PLAN DE TRATAMIENTOS DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN SOLUCIÓN TECNOLÓGICA DE LA AGENCIA PARA LA GESTIÓN DEL PAISAJE, EL PATRIMONIO Y LAS ALIANZAS PÚBLICO PRIVADAS - APP

Enero de 2024
Medellín

1 Tabla de Contenido

Fecha	Versión	Realizado por	Descripción
15 de enero 2024	2.0	Andrés Mauricio Moreno Álvarez	Creación de documento Plan de tratamientos de Riesgos de seguridad y privacidad de la información Solución Tecnológica de la Agencia para la Gestión del Paisaje, el Patrimonio y las Alianzas Público Privadas - APP

1. INTRODUCCIÓN

La Seguridad Informática se basa en la existencia de un conjunto de directrices que brinden instrucciones claras y oportunas, soportando la gestión de la Alta Dirección frente al gran dinamismo de nuevos ataques y violaciones a la seguridad e integridad de la información.

La Seguridad de la Información en las empresas tiene como objetivo la protección de los activos de información en cualquiera de sus estados ante una serie de amenazas o brechas que atenten contra sus principios fundamentales de confidencialidad, integridad y su disponibilidad, a través de la implementación de medidas de control de seguridad de la información, que permitan gestionar y reducir los riesgos e impactos a que está expuesta y se logre alcanzar el máximo retorno de las inversiones en las oportunidades de negocio.

En términos generales el plan de tratamiento de riesgo de seguridad de la información, propende por englobar los procedimientos más adecuados, tomando como lineamientos principales cuatro criterios, que se detallan a continuación:

Seguridad Organizacional: Dentro de este, se establece el marco formal de seguridad que debe sustentar la AGENCIA APP, incluyendo servicios o contrataciones externas a la infraestructura de seguridad, integrando el recurso humano con la tecnología, denotando responsabilidades y actividades complementarias como respuesta ante situaciones anómalas a la seguridad.

Seguridad Lógica: Trata de establecer e integrar los mecanismos y procedimientos, que permitan monitorear el acceso a los activos de información, que incluyen los procedimientos de administración de usuarios, definición de responsabilidades, perfiles de seguridad, control de acceso a las aplicaciones y documentación sobre sistemas, que van desde el control de cambios en la configuración de los equipos, manejo de incidentes, selección y aceptación de sistemas, hasta el control de software malicioso.

Seguridad Física: Identifica los límites mínimos que se deben cumplir en cuanto a perímetros de seguridad, de forma que se puedan establecer controles en el manejo de equipos, transferencia de información y control de los accesos a las distintas áreas con base en la importancia de los activos.

Seguridad Legal: Integra los requerimientos de seguridad que deben cumplir todos los funcionario, contratistas, colaboradores y usuarios de la red institucional bajo la reglamentación de la normativa interna de la AGENCIA APP, en cuanto al recurso humano, tendrá sanciones aplicables ante faltas cometidas de acuerdo con la Ley o la normativa interna estipulada.

2. OBJETIVO

Brindar a la AGENCIA APP una herramienta con enfoque sistemático que proporcione las pautas necesarias para desarrollar y fortalecer una adecuada gestión de los riesgos de seguridad de la información, a través de métodos que faciliten la determinación del contexto estratégico, la identificación de riesgo y oportunidades, el análisis, la valoración y expedición de políticas, así como el seguimiento y monitoreo permanente enfocado a su cumplimiento y mejoramiento continuo

3. ALCANCE

La gestión de riesgos de seguridad de la información y su tratamiento, podrá será aplicada sobre cualquier proceso de la AGENCIA APP, a cualquier sistema de información o aspecto particular de control de la Entidad, a través de los principios básicos y metodológicos para la administración de los riesgos de seguridad de la información, así como las técnicas, actividades y formularios que permitan y faciliten el desarrollo de las etapas de reconocimiento del contexto, identificación de los riesgos de seguridad de la información, análisis y evaluación, opciones de tratamiento o manejo del riesgo según la zona de riesgo; incluye además pautas y recomendaciones para su seguimiento, monitoreo y evaluación.

4. OBJETIVOS ESPECÍFICOS

- Establecer los criterios y comportamientos que deben seguir todos los funcionarios, contratistas, colaboradores y usuarios de la AGENCIA APP, con el fin de velar por la adecuada protección, preservación y salvaguarda de la información y de los sistemas corporativos, respondiendo a los intereses y necesidades organizacionales y dando cumplimiento a los 3 principios de la gestión de la información: **Confidencialidad, Integridad y Disponibilidad**, acogidos de la mejores prácticas de gestión de la información, implícitas en el estándar internacional ISO/IEC-27001:2005.

- Difundir las políticas y estándares de seguridad informática a todo el personal de la AGENCIA APP, para que sea de su conocimiento y cumplimiento en los recursos informáticos utilizados o asignados y establecer las responsabilidades, principios, criterios, directrices y conductas dentro de los lineamientos de la ética y el buen gobierno de la AGENCIA APP.

- Planear, organizar, dirigir y controlar las actividades para mantener y garantizar la integridad física de los recursos informáticos, así como resguardar los activos de la AGENCIA APP.

- Generar una cultura y apropiación de trabajo enfocada a la identificación de los riesgos de seguridad de la información, y su mitigación.

5. VIGENCIA

Todas las amenazas están en continuo proceso de expansión, lo que, unido al progresivo aumento de los sistemas de información y dependencia del negocio, hace que todos los sistemas y aplicaciones estén expuestos a riesgos cada vez mayores, que, sin una adecuada gestión de los mismos, pueden ocasionar que su vulnerabilidad se incremente y consiguientemente los activos se vean afectados. Todo funcionario, contratista, colaborador y usuario de La AGENCIA APP, es responsable del cumplimiento de los estándares, directrices y procedimientos de control de acceso, así como también de notificar a su nivel jerárquico superior, cuando por algún motivo no pueda cumplir con las Políticas de Seguridad indicando el motivo por el cual no le es posible apegarse a la normativa de seguridad. Cabe destacar que este nivel de responsabilidad va a ser conocido por las diferentes áreas de La AGENCIA APP, quien será el garante de que esta información sea conocida por cada integrante de área.

Esta normativa deberá ser revisada y actualizada conforme a las exigencias de la AGENCIA APP o en el momento en que haya la necesidad de realizar cambios sustanciales en la infraestructura tecnológica.

6. DEFINICIONES

A continuación, se listan algunos términos y definiciones de términos que se utilizarán durante el desarrollo de la gestión de riesgos de seguridad de la información, en beneficio de unificar criterios dentro de la AGENCIA APP

Administración del riesgo: Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

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.
Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.
Amenaza: Es la causa potencial de una situación de incidente y no deseada por la organización

Causa: Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.

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.

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

Evaluación de riesgos: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

Evento: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

Estimación del riesgo: Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

Evitación del riesgo: Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

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.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.
Identificación del riesgo. Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

SGSI: Sistema de Gestión de Seguridad de la Información

7. VISIÓN GENERAL PROCESO DE GESTIÓN DE RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN.

Se presenta el modelo de gestión de riesgos de seguridad de la información diseñado basado tanto en la norma ISO/IEC 31000 como en la ISO 27005 para la adecuada administración de riesgos en la seguridad de la información; los elementos que lo componen son:

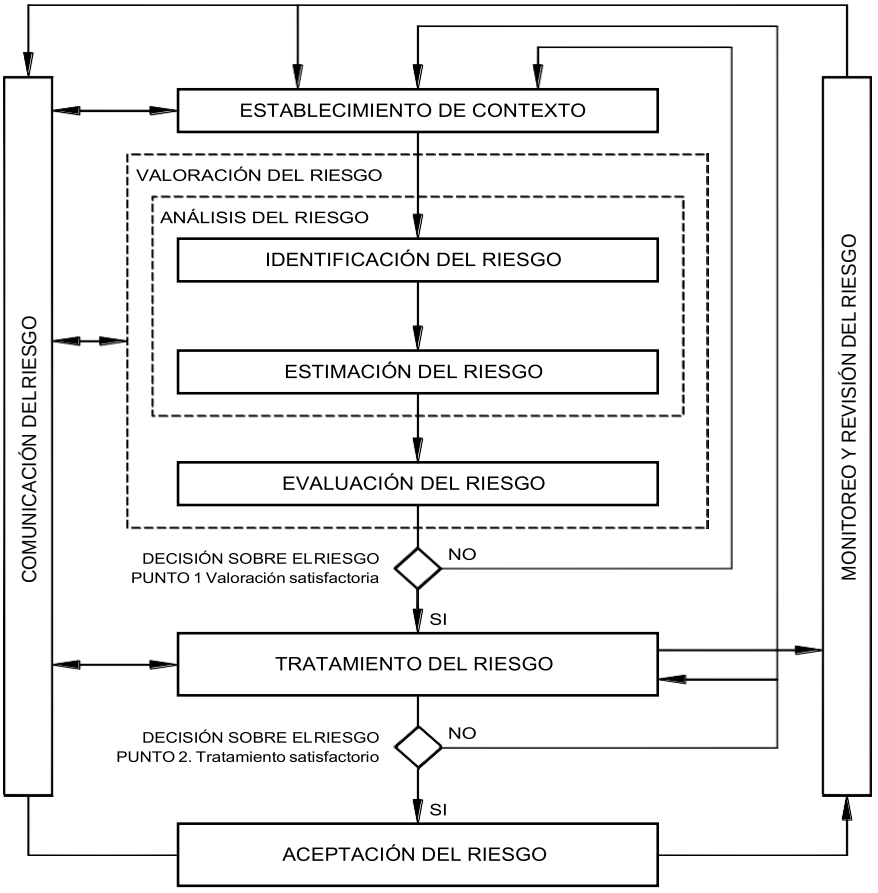


Imagen 1: VISIÓN PROCESO DE RIESGOS DE SEGURIDAD

La gestión de riesgos de seguridad de la información deberá ser iterativa para las actividades de valoración de riesgos y/o tratamiento de estos.

8 RIESGO DE SEGURIDAD DE LA INFORMACIÓN

Como criterios para la gestión de riesgos de seguridad de la información se establecen:

8.1 Criterios de evaluación del riesgo de seguridad de la información:

La evaluación de los riesgos de seguridad de la información se enfocará en:

- El valor estratégico del proceso de información en la AGENCIA APP
- La criticidad de los activos de información involucrados.

- Los requisitos legales y reglamentarios, así como las obligaciones contractuales.
- La importancia de la disponibilidad, integridad y confidencialidad para las operaciones de la AGENCIA APP

8.1.1 Criterios de Impacto

Los criterios de impacto se especificarán en términos del grado, daño o de los costos para La AGENCIA APP causados por un evento de seguridad de la información, considerando aspectos tales como:

- Nivel de clasificación de los activos de información impactados
- Brechas en la seguridad de la información (pérdida de la confidencialidad, integridad y disponibilidad)
- Operaciones deterioradas (afectación a partes internas o terceras partes)
- Pérdida del negocio y del valor financiero
- Alteración de planes o fechas límites
- Daños en la reputación
- Incumplimiento de los requisitos legales, reglamentarios o contractuales

8.1.2 Criterios de Aceptación

Los criterios de aceptación dependerán con frecuencia de las políticas, metas, objetivos de la AGENCIA APP y de las partes interesadas.

8.2 VALORACIÓN DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Previo a la valoración de riesgos de seguridad de la información se determina la relevancia de identificar un inventario de activos de información de los procesos, el cual será la base del enfoque de la valoración de los riesgos de seguridad de la información.

Se deberán identificar, describir cuantitativamente o cualitativamente y priorizarse frente a los criterios de evaluación del riesgo y los objetivos relevantes para La AGENCIA APP esta fase consta de las siguientes etapas:

La valoración del Riesgo de seguridad de la información consta de las siguientes actividades:

- Análisis del riesgo
    - Identificación de los riesgos
    - Estimación del riesgo
- Evaluación del riesgo

8.2.1 Identificación del riesgo

Para la evaluación de riesgos de seguridad de la información en primer lugar se deberán identificar los activos de información por proceso en evaluación.

Los **activos de información** se clasifican en dos tipos:

A. Primarios:

a) **Procesos o subprocesos y actividades del Negocio:** procesos cuya pérdida o degradación hacen imposible llevar a cabo la misión de la organización; procesos que contienen procesos secretos o que implican tecnología propietaria; procesos que, si se modifican, pueden afectar de manera muy significativa el cumplimiento de la misión de la organización; procesos que son necesarios para el cumplimiento de los requisitos contractuales, legales o reglamentarios.

b) **Información:** información vital para la ejecución de la misión o el negocio de la organización; información personal que se puede definir específicamente en el sentido de las leyes relacionadas con la privacidad; información estratégica que se requiere para alcanzar los objetivos determinados por las orientaciones estratégicas; información del alto costo cuya recolección, almacenamiento, procesamiento y transmisión exigen un largo periodo de tiempo y/o implican un alto costo de adquisición, etc.

c) **Actividades y procesos de negocio:** que tienen que ver con propiedad intelectual, los que si se degradan hacen imposible la ejecución de las tareas de la empresa, los necesarios para el cumplimiento legal o contractual,

B. De Soporte

a) **Hardware**: Consta de todos los elementos físicos que dan soporte a los procesos (PC, portátiles, servidores, impresoras, discos, documentos en papel)
b) **Software**: Consiste en todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos (sistemas operativos, paquetes de software o estándar, aplicaciones, mantenimiento o administración.)
c) **Redes**: Consiste en todos los dispositivos de telecomunicaciones utilizados para interconectar varios computadores remotos físicamente o los elementos de un sistema de información (conmutadores, cableado, puntos de acceso.)
d) **Personal**: Consiste en todos los grupos de personas involucradas en el sistema de información (usuarios, desarrolladores, responsables.)
e) **Sitio**: Comprende todos los lugares en los cuales se pueden aplicar los medios de seguridad de la organización (Edificios, salas, y sus servicios.)
f) **Estructura organizativa**: responsables, áreas, contratistas, entre otros.

Después de tener una relación con todos los activos se han de conocer las amenazas que pueden causar daños en la información, los procesos y los soportes. La identificación de las amenazas y la valoración de los daños que pueden producir se puede obtener preguntando a los propietarios de los activos, usuarios y expertos.

Posterior a la identificación del listado de activos, sus amenazas y las medidas que ya se han tomado, a continuación, se revisarán las vulnerabilidades que podrían aprovechar las amenazas y causar daños a los activos de información de La AGENCIA APP. Existen distintos métodos para analizar amenazas, por ejemplo:

- Entrevistas con líderes de procesos y usuarios
- Inspección física
- Uso de las herramientas para el escaneo automatizado y vulnerabilidades.

Para cada una de las amenazas analizaremos las vulnerabilidades (debilidades) que podrían ser explotadas.

Finalmente se identificarán las consecuencias, es decir, cómo estas amenazas y vulnerabilidades podrían afectar la confidencialidad, integridad y disponibilidad de los activos de información.

8.2.2 Estimación del riesgo

La estimación del riesgo busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo, su priorización y estrategia de tratamiento de estos. El objetivo de esta etapa es el de establecer una valoración y priorización de los riesgos.

Para adelantar la estimación del riesgo se deben considerar los siguientes aspectos:

- **Probabilidad**: La posibilidad de ocurrencia del riesgo, representa el número de veces que el riesgo se ha presentado en un determinado tiempo o pudiese presentarse.

- **Impacto**: Hace referencia a las consecuencias que puede ocasionar a la AGENCIA APP la materialización del riesgo; se refiere a la magnitud de sus efectos.

Se sugiere realizar este análisis con todas o las personas que más conozcan del proceso, y que por sus conocimientos o experiencia puedan determinar el impacto y la probabilidad del riesgo de acuerdo con los rangos señalados en las tablas que se muestran más adelante.

Como criterios para la estimación del riesgo desde el enfoque de impacto y consecuencias se podrán tener en cuenta: pérdidas financieras, costes de reparación o sustitución, interrupción del servicio, disminución del rendimiento, infracciones legales, pérdida de ventaja competitiva, daños personales, entre otros.

PROBABILIDAD			
Concepto	**Valor**	**Descripción**	**Frecuencia**
Raro	1	El evento puede ocurrir sólo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años
Improbable	2	Es muy poco factible que el evento se presente.	Al menos de 1 vez en Los últimos 5 años.
Posible	3	El evento podría ocurrir en algún momento.	Al menos de 1 vez en Los últimos 2 años.
Probable	4	El evento probablemente ocurrirá en la mayoría de las circunstancias,	Al menos de 1 vez en El último año.
Casi Certeza	5	Se espera que ocurra en la mayoría de las circunstancias	Más de 1 vez al año.

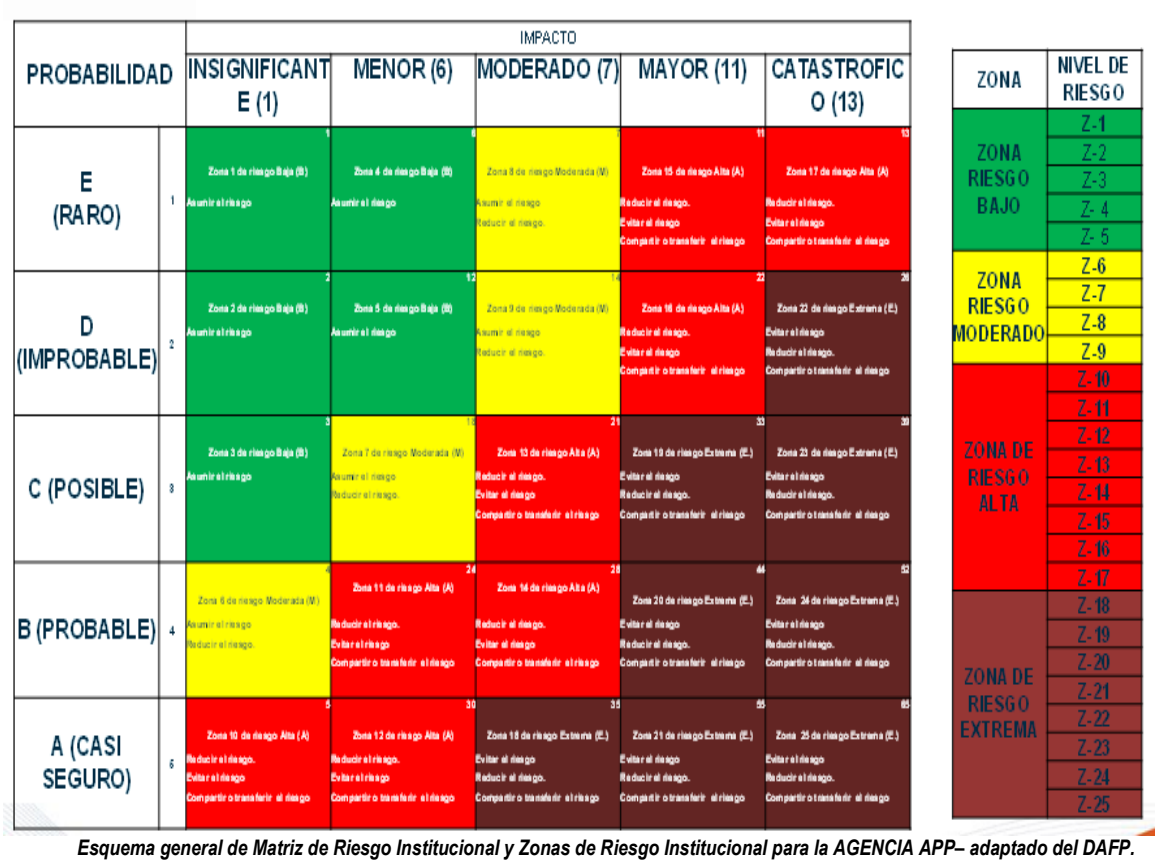
Adaptado para la AGENCIA APP de la Guía de Riesgos DAFP, 2020

Impacto		
Concepto	**Valor**	**Descripción**
Insignificante	1	La materialización del riesgo **puede ser controlado** por los participantes del proceso, y **no afecta los objetivos del proceso**.
Menor	6	La materialización del riesgo ocasiona **pequeñas demoras** en el cumplimiento de las actividades del proceso, y **no afecta significativamente el cumplimiento de los objetivos** de la AGENCIA APP. Tiene un impacto bajo en los procesos de otras áreas de la Agencia.
Moderado	7	La materialización del riesgo **demora el cumplimiento de los objetivos del proceso,** y tiene un **impacto moderado en los procesos de otras áreas** de la AGENCIA APP. Puede además causar un deterioro en el desarrollo del proceso dificultando o retrasando el cumplimiento de sus objetivos, impidiendo que éste se desarrolle en forma normal.
Mayor	11	La materialización del riesgo **retrasa el cumplimiento de los objetivos de la AGENCIA APP** y tiene un **impacto significativo en la imagen pública** de la Agencia y/o del Municipio.
Catastrófico	13	La materialización del riesgo **imposibilita el cumplimiento de los objetivos de la AGENCIA APP,** tiene un **impacto catastrófico en la imagen pública de la Agencia y/o del Municipio**

Adaptado para la AGENCIA APP de la Guía de Riesgos DAFP, 2020

8.2.3 Determinación del riesgo inherente y residual

El análisis del riesgo determinado por su probabilidad e impacto permite tener una primera evaluación del riesgo inherente (escenario sin controles) y ver el grado de exposición al riesgo que tiene la entidad. La exposición al riesgo es la ponderación de la probabilidad e impacto, y se puede ver gráficamente en la matriz de riesgo, instrumento que muestra las zonas de riesgos y que facilita el análisis gráfico. Permite analizar de manera global los riesgos que deben priorizarse según la zona en que quedan ubicados los mismos (zona de riesgo bajo, moderado, alto o extremo) facilitando la organización de prioridades para la decisión del tratamiento e implementación de planes de acción.



Esquema general de Matriz de Riesgo Institucional y Zonas de Riesgo Institucional para la AGENCIA APP– adaptado del DAFP.

Las zonas de riesgo se diferencian por colores y por número de la zona de la siguiente manera:

Zona de Riesgo
B: Zona de riesgo Baja (Color Verde): 5 zonas, siendo Z- 5 la zona de mayor riesgo.
M: Zona de riesgo Moderada (color Amarillo): 4 zonas, siendo Z- 9 la zona de mayor riesgo.
A: Zona de riesgo Alta (Color Rojo): 8 zonas, siendo Z- 17 la zona de mayor riesgo.
E: Zona de riesgo Extrema (Color Vino tinto): 8 zonas, siendo la Z-25 la de más alto riesgo.

8.2.4 Evaluación de los riesgos

Una vez se valoran los impactos, la probabilidad y las consecuencias de los escenarios de incidentes sobre los activos de información, se obtendrán los niveles de riesgo, para los cuales se deberán comparar frente a los criterios básicos del contexto, para una adecuada y pertinente toma de decisiones basada en riesgos de seguridad de la información y en beneficio de reducir su impacto a los procesos de la AGENCIA APP.

8.3 TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Como resultado de la etapa de evaluación del riesgo tendremos una lista ordenada de riesgos o una matriz con la identificación de los niveles de riesgo de acuerdo con la zona de ubicación, por tanto, se deberá elegir la(s) estrategia(s) de tratamiento del riesgo en virtud de su valoración y de los criterios establecidos en el contexto de gestión de riesgos.

De acuerdo con el nivel evaluación de los riesgos, se deberá seleccionar la opción de tratamiento adecuada por cada uno de los riesgos identificados; el costo/beneficio del tratamiento deberá ser un factor de decisión relevante para la decisión.

COSTO - BENEFICIO	OPCIÓN DE TRATAMIENTO
El nivel de riesgo está muy alejado del nivel de tolerancia, su costo y tiempo del tratamiento es muy superior a los beneficios	**Evitar** el riesgo, su propósito es no proceder con la actividad o la acción que da origen al riesgo (ejemplo, dejando de realizar una actividad, tomar otra alternativa, etc.)
El costo del tratamiento por parte de terceros (internos o externos) es más beneficioso que el tratamiento directo	**Transferir o compartir** el riesgo, entregando la gestión del riesgo a un tercero (ejemplo, contratando un seguro o subcontratando el servicio).
El costo y el tiempo del tratamiento es adecuado a los beneficios	**Reducir o Mitigar** el riesgo, seleccionando e implementando los controles o medidas adecuadas que logren que se reduzca la probabilidad o el impacto
La implementación de medidas de control adicionales no generará valor agregado para reducir niveles de ocurrencia o de impacto.	**Retener o aceptar** el riesgo, no se tomará la decisión de implementar medidas de control adicionales. Monitorizarlo para confirmar que no se incrementa

El resultado de esta fase se concreta en un plan de tratamiento de riesgos, es decir, la selección y justificación de una o varias opciones para cada riesgo identificado, que permitan establecer la relación de riesgos residuales, es decir, aquellos que aún siguen existiendo a pesar de las medidas tomadas.

Nota: Será conveniente que para la selección de los controles se consideren posibles restricciones o limitantes que impidan su elección tales como: restricciones de tiempo, financieras, técnicas, operativas, culturales, éticas, ambientales, legales, uso, de personal o las restricciones para la integración de controles nuevos y existentes.

8.4 MONITOREO Y SEGUIMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Periódicamente se revisará el valor de los activos, impactos, amenazas, vulnerabilidades y probabilidades en busca de posibles cambios, que exijan la valoración iterativa de los riesgos de seguridad de la información.

Los riesgos son dinámicos como la misma Entidad por tanto podrán cambiar de forma o manera radical sin previo aviso. Por ello es necesaria una supervisión continua que detecte: (1) nuevos activos o modificaciones en el valor de los activos, (2) nuevas amenazas, (3) cambios o aparición de nuevas vulnerabilidades, (4) aumento de las consecuencias o impactos, (5) incidentes de seguridad de la información.

Con el propósito de conocer los estados de cumplimiento de los objetivos de la gestión de los riesgos de seguridad de la información, se deberán definir esquemas de seguimiento y medición al sistema de gestión de riesgos de la seguridad de la información que permitan contextualizar una toma de decisiones de manera oportuna.