

**MANUAL**

**Política De Administración Del Riesgo**

**BOGOTÁ, D.C. JUNIO**

**2020**

CONTENIDO

[POLÍTICA DE ADMINISTRACIÓN DE RIESGO 3](#_Toc43217242)

[1. OBJETIVO GENERAL 4](#_Toc43217243)

[1.1. OBJETIVOS ESPECÍFICOS 4](#_Toc43217244)

[2. ALCANCE DE LA POLÍTICA 4](#_Toc43217245)

[3. TÉRMINOS Y DEFINICIONES 4](#_Toc43217246)

[4. ROLES Y RESPONSABILIDADES 7](#_Toc43217247)

[5. METODOLOGÍA PARA LA ADMINISTRACIÓN DE RIESGOS 9](#_Toc43217248)

[5.1. ESTABLECIMIENTO DEL CONTEXTO 9](#_Toc43217249)

[5.3. IDENTIFICACIÓN DE RIESGOS 14](#_Toc43217250)

[5.3.1 REDACCIÓN DE RIESGOS: 15](#_Toc43217251)

[5.3.2 TIPOLOGÍA DE RIESGO 15](#_Toc43217252)

[5.3.3 IDENTIFICACIÓN DE CAUSAS 16](#_Toc43217253)

[5.3.4 RIESGOS DE GESTIÓN 16](#_Toc43217254)

[5.3.5 RIESGOS DE CORRUPCIÓN 17](#_Toc43217255)

[5.3.6 RIESGOS DE SEGURIDAD DIGITAL 17](#_Toc43217256)

[IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES 18](#_Toc43217257)

[5.4 VALORACIÓN DE RIESGOS 22](#_Toc43217258)

[5.4.1. ANÁLISIS DE RIESGOS 22](#_Toc43217259)

[Cálculo de la Probabilidad 23](#_Toc43217260)

[Cálculo del Impacto: 23](#_Toc43217261)

[5.4.2. RIESGO INHERENTE - ANTES DE CONTROLES 27](#_Toc43217262)

[5.4.3. TRATAMIENTO DEL RIESGO 27](#_Toc43217263)

[5.4.3.1. Tratamiento de Riesgos de Seguridad Digital 28](#_Toc43217264)

[5.4.4. EVALUACIÓN DE RIESGOS 29](#_Toc43217265)

[5.4.6. VALORACIÓN DE LOS CONTROLES 37](#_Toc43217266)

[Evaluación del Diseño del control 37](#_Toc43217267)

[Evaluación del Ejecución del control 38](#_Toc43217268)

[Cálculo del riesgo residual: 39](#_Toc43217269)

[6. PLAN DE TRATAMIENTO DE RIESGOS 40](#_Toc43217270)

[7. MONITOREO, SEGUIMIENTO Y AJUSTES 41](#_Toc43217271)

[8. LINEAMIENTOS PARA EL MANEJO DE RIESGOS MATERIALIZADOS 43](#_Toc43217272)

**LISTADO DE TABLAS**

[Tabla 1 Factores para cada categoría del contexto de la UAERMV 10](#_Toc42867622)

[Tabla 2 Clasificación de Activos 12](#_Toc42867623)

[Tabla 3 Clasificación de acuerdo con la confidencialidad 13](#_Toc42867624)

[Tabla 4 Clasificación de acuerdo con la integridad 13](#_Toc42867625)

[Tabla 5 Clasificación de acuerdo con la disponibilidad 13](#_Toc42867626)

[Tabla 6 Niveles de clasificación 14](#_Toc42867627)

[Tabla 7 Tipología del Riesgo 15](#_Toc42867628)

[Tabla 8 Ejemplos De Riesgo de gestión 16](#_Toc42867629)

[Tabla 9 Matriz de definición de riesgo de Corrupción 17](#_Toc42867630)

[Tabla 10 Ejemplos de Riesgo de Corrupción 17](#_Toc42867631)

[Tabla 11 Ejemplos de Riesgo de seguridad digital 18](#_Toc42867632)

[Tabla 12 Amenazas más comunes 19](#_Toc42867633)

[Tabla 13 Vulnerabilidades más comunes 20](#_Toc42867634)

[Tabla 14 Ejemplos de vulnerabilidades y amenazas 20](#_Toc42867635)

[Tabla 15 Criterios parar calificar la probabilidad 23](#_Toc42867636)

[Tabla 16 Matriz de priorización de probabilidad 23](#_Toc42867637)

[Tabla 17 Criterios para calificar el impacto de riesgos de gestión 24](#_Toc42867638)

[Tabla 18 Criterios para determinar impacto de corrupción 25](#_Toc42867639)

[Tabla 19 Criterios para determinar impacto de seguridad digital 26](#_Toc42867640)

[Tabla 20 Mapa de calor 27](#_Toc42867641)

[Tabla 21 Riesgo Inherente 27](#_Toc42867642)

[Tabla 22 Opciones de manejo del riesgo 28](#_Toc42867643)

[Tabla 23 Ejemplos controles 29](#_Toc42867644)

[Tabla 24 Controles de referencia para la mitigación de riesgos de seguridad digital 29](#_Toc42867645)

[Tabla 25 Variables a evaluar para el adecuado diseño de controles 37](#_Toc42867646)

[Tabla 26 Rango de calificación del diseño 38](#_Toc42867647)

[Tabla 26 Criterio para a evaluar para la ejecución del control 38](#_Toc42867648)

[Tabla 28 Rango de calificación de la ejecución 38](#_Toc42867649)

[Tabla 29 Rango de calificación de la solidez de controles 39](#_Toc42867650)

[Tabla 30 Cuadrantes a disminuir después de controles 40](#_Toc42867651)

# POLÍTICA DE ADMINISTRACIÓN DE RIESGO

La Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial-UAERMV, se compromete a administrar los riesgos que puedan dificultar la misión y el cumplimiento de los objetivos institucionales, para lo cual implementará mecanismos efectivos que permitan identificar, analizar, valorar y definir acciones para controlar riesgos de gestión, corrupción y seguridad digital. Este proceso debe contar con la activa participación de los colaboradores de los procesos y proyectos quienes propenderán por la mitigación de los riesgos.

# OBJETIVO GENERAL

Suministrar lineamientos para la administración de gestión del riesgo, que permitan reducir de manera efectiva los riesgos que afectan el logro, la misión, la visión, los objetivos protegiendo y preservando la integridad, confidencialidad, disponibilidad y autenticidad de la información.

## OBJETIVOS ESPECÍFICOS

* Garantizar la identificación de los riesgos que pueden llegar a afectar el cumplimiento de la misión encomendada a la Entidad, a través de los procesos.
* Implementar acciones para prevenir la materialización del riesgo y controlar los riesgos
* Involucrar y comprometer a todos los colaboradores de la entidad en la búsqueda de acciones efectivas para prevenir y administrar los riesgos.
* Contribuir a que se genere una cultura de pensamiento basado en riesgos, con autocontrol y auto evaluación al interior de la Entidad.
* Realizar monitoreo y seguimiento a la administración del riesgo en la Entidad.

# ALCANCE DE LA POLÍTICA

La política de riesgos es aplicable a todos los procesos y proyectos de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial. Esta debe ser conocida y aplicada por todos los colaboradores de la entidad y abarca los principios básicos y metodológicos para la administración y gestión de riesgos a nivel de procesos, aprobados para las entidades públicas y adaptados en lo pertinente a las funciones de la Entidad.

Las políticas y las acciones definidas para el manejo de los riesgos son de carácter obligatorio para todos los colaboradores, en las diferentes dependencias de la Entidad.

Los mapas de riesgos por proceso deberán ser aprobados por los Responsables Directivos. Además, el Representante de la Alta Dirección de la Unidad en nombre propio o a través de sus delegados del Comité Institucional de Gestión y Desempeño, podrá incluir los riesgos potenciales que no hayan sido incluidos en el mapa de riesgos.

# TÉRMINOS Y DEFINICIONES

* **Activo** es cualquier elemento que tenga valor para la entidad, sin embargo, en el contexto de seguridad digital son activos elementos tales como aplicaciones de la entidad pública, servicios Web, redes, información física o digital, Tecnologías de la Información -TI- o Tecnologías de la Operación -TO-) que utiliza la organización para su funcionamiento.
* **Administración del riesgo:** “Un proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos. El enfoque de riesgos no se determina solamente con el uso de la metodología, sino logrando que la evaluación de los riesgos se convierta en una parte natural del proceso de planeación”[[1]](#footnote-2)
* **Amenaza:** situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
* **Análisis del Riesgo:** 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.
* **Autocontrol:** Es la capacidad que tiene cada servidor público, independientemente de su nivel jerárquico dentro de la institución, para evaluar su trabajo, detectar desviaciones, efectuar correctivos, mejorar y solicitar ayuda cuando lo considere necesario, de tal manera que la ejecución de los procesos, actividades y tareas bajo su responsabilidad garanticen el ejercicio de una función administrativa transparente y eficaz.
* **Causas:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
* **Consecuencias:** los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
* **Confidencialidad:** propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
* **Controles:** Son mecanismos que permiten asegurar que las actividades reales se ajusten a las programadas. También son utilizados para detectar la presencia de errores y de evitar la materialización de los riesgos.
* **Disponibilidad:** propiedad de ser accesible y utilizable a demanda por una entidad.
* **Evento:** Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.
* **Factores de Riesgo:** Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.
* **Gestión de Riesgo:** proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.
* **Impacto**: Hace referencia a las consecuencias que puede ocasionar a la organización la materialización del riesgo; se refiere a la magnitud de sus efectos.
* **Integridad:** propiedad de exactitud y completitud.
* **Mapa de riesgos:** Es la herramienta metodológica que permite hacer un inventario de los riesgos de manera ordenada y sistemática. Permite definirlos, describirlos, indicar sus posibles consecuencias, así como indicar la probabilidad, el impacto inherente facilitando el registro de las acciones a seguir.
* **Monitoreo:** Es una evaluación continua de una acción en desarrollo. Es un proceso interno coordinado por los responsables de la acción. El sistema de monitoreo debe ser integrado en el trabajo cotidiano.
* **Plan anticorrupción y de atención al ciudadano** plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades
* **Probabilidad:** se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad expresados de manera cualitativa y cuantitativa.
* **Proceso:** Conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados.
* **Riesgo:** Posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso. Se expresa en términos de probabilidad e impacto.
* **Riesgo Inherente:** Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.
* **Riesgo residual:** Nivel de riesgo que permanece luego de tomar medidas de tratamiento del riesgo.
* **Riesgo de gestión:** posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.[[2]](#footnote-3)
* **Riesgo de corrupción:** posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
* **Riesgo de seguridad digital:** combinación de amenazas y vulnerabilidades en el entorno digital. Condiciones que pueden debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.
* **Seguimiento**: Observación minuciosa del desarrollo de un proceso, revisa continuamente la evolución del rendimiento respecto de lo previsto, mediante el análisis de datos e indicadores establecidos con fines de seguimiento y evaluación.
* **Vulnerabilidad** es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.

# ROLES Y RESPONSABILIDADES

**LÍNEA ESTRATEGICA:**

**(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:**

**(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**

**(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 DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN**

**(Se establece en la resolución del CIGD)**

* 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.

# METODOLOGÍA PARA LA ADMINISTRACIÓN DE RIESGOS

Con el fin de ejercer una correcta administración del riesgo, la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial-UAERMV en cumplimiento de la normatividad, adoptó la guía establecidas por el Departamento Administrativo de la Función Pública DAFP.

A continuación, se presentan los elementos y procedimientos indicados, y adoptados por la UAERMV para la adecuada administración de los riesgos.

**Esquema 1** Metodología para la administración del riesgo

Captura de pantalla de un celular

Descripción generada automáticamente

Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades Públicas Riesgo de gestión, Corrupción y seguridad Digital. Octubre 2018. DAFP. Pág. 13.*

## 5.1. ESTABLECIMIENTO DEL CONTEXTO

En este ejercicio se analizan las condiciones internas y externas (del entorno) de la Unidad y de los procesos, que pueden generar eventos o situaciones que afecten negativamente el cumplimiento de la misión y objetivos de la UAERMV.

**Análisis Interno**: El análisis interno se realiza identificando debilidades y fortalezas en la organización que puedan interferir con el logro de los objetivos corporativos. Están relacionadas con la estructura orgánica, cultura organizacional, el modelo de operación por procesos, el cumplimiento de los planes y programas, los sistemas de información, los procesos y procedimientos, los recursos humanos y económicos con los que cuenta la entidad.

**Análisis Externo**: Aquí se identifican circunstancias externas a la entidad que pueden intervenir en el cumplimiento de los objetivos. Las cuales pueden ser de carácter social, cultural, económico, ambiental, cambio tecnológico, político-legal, internacional, nacional o regional según sea el análisis.

Es importante tener presente que el objetivo de esta etapa es reunir toda la información que permita tener una mirada global sobre los factores de riesgo que rodean a la entidad y al proceso que se está analizando. El contexto estratégico es la base para la identificación del riesgo, dado que su análisis suministra la información sobre sus causas.

Tabla 1 Factores para cada categoría del contexto de la UAERMV

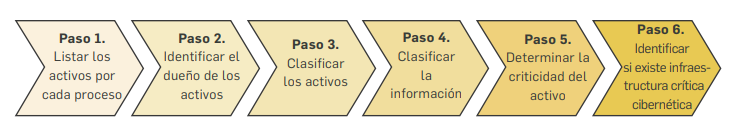
| CONTEXTO | CATEGORIA | DESCRIPCIÓN |
| --- | --- | --- |
| Contexto Externo | **Políticos** | Cambios de gobierno, legislación, políticas públicas, regulación. |
| **Económicos y financieros** | Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia. |
| **Sociales y culturales** | 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 y disponibilidad del personal, seguridad y salud ocupacional, Cultura organizacional |
| **Procesos:** | Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento. |
| **Tecnología:** | Integridad de los datos, disponibilidad de datos y sistemas, desarrollo, producción y mantenimiento de sistemas de información. |
| **Estratégicos:** | Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo, Estructura organizacional |
| **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 y de cara al ciudadano. |

Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades Públicas Riesgo de gestión, Corrupción y seguridad Digital. Octubre 2018. DAFP. Pág. 20.*

5.2. IDENTIFICACIÓN DE ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN

Un activo es cualquier elemento que tenga valor para la organización. Sin embargo, en el contexto de la seguridad digital, son activos elementos tales como: aplicaciones de la entidad pública, servicios Web, redes, información física o digital, Tecnologías de la Información -TI- o Tecnologías de la Operación -TO-) que utiliza la organización para su funcionamiento[[3]](#footnote-4). Los procesos deben realizar la identificación de los activos de información y documentar el inventario de activos, así podrán saber lo que deben hacer para proteger y garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano.

La identificación y valoración de activos debe ser realizada por la **Primera Línea de Defensa – Líderes de Proceso**, en cada proceso donde aplique la gestión del riesgo de seguridad digital[[4]](#footnote-5).

Esquema 2 Pasos para identificar los activos son:  Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades Públicas Riesgo de gestión, Corrupción y seguridad Digital. Octubre 2018. DAFP. Pág. 22.*

1. **Listar los activos por cada proceso:** En cada proceso deberán listarse los activos indicando algún consecutivo, nombre y descripción breve de cada uno.
2. **Identificar el dueño de los activos:** Cada uno de los activos identificados deberá tener un dueño designado (área/ dependencia), Si un activo no posee un dueño, nadie se hará responsable ni lo protegerá debidamente.
3. **Clasificar los activos**: Cada activo debe tener una clasificación o pertenecer a un determinado grupo de activos según su naturaleza cómo, por ejemplo: Información, Software, Hardware, Componentes de Red entre otros (ver tabla 2).

Tabla 2 Clasificación de Activos

| **CLASIFICACION**  **DE ACTIVOS** | **DESCRIPCION** |
| --- | --- |
| **Hardware** | Equipos físicos de cómputo y de comunicaciones como, servidores, biométricos que por su criticidad son considerados activos de información |
| **Información** | Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores), teniendo en cuenta lo anterior, se puede distinguir como información: Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros. |
| **Componentes de red** | Medios necesarios para realizar la conexión de los elementos de hardware y software en una red, por ejemplo, el cableado estructurado y tarjetas de red, routers, switches, entre otros |
| **Hardware** | Equipos físicos de cómputo y de comunicaciones como, servidores, biométricos que por su criticidad son considerados activos de información. |
| **Know-How - Servicios** | Servicio brindado por parte de la entidad para el apoyo de las actividades de los procesos, tales como: Servicios WEB, intranet, CRM, ERP, Portales organizacionales, Aplicaciones entre otros (Pueden estar compuestos por hardware y software) |
| **Software** | Activo informático lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades |
| **Intangibles** | Se consideran intangibles aquellos activos inmateriales que otorgan a la entidad una ventaja competitiva relevante, uno de ellos es la imagen corporativa, reputación o el goodwill, entre otros |
| **Personas** | Aquellos roles que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información, por ejemplo: personal con experiencia y capacitado para realizar una tarea específica en la ejecución de las actividades. |
| **Información** | Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores), teniendo en cuenta lo anterior, se puede distinguir como información: Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros. |
| **Instalaciones** | Espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para la empresa |

Fuente: Adaptado Anexo 4 Lineamientos para la Gestión del Riesgo de Seguridad Digital en Entidades Públicas - Guía riesgos 2018

1. **Clasificar la información:** Realizar la clasificación de la información conforme lo indican las leyes 1712 de 2014, 1581 de 2012, y demás normatividad aplicable. Esto adicionalmente ayudará a dilucidar la importancia de los activos de información

**CONFIDENCIALIDAD** se refiere a que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Tabla 3 Clasificación de acuerdo con la confidencialidad

|  |  |
| --- | --- |
| INFORMACIÓN PÚBLICA RESERVADA | Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica. |
| INFORMACION PÚBLICA CLASIFICADA | Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de esta. La información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario |
| INFORMACIÓN PÚBLICA | Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad. |
| NO CLASIFICADA | Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad. |

Fuente: Guía para la Gestión y Clasificación de Activos de Información MINTIC

**INTEGRIDAD**: se refiere a la exactitud y completitud de la información (ISO 27000) esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción.

Tabla 4 Clasificación de acuerdo con la integridad

|  |  |
| --- | --- |
| A (ALTA) | Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad. |
| M (MEDIA) | Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad. |
| B (BAJA) | Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos |
| NO CLASIFICADA | Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad ALTA. |

Fuente: Guía para la Gestión y Clasificación de Activos de Información MINTIC

**DISPONIBILIDAD:** La disponibilidad es la propiedad de la información que se refiere a que ésta debe ser accesible y utilizable por solicitud de una persona entidad o proceso autorizada cuando así lo requiera está, en el momento y en la forma que se requiere ahora y en el futuro, al igual que los recursos necesarios para su uso.

Tabla 5 Clasificación de acuerdo con la disponibilidad

|  |  |
| --- | --- |
| 1 (ALTA) | La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos |
| 2 (MEDIA) | La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad |
| 3 (BAJA) | La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen. |
| NO CLASIFICADA | Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad ALTA. |

Fuente: Guía para la Gestión y Clasificación de Activos de Información MINTIC

1. **Determinar la criticidad del activo: se** debe evaluar la criticidad de los activos, a través de preguntas que le permitan determinar el grado de importancia de cada uno, para posteriormente, durante el análisis de riesgos tener presente esta criticidad para hacer una valoración adecuada de cada caso.

Tabla 6 Niveles de clasificación

|  |  |
| --- | --- |
| (ALTA) | Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta. |
| (MEDIA) | Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio. |
| (BAJA) | Activos de información en los cuales la clasificación de la información en todos sus niveles es baja. |

**Fuente**: Guía para la Gestión y Clasificación de Activos de Información MINTIC

## 5.3. IDENTIFICACIÓN DE RIESGOS

Consiste en determinar qué eventos o riesgos pueden afectar el cumplimiento de los objetivos la entidad y de los procesos.

*¿Qué se debe tener en cuenta para identificar los riesgos?*

* Entender el proceso.
* Identificar el objetivo del proceso.
* Revisar los factores de riesgo detectados en la etapa del análisis del contexto estratégico.
* Identificar “qué puede fallar” para cada actividad clave del proceso.
* Identificar el inventario de activos de información

Una forma práctica de identificar los riesgos del proceso es partiendo del peor escenario, el cual es no lograr el objetivo de la entidad o el proceso, posteriormente se continúa la identificación de otros riesgos tomando como pauta los escenarios negativos para cada una de las salidas y/o productos del proceso.

Con base en el contexto se identifica el riesgo, el cual estará asociado a aquellos eventos o situaciones que pueden entorpecer el normal desarrollo de los objetivos del proceso o los objetivos estratégicos.

Se debe realizar una **descripción** del **riesgo**, ésta debe estar escrita de manera clara, sin que su redacción dé lugar a ambigüedades o confusiones.

PREGUNTAS CLAVES PARA LA IDENTIFICACIÓN DEL RIESGO:

* ¿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

### 5.3.1 REDACCIÓN DE RIESGOS:

Evitar iniciar con palabras negativas como: “No…”, “Que no…”, o con palabras que denoten un factor de riesgo (causa) tales como: “ausencia de”, “falta de”, “poco(a)”, “escaso(a)”, “insuficiente”, “deficiente”, “debilidades en…”

Pregúntese si el riesgo identificado está relacionado directamente con las características del objetivo. Si la respuesta es “no” este puede ser la causa o la consecuencia.

Si el riesgo es de gestión o de corrupción no se deben diligenciar las columnas de activo de información, tipo de amenaza y amenaza

### 5.3.2 TIPOLOGÍA DE RIESGO

Se debe realizar la clasificación de riesgos según su naturaleza en: Estratégicos, operativos, de corrupción, de imagen, operativos, financieros, de cumplimiento, y de tecnología. En el formatomapa de riesgos **DESI-FM-018** seleccione de la lista desplegable el “tipo de riesgo” teniendo en cuenta la siguiente tabla:

Tabla 7 Tipología del Riesgo

| **TIPOLOGÍA DE RIESGOS** | | |
| --- | --- | --- |
| **GESTIÓN** | **Estratégicos** | Son aquellos que se asocian con la posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública y por tanto impactan toda la entidad. |
| **Gerenciales** | Son aquellos que se asocian con la posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o de la alta dirección. |
| **Operativos** | Son aquellos relacionados con posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad. |
| **Financieros** | Son los relacionados con la Gestión Financiera de la entidad, los cuales pueden estar relacionados con la posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, central de cuentas, costos, etc. |
| **De Cumplimiento** | Son aquellos que se asocian con la posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal y las obligaciones contractuales. |
| **Tecnológicos** | Son los relacionados con la posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad. |
| **De imagen** | Están relacionados con la posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización, ante sus clientes y partes interesadas |
| **CORRUPCIÓN** | | Son todos los relacionados con la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado. |
| **RIESGOS DE SEGURIDAD DIGITAL** | | Están relacionados con posibilidad de la combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas. |

Fuente: Adaptado *Guía para la administración del riesgo y el diseño de controles en entidades Públicas. Pág, 28.*

### 5.3.3 IDENTIFICACIÓN DE CAUSAS

Identificar las causas es descubrir todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros. Para lo anterior, con base en el análisis de contexto para la entidad y del proceso, se describen las causas que pueden afectar el logro de los objetivos

* Como mínimo un riesgo debe identificar dos causas.
* Para cada causa debe existir un control.
* Las causas se deben trabajar de manera separada (no se deben combinar en una misma columna o renglón).

Los objetivos estratégicos y de proceso se desarrollan a través de actividades, pero no todas tienen la misma importancia, por lo tanto, se debe establecer cuáles de ellas contribuyen mayormente al logro de los objetivos y estas son las actividades críticas o factores claves de éxito; estos factores se deben tener en cuenta al identificar las causas que originan la materialización de los riesgos

Describir las **consecuencias** **o efectos** resultantes de la materialización del riesgo, sea éste una pérdida, perjuicio, desventaja o ganancia, frente a la consecución de los objetivos de la entidad o del proceso.

### **5.3.4 RIESGOS DE GESTIÓN**

Es aquella posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

Tabla 8 Ejemplos De Riesgo de gestión

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Proceso** | **Riesgo** | **Descripción** | **Tipo de riesgo** | **Tipología de riesgos** | **Activo de información** | **Tipo de**  **amenaza** | **Amenaza** | **Causa / vulnerabilidad** | **Consecuencias** |
|
|
| **Gestión contractual** | Inoportunidad en la adquisición de los bienes y servicios  requeridos por la entidad | La combinación de factores como insu­ficiente capacitación del personal de con­tratos, cambios en la regulación contractual, inadecuadas políticas de operación y caren­cia de controles en el procedimiento de contratación pueden ocasionar inoportunidad en la adquisición de los bienes y servicios requeridos por la enti­dad y, en consecuencia, afectar la continuidad de su operación. | **Gestión** | **Operativo** | **NA** | NA | NA | Carencia de controles en el procedimiento de contratación Insuficiente capacitación del personal de contratos Desconocimiento de los cambios en la regulación contractual Inadecuadas políticas de operación | **1**. Parálisis en los procesos  2. Incumplimiento en la entrega de bienes y servicios a los grupos de valor  3. Demandas y demás acciones jurídicas  4. Detrimento de la imagen de la entidad ante sus grupos de valor  5. Investigaciones disciplinarias |

Fuente: Adaptado, *Guía para la administración del riesgo y el Diseño de controles en Entidades Públicas. Octubre, 2018. Pág. 30.*

### **5.3.5 RIESGOS DE CORRUPCIÓN**

Es necesario que en la descripción del riesgo concurran los componentes de su definición, así:

Tabla 9 Matriz de definición de riesgo de Corrupción

|  |  |  |  |
| --- | --- | --- | --- |
| **Acción u omisión** | **Uso del poder** | **Desviar la gestión de lo público** | **Beneficio privado.** |
| X | X | X | X |

**Fuente:** Adaptado *Guía para la administración del riesgo y el Diseño de controles en Entidades Públicas. Octubre, 2018. P, 24.*

Tabla 10 Ejemplos de Riesgo de Corrupción

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Proceso** | **Riesgo** | **Descripción** | **Tipo de riesgo** | **Tipología de riesgos** | **Activo de información** | **Tipo de amenaza** | **Amenaza** | **Causa / vulnerabilidad** | **Consecuencias** |
|
|
| Gestión contractual | Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre  propio o de terceros con el fin celebrar un contrato | Situaciones como: debilidades en la etapa de la planeación del contrato, la excesiva discrecionalidad, las presiones indebidas, la carencia de controles, la falta de conocimiento y/o experiencia, sumados a la falta de integridad pueden generar un riesgo de corrupción en la contratación, como por ejemplo “exigencias de condiciones en los procesos de selección que solo cumple un determinado proponente”. | Corrupción | Corrupción | NA | NA | NA | Debilidades en la etapa de planeación, que faciliten la inclusión en los estudios previos, y/o en los pliegos de condiciones de requisitos orientados a favorecer a un proponente.  Presiones indebidas.  Carencia de controles  en el procedimiento de  contratación. | 1. Pérdida de la imagen institucional.  2. Demandas contra el Estado.  3. Pérdida de confianza en lo público.  4.Investigaciones penales, disciplinarias y fiscales.  Detrimento patrimonial. |

Fuente: Adaptado *Guía para la administración del riesgo y el Diseño de controles en Entidades Públicas. Octubre, 2018. P, 31.*

### **5.3.6 RIESGOS DE SEGURIDAD DIGITAL**

La identificación de riesgos de seguridad digital consiste en tener consolidado y clasificado los activos de información de la entidad de acuerdo con los atributos de confidencialidad, integridad y disponibilidad que defina el grado o nivel de criticidad que poseen los activos para la entidad.

En esta etapa se identifica las fuentes que originan el riesgo, así como factores internos o externos por los cuales se presentan las vulnerabilidades, amenazas e impactos haciendo uso de métodos como lluvia de ideas, juicios de expertos y análisis de escenarios entre otro. Es necesario lograr identificar los agentes generadores de causas, así como la descripción de los riesgos y las situaciones o consecuencias que se presentan producto de la materialización de los riesgos sobre los procesos de la UAERMV. En razón a esto, las actividades de esta etapa deben ser enfocadas a los riesgos potenciales que ocasionen una incidencia negativa sobre el desarrollo de los objetivos de los procesos estratégicos, misionales, de soporte, de verificación y mejora caracterizados en el mapa de procesos.

Los riesgos de seguridad digital se basan en la afectación de tres criterios en un activo o un grupo de activos dentro del proceso:

* Perdida de Integridad,
* Perdida de Confidencialidad
* Perdida de disponibilidad

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

Tabla 11 Ejemplos de Riesgo de seguridad digital

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Proceso** | **Riesgo** | **Descripción** | **Tipo de riesgo** | **Tipología de riesgos** | **Activo de información** | **Tipo de amenaza** | **Amenaza** | **Causa / vulnerabilidad** | **Consecuencias** |
|
|
| Gestión contractual | Pérdida  de la integridad | La falta de políticas de seguridad digital, ausencia de políti­cas de control de acceso, contraseñas sin protección y mecanismos de autenticación débil, pueden facilitar una modificación no autorizada, lo cual causaría la pérdida de la integridad de la base de datos de nómina. | Seguridad digital | Seguridad digital | Base de datos de nómina | Acciones no autorizadas | Modificación  no  autorizada | Falta de políticas de seguridad digital  Ausencia de políticas de control de acceso  Contraseñas sin protección | Posibles consecuencias que pueda enfrentar la entidad o el proceso a causa de la materialización del riesgo (legales, económicas, sociales, reputacionales, confianza en el ciudadano).  Ej.: posible retraso en el pago de nómina. |

Fuente: Adaptado *Guía para la administración del riesgo y el Diseño de controles en Entidades Públicas. Octubre, 2018. P, 34.*

IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES

Para cada riesgo, se deben asociar el grupo de activos o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. A continuación, se mencionan un listado de amenazas y vulnerabilidades que podrían materializar los tres (3) riesgos previamente mencionados:

Se deben identificar las amenazas de los activos: en la siguiente tabla se listan las amenazas, que representan situaciones o fuentes que pueden hacer daño a los activos y materializar los riesgos. A manera de ejemplo se citan las siguientes amenazas:

Tabla 12 Amenazas más comunes

| **TIPO** | **AMENAZA** |
| --- | --- |
| **Daño físico** | Fuego |
| Agua |
| Contaminación |
| Accidente Importante |
| Destrucción del equipo o medios |
| Polvo, corrosión, congelamiento |
| **Eventos naturales** | Fenómenos climáticos |
| Fenómenos sísmicos |
| Fenómenos volcánicos |
| Fenómenos meteorológicos |
| Inundación |
| **Perdida de los servicios esenciales** | Fallas en el sistema de suministro de agua o aire acondicionado |
| Perdida de suministro de energía |
| Falla en equipo de telecomunicaciones |
| **Perturbación debida a la radiación** | Radiación electromagnética |
| Radiación térmica |
| Impulsos electromagnéticos |
| **Compromiso de la información** | Interceptación de señales de interferencia comprometida |
| Espionaje remoto |
| Escucha encubierta |
| Hurto de medios o documentos |
| Hurto de equipo |
| Recuperación de medios reciclados o desechados |
| Divulgación |
| Datos provenientes de fuentes no confiables |
| Manipulación con hardware |
| Manipulación con software |
| Detección de la posición |
| **Fallas técnicas** | Fallas del equipo |
| Mal funcionamiento del equipo |
| Saturación del sistema de información |
| Mal funcionamiento del software |
| Incumplimiento en el mantenimiento del sistema de información. |
| **Acciones no autorizadas** | Uso no autorizado del equipo |
| Copia fraudulenta del software |
| Uso de software falso o copiado |
| Corrupción de los datos |
| Procesamiento ilegal de datos |
| **Compromiso de las funciones** | Error en el uso |
| Abuso de derechos |
| Falsificación de derechos |
| Negación de acciones |
| Incumplimiento en la disponibilidad del personal |

Fuente: Adaptado Anexo 4 Lineamientos para la Gestión del Riesgo de Seguridad Digital en Entidades Públicas - Guía riesgos 2018

Se deben identificar las vulnerabilidades (debilidades) en la siguiente tabla se lista más comunes:

Tabla 13 Vulnerabilidades más comunes

| **Tipo** | **Vulnerabilidades** |
| --- | --- |
| **Hardware** | Mantenimiento insuficiente |
| Ausencia de esquemas de reemplazo periódico |
| Sensibilidad a la radiación electromagnética |
| Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad) |
| Almacenamiento sin protección |
| Falta de cuidado en la disposición final |
| Copia no controlada |
| **Software** | Ausencia o insuficiencia de pruebas de software |
| Ausencia de terminación de sesión |
| Ausencia de registros de auditoría |
| Asignación errada de los derechos de acceso |
| Interfaz de usuario compleja |
| Ausencia de documentación |
| Fechas incorrectas |
| Ausencia de mecanismos de identificación y autenticación de usuarios |
| Contraseñas sin protección |
| Software nuevo o inmaduro |
| **Red** | Ausencia de pruebas de envío o recepción de mensajes |
| Líneas de comunicación sin protección |
| Conexión deficiente de cableado |
| Tráfico sensible sin protección |
| Punto único de falla |
| **Personal** | Ausencia del personal |
| Entrenamiento insuficiente |
| Falta de conciencia en seguridad |
| Ausencia de políticas de uso aceptable |
| Trabajo no supervisado de personal externo o de limpieza |
| **Lugar** | Uso inadecuado de los controles de acceso al edificio |
| Áreas susceptibles a inundación |
| Red eléctrica inestable |
| Ausencia de protección en puertas o ventanas |
| **Organización** | Ausencia de procedimiento de registro/retiro de usuarios |
| Ausencia de proceso para supervisión de derechos de acceso |

Fuente: Adaptado Anexo 4 Lineamientos para la Gestión del Riesgo de Seguridad Digital en Entidades Públicas - Guía riesgos 2018

Tabla 14 Ejemplos de vulnerabilidades y amenazas

| **TIPO DE ACTIVO** | **EJEMPLOS DE VULNERABILIDADES** | **EJEMPLOS DE AMENAZAS** |
| --- | --- | --- |
| **HARDWARE** | Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento | Incumplimiento en el mantenimiento del sistema de información. |
| Ausencia de esquemas de reemplazo periódico | Destrucción de equipos o medios. |
| Susceptibilidad a la humedad, el polvo y la suciedad | Polvo, corrosión y congelamiento |
| Sensibilidad a la radiación electromagnética | Radiación electromagnética |
| Ausencia de un eficiente control de cambios en la configuración | Error en el uso |
| Susceptibilidad a las variaciones de voltaje | Pérdida del suministro de energía |
| Susceptibilidad a las variaciones de temperatura | Fenómenos meteorológicos |
| Almacenamiento sin protección | Hurtos medios o documentos. |
| Falta de cuidado en la disposición final | Hurtos medios o documentos. |
| Copia no controlada | Hurtos medios o documentos. |
| **SOFTWARE** | Ausencia o insuficiencia de pruebas de software | Abuso de los derechos |
| Defectos bien conocidos en el software | Abuso de los derechos |
| Ausencia de “terminación de sesión” cuando se abandona la estación de trabajo | Abuso de los derechos |
| Disposición o reutilización de los medios de almacenamiento sin borrado adecuado | Abuso de los derechos |
| Ausencias de pistas de auditoria | Abuso de los derechos |
| Asignación errada de los derechos de acceso | Abuso de los derechos |
| Software ampliamente distribuido | Corrupción de datos |
| En términos de tiempo utilización de datos errados en los programas de aplicación | Corrupción de datos |
| Interfaz de usuario compleja | Error en el uso |
| Ausencia de documentación | Error en el uso |
| Configuración incorrecta de parámetros | Error en el uso |
| Fechas incorrectas | Error en el uso |
| Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario | Falsificación de derechos |
| Tablas de contraseñas sin protección | Falsificación de derechos |
| Gestión deficiente de las contraseñas | Falsificación de derechos |
| Habilitación de servicios innecesarios | Procesamiento ilegal de datos |
| Software nuevo o inmaduro | Mal funcionamiento del software |
| Especificaciones incompletas o no claras para los desarrolladores | Mal funcionamiento del software |
| Ausencia de control de cambios eficaz | Mal funcionamiento del software |
| Descarga y uso no controlado de software | Manipulación con software |
| Ausencia de copias de respaldo | Manipulación con software |
| Ausencia de protección física de la edificación, puertas y ventanas | Hurto de medios o documentos |
| Fallas en la producción de informes de gestión | Uso no autorizado del equipo |
| Ausencia de pruebas de envío o recepción de mensajes | Negación de acciones |
| Líneas de comunicación sin protección | Escucha encubierta |
| Tráfico sensible sin protección | Escucha encubierta |
| Conexión deficiente de los cables | Fallas del equipo de telecomunicaciones |
| Punto único de fallas | Fallas del equipo de telecomunicaciones |
| Ausencia de identificación y autentificación de emisor y receptor | Falsificación de derechos |
| Arquitectura insegura de la red | Espionaje remoto |
| Transferencia de contraseñas en claro | Espionaje remoto |
| Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento) | Saturación del sistema de información |
| Conexiones de red pública sin protección | Uso no autorizado del equipo |
| Ausencia del personal | Incumplimiento en la disponibilidad del personal |
| Procedimientos inadecuados de contratación | Destrucción de equipos y medios |
| Entrenamiento insuficiente en seguridad | Error en el uso |
| Uso incorrecto de software y hardware | Error en el uso |
| Falta de conciencia acerca de la seguridad | Error en el uso |
| Ausencia de mecanismos de monitoreo | Procesamiento ilegal de los datos |
| Trabajo no supervisado del personal externo o de limpieza | Hurto de medios o documentos. |
| Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería | Uso no autorizado del equipo |
| **LUGAR** | Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos |  |
| Ubicación en área susceptible de inundación |  |
| Red energética inestable |  |
| Ausencia de protección física de la edificación (Puertas y ventanas) |  |
| **ORGANIZACION** | Ausencia de procedimiento formal para el registro y retiro de usuarios | Abuso de los derechos |
| Ausencia de proceso formal para la revisión de los derechos de acceso | Abuso de los derechos |
| Ausencia de disposición en los contratos con clientes o terceras partes (con respecto a la seguridad) | Abuso de los derechos |
| Ausencia de procedimientos de monitoreo de los recursos de procesamiento de la información | Abuso de los derechos |
| Ausencia de auditorias | Abuso de los derechos |
| Ausencia de procedimientos de identificación y valoración de riesgos | Abuso de los derechos |
| Ausencia de reportes de fallas en los registros de | Abuso de los derechos |
| administradores y operadores |  |
| Respuesta inadecuada de mantenimiento del servicio | Incumplimiento en el mantenimiento del sistema de información |
| Ausencia de acuerdos de nivel de servicio o insuficiencia de estos | Incumplimiento en el mantenimiento del sistema de información |
| Ausencia de procedimientos de control de cambios | Incumplimiento en el mantenimiento del sistema de información |
| Ausencia de procedimiento formal para la documentación del MSPI | Corrupción de datos |
| Ausencia de procedimiento formal para la supervisión del registro del MSPI | Corrupción de datos |
| Ausencia de procedimiento formal para la autorización de la información disponible al público | Datos provenientes de fuentes no confiables |
| Ausencia de asignación adecuada de responsabilidades en seguridad de la información | Negación de acciones |
| Ausencia de planes de continuidad | Falla del equipo |
| Ausencia de políticas sobre el uso de correo electrónico | Error en el uso |
| Ausencia de procedimientos para introducción del software en los sistemas operativos | Error en el uso |
| Ausencia de registros en bitácoras | Error en el uso |
| Ausencia de procedimientos para el manejo de información clasificada | Error en el uso |
| Ausencia de responsabilidad en seguridad de la información en la descripción de los cargos | Error en el uso |
| Ausencia de los procesos disciplinarios definidos en caso de incidentes de seguridad de la información | Hurto de equipo |
| Ausencia de política formal sobre la utilización de computadores portátiles | Hurto de equipo |
| Ausencia de control de los activos que se encuentran fuera de las instalaciones | Hurto de equipo |
| Ausencia de política sobre limpieza de escritorio y pantalla | Hurto de medios o documentos |
| Ausencia de autorización de los recursos de procesamiento de información | Hurto de medios o documentos |
| Ausencia de mecanismos de monitoreo establecidos para las brechas en seguridad | Hurto de medios o documentos |
| Ausencia de revisiones regulares por parte de la gerencia | Uso no autorizado de equipo |
| Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad | Uso no autorizado de equipo |
| Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales. | Uso de software falsificado o copiado |

**Fuente:** ISO 27005

## 5.4 VALORACIÓN DE RIESGOS

En este paso se establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE).

### 5.4.1. ANÁLISIS DE RIESGOS

El análisis del riesgo busca establecer la probabilidad de ocurrencia de los riesgos y el nivel de consecuencias o impacto, calificándolos y evaluándolos con el fin de estimar la zona de riesgo inherente sin controles, ni acciones de tratamiento y ver el grado de exposición al riesgo que tiene la entidad.

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

Para adelantar el análisis del riesgo se deben considerar los siguientes aspectos:

Cálculo de la Probabilidad:

La posibilidad de ocurrencia del riesgo representa el número de veces que el riesgo se ha presentado en un determinado tiempo o puede presentarse. Puede ser medida con criterios de frecuencia o factibilidad

* + Frecuencia: Se analizan el # eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo.
  + Factibilidad: Se analiza la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado, pero es posible que se dé.

Para su determinación se utiliza la tabla de probabilidad

Tabla 15 Criterios parar calificar la probabilidad

|  |  |  |  |
| --- | --- | --- | --- |
| **PROBABILIDAD** | | | |
| **NIVEL** | **DESCRIPTOR** | **DESCRIPCIÓN** | **FRECUENCIA** |
| **5** | **Casi Cierta** | Se espera que el evento ocurra en la mayoría de las circunstancias. | Más de vez al año. |
| **4** | **Probable** | Es viable que el evento ocurra en la mayoría de las circunstancias. | Al menos 1 vez en el último año. |
| **3** | **Posible** | El evento podría ocurrir en algún momento. | Al menos 1 vez en los últimos 2 años. |
| **2** | **Improbable** | El evento puede ocurrir en algún momento. | Al menos 1 vez en los últimos 4 años. |
| **1** | **Raro** | El evento puede ocurrir solo en circunstancias excepcionales. (poco comunes o anormales) | No se ha presentado en los últimos 4 años. |

Fuente: DESI-FM-018 Formato mapa de riesgos por proceso

Para este paso los integrantes del equipo de trabajo designados por el responsable directivo, a menos que posean datos históricos sobre el número de eventos que se hayan materializado en un periodo de tiempo, deben calificar el nivel de probabilidad en términos de factibilidad, se trabajará de acuerdo con la experiencia de los responsables que desarrollan el proceso y de sus factores internos y externos., de acuerdo con la tabla de criterios establecida.

Tabla 16 Matriz de priorización de probabilidad

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Nro** | **RIESGO** | **P1** | **P2** | **P3** | **P4** | **P5** | **Tot** | **PROM** |
| 1 | Inoportunidad en la adquisición de los bienes y servicios requeridos por la entidad |  |  |  |  |  |  |  |
| 2 | Otros riesgos identificados |  |  |  |  |  |  |  |
| 3 | Otros riesgos |  |  |  |  |  |  |  |
| Convenciones: **N.** Numero consecutivo del riesgo - P Participante **Tot:** total puntaje - **Prom.:** promedio | | | | | | | | |

Fuente: *Guía para la administración del riesgo y el Diseño de controles en Entidades Públicas. Octubre, 2018. Pág, 39.*

Cálculo del Impacto:

Hace referencia a las consecuencias que puede ocasionar a la organización la materialización del riesgo; se refiere a la magnitud de sus efectos.

Tabla 17 Criterios para calificar el impacto de riesgos de gestión

| **IMPACTO DE GESTIÓN** | | | |
| --- | --- | --- | --- |
| **Niveles para calificar el impacto** | | **Impacto (consecuencias) Cuantitativo** | **Impacto (consecuencias) Cualitativo** |
| 1 | **Insignificante** | -Impacto que afecte la ejecución presupuestal en un valor ≤0,5%  -Pérdida de cobertura en la prestación de los servicios de la entidad ≤1%.  -Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≤0,5%  -Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≤0,5% del presupuesto general de la entidad. | - No hay interrupción de las operaciones de la entidad.  - No se generan sanciones económicas o administrativas.  - No se afecta la imagen institucional de forma significativa.  **Para el proceso de gestión del laboratorio se deben tener en cuenta adicionalmente los siguientes criterios:**  - No hay interrupción de las operaciones del laboratorio.  - No se afecta la imagen del laboratorio a nivel institucional o distrital de forma significativa. |
| 2 | **Menor** | -Impacto que afecte la ejecución presupuestal en un valor ≤1%  - Pérdida de cobertura en la prestación de los servicios de la entidad ≤5%.  - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≤1%  - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≤1%del presupuesto general de la entidad. | - Interrupción de las operaciones de la Entidad por algunas horas.  - Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias.  - Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.  **Para el proceso de gestión del laboratorio se deben tener en cuenta adicionalmente los siguientes criterios:**  - Interrupción de las operaciones del laboratorio por algunas horas.  - Reclamaciones o quejas de los usuarios o clientes internos que implican investigaciones internas disciplinarias.  - Imagen del laboratorio afectada institucionalmente por retrasos en la prestación del servicio a los usuarios o clientes internos. |
| 3 | **Moderado** | -Impacto que afecte la ejecución presupuestal en un valor ≥5%  - Pérdida de cobertura en la prestación de los servicios de la entidad ≥10%.  - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥5%  - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥5% del presupuesto general de la entidad. | - Interrupción de las operaciones de la Entidad por un (1) día.  - Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad.  - Inoportunidad en la información ocasionando retrasos en la atención a los usuarios.  - Reproceso de actividades y aumento de carga operativa.  - Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos.  - Investigaciones penales, fiscales o disciplinarias.  **Para el proceso de gestión del laboratorio se deben tener en cuenta adicionalmente los siguientes criterios:**  - Interrupción de las operaciones del laboratorio por un (1) día.  - Inoportunidad en la información ocasionando retrasos en la atención a los usuarios o clientes internos.  - Reproceso de actividades y aumento de carga operativa.  - Imagen del laboratorio afectada en el orden institucional o distrital por retrasos en la prestación del servicio a los usuarios o clientes internos. |
| 4 | **Mayor** | -Impacto que afecte la ejecución presupuestal en un valor ≥20%  - Pérdida de cobertura en la prestación de los servicios de la entidad ≥20%.  - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥20%  - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥20% del presupuesto general de la entidad. | - Interrupción de las operaciones de la Entidad por más de dos (2) días.  - Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta.  - Sanción por parte de ente de control u otro ente regulador.  - Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno.  - Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.  **Para el proceso de gestión del laboratorio se deben tener en cuenta adicionalmente los siguientes criterios:**  - Interrupción de las operaciones del laboratorio por más de dos (2) días.  - Incumplimiento en las metas y objetivos del laboratorio afectando el cumplimiento en las metas del proceso.  - Imagen del laboratorio afectada en el orden institucional o distrital por incumplimientos en la prestación del servicio a los usuarios o clientes internos. |
| 5 | **Catastrófico** | -Impacto que afecte la ejecución presupuestal en un valor ≥50% - Pérdida de cobertura en la prestación de los servicios de la entidad ≥50%.  - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥50%  - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto general de la entidad. | Interrupción de las operaciones de la Entidad por más de cinco (5) días.  - Intervención por parte de un ente de control u otro ente regulador.  - Pérdida de Información crítica para la entidad que no se puede recuperar.  - Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal.  - Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.  **Para el proceso de gestión del laboratorio se deben tener en cuenta adicionalmente los siguientes criterios:**  -Interrupción de las operaciones del laboratorio por más de cinco (5) días.  - Pérdida de Información crítica para el laboratorio que no se puede recuperar.  - Incumplimiento en las metas y objetivos del laboratorio. |

Fuente: *Adaptado* *Guía para la administración del riesgo y el Diseño de controles en Entidades Públicas. Octubre, 2018. Págs. 40-41*

* El impacto de un riesgo de corrupción se mide según el efecto que pueda causar el hecho al cumplimiento de los fines de la entidad.

Para medir el impacto se tiene en cuenta los niveles: Catastrófico, Mayor y Moderado, dado que estos riesgos siempre serán significativos; De acuerdo con lo anterior, se deben diligenciar las siguientes preguntas:

Tabla 18. Criterios para determinar impacto de corrupción

| **IMPACTO CORRUPCIÓN** | | | |
| --- | --- | --- | --- |
| **No.** | **SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...** | **RESPUESTA** | |
| **SI** | **NO** |
| 1 | ¿Afectar al grupo de funcionarios del proceso? |  |  |
| 2 | ¿Afectar el cumplimiento de metas y objetivos de la dependencia? |  |  |
| 3 | ¿Afectar el cumplimiento de misión de la Entidad? |  |  |
| 4 | ¿Afectar el cumplimiento de la misión del sector al que pertenece la Entidad? |  |  |
| 5 | ¿Generar pérdida de confianza de la Entidad, afectando su reputación? |  |  |
| 6 | ¿Generar pérdida de recursos económicos? |  |  |
| 7 | ¿Afectar la generación de los productos o la prestación de servicios? |  |  |
| 8 | ¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien o servicios o los recursos públicos? |  |  |
| 9 | ¿Generar pérdida de información de la Entidad? |  |  |
| 10 | ¿Generar intervención de los órganos de control, de la Fiscalía, u otro ente? |  |  |
| 11 | ¿Dar lugar a procesos sancionatorios? |  |  |
| 12 | ¿Dar lugar a procesos disciplinarios? |  |  |
| 13 | ¿Dar lugar a procesos fiscales? |  |  |
| 14 | ¿Dar lugar a procesos penales? |  |  |
| 15 | ¿Generar pérdida de credibilidad del sector? |  |  |
| **16** | **¿Ocasionar lesiones físicas o pérdida de vidas humanas?** |  |  |
| 17 | ¿Afectar la imagen regional? |  |  |
| 18 | ¿Afectar la imagen nacional? |  |  |
| 19 | ¿Generar daño ambiental? |  |  |
| **TOTAL, RESPUESTAS AFIRMATIVAS** | | **0** | |
| Responder afirmativamente de 1 a 5 pregunta(s) genera un impacto **Moderado**  Genera medianas consecuencias sobre la entidad  Responder afirmativamente de 6 a 11 preguntas genera un impacto **Mayor**  Genera altas consecuencias sobre la entidad.  Responder afirmativamente de 12 a 19 preguntas genera un impacto **Catastrófico**.  Genera consecuencias desastrosas para la entidad | | | |

Fuente: *Guía para la administración del riesgo y el Diseño de controles en Entidades Públicas. Octubre, 2018. Pág. 46.*

Si la respuesta a la pregunta 16 es afirmativa, el riesgo inmediatamente se considera catastrófico. Por cada riesgo de corrupción identificado, se debe diligenciar una tabla de estas.

Tabla 19 Criterios para determinar impacto de seguridad digital

| **IMPACTO DE SEGURIDAD DIGITAL** | | |
| --- | --- | --- |
| **Niveles para calificar el impacto** | | **Impacto (consecuencias)  Cualitativo** |
| 1 | **Insignificante** | Sin afectación de la integridad |
| Sin afectación de la disponibilidad |
| Sin afectación de la confidencialidad |
| 2 | **Menor** | Afectación leve de la integridad |
| Afectación leve de la disponibilidad |
| Afectación leve de la confidencialidad |
| 3 | **Moderado** | Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros |
| Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros |
| Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros |
| 4 | **Mayor** | Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros |
| Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros |
| Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros |
| 5 | **Catastrófico** | Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros |
| Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros |
| Afectación muy grave confidencialidad de la información debido al interés particular de los empleados y terceros |

Fuente: Adaptado *Guía para la administración del riesgo y el Diseño de controles en Entidades Públicas. Octubre, 2018. Págs. 42-43.*

### 5.4.2. RIESGO INHERENTE - ANTES DE CONTROLES

El riesgo inherente se establece con la estimación de la probabilidad y el impacto que pueda causar la materialización del riesgo. Se debe ubicar en el mapa de calor el punto de intercepción resultante de la probabilidad y el impacto para establecer el nivel del riego, en el DESI-FM-018: Formato mapa de riesgos de proceso al seleccionar la probabilidad y el impacto de las listas desplegables, se realiza automáticamente la intercepción.

Tabla 20. Mapa de calor

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Probabilidad** | **Mapa De Calor** | | | | |
| **Casi Cierta (5)** | Riesgo  alto | Riesgo  Alto | Riesgo extremo | Riesgo extremo | Riesgo extremo |
| **Probable (4)** | Riesgo moderado | Riesgo  Alto | Riesgo  alto | Riesgo extremo | Riesgo extremo |
| **Posible (3)** | Riesgo bajo | Riesgo moderado | Riesgo  alto | Riesgo extremo | Riesgo extremo |
| **Improbable (2)** | Riesgo bajo | Riesgo bajo | Riesgo moderado | Riesgo  alto | Riesgo extremo |
| **Raro (1)** | Riesgo bajo | Riesgo bajo | Riesgo moderado | Riesgo  alto | Riesgo extremo |
|  | **Insignificante (1)** | **Menor (2)** | **Moderado (3)** | **Mayor (4)** | **Catastrófico (5)** |
|  | **Impacto** | | | | |

Fuente: *Guía para la administración del riesgo y el Diseño de controles en Entidades Públicas. Octubre, 2018. Pág, 45.*

Se toma la calificación de la probabilidad (resultante de la tabla Matriz de priorización de probabilidad), y la calificación de impacto, y se selecciona en la lista desplegable del formato DESI-FM-018 Formato Mapa de Riesgos de Proceso, en donde posteriormente se calcula la zona del **riesgo inherente.**

Tabla 21 Riesgo Inherente

|  |  |  |
| --- | --- | --- |
| **CALIFICACIÓN DEL RIESGO** | | **EVALUACIÓN DEL RIESGO INHERENTE** |
| **PROBABILIDAD** | **IMPACTO** | **ZONA DE RIESGO** |
|  |  |  |

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

### 5.4.3. TRATAMIENTO DEL RIESGO

Es la respuesta establecida por la primera línea de defensa (líderes de los procesos) para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción. A la hora de evaluar las opciones existentes en materia de tratamiento del riesgo,

Los líderes de los procesos tendrán en cuenta la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto de este y la relación costo-beneficio de las medidas de tratamiento.

Pero en caso de que una respuesta ante el riesgo derive en un riesgo residual que supere los niveles aceptables para la dirección, se deberá volver a analizar y revisar dicho tratamiento. En todos los casos para los riesgos de corrupción la respuesta será evitar, compartir o reducir el riesgo. El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías

Tabla 22 Opciones de manejo del riesgo

|  |  |
| --- | --- |
| **Nivel de aceptación** | **Tratamiento** |
| **Aceptar el riesgo.** | No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo.  (**Ningún riesgo de corrupción podrá ser aceptado)** |
| **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 acciones que fortalezcan los controles. |
| **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. |
| **Compartir el riesgo** | Se reduce la probabilidad o el impacto del riesgo, transfiriendo o compartiendo una parte del riesgo. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad. |

Fuente: adaptación *Guía para la administración del riesgo y el Diseño de controles en Entidades Públicas. Octubre, 2018. Pág. 68.*

**Aceptar el riesgo:** Si el nivel de riesgo cumple con los criterios de aceptación de riesgo no es necesario poner controles y este puede ser aceptado. Esto debería aplicar para **riesgos inherentes** en la zona de calificación de riesgo bajo.

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

La menos arriesgada y costosa, pero es un obstáculo para el desarrollo de las actividades de la entidad y, por lo tanto, hay situaciones donde no es una opción.

**Compartir el riesgo**: 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. Cabe señalar que normalmente no es posible transferir la responsabilidad del riesgo.

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.

**Reducir el riesgo**: El nivel de riesgo debería ser administrado mediante el establecimiento de controles, de modo que el riesgo residual se pueda reevaluar como algo aceptable para la entidad. Estos controles disminuyen normalmente la probabilidad y/o el impacto del riesgo.

Para mitigar/tratar los riesgos de seguridad digital se deben emplear como mínimo los controles del anexo A de la ISO/IEC 27001:2013, estos también se encuentran en el anexo 4. “*Lineamientos para la*

*gestión del riesgo de seguridad digital de la presente guía*”.

### 5.4.3.1 Tratamiento de Riesgos de Seguridad Digital

De acuerdo con la valoración de los riesgos de seguridad digital realizada, se determinan las opciones para tratar los riesgos a través de políticas que permitan controlar y hacer seguimiento sobre la gestión realizada a los riesgos con estrategias de tratamiento en donde se tome decisiones para mitigar, retener, transferir o asumir los riesgos. En razón a esto, las formulaciones de políticas deberán contemplar los objetivos a alcanzar, una estrategia de cómo se desarrollarán las políticas a corto, mediano y largo plazo, indicar qué riesgos se van a priorizar y controlar, estimar los recursos necesarios y finalmente hacer seguimiento a la efectividad de las políticas de administración de riesgos de seguridad digital definidas.

### 5.4.4. EVALUACIÓN DE RIESGOS

En esta etapa se busca confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (RIESGO RESIDUAL).

**5.4.5.** DISEÑO DE CONTROLES

Al momento de definir si un control o el conjunto de controles mitigan de manera adecuada el riesgo, se deben considerar, desde la redacción de este, con las siguientes variables:

1. Debe tener definido el **responsable** de realizar la actividad de control. (Debe tener la autoridad, competencias y conocimientos para ejecutar el control dentro del proceso y sus responsabilidades deben ser adecuadamente segregadas o redistribuidas entre diferentes individuos)
2. Debe tener una **periodicidad** definida para su ejecución. (diario, mensual, trimestral, anual, cada vez etc.)
3. Debe indicar cuál es el **propósito** del control (verificar, validar, cotejar, comparar, revisar, etc.) para mitigar la causa de la materialización del riesgo.
4. Debe establecer el **cómo** se realiza la actividad de control.
5. Debe indicar qué pasa con las observaciones o **desviaciones** resultantes de ejecutar el control.
6. Debe dejar **evidencia** de la ejecución del control.

Tabla 23 Ejemplos controles

|  |
| --- |
| **EJEMPLOS** |
| El profesional de contratación cada vez que se va a realizar un contrato verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación, a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el proveedor. En caso de encontrar información faltante, requiere al proveedor a través de correo para el suministro de ésta y así poder continuar con el proceso de contratación. Como evidencia se tiene la respectiva lista de chequeo diligenciada con la información de la carpeta del cliente y correos solicitando la información faltante en los casos que aplique. |
| El auxiliar de cartera mensualmente verifica que los valores recaudados en Banco correspondan con los saldos adeudados por los clientes, extrayendo la información directamente del portal Bancario y generando el reporte de cuentas por cobrar del aplicativo, identificando las cuentas x cobrar pendientes de pago que fueron canceladas según extracto bancario. En caso de observar cuentas de cobro que a la fecha no se han recibido el pago procede a listarlas y realiza llamadas a los clientes solicitando que le indiquen la fecha para el pago oportuno de las mismas. Como evidencia queda el listado de cuentas por cobrar pendientes de pago en Excel con los compromisos acordados con los clientes y el extracto bancario. |

Fuente: *Guía para la administración del riesgo de gestión, Corrupción y seguridad Digital. Octubre, 2018.Pág, 56.*

Para mitigar/tratar los riesgos de seguridad digital, se deben emplear como mínimo los controles del Anexo A de la ISO/IEC 27001:2013, estos también se presentan en la siguiente tabla.

Tabla 24 Controles de referencia para la mitigación de riesgos de seguridad digital

|  |  |  |
| --- | --- | --- |
| **A.5 Políticas de seguridad de la información** | | |
| **A.5.1** | **Directrices establecidas por la dirección para la seguridad de la información** | **Objetivo: Brindar orientación y apoyo por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.** |
| A.5.1.1 | Políticas seguridad  Información de la información | Control: Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los  empleados y partes externas pertinentes. |
| A.5.1.2 | Revisión de las políticas  para seguridad de la información | Control: Las políticas para seguridad de la información se deberían revisar  a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas. |
| **A.6 Organización de la seguridad de la información** | | |
| **A.6.1** | **Organización interna** | **Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.** |
| A.6.1.1 | Roles y responsabilidades para la seguridad de  información | Control: Se deberían definir y asignar todas las responsabilidades de la seguridad de la información. |
| A.6.1.2 | Separación de deberes | Control: Los deberes y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización. |
| A.6.1.3 | Contacto con las autoridades | Control: Se deberían mantener los contactos apropiados con las autoridades pertinentes. |
| A.6.1.4 | Contacto con grupos de interés especial | Control: Es conveniente mantener contactos apropiados con grupos de  interés especial u otros foros y asociaciones profesionales especializadas en seguridad. |
| A.6.1.5 | Seguridad de la información en la gestión  de proyectos | Control: La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto. |
| **A.6.2** | **Dispositivos móviles y teletrabajo** | **Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.** |
| A.6.2.1 | Política para dispositivos móviles | Control: Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles. |
| A.6.2.2 | Teletrabajo | Control: Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo. |

|  |  |  |  |
| --- | --- | --- | --- |
| **A.7 Seguridad de los recursos humanos** | | | |
| **A.7.1** | **Antes de asumir el empleo** | **Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.** | |
| A.7.1.1 | Selección | Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los  riesgos percibidos. | |
| A.7.1.2 | Términos y condiciones del empleo | Control: Los acuerdos contractuales con empleados y contratistas, deberían  establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información. | |
| **A.7.2** | **Durante la ejecución del empleo** | **Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.** | |
| A.7.2.1 | Responsabilidades de la dirección | Control: La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y  procedimientos establecidos por la organización. | |
| A.7.2.2 | Toma de conciencia, educación y formación en la seguridad de la  información | Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las  políticas y procedimientos pertinentes para su cargo. | |
| A.7.2.3 | Proceso disciplinario | Control: Se debería contar con un proceso disciplinario formal el cual  debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información. | |
| **A.7.3** | **Terminación o cambio de empleo** | **Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación del contrato.** | |
| A.7.3.1 | Terminación o cambio de responsabilidades de empleo | Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se  deberían hacer cumplir. | |
| **A.8 Gestión de activos** | | | |
| **A.8.1** | **Responsabilidad por los activos** | **Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.** | |
| A.8.1.1 | Inventario de activos | Control: Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y  mantener un inventario de estos activos. | |
| A.8.1.2 | Propiedad de los activos | Control: Los activos mantenidos en el inventario deberían tener un  propietario. | |
| A.8.1.3 | Uso aceptable activos | Control: Se deberían identificar, documentar e implementar reglas para el  uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información. | |
| A.8.1.4 | Devolución de activos | Control: Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo,  al terminar su empleo, contrato o acuerdo. | |
| **A.8.2** | **Clasificación de la información** | **Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.** | |
| A.8.2.1 | Clasificación información | Control: La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada | |
| A.8.2.2 | Etiquetado información | Control: Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización. | |
| A.8.2.3 | Manejo de activos | Control: Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización. | |
| **A.8.3** | **Manejo de Medios** | **Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios.** | |
| A.8.3.1 | Gestión de medios removibles | Control: Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización. | |
| A.8.3.2 | Disposición de los medios | Control: Se debería disponer en forma segura de los medios cuando ya no  se requieran, utilizando procedimientos formales. | |
| A.8.3.3 | Transferencia de medios  físicos | Control: Los medios que contienen información se deberían proteger contra  acceso no autorizado, uso indebido o corrupción durante el transporte. | |
| **A.9 Control de acceso** | | | |
| **A.9.1** | **Requisitos del negocio para control de acceso** | **Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.** | |
| A.9.1.1 | Política de control de acceso | Control: Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información. | |
| A.9.1.2 | Política sobre el uso de los servicios de red | Control: Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente. | |
| **A.9.2** | **Gestión de acceso de usuarios** | **Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.** | |
| A.9.2.1 | Registro y cancelación del registro de usuarios | Control: Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso. | |
| A.9.2.2 | Suministro de acceso de usuarios | Control: Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios. | |
| A.9.2.3 | Gestión de derechos de  acceso privilegiado | Control: Se debería restringir y controlar la asignación y uso de derechos de  acceso privilegiado. | |
| A.9.2.4 | Gestión de información  de autenticación secreta de usuarios | Control: La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal. | |
| A.9.2.5 | Revisión de los derechos  de acceso de usuarios | Control: Los propietarios de los activos deberían revisar los derechos de  acceso de los usuarios, a intervalos regulares. | |
| A.9.2.6 | Retiro o ajuste de los derechos de acceso | Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de  información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios. | |
| **A.9.3** | **Responsabilidades de los usuarios** | **Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.** | |
| A.9.3.1 | Uso de la información de autenticación secreta | Control: Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta. | |
| **A.9.4** | **Control de acceso a sistemas y aplicaciones** | **Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.** |
| A.9.4.1 | Restricción de acceso información | Control: El acceso a la información y a las funciones de los sistemas de las  aplicaciones se debería restringir de acuerdo con la política de control de acceso. |
| A.9.4.2 | Procedimiento de ingreso seguro | Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro. |
| A.9.4.3 | Sistema de gestión de  contraseñas | Control: Los sistemas de gestión de contraseñas deberían ser interactivos y  deberían asegurar la calidad de las contraseñas. |
| A.9.4.4 | Uso de programas utilitarios privilegiados | Control: Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones. |
| A.9.4.5 | Control de acceso a códigos fuente de programas | Control: Se debería restringir el acceso a los códigos fuente de los programas. |
| **A.10 Criptografía** | | |
| **A.10.1** | **Controles criptográficos** | **Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información** |
| A.10.1.1 | Política sobre el uso de controles criptográficos | Control: Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información. |
| A.10.1.2 | Gestión de llaves | Control: Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su  ciclo de vida. |
| **A.11 Seguridad física y del entorno** | | |
| **11.1** | **Áreas seguras** | **Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.** |
| A.11.1.1 | Perímetro de seguridad física | Control: Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones  de manejo de información. |
| A.11.1.2 | Controles físicos de entrada | Control: Las áreas seguras se deberían proteger mediante controles de  entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado. |
| A.11.1.3 | Seguridad de oficinas,  recintos e instalaciones | Control: Se debería diseñar y aplicar seguridad física a oficinas, recintos e  instalaciones. |
| A.11.1.4 | Protección contra amenazas externas y ambientales | Control: Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes. |
| A.11.1.5 | Trabajo en áreas seguras | Control: Se deberían diseñar y aplicar procedimientos para trabajo en áreas  seguras. |
| A.11.1.6 | Áreas de despacho y carga | Control: Se deberían controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento  de información para evitar el acceso no autorizado. |
| **A.11.2** | **Equipos** | **Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.** |
| A.11.2.1 | Ubicación y protección | Control: Los equipos deberían estar ubicados y protegidos para reducir los |
|  | de los equipos | riesgos de amenazas y peligros del entorno, y las oportunidades para acceso  no autorizado. |
| A.11.2.2 | Servicios de suministro | Control: Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro. |
| A.11.2.3 | Seguridad del cableado | Control: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra  interceptación, interferencia o daño. |
| A.11.2.4 | Mantenimiento de equipos | Control: Los equipos se deberían mantener correctamente para asegurar su  disponibilidad e integridad continuas. |
| A.11.2.5 | Retiro de activos | Control: Los equipos, información o software no se deberían retirar de su  sitio sin autorización previa. |
| A.11.2.6 | Seguridad de equipos y activos fuera de las instalaciones | Control: Se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones. |
| A.11.2.7 | Disposición segura o reutilización de equipos | Control: Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma  segura antes de su disposición o reutilización. |
| A.11.2.8 | Equipos de usuario desatendidos | Control: Los usuarios deberían asegurarse de que a los equipos  desatendidos se les dé protección apropiada. |
| A.11.2.9 | Política de escritorio y pantalla limpios | Control: Se debería adoptar una política de escritorio limpio para los  papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información. |
| **A.12 Seguridad de las operaciones** | | |
| **A.12.1** | **Procedimientos operacionales y responsabilidades** | **Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.** |
| A.12.1.1 | Procedimientos de  operación documentados | Control: Los procedimientos de operación se deberían documentar y poner  a disposición de todos los usuarios que los necesiten. |
| A.12.1.2 | Gestión de cambios | Control: Se deberían controlar los cambios en la organización, en los  procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información. |
| A.12.1.3 | Gestión de capacidad | Control: Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones  de los requisitos sobre la capacidad futura. |
| A.12.1.4 | Separación de los ambientes de desarrollo, pruebas y operación | Control: Se deberían separar los ambientes de desarrollo, prueba y  operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación. |
| **A.12.2** | **Protección contra códigos maliciosos** | **Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.** |
| A.12.2.1 | Controles contra códigos maliciosos | Control: Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los  usuarios, para proteger contra códigos maliciosos. |
| **A.12.3** | **Copias de respaldo** | **Objetivo: Proteger contra la perdida de datos.** |
| A.12.3.1 | Respaldo de información | Control: Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de  acuerdo con una política de copias de respaldo aceptada. |
| **A.12.4** | **Registro y seguimiento** | **Objetivo: Registrar eventos y generar evidencia.** |
| A.12.4.1 | Registro de eventos | Control: Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información. |
| A.12.4.2 | Protección de la información de registro | Control: Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado. |
| A.12.4.3 | Registros del administrador y del operador | Control: Las actividades del administrador y del operador del sistema se  deberían registrar, y los registros se deberían proteger y revisar con regularidad. |
| A.12.4.4 | sincronización de relojes | Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían  sincronizar con una única fuente de referencia de tiempo. |
| **A.12.5** | **Control de software operacional** | **Objetivo: Asegurar la integridad de los sistemas operacionales.** |
| A.12.5.1 | Instalación de software en  sistemas operativos | Control: Se deberían implementar procedimientos para controlar la  instalación de software en sistemas operativos. |
| **A.12.6** | **Gestión de la vulnerabilidad técnica** | **Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.** |
| A.12.6.1 | Gestión de las vulnerabilidades técnicas | Control: Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen;  evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado. |
| A.12.6.2 | Restricciones sobre la  instalación de software | Control: Se deberían establecer e implementar las reglas para la instalación  de software por parte de los usuarios. |
| **A.12.7** | **Consideraciones sobre auditorias de sistemas de información** | **Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.** |
| A.12.7.1 | Información controles de auditoría de sistemas | Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar  cuidadosamente para minimizar las interrupciones en los procesos del negocio. |
| **A.13 Seguridad de las comunicaciones** | | |
| **A.13.1** | **Gestión de la seguridad de las redes** | **Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.** |
| A.13.1.1 | Controles de redes | Control: Las redes se deberían gestionar y controlar para proteger la  información en sistemas y aplicaciones. |
| A.13.1.2 | Seguridad de los servicios de red | Control: Se deberían identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se  presten internamente o se contraten externamente. |
| A.13.1.3 | Separación en las redes | Control: Los grupos de servicios de información, usuarios y sistemas de  información se deberían separar en las redes. |
| **A.13.2** | **Transferencia de información** | **Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.** |
| A.13.2.1 | Políticas y procedimientos de transferencia de información | Control: Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación. |
| A.13.2.2 | Acuerdos sobre transferencia de información | Control: Los acuerdos deberían tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas. |
| A.13.2.3 | Mensajería electrónica | Control: Se debería proteger adecuadamente la información incluida en la  mensajería electrónica. |
| A.13.2.4 | Acuerdos de confidencialidad o de no divulgación | Control: Se deberían identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la  información. |
| **A.14 Adquisición, desarrollo y mantenimientos de sistemas** | | |
| **A.14.1** | **Requisitos de seguridad de los sistemas de información** | **Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.** |
| A.14.1.1 | Análisis y especificación  de requisitos de seguridad de la información | Control: Los requisitos relacionados con seguridad de la información se  deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes. |
| A.14.1.2 | Seguridad de servicios de las aplicaciones en redes  publicas | Control: La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas,  disputas contractuales y divulgación y modificación no autorizadas. |
| A.14.1.3 | Protección de transacciones de los servicios de las aplicaciones | Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debería proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes  no autorizada. |
| **A.14.2** | **Seguridad en los procesos de desarrollo y soporte** | **Objetivo: Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.** |
| A.14.2.1 | Política de desarrollo seguro | Control: Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización. |
| A.14.2.2 | Procedimientos de  control de cambios en sistemas | Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo  se deberían controlar mediante el uso de procedimientos formales de control de cambios. |
| A.14.2.3 | Revisión técnica de las aplicaciones después de cambios en la plataforma  de operación | Control: Cuando se cambian las plataformas de operación, se deberían revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la  organización. |
| A.14.2.4 | Restricciones en los  cambios a los paquetes de software | Control: Se deberían desalentar las modificaciones a los paquetes de  software, que se deben limitar a los cambios necesarios, y todos los cambios se deberían controlar estrictamente. |
| A.14.2.5 | Principios de  construcción de sistemas seguros | Control: Se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información. |
| A.14.2.6 | Ambiente de desarrollo seguro | Control: Las organizaciones deberían establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e  integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas. |
| A.14.2.7 | Desarrollo contratado  externamente | Control: La organización debería supervisar y hacer seguimiento de la  actividad de desarrollo de sistemas contratados externamente. |
| A.14.2.8 | Pruebas de seguridad de  sistemas | Control: Durante el desarrollo se deberían llevar a cabo pruebas de  funcionalidad de la seguridad. |
| A.14.2.9 | Prueba de aceptación de sistemas | Control: Para los sistemas de información nuevos, actualizaciones y nuevas  versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados. |
| **A.14.3** | **Datos de prueba** | **Objetivo: Asegurar la protección de los datos usados para pruebas.** |
| A.14.3.1 | Protección de datos de prueba | Control: Los datos de ensayo se deberían seleccionar, proteger y controlar cuidadosamente. |
| **A.15 Relación con los proveedores** | | |
| **A.15.1** | **Seguridad de la información en las relaciones con los proveedores** | **Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.** |
| A.15.1.1 | Política de seguridad de la información para las relaciones con  proveedores | Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deberían acordar con estos y se deberían documentar. |
| A.15.1.2 | Tratamiento de la seguridad dentro de los acuerdos con proveedores | Control: Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de  infraestructura de TI para la información de la organización. |
| A.15.1.3 | Cadena de suministro de tecnología de información y comunicación | Control: Los acuerdos con proveedores deberían incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y  comunicación. |
| **A.15.2** | **Gestión de la prestación de servicios con los proveedores** | **Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.** |
| A.15.2.1 | Seguimiento y revisión de los servicios de los proveedores | Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores. |
| A.15.2.2 | Gestión de cambios en los servicios de proveedores | Control: Se deberían gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información  existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos. |
| **A.16 Gestión de incidentes de seguridad de la información** | | |
| **A.16.1** | **Gestión de incidentes y mejoras en la seguridad de la información** | **Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.** |
| A.16.1.1 | Responsabilidad y procedimientos | Control: Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los  incidentes de seguridad de la información. |
| A.16.1.2 | Reporte de eventos de seguridad de la información | Control: Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible. |
| A.16.1.3 | Reporte de debilidades de seguridad de la información | Control: Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios. |
| A.16.1.4 | Evaluación de eventos de seguridad de la información y decisiones  sobre ellos | Control: Los eventos de seguridad de la información se deberían evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información. |
| A.16.1.5 | Respuesta a incidentes de seguridad de la información | Control: Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados. |
| A.16.1.6 | Aprendizaje obtenido de los incidentes de seguridad de la información | Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros. |
| A.16.1.7 | Recolección de evidencia | Control: La organización debería definir y aplicar procedimientos para la  identificación, recolección, adquisición y preservación de información que pueda servir como evidencia. |
| **A. 17 Aspectos de seguridad de la información de la gestión de continuidad de negocio** | | |
| **A.17.1** | **Continuidad de seguridad de la información** | **Objetivo: La continuidad de seguridad de la información se debería incluir en los sistemas de gestión de la continuidad de negocio de la organización.** |
| A.17.1.1 | Planificación de la continuidad de la seguridad de la  información | Control: La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o  desastre. |
| A.17.1.2 | Implementación de la continuidad de la seguridad de la información | Control: La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa. |
| A.17.1.3 | Verificación, revisión y evaluación de la continuidad de la seguridad de la  información | Control: La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas. |
| **A.17.2** | **Redundancias** | **Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.** |
| A.17.2.1 | Disponibilidad de instalaciones de procesamiento de información. | Control: Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad. |
| **A. 18 Cumplimiento** | | |
| **A.18.1** | **Cumplimiento de requisitos legales y contractuales** | **Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.** |
| A.18.1.1 | Identificación de la legislación aplicable y de los requisitos  contractuales | Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deberían  identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización. |
| A.18.1.2 | Derechos de propiedad intelectual | Control: Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el  uso de productos de software patentados. |
| A.18.1.3 | Protección de registros | Control: Los registros se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de  negocio. |
| A.18.1.4 | Privacidad y protección de datos personales | Control: Cuando sea aplicable, se deberían asegurar la privacidad y la protección de la información de datos personales, como se exige en la  legislación y la reglamentación pertinente. |
| A.18.1.5 | Reglamentación de controles criptográficos | Control: Se deberían usar controles criptográficos, en cumplimiento de  todos los acuerdos, legislación y reglamentación pertinentes. |
| **A.18.2** | **Revisiones de seguridad de la información** | **Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.** |
| A.18.2.1 | Revisión independiente de la seguridad de la información | Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deberían revisar independientemente a intervalos  planificados o cuando ocurran cambios significativos. |
| A.18.2.2 | Cumplimiento con las políticas y normas de seguridad | Control: Los directores deberían revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y  cualquier otro requisito de seguridad. |
| A.18.2.3 | Revisión del cumplimiento técnico | Control: Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de  la información. |

**Fuente:** *Anexo 4* Lineamientos para la gestión del riesgo de seguridad digital” de la presente guía.

**CLASIFICACIÓN DE CONTROLES**

Las actividades de control, independientemente de la tipología de riesgo a tratar, deben tener una adecuada combinación para prevenir que la situación de riesgo se origine. Ahora, en caso de que la situación de riesgos se presente, esta debe ser detectada de manera oportuna.

**CONTROLES PREVENTIVOS:** Controles que están diseñados para evitar un evento no deseado en el momento en que se produce. Este tipo de controles intentan evitar la ocurrencia de los riesgos que puedan afectar el cumplimiento de los objetivos. **Ejemplo:** Revisión al cumplimiento de los requisitos contractuales en el proceso de selección del contratista o proveedor

**CONTROLES DETECTIVOS:** Controles que están diseñados para identificar un evento o resultado no previsto después de que se haya producido. Buscan detectar la situación no deseada para que se corrija y se tomen las acciones correspondientes. **Ejemplo:** Realizar una conciliación bancaria para verificar que los saldos en libros corresponden con los saldos en bancos.

### 5.4.6. VALORACIÓN DE LOS CONTROLES

Sobre los controles es necesario tener claridad que:

* Una política por sí sola no es un control.
* Los controles se despliegan a través de los procedimientos documentados.
* La actividad de control debe por si sola mitigar o tratar la causa del riesgo y ejecutarse como parte del día a día de las operaciones.
* Para mitigar/tratar los riesgos de seguridad digital, se deben emplear como mínimo los controles incluidos en el documento: *“Lineamientos para la gestión del riesgo de seguridad digital”*

### Evaluación del Diseño del control

Se debe evaluar si el control está bien diseñado de acuerdo con las seis (6) variables establecidas:

Tabla 25 Variables a evaluar para el adecuado diseño de controles

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ¿Existe un responsable asignado a la ejecución del control? | ¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control? | ¿La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna? | ¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo, ejemplo Verificar, Validar Cotejar, Comparar, Revisar, etc.? | ¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo? | ¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna? | ¿Se deja evidencia o rastro de la ejecución del control, que permita a cualquier tercero con la evidencia, llegar a la misma conclusión? | Puntaje |
| * Asignado * No asignado | * Adecuado * Inadecuado | * Oportuna * Inoportuna | * Prevenir * Detectar * No es un control | * Confiable * No confiable | * Se investigan y resuelven oportunamente * No se investigan y resuelven oportunamente | * Completa * Incompleta * No existe | * Fuerte * Moderado * Débil   El formato lo calcula |

Fuente: Adaptado de la *Guía para la administración del riesgo y el Diseño de controles en Entidades Públicas. Octubre, 2018.Pág, 60.*

El resultado de cada variable de diseño va a afectar la calificación del diseño del control, ya que deben cumplirse todas las variables, para que un control se evalúe como fuerte. En el formato mapa de riesgos **DESI-FM-018** se debe seleccionar en la lista desplegable las respuestas para: *“Variables a evaluar para el adecuado diseño de controles”* y en ella las diferentes opciones y el formato calcula el puntaje

Tabla 26 Rango de calificación del diseño

|  |  |
| --- | --- |
| **Rango de calificación del diseño** | **Resultado - peso en la evaluación del diseño del control** |
| **Fuerte** | Calificación entre 96 y 100 |
| **Moderado** | Calificación entre 86 y 95 |
| **Débil** | Calificación entre 0 y 85 |

Fuente: *Guía para la administración del riesgo y el Diseño de controles en Entidades Públicas. Octubre, 2018.Pág 62.*

### Evaluación del Ejecución del control

Para la adecuada mitigación de los riesgos, no basta con que un control esté bien diseñado, el control debe ejecutarse por parte de los responsables tal como se diseñó. Porque un control que no se ejecute, o un control que se ejecute y esté mal diseñado, no va a contribuir a la mitigación del riesgo.

Tabla 26 Criterio para evaluar para la ejecución del control

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **PUNTAJE** | **Evaluación del diseño del control** | **El control se ejecuta de manera consistente por los responsables** | | **Solidez del control** | **Requiere plan de acción para fortalecer el control** | **Solidez del conjunto de controles** |
| El formato lo calcula | El formato lo calcula | **Siempre se ejecuta**  **Algunas veces de ejecuta**  **No se ejecuta** | **Fuerte**  **Moderado**  **Débil**  El formato lo calcula | El formato lo calcula | El formato lo calcula | El formato lo calcula |

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

Aunque un control este bien diseñado, este debe ejecutarse de manera consistente, de tal forma que se pueda mitigar el riesgo. No basta solo con tener controles bien diseñados, debe asegurarse que se ejecute.

Tabla 28 Rango de calificación de la ejecución

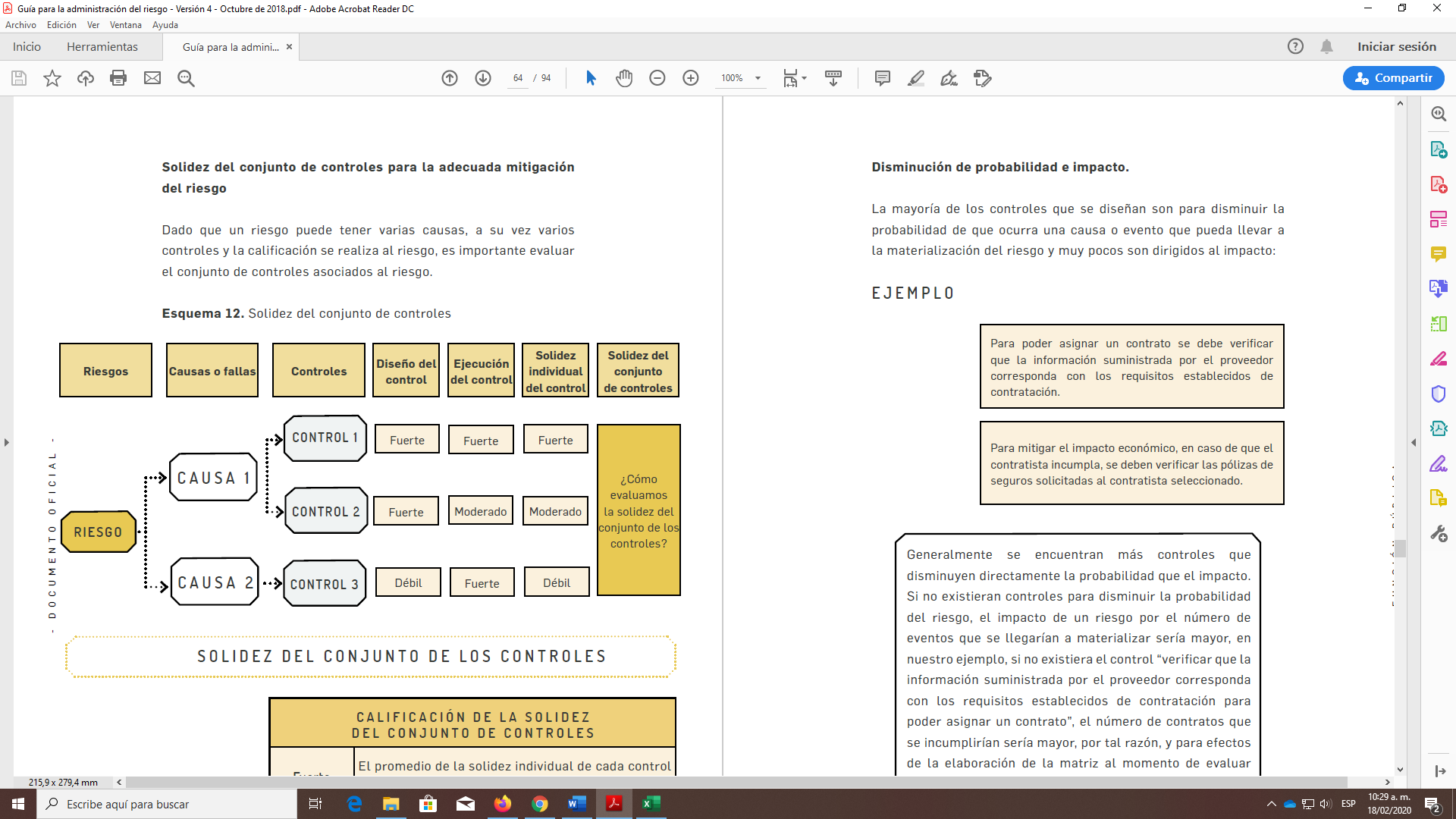
|  |  |
| --- | --- |
| **Rango de calificación del diseño** | **Resultado - peso en la evaluación de la ejecución del control** |
| **Fuerte** | El control se ejecuta de manera consistente por parte del responsable |
| **Moderado** | El control se ejecuta algunas veces por parte del responsable. |
| **Débil** | El control no se ejecuta por parte del responsable. |

Fuente: *Guía para la administración del riesgo y el Diseño de controles en Entidades Públicas. Octubre,*

En el formato mapa de riesgos **DESI-FM-018** se debe seleccionar en la lista desplegable “¿El control se ejecuta de manera consistente por los responsables?”. De esta forma la tabla calcula el valor de la solidez del conjunto de controles

***Nota:*** *La calificación de los controles deberá tener los documentos necesarios que soporten la evaluación suministrada.*

Dado que un riesgo puede tener varias causas y así mismo varios controles, y que la calificación se realiza al riesgo, es importante evaluar el conjunto de controles asociados al riesgo.



Fuente: *Guía para la administración del riesgo y el Diseño de controles en Entidades Públicas. Octubre, 2018. Pág, 64.*

La solidez del conjunto de controles se obtiene calculando el promedio aritmético simple de los controles por cada riesgo.

Tabla 29 Rango de calificación de la solidez de controles

|  |  |
| --- | --- |
| **Calificación de la Solidez del conjunto de controles** | |
| **Fuerte** | El promedio de la solidez individual de cada control al sumarlos y ponderarlos es igual a 100. |
| **Moderado** | El promedio de la solidez individual de cada control al sumarlos y ponderarlos la calificación está entre 50 y 99. |
| **Débil** | El promedio de la solidez individual de cada control al sumarlos y ponderarlos la calificación es menor a 50. |

Fuente: *Guía para la administración del riesgo y el Diseño de controles en Entidades Públicas. Octubre, 2018. Pág, 64.*

### Cálculo del riesgo residual:

Dado que ningún riesgo con una medida de tratamiento se evita o elimina, el desplazamiento de un riesgo inherente en su probabilidad o impacto para el cálculo del riesgo residual se realizará de acuerdo con la tabla de cuadrantes a disminuir después de controles.

Una vez diligenciada la evaluación del diseño y la ejecución de cada uno de los controles, en el formato mapa de riesgos **DESI-FM-018,** se determinarán las casillas a disminuir en probabilidad y/o riesgo, o si por el contrario el riesgo se mantiene ubicado en la misma zona, debido a que los controles son catalogados como débiles de acuerdo con la siguiente tabla:

Tabla 30 Cuadrantes a disminuir después de controles

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Resultados de los posibles desplazamientos de la probabilidad y del impacto de los riesgos.** | | | | |
| **Solidez del conjunto de los controles** | **Controles ayudan a disminuir la probabilidad** | **Controles ayudan a disminuir impacto** | **# Columnas en la matriz de riesgo que se desplaza en el eje de la probabilidad** | **# Columnas en la matriz de riesgo que se desplaza en el eje de impacto** |
| **Fuerte** | Directamente | Directamente | 2 | 2 |
| **Fuerte** | Directamente | Indirectamente | 2 | 1 |
| **Fuerte** | Directamente | No disminuye\* | 2 | 0 |
| **Fuerte** | No directamente | Directamente | 0 | 2 |
| **Moderado** | Directamente | Directamente | 1 | 1 |
| **Moderado** | Directamente | Indirectamente | 1 | 0 |
| **Moderado** | Directamente | No disminuye\* | 1 | 0 |
| **Moderado** | No directamente | Directamente | 0 | 1 |

Fuente: *Guía para la administración del riesgo y el Diseño de controles en Entidades Públicas. Octubre,2018. Pág. 66.*

Generalmente se encuentran más controles que disminuyen directamente la probabilidad que el impacto, si no existieran controles para disminuir la probabilidad del riesgo, el impacto de un riesgo por el número de eventos que se llegarían a materializar seria mayor, por lo que al momento de evaluar los controles estos ayudan a disminuir el impacto de manera indirecta.

\*Tratándose de riesgos de corrupción únicamente hay disminución de probabilidad. Es decir, para el impacto no opera el desplazamiento.

Si la solidez del conjunto de los controles es débil, este no disminuirá ningún cuadrante de impacto o probabilidad asociado al riesgo.

# PLAN DE TRATAMIENTO DE RIESGOS

**Actividades de control**: Son las acciones establecidas a través de políticas y procedimientos que contribuyen a garantizar que se lleven a cabo las instrucciones de la dirección para mitigar los riesgos que inciden en el cumplimiento de los objetivos.

Se establecen las actividades de control, luego se relaciona el soporte con el que se evidenciará el cumplimiento de cada actividad, el responsable de adelantarla (relacionando el cargo y no el nombre), el tiempo específico para cumplir con la actividad o la periodicidad de ejecución.

**Acción de contingencia**

Al final de todas las actividades de control establecidas para atacar las causas del riesgo, se debe relacionar la acción de contingencia a implementar una vez el riesgo se materialice. Se debe colocar el soporte, responsable y tiempo de ejecución, teniendo en cuenta que este tipo de acciones son de aplicación inmediata y a corto plazo para restablecer cuanto antes la normalidad de las actividades para el logro de los objetivos del proceso o la estrategia.

**Indicadores**

Por último, se formulan los indicadores clave de riesgo que permitan monitorear el cumplimiento (eficacia) e impacto (efectividad) de las actividades de control, siempre y cuando conduzcan a la toma de decisiones (por riesgo identificado en los procesos).

# MONITOREO, SEGUIMIENTO Y AJUSTES

**Monitoreo**

Su importancia radica en la necesidad de monitorear permanentemente la gestión del riesgo y la efectividad de los controles establecidos. Porque la entidad debe asegurar el logro de sus objetivos anticipándose a los eventos negativos relacionados con la gestión de la entidad.

* Primera línea - Líderes de los procesos en conjunto con sus equipos deben monitorear y revisar:
* Revisar los cambios en el entorno y como estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de sus procesos, para la actualización del mapa de riesgos de su proceso.
* Revisión del adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos.
* Revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los procedimientos.
* Revisar el cumplimiento de los objetivos de sus procesos y sus indicadores de desempeño, e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos.
* Revisar y reportar a la Oficina Asesora de Planeación, 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 los planes de acción establecidos 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 y lograr el cumplimiento a los objetivos.
* Revisar, hacer seguimiento del cumplimiento de los controles y actividades de mitigación de riesgos, con relación a la gestión

Por lo que remitirán **cuatrimestralmente** a la Oficina Asesora de Planeación el DESI-FM-019 Formato Monitoreo al Mapa de Riesgos por Proceso diligenciado

* Segunda línea - Oficina Asesora de Planeación, supervisores e interventores de contratos o proyectos, responsables de sistemas de gestión, etc. deben monitorear y revisar:
* Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar.
* Revisar el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y determinar las recomendaciones y seguimiento para el fortalecimiento de estos.
* Revisar el perfil de riesgo inherente y residual por cada proceso y consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad.
* Hacer seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos.
* Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelva a materializar el riesgo y lograr el cumplimiento a los objetivos.

Para este monitoreo se usará el DESI-FM-019 formato Monitoreo al Mapa de Riesgos por Proceso, donde se consignarán sus observaciones

* Tercera línea - Oficina de Control Interno, evaluará en sus auditorías internas y/o pruebas de recorrido proporcionando un aseguramiento basado en el más alto nivel de independencia y objetividad

**Seguimiento de riesgos de corrupción**

**Primer seguimiento:** Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días del mes de mayo.

**Segundo seguimiento:** Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de septiembre.

**Tercer seguimiento:** Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de enero.

**Ajustes y modificaciones:**

Se podrán llevar a cabo los ajustes y modificaciones necesarias de los mapas de riesgos integrados (de gestión, corrupción y seguridad digital) de la Unidad, orientadas a mejorar. En este caso deberán dejarse por escrito los ajustes, modificaciones o inclusiones realizadas

De acuerdo con el monitoreo y seguimiento realizado es importante revisar al final de cada vigencia si los Mapas de Riesgos deben ser actualizados o si se mantienen bajo las mismas condiciones en cuanto a factores de riesgo, identificación, análisis y valoración del riesgo. Para poder determinarlo, se analizará si no se han presentado hechos significativos como son:

* Riesgos materializados relacionados con posibles actos de corrupción.
* Riesgos de gestión materializados en cualquiera de los procesos.
* Observaciones o hallazgos por parte de la Oficina de Control Interno o bien por parte de un ente de control, respecto a la idoneidad y efectividad de los controles.
* Cambios importantes en el entorno que puedan generar nuevos riesgos

Para la eliminación de cualquier riesgo el líder del proceso debe presentar una justificación y ésta deberá ser aprobada por el Representante de la Alta Dirección.

# LINEAMIENTOS PARA EL MANEJO DE RIESGOS MATERIALIZADOS

En el evento de materializarse un riesgo, es necesario realizar los ajustes necesarios con acciones tales como:

1. Informar a las autoridades de la ocurrencia del hecho de corrupción. Riesgo de corrupción
2. Aplicar el Plan de contingencia, que se encuentra en el mapa de riesgos del proceso.
3. Se debe volver a realizar la valoración del riesgo (causas, probabilidad, impacto)
4. Revisar controles y ajustar estos.
5. Evaluar si se necesitan nuevos controles
6. Revisar las causas y riesgos y ajustar si es pertinente.
7. Realizar un monitoreo permanente.

**REVISIÓN Y APROBACIÓN:**

|  |  |  |
| --- | --- | --- |
| **Elaborado y/o Actualizado por:** | **Validado por**  **Líderes (Estratégico u Operativo) del Proceso:** | **Aprobado por:** |
| **MARIA NATALIA NORATO MORA**  **Contratista OAP -DESI** | Firma: | Firma: |
| **Acompañamiento Asesor OAP:** |
| **ANDREA DE PILAR ZAMBRANO**  **Contratista OAP- DESI** |
| **MARTHA PATRICIA AGUILAR COPETE**  Jefe Oficina Asesora de Planeación | **MARTHA PATRICIA AGUILAR COPETE**  **Representante Alta Dirección** |

**CONTROL DE CAMBIOS:**

|  |  |  |  |
| --- | --- | --- | --- |
| **VERSIÓN** | **DESCRIPCIÓN** | **FECHA** | **APROBADO**  **Representante de la Alta Dirección** |
| 1 | Se estructura política de riesgo teniendo en cuenta la metodología del Departamento Administrativo de la Gestión Pública DAFP, y el cronograma establecido en el plan anticorrupción y de atención al ciudadano. | ABRIL 2016 | Jefe Oficina Asesora de Planeación |
| 2 | Se ajustó la metodología según lineamientos normativos de Departamento Administrativo de la Gestión Pública DAFP y la Presidencia de la Republica. Se actualiza normatividad MECI:2014 | DICIEMBRE 2016 | MARTHA PATRICIA AGUILAR COPETE |
| 3 | Se ajustó la política, la metodología de identificación evaluación y tratamiento de riesgos conforme a la normatividad vigente | OCTUBRE  2017 | Jefe Oficina Asesora de Planeación |
| 4 | Se actualiza la codificación del documento conforme al nuevo mapa de procesos. | ENERO 2019 | Jefe Oficina Asesora de Planeación |
| 5 | Se actualizo la política de administración de riesgo y su metodología de acuerdo con la Guía para la administración del riesgo de gestión, Corrupción y seguridad Digital y el Diseño de controles en Entidades Públicas agosto de 2018 | ENERO 2019 | Jefe Oficina Asesora de Planeación |
| 6 | Se agregan criterios adicionales para el proceso de gestión del laboratorio en los Criterios para calificar el impacto de riesgos de gestión y se ajustan los lineamientos en caso de materializarse un riesgo | SEPTIEMBRE  2019 | Jefe Oficina Asesora de Planeación |
| 7 | Se ajustó el documento para alinear política a los Lineamientos para la Gestión del Riesgo de Seguridad Digital en Entidades Públicas e incorporar la EGTI-PL-002-V1 Plan de tratamiento de riesgo y EGTI-DI-013V1 política de Seguridad para la gestión de Riesgos | JUNIO 2020 | Martha Patricia Aguilar Copete  Jefe Oficina Asesora de Planeación |

1. Intosai: Guía para las normas de control interno del sector público http://www.Intosai.org [↑](#footnote-ref-2)
2. 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-3)
3. Anexo 4 Lineamientos para la Gestión del Riesgo de Seguridad Digital en Entidades Públicas. [↑](#footnote-ref-4)
4. Anexo 4 Lineamientos para la Gestión del Riesgo de Seguridad Digital en Entidades Públicas. [↑](#footnote-ref-5)