****

**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

***UAESP***

***Enero 2025***

**CONTENIDO**

[ÍNDICE DE TABLAS 2](#_Toc156294900)

[TERMINOS Y DEFINICIONES 3](#_Toc156294901)

[1. INTRODUCCIÓN 5](#_Toc156294902)

[2. OBJETIVOS 5](#_Toc156294903)

[3. ALCANCE 6](#_Toc156294904)

[4. METODOLOGÍA DE TRATAMIENTO DE RIESGOS 6](#_Toc156294905)

[5. PLAN DE TRATAMIENTO DE RIESGOS 6](#_Toc156294906)

[6. VERIFICACIÓN 8](#_Toc156294907)

[7. APROBACIÓN 8](#_Toc156294908)

# ÍNDICE DE TABLAS

[Tabla 1 Plan de tratamiento de riesgos 2025 6](#_Toc188000933)

# 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.

# INTRODUCCIÓN

En un entorno dinámico e interconectado, la Unidad Administrativa Especial de Servicios Públicos reconoce la necesidad de gestionar proactivamente los riesgos asociados con la seguridad y privacidad de la información. El Plan de Tratamiento de Riesgos, integrado con el Plan de Seguridad y Privacidad de la Información, proporciona una orientación estratégica enfocada en la prevención, permitiendo a la Entidad adoptar una transformación digital progresiva mientras salvaguarda la confidencialidad, integridad y disponibilidad de la información bajo su custodia. Este plan, alineado con la normativa colombiana, las guías del DAFP y las mejores prácticas internacionales, busca mitigar los impactos de los riesgos materializados y garantizar la continuidad de las operaciones de la Entidad.

# OBJETIVOS

* Gestionar los riesgos asociados con la seguridad y privacidad de la información, seguridad digital y continuidad de los servicios de TI, en alineación con los lineamientos establecidos por la Entidad.
* Garantizar la disponibilidad de los servicios críticos de TI, mitigando interrupciones y contribuyendo a la eficiencia operativa de la organización.
* Promover el fortalecimiento y apropiación de conocimientos en la gestión de riesgos de seguridad y privacidad de la información, impulsando una cultura de seguridad dentro de la Entidad.

# ALCANCE

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

# METODOLOGÍA DE TRATAMIENTO DE RIESGOS

La metodología para el tratamiento de riesgos de seguridad y privacidad de la información en los procesos y actividades de la Entidad está integrada en la Política de Administración del Riesgo. Esta metodología permite identificar, valorar y gestionar los riesgos hasta alcanzar niveles aceptables, garantizando un seguimiento continuo para prevenir su materialización.

El presente plan se elabora con base en la guía para la administración del riesgo en el diseño de controles del Departamento Administrativo de la Función Pública (DAFP) V5, 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. En cumplimiento de la Resolución 500 del 10 de marzo de 2021, este plan se integra con el Plan de Seguridad y Privacidad de la Información, asegurando un enfoque coordinado y alineado con las mejores prácticas y lineamientos normativos.

# 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 2025

| **ACTIVIDAD** | **#** | **ENTREGABLE** | **RESPONSABLE** | **FECHA** |
| --- | --- | --- | --- | --- |
| Revisar y actualizar los lineamientos para la gestión de riesgos, de ser necesario |  | Política de administración del riesgo actualizada o comunicación oficial de la pertinencia de la política. | Oficina Asesora de Planeación / OTIC | 31/12/2025 |
| Sensibilizar la política de administración de riesgos. |  | Sensibilizar la política de administración de riesgos. | Oficina Asesora de Planeación / OTIC | 31/12/2025 |
| Actualizar 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 | Oficina TIC | 30/04/2025 |
| Monitorear y Revisar controles de seguridad segunda linea de defensa. |  | Informe de revisión de riesgos y controles por parte de la segunda línea de defensa. | Oficina Asesora de Planeación / Oficina TIC | 30/04/2025 |
|  | Informe de revisión de riesgos y controles por parte de la segunda línea de defensa. | Oficina Asesora de Planeación / Oficina TIC | 31/07/2025 |
|  | Informe de revisión de riesgos y controles por parte de la segunda línea de defensa. | Oficina Asesora de Planeación / Oficina TIC | 30/11/2025 |
| Revisar y actualizar el plan de tratamiento de riesgos vigencia 2026 |  | Comunicación Oficial del Plan de tratamiento enviado a la OAP para actualizar en la siguiente vigencia | Oficina TIC | 31/12/2025 |

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](https://www.uaesp.gov.co/mipg/sig.php).

# VERIFICACIÓN

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

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

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.

# REVISIÓN Y ACTUALIZACIÓN

El presente plan será revisado y actualizado al menos una vez al año o con mayor frecuencia, según lo requieran los lineamientos normativos o los cambios en el contexto interno o externo de la UAESP. Todas las actualizaciones deberán ser aprobadas por el comité institucional de gestión y desempeño para garantizar su alineación con los objetivos estratégicos de la Entidad.

# APROBACIÓN

|  |  |
| --- | --- |
| **Elaboró** | Juan Sebastián Perdomo Méndez – Profesional Universitario OTIC |
| **Revisó** | Yuli Marcela Toro Pascagaza – Jefe Oficina Asesora de PlaneaciónJorge Alexis Rodriguez Meza – Jefe Oficina TIC |
| **Aprobó** | Comité Institucional de Gestión y Desempeño – Acta de reunión xx/01/2025 |

