UNIDAD DE SERVICIOS PENITENCIARIOS Y CARCELARIOS - USPEC

INFORME PLAN DE TRATAMIENTO DE RIESGOS

BOGOTÁ D.C., JULIO 2026

VERSIÓN 01

USPEC

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La seguridad digital se ha convertido en un pilar fundamental para el correcto funcionamiento de las entidades públicas. Los riesgos de seguridad digital, entendidos como el conjunto de amenazas y vulnerabilidades presentes en el entorno digital, pueden comprometer la confidencialidad, integridad y disponibilidad de los activos de información, obstaculizando el cumplimiento de los objetivos institucionales. Por ello, la identificación oportuna de estos riesgos y el establecimiento de controles para su mitigación son esenciales.

En este contexto, la USPEC ha adoptado la "Política de Administración de Riesgos", alineándose con los lineamientos establecidos por el Departamento Administrativo de la Función Pública (DAFP) en su "Guía para la administración del riesgo y el diseño de controles en entidades públicas". Esta guía define los requisitos para la gestión de riesgos de gestión, corrupción y seguridad digital, mediante la identificación, análisis, valoración, tratamiento y seguimiento de acciones que permitan mitigar dichos riesgos.

En cumplimiento con las buenas prácticas establecidas por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), y en concordancia con la Ley 1712 de 2014, este informe ejecutivo presenta el avance porcentual de la ejecución del plan de tratamiento de riesgos de seguridad de información por cada riesgo, sin detallar información clasificada o reservada sobre riesgos, amenazas o vulnerabilidades específicas.

El alcance del presente informe, corresponde a lo realizado en el II trimestre de 2026 y se limita a los riesgos de seguridad identificados en el proceso de Gestión de Tecnologías de la Información.

2. OBJETIVO

Presentar un informe detallado sobre el avance del plan de tratamiento de riesgos durante el segundo trimestre de 2026 y comparándolo con las metas definidas en la planeación.

3. SEGUIMIENTO PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Durante el segundo trimestre de 2026, se realizó el seguimiento de los seis (6) riesgos de seguridad definidos, abordando las siguientes actividades:

- ✓ Se realizó seguimiento al plan de mantenimiento 2026, mediante intervenciones preventivas y correctivas según aplique y gestionadas bajo el cronograma de seguimiento.

- ✓ Se realizaron controles de cambios como un mecanismo fundamental para garantizar la estabilidad, seguridad y eficiencia de los servicios de TI.

- ✓ Se realizó el monitoreo constante de la infraestructura tecnológica mediante la herramienta de monitoreo, lo que permitió generar informes mensuales sobre rendimiento, alertas recurrentes y capacidad de almacenamiento. Simultáneamente, se optimizó la Gestión de la Capacidad a través de la actualización del procedimiento

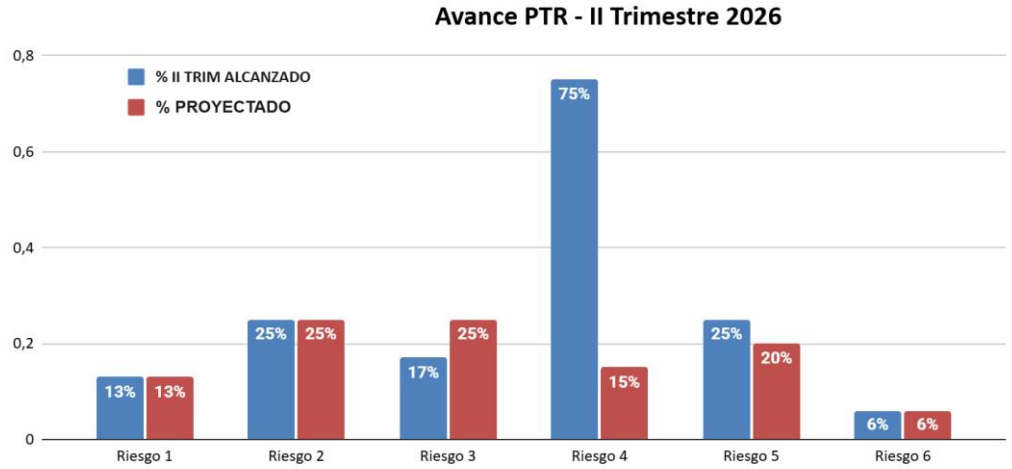
- ✓ El despliegue de la herramienta de evaluación y gestión de vulnerabilidades presenta un avance cercano al 100%, sin embargo, está pendiente iniciar la gestión y remediación de las vulnerabilidades identificadas a la fecha, para lo cual se están realizando sesiones de trabajo con el proveedor del servicio.

- ✓ Se cuenta con políticas de DLP (Prevención de Pérdida de Datos) activas desde la consola de administración de correo. Las pruebas unitarias para ampliar el alcance de protección se están avanzado con la implementación de la nueva herramienta.

- ✓ Se realizó el monitoreo constante del MFA de las cuentas de correo institucional.

Figura 1

Avance Riesgos de Seguridad



Nota: Captura Propia

Durante el segundo trimestre de 2026, el seguimiento del plan de tratamiento de riesgos alcanzó un avance del 17% frente al 27% proyectado. Los pendientes incluyen la actualización del instructivo de gestión de vulnerabilidades, la continuidad en la implementación de la herramienta DLP, y la formalización del procedimiento de Gestión de la Capacidad.

4. CONCLUSIÓN

- Durante el segundo trimestre, el Plan de Tratamiento de Riesgos de Seguridad de la Información alcanzó un 17% de ejecución, frente al 27% programado. Se proyecta el cumplimiento de las actividades pendientes para el cierre del tercer trimestre de 2026.

IMELDA MUÑOZ MANCIPE
JEFE OFICINA DE TECNOLOGÍA

Elaboró: Edwin Fabián Sánchez Amaya / Profesional Especializado OTEC
Revisó: Imelda Muñoz Mancipe / Jefe Oficina de Tecnología