ALCALDÍA MAYOR
DE BOGOTÁ D.C.
SECRETARÍA DE EDUCACIÓN

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

ATENEA
AGENCIA DISTRITAL PARA LA EDUCACIÓN SUPERIOR LA CIENCIA Y LA TECNOLOGÍA

Subgerencia de Tecnologías de la Información y las Comunicaciones

2023

Versión 1

Carrera 10 No. 28 – 49 torre A piso 26
PBX: (601) 6660006
www.agenciaatenea.gov.co
atencionalciudadanoatenea@educacionbogota.gov.co
Información: Línea 195

ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE EDUCACIÓN | ATENEA AGENCIA DISTRITAL PARA LA EDUCACIÓN SUPERIOR LA CIENCIA Y LA TECNOLOGÍA | BOGOTÁ

Contenido

INTRODUCCIÓN

La Agencia Distrital para la Educación Superior la Ciencia y la Tecnología - ATENEA en su responsabilidad de establecer condiciones de uso confiable en el entorno digital y físico de la información, define el plan de tratamiento de riesgos de Seguridad y Privacidad de la información el cual describe estrategias de carácter preventivo iniciando desde la comprensión del contexto hasta establecer los planes de acción que reduzcan la afectación de los activos de información en caso de materialización.

Lo anterior basado en las buenas prácticas de la Norma Técnica ISO 31000:2018, ISO 27001:2013, el concepto de Gobierno Digital y la alineación de la Política de Seguridad Digital como una de las dimensiones del Modelo Integrado de Planeación y Gestión – MIPG, así como las demás disposiciones en materia establecidas por el Estado Colombiano.

OBJETIVO

Definir y aplicar los lineamientos para la gestión de riesgos de seguridad de la información y seguridad digital que permita preservar la integridad, confidencialidad y disponibilidad de la información institucional.

ALCANCE

Este documento es aplicable para todas las oficinas, gerencias y subgerencias pertenecientes a la Entidad, por tal motivo en su ciclo de ejecución se involucran todos los procesos.

METODOLOGIA APLICABLE

A continuación, se describe la metodología definida para la gestión de riesgos de seguridad de la información, siguiendo las metodologías -Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP, en su versión 5 de diciembre del 2020 y -Guía de orientación para la gestión de riesgos de seguridad digital en el gobierno nacional, territoriales y sector público de MinTic.

Las fases metodológicas aprehendidas en el plan se encuentran articuladas con la Política de Administración de Riesgos de la Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología “Atenea” desde la incorporación estratégica en la definición de los riesgos de seguridad digital, hasta las etapas sobre la gestión de los riesgos institucionales.

El ciclo de gestión del riesgo consta de 4 pasos macro descritos a continuación:

Fase 1- Planificación

En esta fase se identifica el contexto -interno y -externo institucional, el ecosistema -activos de información, los criterios para la identificación, evaluación, análisis, valoración y control del riesgo de seguridad de la información.

Fase 2- Ejecución

Una vez desarrollada la fase anterior se procede con el cumplimiento de los criterios establecidos para todo el ciclo de la gestión del riesgo; inicia con la identificación de los activos de información y riesgos hasta el tratamiento para cada uno de los riesgos analizados y evaluados, conforme a los criterios y al apetito de riesgo definidos en la etapa de planificación.

Fase 3- Monitoreo y Revisión

En esta fase se evalúan periódicamente los riesgos residuales para determinar si los controles y planes establecidos han sido efectivos, contribuyendo así a la toma de decisiones en el proceso de revisión de riesgo por parte de las partes interesadas internas.

Fase 4 – Mejoramiento continuo de la gestión del riesgo de seguridad

Con el fin de garantizar la mejora continua en la gestión de riesgos de seguridad de la información/digital, la Agencia -ATENA establecerá la ruta correspondiente para mitigar el impacto y toma de acciones que permitan controlar los hallazgos, falencias e incidentes detectados

ESTRATEGIA DE IMPLEMENTACIÓN

A continuación, se relacionan las actividades a realizar en cada una de las fases metodológicas definidas, las cuales serán ejecutadas durante la vigencia 2023.

FASE	ACTIVIDADES	ENTREGABLE	RESPONSABLE	FINALIZACIÓN
Planificación	Articular el ciclo de gestión de riesgos de seguridad de la información con la Política de riesgos institucional.	Política de riesgos articulada con los riesgos de seguridad de la información.	Subgerencia TIC	31-Mar-2023
	Identificar múltiples partes interesadas	Contexto institucional – Partes interesadas del SGSI.	Subgerencia TIC	31-Mar-2023
	Identificar el alcance de los procesos institucionales donde sea aplicable la gestión de riesgos de	Manual de gestión de riesgos de seguridad de la información/digital .	Subgerencia TIC	31-Mar-2023

FASE	ACTIVIDADES	ENTREGABLE	RESPONSABLE	FINALIZACIÓN
	seguridad.			
	Definir roles y responsabilidades	Manual de gestión de riesgos de seguridad de la información/digital .	Subgerencia TIC	31-Mar-2023
	Establecer y documentar los criterios para la identificación, análisis y evaluación de los riesgos de seguridad de la información/digital	Manual de gestión de riesgos de seguridad de la información/digital .	Subgerencia TIC	31-Mar-2023
	Adoptar formato para reportar los riesgos de seguridad.	Formato riesgos de seguridad de la información.	Subgerencia TIC	31-Mar-2023
Ejecución	Identificar activos de información que tengan un valor alto para la Agencia - ATENEA	Matriz activos de información por proceso.	Subgerencia TIC	07-Jul-2023
	Identificar los riesgos inherentes de seguridad (amenazas, vulnerabilidades)	Matriz de riesgos.	Todos los procesos	05-May-2023
	Valorar los riesgos de seguridad identificados (probabilidad, impacto)	Matriz de riesgos.	Todos los procesos	05-May-2023
	Establecer y evaluar los controles	Matriz de riesgos.	Todos los procesos	05-May-2023
	Definir los planes de tratamiento para cada uno de los riesgos identificados.	Planes de tratamiento de riesgos de seguridad.	Todos los procesos	05-May-2023
Monitoreo y Revisión	Analizar los eventos e	Reporte de eventos e incidentes.	Subgerencia TIC	31-Mar-2023 30-Jun-2023

FASE	ACTIVIDADES	ENTREGABLE	RESPONSABLE	FINALIZACIÓN
	incidentes de seguridad reportados.			31-Oct-2023 31-Dic-2023
	Reportar la gestión del riesgo de seguridad de la información/digital	Reportes internos – Grupos de interés especial	Todos los procesos	31-Mar-2023 30-Jun-2023 31-Oct-2023 31-Dic-2023
Mejoramiento Continuo	Realizar seguimiento a los hallazgos reportados por la oficina correspondiente.	Documento con seguimiento de hallazgos.	Subgerencia TIC	31-Mar-2023 30-Jun-2023 31-Oct-2023 31-Dic-2023
	Definir plan de comunicación y consulta transversal a toda la gestión de riesgo.	Boletines informativos – Informes – Piezas gráficas.	Subgerencia TIC	30-Jun-2023 15-Dic-2023