PLAN TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

UAESP

Enero 2024

CONTENIDO

ÍNDICE DE TABLAS

TERMINOS Y DEFINICIONES

Aceptación de riesgo: Decisión de asumir un riesgo Amenazas: situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

Activo: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

Análisis de Riesgo: Uso sistemático de la información para identificar fuentes y estimar el riesgo (Guía ISO/IEC 73:2002).

Confidencialidad: Propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

Control: Medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.

Evaluación del riesgo: Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

Gestión del riesgo: Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Impacto: Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Integridad: Propiedad de exactitud y completitud.

Mapa de riesgos: Documento con la información resultante de la gestión del riesgo.

Riesgo: Efecto de la incertidumbre sobre el cumplimiento de los objetivos.

Riesgo de seguridad digital: combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

Tratamiento del riesgo: Decisión que se toma frente a un determinado nivel de riesgo, dicha decisión puede ser aceptar, reducir o evitar y se analiza frente al riesgo residual.

Valoración del riesgo: Proceso de análisis y evaluación del riesgo.

Vulnerabilidad: La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.

1. INTRODUCCIÓN

En un entorno dinámico y altamente interconectado, la Unidad Administrativa Especial de Servicios Públicos reconoce la importancia de salvaguardar la confidencialidad, integridad y disponibilidad de la información que gestiona. La creciente complejidad de las amenazas cibernéticas y los requisitos normativos exige una respuesta proactiva y estructurada para gestionar los riesgos asociados con la seguridad y privacidad de la información.

El plan de tratamiento de riesgos de seguridad y privacidad de la información se basa en una orientación estratégica sobre la prevención, de manera que, se comprenda y apropie el concepto de riesgo y permita a la Entidad adoptar una adecuada transformación digital y hacer frente a los retos globales de manera progresiva y preservando la confidencialidad, integridad y disponibilidad de la información que se encuentra en su custodia.

Así mismo, el plan busca cumplir con la normativa colombiana, la guía para la administración del riesgo del DAFP y las mejores prácticas de gestión de riesgos, que

permita mitigar los impactos generados por la materialización de riegos y aportar de manera integral a la continuidad de las operaciones de la Entidad.

2. OBJETIVOS

- Gestionar los riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios de TI, de acuerdo con los lineamientos establecidos en la Entidad.
- Asegurar la disponibilidad de los servicios críticos de TI y mitigando las interrupciones que aporten a la eficiencia operativa de la Entidad.
- Fortalecer la apropiación de conocimientos en relación con la gestión de riesgos de seguridad y privacidad de la información.

3. ALCANCE

El plan de tratamiento de riesgos de seguridad y privacidad de la información aplica a todos los procesos de la Entidad y a todas sus actividades.

4. METODOLOGÍA DE TRATAMIENTO DE RIESGOS

La metodología para el tratamiento de los riesgos de seguridad y privacidad de la información derivados de los procesos y actividades de la entidad se encuentra integrada en la Política de Administración del Riesgo que busca identificar, valorar, y gestionarlos a un nivel aceptable, haciendo un seguimiento oportuno a los riesgos con el fin de evitar su materialización.

En concordancia, la Entidad elabora el presente plan basado en la guía para la administración del riesgo en el diseño de controles del Departamento Administrativo de la Función Pública (DAFP) V5, en la Política de Administración del Riesgo vigente de la

Unidad Administrativa Especial de Servicios Públicos (UAESP), el Modelo de Seguridad y Privacidad de la Información, y la estrategia de seguridad digital que, de acuerdo con la Resolución 500 del 10 de marzo de 2021, debe integrarse con el Plan de Seguridad y Privacidad de la Información.

5. PLAN DE TRATAMIENTO DE RIESGOS

Considera la definición de las actividades a llevar a cabo con el fin de mitigar los riesgos relacionados con los activos de información. Estas actividades se han estructurado de la siguiente manera:

Tabla 1 Plan de tratamiento de riesgos 2024

ACTIVIDAD	#	ENTREGABLE	RESPONSABLE	FECHA
Revisar y actualizar los lineamientos para la gestión de riesgos, de ser necesario	1.	Política de administración del riesgo actualizada o acta de reunión de pertinencia de la política.	Oficina Asesora de Planeación / OTIC	31/12/2024
Sensibilización	2.	Sensibilizar la política de administración de riesgos	Oficina Asesora de Planeación / OTIC	31/12/2024
Declaración de Aplicabilidad (SOA)	3.	Actualizar y Aprobar la Declaración de aplicabilidad (SOA), de acuerdo con los controles de seguridad establecidos en el Anexo A del	Oficina TIC / Oficina Asesora de Planeación.	30/04/2024

ACTIVIDAD	#	ENTREGABLE	RESPONSABLE	FECHA
		estándar ISO/IEC		
Monitorear y Revisar	4.	Informe de revisión de riesgos y controles por parte de la segunda línea de defensa.	Oficina Asesora de Planeación / Oficina TIC	30/04/2024
	5.	Informe de revisión de riesgos y controles por parte de la segunda línea de defensa.	Oficina Asesora de Planeación / Oficina TIC	31/07/2024
	6.	Informe de revisión de riesgos y controles por parte de la segunda línea de defensa.	Oficina Asesora de Planeación / Oficina TIC	30/11/2024
Revisar y actualizar el plan de tratamiento de riesgos vigencia 2025	7.	Comunicación Oficial del Plan de tratamiento enviado a la OAP para actualizar en la siguiente vigencia	Todos los procesos	31/12/2024

Fuente: Elaboración propia

El tratamiento de los riesgos de seguridad y privacidad de la información identificados se encuentra documentado en el Mapa y plan de manejo de riesgos y oportunidades de los diferentes procesos de la Entidad y que se pueden consultar en el Sistema Integrado de Gestión.

6. VERIFICACIÓN

Para verificación del cumplimiento del plan se realizará a través del número de actividades ejecutadas sobre las programadas en la tabla 1.

$$Cumplimiento\ del\ Plan\ de\ TRSPI\ 2024 = \frac{Actividades\ Ejecutadas}{Actividades\ Planeadas} \times 100\%$$

De igual forma, la eficacia de las acciones definidas se observará a través del informe de segunda línea de defensa o informe final de gestión del riesgo.

7. APROBACIÓN

Elaboró	Juan Sebastián Perdomo Méndez – Profesional Universitario OTIC
Revisó	Luz Mary Palacios Castillo – Profesional Universitario OAP Cesar Mauricio Beltran Lopez – jefe oficina TIC
Aprobó	Comité Institucional de Gestión y Desempeño – Acta de reunión Ni 1 30/01/2024

ALCALDÍA MAYOR
DE BOGOTÁ D.C.

UAESP
Unidad Administrativa Especial
de Servicios Públicos

BOGOTÁ