

# PLAN GENERAL PARA EL TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Medellín

2019



*Plan general para el tratamiento de riesgos de seguridad de la información*

1	Contenido	
2	INTRODUCCIÓN	3
3	OBJETIVO	3
4	ALCANCE	4
5	OBJETIVOS ESPECIFICOS	4
6	TERMINOS Y DEFINICIONES	4
7	VISION GENERAL DEL PROCESO DE GESTION DE RIESGO EN LA SEGURIDAD DE LA INFORMACION	8
7.1	ESTABLECIMIENTO DEL CONTEXTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	8
7.1.1	Criterios de evaluación del riesgo de seguridad de la información:	9
7.1.2	Criterios de Impacto	9
7.1.3	Criterios de Aceptación	10
7.2	VALORACIÓN DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	10
7.2.1	Identificación del riesgo	10
7.2.2	Estimación del riesgo	12
7.2.3	Determinación del riesgo inherente y residual	14
7.2.4	Evaluación de los riesgos	15
7.3	TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	15
7.4	MONITOREO Y SEGUIMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	16
7.5	CRONOGRAMA VALORACION DEL RIESGO	

*Plan general para el tratamiento de riesgos de seguridad de la información*

## 2 INTRODUCCIÓN

Hoy día, las entidades estatales o empresas privadas inmersas en la denominada revolución digital, reconocen el protagonismo de la información en sus procesos administrativos, misionales o tecnológicos por tanto la importancia de tener su información adecuadamente identificada y protegida, como también la que ingresa desde usuarios, beneficiarios, contratistas y demás público en general, enmarcada bajo las relaciones de cumplimientos contractuales como los son acuerdos de confidencialidad y demás compromisos, que obligan a dar un tratamiento, manejo y clasificación a la información bajo una correcta administración y custodia.

La Seguridad de la Información en las entidades públicas y privadas 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.

De acuerdo con lo anterior, la IU Digital decide crear un modelo de administración de los riesgos de seguridad de la información como medio o herramienta para el logro de los objetivos de mantener la información de la institución de forma confidencial, íntegra y disponible, a través de su ciclo de vida desde su captura, almacenamiento, explotación, hasta su eliminación.

Los principios de protección de la información se enmarcan en:

- **Confidencialidad:** Propiedad que la información sea concedida únicamente a quien esté autorizado.
- **Integridad:** Propiedad que la información se mantenga exacta y completa.
- **Disponibilidad:** propiedad que la información sea accesible y utilizable en el momento que se requiera.

## 3 OBJETIVO

Brindar a la IU Digital 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.

*Plan general para el tratamiento de riesgos de seguridad de la información*

## 4 ALCANCE

La gestión de riesgos de seguridad de la información y su tratamiento, podrá ser aplicada sobre cualquier proceso de la IU Digital, 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.

## 5 OBJETIVOS ESPECIFICOS

En beneficio del apoyo y cumplimiento de los propósitos de la política estratégica de seguridad de la información en la IU Digital, se declaran los siguientes objetivos específicos:

- Brindar lineamientos y principios para garantizar la unificación de criterios para la administración de los riesgos de seguridad de la información.
- Fortalecer el sistema de gestión de riesgos de la Institución incorporando controles y medidas de seguridad de la información que estén acordes al entorno operativo de la misma.
- Generar una cultura y apropiación de trabajo, enfocada a la identificación de los riesgos de seguridad de la información, y su mitigación.
- Minimizar el impacto bien en la información o cualquier otro activo de información asociado, a través de la gestión adecuada de los riesgos de la seguridad de la información.

## 6 TERMINOS Y 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 IU Digital.

**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

### *Plan general para el tratamiento de riesgos de seguridad de la información*

afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

**Acceso a la Información Pública** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

**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 institución.

**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 institución.

**Bases de Datos Personales:** Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581

de 2012, art 3).

**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 evalúa.

**Control:** Medida que modifica el riesgo.

**Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

**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.

*Plan general para el tratamiento de riesgos de seguridad de la información*

**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.

**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.

**Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

**Información Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

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

**Nivel de riesgo:** Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.

**Matriz de riesgos:** Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.

*Plan general para el tratamiento de riesgos de seguridad de la información*

**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 control o las diferentes auditorías de los sistemas integrados de gestión.

**Propietario del riesgo:** Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

**Proceso:** Conjunto de actividades interrelacionadas o que interactúan para transformar una entrada en salida.

**Riesgo Inherente:** Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

**Riesgo Residual:** El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.

**Riesgo:** Efecto de la incertidumbre sobre los objetivos.

**Riesgo en la seguridad de la información.** Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.

**Reducción del riesgo.** Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.

**Retención del riesgo.** Aceptación de la pérdida o ganancia proveniente de un riesgo particular

**Seguimiento:** Mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación de los controles de seguridad de la información sobre cada uno de los procesos.

**Tratamiento del Riesgo:** Proceso para modificar el riesgo” (Icontec Internacional, 2011).

**Valoración del Riesgo:** Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

**Vulnerabilidad:** Es aquella debilidad de un activo o grupo de activos de información

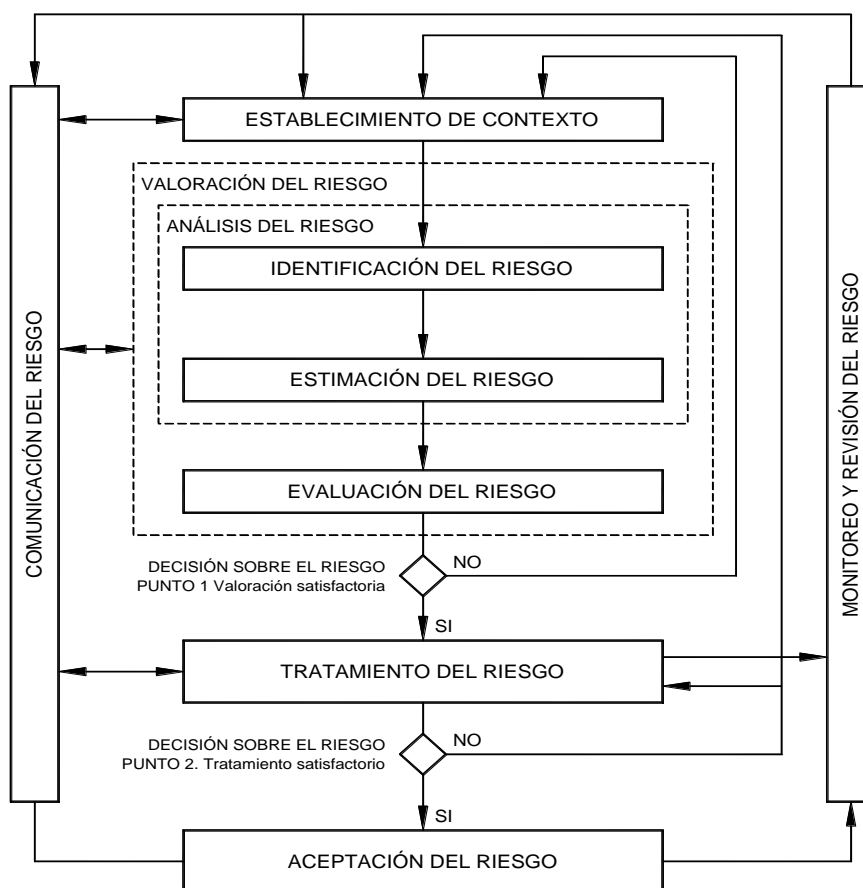
**Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información.

**SGSI:** Sistema de Gestión de Seguridad de la Información.

Plan general para el tratamiento de riesgos de seguridad de la información

## 7 VISION GENERAL DEL PROCESO DE GESTION DE RIESGO EN LA SEGURIDAD DE LA INFORMACION

A continuación, se presenta el modelo de gestión de riesgos de seguridad de la información apropiado por la IU digital, basado tanto en la norma ISO/IEC 31000 como en la ISO 27005 y los elementos que lo componen son:



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

### 7.1 ESTABLECIMIENTO DEL CONTEXTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN



### *Plan general para el tratamiento de riesgos de seguridad de la información*

El contexto de gestión de riesgos de seguridad de la información define los criterios básicos que serán necesarios para enfocar el ejercicio por parte de la IU Digital y obtener los resultados esperados, basándose en, la identificación de las fuentes que pueden dar origen a los riesgos y oportunidades en los procesos de la IU Digital, en el análisis de las debilidades y amenazas asociadas, en la valoración de los riesgos en términos de sus consecuencias para la Entidad y en la probabilidad de su ocurrencia, al igual que en la construcción de acciones de mitigación en beneficio de lograr y mantener niveles de riesgos aceptables para la Entidad.

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

#### **7.1.1 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 gestión de información definido por la IU Digital.
- La criticidad de los activos de información involucrados.
- Los requisitos legales y reglamentarios, así como las obligaciones contractuales.

#### **7.1.2 Criterios de Impacto**

Los criterios de impacto se especificarán en términos del grado, daño o de los costos para la IU Digital, 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 de valor financiero
- Daños en la reputación
- Incumplimiento de los requisitos legales, reglamentarios o contractuales

*Plan general para el tratamiento de riesgos de seguridad de la información*

### 7.1.3 Criterios de Aceptación

Los criterios de aceptación dependerán con frecuencia de las políticas, metas, objetivos de la IU Digital.

## 7.2 VALORACIÓN DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Los riesgos se deberán identificar, describir cuantitativa o cualitativamente y priorizarse frente a los criterios de evaluación del riesgo y los objetivos relevantes para la IU Digital, esta fase consta de las siguientes etapas:

La IU Digital, definir la valoración del Riesgo de seguridad de la información a través de las siguientes actividades:

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

### 7.2.1 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 de la Institución:** procesos cuya pérdida o degradación hacen imposible llevar a cabo la misión de la institución; procesos que contienen procesos secretos o que implican tecnología propietaria; procesos que, si se modifican, pueden afectar

*Plan general para el tratamiento de riesgos de seguridad de la información*

de manera muy significativa el cumplimiento de la misión de la institución; 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, etc.

**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, etc.).
- 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, etc.)
- 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, etc.)
- d. **Personal:** Consiste en todos los grupos de personas involucradas en el sistema de información (usuarios, desarrolladores, responsables, etc.)
- e. **Sitio:** Comprende todos los lugares en los cuales se pueden aplicar los medios de seguridad de la organización (Edificios, salas, y sus servicios, etc.)
- f. **Estructura organizativa:** responsables, áreas, contratistas, etc.

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, expertos, etc.

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 IU Digital. Existen distintos métodos para analizar amenazas, por ejemplo:

### Plan general para el tratamiento de riesgos de seguridad de la información

- Entrevistas con líderes de procesos
- Inspección física
- Uso de las herramientas para el escaneo automatizado

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.

## 7.2.2 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 IU Digital la materialización del riesgo; se refiere a la magnitud de sus efectos.

La IU Digital, desarrolla este proceso con el personal que tiene mayor conocimiento, 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.

Además de medir las posibles consecuencias se deberán analizar o estimar la probabilidad de ocurrencia de situaciones que generen impactos sobre los activos de información.

### Formulario para el registro de la estimación de los riesgos de seguridad de la información:

Para realizar el análisis de riesgo de un proceso, se ha definido un formato de calificación del riesgo en el cual personas del equipo deberán calificar el impacto y la probabilidad de cada uno de los riesgos identificados de acuerdo con los niveles para la estimación de los riesgos.

*Plan general para el tratamiento de riesgos de seguridad de la información*

PROBABILIDAD			
Concepto	Valor	Descripción	Frecuencia
Raro	1	El evento puede ocurrir sólo en circunstancias excepcionales.	No se ha presentado en los últimos 3 años
Improbable	2	Es muy poco factible que el evento se presente.	Al menos de 1 vez en Los últimos 3 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.

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 IU Digital. Tiene un impacto bajo en los procesos de otras áreas de la IU Digital.
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 IU Digital. 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 IU Digital y tiene un impacto significativo en la imagen pública de la institución y/o del Departamento. Puede además generar impactos en: la industria; sectores económicos, el cumplimiento de acuerdos y obligaciones legales nacionales e internacionales; multas y las finanzas públicas; entre otras
Catastrófico	13	La materialización del riesgo imposibilita el cumplimiento de los objetivos de la IU Digital, tiene un impacto catastrófico en la imagen pública de la IU Digital y/o del Departamento. Puede además generar impactos en: sectores económicos, los



Plan general para el tratamiento de riesgos de seguridad de la información

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.

### 7.2.4 Evaluación de los riesgos

Una vez valorados 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 la Alta Entidad.

## 7.3 TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Como resultado de la etapa de evaluación del riesgo se cuenta con 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	OPCION 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	<b>Evitar</b> 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	<b>Transferir o compartir</b> 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	<b>Reducir o Mitigar</b> el riesgo, seleccionando e implementando los controles o medidas adecuadas que logren que se reduzca la probabilidad o el impacto

*Plan general para el tratamiento de riesgos de seguridad de la información*

<p>La implementación de medidas de control adicionales no generará valor agregado para reducir niveles de ocurrencia o de impacto.</p>	<p><b>Retener o aceptar</b> el riesgo, no se tomará la decisión de implementar medidas de control adicionales. Monitorizarlo para confirmar que no se incrementa</p>
--	--

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.

## 7.4 MONITOREO Y SEGUIMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Periódicamente la Institución 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 Institución 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.



*Plan general para el tratamiento de riesgos de seguridad de la información*

## 7.5 CRONOGRAMA VALORACION DE RIESGOS DE SEGURIDAD DE LA INFORMACION

La IU Digital definirá y mantendrá un cronograma de actividades para la realización de la valoración de los riesgos de seguridad de la información en los procesos de la organización, basado con su criticidad y su valor para el cumplimiento de la misionalidad de la institución.

<b>Proyectó</b>	<b>Revisó</b>	<b>Aprobó</b>
Juan Antonio Campo Herrera Profesional Universitario	Olga Constanza Bermúdez Jaimes Directora de Tecnología	Comité de gestión y desempeño Aprobado según Acta No 01 Enero 30 de 2019

# IU Digital de Antioquia

[www.iudigital.edu.co](http://www.iudigital.edu.co)

Esta licencia permite a otros distribuir, remezclar, retocar, y crear a partir de esta obra de manera no comercial y, a pesar que sus nuevas obras deben siempre mencionar a la IU Digital y mantenerse sin fines comerciales, no están obligados a licenciar obras derivadas bajo las mismas condiciones.

