UNIDAD DE SERVICIOS PENITENCIARIOS Y CARCELARIOS - USPEC

SEGUIMIENTO SEGUNDA LÍNEA DE DEFENSA - PLAN DE TRATAMIENTO DE RIESGOS

BOGOTÁ D.C., ENERO 2026

USPEC

INTRODUCCIÓN

El presente informe tiene como objetivo proporcionar una evaluación independiente y objetiva del estado actual del Plan de Tratamiento de Riesgos de Seguridad de la Información de la USPEC.

La Oficina de Tecnología, en colaboración con el Oficial de Seguridad (segunda línea de defensa), supervisa el Plan de Tratamiento de Riesgos de Seguridad. Este proceso de monitoreo busca verificar el avance en la implementación de controles y emitir recomendaciones que fortalezcan la mitigación de riesgos.

El actual plan de tratamiento de riesgos se enfoca en el proceso de Gestión de Tecnologías de la Información - GTI. La incorporación de los demás procesos se realizará progresivamente, una vez que cada área actualice sus activos de información según el nuevo Modelo de Seguridad y Privacidad de la Información del MINTIC (Resolución 2277 de 2025). Posteriormente, se analizarán los activos más críticos para establecer controles que mitiguen los riesgos en cada proceso.

Este seguimiento es esencial para cumplir con la Política de Privacidad y Seguridad de la Información, cuyo objetivo es gestionar los riesgos de los activos de información mediante la implementación de controles de seguridad adecuados. De esta manera, se asegura la mejora continua del Sistema de Gestión de Seguridad de la Información de la USPEC.

1. **Objetivo:** Realizar el seguimiento independiente al Plan de Tratamiento de Riesgos de Seguridad, verificando el cumplimiento de las actividades programadas y los controles definidos. Este proceso, como segunda línea de defensa, busca identificar desviaciones o debilidades en la gestión del riesgo y emitir recomendaciones técnicas para fortalecer el sistema de control interno y promover la mejora continua.

2. **Alcance:** Este informe comprende el seguimiento realizado por la segunda línea de defensa al Plan seguimiento al Plan de Tratamiento de Riesgos de seguridad a cargo del proceso Gestión de Tecnologías de la Información correspondiente al cuarto trimestre del 2025

3. **Metodología:** El seguimiento al Plan de Tratamiento de Riesgos de seguridad se desarrolla bajo la siguiente metodología:

    - **Revisión documental:** Análisis del plan de tratamiento vigente definido por cada proceso institucional, matriz de riesgos, cronogramas de actividades, valoración de controles, reporte de avance entregados por los procesos responsables y evidencias.
    - **Verificación de cumplimiento:** Contraste entre actividades programadas y ejecutadas, con base en evidencias (actas, informes, registros de implementación, informes, etc.).
    - **Evaluación de controles:** Valoración del estado de implementación de los controles definidos en el plan, considerando su pertinencia y trazabilidad.
    - **Identificación de desviaciones:** Detección de brechas, retrasos o inconsistencias en la ejecución del plan.
    - **Recomendaciones:** Formulación de propuestas técnicas orientadas a fortalecer la gestión del riesgo, mejorar la trazabilidad y asegurar la continuidad del tratamiento.
    - **Retroalimentación a procesos responsables:** Socialización de recomendaciones con los procesos responsables, promoviendo la mejora continua y la gestión oportuna en pro de la mitigación de los riesgos.

4. **Inventario y estado de riesgos:** A continuación, se presenta el inventario actualizado de los riesgos de seguridad incluidos en el Plan de Tratamiento vigente, junto con su estado de implementación:

Riesgo	Proceso responsable	Control definido	Estado de Plan de tratamiento	Recomendaciones
RS-001	Gestión de Tecnologías de la Información	Administrador de Infraestructura Gestiona el mantenimiento de los sistemas de respaldo eléctrico a través de la revisión trimestral de las actividades de mantenimiento ejecutadas por los proveedores correspondientes de la plataforma e infraestructura tecnológica, en el caso de no llevarse a cabo la actividad de mantenimiento programada se informa a través de correo al grupo administrativo o los administradores de la plataforma tecnológica.	Ejecutado	Se verificó la ejecución del plan de mantenimiento. Para actualizaciones posteriores del plan, se recomienda incluir todas las actividades de mantenimiento de la infraestructura tecnológica, gestionadas a través de los contratos vigentes a cargo de la OTEC, con el propósito de llevar a cabo la trazabilidad integral de todas las actividades propuestas y requeridas.
RS-002	Gestión de Tecnologías de la Información	El comité de cambios valida los cambios a realizar en la plataforma tecnológica y servicios de TI por parte de los proveedores o de los administradores de la infraestructura tecnológica, cada vez que se requiera, y registra los resultados obtenidos a través del formato RFC Control de Cambios - TI-FO-029, en caso de no documentarse el cambio se deberá solicitar la gestión al proveedor	Ejecutado	Se recomienda evaluar la pertinencia de la intervención del Comité de Gestión de Cambios dentro de la ejecución actual del control. En caso de determinar que no es determinante su participación, se deberá actualizar el procedimiento respectivo para asegurar la coherencia entre la información documentada y la práctica.
RS-003	Gestión de Tecnologías de la Información	El personal de la mesa de servicios reporta a los administradores de la infraestructura tecnológica, los eventos o alertas registrados en la herramienta de monitoreo cada vez que	En proceso	La sola acción de monitoreo no es suficiente para la mitigación del riesgo. Para la próxima actualización de riesgos de seguridad, se recomienda:

		se requiera, teniendo en cuenta los dashboard de la herramienta de monitoreo y registran a través de la plataforma de casos aquellas situaciones que requieren escalamiento, en caso que no se atienda esta solicitud el personal de la mesa deberá informar al Coordinador del Grupo de Telecomunicaciones		Actualizar los umbrales de capacidad de los diferentes activos y servicios de TI, con el fin de contar con valores de referencia que permitan evaluar la necesidad de tomar acciones frente a las alertas generadas en los informes de monitoreo, de esta manera se garantiza la disponibilidad y rendimiento de los diferentes activos que componen la infraestructura tecnológica. Definir criterios de categorización y priorización para las alertas generadas por la herramienta de monitoreo, definiendo tiempos de atención y respuesta. Así mismo, se sugiere formalizar un protocolo para la implementación de las recomendaciones técnicas que contienen los informes de monitoreo. No se evidenció en su totalidad el cumplimiento del control establecido.
RS-004	Gestión de Tecnologías de la Información	El Coordinador del Grupo de Telecomunicaciones verifica la ejecución de las actividades de mitigación de vulnerabilidades mediante la revisión trimestral del plan de remediación y registra los avances en las columnas de seguimiento del mismo plan, en caso no de ejecutarse el plan establecido se debe reportar al Jefe de la Oficina de Tecnología a través de correo electrónico.	En proceso	Teniendo en cuenta la adquisición de la herramienta de gestión de vulnerabilidades, conviene en la actualización de los riesgos de seguridad ajustar el control para continuar con la mitigación del riesgo y de acuerdo a la gestión que se realice a través de la misma, actualizar el instructivo TI-IN-005 Gestión de vulnerabilidades.

RS-005	Gestión de Tecnologías de la Información	La Plataforma de Google Workspace verifica las acciones de detección de fuga de datos (DLP) disponibles en el servicio de Google Workspace permanentemente. En caso que no se pueda ejecutar la actividad se debe solicitar apoyo técnico al proveedor de servicio de Google Workspace.	Ejecutado	Control y plan de tratamiento ejecutados en su totalidad.
RS-006	Gestión de Tecnologías de la Información	El administrador de la plataforma de correo verifica que el multifactor de autenticación (MFA) se encuentre activo para todos los usuarios de la entidad, y mensualmente genera el reporte de acuerdo a lo evidenciado en la herramienta de correo, en caso que no se encuentre activo se debe informar al líder de proceso del usuario con el fin de realizar el proceso de activación. Evidencia: Informes de google sobre cuentas con MFA.	En proceso	Teniendo en cuenta que el riesgo está enfocado en los buzones de correo compartido, conviene para la vigencia 2026 enfocar en este activo las actividades de tratamiento y el o los respectivos controles.

5. Análisis consolidado sobre el estado de implementación del PTR

La actualización realizada al mapa de riesgos de seguridad de información a inicios del 2025, solo se enmarca en el proceso Gestión de Tecnologías de la Información teniendo en cuenta el impacto que sus activos críticos generan en la plataforma tecnológica y por ende en la operación de la Entidad. Los demás procesos se encuentran pendientes por incorporarlos al mapa de riesgos y por ende al plan de tratamiento y dependen del proceso de actualización de activos de información a través del cual se valora su criticidad y posteriormente mediante el análisis de

riesgos se determinan sus amenazas, sus vulnerabilidades y sobre todo el impacto que estos elementos representan para la información institucional.

Es de aclarar que esta labor estaba programada para el primer trimestre del año, sin embargo fue necesario extender la gestión tomando como referencia que depende por un lado de la actualización de los activos de información, tarea que se requiere hacer en conjunto con cada proceso institucional y adicionalmente, en el mes de junio se actualizó el Modelo de Seguridad y Privacidad de Información (Resolución 2277 del 2025 - MINTIC) razón por la cual es necesario apropiar las actualizaciones antes de continuar con la labor en la USPEC. Cabe mencionar, que con corte al 31 de diciembre de 2025, se logró consolidar la actualización de los siguientes inventarios:

- Gestión documental
- Gestión de infraestructura
- Gestión de atención a establecimientos de reclusión
- Gestión de la Comunicación Institucional
- Gestión de Atención al Ciudadano
- Evaluación y control
- Gestión de tecnologías de la información.

Para la vigencia 2026, se proyecta avanzar con la actualización del plan de tratamiento de riesgos de acuerdo al trabajo realizado con cada uno de los procesos.

En cuanto a los riesgos del 2025, a cargo de la OTEC se contó con un porcentaje acumulado de ejecución del plan de tratamiento de riesgos de seguridad de información del 89%, distribuido de la siguiente forma:

- Primer trimestre: 22%
- Segundo trimestre: 17%
- Tercer trimestre: 21%
- Cuarto trimestre: 29%

6. **Conclusiones:**

- Con el fin de garantizar la correcta implementación de los controles y darles continuidad a través del tiempo es importante formalizarlos a

través de documentos oficiales (políticas, procedimientos, manuales, guías, instructivos).

- Para llevar a cabo la actualización de riesgos de seguridad de información para la vigencia 2026, se sugiere tener en cuenta las recomendaciones del presente informe.

- Con el propósito de avanzar en la mitigación de los riesgos, es fundamental cumplir con los plazos establecidos en los planes de tratamiento e implementar los controles conforme a lo definido por el proceso.

- Al definir un control, conviene precisar con exactitud el responsable idóneo de su implementación, ya que de esto dependerá la efectividad y el cumplimiento de dicho control

IMELDA MUÑOZ MANCIPE

JEFE OFICINA DE TECNOLOGÍA

Elaboró: Mayra Alexandra Agudelo Carvajal / Oficial de Seguridad de la Información
Revisó: Imelda Muñoz Mancipe / Jefe Oficina de Tecnología