Plan de tratamiento de riesgos de seguridad y privacidad de la información

Aprobado por Equipo Técnico de Seguridad Digital – SED – Diciembre 2021

Av. El Dorado No. 66 - 63
Código postal: 111321
PBX: 324 1000 - Fax: 315 34 48
www.educacionbogota.edu.co
Info: Línea 195

Tabla de contenido

1. OBJETIVO 3
2. ALCANCE 3
3. MARCO LEGAL 3
4. REQUISITOS TÉCNICOS 3
5. DOCUMENTOS ASOCIADOS 4
6. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 4
6.1. Planes desarrollados de riesgos de seguridad y privacidad de la información 4
6.2. Plan de acción 2021 para el tratamiento de riesgos de seguridad y privacidad de la información 5
6.3. Riesgos de seguridad y privacidad de la información 6
7. TERMINOS Y DEFINICIONES 7

1. OBJETIVO

Establecer el plan de tratamiento de riesgos el cual hace parte del Sistema de Gestión de Seguridad de la Información – SGSI de la Secretaría de Educación del Distrito SED, a fin de identificar, definir y aplicar los controles con los cuales se busca mitigar la materialización de los riesgos de seguridad de la información en la entidad. De esta forma, se busca que, mediante el tratamiento de los riesgos y la mejora continua de la Seguridad y Privacidad de la Información, las partes interesadas tengan mayor confianza en el tratamiento de la información que almacena y maneja en la Entidad.

2. ALCANCE

El plan de tratamiento de riesgos tiene alcance para los procesos aprobados de la SED, en concordancia con el alcance del Modelo de Seguridad y Privacidad de la Información, habilitador transversal de la Política de Gobierno Digital expedida por el MINTIC.

3. MARCO LEGAL

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.
- Ley 1712 del 6 de marzo de 2014, Transparencia y de Derecho al acceso de la información Pública 2014.
- Decreto 612 del 4 de abril 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 1008 del 14 de junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
- Resolución 1944 de 2016 de la SED. Política de Seguridad y Privacidad de la información.

4. REQUISITOS TÉCNICOS

- Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.
- Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías y Sistemas de Información.

5. DOCUMENTOS ASOCIADOS

- Lineamientos para la Administración del Riesgo de la SED.
- Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas. DAFP. Octubre 2018, Bogotá.
- Manual de Políticas de Seguridad de la Información de la SED.

6. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

En el marco del Modelo de Seguridad y Privacidad de la Información y el Sistema de Gestión de Seguridad de la Información de la SED, se busca prevenir los efectos no deseados que se puedan presentar en cuanto a seguridad de la información, por lo cual es importante identificar y controlar los riesgos de seguridad de la información presentes en los diferentes procesos de la entidad.

Lo anterior, con el objeto de garantizar el tratamiento y gestión de los riesgos de seguridad de la información, de acuerdo con las orientaciones brindadas en la nueva *"Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas"* emitida por el DAFP, y lineamientos internos adoptados por la entidad.

6.1. Planes desarrollados de riesgos de seguridad y privacidad de la información

En la vigencia 2020, se definió la metodología para el tratamiento de riesgos de seguridad y privacidad de la información, de acuerdo con los nuevos lineamientos para la gestión del riesgo de seguridad digital en entidades públicas, dispuesto por el Departamento Administrativo de la Función Pública[1].

De igual manera, para el mismo periodo se definió la Matriz para la gestión de riesgos de seguridad digital de la SED, para el manejo y control de los riesgos de seguridad.

Estos documentos se encuentran publicados en el repositorio documental Isolucion.

1 https://www.funcionpublica.gov.co/documents/418548/34316316/Anexo+4+Lineamientos+para+la+Gestion+del+Riesgo+de++Seguridad+Digital+en+Entidades+Públicas+-+Guía+riesgos+2018.pdf/1ce5099d-c5e5-8ba2-00bc-58f801d3657b

6.2. Plan de acción 2021 para el tratamiento de riesgos de seguridad y privacidad de la información

Actividad	Descripción	Responsable	Planificación	
			Inicio	Final
Actualizar el autodiagnóstico del estado actual del modelo de seguridad y privacidad de la información	Medir el avance en la implementación de la Política de Gobierno Digital según herramientas del MINTIC	Grupo de Seguridad de la Información – Oficina Administrativa de REDP	01/06/2021	31/06/2021
Definición del alcance de los controles a implementar de acuerdo con el anexo A de la norma ISO 27001	Declarar matriz de aplicabilidad para Identificar y complementar la lista de controles del Anexo A, en lo referente a la infraestructura tecnológica de la SED. Estructurar, socializar y hacer seguimiento	Grupo de Seguridad de la Información – Oficina Administrativa de REDP	30/04/2021	31/10/2021
Ejecutar el plan de comunicación y sensibilización del Sistema de gestión de Seguridad de la Información de la SED.	Efectuar espacios de sensibilización en materia de la Política de seguridad y privacidad de la información así como en los riesgos de seguridad a los sistemas de información, los usuarios, las redes y la información en general están expuestos, para generar dentro de los funcionarios buenas prácticas respecto a la seguridad de la	Grupo de Seguridad de la Información – Oficina Administrativa de REDP	20/05/2021	17/06/2021

	información, y de manera preventiva ayudando a la entidad a salvaguardar sus activos de información			
Aplicar y mejorar la seguridad y privacidad de la información en el marco de SGSI de la SED.	Se realizará las actividades para el seguimiento que permitan la medición, análisis y evaluación del desempeño de la seguridad y privacidad de la información, con el fin de generar los ajustes o cambios pertinentes y oportunos.	Grupo de Seguridad de la Información – Oficina Administrativa de REDP	02/01/2021	31/12/2021

6.3. Riesgos de seguridad y privacidad de la información

A continuación, se visualizan los riesgos de Seguridad de la Información que se encuentran identificados y asociados al Sistema de Gestión de Seguridad de la Información – SGSI de la SED, los cuales serán monitoreados trimestralmente.

Nombre	Estado Del Riesgo	Responsable	Monitoreo Realizado por	Materializados en el último monitoreo
Incumplimiento de los procedimientos en los Sistemas de Información	Gestionado	Grupo de Seguridad de la Información – Oficina Administrativa de REDP	Gestión de Tecnologías de Información y comunicaciones	NO

Ataque informático	Gestionado	Grupo de Seguridad de la Información – Oficina Administrativa de REDP	Gestión de Tecnologías de Información y comunicaciones	La herramienta de protección WEB identificó y contuvo 26.236 intentos clasificados como ataques sobre las diferentes aplicaciones publicadas por la entidad desde el 1/01/2021 al 31/05/2021.
Interrupción de la operación de la(s) plataforma(s) tecnológica(s)	Gestionado	Grupo de Seguridad de la Información – Oficina Administrativa de REDP	Gestión de Tecnologías de Información y comunicaciones	Se presentaron 5 interrupciones en la prestación del servicio, debido a fallas eléctricas asumidas por el prestador del servicio "Codensa"
Pérdida, alteración o sustracción de información en medio magnético o físico.	Gestionado	Grupo de Seguridad de la Información – Oficina Administrativa de REDP	Gestión de Tecnologías de Información y comunicaciones	NO
Alteración, pérdida, divulgación, o uso malintencionado de información sensible para la Entidad	Gestionado	Grupo de Seguridad de la Información – Oficina Administrativa de REDP	Gestión de Tecnologías de Información y comunicaciones	NO

7. TERMINOS Y DEFINICIONES

Riesgo: Posibilidad de ocurrencia del evento que tiene un efecto positivo o negativo sobre el producto o servicio generado de un proceso o el cumplimiento de los objetivos institucionales.

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta

que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; estos daños consisten en la afectación de laconfidencialidad, integridad o disponibilidad de la información. Cuando la amenazase convierta en una oportunidad se debe tener en cuenta en el beneficio que se genera

También se puede generar riesgo positivo en la seguridad de la información por el aprovechamiento de oportunidades y fortalezas que se presenten.

Riesgo Positivo: Posibilidad de ocurrencia de un evento o situación que permita optimizar los procesos y/o la gestión institucional, a causa de oportunidades y/o fortalezas que se presentan en beneficio de la entidad.

Seguridad de la Información: Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.

Firma: _____

Aprobado por: Wilson Adiel Rodriguez Rodriguez
Jefe Oficina Administrativa de REDP

Revisado: Jairo Alberto Orduz Salamanca. Profesional Especializado OAREDP
Revisado: Equipo de Seguridad y Gobierno Digital

Elaborado: Juan Carlos Parra. Profesional Contratista OAREDP