Informe de

Plan de Tratamiento de Riesgos de Seguri

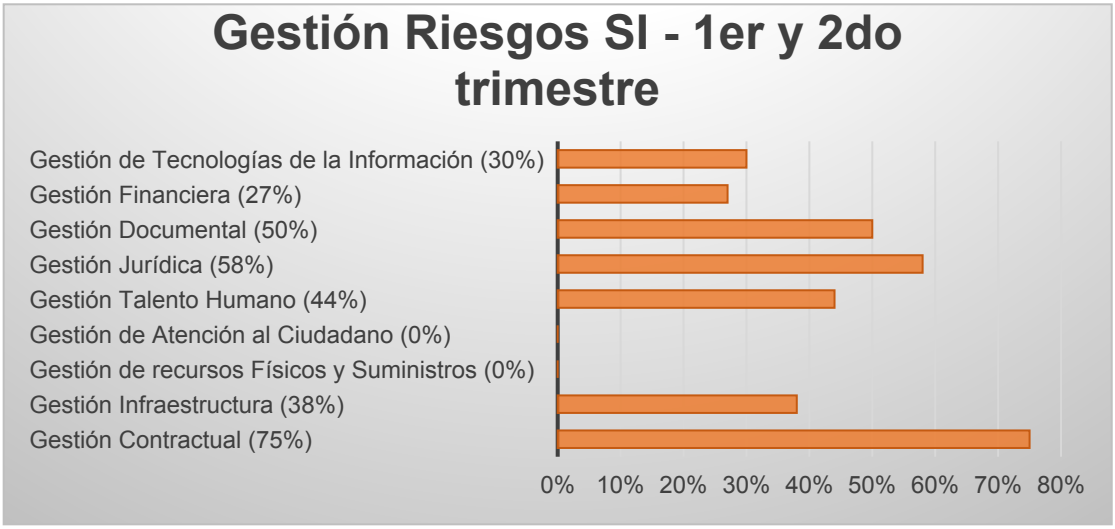
Un riesgo de seguridad digital se conoce como un conjunto de amenazas y vulnerabilidades derivadas del entorno digital y que pueden comprometer la confidencialidad, integridad y su disponibilidad de los activos de información, afectando el logro de los objetivos institucionales, por tanto es importante 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.

1. SEGUIMIENTO AL PLAN DE TRATAMIENTO DE RIESGOS POR PROCESO

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 continuación se presenta el avance porcentual de la ejecución del plan de tratamiento de riesgos de seguridad de información por cada uno de los procesos institucionales, con los valores acumulados para el primer y segundo trimestre del 2023:



De acuerdo a las actividades ejecutadas y reportadas por los procesos institucionales, durante el primer trimestre se avanzó en un 21% y un porcentaje total acumulado para la vigencia de 36% del plan de tratamiento de riesgos de seguridad de información.

PROCESO	PORCENTAJE DE AVANCE I TRIMESTRE	PORCENTAJE DE AVANCE II TRIMESTRE	ACUMULADO VIGENCIA 2023
Gestión de Contractual	63%	13%	76%
Gestión Infraestructura	13%	25%	38%

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

Gestión de recursos Físicos y Suministros	0%	0%	0%
Gestión de Atención al Ciudadano	0%	0%	0%
Gestión Talento Humano	13%	32%	44%
Gestión Jurídica	33%	25%	58%
Gestión Documental	0%	50%	50%
Gestión Financiera	0%	27%	27%
Gestión de Tecnologías de la Información	10%	20%	30%
TOTAL	**14,56%**	**21,28%**	**36%**

Nota: El detalle del avance y gestión de cada una de las actividades propuestas por los procesos institucionales se compartirá con las dependencias competentes para su revisión.

Aprobó: Imelda Muñoz Mancipe
Jefe Oficina de Tecnología

Elaboró: Mayra Alexandra Agudelo Carvajal
Profesional Especializado