Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2022 – 2024

Versión preliminar

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

Subgerencia de Tecnologías de la Información y las Comunicaciones

Bogotá D.C., enero 2022

Av. Eldorado No. 66 – 63
PBX: 324 10 00 Fax: 315 34 48
Código postal: 111321
www.educacionbogota.edu.co
Información: Línea 195

Contenido

INTRODUCCIÓN

La Agencia Distrital para la Educación Superior la Ciencia y la Tecnología 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 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.

DEFINICIONES

- Aceptación del riesgo: Decisión informada de tomar un riesgo particular.
- Análisis de riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de este.
- Causa: Origen, comienzo de una situación determinada que genera un efecto o consecuencia.
- Consecuencia: Resultado de un evento que afecta los objetivos.
- Control: Medida que modifica el riesgo.
- Evaluación de riesgos: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.
- Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).
- SGSI: Subsistema de Gestión de Seguridad de la Información.
- Propietario del riesgo: Persona o Entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.
- Riesgo inherente: Efecto de la incertidumbre sobre los objetivos.
- Riesgo de Seguridad de la Información: Probabilidad de ocurrencia de un evento que genere un impacto sobre la Confidencialidad, Integridad y Disponibilidad de la Información.
- Valoración del riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

- Tratamiento del Riesgo: Proceso para modificar el riesgo.
- Vulnerabilidad: Debilidad de un activo que puede ser explotada por una o más amenazas

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.

METODOLOGÍA APLICADA

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 y -Guía de orientación para la gestión de riesgos de seguridad digital en el gobierno nacional, territoriales y sector pública de MinTic.

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 las vigencias 2022-2024.

Tabla 1: Estrategias de implementación

FASE	ACTIVIDADES	ENTREGABLE
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.
	Identificar múltiples partes interesadas	Contexto institucional – Partes interesadas del SGSI.
	Identificar el alcance de los procesos institucionales donde sea aplicable la gestión de riesgos de seguridad.	Manual de gestión de riesgos de seguridad de la información/digital.
	Definir roles y responsabilidades	Manual de gestión de riesgos de seguridad de la información/digital.
	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.
	Adoptar formato para reportar los riesgos de seguridad.	Formato riesgos de seguridad de la información.
Ejecución	Identificar activos de información que tengan un valor alto para la Agencia -ATENEA	Matriz activos de información por proceso.
	Identificar los riesgos inherentes de seguridad (amenazas, vulnerabilidades)	Matriz de riesgos.

FASE	ACTIVIDADES	ENTREGABLE
	Valorar los riesgos de seguridad identificados (probabilidad, impacto)	Matriz de riesgos.
	Establecer y evaluar los controles	Matriz de riesgos.
	Definir los planes de tratamiento para cada uno de los riesgos identificados.	Planes de tratamiento de riesgos de seguridad.
Monitoreo y Revisión	Analizar los eventos e incidentes de seguridad reportados.	Reporte de eventos e incidentes.
	Reportar la gestión del riesgo de seguridad de la información/digital	Reportes internos – Grupos de interés especial
	Solicitar programación y ejecución de auditorias dentro del plan anual de auditoria institucional.	Correo electrónico – Programa de auditorías.
Mejoramiento Continuo	Realizar seguimiento a los hallazgos reportados por la oficina correspondiente.	Documento con seguimiento de hallazgos.
	Definir plan de comunicación y consulta transversal a toda la gestión de riesgo.	Boletines informativos – Informes – Piezas gráficas.

MARCO NORMATIVO

- Decreto 1078 del 26 de mayo del 2015 “Por medio del cual se expide el Decreto único Reglamentario del Sector de Tecnologías de la Información y Comunicaciones”
- Modelo Nacional de Gestión de Riesgos de Seguridad Digital, Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)
- Guía de orientación para la Gestión de Riesgos de Seguridad Digital en el Gobierno Nacional, territoriales y sector público, Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)
- Guía de gestión del riesgo, Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)
- Norma Técnica Colombiana NTC-ISO-IEC 27001:2013
- Norma Técnica Colombiana NTC-ISO 31000:2011
- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012
- Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, Departamento Administrativo de la Función Pública 2020.
- Resolución 500 del 2021 “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”
- CONPES 3854 de 2016. Política Nacional de Seguridad digital
- Decreto 612 de 2018. Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
- Decreto 1083 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública”, el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de “11. Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital”.

FIRMAS

	NOMBRE	CARGO	FECHA	FIRMA
APROBADO POR:				
REVISADO POR:	Lira Jazmín Pineda Moreno	Subgerente TIC	28/01/2022	
ELABORADO POR:	Maria Alejandra Suarez	Contratista TIC	24/01/2022	