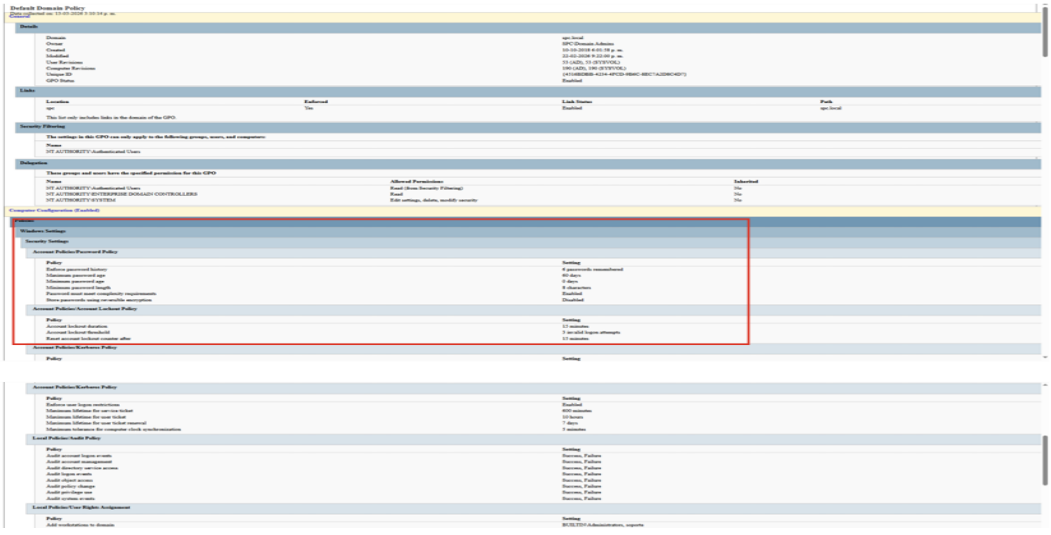
GPO:

60 días cambio de contraseña

Y 8 caracteres.

La Política de gestión de contraseñas no coincide con las condiciones establecidas en el procedimiento de gestión de contraseñas.

Usuario super administrador: 4+ personas de mesa de ayuda (4)



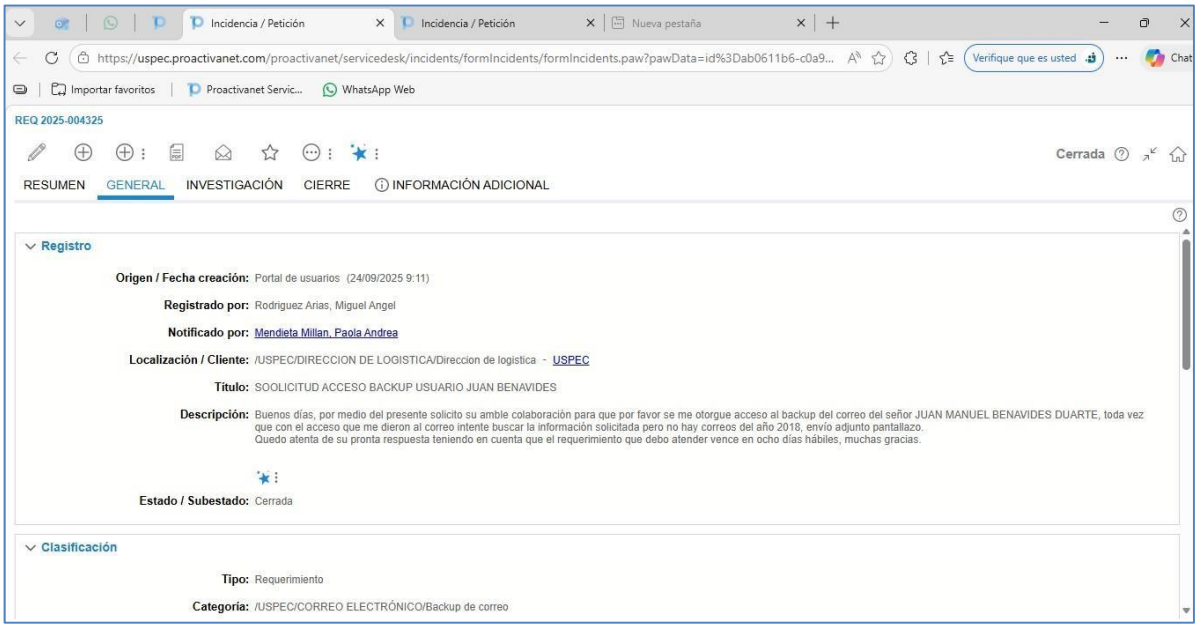
Validación en sitio sobre las configuraciones de las contraseñas.

Evidencia hallazgo 19: Deficiencias en la trazabilidad y formalización de la gestión de solicitudes e incidentes de la Mesa de Ayuda de TI. (No Conformidad Menor).

19.1

Notificación por correo electrónico acerca de la asignación de los casos a una persona en específico.

19.2



Asignación del caso a través del sistema de información de la mesa de ayuda: "Proactivanet."

Elaboró	Revisó:	Aprobó:
Nombre: Walter Raúl Niño Pérez Walter Raúl Niño Pérez	Nombre: Lady Marcela Meléndez	Nombre: Germán Gaitán
Cargo: Contratista Control Interno	Cargo: Profesional Universitario	Cargo: Jefe de oficina
Dependencia: Oficina Control Interno	Dependencia: Oficina Control Interno	Dependencia: Oficina Control Interno