UNIDAD DE BÚSQUEDA
DE PERSONAS DADAS POR DESAPARECIDAS
UBPD

INFORME EJECUTIVO FINAL DE AUDITORIA

Auditoria de Seguimiento a los Resultados de la Auditoria al Sistema de Seguridad de la Información SSI de la vigencia 2024.

CIUDAD Y FECHA: BOGOTA, 19 DE DICIEMBRE DE 2025

Dirigido a: Doctora Luz Janeth Forero Martínez, Directora General

Miembros Comité Institucional de Coordinación de Control Interno

Tabla 1 - Datos Generales

Tipo de Informe	Ejecutivo
Título del Informe de Auditoría:	Auditoria de Seguimiento a los Resultados de Auditoria al Sistema de Seguridad de la Información SSI de la vigencia 2024
Unidad Auditable:	Oficial de Seguridad de la Información OSI Oficina de Tecnologías de la Información y las Comunicaciones OTIC
Líder de Proceso / Jefe(s) Dependencia(s):	Oficial de Seguridad de la Información OSI Jefe de Oficina de Tecnologías de la Información y las
Objetivo de la Auditoría:	Verificar el estado de gestión adelantada frente a los resultados presentados del informe definitivo de auditoria al SSI de la vigencia 2024.
Objetivos Específicos:	Verificar el estado de gestión de las 3 Observaciones y 17 Recomendaciones del Informe de Auditoría.
Alcance de la Auditoría:	Actividades desarrolladas entre el 12 de marzo de 2025 al 31 de octubre de 2025, en relación con las observaciones y recomendaciones presentadas en el informe definitivo de auditoria al SSI de la vigencia 2024.
Criterios de la Auditoría:	Informe Definitivo de Auditoría al SSI vigencia 2024 Planes de Mejoramiento Resultados de Auditoria/Situación Política General de Seguridad de la Información GTI-PC-001 V1 GSI Manual de Seguridad de la Información GTI-MN-002 V2 GSI Declaración de Aplicabilidad SoA Matriz de Riesgos del SSI Instrumento de Autoevaluación/Autodiagnóstico Plan de Recuperación de Desastres GTI-PL-002 V1 Plan Estratégico de Seguridad de la Información PESI Resolución No. 1269 de 2023 Documentos del Sistema Integrado de Gestión SIG relacionados Resolución No. 277 de 2025 Norma Técnica NTC-ISO/IEC 27001:2013 Norma Técnica NTC-ISO/IEC 27001:2022 Decreto No. 1393 de 2018.pdf
Equipo Auditor	**Líder de la Auditoría:** Carlos Andrés Rico Reina, Experto Técnico. **Auditor (es):** Carlos Andrés Rico Reina, Experto Técnico.
Jefe Oficina de Control Interno	Duvy Johanna Plazas Socha

Tabla 2 - Hitos Principales

REUNIÓN DE APERTURA	EJECUCIÓN DE LA AUDITORIA	REUNIÓN DE CIERRE
10 de noviembre de 2025	10 de noviembre al 05 de diciembre de 2025	18 de diciembre de 2025

1. RESUMEN DE RESULTADOS

Tabla 3 - Resultados

FORTALEZAS	HALLAZGOS	OBSERVACIONES	RECOMENDACIONES
4	10	0	36

2. RESULTADOS DE LA AUDITORIA

2.1. FORTALEZAS

1. Fortaleza Estructural de Gobernanza: Se logró un hito importante y estratégico al separar formalmente el apoyo técnico del Oficial de Seguridad de la Información OSI de la Oficina de Tecnologías de la Información y las Comunicaciones OTIC. Esto garantiza la independencia estructural y la objetividad de la Segunda Línea de Defensa del Sistema de Seguridad de la Información SSI.

2. La Oficina de Tecnologías de la Información y las Comunicaciones OTIC demostró capacidad de respuesta al migrar de un Plan de Recuperación ante Desastres DRP manual a un modelo "Asistido Automático - Burbuja - SureBackup". Esto hace que las pruebas de recuperación sean seguras, repetibles y programables, eliminando el riesgo de afectar las operaciones.

3. La Oficina de Tecnologías de la Información y las Comunicaciones OTIC utiliza tecnologías avanzadas como lo es el Firewall de Aplicaciones Web WAF bajo el modo de detección NOC y realiza análisis forenses y ejercicios de *reversing* (simulación de ataques) para asegurar la infraestructura. Esto supera el requisito de solo tener un antivirus y proporciona una defensa proactiva contra amenazas complejas.

4. En julio de 2025, el Oficial de Seguridad de la Información OSI elaboró el “Reporte de Diagnostico – Sistema de Gestión de Seguridad de la Información SGSI”, donde, en resumen, se indicó que, presenta un estado de alta vulnerabilidad y riesgo operativo, a pesar de tener una base sólida en la identificación de riesgos con un 60% de madurez. El principal riesgo existencial es la ausencia casi total de un Plan de Continuidad del Negocio BCP y Plan de Recuperación de Desastres DRP, con solo un 10% de madurez. Esta situación se agrava por el hecho de que la documentación de gobernanza es obsoleta, incluyendo manuales, guías y políticas que datan de 2020, y la estructura de Roles y Responsabilidades y la Política General de Seguridad carecen de la aprobación formal del Comité Directivo. A pesar de que la Gestión de Riesgos está en un 90% de madurez, el problema más crítico es la inacción para corregir las fallas; una auditoría de noviembre de 2024 identificó 20 hallazgos que fueron aceptados, pero el avance en los planes de mejoramiento correspondientes a 2025 es de un alarmante 20%, lo que compromete la sostenibilidad y la misión de la entidad.

   A partir del informe de diagnóstico, el Oficial de Seguridad de la Información OSI elaboro el “Plan de Acción del Sistema de Seguridad de la Información SSI, que busca aumentar la madurez y eficacia del SSI, mitigar riesgos y promover una cultura de seguridad mediante el monitoreo.

   El OSI ha cumplido con la fase, "Planificación", al incluir los indicadores clave de desempeño KPI iniciales, que abarcan métricas de riesgo, cumplimiento y cultura de seguridad. Dicha inclusión marca el cambio estratégico de la medición de proyectos a la medición de resultados.

2.2. Hallazgos

1. Gestión de Seguridad de la Información para Dispositivos Personales, Móviles e Institucionales para Labores por Fuera de las Instalaciones y su Uso Seguro de los Servicios de Red. (Recomendaciones 1, 7, 12, Observaciones 1 y 2 del informe de Auditoría SSI 2024)

No.	Descripción(es) del Hallazgo	Criterio(s)	Recomendación(es)
H1	1) El formato de inscripción de trabajo flexible o fuera de la sede (GTH-FT-038) sigue sin incluir la pregunta obligatoria para que el servidor declare si usará equipo personal o asignado por la Unidad. Además, la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) no realizó verificaciones de las condiciones de seguridad ni autorizó el uso de equipos personales para servidores con trabajo fuera de las instalaciones. La OCI verificó que los cambios recomendados para ser incluidos en el aplicativo "Tramitemos" no fueron implementados, dejando el control A.8.1 (Dispositivos de punto final del usuario) ineficaz. 2) Las políticas del Manual exigen autorizaciones y verificaciones manuales por parte de la OTIC para el uso de dispositivos móviles personales, pero la práctica actual es que la seguridad se establece automáticamente mediante un perfil de trabajo controlado al acceder a los recursos. Esta desalineación formal entre la política escrita (ISO 7.5) y el control técnico real deja en incumplimiento textual el control A.7.9 (Seguridad de los activos fuera de las instalaciones).	1) Políticas: 8.6 (Uso de dispositivos móviles) y 8.21 (Control para el Trabajo Seguro en Casa) del Manual de Seguridad de la Información GTI-MN-002 2) Cláusulas ISO/IEC 27001:2022: 5.1 (Políticas de seguridad de la información), 7.5 (Información documentada), 10.2 (No conformidad y acción correctiva) 3) Controles ISO/IEC 27001:2022: A7.9 (Seguridad de los activos fuera de las instalaciones), A.6.7 (Trabajo a distancia) y A.8.1 (Dispositivos de punto final del usuario),	Como bien se identificó en el diagnóstico y en el marco del Plan de Acción del Sistema de Seguridad de la Información SSI, se recomienda complementar las acciones con lo siguiente: 1) Realizar las verificaciones de gestión de seguridad para todos los equipos personales que van a ser utilizados por Servidores y Contratistas que acceden a los recursos de forma remota o interna 2) Para lo anteriores casos, monitorear y controlar las actividades de acceso y uso de activos de información críticos 3) De acuerdo con el proceso y plan actual de actualización del Manual de Seguridad de la Información liderado por el Oficial de Seguridad de la Información OSI, revisar y/o ajustar la pertinencia operativa de las

No.	Descripción(es) del Hallazgo	Criterio(s)	Recomendación(es)
	3) Falla en el monitoreo y la documentación de la seguridad de red. No se evidenció un proceso formal y documentado de revisión de las reglas del *firewall* y los componentes de la red accedidos por dispositivos móviles personales e institucionales. El control A.8.21 (Seguridad de los servicios de red) es débil porque falta una política clara y actualizada sobre el control de los dispositivos móviles y la segmentación de red. 4) Las Observaciones No. 1 y 2, codificadas como Acción de Mejora "SSI/59", se encuentran vencidas y con 0% de avance al reporte del último seguimiento (III trimestre de 2025). Se evidencio en los seguimientos que las evidencias reportadas (I Trimestre de 2025) no presentaron avances, ni cumplimiento a las acciones suscritas por el responsable de la acción, asimismo, no se presentaron monitoreos de avance.	A.8.21 (Seguridad de los servicios de red)	Políticas 8.6 y 8.21 sus lineamientos y literales 4) Incorporar en el formulario "Trabajo fuera de las instalaciones" del sistema informático Tramitemos, las declaraciones de uso de equipos de cómputo y/o dispositivos móviles personales o en su defecto institucionales, con el fin de que la Oficina de Tecnologías de la Información y las Comunicaciones OTIC realice las verificaciones de seguridad pertinentes 5) Monitorear el acceso remoto a activos de información críticos.

2. Controles Estructurales de Gobernanza, Restricción de Acceso a la Información, Administración de Derechos de Acceso Privilegiado (Recomendación No. 2, 8, 11 y Observación No. 3 del Informe de Auditoría SSI 2024).

No.	Descripción(es) del Hallazgo	Criterio(s)	Recomendación(es)
H2	1) En lo que respecta a la consistencia y efectividad de controles de seguridad en Roles y responsabilidades, la herramienta de gestión (Matriz de Roles y Perfiles) es inadecuada para el propósito del control. Carece de la información necesaria para auditar datos básicos del ciclo de	1) Política 8.9. (Control de cuentas privilegiadas) del Manual de Seguridad de la Información GTI-MN-002.	Como bien se identificó en el diagnóstico y en el marco del Plan de Acción del Sistema de Seguridad de la Información SSI, se recomienda complementar las acciones con lo siguiente:

No.	Descripción(es) del Hallazgo	Criterio(s)	Recomendación(es)
	vida de los usuarios como lo son: identificador del rol, descripción del rol, tipo de permisos, justificación, segregación (límite de la función), propietario del rol, fecha de última revisión, además, continua incompleta tal como lo informo la Oficina de Control Interno en la auditoria de 2024, debido a que, no contiene información de los sistemas informáticos “Tramitemos”, “Sistema de Seguridad de la Información” y “SIGEP Nomina”. 2) La Matriz de Roles y Perfiles (la herramienta clave para validar el mínimo privilegio) al momento de realizar la prueba del 20 de noviembre de 2025, no estaba disponible para su verificación según lo informo la Oficina de Tecnologías de la Información y las Comunicaciones OTIC, donde, el Oficial de Seguridad de la Información OSI y la Oficina de Control Interno OCI coincidieron en que la matriz vigente no cumple con los requisitos mínimos de calidad de la información. Esto implica que la herramienta de control es deficiente y potencialmente ineficaz. 3) Con relación a la Segregación de funciones, se observó la existencia de conflictos en el sistema de información misional SIM Busquemos y la debilidad de la Matriz de Roles para prevenirlos, demuestran que este control es ineficaz y permite la acumulación de privilegios peligrosos, cuentas privilegiadas que tengan conflictos con otros roles, como por ejemplo la de un usuario verificado que tiene rol de administrador y de rol de usuario final con funciones rutinarias como las de aprobaciones en el SIM Busquemos.	2) Controles ISO/IEC 27001:2022: A5.3 (Segregación de funciones), A5.2 (Roles y responsabilidades de seguridad de la información), A8.3. (Restricción de acceso a la información). 3) Clausula ISO/IEC 27001:2022: 9.1 Cláusula 9.1 (Monitoreo, medición, análisis y evaluación).	1) El Oficial de Seguridad de la Información OSI debe coordinar con la Oficina de Tecnologías de la Información y las Comunicaciones OTIC y con los administradores de los sistemas de información de la Unidad, con el fin de elaborar un “Catálogo de Conflictos” de Segregación de Conflictos, por ejemplo: "Función A + Función B = Conflicto" para cada sistema informático 2) Redefinir la estructura de la Matriz de Roles y Perfiles para incluir los criterios mínimos de calidad de la información de este instrumento y pilar. 3) Implementación del Proceso de Certificación de Privilegios: Establecer un proceso de revisión de accesos periódicos, donde, los Líderes de Proceso o Propietarios de Activos deban certificar formalmente los privilegios de sus equipos en la Matriz. Esto garantiza que el exceso de privilegios se elimine activamente. 4) Monitoreo Detective de Registros de Acceso: Documentar y formalizar las reglas de correlación (*casos de uso*) para

No.	Descripción(es) del Hallazgo	Criterio(s)	Recomendación(es)
	4) Los controles “5.2 Roles y responsabilidades de seguridad de la información” y “5.3 de Segregación de funciones” se encuentran definidos por la Unidad como de “Cumplimiento” en la “Declaración de Aplicabilidad” de la norma técnica ISO/IEC 27001:2022 y evaluados por la Unidad como “Aplicados” en la herramienta de autoevaluación que define el grado de madurez del Sistema de Seguridad de la Información SSI, en este sentido y bajo los escenarios de los anteriores numerales, se confirma que las evaluaciones realizadas a estos controles no son reales. El problema no es solo de consistencia, sino de diseño estructural (el sistema permite el conflicto, y el control de roles no lo previene). 5) Observación No. 3: este resultado de la auditoria de 2024 hace parte del Plan de Mejoramiento suscrito desde el 13 de enero de 2025 por el entonces Oficial de Seguridad de la Información OSI, se encuentran unificados y codificados como Acción de Mejora “SSI/60” y con entregable “Matriz Actualizada” en el instrumento consolidado de planes de mejoramiento de la Oficina de Control Interno OCI, donde, al corte del último seguimiento (tercer trimestre de 2025), la acción se encontraba vencida y con 0 % de avance, debido a que, la “Matriz de Roles y Perfiles” entregada por la Oficina de Tecnologías de la Información OTIC en periodos anteriores no cumplió con requisitos mínimos técnicos de calidad, en lo que refiere a las carencias criticas		identificar "actividad sospechosa" (ej. múltiples intentos fallidos, acceso a carpetas críticas fuera de horario laboral, en periodos de desvinculación, licencias, incapacidades) y asegurar que estas alertas sean investigadas.

No.	Descripción(es) del Hallazgo	Criterio(s)	Recomendación(es)
	mencionadas anteriormente (datos del ciclo de vida de roles y perfiles, información completa de sistemas informáticos).		

3. Gestión de la Continuidad de las TIC y Recuperación ante Desastres DRP (Recomendación No. 3 de la Auditoria SSI 2024)

No.	Descripción(es) del Hallazgo	Criterio(s)	Recomendación(es)
H3	1) El documento base de recuperación que, se encontró publicado en el Sistema Integrado de Gestión SIG es el mismo observado en la auditoria de la vigencia 2024 que corresponde al Plan de Recuperación ante Desastres DRP "GTI-PL-002 V01 01/12/2021", por otro lado, el 25 de noviembre de 2025 la Oficina de Tecnologías de la Información y las Comunicaciones OTIC hizo entrega del Plan con fecha de noviembre de 2025, lo que corresponde a un borrador que evidencia un proceso de actualización del Plan de Recuperación de Desastres, por lo tanto, la línea base oficial sigue siendo obsoleta, tal como lo presento la Oficina de Control Interno en la reunión realizada el 20 de noviembre de 2025, el plan de 2021 presenta las estrategias de recuperación bajo un escenario tecnológico en la vigencia 2021, donde, al corte de la vigencia 2025 el escenario es diferente lo cual es un incumplimiento a la obligatoriedad operativa del control en cuanto a su mantenimiento y revisión periódica de la documentación que soporta el DRP. 2) Ambos planes (el publicado y el borrador de noviembre 2025) omiten una estrategia formal y documentada para la	1) ISO 27001:2022, Cláusula 7.5 (Información documentada) 2) ISO 27001:2022, Control 5.30 (Preparación de las TIC para la continuidad del negocio) 3) La Cláusula 6.1.2 (Evaluación de riesgos de seguridad de la información)	Como bien se identificó en el diagnóstico y en el marco del Plan de Acción del Sistema de Seguridad de la Información SSI, se recomienda complementar las acciones con lo siguiente: 1) Actualización Formal del Plan de Recuperación de Desastres DRP y de los Análisis de Impacto del Negocio BIA institucionales. 2) Integración de Controles de Seguridad y Limpieza de Indicadores de Compromiso IoC. 3) Refuerzo de la Defensa Web y de la Identidad.

No.	Descripción(es) del Hallazgo	Criterio(s)	Recomendación(es)
	continuidad y recuperación de los servicios críticos en la Nube, por ejemplo: Identidad Digital y Correo Institucional. A pesar de los esfuerzos técnicos por detectar malware (Indicadores de Compromiso IoC), los demás análisis de seguridad y respuestas a vulnerabilidades detectadas en la presente vigencia y que amenazan la integridad de la información no están formalmente integradas en el proceso de recuperación documentado. Adicionalmente, el documento borrador del DRP no hace mención del diseño del DRP bajo un modelo “Asistido Automático - Burbuja - SureBackup" que describe la estrategia de recuperación de desastres más avanzada y confiable implementada, la cual elimina la dependencia de procedimientos manuales y reduce drásticamente el riesgo de fallas.		

4. Gestión de la Confidencialidad y Acuerdos de No Divulgación (Recomendación No. 4 de la Auditoria SSI 2024)

No.	Descripción(es) del Hallazgo	Criterio(s)	Recomendación(es)
H4	1) Falta de implementación de las estrategias de monitoreo. El Oficial de Seguridad de la Información OSI y la Oficina de Control Interno OCI reconocieron que la calificación de madurez del control A.6.6 (Acuerdos de confidencialidad) en la herramienta de autoevaluación es irreal ("optimizado"), ya que no existe evidencia objetiva de la ejecución de las fases de Verificar y Actuar del ciclo PHVA para este control.	1) ISO/IEC 27001:2022, Cláusula 9.1 (Monitoreo, medición, análisis y evaluación): La organización no está utilizando la información de monitoreo y medición para	Como bien se identificó en el diagnóstico y en el marco del Plan de Acción del Sistema de Seguridad de la Información SSI, se recomienda complementar las acciones con lo siguiente:

No.	Descripción(es) del Hallazgo	Criterio(s)	Recomendación(es)
	No obstante, en la reunión del 19 de noviembre de 2025, el Oficial de Seguridad de la Información OCI presento un Plan de Acción, donde, se definieron actividades para el fortalecimiento del monitoreo y controles operacionales, incluyendo un cronograma de revisión de acuerdos de confidencialidad y un proceso de monitoreo periódico para la evaluación del personal con acceso, que al corte de la prueba de recorrido no se ha desarrollado.	determinar la eficacia del control A.6.6. 2) ISO/IEC 27001:2022, Control A.6.6 (Acuerdos de confidencialidad o no divulgación): El control es solo documental y no opera bajo un proceso continuo de gestión y monitoreo. 3) ISO/IEC 27001:2022, Cláusula 10.2 (Mejora continua): Ante la ausencia de mediciones, se presenta por consecuencia, debilidades en la capacidad de la Unidad para identificar y corregir deficiencias en el proceso de Acuerdos de Confidencialidad.	1) Desarrollar una Métrica de Eficacia: se recomienda Implementar un Indicador Clave de Rendimiento KPI objetivo para el control A.6.6, utilizando, por ejemplo, marcos de buenas prácticas como lo son las directrices de la norma técnica ISO/IEC 27004. 2) Fortalecer el Control de Terceros: El Oficial de Seguridad de la Información OSI y la secretaria general SG deben revisar conjuntamente la plantilla de contratos con personas jurídicas para asegurar la inclusión de cláusulas de confidencialidad claras, requisitos de notificación de incidentes y requisitos de seguridad alineados con las directrices de seguridad de la información en las relaciones con los proveedores.

5. Gestión del Riesgo Interno y Control de Acceso (Recomendaciones No. 5 y 6 de la Auditoria SSI 2024)

No.	Descripción(es) del Hallazgo	Criterio(s)	Recomendación(es)
H5	1) El cribado (análisis de seguridad pre-vinculación) se realiza solo para Servidores y se aplica de forma general para todas las vinculaciones y no existe un cribado especifico según el nivel de acceso a información confidencial y/o sensible, en cuanto a Contratistas no se	1) Manual de Seguridad de la Información: en la Política 8.8 y el literal f) se especifica que la inhabilitación de accesos debe ser inmediata, lo cual es el origen	Como bien se identificó en el diagnóstico y en el marco del Plan de Acción del Sistema de Seguridad de la Información SSI, se recomienda complementar las acciones con lo siguiente:

No.	Descripción(es) del Hallazgo	Criterio(s)	Recomendación(es)
	hace el cribado, lo que introduce un riesgo de ingreso de personal sin la debida verificación. 2) Aun se observan diferencias de tiempos entre la fecha final del vínculo y la inhabilitación expedita de accesos, lo anterior debido al tiempo que se da para la entrega de cargo, donde, se requiere acceso a información y a recursos tecnológicos, creando una "ventana de riesgo" para posibles fugas de información y en el peor de los casos sabotajes, ante un caso por ejemplo de insatisfacción por la desvinculación.	de la brecha operativa, la falta de un proceso de desvinculación y entrega controlado expone a la Unidad al riesgo de un "empleado insatisfecho" que pueda explotar su acceso no revocado. 2) ISO/IEC 27001:2022, Control A.6.5 (Responsabilidades después de la terminación o cambio de empleo) 3) ISO/IEC 27001:2022, Control A.6.1 (Cribado)	1) Reforzar o implementar actividades de desvinculación y entrega controlada. 2) Aplicación universal del cribado para servidores y contratistas, no solo en etapas de vinculación, sino también, en la contratación, desvinculación (personas que puedan representar una amenaza de seguridad de la información) y en cambios de roles. 3) Articulación entre el procedimiento de Vinculación y Retiro “GTH-PR-013” y el Manual de Seguridad de la Información, donde, en la actividad número 10 del procedimiento se da un plazo de 10 días hábiles iniciales (y 10 de prorroga si se requiere) para la entrega de la documentación asociada al retiro.

6. Protección Proactiva contra Malware (Recomendación No. 9 de la Auditoria SSI 2024)

No.	Descripción(es) del Hallazgo	Criterio(s)	Recomendación(es)
H6	Falla de Reporte y Medición de la Eficacia. La Oficina de Tecnologías de la Información y las Comunicaciones OTIC demostró la realización de actividades técnicas, relacionadas con el monitoreo del Firewall de Aplicaciones	1) Clausulas ISO/IEC 27001:2022: 1) 9.1 (Monitoreo, medición, análisis y evaluación)	Como bien se identificó en el diagnóstico y en el marco del Plan de Acción del Sistema de Seguridad de la Información SSI, se

No.	Descripción(es) del Hallazgo	Criterio(s)	Recomendación(es)
	Web WAF, análisis forense, ejercicios de reversing o simulación de ataques, análisis de gestores de contenidos, remediación de vulnerabilidades, la Oficina hizo entrega de 4 documentos de ejercicios realizados en segundo semestre de 2025, la OCI observó que el responsable de seguridad digital registro textualmente acciones realizadas y para realizar por otras instancias o responsables, sin embargo, no se evidencio la realización de estas acciones correctivas, ni de las pruebas de las correcciones. En este sentido, el esfuerzo técnico no se ha formalizado en la capa de gobernanza, tal como se indicó anteriormente, los outputs o salidas (resultados) del proceso técnico, no se encuentran documentados o formalizados para que sean inputs o entradas del proceso de gestión y cerrar la brecha de reporte en la fase “Verificar” y se tomen acciones correctivas o de mejora en la fase “Actuar” del ciclo Planificar, Hacer, Verificar, Actuar PHVA, siendo, soportes de la madurez del Sistema de Seguridad de la Información SSI de la Unidad	2) Cláusula 7.5 (Información documentada) 3) Controles ISO/IEC 27001:2022: A.8.7 (Protección contra malware).	recomienda complementar las acciones con lo siguiente: 1) Transformación del Dato Técnico en Dato de Gestión (según la norma ISO 27004): se recomienda al Oficial de Seguridad de la Información OSI y a la Oficina de Tecnologías de la Información y las Comunicaciones OTIC definir un "Formato de Reporte Trimestral de Ciberseguridad" estandarizado. Este reporte debe extraer los resultados clave del Firewall de Aplicaciones Web WAF/Sin Operación NOP (por ejemplo: Número de ataques bloqueados, Número de scripts maliciosos detenidos) y los hallazgos forenses (decisiones tomadas) para medir la eficacia del control A.8.7 Protección contra el malware. 2) Integrar el Reporte a la Evaluación de Riesgos (según la norma ISO 27005): El reporte trimestral debe ser utilizado como evidencia para la revaluación de la Probabilidad del "Riesgo de Infección por Malware" en la Matriz de Riesgos. Para esto se recomienda hacer uso del marco de buenas prácticas de las directrices de ISO/IEC 27005:2022 para retroalimentar la evaluación de riesgos.

No.	Descripción(es) del Hallazgo	Criterio(s)	Recomendación(es)
			3) Formalización del Proceso de Auditoría de Herramientas: En conjunto entre el Oficial de Seguridad de la Información OSI y la Oficina de Tecnologías de la Información y las Comunicaciones OTIC, se recomienda establecer un protocolo formal para la auditoría periódica de las herramientas de seguridad (Firewall de Aplicaciones Web WAF, Sin Operación NOP, Antivirus), asegurando que se revise la configuración, las políticas de detención y los logs para verificar el cumplimiento del Control A.8.7 Protección contra el malware. 4) Estandarizar el proceso de análisis, reporte, acciones y pruebas.

7. Protección de Sistemas durante Auditoría (Recomendación No. 10 de la Auditoria SSI 2024)

No.	Descripción(es) del Hallazgo	Criterio(s)	Recomendación(es)
H7	Hay falla de documentación, debido a que la Oficina de Tecnologías de la Información y las Comunicaciones OTIC aplica prácticas avanzadas para proteger los sistemas durante las pruebas, tales como el uso de ambientes virtualizados, aislados y monitoreados , así como el refuerzo con el Firewall de Aplicaciones Web WAF y el Multifactor de Autenticación MFA, sin embargo, la Oficina de Control	1) Control ISO/IEC 27001:2022: A.8.34 (Protección de los sistemas de información durante las pruebas de auditoría)	Como bien se identificó en el diagnóstico y en el marco del Plan de Acción del Sistema de Seguridad de la Información SSI, se recomienda complementar las acciones con lo siguiente:

No.	Descripción(es) del Hallazgo	Criterio(s)	Recomendación(es)
	Interno OCI en la reunión del 20 de noviembre de 2025 enfatizó que, esta práctica técnica, aunque eficaz, no ha sido formalmente documentada ni estandarizada en un documento formal. Esto implica que la protección se basa en el conocimiento individual del personal técnico (riesgo humano) y no en un activo formal de la organización.	2) Clausula ISO/IEC 27001:2022: 7.5 (Información documentada)	1) Estandarización Documental: El Oficial de Seguridad de la Información OSI y la Oficina de Tecnologías de la Información y las Comunicaciones OTIC, deben coordinar esfuerzos con el fin de documentar y formalizar la seguridad en los ambientes tecnológicos. Se recomienda que, el documento detalle los requisitos mínimos para establecer un ambiente de auditoría, por ejemplo: virtualización obligatoria, monitoreo de acceso, proceso de borrado posprueba, control sobre el entorno, el uso de doble factor de autenticación en los accesos en pruebas de auditoría. 2) Actualizar el Manual de Seguridad de la Información: incluir la Política, lineamiento y literales al respecto.

8. Medición del Cumplimiento, Madurez y Eficacia del Sistema de Seguridad de la Información SSI (Recomendación No. 13 y 16 de la Auditoria SSI 2024)

No.	Descripción(es) del Hallazgo	Criterio(s)	Recomendación(es)
H8	1) Se observó que las calificaciones de madurez en el Instrumento de Autodiagnóstico presentado en la auditoria 2024 el cual mostraba que "*el 81,72 % (76) de los controles se encuentran bien calificados*	1) Cláusulas ISO/IEC 27001:2022: 9.1 (Monitoreo, medición, análisis y evaluación), 9.3 (Revisión por la dirección).	Como bien se identificó en el diagnóstico y en el marco del Plan de Acción del Sistema de Seguridad de la Información SSI, se

No.	Descripción(es) del Hallazgo	Criterio(s)	Recomendación(es)
	(Aplicados y En Optimización) y el 18,27 % (17) se encuentran calificados (Documentado y Definido)", no contaron en la vigencia 2025 con una medición periódica que permitiera sustentar los estados de cada uno de los controles reportados en la vigencia 2024, en este sentido no se cumple con la Clausula 9.1 el cual establece que cada control debe cumplir con el ciclo Planificar, Hacer, Verificar y Actuar PHVA. En consecuencia, los 17 controles verificados en la auditoria de la vigencia 2024 que se definieron como recomendaciones, se materializo la falta de Monitoreo, medición, análisis y evaluación, por este motivo se declaran como hallazgos en la presente auditoria de seguimiento, asimismo, los controles presentados en las 3 observaciones continúan bajo el mismo escenario informado en la pasada vigencia.		recomienda complementar las acciones con lo siguiente: 1) Adopción de ISO/IEC 27004 para la Estructura de Métricas: El Oficial de Seguridad de la Información OSI, utilizar la guía ISO/IEC 27004 para redefinir los Indicadores Clave de Rendimiento KPI, asegurando que cada métrica se alinee a un control específico y mida su eficacia (el resultado o impacto), no solo su existencia. (Fortalecer la Clausula 9.1). 2) Reevaluar el estado de madurez de cada uno de los 93 controles, asegurándose que cada uno cumpla con las fases del ciclo Planificar, Hacer, Verificar y Actuar PHVA, lo anterior, con el fin de establecer una línea base real del estado general del Sistema de Seguridad de la Información SSI, para así, tomar acciones de mejora y apuntar a la optimización del sistema. 3) Los Indicadores Clave de Desempeño KPI de cumplimiento deben vincularse directamente con los riesgos identificados en la Matriz de Riesgos. Por ejemplo, la métrica de "Falla de Inhabilitación de Acceso" (Recomendación 5) debe ser un

No.	Descripción(es) del Hallazgo	Criterio(s)	Recomendación(es)
			input directo para recalcular la Probabilidad del "Riesgo de Fuga de Información por Empleado Saliente", asegurando que la medición retroalimente la evaluación de riesgos.

9. Publicación del Plan Estratégico de Seguridad de la Información PESI (Recomendación No. 14 de la Auditoria SSI 2024)

No.	Descripción(es) del Hallazgo	Criterio(s)	Recomendación(es)
H9	Se evidencio que el Plan Estratégico de Seguridad de la Información PESI 2022 - 2024 no fue aprobado ni publicado en el repositorio del Modelo de Operación por Procesos MOP ni en la página Web de la Unidad, adicionalmente, a la fecha no se cuenta con Plan Estratégico de Seguridad de la Información PESI 2025 aprobado por la Alta Dirección, de acuerdo a lo informado por la Oficina de Tecnologías de la Información y las Comunicaciones OTIC este se encuentra en construcción y que una vez se tenga la versión final aprobada será publicado.	1) Controles ISO/IEC 27001:2022: Control A.5.36 (Cumplimiento de políticas, normas y estándares de seguridad de la información), Control A.5.1 (Políticas de seguridad de la información). 2) Clausula ISO/IEC 27001:2022: 7.5 (Información documentada).	Como bien se identificó en el diagnóstico y en el marco del Plan de Acción del Sistema de Seguridad de la Información SSI, se recomienda complementar las acciones con lo siguiente: 1) Finalizar y Publicar el Plan Estratégico de Seguridad de la Información PESI: Trabajo coordinado entre el Oficial de Seguridad de la Información OSI y la Oficina de Tecnologías de la Información y las Comunicaciones OTIC, con el fin de materializar la oficialización y la publicación de las versiones del plan en los sitios requeridos. 3) Publicar en el menú de Transparencia de la página web de la Unidad, una versión ejecutiva. 2) Documentar y justificar la decisión del contenido a publicar externamente.

10. Cumplimiento de la Política de Escritorio Limpio (Recomendación No. 17 de la Auditoria SSI 2024)

No.	Descripción(es) del Hallazgo	Criterio(s)	Recomendación(es)
H10	1) La Oficina de Control Interno informó que, a pesar de la Política 8.7 (Manejo de Equipos de cómputo) que prohíbe guardar archivos en el escritorio, se siguen encontrando documentos expuestos en los escritorios de equipos de cómputo, incluso por parte de personal directivo con conocimiento de la política.	1) Política Interna (GTI-MN-002 Política 8.7 Manejo de Equipos de cómputo). 2) Control ISO/IEC 27001:2022: A.7.7 (Escritorio y pantalla limpios). 3) Clausula ISO/IEC 27001:2022: 5.1 (Políticas de seguridad de la información)	Como bien se identificó en el diagnóstico y en el marco del Plan de Acción del Sistema de Seguridad de la Información SSI, se recomienda complementar las acciones con lo siguiente: 1) Monitoreo Periódico: El Oficial de Seguridad de la Información OSI debe establecer un programa formal de "Recorridos de Escritorio y Pantalla Limpia" no anunciados (auditorías puntuales), asimismo, se recomienda documentar los resultados en un instrumento y reportarse como un Indicador Clave de Desempeño KPI de cumplimiento. 2) Refuerzo de la Cultura de Liderazgo: El Oficial de Seguridad de la Información OSI debe comunicar a la Dirección General formalmente que el cumplimiento de las políticas de seguridad (incluido el Escritorio Limpio) es un factor de evaluación de desempeño y de madurez del Sistema de Seguridad de la Información SSI, que depende de todos los actores (incluido el nivel directivo). El cumplimiento debe empezar por el liderazgo para que la concientización sea efectiva. 3) Implementación de Controles Técnicos Complementarios: La Oficina de Tecnologías de la Información y las Comunicaciones OTIC debe analizar la implementación de una política que impida guardar documentos en el escritorio del equipo de cómputo.

2.3. RECOMENDACIONES ESTRATÉGICAS

Como bien se identificó en el diagnóstico y en el marco del Plan de Acción del Sistema de Seguridad de la Información SSI, se recomienda complementar las acciones con lo siguiente:

- Implementación de un Marco de Gobernanza Orientado a la Eficacia, en este sentido, se recomienda el establecimiento de un Marco de Gobernanza que se enfoque en la Medición Objetiva de la Eficacia y la Integridad Operacional.

Por otro lado, a nivel de Madurez, Cumplimiento, Controles, Gestión del Riesgo y Sostenibilidad del Sistema de Seguridad de la Información SSI, se recomienda complementar con lo siguiente:

I. Mejora de la Madurez y Cumplimiento (Ciclo Planificar, Hacer, Verificar, Actuar PHVA)

- Acción Central: Establecer un nivel de madurez real apoyado en el ciclo de Planificar, Hacer, Verificar y Actuar PHVA, con el fin de que exista evidencia objetiva de cada fase e implementar la Ingeniería de Métricas de Eficacia, se recomienda utilizar marcos técnicos de buenas prácticas como la norma ISO/IEC 27004.
- Detalle: El Oficial de Seguridad de la Información OSI debe redefinir los Indicadores Claves de Desempeño KPI para que midan el resultado (ejemplo: reducción de incidentes) en lugar de la actividad (ejemplo: número de documentos revisados).
- Impacto: Esto convierte la Cláusula 9.1 (Monitoreo y Medición) de la norma ISO/IEC 27001:2022 en un proceso objetivo, proporcionando datos fiables a la Alta Dirección (Cláusula 9.3) y cerrando el riesgo de reportar un nivel de Madurez no real.

II. Fortalecimiento de Controles Críticos y Gestión del Riesgo

- Acción Central: Priorizar la corrección inmediata de los fallos operativos que impactan la Confidencialidad e Integridad (Riesgo Máximo).
- Detalle (Riesgo Interno/segregación de Funciones SoD): El Oficial de Seguridad de la Información OSI debe trabajar conjuntamente con los administradores de sistemas de información y demás recursos en el diseño e implementación de un

proyecto de Gobierno de Acceso (Recomendaciones 8 y 11), cerrando la brecha de la Matriz de Roles. La implementación debe incluir la Validación de Segregación de Funciones SoD y el Protocolo “T+0” (Inhabilitación Inmediata de Accesos), eliminando el riesgo de fuga por parte de personal desvinculado (Recomendación 6).

- Detalle (Riesgo de Continuidad): Integrar los hallazgos de Inteligencia de Amenazas IoC como escenarios obligatorios de prueba en el Plan de Recuperación de Desastres DRP. Este plan debe garantizar que la fase de recuperación incluya la limpieza proactiva de amenazas persistentes (Integridad) antes de volver a producción (Recomendación 9).

III. Sostenibilidad y Control Documental

- Acción Central: Asegurar el avance de la reimplementación de los 93 controles a la calidad de la documentación, como línea base del ciclo de Planificar, Hacer, Verificar y Actuar PHVA.
- Detalle: El Oficial de Seguridad de la Información OSI debe asegurarse de imponer la aplicación estricta del Control de Información Documentada (Cláusula 7.5 de la norma técnica ISO/IEC 27001:2022). No se debe aceptar ni registrar ningún avance de control (Recomendaciones. 1, 7 y 12) si la política o la matriz de soporte no está formalmente actualizada, versionada y alineada a la capacidad técnica real de actores técnicos e implementadores como lo es la Oficina de Tecnologías de la Información y las Comunicaciones OTIC (por ejemplo: el uso de Gestión de Dispositivos Móviles MDM en equipos móviles).

3. APROBACIÓN Y FIRMAS

Nombre	Cargo	Firma
Duvy Johanna Socha Plazas	Jefe Oficina Control Interno	PLAZAS SOCHA DUVY JOHANNA
Carlos Andrés Rico Reina	Experto Técnico