PLAN TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

UAESP
Enero 2023

Comité Institucional de Gestión y Desempeño

Director(a) General
Jefe(a) Oficina Asesora de Planeación
Jefe(a) Oficina Asesora de Comunicaciones
Jefe(a) Oficina de Tecnologías de Información y Comunicaciones
Jefe(a) Oficina de Control Interno Disciplinario
Subdirector(a) Administrativo y Financiero
Subdirector(a) Asuntos Legales.
Subdirector(a) Recolección Barrido y Limpieza.
Subdirector(a) Aprovechamiento
Subdirector(a) Disposición Final
Subdirector(a) Servicios Funerarios y Alumbrado público.

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

TERMINOS Y DEFINICIONES

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.

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.

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

Apetito al riesgo: magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener.

Causa: Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

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.

Nivel de riesgo: Da el resultado en donde se ubica el riesgo por cada activo de información.

Probabilidad: Se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.

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.

Riesgo Inherente: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.

Riesgo residual: Nivel restante de riesgo después del tratamiento del riesgo.

Tratamiento del riesgo: Proceso de selección e implementación de acciones de mejorar que permitan mitigar el riesgo.

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

El plan de tratamiento de riesgos de seguridad y privacidad de la información de la Unidad Administrativa Especial de servicios Públicos 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

- Establecer las actividades para realizar la gestión de riesgos de seguridad y privacidad de la información en la Unidad Administrativa Especial de Servicios Públicos (UAESP)
- Fortalecer la apropiación de conocimientos en relación con la gestión de riesgos de seguridad y privacidad de la información.
- Contribuir con la mejora continua del proceso de gestión de riesgos y continuidad de las operaciones de la Entidad.

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, planificar y adelantar el tratamiento oportuno que mantenga los riesgos en niveles óptimos de control y así preparar a la Entidad ante una posible materialización de alguno de los riesgos identificados, así mismo, poder adelantar procesos de seguimiento, monitoreo, evaluación, o auditoría, según corresponda.

En concordancia, la entidad realiza el plan basado en la guía para la administración del riesgo en el diseño en controles del Departamento Administrativo de Función Pública-DAFP V5, en la Política de Administración del Riesgo vigente de la Unidad Administrativa Especial de Servicios Públicos (UAESP) y la norma técnica ISO/IEC 27001:2013.

5. PLAN DE TRATAMIENTO DE RIESGOS

Contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos de información, las cuales se estructuraron de la siguiente manera:

Tabla 1 Plan de tratamiento de riesgos 2023

ACTIVIDAD	ENTREGABLE	RESPONSABLE	FECHA INICIO	FECHA FIN
Realizar una socialización de la Política de Administración del Riesgo Vigente	Listado de Asistencia	Oficina Asesora de Planeación / OTIC	01/02/2023	31/12/2023
Publicación de riesgos y oportunidades 2023.	Matriz de Riesgos publicada	Oficina Asesora de Planeación	01/02/2023	28/02/2023
Actualización de la Declaración de Aplicabilidad (SOA).	Actualizar y Aprobar la Declaración de aplicabilidad (SOA), de acuerdo con los controles de seguridad establecidos en el Anexo A del estándar ISO/IEC 27001.	Oficina TIC / Oficina Asesora de Planeación.	01/02/2023	31/12/2023
Actualizar inventario de activos de información	Inventario actualizado y aprobado	Todos los procesos	01/02/2023	31/12/2023
Monitorear y Revisar.	Informe de revisión de riesgos y controles por parte de la segunda línea de defensa.	Oficina Asesora de Planeación / Oficina TIC	10/04/2023 10/07/2023 10/10/2023 10/01/2024	30/04/2023 30/07/2023 30/10/2023 30/01/2023
Actualizar lineamientos para la administración del riesgo.	Política de Administración del Riesgo actualizada. En caso de no ser requerida la actualización, informe de la revisión de su	CICCI	01/02/2023	30/11/2023

ACTIVIDAD	ENTREGABLE	RESPONSABLE	FECHA INICIO	FECHA FIN
	adecuación.			
Revisar y actualizar el plan de tratamiento de riesgos vigencia 2024	Plan de tratamiento enviados a la OAP para actualizar en la siguiente vigencia	Todos los procesos	01/12/2023	31/12/2023
Aprobar plan de tratamiento de riesgos 2024	Acta de aprobación del CIGD del plan de tratamiento de riesgos 2024	OAP	01/01/2024	31/01/2024

Fuente: Elaboración propia

6. VERIFICACIÓN

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

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	Luz Mary Palacios Castillo – Profesional Universitario OAP Juan Sebastián Perdomo Méndez – Profesional Universitario OTIC
Revisó	Sayra Paola Nova Murcia – Oficial de Seguridad de la Información. Cesar Mauricio Beltrán López – Jefe Oficina TIC
Aprobó	Comité Institucional de Gestión y Desempeño – Acta de Reunión 30 de enero de 2023

UAESP
Unidad Administrativa Especial
de Servicios Públicos

BOGOTÁ