UNIDAD DE SERVICIOS PENITENCIARIOS Y CARCELARIOS - USPEC

INFORME DE EJECUCIÓN DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE INFORMACIÓN - PTR

BOGOTÁ D.C., 30 DE DICIEMBRE 2024

CUARTO TRIMESTRE 2024

1. INTRODUCCIÓN

Un riesgo de seguridad digital se conoce como un conjunto de amenazas y vulnerabilidades derivadas del entorno digital y que pueden comprometer la confidencialidad, integridad y su disponibilidad de los activos de información, afectando el logro de los objetivos institucionales, por tanto es importante realizar una identificación oportuna de posibles riesgos, así como el establecimiento de controles que permitan su mitigación.

En tal sentido, la USPEC definió la "Política de Administración de Riesgos" incluyendo lineamientos establecidos por el DAFP a través de la "Guía para la administración del riesgo y el diseño de controles en entidades públicas". Esta guía definió los requisitos para la administración de riesgos de gestión, corrupción y seguridad digital a través de la identificación, análisis, valoración, tratamiento y seguimiento de aquellas acciones que permitirán mitigar los riesgos. Ahora bien, durante el primer trimestre se trabajó de manera integrada entre la Oficina de Tecnología y los diferentes procesos institucionales con el fin de actualizar las matrices de riesgos de seguridad digital, así mismo se definieron planes de tratamiento de riesgos con el fin de mitigar las vulnerabilidades detectadas.

De acuerdo a las buenas prácticas establecidas por el Ministerio de Tecnologías de la Información y las Comunicaciones en cuanto a la publicación de los informes del plan de tratamiento de riesgos de seguridad de información se recomienda "En el informe ejecutivo no deberá brindarse ningún tipo de detalle sobre los riesgos específicos, amenazas o vulnerabilidades analizados durante el proceso de gestión de riesgos, ya que esta información es clasificada o reservada de acuerdo con la ley 1712 de 2014, por esta razón solo se deben indicar cantidades"[1].

En tal sentido a través del presente informe se refleja el avance porcentual de la ejecución del plan de tratamiento de riesgos de seguridad de información por cada riesgo para el primer trimestre. Cabe mencionar, que con corte al 31 de marzo solo se encuentran definidos los riesgos de seguridad para el proceso Gestión de Tecnologías de la Información, dado que de acuerdo al informe de auditoría de seguridad realizada a finales del 2023 es necesario llevar a cabo un nuevo análisis con cada proceso, iniciando con la actualización de los inventarios de activos. Esta gestión se tiene proyectada para iniciar en el segundo trimestre del año.

2. SEGUIMIENTO AL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE INFORMACIÓN

A continuación se presenta el porcentaje de avance por cada trimestre de la vigencia para cada uno de los riesgos de seguridad a cargo del proceso Gestión de Tecnologías de la Información:

[1] https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Iniciativas/Buenas-practicas/

RIESGO	% I TRIM	% II TRIM	% III TRIM	% IVTRIM	ACUMULADO
R1.	0%	50%	25%	25%	100%
R2.	25%	25%	25%	25%	100%
R3.	20%	20%	30%	10%	80%
R4.	33%	27%	8%	8%	76%
Total	20%	30%	23%	17%	90%

En resumen dentro de las actividades ejecutadas se encuentran labores relacionadas con:

- ✔ Seguimiento al plan de mantenimiento de la plataforma tecnológica
- ✔ Trazabilidad de los cambios realizados a la infraestructura de TI
- ✔ Generación de informes de gestión de la capacidad de TI
- ✔ Actualización de documentos de operación de la plataforma tecnológica
- ✔ Seguimiento a la gestión de paz y salvos del personal de planta que se desvinculó de la entidad.

3. CONCLUSIONES

En conclusión durante el cuarto trimestre se avanzó en un 17% de las actividades programadas y un porcentaje total de avance para la vigencia del 90%.

El 10% restante estaba vinculado con la ejecución del plan de remediación de vulnerabilidades definido en el tercer trimestre, estas pueden haber sido solucionadas con actualizaciones de seguridad de la infraestructura tecnológica y/o la depuración de servicios, lo cual ha generado mejoras en el segundo semestre del año, en los activos con vulnerabilidades previamente identificadas.

Adicionalmente el proceso de ethical hacking que se encuentra pendiente por ejecutar como parte de la contratación de la firma Five Strategy, proporcionará una visión actualizada del estado de seguridad de la plataforma, lo que permitirá una remediación más precisa y efectiva. Por lo anterior las actividades de remediación de vulnerabilidades se ejecutarán en el 2025.

IMELDA MUÑOZ MANCIPE
JEFE OFICINA DE TECNOLOGÍA

Elaboró: Mayra Alexandra Agudelo Carvajal- Profesional Especializado

Revisó: Imelda Muñoz Mancipe- Jefe Oficina de Tecnología