

**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL**

**Bogotá, D.C.,**

**DICIEMBRE DE 2021**

**CONTENIDO**

[**1.** **INTRODUCCIÓN.** 3](#_Toc89965353)

[**2.** **OBJETIVOS.** 4](#_Toc89965354)

[**3.** **ALCANCE.** 4](#_Toc89965355)

[**4.** **GLOSARIO.** 5](#_Toc89965356)

[**5.** **ROLES Y RESPONSABILIDADES.** 7](#_Toc89965357)

[**6.** **PLAN DE TRATAMIENTO DE RIESGOS.** 9](#_Toc89965359)

[**6.1.** **Establecimiento de Contexto.** 10](#_Toc89965361)

[**6.2.** **Criterios para la Gestión de Riesgos de Seguridad de la Información.** 11](#_Toc89965363)

[**6.3.** **Identificación del Riesgo.** 12](#_Toc89965365)

[**6.4.** **Análisis del Riesgo.** 14](#_Toc89965367)

[**6.5.** **Valoración del Riesgo.** 16](#_Toc89965370)

[**6.6.** **Controles asociados a la seguridad de la información** 17](#_Toc89965372)

[**7.** **MONITOREO Y REVISIÓN:** 17](#_Toc89965373)

[**7.1.** **Valoración de los Controles.** 18](#_Toc89965375)

[**7.2.** **Tratamiento del Riesgo.** 19](#_Toc89965376)

**INDICE DE TABLAS**

[**Tabla No 1. Roles y Responsabilidades.** 7](#_Toc89965215)

[**Tabla No 2. Establecimiento del Contexto.** 11](#_Toc89965219)

[**Tabla No 03. Criterio para Definir la Probabilidad.** 15](#_Toc89965224)

[**Tabla No 04. Criterio para Definir el Impacto** 15](#_Toc89965225)

**INDICE DE ILUSTRACIONES**

[**Ilustración No. 01. Metodología Gestión del Riesgo.** 10](#_Toc89965217)

[**Ilustración No. 02. Metodología.** 12](#_Toc89965364)

[**Ilustración No. 03. Tipos de Riesgo Seguridad Digital** 14](#_Toc89965366)

[**Ilustración No. 04. Tipos de Controles.** 17](#_Toc89965371)

[**Ilustración No. 05. Tipos de Controles.** 18](#_Toc89965374)

## **INTRODUCCIÓN.**

La Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, a través del presente documento, establece los lineamientos para lograr la gestión del riesgo en materia seguridad digital al interior de la entidad, a los cuales pueden estar expuestos los activos de información.

Por medio de los lineamientos establecidos, la entidad puede controlar el grado de exposición a potenciales amenazas o vulnerabilidades sobre los activos de información en sus diferentes procesos, determinando el uso correcto y adecuado de cada uno de ellos, clasificándolos según su nivel de exposición al riesgo y su importancia en la misionalidad de la entidad.

Adicional, el presente documento establece los roles y las responsabilidades que tienen las diferentes líneas de defensa al interior de la entidad, permitiendo tener la claridad acerca de las respectivas funciones que se deben llevar a cabo en cada una de las líneas defensa, permitiendo la articulación apropiada en cada una de ellas.

Finalmente, el documento establece las pautas necesarias que se deben tener en cuenta al realizar los controles sobre los diferentes riesgos identificados en los activos de información, permitiendo que su elaboración cumpla con el propósito de mitigar posibles eventos y/o incidentes de seguridad de la información.

## **OBJETIVOS.**

* Establecer los lineamientos al interior de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, que mitiguen las amenazas y/o vulnerabilidades que afecten la confidencialidad, integridad y disponibilidad de los activos de información de la entidad.
* Evaluar y analizar por el responsable de la información, los riesgos asociados a los activos de información de la entidad, estableciendo los controles correspondientes para la mitigación de eventos y/o incidentes de seguridad de la información.
* Establecer las acciones a seguir por parte de los colaboradores de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, para la realización de identificación, valoración y control de los riesgos correspondientes a los activos de información.

## **ALCANCE.**

Aplica para todos los colaboradores de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, que tengan acceso a los recursos y activos de información, en todas sus formas (digital, impresa, escrita, y hablada), durante su ciclo de vida (creación, distribución, transmisión, almacenamiento, eliminación), adicional se encuentra orientada a preservar la confidencialidad, integridad y disponibilidad de la información de la entidad, los cuales están sujetos a los mismos requerimientos de seguridad, y tienen las mismas responsabilidades de salvaguardar la información; por lo tanto, están obligados a continuar protegiendo y cumpliendo las políticas de confidencialidad durante y una vez terminada su relación laboral y/o contractual con la entidad.

## **GLOSARIO.**

* **Activo:** En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.
* **Activos de Información:** Cualquier elemento de información o que interactúe con ella que sea necesario para desempeñar las actividades diarias y cuya no disponibilidad o deterioro supone un agravio o coste. La naturaleza de los activos dependerá de la empresa, pero su protección es el fin último de la gestión de riesgos. La valoración de los activos es importante para la evaluación de la magnitud del riesgo.
* **Amenazas:** Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
* **Causa:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
* **Causa Raíz:** Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.
* **Confidencialidad:** Propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
* **Consecuencia:** Efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas
* **Control:** Medida que se toma para modificar la exposición al riesgo, bien sea para disminuir la probabilidad de ocurrencia del evento o para disminuir su impacto.
* **Colaboradores:** Todos los servidores públicos, trabajadores oficiales, orden de prestación de servicios y todas las personas que se encuentren vinculadas a la Entidad y que deban generar algún trabajo para la misma.
* **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.
* **Impacto:** Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.
* **Integridad:** propiedad de exactitud y completitud.
* **Inventario de Activos**: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.)
* **Mapa de Riesgos:** Documento con la información resultante de la gestión del riesgo.
* **Probabilidad:** se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.
* **Riesgo**: Es la definición de un escenario bajo el cual una amenaza puede explotar una vulnerabilidad, generando un impacto negativo al negocio (por ejemplo, pérdida de la continuidad, incumplimiento, pérdida de ingresos, entre otros).
* **Riesgo Inherente:** Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.
* **Riesgo Residual:** El resultado de aplicar la efectividad de los controles al riesgo inherente.
* **Riesgo Seguridad de la Información:** 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. (ISO/IEC27000).
* **Seguridad de la información:** Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener su confidencialidad, disponibilidad y la integridad de los datos y que la conforman.
* **Tolerancia al Riesgo:** Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.
* **Vulnerabilidad**: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

## **ROLES Y RESPONSABILIDADES.**

La gestión del riesgo es una responsabilidad que cada una de las áreas y/o dependencias de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial deben asumir. Por lo anterior, se contemplan los siguientes roles y responsabilidades al interior de la entidad, enfocados en salvaguardar los activos de información ante posibles eventos y/o incidentes de seguridad de la información:

## **Tabla No 1. Roles y Responsabilidades.**

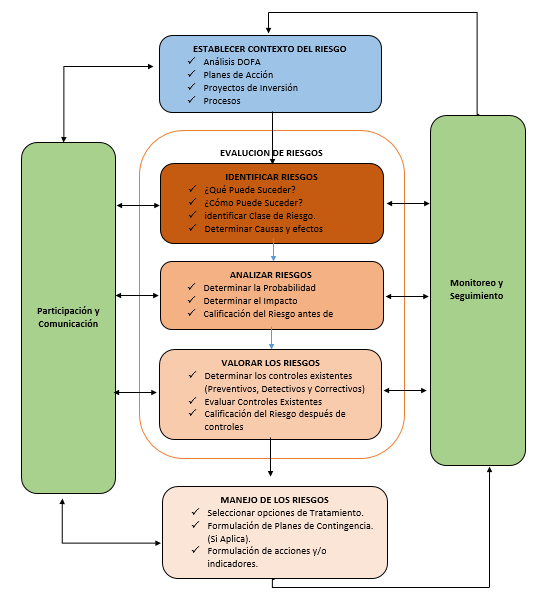
| **ROLES** | **RESPONSABILIDADES** |
| --- | --- |
| **Línea Estratégica**  (Está conformada por la alta dirección y el Comité Institucional De Coordinación De Control Interno) | * Definir y aprobar la Política de Administración del Riesgo, la cual incluye los niveles de responsabilidad y autoridad. * Analizar los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación de la entidad y que puedan generar cambios en la estructura de riesgos y controles. * Hacer seguimiento en el Comité Institucional y de Control Interno a la implementación de cada una de las etapas de la gestión del riesgo y los resultados de las evaluaciones realizadas por Control Interno o Auditoría Interna * Revisar el cumplimiento a los objetivos institucionales y de procesos y sus indicadores e identificar en caso de que no se estén cumpliendo, los posibles riesgos. * Hacer seguimiento y pronunciarse por lo menos cada cuatrimestre sobre el perfil de riesgo inherente y residual de la entidad, incluyendo los riesgos de corrupción * Revisar los informes presentados por lo menos cada cuatrimestre de los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos de riesgos materializados, como aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas, a través del análisis de indicadores asociados a dichos objetivos. * Revisar las acciones de contingencia establecidas para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento. * Asegurar los recursos necesarios para ayudar a los responsables de gestionar y tratar los riesgos. |
| **Primera Línea de Defensa**  (Está conformada por los gerentes públicos y líderes de los procesos, programas y proyectos de la entidad) | * Conocer y apropiar las políticas, procedimientos, manuales, protocolos y otras herramientas que permitan tomar acciones para el autocontrol en sus procesos. * Identificar, analizar y valorar los riesgos que pueden afectar los programas, proyectos, planes y procesos a su cargo y actualizar el mapa de riesgos cuando se requiera. * Realizar la identificación de activos de información, físicos y humanos en su proceso. * Definir, aplicar, monitorear y hacer seguimiento a los controles para mitigar los riesgos identificados alineándolos con las metas y objetivos de la entidad y proponer mejoras a la gestión del riesgo en su proceso. * Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar. * Desarrollar ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles. * Revisar y reportar la Oficina Asesora de Planeación (segunda línea) sobre los riesgos materializados en los programas, proyectos, planes y/o procesos a su cargo. * Reportar a la Oficina Asesora de Planeación (segunda línea) los avances y evidencias de la gestión de los riesgos a cargo del proceso asociado. |
| **Segunda Línea de Defensa**  (Está conformada por la Oficina Asesora de Planeación, supervisores e interventores de contratos o proyectos o referentes de sistemas de gestión.) | * Asesorar a la línea estratégica en el análisis del contexto interno y externo, para la definición de la política de riesgos, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo. * Consolidar el mapa de riesgos institucional (riesgos de mayor criticidad frente al logro de los objetivos) y presentarlo para análisis y seguimiento ante el Comité CIGD. * Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis y valoración del riesgo. * Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos * Presentar al Comité CIGD el seguimiento de los controles en los procesos. |
| **Tercera Línea de Defensa**  (Está conformada por la Oficina de Control Interno) | * Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y los controles, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos. * Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa * Asesorar de forma coordinada con la Oficina Asesora de Planeación, a la primera línea de defensa en la identificación de los riesgos institucionales y en el diseño de controles * Llevar a cabo el seguimiento a los riesgos consolidados en los mapas de riesgos de conformidad con el Plan Anual de Auditoria y reportar los resultados al Comité. * Recomendar mejoras a la política de administración del riesgo. |
| **Líder Política de Seguridad Digital** | * Definir el procedimiento para la Identificación y Valoración de Activos. * Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad digital (Identificación, Análisis, Evaluación y Tratamiento). * Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de seguridad digital y en la recomendación de controles para mitigar los riesgos. * Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos. * Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad digital. |

**Fuente:** DESI-MA-002 Manual Política Administración del Riesgo.

## **PLAN DE TRATAMIENTO DE RIESGOS.**

Para la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, realizar una adecuada gestión del riesgo sobre cada uno de sus activos de información le permitirá determinar los controles a aplicar, las acciones y/o tratamientos a realizar mitigando posibles eventos y/o incidentes de seguridad de la información. Por lo anterior, se establece la siguiente metodología para realizar una adecuada gestión del riesgo en la entidad.

## **Ilustración No. 01. Metodología Gestión del Riesgo.**



**Fuente:** Cartilla Guía para la Administración del Riesgo DAFP.

## **Establecimiento de Contexto.**

La finalidad de establecer el contexto es determinar los posibles factores, tanto internos como externos que pueden influir en la generación de eventos que afecten negativamente la misionalidad de la entidad.

Dentro del contexto se catalogan situaciones de carácter político, social, ambiental, cultural, económico, tecnológico y legal, tanto a nivel nacional, regional y/o internacional según sea el caso.

Para el caso del contexto interno se deben catalogar las situaciones relacionadas con la cultura organizacional, recursos humanos, procesos, recursos financieros, recursos tecnológicos y todos aquellos con los que cuenta la entidad.

## **Tabla No 2. Establecimiento del Contexto.**

|  |  |
| --- | --- |
| **CONTEXTO EXTERNO** | **POLÍTICOS**: cambios de gobierno, legislación, políticas públicas, regulación. |
|  |
| **ECONÓMICOS Y FINANCIEROS:** disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia. |  |
|  |
| **SOCIALES Y CULTURALES:** demografía, responsabilidad social, orden público. |  |
|  |
| **TECNOLÓGICOS:** avances en tecnología, acceso a sistemas de información externos, gobierno en línea. |  |
|  |
| **AMBIENTALES:** emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible |  |
|  |
| **LEGALES Y REGLAMENTARIOS:**  Normatividad externa (leyes, decretos, ordenanzas y acuerdos). |  |
|  |
| **CONTEXTO INTERNO** | **FINANCIEROS:**  presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada |  |
|  |
| **PERSONAL:** competencia del personal, disponibilidad del personal, seguridad y salud ocupacional. |  |
|  |
| **PROCESOS:** capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento. |  |
|  |
| **TECNOLOGÍA:**  integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información. |  |
|  |
| **ESTRATÉGICOS:** direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo. |  |
|  |
| **COMUNICACIÓN INTERNA:**  canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones. |  |
|  |
| **CONTEXTO DEL PROCESO** | **DISEÑO DEL PROCESO:** claridad en la descripción del alcance y objetivo del proceso. |  |
|  |
| **INTERACCIONES CON OTROS PROCESOS:** relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes. |  |
|  |
| **TRANSVERSALIDAD:** procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad. |  |
|  |
| **PROCEDIMIENTOS ASOCIADOS:**  pertinencia en los procedimientos que desarrollan los procesos. |  |
|  |
| **RESPONSABLES DEL PROCESO:** grado de autoridad y responsabilidad de los funcionarios frente al proceso. |  |
|  |
| **COMUNICACIÓN ENTRE LOS PROCESOS:**  efectividad en los flujos de información determinados en la interacción de los procesos. |  |
|  |
| **ACTIVOS DE SEGURIDAD DIGITAL DEL PROCESO:** información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso |  |
|  |
|  |

**Fuente:** Guía para la Administración del Riesgo – DAFP.

# **Criterios para la Gestión de Riesgos de Seguridad de la Información.**

Con el fin de evitar la posible materialización de riesgos de seguridad de la información, la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, en primera instancia debe realizar la identificación y valoración de activos de información en cada una de las áreas y/o procesos, siguiendo la metodología dispuesta en **EGTI-DI-012 Política de Seguridad de Gestión de Activos de Información.**

# **Ilustración No. 02. Metodología.**

Diagrama

Descripción generada automáticamente

**Fuente:** Ministerio de Tecnologías de la Información y Comunicaciones.

## **Identificación del Riesgo.**

La identificación del riesgo tiene como finalidad conocer las situaciones que se puedan presentar en la entidad y las consecuencias que las materializaciones de estos riesgos pueden causar en la misionalidad de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial.

Por lo anterior, se debe realizar la identificación de los activos de información, en cada uno de los procesos o grupos de trabajo que hay en la entidad, permitiendo conocer a los mismos, sus activos de información, para que, de esta manera, logren establecer los mecanismos y/o controles correspondientes para la mitigación de posibles eventos y/o incidentes a nivel de Seguridad. Al interior de la entidad, se ha adaptado la metodología de Gestión de Activos de Información, para que cada una de las áreas y/o dependencias realice su respectiva identificación, valoración y control sobre los activos identificados. Esta metodología se encuentra en ***EGTI-DI-012 Política de Seguridad de Gestión de Activos de Información.***

Una vez realizado el inventario de activos de información en cada uno de los procesos, se deben establecer los siguientes interrogantes[[1]](#footnote-1) con la finalidad de determinar las posibles causas que afectan el desarrollo de la misionalidad de la entidad, teniendo como base tanto el contexto externo como el interno:

* **¿QUÉ PUEDE SUCEDER?** Identificar la afectación del cumplimiento del objetivo estratégico o del proceso según sea el caso.
* **¿CÓMO PUEDE SUCEDER?** Establecer las causas a partir de los factores determinados en el contexto.
* **¿CUÁNDO PUEDE SUCEDER?** Determinar de acuerdo con el desarrollo del proceso.
* **¿QUÉ CONSECUENCIAS TENDRÍA SU MATERIALIZACIÓN?** Determinar los posibles efectos por la materialización del riesgo.

La manera para que los colaboradores de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, visualicen los riesgos dentro de sus respectivos procesos, es mediante el diligenciamiento de la herramienta ***DESI-FM-018 Formato Mapa de Riesgos de Procesos,*** la cual permite tener un inventario de riesgos por procesos, estableciendo las causas con base en el contexto externo e interno, detallando la forma en que estos factores afectarían el activo de información, sus consecuencias y su impacto en la misionalidad de la entidad.

Por consiguiente, se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

* Pérdida de la Confidencialidad.
* Pérdida de la Integridad.
* Pérdida de la Disponibilidad.

Para cada riesgo se deben asociar el grupo de activos, o activos específicos del área y/o proceso y analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

# **Ilustración No. 03. Tipos de Riesgo Seguridad Digital**

Texto

Descripción generada automáticamente

**Fuente:** DESI-MA-002 Manual Política de Administración del Riesgo.

## **Análisis del Riesgo.**

Una vez completada la identificación de los riesgos, se debe proceder con su respectivo análisis, en el cual se busca determinar la probabilidad de ocurrencia del riesgo y sus respectivas consecuencias. Además, al lograr establecer las consecuencias, sirve de insumo para la orientación de la clasificación del riesgo, con el fin de obtener la información para establecer el nivel del riesgo y las acciones que se van a implementar.

En este punto se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE).[[2]](#footnote-2)

A continuación, se mencionan los pasos claves para la realización del análisis de riesgos:

* Determinar probabilidad.
* Determinar impacto (consecuencias).
* Clasificar el riesgo.
* Estimar nivel del riesgo.

Existen dos (2) aspectos que se deben tener en cuenta sobre el análisis de los riesgos identificados: probabilidad e impacto.

* **Probabilidad:** es la posibilidad de ocurrencia del riesgo.
* **Impacto:** son las consecuencias que puede ocasionar la materialización del riesgo.

Para realizar el análisis del riesgo se deben considerar los siguientes dos (2) aspectos: Clasificación del riesgo y evaluación del riesgo.

* **Clasificación del Riesgo:** se determina a través de la probabilidad de ocurrencia y el impacto que significaría su materialización, teniendo en cuenta los criterios de probabilidad e impacto; donde la probabilidad debe ser medida a partir de las siguientes especificaciones:

## **Tabla No 03. Criterio para Definir la Probabilidad.**

|  |  |  |
| --- | --- | --- |
|  | **Frecuencia de la Actividad** | **Probabilidad** |
| Muy Baja | La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año | 20% |
| Baja | La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año | 40% |
| Media | La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año | 60% |
| Alta | La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año | 80% |
| Muy Alta | La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año | 100% |

**Fuente:** DESI-MA-002 Manual Política de Administración del Riesgo.

## **Tabla No 04. Criterio para Definir el Impacto**

|  |  |  |
| --- | --- | --- |
|  | **Afectación Económica (o presupuestal)** | **Pérdida Reputacional** |
| Leve 20% | Afectación menor a 130 SMLMV | El riesgo afecta la imagen de alguna área de la organización |
| Menor 40% | Entre 130 y 650 SMLMV | El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta directiva y accionistas y/o de proveedores |
| Moderado 60% | Entre 650 y 1300 SMLMV | El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos |
| Mayor 80% | Entre 1300 y 6500 SMLMV | El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal |
| Catastrófico 100% | Mayor a 6500 SMLMV | El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitarios sostenible a nivel país |

**Fuente:** DESI-MA-002 Manual Política de Administración del Riesgo.

* **Evaluación del Riesgo:** Permite comparar los resultados de la calificación del riesgo, con los criterios definidos para establecer el grado de exposición en el que se encuentra la entidad; de esta manera la entidad puede determinar y distinguir entre los riesgos aceptable, tolerable, moderados, importantes y/o inaceptables y fijar las prioridades de las acciones necesarias para su tratamiento.[[3]](#footnote-3)

## **Valoración del Riesgo.**

La valoración del riesgo se obtiene de confrontar los resultados de la evaluación del riesgo con los controles identificados, lo cual permitirá a la entidad establecer las prioridades para el tratamiento de estos. Para adelantar esta etapa se debe tener claridad sobre los puntos de control existentes en los diferentes procesos, esto permitirá mejorar la toma de decisiones.[[4]](#footnote-4)

A continuación, se mencionan las pautas claves para la valoración del riesgo:

* Identificar controles existentes.
* Verificar efectividad de los controles.
* Establecer prioridad de tratamiento.

Para la realizar la valoración de los controles existentes se debe tener en cuenta que estos se clasifican en:

# **Ilustración No. 04. Tipos de Controles.**

Diagrama

Descripción generada automáticamente

**Fuente:** DESI-FM-018 Formato Mapa de Riesgos de Proceso.

# **Controles asociados a la seguridad de la información**

Para mitigar/tratar los riesgos de seguridad de la información emplear como mínimo los controles del Anexo A de la ISO/IEC 27001:2013, estos controles se encuentran en el anexo 4. “Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas”, siempre y cuando se ajusten al análisis de riesgos. En virtud de lo anterior, la entidad debe desarrollar conforme a sus necesidades, las actividades correspondientes para realizar la identificación y valoración de los riesgos de seguridad de la información con base en los activos de información identificados con criticidad alta.

# **MONITOREO Y REVISIÓN:**

Para los riesgos de **seguridad de la información** se realizará el monitoreo y el seguimiento a su plan de acción y controles **CUATRIMESTRAL** y lo realizará la mesa de trabajó de activos de información o las personas designadas.

# **Ilustración No. 05. Tipos de Controles.**

Texto

Descripción generada automáticamente

**Fuente:** DESI-MA-002 Política Administración del Riesgo

## **Valoración de los Controles.**

Si el control establecido está bien diseñado y se ejecuta según el diseño de forma consistente, permitirá a la entidad mitigar posibles riesgos de seguridad de la información contribuyendo a salvaguardar los activos de información.

La valoración de los controles en su diseño y ejecución que contribuyen a la gestión del riesgo, al interior de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, es una responsabilidad de la tercera línea de defensa, según lo contemplado en ***CEM-CP-001 Caracterización de proceso.***

## **Tratamiento del Riesgo.**

El tratamiento del riesgo es la respuesta que brinda la primera línea de defensa para lograr mitigar los posibles riesgos que puedan afectar los activos de información de la entidad. La primera línea de defensa, deberán tener en cuenta la importancia del riesgo, lo cual incluye el efecto que pueda causar en la entidad, la probabilidad e impacto de este y la relación costo-beneficio de las medidas de tratamiento necesarias para realizar la respectiva mitigación.

Por lo anterior, el tratamiento del riesgo se enmarca en las siguientes categorías:

* **Aceptar el riesgo:**

No se adopta ninguna medida que cambie y/o afecte la probabilidad e impacto del riesgo.

La aceptación del riesgo se puede adoptar para los riesgos clasificados como bajos, adicional, pueden existir escenarios de riesgos a los que no se le puede aplicar controles y por consiguiente se acepta el riesgo. Sin embargo, en ambas situaciones se deben realizar los seguimientos correspondientes.

* **Reducir el riesgo:**

Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles.

La reducción del riesgo puede ser administrado mediante el establecimiento de controles, de tal manera que el riesgo residual pueda se reevaluado y tener valores aceptables para la entidad. El establecimiento de estos controles permite disminuir la probabilidad y/o impacto del riesgo. Adicional, se debe seleccionar los controles apropiados y con una adecuada segregación de funciones, de tal manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este.

* **Evitar el riesgo:**

Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.

Cuando los escenarios de riesgo identificados se consideran demasiado extremos, se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o un conjunto de actividades.

* **Compartir el riesgo:**

Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este.

Cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable o se carece de conocimientos necesarios para gestionarlo, este puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia.

Los dos principales métodos de compartir o transferir parte del riesgo son: seguros y tercerización. Estos mecanismos de transferencia de riesgos deberían estar formalizados a través de un acuerdo contractual.

**REVISIÓN Y APROBACIÓN:**

|  |  |  |
| --- | --- | --- |
| **Elaborado y/o Actualizado por** | **Validado por**  **Líderes (Estratégico u Operativo) del Proceso:** | **Aprobado:** |
| **LUIS ENRIQUE PARIS GARCIA /**  **GLORIA MENDEZ RUIZ**  Contratista / Proceso EGTI | **Firma:** | **Firma:** |
| **Acompañamiento Asesor OAP:** |
| **CHRISTIAN MEDINA FANDIÑO**  Contratista/ Proceso DESI |
| **MARTHA PATRICIA AGUILAR COPETE**  Secretaria General | **JUAN HERNANDO LIZARAZO**  Jefe-OAP (E)  Representante Alta Dirección |

**CONTROL DE CAMBIOS:**

|  |  |  |  |
| --- | --- | --- | --- |
| **VERSIÓN** | **DESCRIPCIÓN** | **FECHA** | **APROBADO**  **Representante de la Alta Dirección** |
| 1 | Elaborado por el Ing. Omar Fdo. Garzón Giraldo (especialista en seguridad de la información), versión inicial del documento conforme a los requerimientos de MINTIC. | Febrero 2019 | Jefe Oficina Asesora de Planeación |
| 2 | Se actualizan objetivos, se articula roles y responsabilidades con la Política de Administración del Riesgo, se incluye metodología de activos de información, se incorpora pasos para la identificación, análisis y controles de riesgos. Se incorpora valoración de los controles. | Noviembre 2020 | Jefe Oficina Asesora de Planeación |
| 3 | Se actualiza plan conforme a la nueva metodología de riesgos del DAFP. | Diciembre 2021 | Jefe Oficina Asesora de Planeación |

1. Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 [↑](#footnote-ref-1)
2. Guía para la administración del riesgo y el diseño de controles en entidades Públicas. [↑](#footnote-ref-2)
3. Guía para la administración del riesgo. [↑](#footnote-ref-3)
4. Ibidem, p.32 [↑](#footnote-ref-4)