UNIDAD DE SERVICIOS PENITENCIARIOS Y CARCELARIOS - USPEC

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

BOGOTÁ D.C., AGOSTO 2026

VERSIÓN 01

USPEC

1. OBJETIVO:

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.

2. ALCANCE:

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.

3. RESULTADOS

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%.

Resumen de los Hallazgos 27001 y MSPI

Criticidad	Resumen del hallazgo	Riesgo de exposición de la entidad
● Crítica	**1. Continuidad del negocio y resiliencia institucional – H10.** No se evidenció un BCP formalizado, probado y actualizado; tampoco BIA, RTO/RPO, estrategias de continuidad, operación en contingencia ni pruebas periódicas. Adicionalmente, las conclusiones señalan inexistencia de un DRP formalizado y probado.	**Interrupción prolongada de funciones y servicios institucionales.** Ante ransomware, indisponibilidad del centro de cómputo, desastre o falla de un proveedor crítico, la USPEC podría no tener previamente definido **qué recuperar primero, en cuánto tiempo, con qué información, recursos, responsables y mecanismos alternos de operación**, exponiendo directamente el cumplimiento de su misión.
● Crítica	**2. Capacidad de recuperación de información no demostrada – H9.**	

	Aunque existen rutinas automatizadas de backup, no se evidenció un programa periódico de restauración y verificación de integridad que demuestre que los respaldos son recuperables.	**Pérdida irreversible o recuperación tardía de información.** Ante ransomware, corrupción de datos o falla tecnológica, la entidad podría descubrir durante la emergencia que un respaldo es incompleto, inconsistente o inutilizable. Esto agrava directamente el riesgo de continuidad, pero constituye una barrera de control diferente al BCP/BIA.
● Crítica	**3. Control de identidades, accesos y privilegios – H3, H6, H8 y H11.** Se evidenciaron debilidades en depuración de cuentas, ausencia de matrices formales de roles/perfiles, conservación de privilegios ante movilidad interna y utilización de credenciales compartidas.	**Acceso, modificación, extracción o eliminación de información por usuarios que no deberían conservar determinados privilegios, con debilitamiento de la segregación de funciones y de la capacidad para atribuir responsabilidades.** Una credencial residual, excesiva o compartida también puede facilitar persistencia de un atacante dentro de la infraestructura.
● Crítica	**4. Administración privilegiada por terceros – H5.** Se detectó acceso de un proveedor externo al Controlador de Dominio utilizando privilegios de Administrador, sin solicitud formal aprobada, supervisión técnica ni mecanismo suficiente de registro de sesión.	**Compromiso transversal de la infraestructura tecnológica.** Un acceso administrativo no suficientemente gobernado sobre el Directorio Activo puede permitir alterar configuraciones, cuentas, privilegios y políticas de seguridad, convirtiéndose potencialmente en un punto de propagación de ataques o afectación masiva de servicios.
● Alta	**5. Exposición a malware, ransomware y exfiltración – H17 + conclusión sobre vulnerabilidades.** Se evidenció navegación hacia categorías de alto riesgo y ausencia de políticas homogéneas de filtrado; adicionalmente, el informe concluye que no se realizan periódicamente	**Incremento de la superficie de ataque.** La combinación facilita phishing, descarga de malware, ransomware, explotación de vulnerabilidades no identificadas y salida de información mediante correo o almacenamiento externo no autorizado.

	escaneos de vulnerabilidades ni pentesting.	
Alta	**6. Riesgo de terceros y cadena de suministro – H7.** Aunque existe seguimiento contractual, no se evidenció un proceso periódico suficiente para evaluar controles de seguridad, riesgos, incidentes y cumplimiento de proveedores críticos.	**Materialización de incidentes originados en terceros sin detección o tratamiento oportuno.** La entidad puede quedar expuesta a vulnerabilidades del proveedor y, adicionalmente, tener dificultades para demostrar que supervisó efectivamente las obligaciones de seguridad durante la ejecución contractual.
Alta	**7. Gobierno y sostenibilidad del SGSI – H4 y conclusiones.** Documentos estratégicos y operativos se encuentran desactualizados o sin suficiente formalización; la auditoría concluye además que el SGSI no alcanza el nivel de gobernanza requerido.	**Riesgo de un SGSI formal pero no plenamente efectivo.** Políticas desactualizadas pueden no responder a la arquitectura, amenazas y operación actuales; además, la falta de liderazgo y revisión directiva puede impedir que las brechas tecnológicas se conviertan oportunamente en decisiones, recursos y acciones institucionales.
Alta	**8. Seguridad física de información e infraestructura crítica – H1, H2 y H12.** Se evidenciaron debilidades en puertas de emergencia, depósito de planos históricos y formalización del acceso a áreas críticas como Data Center y cuartos tecnológicos.	**Acceso físico no autorizado, sabotaje, hurto o consulta de información sensible.** La debilidad física puede permitir eludir controles tecnológicos mediante acceso directo a infraestructura, documentación o dispositivos críticos.
Media-Alta	**9. Control físico y trazabilidad de activos – H13, H15 y H16.** Existen debilidades en salida/ingreso de activos tecnológicos, administración de biometría y condiciones de almacenamiento y protección de equipos.	**Pérdida o sustracción de activos e información, ingreso de dispositivos no autorizados, permanencia de accesos físicos indebidos y afectación de equipos críticos por condiciones físicas inadecuadas.** También disminuye la capacidad institucional para reconstruir responsabilidades ante un incidente.
Media-Alta	**10. Gestión y respuesta a incidentes – H19 y conclusión de auditoría.** La Mesa de Ayuda presenta debilidades de trazabilidad,	**Incidentes que pueden permanecer abiertos o ser gestionados sin suficiente trazabilidad, aumentando el tiempo de**

	autorización, clasificación y cierre; adicionalmente, la auditoría concluye que existen debilidades en el proceso formal de identificación, reporte y atención de incidentes.	**exposición.** También dificulta reconstruir qué ocurrió, quién autorizó actuaciones, qué acciones se ejecutaron y qué lecciones deben incorporarse para evitar recurrencia.
Media	**11. Autenticación y coherencia de controles – H18.** La configuración técnica de contraseñas no coincide con lo definido en el procedimiento institucional.	**Debilitamiento de la autenticación y falsa percepción de control:** la Dirección puede considerar implementada una política que técnicamente opera bajo parámetros diferentes, aumentando la exposición de credenciales y afectando el cumplimiento del SGSI.
Media	**12. Protección de información física – H14.** No se evidenció procedimiento formal para destrucción segura de documentos clasificados, reservados o con datos personales.	**Divulgación no autorizada de información sensible por disposición física inadecuada**, aun cuando la versión digital se encuentre protegida mediante controles tecnológicos.

Análisis de los mapas de riesgos y los controles: Se recomienda al 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.

4. CONCLUSIONES GENERALES

- ✓ 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.

- ✓ 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.

- ✓ 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.

- ✓ 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.

- ✓ 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.

- ✓ 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.

- ✓ 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.

- ✓ 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.

Elaboró	Revisó:	Aprobó:
Nombre: Walter Raúl Niño Pérez Walter Raúl Niño Pérez	Nombre: German Heberto Gaitán Rengifo	Nombre: German Heberto Gaitán Rengifo
Cargo: Contratista	Cargo: Jefe Oficina Control Interno	Cargo: Jefe Oficina Control Interno
Dependencia: Oficina Control Interno	Dependencia: Oficina Control Interno	Dependencia: Oficina Control Interno