UNIDAD DE SERVICIOS PENITENCIARIOS Y CARCELARIOS - USPEC

INFORME DE SEGUIMIENTO MAPA DE RIESGOS INSTITUCIONAL (MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN-MSPI)

BOGOTÁ D.C., FEBRERO DE 2026

USPEC

TABLA DE CONTENIDO

OFICINA DE CONTROL INTERNO

1 OBJETIVO

Verificar y evaluar la efectividad de los controles implementados en el Modelo de Seguridad y Privacidad de la Información (MSPI) durante la vigencia 2025, en cumplimiento de lo establecido en el Decreto 1078 de 2015 y la Resolución 500 de 2021 de MinTIC, mediante el seguimiento sistemático a los riesgos institucionales y el análisis de su tratamiento, con el fin de determinar el nivel de mitigación alcanzado y proponer acciones de mejora continua que fortalezcan la resiliencia tecnológica de la USPEC para el ciclo 2026.

2 ALCANCE

El presente seguimiento evalúa de manera integral la gestión del Modelo de Seguridad y Privacidad de la Información (MSPI) durante la vigencia 2025. La evaluación se centra al entorno lógico y físico de la Sede Administrativa de la USPEC, analizando la efectividad de los controles y activos gestionados por la OTEC bajo las directrices del Ministerio TIC. El análisis se estructura en las siguientes etapas metodológicas:

- Fase 1: Planificación: Verificación del contexto organizacional, liderazgo, inventario de activos y la valoración de riesgos institucionales.
- Fase 2: Operación: Evaluación de la ejecución del plan de tratamiento de riesgos y la implementación de controles operativos de seguridad.
- Fase 3: Evaluación de desempeño: Revisión de indicadores de gestión, monitoreo de eventos y resultados de auditorías o revisiones directivas.
- Fase 4: Mejoramiento continuo: Análisis de la gestión de incidentes, efectividad de acciones correctivas y el estado final de no conformidades al cierre del año.

Esta evaluación se realiza bajo los criterios técnicos del Documento Maestro de MinTIC, el Decreto 1078 de 2015 y la Resolución 500 de 2021, asegurando una revisión exhaustiva del ciclo de vida de la seguridad de la información en la entidad.

3 MARCO LEGAL

El presente informe de seguimiento se fundamenta en el marco normativo vigente que regula la seguridad de la información, la protección de datos personales y la gobernanza digital en el Estado colombiano, destacando los siguientes referentes:

- Constitución Política de Colombia (Art. 15): Garantiza el derecho fundamental al Habeas Data y la privacidad de la información.
- Ley 1581 de 2012: Dicta las disposiciones generales para la protección de datos personales.
- Ley 1712 de 2014: Regula la transparencia y el derecho de acceso a la información pública nacional.
- Decreto 1078 de 2015: Define los lineamientos de la Política de Gobierno Digital y la obligatoriedad del Modelo de Seguridad y Privacidad de la Información (MSPI).
- Resolución 500 de 2021 (MinTIC): Establece los estándares para la seguridad, privacidad y seguridad

digital en las entidades del Estado.

- Norma ISO/IEC 27001:2022: Referente técnico internacional que establece los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI), adoptado por el Documento Maestro de MinTIC como base para el diseño de controles.
- Directiva Presidencial 07 de 2022: Imparte instrucciones sobre la protección de la infraestructura crítica cibernética en entidades públicas.
- Resolución número 000008 del 09 de enero de 2025: Por la cual se actualizan los lineamientos del Sistema de Gestión de Seguridad de Información de la USPEC y la política de privacidad y seguridad de la información, el cual deroga la Resolución 000181 del 17 de abril de 2022.

4 METODOLOGÍA DE EVALUACIÓN

Para el desarrollo del presente seguimiento al Mapa de Riesgos Institucional del Modelo de Seguridad y Privacidad de la Información (MSPI) correspondiente a la vigencia 2025, la Oficina de Control Interno aplicó una metodología de evaluación basada en la verificación documental y técnica de evidencias. El proceso se estructuró en las siguientes etapas:

- Solicitud de Insumos y Evidencias: Se realizaron requerimientos formales de información a la Oficial de Seguridad de la Información de la Oficina de Tecnología - OTEC mediante comunicaciones electrónicas los días 10 y 13 de febrero de 2026. En dichas solicitudes, se instó a la entrega de soportes organizados bajo la estructura del Documento Maestro de MinTIC, abarcando las fases de Planificación, Operación, Evaluación de Desempeño y Mejoramiento Continuo.
- Alcance Técnico de la Información: Con el fin de robustecer el análisis, la solicitud incluyó evidencias específicas de operación técnica (logs, monitoreo perimetral), gestión del factor humano, ciclo de vida de activos (obsolescencia), seguridad de terceros, protocolos de continuidad (backups y pruebas de restauración) y configuraciones de acceso remoto (VPN/MFA) implementadas durante el año 2025.
- Análisis y Diagnóstico: La metodología consistió en el cotejo de los insumos cargados en el espacio de Drive asignado por la Oficina de Control Interno, frente a los controles establecidos en el Mapa de Riesgos. A partir de esta revisión, se determinó el nivel de cumplimiento, la gestión de acciones correctivas ante no conformidades y, finalmente, se emitió el diagnóstico sobre la efectividad real de los controles para la mitigación de los riesgos de seguridad y privacidad de la información en la entidad.

5 ANÁLISIS DE LA INFORMACIÓN Y SOPORTES ENTREGADOS

Tras la carga de los soportes solicitados, la Oficina de Control Interno procedió a la verificación de la información. A continuación, se presenta el análisis detallado de la documentación suministrada.

5.1 Fase 1: Planificación (Contexto, Alcance, Liderazgo, Activos y Riesgos)

En esta fase se verificó el cumplimiento de los numerales 7.1 al 7.4 del Documento Maestro del MSPI:

Contexto y Alcance: Se constató la existencia del documento “Plataforma-estrategica-v05 CONTEXTO”, el cual alinea la seguridad de la información con los objetivos institucionales 2023-2026. Mediante la Resolución 000008 de 2025, la entidad formalizó el alcance del MSPI y la Política de Seguridad y Privacidad

de la Información, definiendo claramente las responsabilidades de la Alta Dirección, la Oficina de Tecnología (OTEC) y el Oficial de Seguridad.

Gestión de Activos y Riesgos: Se evidenció un ejercicio transversal de identificación en dependencias como Gestión Contractual, Jurídica, Financiera, Talento Humano y Gestión Documental. En el proceso de Gestión de Tecnologías de la Información, se identificaron 33 activos críticos (valoración 8/9), con especial prioridad en el control de cambios y gestión de usuarios. Este inventario cumple con las leyes 1712 de 2014 y 1581 de 2012.

No obstante, se identifica como una debilidad que el inventario de activos se gestione actualmente mediante archivos de Excel. Esta metodología es altamente vulnerable al factor humano, ya que tanto errores involuntarios como acciones dolosas pueden comprometer la integridad de los datos. Al carecer de pistas de auditoría robustas, resulta imposible identificar responsables ante cualquier alteración o pérdida de información, un riesgo que suele pasar inadvertido en las revisiones superficiales.

Toma de Conciencia y Comunicación: La entidad ejecutó el "Plan de Sensibilización 2025", incluyendo piezas como los "5 Mandamientos de Ciberseguridad" y simulacros de phishing. No obstante, se detectó que solo 174 colaboradores (58%) formalizaron la aceptación de la política. La OTEC debe fortalecer el seguimiento, ya que el 42% de brecha en el factor humano eleva la vulnerabilidad ante ataques de ingeniería social.

5.2 Fase 2: Operación (Ejecución y Control Operacional)

Evaluación de los numerales 8.1 al 8.3 enfocada en la implementación técnica de los controles:

Control Operacional: Se constató que la OTEC asegura el cumplimiento de los requisitos de seguridad mediante la ejecución sistemática de los procesos definidos en la fase de planificación. Los soportes analizados, especialmente las matrices de seguimiento y los registros de la hoja de Control de Cambios del 4to Trimestre, evidencian que las modificaciones en la plataforma tecnológica (como actualizaciones de certificados y parches de seguridad) se realizan bajo criterios de control definidos. Asimismo, la vinculación operativa con el Contrato 290 de 2025 (Solución tecnológica para el fortalecimiento y modernización de la infraestructura tecnológica de la USPEC y administración de recursos y servicios de TI) demuestra una debida diligencia en la gestión de la seguridad de la información aplicada a los servicios tercerizados, garantizando la trazabilidad y el control operacional durante toda la vigencia.

Plan de Tratamiento de Riesgos (PTR): Se cotejó la ejecución del Plan de Tratamiento de Riesgos mediante los informes de seguimiento y las matrices técnicas de los cuatro trimestres de la vigencia 2025. De allí se destaca el cumplimiento de hitos como el despliegue del Múltiple Factor de Autenticación (MFA), la actualización de la Política de Correo (TI-PO-012) y el monitoreo mediante Solarwinds. Aunque el primer semestre tuvo rezagos, dado que de un 70% programado solo se ejecutó un 39%, el segundo semestre superó las proyecciones pasando de un 30% programado a ejecutar un 50%, para ejecutar un acumulado del 89% al final de la vigencia.

Realizando el análisis de la siguiente tabla, este revela una gestión de riesgos con contrastes críticos: mientras la disponibilidad operativa (R1 y R2) alcanza un cumplimiento del 100%, garantizando estabilidad ante fallas eléctricas o cambios de configuración, la seguridad lógica presenta brechas alarmantes. El riesgo R4 (Explotación de Vulnerabilidades) a pesar de que bajara de nivel Extremo a Medio, es el punto más vulnerable, debido a que la actualización del instructivo TI-IN-005 de gestión de vulnerabilidades se encuentra estancada en un 0%, lo que invalida la estructura normativa necesaria para proteger la confidencialidad e integridad de la plataforma tecnológica.

Tabla 1. Resumen Matriz de Riesgos TI a cierre Vigencia 2025.

No. RIESGO	RIESGO	DESCRIPCIÓN DE LA ACCIÓN	RESULTADO
R1	Posibilidad de pérdida de disponibilidad por interrupción de los servicios tecnológicos debido a fallas en el suministro eléctrico	Actualizar el plan de mantenimiento de la plataforma tecnológica incluyendo la descripción del control y la definición del cronograma de trabajo. (100%) Realizar seguimiento trimestral al cronograma establecido a través del plan de mantenimiento de la plataforma tecnológica. (100%)	100%
R2	Posibilidad de pérdida de disponibilidad por interrupción de los servicios tecnológicos debido a cambios no autorizados en la configuración de la plataforma tecnológica	Realizar seguimiento a los controles de cambios realizados durante el trimestre. (100%)	100%
R3	Posibilidad de pérdida de disponibilidad por interrupción de los servicios tecnológicos debido a la baja gestión de la capacidad o fallas relacionadas con el almacenamiento	Realizar seguimiento al estado del monitoreo y escalamiento de las alertas presentadas. (El informe debe contener el total de alertas generadas durante el mes y el total de alertas gestionadas). (100%) Gestionar las observaciones o hallazgos del informe de monitoreo de la infraestructura tecnológica, con el fin de identificar el almacenamiento disponible y proyectar necesidades futuras. (75%)	88%
R4	Posibilidad de pérdida de confidencialidad, integridad y disponibilidad por explotación de vulnerabilidades tecnológicas debido a la falta de un proceso eficiente de gestión de vulnerabilidades.	Actualizar el instructivo TI-IN-005 Gestión de Vulnerabilidades. (10%) Nota: Es necesario incluir dentro del plan de remediación de vulnerabilidades las demás detectadas fuera de la gestión de los procesos contractuales relacionados con ethical hacking y gestión de vulnerabilidades.	70%

		Actualizar el plan de remediación de vulnerabilidades de la plataforma tecnológica, incluyendo (Es necesario incluir las vulnerabilidades detectadas por los administradores de la plataforma tecnológica). (100%)	
		Realizar seguimiento al plan de remediación de vulnerabilidades. (100%)	
R5	Posibilidad de pérdida de confidencialidad, integridad y disponibilidad por fuga de información sensible debido a la falta de gestión de los documentos electrónicos	Documentar a través de la política de correo electrónico institucional los controles relacionados a la prevención de fuga de información. (100%)	90%
		Implementar las características detección de fuga de datos en la plataforma de correo. (80%)	
R6	Posibilidad de Pérdida de confidencialidad por acceso no autorizado a la información del buzón de correo compartido debido a fallas en los controles de acceso, perfiles de usuario y credenciales de acceso débiles o comprometidas	Documentar a través de la política de correo electrónico institucional los controles relacionados al fortalecimiento de la autenticación. (100%)	84%
		Implementar los controles relacionados al fortalecimiento de la autenticación. (100%)	
		Realizar seguimiento al estado de las cuentas de correo con la característica de MFA activa. (El informe debe contener el total de cuentas habilitadas con la característica de MFA). (100%)	
		Realizar el cambio de contraseñas de los buzones compartidos trimestralmente o en caso de requerirse. (35%)	
Promedio ejecución PTR			89%

Fuente: Propia Oficina de Control Interno.

A pesar de los avances significativos en la gestión de almacenamiento (R3 con 88%) y la prevención de fuga de datos (R5 con 90%), la seguridad de acceso en el riesgo R6 se ve seriamente comprometida, en razón a que el bajísimo cumplimiento en el cambio de contraseñas de buzones compartidos, que apenas llega al 35%, junto con la parálisis en R4, en cuanto a No actualizar el instructivo TI-IN-005 Gestión de Vulnerabilidades, que deja a la organización expuesta ante posibles intrusiones y compromete la trazabilidad de la información institucional.

Observación Crítica: El análisis cuantitativo inicial indicaba que el Riesgo R1 (Indisponibilidad por fallas eléctricas) persistía en nivel Extremo al cierre de la vigencia, a pesar de la ejecución del plan de mantenimiento preventivo. No obstante, la Oficina de Tecnología (OTEC) aclaró mediante correo electrónico

que dicha calificación se debió a una falla técnica en la formulación de la herramienta utilizada para el registro de la matriz de riesgos del año anterior, la cual no permitió reflejar el impacto real de los controles aplicados. Tras la validación en la matriz de la presente vigencia, se confirma que el riesgo residual ha sido mitigado efectivamente, ubicándose actualmente en zona de riesgo BAJO.

Indicadores: Se concluye una gestión efectiva con un 100% de cierre de incidentes en el último trimestre y un avance acumulado del PTR del 89%.

5.3 Fase 3: Evaluación de desempeño (Monitoreo y Auditoría)

En cumplimiento de los numerales 9.1 al 9.3, se analizaron los siguientes soportes:

Informes de Revisión: Se presentaron los informes de revisión del SGSI del primer y segundo semestre del 2025. Estos documentos consolidan la medición de objetivos, autodiagnósticos de controles bajo ISO 27001:2022 y el desempeño de los procesos.

Revisión por la Dirección: Los informes de revisión del SGSI se presentaron ante el comité directivo los días 8 de julio de 2025 y 30 de enero de 2026. Estos documentos, correspondientes al primer y segundo semestre respectivamente, constituyen el soporte formal con el cual la Alta Dirección evaluó el estado del sistema, el análisis de incidentes y las oportunidades de mejora, sirviendo como base para la planeación estratégica de 2026.

5.4 Fase 4: Mejoramiento continuo

Evaluación del cierre de brechas y cumplimiento de los numerales 10.1 y 10.2:

Hallazgos de Auditoría: Al analizar el Plan de Mejoramiento Institucional a corte de Octubre 2025, se advierte una debilidad significativa en el cierre de hallazgos de alta criticidad técnica. Específicamente, las acciones orientadas al Control A.12.3.1 (Respaldo de información), que incluyen la actualización de la política de copias de seguridad, la ejecución de pruebas de integridad/restauración y la gestión de logs de respaldo, presentan un avance del 0% ('Acción sin avance'). Debido a que las actualizaciones del instructivo TI-GU-003 Borrado Seguro de Información y de la Política de Generación y Restauración de Copias de Respaldo TI-PO-01 tenían fecha de ejecución en el plan de mejora para el 25 de diciembre de 2025.

Brechas Técnicas: No se evidencia la actualización de la política de copias de seguridad ni la ejecución de pruebas de integridad y restauración. Asimismo, existen retrasos en los lineamientos para el borrado seguro de datos.

Requerimiento Especial: Dado que documentalmente estas acciones figuran como "sin avance" a octubre de 2025, es indispensable que la OTEC aporte evidencias técnicas de ejecución (especialmente las actas de pruebas de restauración) realizadas entre octubre y diciembre. Sin estos soportes, la disponibilidad y confidencialidad de la información institucional se encuentran bajo un riesgo latente no mitigado al cierre de la vigencia.

6 CONCLUSIONES

- La gestión de activos en Excel representa una debilidad crítica debido a su vulnerabilidad al error humano y la falta de trazabilidad. Al carecer de registros de auditoría, cualquier daño o alteración, ya sea por culpa o dolo, impide identificar responsables y compromete la integridad de la información.

- Se destaca el monitoreo proactivo a través de herramientas como HELPTIC y GLPI, logrando la contención y cierre de eventos de seguridad registrados.

- La auditoría interna de 2025 evaluó procesos clave como Talento Humano, Infraestructura y Tecnología, identificando la necesidad de actualizar lineamientos de borrado seguro (NIST SP 800-88) y fortalecer la gestión de respaldos.

- Se ejecutaron simulacros de ataques (Phishing) y planes de sensibilización dirigidos a diferentes niveles de la organización para fortalecer la resiliencia ante amenazas digitales.

- De acuerdo con el reciente Informe de Auditoría Externa 2025 (EI-FO-004_V4) realizado por la firma Five Strategy SAS, la Entidad presenta los siguientes indicadores:

  Nivel de Madurez: La USPEC alcanzó un destacable 93% de implementación del MSPI. Sin embargo, la efectividad de los controles técnicos frente a la norma ISO 27001 se sitúa en un 67% (Nivel Gestionado).

  Riesgos Críticos bajo monitoreo (No Conformidades): Se ha estructurado el Plan de Mejoramiento para dar tratamiento a 9 No Conformidades (NC) recientes y 6 en seguimiento. Los riesgos que requieren mayor atención son:

  - (NC 5) Continuidad del Negocio: Inexistencia de un Plan de Continuidad de Negocio (BCP) consolidado y falta de un Data Center alterno (con un avance de cierre de apenas el 10%).
  - (NC 6) Fuga de Información Física: Deficiencia en los controles de acceso a documentos de extrema criticidad y seguridad nacional (Planos de centros penitenciarios ERON).
  - (NC 9) Monitoreo de Red: Necesidad de implementar monitoreo avanzado y auditorías a cuentas con privilegios administrativos.

7 RECOMENDACIONES

- Se recomienda la implementación de un software especializado en la gestión de activos. Esta herramienta garantiza la segregación de funciones, limitando las modificaciones exclusivamente a usuarios con perfiles de administrador debidamente autorizados. Asimismo, el sistema facilitaría un control de cambios automatizado (log de auditoría) y asegurar la alta disponibilidad de los datos, permitiendo un registro, administración y mantenimiento de la información con total completitud y trazabilidad.

- Se sugiere establecer un control conjunto con el área de Gestión Documental para validar la alineación de los activos de información con las Tablas de Retención Documental (TRD). Este proceso consistiría en auditorías periódicas a los repositorios en la nube (Drive) de cada área, verificando que la totalidad de los activos estén debidamente tipificados y amparados bajo las TRD vigentes. Esta sinergia institucional garantizará la actualización constante y el cumplimiento normativo de la información almacenada y asegurar que todas las dependencias actualicen y mantengan vigente el Inventario de Activos (TI-FO-056) al menos cada 6 meses.

- Es imperativo actualizar la política de copias de respaldo (TI-PO-01) para incluir lineamientos claros sobre la gestión de logs y realizar pruebas periódicas de restauración que validen la integridad de los datos.

- Se recomienda estandarizar el cambio de contraseñas en buzones institucionales compartidos y actualizar la "Guía de Manejo de Contraseñas Seguras" (TI-GU-001) para mitigar el riesgo de acceso no autorizado.

- Reforzar el proceso de "Paz y Salvo" para asegurar la devolución oportuna de activos de información y la cancelación inmediata de accesos cuando el personal (funcionarios o contratistas) se retira de la entidad.

- Definir formalmente un responsable para la implementación de la Política de Protección de Datos Personales, asegurando el cumplimiento de la Ley 1581 de 2012.

- Viabilizar e impulsar el proyecto del Data Center Alterno, pilar fundamental del Plan de Continuidad de Negocio Institucional.

GERMAN HEBERTO GAITÁN RENGIFO
Jefe Oficina de Control Interno

Elaboró: José Mauricio Guerrero - Profesional Universitario OCI
Revisó: Alexi Mauredy Perdomo Bambague
Revisó: Luis Adolfo Romero Cardozo – Contratista OCI
Aprobó: German Heberto Gaitan Rengifo – Jefe OCI
Ruta: https://drive.google.com/drive/folders/1qOqLMniXE0gNhbbJMUxb4ilVAeGk-0li?usp=drive_link