

**PLAN TRATAMIENTO DE**

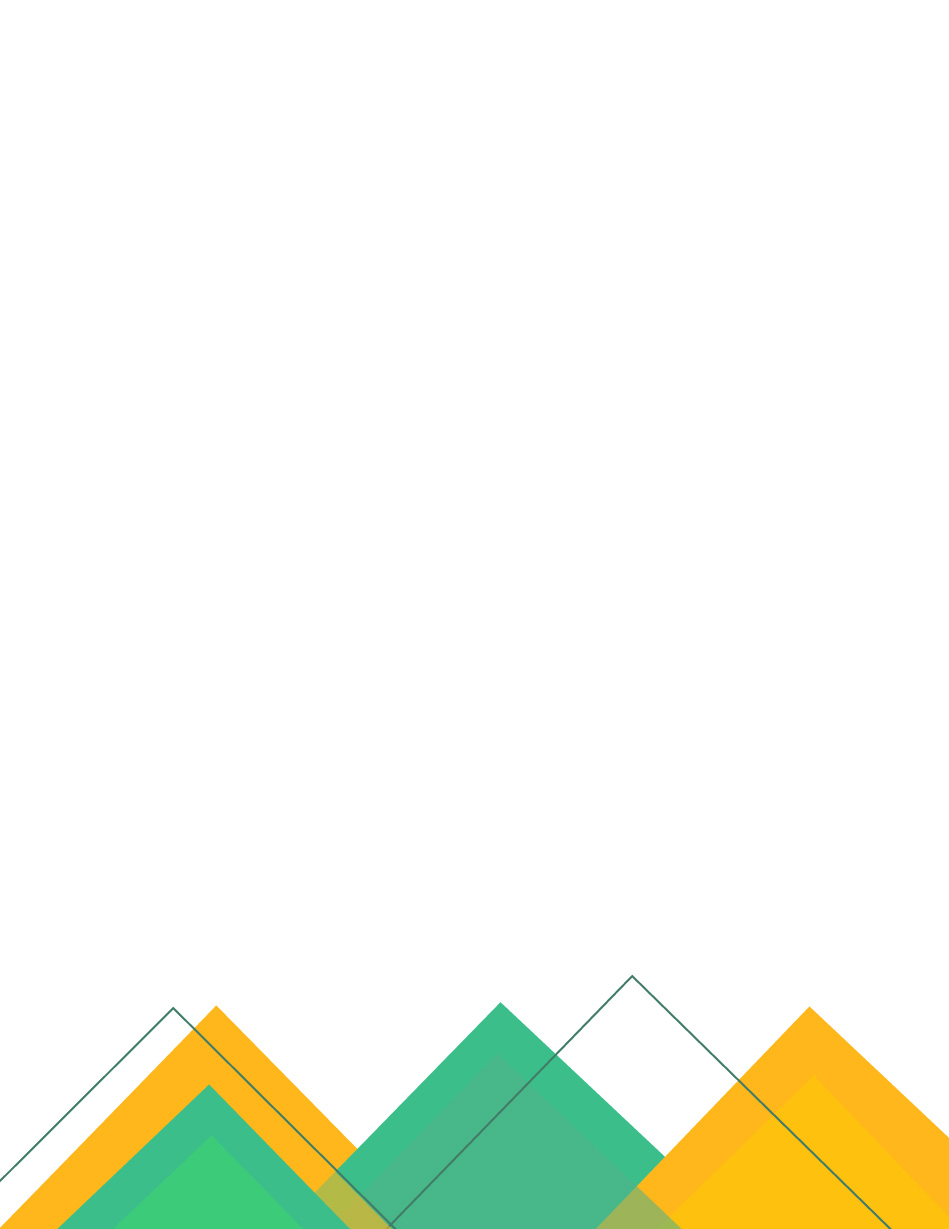
**RIESGOS DE SEGURIDAD**

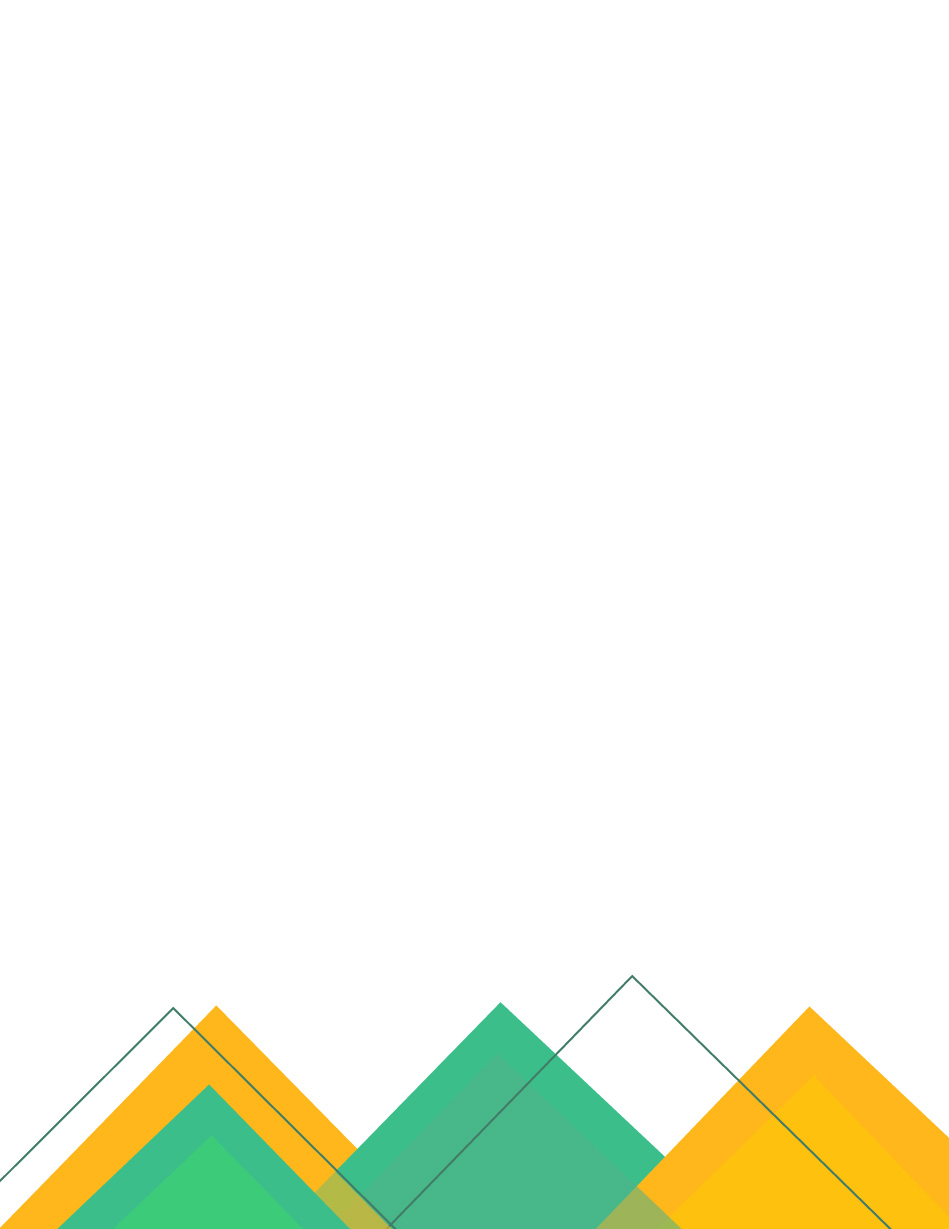
**Y PRIVACIDAD DE LA**

**INFORMACIÓN**

***UAESP***

***Enero 2022***





***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

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

[TABLA DE CONTENIDO 4](#_Toc93584233)

[ÍNDICE DE TABLAS 4](#_Toc93584234)

[GLOSARIO 5](#_Toc93584235)

[1. OBJETIVO 6](#_Toc93584236)

[2. ALCANCE 6](#_Toc93584237)

[3. METODOLOGÍA DE TRATAMIENTO DE RIESGOS 6](#_Toc93584238)

[4. PLAN DE TRATAMIENTO DE RIESGOS 7](#_Toc93584239)

# 

# ÍNDICE DE TABLAS

[**Tabla 1 Plan Actividades Tratamiento de Riesgos 7**](#_Toc93508784) **- 8**

# GLOSARIO

**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.

# OBJETIVO

Establecer el plan de trabajo para realizar la gestión de riesgos de seguridad de la información en la Unidad Administrativa Especial de Servicios Públicos (UAESP), la cual debe incluir amenazas, vulnerabilidades, riesgos, controles, niveles aceptables de riesgo y el tratamiento de riesgos.

# ALCANCE

El plan de tratamiento de riesgos de seguridad y privacidad de la información aplica a todos los procesos, servidores(as) públicos(as) y contratistas de la Entidad, basado en la guía para la administración del riesgo en el diseño en controles del Departamento Administrativo de Función Pública-DAFP V5, y en la Política de Administración del Riesgo V3 de la Unidad Administrativa Especial de Servicios Públicos (UAESP) y la norma técnica ISO/IEC 27001.

# METODOLOGÍA DE TRATAMIENTO DE RIESGOS

La metodología para el tratamiento de los riesgos de seguridad de la información y comunicaciones derivados de los procesos de la entidad que busca descubrir, valorar, planificar y adelantar el tratamiento oportuno que busque mantener los riesgos en niveles óptimos de control y así preparar a la entidad para una posible materialización de alguno de los riesgos y dentro de la misma línea, 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 V3 de la Unidad Administrativa Especial de Servicios Públicos (UAESP) y la norma técnica ISO/IEC 27001.

# 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 Actividades Tratamiento de Riesgos

|  |  |  |  |
| --- | --- | --- | --- |
| **ACTIVIDADES** | **TAREAS** | **RESPONSABLE DE LA TAREA** | **FECHAS LÍMITE PROGRAMACIÓN TAREAS** |
| Sensibilización. | Socializar la Política Administración del Riesgo. | Oficina Asesora de Planeación. | 31 de marzo del 2022. |
| Identificación y actualización de riesgos de seguridad y privacidad de la información. | Identificar y actualizar los riesgos de seguridad y privacidad de la información.  Identificación de riesgos residuales. | Todos los procesos. | 31 de diciembre del 2022. |
| Aprobación de los riesgos identificados. | Aprobar los riesgos identificados. | Comité Institucional de Gestión y Desempeño. | 31 de enero de 2022. |
| Publicación del Mapa y plan de manejo de riesgos y oportunidades 2022. | Publicar el Mapa y plan de manejo de riesgos y oportunidades 2022. | Oficina Asesora de Planeación | 31 de enero de 2022. |
| Seguimiento fase de tratamiento de riesgos. | Seguimiento del estado de los planes de tratamiento de riesgos identificados y verificación de evidencias. | Oficina de Tecnologías de la Información | Trimestral durante la vigencia. |
| Verificación de la Matriz de Riesgos. | Verificar la matriz de Riesgos de Seguridad de la Información. | Oficina de Tecnologías de la Información y Oficina Asesora de Planeación. | Trimestral durante la vigencia. |
| 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 de Tecnologías de la Información y Oficina Asesora de Planeación. | 31 de agosto de 2022. |
| Infraestructura Critica Cibernética. | Revisar y reportar la infraestructura critica cibernética de la entidad. | Oficina de Tecnologías de la Información. | 30 de junio de 2022. |
| Mejoramiento. | Revisar o actualizar del Plan de tratamiento de riesgos de Seguridad de la Información. | Oficina de Tecnologías de la Información. | 30 de junio de 2022 |
| Monitoreo. | Monitorear el cumplimiento de las políticas y procedimientos en materia de seguridad y estar al tanto de las modalidades de ciberataque que puedan afectar la entidad. | Oficina de Tecnologías de la Información. | 31 de diciembre de 2022. |
| Comunicar. | Comunicar el Plan de tratamiento de Riesgos de Seguridad de la Información a la entidad. | Oficina de Tecnologías de la Información. | 31 de enero de 2022 |
| Reportes al Comité Institucional de Gestión y Desempeño. | Reportar los resultados del análisis de riesgos al comité institucional de gestión y desempeño. | Oficina Asesora de Planeación y Oficina de Tecnologías de la Información. | Trimestral vencido |

Fuente Propia