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

HÉCTOR RANGEL PALACIOS
Alcalde 2024 – 2027

MARTA CECILIA RIVERA HIGUITA
Subsecretaria Tics y Gestión Documental

ENERO DE 2024

CONTENIDO

1. OBJETIVO

Definir el plan de tratamiento de riesgos, de tal forma que se precisen y apliquen los controles con lo cual se busca mitigar la materialización de los riesgos de seguridad de la información en la Alcaldía de Apartadó. 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 se almacena y maneja en la Entidad.

2. ALCANCE

El plan de tratamiento de riesgos tiene alcance para todos los procesos de la Alcaldía de Apartadó.

3. TERMINOS Y DEFINICIONES

Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.

Amenaza: Es la causa potencial de una situación de incidente y no deseada por la organización.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Consecuencia: Resultado de un evento que afecta los objetivos. Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.

Control: Medida que modifica el riesgo. Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Evento: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.
Factores de Riesgo: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

Identificación del riesgo: Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Impacto: Cambio adverso en el nivel de los objetivos del negocio logrados.

Monitoreo: Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de con trol o las diferentes auditorías de los sistemas integrados de gestión.

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos inaceptables en el marco de la seguridad de la información e implantar los controles necesarios para proteger la misma.

Partes interesadas (Stakeholder): Personas u organizaciones que puede afectar a, ser afectada por, o percibirse a sí misma como afectada por una decisión o actividad.

Proceso: Conjunto de actividades interrelacionadas que apuntan a un objetivo o que interactúan para transformar una entrada en salida.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

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.

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.

4. TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Los riesgos en relación con la privacidad pueden ser de varios tipos:

- En relación con la información personal de los individuos
  - Se expone información clasificada (datos personales no públicos) sin que medie autorización para ello
  - Uso de sistemas de información o aplicaciones en la interacción con los ciudadanos que pueden ser intrusivos sobre su privacidad sin advertir previamente a los usuarios sobre ello (geolocalización)
  - Información que permanece en poder de la entidad por más tiempo de la vigencia que tiene la base de datos o en contra del ejercicio de derecho de supresión por parte del titular-ciudadano.

- En relación con la información de usuarios institucionales
  - Se divulga información que puede ser clasificada como secreto industrial o que pone en riesgo la imagen corporativa.
  - En relación con los sistemas de información y programas usados o los procedimientos y procesos relacionados con la gestión administrativa a cargo.
  - Procesos no ajustados al sistema de gestión documental que garanticen medidas de protección sobre la información.
  - Adquisición de programas que no garanticen un nivel adecuado de privacidad, por ejemplo que permitan recolección masiva de datos sin conocimiento de los usuarios.
  - Indebida utilización de datos personales en ejercicios de divulgación tales como procesos de rendición de cuentas, publicación de información en la página web, etc.
  -

El análisis debe reflejarse en una matriz de riesgos ponderando la probabilidad de su ocurrencia (ejemplo: baja-intermedia-alta) y el impacto que puede generar su causación (se sugiere utilizar una tabla numérica, por ejemplo - 1 ningún impacto a 10 impacto considerable).

4.1 RIESGOS DE SEGURIDAD DE LA INFORMACIÓN ASOCIADOS AL MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

A continuación, se visualizan los riesgos de Seguridad de la Información, los cuales se encuentran asociados al modelo de Gestión de Seguridad de la Información.

CODIGO	NOMBRE RIESGO	ESTADO	DESCRIPCION	RESPONSABLE
R01	Obsolescencia de hardware, software.	Gestionado	El cambio de manera acelerada de la tecnología. Poca inversión por temas políticos, de presupuesto o por ser irrelevante en el plan de desarrollo.	Subsecretaria de Tics y Gestión Documental.
R02	Perdida de la información alojada en el centro de datos.	No se encuentra gestionado en su totalidad	Podría presentarse por cortes de energía de manera repentina. Por catástrofes naturales. Actos vandálicos de terrorismo o asonadas. Mal funcionamiento del software y/o hardware donde se almacena esta información. Copias de seguridad no realizadas o mal realizadas. Por incendios, inundaciones, plagas.	Subsecretaria de Tics y Gestión Documental. Profesional Universitario Sistemas
R03	Perdida de documentos físicos.	No se encuentra gestionado en su totalidad	Por catástrofes naturales. Actos vandálicos de terrorismo o asonadas. Por incendios, inundaciones, plagas.	Subsecretaria de Tics y Gestión Documental. Profesional Universitario Archivo

R04	Perdida de la información alojada en estaciones de trabajo.	No se encuentra gestionado.	Podría presentarse por cortes de energía de manera repentina. Por catástrofes naturales. Actos vandálicos de terrorismo o asonadas. Mal funcionamiento del software y/o hardware donde se almacena esta información. Copias de seguridad no realizadas o mal realizadas. Por incendios, inundaciones, plagas.	Subsecretaria de Tics y Gestión Documental. Profesional Universitario Sistemas
R05	Afectación de la información por ataques cibernéticos (Software malicioso, virus, ataques ingeniería social).	No se encuentra gestionado en su totalidad	Podría presentarse por una gestión equivocada de la seguridad, baja inversión en conocimientos de este tipo y terrorismo.	Subsecretaria de Tics y Gestión Documental. Profesional Universitario Sistemas
R06	Fallas en la Disponibilidad de la información.	Gestionado	Podría presentarse por Mal funcionamiento del software y/o hardware donde se procesa esta, también en los equipos de comunicación utilizados. Contrataciones mal realizadas para servicio de software de mantenimiento y/o acuerdos de nivel de servicio o software no cumplidos.	Subsecretaria de Tics y Gestión Documental. Profesional Universitario Sistemas

			Fallas en la consecución de la TRD Falta de personal idóneo y capacitado. Interrupciones Eléctricas.	
R07	Violación a la confidencialidad de la información.	No se encuentra gestionado en su totalidad	Esta se puede presentar por problemas en los perfiles asignados en los diferentes softwares, también por fallas en estos. Por intrusiones realizadas de manera no autorizadas a la información ya sea física o digital.	Subsecretaria de Tics y Gestión Documental. Profesional Universitario Archivo Profesional Universitario Sistemas
R08	Violación a la Integridad de la información.	Gestionado	Esta se puede presentar por intrusiones realizadas de manera no autorizada a la información ya sea física o digital. Alteración indebida de manera consciente o inconsciente. Fallas en los diferentes softwares. Falta de personal idóneo y capacitado.	Subsecretaria de Tics y Gestión Documental. Profesional Universitario Archivo Profesional Universitario Sistemas

5. MARCO LEGAL

- ✓ Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.
- ✓ Ley 1581 de 2012 Por la cual se dictan disposiciones generales para la protección de datos personales.
- ✓ Decreto 1083 de 2015 Artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos y publicarlos, en su respectiva página web, a más tardar el 31 de enero de cada año. (Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y Plan de Seguridad y Privacidad de la Información, entre otros).
- ✓ Decreto 1078 de 2015 Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- ✓ Decreto 612 de 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 de 14 de junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
- ✓ Decreto 767 del 16 de mayo 2022, Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- ✓ Decreto 1389 de 2022 Por el cual se adiciona el Título 24 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para la gobernanza en la infraestructura de datos y se crea el Modelo de gobernanza de la infraestructura de datos
- ✓ Directiva Presidencial 03 de marzo de 2021 Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.
- ✓ Directiva Presidencial 24 de febrero de 2022 Reiteración de la política pública en materia de seguridad digital.

6. REQUISITOS TÉCNICOS

- ✓ Norma Técnica Colombiana NTC/ISO 27001:2022 Sistemas de gestión de la seguridad de la información.
- ✓ Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías y Sistemas de Información.

7. MONITOREO Y REVISIÓN

La subsecretaria Tics y de Gestión Documental o quien haga sus veces y el funcionario líder de cada uno de los componentes, son responsables de formular, ejecutar, monitorear las actividades establecidas en los componentes del Plan de riesgos de Seguridad y privacidad de la Información.

8. DOCUMENTOS ASOCIADOS

- ✓ Procedimiento para la Seguridad de la Información.
- ✓ Manual de Políticas de Seguridad de la Información.

9. RESPONSABLE DEL DOCUMENTO

Subsecretaria Tics y Gestión Documental.