# CORPORACIÓN AUTÓNOMA REGIONAL DEL VALLE DEL CAUCA - CVC

# MANUAL METODOLOGÍA GESTIÓN DE RIESGO SEGURIDAD DE LA INFORMACIÓN

**Santiago de Cali, marzo de 2020**

# MANUAL GESTIÓN DE RIESGO SEGURIDAD DE LA INFORMACIÓN

## TABLA DE CONTENIDO

## 1. OBJETIVO

Proporcionar directrices para la valoración y el tratamiento de los riesgos de seguridad de la información de la Corporación Autónoma Regional del Valle del Cauca, en adelante CVC, que permitan reducir el riesgo hasta un nivel aceptable y garantizar el cumplimiento y la eficacia del Sistema de Gestión de Seguridad de la Información.

## 2. ALCANCE

Teniendo como base las normas NTC-ISO/IEC 27005:2009 y NTC-ISO 31000:2011, el proceso de gestión del riesgo en la seguridad de la información de la CVC incluye las siguientes etapas:

- Establecimiento del contexto
- Valoración del riesgo (análisis y evaluación del riesgo)
- Tratamiento del riesgo
- Aceptación del riesgo
- Comunicación del riesgo
- Monitoreo y revisión del riesgo

El proceso de gestión del riesgo se llevará a cabo teniendo en cuenta el alcance definido para el SGSI, el cual puede ser consultado en el manual del SGSI.

## 3. DEFINICIONES

Los términos y las definiciones para la gestión de riesgos de seguridad de la información se referencian en la norma técnica colombiana NTC-ISO/IEC 27005:2009, adicionalmente se describen en forma general los siguientes conceptos:

**Aceptación del riesgo:** Decisión informada de asumir un riesgo concreto.

**Activo de información:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, entre otros) que tenga valor para la CVC.

**Amenaza:** Una causa potencial de un incidente no deseado, el cual puede resultar en daño a un sistema u organización.

**Análisis 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 y las acciones que se van a implementar.

**Comunicación del riesgo:** Comunicar o intercambiar la información acerca del riesgo entre la persona que toma la decisión y otras partes interesadas.

**Confidencialidad:** La propiedad que esa información esté disponible y no sea divulgada a entidades, personas o procesos no autorizados.

**Control:** 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. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

**Disponibilidad:** La propiedad de estar disponible o utilizable cuando se requiera para personal autorizado.

**Establecimiento del contexto:** Al establecer el contexto, La CVC articula sus objetivos estratégicos y de calidad, define los parámetros externos e internos que se van a considerar en la gestión de riesgos y establece el alcance y los criterios de riesgo.

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

**Evaluación del riesgo:** Proceso usado para determinar las prioridades de gestión del riesgo mediante la comparación de los resultados de la calificación y el grado de exposición al riesgo.

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

**Gestión del riesgo:** Actividades coordinadas para dirigir y controlar una organización con relación al riesgo.

**Identificación del riesgo:** Proceso para encontrar, numerar y caracterizar los elementos del riesgo.

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

**Integridad:** La propiedad de salvaguardar la integridad y exactitud de los activos.

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

**Probabilidad:** Frecuencia o factibilidad de ocurrencia del riesgo.

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

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

**Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

**Riesgo de 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.

**Riesgo residual:** El riesgo remanente después del tratamiento del riesgo.

**Transferencia del riesgo:** Compartir con otra de las partes la ganancia o pérdida de un riesgo.

**Valor del Activo:** Está determinado por el valor de la confidencialidad, integridad y disponibilidad del activo de información.

**Valor del Impacto:** Está determinado por el responsable del activo de información, quién provee cuanto se vería afectado por incidentes de los activos a cargo.

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

## 4. DESARROLLO

La información, en buena parte como cualquier otro activo de la CVC, ha de gestionarse y protegerse estratégicamente. Es imprescindible entonces que los directivos comprendan el

valor de la información contenida en los procesos que lideran y que dispongan de un marco para la evaluación y la ejecución de las medidas o controles de seguridad de la información.

Para el logro de este objetivo, se ha definido la metodología que a continuación se describe, basada en las normas NTC-ISO/IEC 27005:2009 y NTC-ISO 31000:2011. El proceso de Gestión de Riesgos en la Seguridad de la Información de la CVC consta entonces del establecimiento del contexto, valoración del riesgo, tratamiento del riesgo, aceptación del riesgo, comunicación del riesgo, y monitoreo y revisión del riesgo.

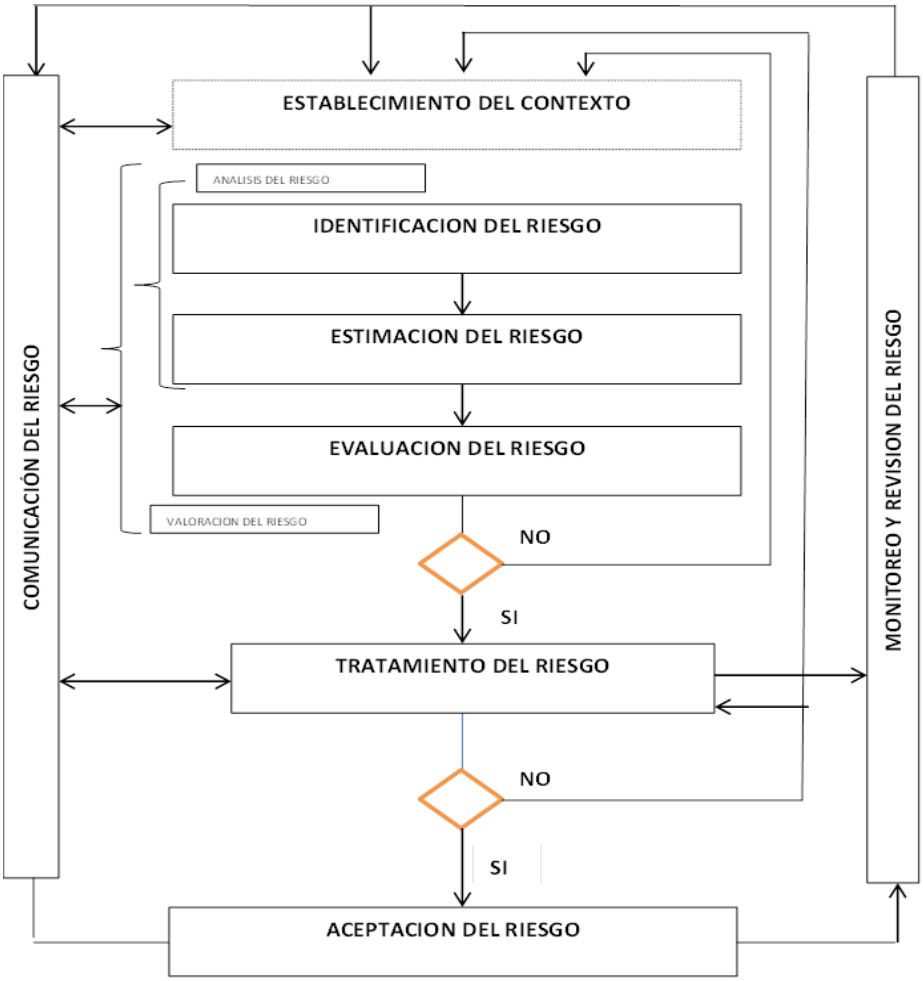


***Figura 1.*** *Proceso de gestión del riesgo en la seguridad de la información.*[1]

[1] NTC-ISO/IEC 27005:2009, NTC-ISO 31000:2011

### 4.1. ESTABLECIMIENTO DEL CONTEXTO

El objetivo de esta etapa es conocer a la organización para determinar lo que puede afectarla a nivel interno y externo, qué requiere proteger y de acuerdo con los recursos actuales, cómo podría darse esa protección, para establecer el nivel de aceptación de riesgo al cual están dispuestos, y para determinar los alcances y limitaciones existentes.

Para el establecimiento del contexto, la CVC identifica y revisa las condiciones internas y externas del entorno que pueden generar eventos que afecten su capacidad para lograr los resultados previstos de su sistema de gestión de seguridad de la información. Como resultado se definen el alcance y los límites, los criterios básicos y los recursos y organización necesarios para la gestión de riesgos en la seguridad de la información.

Como fuentes de información se emplea la documentación existente relacionada con calidad, seguridad, planeación estratégica y continuidad las cuales brindan información que permite posicionar a la CVC con respecto a su medio; de igual forma se utilizan entrevistas con altos mandos, encuestas con el personal, visitas a instalaciones y las demás que se consideren necesarias.

Se establecen los criterios de valoración de activos de información, probabilidad de ocurrencia, impacto, evaluación de riesgo, tratamiento del riesgo y aceptación del riesgo teniendo en cuenta los siguientes aspectos:

#### 4.1.1. Criterios de probabilidad de ocurrencia

Se estima la probabilidad de ocurrencia de un riesgo sobre uno o varios activos de información debido a la explotación de amenazas por una o más vulnerabilidades (causantes de riesgo).

Se tiene en cuenta los siguientes aspectos para calificar la probabilidad de ocurrencia:

- Evaluación de riesgos.
- Cambios en la tecnología.
- Vulnerabilidades de día cero.
- Personas.
- Implementación de controles.
- No conformidades.

- Tiempos de respuesta.
- Criticidad de los activos de información.

### 4.1.2. Criterios del impacto

Los criterios de impacto del riesgo, en términos del grado de daño o de costos, causados por un evento de seguridad de la información, considera los siguientes aspectos:

- Incumplimiento de los requisitos legales, reglamentarios o contractuales.
- Impactos organizacionales definidos.
- Pérdida del negocio y del valor económico.
- Nivel de clasificación de los activos de información impactados.
- Brechas de seguridad de la información (por ejemplo, pérdida de confidencialidad, integridad y disponibilidad).
- Operaciones deterioradas (partes internas o terceras partes).
- Alteración de planes y fechas límites.
- Daños para la reputación.

### 4.1.3. Criterios de evaluación de riesgos

Los criterios de evaluación de riesgos tienen en cuenta los siguientes aspectos:

- Criticidad de los activos involucrados.
- Expectativas y percepciones de las partes interesadas.
- Requisitos legales y reglamentarios.
- La importancia de la disponibilidad, confidencialidad e integridad para las operaciones y el negocio.

### 4.1.4. Criterios de tratamiento del riesgo

Los valores de riesgo tratables definidos por la CVC se establecen en los siguientes rangos cualitativos y cuantitativos:

- **INACEPTABLE (176 – 279)**
- **INADMISIBLE (280 – 375)**

Los rangos seleccionados se consideran como tratables ya que de materializarse un riesgo generan graves consecuencias en la CVC.

#### 4.1.5. Criterios de aceptación del riesgo

Los criterios de aceptación del riesgo se pueden expresar como la relación entre el beneficio estimado (u otros beneficios del negocio) y el riesgo estimado.

Los valores de riesgo aceptables para la CVC se establecen en los siguientes rangos cualitativos y cuantitativos:

- **ADMISIBLE (3 – 43)**
- **ACEPTABLE (44 – 104)**
- **TOLERABLE (105 – 175)**

Los rangos seleccionados se consideran como valores de riesgo aceptables debido a que si se materializan en la CVC no tienen consecuencias críticas o pueden ser controladas.

Los criterios del contexto establecido se registran en la Matriz de gestión de riesgos de seguridad de la información.

### 4.2. VALORACIÓN DEL RIESGO

La valoración del riesgo describe cualitativa y cuantitativamente el riesgo y permite a los líderes de procesos priorizar los riesgos de acuerdo con la gravedad percibida u otros criterios establecidos.

La valoración del riesgo determina el valor de los activos de información, identifica los causales de riesgo que existen (o que podrían existir), identifica el impacto en los riesgos identificados, determina las consecuencias potenciales, y finalmente prioriza los riesgos derivados y los clasifica frente a los criterios de evaluación del riesgo determinados en el contexto establecido.

La valoración del riesgo es el proceso total de análisis y evaluación del riesgo.

En la CVC se ha establecido un enfoque de valoración cualitativa a Alto Nivel de riesgos en seguridad de la información, basados en la norma NTC-ISO/IEC 27005:2009 y NTC-ISO 31001:2011. Las características principales de este enfoque son:

- Aborda una visión global de la organización y su sistema de información, de modo que se puedan atender los riesgos más críticos a través del proceso de tratamiento de los riesgos.
- Aborda diferentes causales de riesgos identificando posibles amenazas y vulnerabilidades que permiten su consulta y adaptación a las necesidades reales y específicas de la empresa.

- Los controles que se establecen a partir de la valoración del riesgo son manejados de manera organizacional de tal manera que permitan la adaptabilidad a las necesidades de la empresa.

Las ventajas de este enfoque a Alto nivel son:

- La incorporación de un enfoque inicial sencillo que facilita la aceptación y manejo para todos los involucrados.

- Ayuda a la construcción de un panorama estratégico.

- Los recursos se aplican donde son de más beneficio y se tratan primero los sistemas que tengan mayor necesidad de protección.

El proceso utilizado para la valoración de los riesgos en la CVC comprende las siguientes etapas:

### 4.2.1. Análisis del riesgo

Esta etapa 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 y las acciones que se van a implementar, lo cual comprende los siguientes aspectos:

#### 4.2.1.1. Identificación del riesgo

Es el proceso para encontrar, numerar y caracterizar los elementos del riesgo. El propósito de la identificación del riesgo es determinar qué podría suceder que cause una pérdida potencial y llegar a comprender el cómo, dónde y por qué podría ocurrir esta

pérdida. Para llevar a cabo esta actividad es importante contar con la información que se relaciona a continuación:

#### 4.2.1.1.1. Identificación de los activos de información

Teniendo claro cuál es el alcance y los límites de la gestión de riesgos, se identifican los activos de información teniendo claro que un activo es todo aquello que tiene valor para la CVC. Estos activos se listan incluyendo:

- Nombre del activo
- Tipo de activo de información
- Cargo responsable
- Custodio
- Medio de almacenamiento
- Ubicación
- Estado del activo
- Propiedades del activo de información: confidencialidad, integridad, disponibilidad
- Valor del activo

Los tipos de activos de información se definen en la CVC de la siguiente manera:

- **Software:** Software de aplicación, software del sistema, herramientas de desarrollo y utilidades.

- **Hardware:** Equipo de tratamiento (procesadores, monitores, portátiles, módems), equipo de comunicaciones (routers, centrales digitales, máquinas de fax), medios magnéticos (discos y cintas), medios removibles y otro equipo técnico (suministro de energía, unidades de aire acondicionado).

- **Información pura:** Información almacenada física o digitalmente como bases de datos y archivos de datos, contratos, acuerdos, documentación del sistema, información sobre investigación, manuales de usuario, registros de auditoria, procedimientos, instructivos, planes de continuidad, actas, hojas de vida, información archivada.

- **Intangibles:** Reputación, imagen.

- **Conocimiento:** Personas y sus calificaciones, habilidades y experiencia.

- **Servicios de computación y comunicaciones**, tales como Internet, correo electrónico, páginas de consulta, directorios compartidos e Intranet, entre otros. También servicios de mantenimiento.

#### 4.2.1.1.2. Valoración del activo de información

Para determinar el valor del activo se analiza en primera instancia la pérdida de las propiedades de confidencialidad, de integridad y de disponibilidad para cada uno de los activos de información, teniendo en cuenta los criterios descritos en la siguiente figura:

| VALOR | NIVEL | CONFIDENCIALIDAD | INTEGRIDAD | DISPONIBILIDAD |
|---|---|---|---|---|
| 1 | MUY BAJA | El acceso no autorizado al activo de información y a la información que este gestiona no genera ningún impacto negativo en el proceso evaluado. | La pérdida de la exactitud y el estado completo del activo de información y la información que este gestiona no genera impacto negativo en el proceso evaluado. | La ausencia del activo de información y la información que este gestiona no genera ningún impacto negativo en el proceso evaluado. |
| 2 | BAJA | El acceso no autorizado al activo de información y a la información que este gestiona impacta negativamente de manera leve al proceso evaluado. | La pérdida de la exactitud y el estado completo del activo de información y la información que este gestiona impacta negativamente de manera leve al proceso evaluado. | La ausencia del activo de información y la información que este gestiona impacta negativamente de manera leve al proceso evaluado. |
| 3 | MEDIA | El acceso no autorizado al activo de información y a la información que este gestiona impacta negativamente al proceso evaluado. | La pérdida de la exactitud y el estado completo del activo de información y la información que este gestiona impacta negativamente al proceso evaluado. | La ausencia del activo de información y la información que este gestiona impacta negativamente al proceso evaluado. |
| 4 | ALTA | El acceso no autorizado al activo de información y a la información que este gestiona impacta negativamente a la Organización. | La pérdida de la exactitud y el estado completo del activo de información y la información que este gestiona impacta negativamente a la Organización. | La ausencia del activo de información y la información que este gestiona impacta negativamente a la Organización. |
| 5 | MUY ALTA | El acceso no autorizado al activo de información y a la información que este gestiona impacta negativamente a la Organización y a terceros asociados. | La pérdida de la exactitud y el estado completo del activo de información y la información que este gestiona impacta negativamente a la Organización y a terceros asociados. | La ausencia del activo de información y la información que este gestiona impacta negativamente a la Organización y a terceros asociados. |

***Figura 2.*** *Valor del activo de información.*

El valor del activo de información (VA) está determinado entonces por la sumatoria obtenida de las variables de Confidencialidad (C), Integridad (I) y Disponibilidad (D) para dicho activo.

Así entonces, VA = C + I + D

Esta valoración del activo hace parte de la etapa de estimación del riesgo donde se definen los rangos de valores cualitativos y cuantitativos.

#### 4.2.1.1.3. Identificación de vulnerabilidades y amenazas (causas de riesgo)

Se realiza la identificación de las vulnerabilidades y amenazas de los activos de información que como resultado de la valoración haya resultado MEDIA, ALTA O MUY ALTA. A continuación, se detalla una descripción general de los conceptos y las responsabilidades:

- Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas. Algunas amenazas pueden afectar a más de un activo, en tales casos puede causar diferentes impactos dependiendo de los activos que se vean afectados.

- Es responsabilidad de los líderes de procesos realizar la identificación de las amenazas.

- Se deben identificar las vulnerabilidades que pueden ser explotadas por las amenazas para causar daños a los activos de información o a la CVC. Es importante anotar que un control implementado de manera incorrecta o que funcione mal, o un control que se utiliza de modo incorrecto podrían por sí solos constituir una vulnerabilidad.

- Es responsabilidad de los líderes de proceso realizar la identificación de las vulnerabilidades.

#### 4.2.1.1.4. Identificación de riesgos en la Corporación

Este proceso consiste en la identificación del riesgo a raíz de las amenazas y vulnerabilidades asociadas. Se realiza una descripción puntual del riesgo asociado a los activos de información.

Existe una base estándar de riesgos como se especifica en la siguiente figura, pero queda abierto para la inserción de nuevos riesgos.

| TABLA DE RIESGOS |
|---|
| Alteración de la información |
| Averías en los equipos |
| Denegación del servicio |
| Desgaste del equipo |
| Desgaste de la infraestructura o red |
| Fuga de información |
| Perdida parcial/total de equipo |
| Perdida total de información |
| Propagación de los impactos |
| Sanciones |
| Incumplimientos legales |
| Incumplimientos financieros |
| No disponibilidad de la información |
| No disponibilidad del servicio |
| Adquisición de virus informático |
| Acceso no autorizado |

***Figura 3.*** *Tabla básica de riesgos.*

#### 4.2.1.1.5. Identificación del tipo de riesgo

Se realiza la tipificación del riesgo identificado según los siguientes criterios:

- Lógico
- Físico
- Locativo
- Legal
- Reputacional
- Financiero

#### 4.2.1.1.6. Identificación del dueño del riesgo

Se realiza la identificación del proceso dueño del riesgo para la definición de responsabilidades y planes de mitigación.

#### 4.2.1.1.7. Identificación de propiedades de la información asociadas al riesgo

Se realiza la identificación de las propiedades de la información que son afectadas por el riesgo. Estas propiedades son confidencialidad, integridad y disponibilidad.

#### 4.2.1.1.8. Identificación tipo de impacto

Se definen los siguientes tipos de impactos de acuerdo con los requerimientos de la CVC:

- Imagen
- Legal
- Continuidad operativa
- Financiero

Los tipos de impactos están relacionados directamente con los tipos de riesgo identificados en el numeral 4.2.1.1.5. Esto permite que basado en el tipo de riesgo identificado se realice una asociación al tipo de impacto que este riesgo genera y se pueda realizar su calificación. Esta relación se evidencia a continuación:

| TIPO DE RIESGO | TIPO DE IMPACTO |
|---|---|
| Lógico | Continuidad Operativa |
| Físico | |
| Locativo | |
| Legal | Legal |
| Reputacional | Imagen |
| Financiero | Financiero |

***Tabla 1.*** *Relación tipo de riesgos – tipo de impactos.*

### 4.2.1.2. Estimación del riesgo

El propósito de la estimación del riesgo es determinar los valores cuantitativos y cualitativos del impacto y la probabilidad de ocurrencia del riesgo. Los rangos y los valores cualitativos son establecidos por la CVC de acuerdo con sus necesidades.

Se realizan las siguientes estimaciones para el riesgo:

- **Estimación de riesgo inherente:** Se evalúa el valor del impacto y la probabilidad de ocurrencia del riesgo inherente, es decir, sin tener en cuenta los controles existentes para el tratamiento del riesgo. El resultado es el nivel del riesgo inherente al que está expuesto la CVC.

- **Identificación de controles:** Se realiza la identificación de los controles implementados en la CVC para tratar los riesgos. Puede que no existan controles para el tratamiento del riesgo, esto afectará el resultado del riesgo residual e indicará, según los niveles de probabilidad de ocurrencia e impacto, que deberán tener un tratamiento mediante la implementación de controles. La identificación de los controles permite hacer un seguimiento a la eficacia de las implementaciones y poder así realizar ciclos de mejora continua a los mismos.

- **Estimación de riesgo residual:** Se evalúa el valor del impacto y la probabilidad de ocurrencia del riesgo residual, es decir, se tienen en cuenta los controles existentes en la CVC para el tratamiento de los riesgos identificados. El resultado es el nivel de riesgo residual controlado mediante salvaguardas.

Para esto se realizan las siguientes etapas:

#### 4.2.1.2.1. Valoración del impacto

El impacto se determina teniendo en cuenta los criterios de impacto definidos en el análisis del contexto numeral 4.1, y según se identifica en la siguiente figura:

| NIVEL | VALOR | FINANCIERO | CONTINUIDAD OPERATIVA |
|---|---|---|---|
| | | La pérdida de ingresos directa y los costos u otros gastos financieros indirectos que se generarían para la Organización. | Tiempo en que se ve afectada la operación de los procesos de la Organización. |
| **Insignificante** | **1** | Si el hecho llegara a presentarse, la Organización no tendría consecuencias económicas que impacten el funcionamiento, por tanto se asumirán las perdidas. | Si el hecho llegara a presentarse, el proceso de la Organización no se vería afectado en su continuidad. |
| **Menor** | **2** | Si el hecho llegara a presentarse, la Organización tendría bajas consecuencias económicas. | Si el hecho llegara a presentarse, el proceso de la Organización se vería afectado en su continuidad de manera mínima. |
| **Moderado** | **3** | Si el hecho llegara a presentarse, la Organización tendría medianas consecuencias económicas. | Si el hecho llegara a presentarse, el proceso de la Organización se vería afectado en su continuidad de manera moderada. |
| **Mayor** | **4** | Si el hecho llegara a presentarse, la Organización tendría altas consecuencias económicas. | Si el hecho llegara a presentarse, el proceso de la Organización se vería afectado en su continuidad de manera considerable interrumpiendo periódicamente el proceso y otros. |
| **Catastrófico** | **5** | Si el hecho llegara a presentarse, la Organización tendría nefastas consecuencias económicas. | Si el hecho llegara a presentarse, el proceso de la Organización se vería afectado en su continuidad de manera total. |

| NIVEL | VALOR | IMAGEN | LEGAL |
|---|---|---|---|
| | | Afectación sobre la imagen y reputación de la Organización. | Emisión de resoluciones administrativas y/o judiciales por el incumplimiento de normas, regulaciones u obligaciones. |
| **Insignificante** | **1** | Si el hecho llegara a presentarse, tendría consecuencias o efectos sobre un grupo de funcionarios de manera interna. | Si el hecho llegara a presentarse, la organización tendría multas. |
| **Menor** | **2** | Si el hecho llegara a presentarse, tendría un impacto leve en la Organización que seria reparable a corto plazo | Si el hecho llegara a presentarse, la organización tendría demandas. |
| **Moderado** | **3** | Si el hecho llegara a presentarse, tendría un impacto medio en la Organización de manera local. | Si el hecho llegara a presentarse, la organización tendría una investigación disciplinaria. |
| **Mayor** | **4** | Si el hecho llegara a presentarse, tendría un impacto alto en la Organización a nivel gremial. | Si el hecho llegara a presentarse, la organización tendría una investigación fiscal. |
| **Catastrófico** | **5** | Si el hecho llegara a presentarse, tendría un impacto catastrófico en la Organización a nivel nacional/ internacional. | Si el hecho llegara a presentarse, la organización tendría sanciones legales. Podría generar el cierre definitivo de la Organización. |

***Figura 4.*** *Valor del impacto.*

Es responsabilidad de los líderes de procesos realizar la identificación de las consecuencias y nivel de impacto que puede tener la pérdida de confidencialidad, integridad y disponibilidad de los activos de información.

#### 4.2.1.2.2. Nivel de probabilidad del riesgo

Se realiza la selección de probabilidad de ocurrencia del riesgo. Se definen los valores en la siguiente figura:

| NIVEL DE PROBABILIDAD | | DESCRIPCIÓN |
|---|---|---|
| 1 | Raro | El riesgo ocurre rara vez en la Organización. |
| 2 | Improbable | El riesgo ocurre en ocasiones especificas en la Organización. |
| 3 | Posible | El riesgo ocurre con cierta periodicidad en la Organización. |
| 4 | Probable | El riesgo ocurre frecuentemente en la Organización. |
| 5 | Casi Seguro | El riesgo ocurre inminentemente en la Organización. |

***Figura 5.*** *Nivel de probabilidad del riesgo.*

### 4.2.2. Evaluación del riesgo

Para el cálculo del valor del riesgo se considera la siguiente ecuación:

**VALOR DEL RIESGO = VA (C, I, D) * Valor Impacto * P(r)**

En donde:

**VA (C, I, D):** Valor del activo de información determinado por la suma de los valores de Confidencialidad, Integridad y Disponibilidad.

**Valor del Impacto (I):** Nivel de impacto que tendría la manifestación de un riesgo sobre los activos de información. Está determinado por el responsable del activo de información o el dueño de los riesgos del proceso.

**P(r):** Es la probabilidad de ocurrencia del riesgo identificado, determinada por el responsable del activo de información o el dueño de los riesgos del proceso.

Como salida de este cálculo se obtiene un valor que determina, según el rango de valores en que se encuentre, el nivel de tolerancia y el tratamiento que se le debe dar a los riesgos identificados, de acuerdo con lo definido en la figura 6.

| Límite Inferior | Límite Superior | NIVELES DE RIESGO | RESPUESTA A LOS RIESGOS | DESCRIPCIÓN |
|---|---|---|---|---|
| 3 | 43 | **Admisible** | **Asumir el riesgo** | El nivel de riesgo es Admisible y se encuentra controlado en la Organización. Los riesgos en este nivel se deben revisar periódicamente. |
| 44 | 104 | **Aceptable** | **Asumir el riesgo** | El nivel de riesgo es Aceptable y se encuentra controlado en la Organización. Los riesgos en este nivel se deben revisar periódicamente. |
| 105 | 175 | **Tolerable** | **Asumir el riesgo** | El nivel de riesgo es Tolerable de acuerdo a los criterios de aceptación de la Organización. Los riesgos en este nivel deben ser monitoreados para identificar oportunamente los cambios en su valoración. |
| 176 | 279 | **Inaceptable** | **Mitigar el riesgo, Evitar, Compartir** | El nivel del riesgo es Inaceptable, por lo que es necesario implementar controles en la Organización para mitigar, evitar o compartir el riesgo y llevar a niveles aceptables. |
| 280 | 375 | **Inadmisible** | **Mitigar el riesgo, Evitar, Compartir** | El nivel del riesgo es Inadmisible, por lo que es necesario implementar controles en la Organización para mitigar, evitar o compartir el riesgo y llevar a niveles aceptables. |

***Figura 6.*** *Valoración del riesgo.*

Se aceptarán los riesgos cuyo resultado después de la evaluación sea "ADMISIBLE", “ACEPTABLE” o "TOLERABLE" (4.1.5 Criterios de aceptación del riesgo).

La salida de este proceso será una lista de riesgos priorizados acorde con los criterios de valoración del riesgo.

Los rangos elegidos para el nivel de riesgo final son determinados conforme a la probabilidad de ocurrencia o frecuencia de los posibles resultados de **VA*I*P(r)**.

### 4.3. TRATAMIENTO DEL RIESGO

Los criterios de tratamiento de riesgos de seguridad de la información definidos por la OTI para la CVC son:

- INACEPTABLE (176 – 279)
- INADMISIBLE (280 – 375)

En esta etapa se seleccionan los controles a aplicar. Las opciones para el tratamiento de los riesgos después de su evaluación son:

- **Reducir el riesgo** mediante la aplicación de controles apropiados de manera que el riesgo residual se pueda reevaluar como aceptable.

- **Asumir el riesgo (Retención)** con el conocimiento y objetividad, siempre que cumplan con la política de seguridad previamente establecida por la CVC.

- **Evitar el riesgo,** la acción que da origen al riesgo particular.

- **Compartir o transferir el riesgo** a entidades como aseguradoras o proveedores que puedan gestionar de manera eficaz el riesgo particular, siempre que no resulte un costo superior al del riesgo mismo.

La siguiente figura ilustra la actividad de tratamiento del riesgo dentro de los procesos de gestión del riesgo en la seguridad de la información:

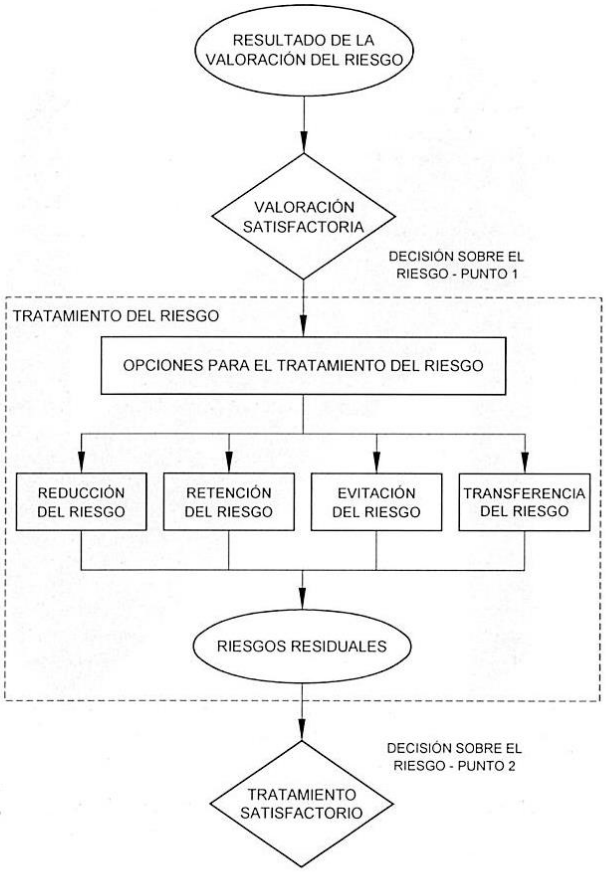


***Figura 7.*** *Tratamiento del riesgo.*[2]

### 4.4. ACEPTACIÓN DEL RIESGO

En esta etapa se evalúa si el tratamiento a los riesgos fue eficaz o necesita ser nuevamente tratado.

Como se estableció, los criterios de aceptación de riesgo definidos por la CVC son:

- ADMISIBLE (3 – 43)
- ACEPTABLE (44 – 104)
- TOLERABLE (105 – 175)

[2] NTC-ISO/IEC 27005:2009.

### 4.5. COMUNICACIÓN DEL RIESGO

Es muy importante un intercambio bidireccional de información y opiniones sobre el riesgo ya que esto promueve una mejor comprensión y toma de decisiones para la gestión de riesgos. Esta comunicación se sucede en varias instancias:

- Al realizar la valoración de los riesgos en los intercambios de información por parte del Oficial de Seguridad de la Información, o quien haga sus veces, y los líderes de procesos.

- Al terminar la valoración de los riesgos se presenta informe ejecutivo a la Dirección General.

- Al materializarse un riesgo con alto impacto se realiza una reunión con la Dirección General, el Oficial de Seguridad de la Información, o quien haga sus veces, y los líderes de los procesos involucrados.

- Anualmente en reunión de revisión por la Dirección.

- En sensibilizaciones y capacitaciones a los empleados y terceras partes.

### 4.6. MONITOREO Y SEGUIMIENTO DE LOS RIESGOS

En la gestión de riesgos es importante monitorear los cambios que se puedan producir en éstos y en sus factores (activos, vulnerabilidades, amenazas, etc.) para así lograr realizar a tiempo modificaciones o adiciones al enfoque en la metodología o instrumentos utilizados dependiendo de los cambios identificados.

Este monitoreo y seguimiento se realiza teniendo en cuenta los siguientes aspectos:

- Identificación de nuevos activos de información incluidos en el alcance del SGSI.
- Modificaciones a los valores de los activos.
- Nuevas causantes de riesgos (amenazas y vulnerabilidades).
- Incidentes de seguridad de la información.

Así mismo, se ha determinado la realización de la valoración de los riesgos al menos una vez al año y teniendo en cuenta cambios en:

- La organización
- La tecnología
- Procesos de negocio

Las actividades definidas para la realización del monitoreo son:

- Auditorías internas y externas de seguridad de la información.
- Auditorias de sistemas de información.
- Reuniones mensuales o según definición de la Dirección y del Oficial de Seguridad de la Información con los líderes de procesos.
- Anualmente en reunión de revisión por la Dirección.
- Análisis de vulnerabilidades técnicas y Ethical hacking.
- Revisión periódica de la eficacia de los controles aplicados.

Los riesgos en seguridad de la información catalogados para seguimiento y periodicidad de su medición serán determinados por la Dirección general, el jefe de la OTI y el Oficial de Seguridad de la Información.

Se determina realizar seguimiento a los riesgos de seguridad de la información con nivel INACEPTABLE e INADMISIBLE, resultado de la valoración de riesgos anual, que tengan un nivel de impacto y de ocurrencia considerable y cuando comprometan directamente la seguridad de la información para la CVC y puedan desencadenar riesgos secundarios.

El seguimiento a los riesgos de seguridad de la información críticos o de alto impacto para la CVC será monitoreado por el Oficial de Seguridad de la Información y se ejecutarán las acciones pertinentes asociadas con el plan de tratamiento de riesgos para el control eficaz del riesgo y su mitigación, así como el seguimiento preventivo del nivel de riesgo.

Todo control aplicado con el fin de mitigar el valor de riesgo calculado debe ser medible a través de su eficacia. La aplicación de un control no necesariamente implica la reducción total del valor de riesgo esperado sino la reducción a los niveles de riesgo aceptables establecidos por la CVC. La funcionalidad de los controles debe ser constantemente evaluada; en caso de no obtener los resultados esperados se les deben aplicar las mejoras a través de una nueva aplicación de la metodología PHVA.

## 4.7. OTROS DOCUMENTOS RELACIONADOS

- Política General SGSI.
- MN.0720.01 Sistema de gestión de la seguridad de la información.
- MN.0720.02 Políticas de seguridad de la información.
- Matriz de gestión de riesgos de seguridad de la información.