**GUÍA METODOLÓGICA PARA LA ADMINISTRACIÓN DEL RIESGO Y DISEÑO DE CONTROLES**

|  |  |  |  |
| --- | --- | --- | --- |
| encabezado central | **INSTITUTO DISTRITAL DE LA PARTICIPACIÓN Y ACCIÓN COMUNAL** | | |
| **SISTEMA INTEGRADO DE GESTIÓN** | | | |
| **Guía metodológica para la administración del riesgo y diseño de controles** | | | |
| **CÓDIGO:** | IDPAC-DE-GU-01 | **VERSIÓN** | 09 |
| **ELABORÓ** | **REVISÓ** | **APROBÓ** | |
| Karen Lorena Cañizales | Silvia Milena Patiño León  Ana Silvia Olano Aponte | Comité Institucional de Coordinación de Control Interno | |
| Contratista – Oficina Asesora de Planeación | Contratista - Oficina Asesora de Planeación  Jefe Oficina Asesora de Planeación | Comité Institucional de Coordinación de Control Interno | |

| **REGISTRO DE MODIFICACIONES** | | |
| --- | --- | --- |
| **VERSIÓN** | **FECHA** | **DESCRIPCIÓN MODIFICACIÓN** |
| 01 | 10/11/2008 | Versión Original. Nota: Se aclara que esta guía hacia parte del proceso de Mejoramiento continuo del mapa de procesos del IDPAC, la cual llego a la versión 3 |
| 02 | 24/05/2016 | Se actualiza la metodología para la identificación de riesgos y se incluyen lo relacionado con la administración de riesgos institucional, de corrupción y de contratación. |
| 03 | 20/11/2016 | Actualización metodológica de acuerdo con el marco normativo vigente. |
| 04 | 27/08/2018 | Se actualiza la metodología debido a la actualización de la ficha técnica de riesgos. |
| 05 | 14-16/08/2019 | Se actualiza la metodología para la administración del riesgo a partir de los lineamientos del Departamento Administrativo de la Función Pública y las características de la herramienta SIG participo. |
| 06 | 20/05/2020 | Se reorganiza el documento con respecto a las fases de la metodología de administración del riesgo definidas en la Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de gestión, corrupción y seguridad digital. Versión 4 Dirección de Gestión y Desempeño Institucional. Octubre 2018 y el Manual Operativo del Modelo Integrado de Planeación y Gestión. Consejo para la Gestión y Desempeño Institucional. Versión 3. Diciembre de 2019. |
| 07 | 26/03/2021 | Se ajusta parcialmente de acuerdo con la Guía para la Administración del riesgo y el diseño de controles en entidades públicas versión 5 de diciembre 2020. Se ajusta la Declaración de la Política de Administración del Riesgo y se complementaron los objetivos y las definiciones, así mismo se incluye una tabla sobre las responsabilidades por Línea de Defensa |
| 08 | 20/12/2021 | Se ajusta de acuerdo con la Guía para la Administración del Riesgo y el Diseño de Controles en entidades públicas - versión 5 de diciembre 2020. Se complementaron los aspectos contenidos en esta, teniendo en cuenta las dos versiones 2018 y 2020. Se actualizó el objetivo y se eliminaron los objetivos específicos, así mismo se actualizaron los roles y responsabilidades de las líneas de defensa, se desarrollaron los aspectos a tener en cuenta antes de iniciar la metodología, se estructuro la metodología de administración del riesgo en tres pasos: Política del riesgo, Identificación y Valoración. En la declaración de política de administración del riesgo, se cambió la palabra “dueños de proceso” por Lideres de proceso, se actualizaron los nombres de la escala para identificar la probabilidad y el impacto, para el diseño y evaluación de los controles se ajusta tabla de calificación, se desarrolló un capítulo específico para Riesgos de Corrupción, y otro para Riesgos de Seguridad de la Información, se separó de la guía los pasos para registro del riesgo en el aplicativo SIGPARTICIPO, los cuales estarán dispuestos ahora como Manual del Usuario para el Registro de Identificación y Valoración de Riesgos. |
| 09 | 29/12/2022 | Se ajustan las responsabilidades definidas para el esquema de las líneas de defensa, se definieron los lineamientos para el manejo posterior cuando se presenta materialización de riesgos, se incluyó la determinación de la opción de tratamiento para el riesgo, y se ajustó la Política de Riesgos con el fin de acatar las recomendaciones dadas por la Oficina de Control Interno como resultado de la Evaluación del Sistema de Control Interno. |

**TABLA DE CONTENIDO**

[INTRODUCCIÓN 6](#_Toc123259485)

[1. OBJETIVO 8](#_Toc123259486)

[2. DOCUMENTOS DE REFERENCIA 8](#_Toc123259487)

[3. DEFINCIONES 8](#_Toc123259488)

[4. ROLES Y RESPONSABILIDADES 12](#_Toc123259489)

[4.1. Responsabilidades – líneas de Defensa 13](#_Toc123259490)

[5. DESCRIPCIÓN 18](#_Toc123259491)

[5.1. METODOLOGÍA PARA LA ADMINISTRACIÓN DE RIESGOS 18](#_Toc123259492)

[**5.1.1.** **Establecimiento del contexto externo** 19](#_Toc123259493)

[**5.1.2.** **Conocimiento del modelo de operación por procesos de la entidad** 19](#_Toc123259494)

[5.1.2.1 Conocimiento del proceso 19](#_Toc123259495)

[5.1.2.2 Establecimiento del contexto del proceso 19](#_Toc123259496)

[5.2. PASOS DE LA METODOLOGÍA PARA LA ADMINISTRACIÓN DE RIESGOS 20](#_Toc123259497)

[5.2.1. Política de Administración de Riesgos 20](#_Toc123259498)

[5.2.2. Identificación de Riesgos 21](#_Toc123259499)

[**5.2.2.1.** **Fases para identificación de riesgos** 22](#_Toc123259500)

[ Análisis de objetivos estratégicos 22](#_Toc123259501)

[ Análisis del objetivo del proceso 22](#_Toc123259502)

[ Identificar los puntos de riesgo 22](#_Toc123259503)

[ Identificar las causas del riesgo 22](#_Toc123259504)

[ Identificar áreas de impacto 23](#_Toc123259505)

[**5.2.2.2.** **Clasificación del riesgo** 23](#_Toc123259506)

[**5.2.2.3.** **Identificación de áreas de factores de riesgo** 23](#_Toc123259507)

[**5.2.2.4.** **Descripción del riesgo** 31](#_Toc123259508)

[**5.2.2.5.** **Tipos de riesgos** 32](#_Toc123259509)

[5.2.3. Valoración de Riesgos 35](#_Toc123259510)

[**5.2.3.1.** **Análisis del riesgo** 35](#_Toc123259511)

[**5.2.3.2.** **Determine la probabilidad del riesgo** 36](#_Toc123259512)

[**5.2.3.3.** **Determine el impacto del riesgo** 37](#_Toc123259513)

[**5.2.3.4.** **Evaluación de riesgos preliminar** 39](#_Toc123259514)

[**5.2.3.5.** **Valoración de controles** 41](#_Toc123259515)

[**5.2.3.6.** **Estructura para la descripción del control** 41](#_Toc123259516)

[**5.2.3.7.** **Tipología de controles y los procesos** 42](#_Toc123259517)

[**5.2.3.8.** **Análisis y evaluación de los controles – Atributos** 42](#_Toc123259518)

[**5.2.3.9.** **Nivel de riesgo (riesgo residual)** 46](#_Toc123259519)

[**5.2.3.10.** **Estrategias para combatir el riesgo** 47](#_Toc123259520)

[5.2.4. Herramientas para la gestión del riesgo 48](#_Toc123259521)

[**5.2.4.1.** **Gestión de eventos de materialización** 48](#_Toc123259522)

[**5.2.4.2.** **Indicadores clave de riesgo** 49](#_Toc123259523)

[**5.2.4.3.** **Diseño de controles** 50](#_Toc123259524)

[5.2.5. Monitoreo y revisión 52](#_Toc123259525)

[**5.2.5.1.** **Definición del semáforo del riesgo.** 54](#_Toc123259526)

[**5.2.5.2.** **Determinación de la opción de tratamiento para el riesgo** 54](#_Toc123259527)

[5.3. LINEAMIENTOS SOBRE LOS RIESGOS RELACIONADOS CON POSIBLES ACTOS DE CORRUPCIÓN 55](#_Toc123259528)

[5.3.1. Valoración de los riesgos de corrupción 57](#_Toc123259529)

[5.3.2. Análisis de la probabilidad 57](#_Toc123259530)

[5.3.3. Análisis de impacto 58](#_Toc123259531)

[5.3.4. Valoración de los controles – diseño de controles 60](#_Toc123259532)

[5.3.5. Generalidades acerca de los riesgos de corrupción 60](#_Toc123259533)

[5.3.6. Tratamiento del riesgo 60](#_Toc123259534)

[5.3.7. Monitoreo de riesgos de corrupción 62](#_Toc123259535)

[5.3.8. Seguimiento 62](#_Toc123259536)

[5.3.9. Acciones para seguir en caso de materialización de riesgos de corrupción 63](#_Toc123259537)

[5.4. LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 63](#_Toc123259538)

[5.4.1. Identificación de los activos de seguridad de la información 63](#_Toc123259539)

[5.4.2. Identificación del riesgo 65](#_Toc123259540)

[5.4.3. Valoración del riesgo de seguridad de la información 66](#_Toc123259541)

[**5.4.3.1.** **Análisis de la probabilidad del riesgo de seguridad de la información** 66](#_Toc123259542)

[**5.4.3.2.** **Análisis del impacto de seguridad de la información** 67](#_Toc123259543)

[5.4.4. Controles para riesgos de seguridad de la información 69](#_Toc123259544)

[5.5. MAPA DE RIESGOS 70](#_Toc123259545)

[5.6. SOLICITUD DE CREACIÓN, AJUSTES O ELIMINACIÓN 71](#_Toc123259546)

[6. ANEXOS 72](#_Toc123259547)

# INTRODUCCIÓN

El Comité Institucional de Coordinación de Control Interno aprobó la versión número 8 de la “Guía para la administración del riesgo y el diseño de controles”, elaborada por la Oficina Asesora de Planeación para precisar algunos elementos metodológicos hacia la mejora del ejercicio de identificación y valoración del riesgo. Esta nueva versión se estructuró bajo los tres pasos principales que ha venido enseñando el Departamento Administrativo de la Función Pública en sus “Guías para la administración del riesgo y el diseño de controles en entidades públicas” - versión de octubre de 2018 y versión 5 de diciembre de 2020, una vez entro en vigencia el Modelo Integrado de Planeación y Gestión (MIPG), que integró los sistemas de gestión de la calidad y de desarrollo administrativo; se creó un único sistema de gestión articulado con el sistema de control interno, el cual se actualiza y alinea con los mejores estándares internacionales, como son el modelo COSO 2013, COSO ERM 2017 y el modelo de las tres líneas de defensa.

La metodología de administración del riesgo, precisa los elementos metodológicos para mejorar el ejercicio de identificar, analizar, valorar, establecer controles, responsables y formular los planes de tratamiento de riesgos de gestión, corrupción, contratación, defensa jurídica, seguridad digital, seguridad y salud en el trabajo, ambientales, entre otros, considerando la planeación estratégica de la entidad, el análisis del contexto interno y externo como preámbulo a la aplicación de la metodología general bajo los tres pasos principales.

Después de forma metodológica, se desarrolla el paso 1, Política de administración del riesgo, el cual es esencial en cabeza de la alta dirección de la entidad, en tanto que da fundamento a la gestión del riesgo en todos los niveles organizacionales; posteriormente en el paso 2 se realiza la identificación del riesgo, teniendo en cuenta la estructura para la redacción adecuada del mismo, facilitando así el análisis de la causa raíz y se hacen señalamientos básicos para evitar errores o generalizaciones del riesgo que dificultan la aplicación de los pasos siguientes definidos en la metodología. En este paso, se agrega una nueva tabla de análisis a partir de la cual se calcularán los movimientos en la matriz de calor; también se especifican los factores de riesgo y su relación con las tipologías de riesgo.

La valoración del riesgo, que establece los criterios para el análisis de probabilidad e impacto del riesgo identificado y su respectivo nivel de rigidez, se desarrollan en el paso 3, donde se presenta la tabla para el análisis de probabilidad con un enfoque en la exposición al riesgo, análisis que le permite a los líderes de cada uno de los procesos, emplear elementos objetivos para su definición; en cuanto a la tabla de impacto se consideran la afectación económica y reputacional como aspectos principales frente a la posible materialización de los riesgos.

Los resultados del desarrollo metodológico de cada uno de los pasos, señalados en esta guía, deben ser registrados en el aplicativo SIGPARTICIPO, siguiendo lo definido en el Instructivo para el manejo del Módulo de Riesgos, sobre la administración del riesgo, factores de riesgo, criterios asociados al contexto interno y externo, periodicidad para la actualización de los mapas de riesgos y su monitoreo, niveles de aceptación y manejo, tabla de impactos, criterios de calificación del impacto, entre otros.

Se espera optimizar y enfocar los esfuerzos institucionales en acciones estandarizadas que permitan abordar y tratar los riesgos identificados en forma eficaz y efectiva en coherencia con la realidad estratégica de la entidad.

# OBJETIVO

Establecer la política y las acciones a aplicar por cada uno de los procesos de la entidad para la administración de los riesgos, con el fin de prevenir su ocurrencia o minimizar su impacto y afectación al cumplimiento de la misión de la entidad así como los objetivos estratégicos de acuerdo con lo establecido por el Departamento Administrativo de la Función Pública (DAFP) en las Guías vigentes para la Administración del riesgo y el diseño de controles en entidades públicas, mediante un ejercicio de identificación, análisis, evaluación, valoración, tratamiento, seguimiento y control de los riesgos

# DOCUMENTOS DE REFERENCIA

* Anexo 4. Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas. <https://www.funcionpublica.gov.co/documents/418548/34316316/Anexo+4+Lineamientos+para+la+Gestion+del+Riesgo+de++Seguridad+Digital+en+Entidades+P%C3%BAblicas+-+Gu%C3%ADa+riesgos+2018.pdf/1ce5099d-c5e5-8ba2-00bc-58f801d3657b>
* Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5. Diciembre de 2020. [file:///C:/Users/jrivera/Downloads/Gu%C3%ADa%20para%20la%20administraci%C3%B3n%20del%20riesgo%20y%20el%20dise%C3%B1o%20de%20controles%20en%20entidades%20p%C3%BAblicas%20-%20Versi%C3%B3n%205%20-%20Diciembre%20de%202020.pdf](file:///C:\Users\spatino\jrivera\Downloads\GuÃ­a%20para%20la%20administraciÃ³n%20del%20riesgo%20y%20el%20diseÃ±o%20de%20controles%20en%20entidades%20pÃºblicas%20-%20VersiÃ³n%205%20-%20Diciembre%20de%202020.pdf)

# DEFINCIONES

Para la administración del riesgo en el Instituto Distrital de la Participación y Acción Comunal, se tendrán en cuenta los siguientes términos y definiciones:

| **Término** | **Definición** |
| --- | --- |
| Activo | En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital. |
| Administración de riesgos | Conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos. |
| Amenaza | Situación externa que no controla la entidad y que puede afectar su operación. |
| Apetito de riesgo | Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar. |
| Calificación del riesgo | Estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización. |
| Capacidad de riesgo | Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad. |
| Causa | Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo  Medios, circunstancias y/o agentes que generan riesgos |
| Causa inmediata | Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo. |
| Causa raíz | Causa principal o básica, corresponde a las razones por la cuales se puede presentar |
| Confidencialidad | Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados |
| Consecuencia | Son 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. |
| Control | Acción o conjunto de acciones que minimiza la probabilidad de ocurrencia o el impacto del riesgo.  Medida que permite reducir o mitigar un riesgo. |
| Control preventivo | Acción o conjunto de acciones que eliminan o mitigan las causas del riesgo; está orientado a disminuir la probabilidad de ocurrencia del riesgo. |
| Contexto de la organización | Corresponde a la determinación de las cuestiones externas e internas que son pertinentes para la gestión institucional y que pueden afectar el logro de los resultados previstos. |
| Debilidad | Situación interna que la entidad puede controlar y que puede afectar su operación. |
| Disponibilidad | Propiedad de ser accesible y utilizable a demanda por el riesgo. |
| Evaluación del riesgo | Resultado del cruce cuantitativo de la calificación de impacto y probabilidad, para establecer la zona donde se ubicará el riesgo. |
| Eventos potenciales | Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.  Evento que tendrá un impacto sobre los objetivos institucionales o del proceso. Se expresa en términos de probabilidad y consecuencias. |
| Factores de riesgo | Son las fuentes generadoras de riesgos |
| Frecuencia | Ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado. |
| Identificación del riesgo | Etapa de administración del riesgo donde se definen los riesgos con sus causas, agentes generadores asociados a las causas, consecuencias, definición de productos y/o servicios que pueden afectarse con la materialización del riesgo, situaciones de deño antijurídico y clasificación. |
| Impacto | Las consecuencias que puede ocasionar a la organización la materialización del riesgo. |
| Integridad | Propiedad de exactitud y completitud |
| Mapa de riesgos | Organización sistemática que muestra el desarrollo de las etapas de la administración del riesgo. |
| Mapa de riesgos de corrupción | Herramienta metodológica para identificar un conjunto sistemático de situaciones de índole administrativa que, por sus características, pueden originar prácticas corruptas, orientan programas de prevención de la corrupción, constituye una opción en la labor de los administradores cuando enfrentan la dirección o conducción de una organización o entidad particular. |
| Materialización del riesgo | Ocurrencia del riesgo identificado. |
| Nivel de riesgo | Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.  En general la fórmula del Nivel del Riesgo poder ser Probabilidad \* Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto. |
| Observaciones o desviaciones del control | Hace referencia a las acciones que deben tomarse, una vez se aplica el control y se evidencia algún incumplimiento en el proceso controlado; la actividad no debería continuarse hasta que se subsane la situación; si es un control que detecta una posible materialización de un riesgo, deberían gestionarse de manera oportuna los correctivos o aclaraciones a las diferencias presentadas u observaciones. |
| Política de administración del riesgo | Conjunto de lineamientos y directrices para la gestión del riesgo en la entidad. Es la declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo. |
| Probabilidad | Es la medida para estimar cuantitativa y cualitativamente la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año. |
| Proceso | Conjunto de operaciones secuenciales que realiza permanentemente la entidad para generar productos/servicios a sus usuarios internos y externos a partir de unos insumos determinados. |
| Producto y/o servicio | Cualquier bien material o servicio final que se genera con la operación de un proceso institucional, orientado a satisfacer la necesidad de un grupo de valor interno o externo. |
| Requisitos legales y otros requisitos | Necesidad o expectativa establecida, generalmente implícita u obligatoria que una organización debe cumplir y otros que una organización decide cumplir. |
| Reducir el riesgo | Opción de manejo que determina la formulación de acciones donde se prevenga la materialización del riesgo mediante el fortalecimiento de controles identificados. |
| Riesgo | Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. |
| 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 gestión | Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos de los procesos o sobre su operación. |
| Riesgo de seguridad digital | Combinación de amenazas y vulnerabilidades en el entorno digital. Puede 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. |
| Riesgo de seguridad y salud en el trabajo | Son aquellos eventos que puedan afectar la seguridad y la salud en los espacios laborales. |
| Riesgos de seguridad y privacidad de la información | Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000). |
| Riesgo inherente | Nivel de riesgo propio de la actividad dentro de una escala de severidad y se obtiene de combinar la probabilidad con el impacto. |
| Riesgo residual | El resultado de aplicar la efectividad de los controles al riesgo inherente. Es el nivel de riesgo que permanece luego de determinar controles para su administración. |
| SIGPARTICIPO | Herramienta oficial para la documentación y administración de los riesgos mediante el módulo de “Gestión del riesgo”. |
| Tolerancia del riesgo. | Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad |
| Valoración del riesgo | Establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización. Es aquí donde se determina el riesgo residual, la opción de manejo a seguir si es necesario y las acciones a desarrollar para el fortalecimiento de controles. |
| Vulnerabilidad | Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas. |
| Capacidad de riesgo | Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por parte de Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad. |

# ROLES Y RESPONSABILIDADES

El éxito de la administración del riesgo depende de la activa participación de la Alta dirección, sus directivos, funcionarios y contratistas, diferentes grupos de valor y/o partes interesadas. Por ello, es preciso identificar los actores que intervienen, de acuerdo con los lineamientos establecidos en el Modelo Integrado de Planeación y Gestión - MIPG, a partir de la estructuración de las líneas de defensa que se presentan a continuación:



Oficinas de Control Interno

3ª Línea de Defensa

Jefe de planeación, coordinadores de equipos de trabajo, comité de contratación, área financiera, TIC y los que generen información para la operación.

Línea Estratégica

2ª. Línea de Defensa

Alta Dirección y Comité Institucional de Coordinación Institucional

**Medidas de Control Interno.** Controles del día a día. Ejecutados por el equipo de trabajo.

**Controles de Gerencia:** Ejecutados por el jefe.

1ª. Línea de

Defensa

**Ilustración 1.** Roles y responsabilidades frente a la administración del riesgo.

## **Responsabilidades – líneas de Defensa**

Modelo de control que establece los roles y responsabilidades de todos los actores del riesgo en una entidad, este proporciona aseguramiento de la gestión y previene la materialización de los riesgos en todos sus ámbitos.

La responsabilidad frente a la gestión del riesgo está definida mediante las líneas de defensa, así:

| **LÍNEA DE DEFENSA** | **RESPONSABLE** | **ROLES - RESPONSABILIDAD** |
| --- | --- | --- |
| Estratégica | Alta Dirección  Comité Institucional de Coordinación de Control Interno. | 1. Definir y aprobar la política para la administración del riesgo mínimo una vez al año. 2. Asumir la responsabilidad primaria del nivel de implementación del Sistema de Control Interno de la entidad, e identificar y evaluar los cambios que podrían tener un impacto significativo en la implementación de este. 3. Evaluar y dar línea sobre la administración de los riesgos, a través del Comité Institucional de Coordinación de Control Interno - CICCI. 4. Incluir en las sesiones del CICCI (en el marco del Comité Institucional de Gestión y Desempeño - CIGD) el reporte de las evaluaciones realizadas a los controles de los riesgos por parte de la segunda y tercera línea de defensa y las acciones de mejora que se han tomado a partir de esta evaluación. 5. Definir y hacer seguimiento a los niveles de aceptación (apetito al riesgo), teniendo en cuenta cada uno de los objetivos establecidos. 6. Analizar los riesgos y amenazas institucionales, que puedan afectar el cumplimiento del Plan Estratégico institucional - PEI. 7. Establecer objetivos institucionales alineados con el propósito fundamental, metas y estrategias de la entidad. 8. Analizar el impacto sobre el control interno por cambios en los diferentes niveles organizacionales. 9. A partir de la información consolidada y reportada por la 2a línea de defensa, analizar los resultados de la gestión del riesgo y especialmente en el caso de que se han presentado materializaciones de riesgos. 10. Acorde con el análisis del entorno interno y externo, definir los procesos, programas o proyectos (según aplique), susceptibles de posibles actos de corrupción. |
| Primera línea | Líderes de Procesos Estratégicos, Misionales, de Apoyo y de Seguimiento y Evaluación. | 1. Identificar, valorar y actualizar, cuando se requiera, los riesgos que pueden afectar el logro de los objetivos institucionales. 2. Retroalimentar a la Alta dirección sobre el monitoreo y efectividad de la gestión del riesgo y de los controles. Así mismo, hacer seguimiento a la gestión de sus riesgos y aplicar los controles, a través del CICCI. 3. Monitorear mínimo una vez al año los factores internos y externos definidos por la entidad, con el fin de establecer cambios en el entorno que determinen nuevos riesgos o ajustes a los existentes. 4. Monitorear la gestión del riesgo y de los controles, acorde con la política de administración de riesgo. 5. 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. 6. Definir, diseñar, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados, y determinar las acciones de mejora a que haya lugar. 7. Establecer sistemas de gestión de riesgos al interior de los procesos a partir de la política de administración del riesgo, fijando las responsabilidades para controlar riesgos específicos bajo la supervisión de la alta dirección, con base en esto, se construye el mapa de riesgos de cada proceso. 8. Identificar y controlar los riesgos relacionados con posibles actos de corrupción en el ejercicio de sus funciones y el cumplimiento de sus objetivos, así como en la prestación del servicio y/o relacionados con el logro de los objetivos. 9. Identificar, disuadir y detectar fraudes; revisar la exposición de la entidad al fraude de acuerdo con los informes generados por la oficina de Control Interno de la entidad. 10. Informar a la Oficina Asesora de Planeación (segunda línea) sobre los riesgos materializados en los objetivos institucionales. 11. Reportar en el aplicativo SIGPARTICIPO los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos. 12. Generar plan de manejo de riesgos para la gestión y tratamiento. 13. Evaluar la estructura de control a partir de los cambios en procesos, procedimientos, u otras herramientas, a fin de garantizar su adecuada formulación y afectación frente a la gestión del riesgo. |
| Segunda línea | Oficina Asesora de Planeación, coordinadores de equipos de trabajo, Secretaria General – Gestión Financiera, Tecnologías de la Información, Gerentes de proyectos de inversión, Comité de contratación, Comité de Conciliación | 1. Asesorar a la línea de defensa estratégica en cabeza de la Oficina Asesora de Planeación en el análisis del contexto interno y externo, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo residual. 2. Consolidar el mapa de riesgos institucional a través de la Oficina Asesora de Planeación, incluyendo riesgos de mayor criticidad frente al logro de los objetivos y presentarlo para análisis y seguimiento ante el CICCI. 3. Consolidar los seguimientos a los mapas de riesgo, mediante el aplicativo SIGPARTICIPO. 4. Informar sobre los eventos en la administración de los riesgos que afectan el logro de los objetivos y evaluar si la valoración del riesgo es la apropiada. 5. Hacer seguimiento a la aplicación de los controles tal como han sido diseñados definidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos, asegurándose desde la Oficina Asesora de Planeación que funcionen correctamente. 6. Verificar que las evaluaciones de riesgo y control incluyan riesgos de fraude. 7. Verificar que la gestión de los riesgos se encuentre articulada con la política de administración de riesgos de la entidad. 8. Monitorear cambios en el riesgo legal, regulatorio y de cumplimiento a través de los supervisores e interventores de contratos o proyectos y del comité de contratación. 9. Realizar seguimiento por parte de los supervisores e interventores a los riesgos de los contratos o proyectos e informar las alertas respectivas. 10. Identificar, analizar, valorar y evaluar los riesgos y controles asociados a su gestión con enfoque en la prevención del daño antijurídico bajo responsabilidad del Comité de Conciliación y Defensa Judicial. 11. Monitorear de acuerdo a la periodicidad los riesgos, revisando que sus condiciones no hayan cambiado y definir su pertinencia para sostenerlos o ajustarlos, a través del CICCI. 12. Asesorar a la primera línea de defensa, sobre la identificación y/o actualización de riesgos, evaluar la adecuación de los controles a las especificidades de cada proceso, considerando cambios en regulaciones, estructuras internas u otros aspectos que determinen cambios en su diseño. 13. Evaluar la planeación estratégica, considerando alertas frente a posibles incumplimientos, necesidades de recursos, cambios en el entorno que puedan afectar su desarrollo, entre otros, aspectos que garanticen de forma razonable su cumplimiento. 14. Revisar y evaluar que la Política para la administración del Riesgo, cumpla con los aspectos definidos por el DAFP, mínimo una vez al año. 15. Hacer seguimiento al Plan de Manejo de Riesgos Institucional. |
| Tercera línea | Oficina de Control Interno | 1. Asesorar en metodologías para la identificación y administración de los riesgos, en coordinación con la segunda línea de defensa. 2. Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos. 3. Revisar la efectividad y la aplicación de controles, planes de contingencia y actividades de monitoreo vinculadas a riesgos claves de la entidad 4. Identificar y evaluar cambios que podrían tener un impacto significativo en el Sistema de Control Interno, durante las evaluaciones periódicas de riesgos y en el curso del trabajo de auditoría interna. 5. Comunicar al Comité de Coordinación de Control Interno posibles cambios e impactos en la evaluación del riesgo, detectados en las auditorías. 6. Alertar sobre la probabilidad de riesgo de fraude o corrupción en las áreas auditadas. |

De manera complementaria, la Oficina Asesora de Planeaciónlleva a cabo las siguientes acciones:

* Socializar anualmente la metodología de riesgos.
* Asesorar al grupo enlace de cada proceso sobre el uso del aplicativo SIG PARTICIPO para la gestión del riesgo.
* Liderar las mesas de trabajo para identificación del riesgo.
* Socializar entre los servidores de la entidad el mapa de riesgos institucional.
* Consolidar el mapa de riesgos institucional.
* Publicar en el portal web, el mapa de riesgos institucional.

Por su parte, los líderes de proceso tienen la responsabilidad de:

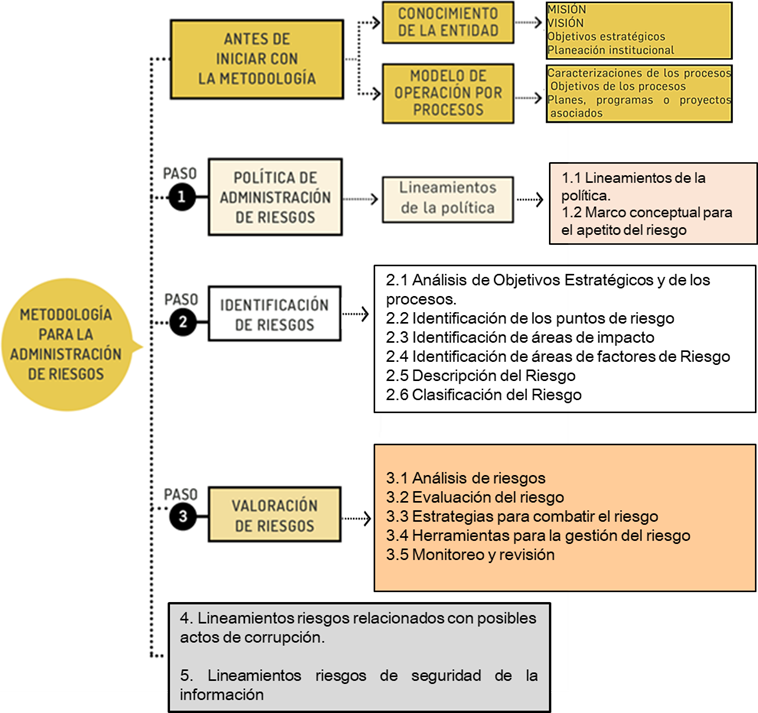
* Asegurarse que al interior de su grupo de trabajo se conozca el concepto de “Administración del riesgo”, la política y la metodología definida, los actores y el entorno del proceso aprobados por la primera línea de defensa.
* Delegar, el (los) funcionarios y contratistas responsables del monitoreo, reporte y socialización del riesgo asociado.

# DESCRIPCIÓN

# METODOLOGÍA PARA LA ADMINISTRACIÓN DE RIESGOS

La gestión de administración de riesgos de la entidad, señalado en la presente guía desarrolla una metodología para gestionar todos los riesgos de la entidad, teniendo en cuenta las particularidades de cada uno de acuerdo con su tipología y con los requerimientos normativos existentes.

A continuación, se muestra la estructura completa con sus desarrollos básicos en cada uno de los pasos:



**Fuente:** *Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.*

Antes de iniciar el desarrollo de la metodología de administración del riesgo en la entidad y garantizar una adecuada identificación de los riesgos de los procesos, es primordial tener claridad sobre el direccionamiento estratégico de esta, el cual se constituye en la base para una adecuada identificación de los riesgos que pueden afectar el cumplimiento de los objetivos institucionales y de proceso.

Para lo cual, se recomienda tener claridad de los siguientes aspectos:

### **Establecimiento del contexto externo**

Se determinan las características o aspectos esenciales del entorno en el cual opera la entidad. Se deben considerar factores: políticos, económicos y financieros, sociales y culturales, tecnológicos, ambientales, legales y reglamentarios; contenidos en el Plan Estratégico Institucional vigente.

### **Conocimiento del modelo de operación por procesos de la entidad**

Es el estándar organizacional que soporta la operación de la entidad, integrando las competencias legales contenidos en el Acuerdo Distrital 257 de 2006, el cual le da vida jurídica al Instituto Distrital de la Participación y Acción Comunal - IDPAC, por tanto, rige en conjunto los planes necesarios para el cumplimiento de la misión, visión, objetivos institucionales y de los procesos. Lo anterior se encuentra determinado de manera gráfica en el mapa o red de procesos de la entidad disponible en el aplicativo SIGPARTICIPO, desde donde se puede acceder entre otros a los documentos que soportan la operación de cada proceso.

#### 5.1.2.1 Conocimiento del proceso

Se deben analizar los factores internos y externos que pueden generar riesgos que afecten el cumplimiento del objetivo del proceso, la herramienta básica para el análisis del contexto del proceso es la caracterización de este, donde es posible visibilizar su alcance y aplicación.

Se recomienda la revisión periódica de la caracterización del proceso, para actualizarlo de ser requerido.

#### 5.1.2.2 Establecimiento del contexto del proceso

Se determinan las características o aspectos esenciales del proceso y sus interrelaciones, para lo cual se deben considerar factores como:

* Objetivo del proceso. Se encuentra definido en su caracterización.
* Alcance del proceso
* Interrelación con otros procesos
* Procedimientos asociados
* Líder del proceso
* Activos de seguridad digital del proceso
* Objetivos de Proyectos de inversión asociados al proceso: Se encuentran definidos el documento de formulación del proyecto de inversión, ficha EBID y ficha MGA.

# PASOS DE LA METODOLOGÍA PARA LA ADMINISTRACIÓN DE RIESGOS

PASO 1

## **Política de Administración de Riesgos**

En este paso se formula la Política de Administración del Riesgo, adoptada en la entidad como parte integral de esta guía; que es la declaración de la dirección de la entidad con el liderazgo del representante legal y la participación del Comité Institucional de Coordinación de Control Interno - CICCI; la cual contiene las intenciones generales respecto a la gestión del riesgo, establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos, a saber:

***“La alta dirección, funcionarios y contratistas del Instituto Distrital de la Participación y Acción Comunal – IDPAC, se comprometen a realizar gestión a los riesgos relacionados con las actividades a ejecutar desde los procesos estratégicos, misionales, de apoyo y de seguimiento y evaluación, para garantizar el cumplimiento de los objetivos institucionales, de proceso y la transparencia en la gestión. La entidad en su tarea de implementar la adecuada gestión de los riesgos requiere que los líderes de los procesos monitoreen los riesgos de acuerdo con la periodicidad definida en los controles, así como hacer seguimiento mínimo una vez al año los factores internos y externos, a fin de establecer nuevos riesgos o ajustes a los existentes; teniendo en cuenta la importancia del riesgo que ha sido identificado, analizando el efecto que puede tener sobre la entidad, la probabilidad e impacto y la relación costo-beneficio de las medidas de tratamiento que podrán ser aceptar, reducir, evitar y/o compartir el riesgo. Los riesgos de corrupción son inaceptables y en consecuencia no se pueden asumir, en todo caso se deberán adelantar acciones para su mitigación y adelantar acciones producto de los resultados de las evaluaciones llevadas a cabo por los organismos de control.”***

Para cumplir la política antes declarada, la Alta Dirección asignará los recursos tanto humanos, presupuestales y tecnológicos necesarios, que permitan implementar la metodología de administración del riesgo y ejecutar eficientemente la formulación, calificación y evaluación.

PASO 2

## **Identificación de Riesgos**

Este paso consiste en conocer los eventos potenciales - estén o no bajo el control de la entidad que ponen en riesgo el logro de la misión por la afectación de los objetivos institucionales y de proceso, estableciendo los agentes generadores internos y externos, las causas, la descripción del riesgo identificado y sus consecuencias.

Antes de señalar las fases de este paso es necesario analizar la adecuada formulación de los objetivos institucionales y de proceso, que contengan las siguientes características mínimas: Específico, Medible, Alcanzable, Relevante y Proyectado en el Tiempo. (SMART). Los objetivos deben incluir el “*qué*”, “*cómo*”, “*para qué*”, “*cuándo*” y “*cuánto*”.

|  |  |  |
| --- | --- | --- |
| **S** | Específico | Se deben resolver cuestiones como: Qué, Cómo, Cuándo, Dónde, Con qué, Quién. Considerar el orden y los necesarios para el cumplimiento de la misión. |
| **M** | Medible | Para ello es necesario involucrar algunos números en su definición, por ejemplo, porcentajes o cantidades exactas. (Cuando aplique). |
| **A** | Alcanzable | Para hacer alcanzable un objetivo, se necesita un previo análisis de lo que se ha hecho y logrado hasta el momento. Esto ayudara a saber si lo que se propone es posible o cómo resultaría mejor. |
| **R** | Relevante | Considerar recursos, factores externos e información de actividades previas, a fin de contar con elementos de juicio para su determinación. |
| **T** | Tiempo | Establecer un tiempo al objetivo, ayudará al objetivo a saber si lo que se está haciendo es lo óptimo para llegar a la meta, así mismo permite determinar el cumplimiento y mediciones finales. |

**Fuente:** *Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5*

Este paso tiene como objetivo identificar los riesgos que estén o no bajo el control de la entidad, para ello se debe tener en cuenta el contexto estratégico en el que opera la entidad, la caracterización de cada proceso que contempla su objetivo y alcance y el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.

### **Fases para identificación de riesgos**

Aplicar las siguientes fases es muy importante, dado que todos los riesgos que se identifiquen deben tener impacto en el cumplimiento del objetivo estratégico y del proceso:

#### Análisis de objetivos estratégicos

Se debe tener claridad sobre la alineación de los objetivos estratégicos con la misión y la visión de la entidad, así como su desdoble hacia el objetivo del proceso.

Así mismo, entender la formulación de los objetivos estratégicos alineados con el objetivo del proceso e identificar los posibles riesgos que afectan su cumplimiento y que puedan ocasionar su éxito o fracaso.

#### Análisis del objetivo del proceso

Analizar que el objetivo de proceso esté alineado con la misión y la visión de la entidad, es decir, asegurarse que contribuya al cumplimiento de los objetivos estratégicos correspondientes, los cuales serían afectados en caso de materializarse un riesgo del proceso.

El desarrollo de esta fase ayuda a identificar los riesgos que están o no bajo el control del proceso, para ello se debe tener en cuenta el contexto estratégico en el que opera la entidad, la caracterización de cada proceso que define su objetivo y alcance.

#### Identificar los puntos de riesgo

Son actividades dentro del flujo del proceso, donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.

#### Identificar las causas del riesgo

Las causas son los medios, circunstancias y/o agentes generadores de riesgos; la definición de las causas es de gran relevancia para lograr una adecuada administración del riesgo. Se debe garantizar la coherencia entre las causas y el riesgo identificado, teniendo en cuenta que los controles estarán orientados a la eliminación de las causas o mitigación de las consecuencias o impacto, asociadas al riesgo.

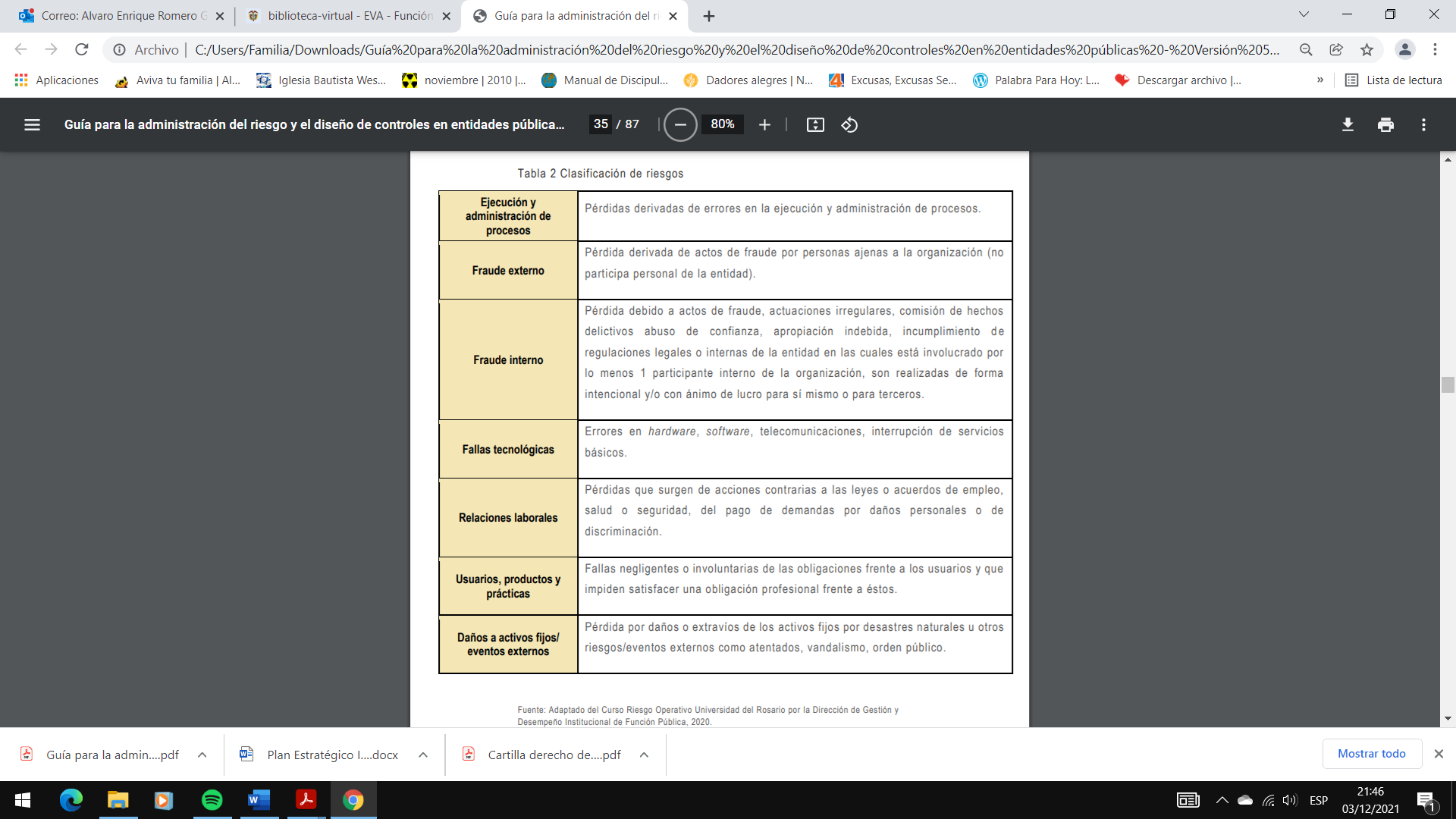
Una definición inadecuada de las causas conlleva a un tratamiento incipiente y poco efectivo de los riesgos identificados por definición errada de los controles.

#### Identificar áreas de impacto

Es la consecuencia económica o reputacional a la cual se ve expuesto la entidad en caso de materializarse un riesgo.

### **Clasificación del riesgo**

Permite agrupar cada uno de los riesgos identificados en las siguientes categorías:



**Fuente:** *Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5*

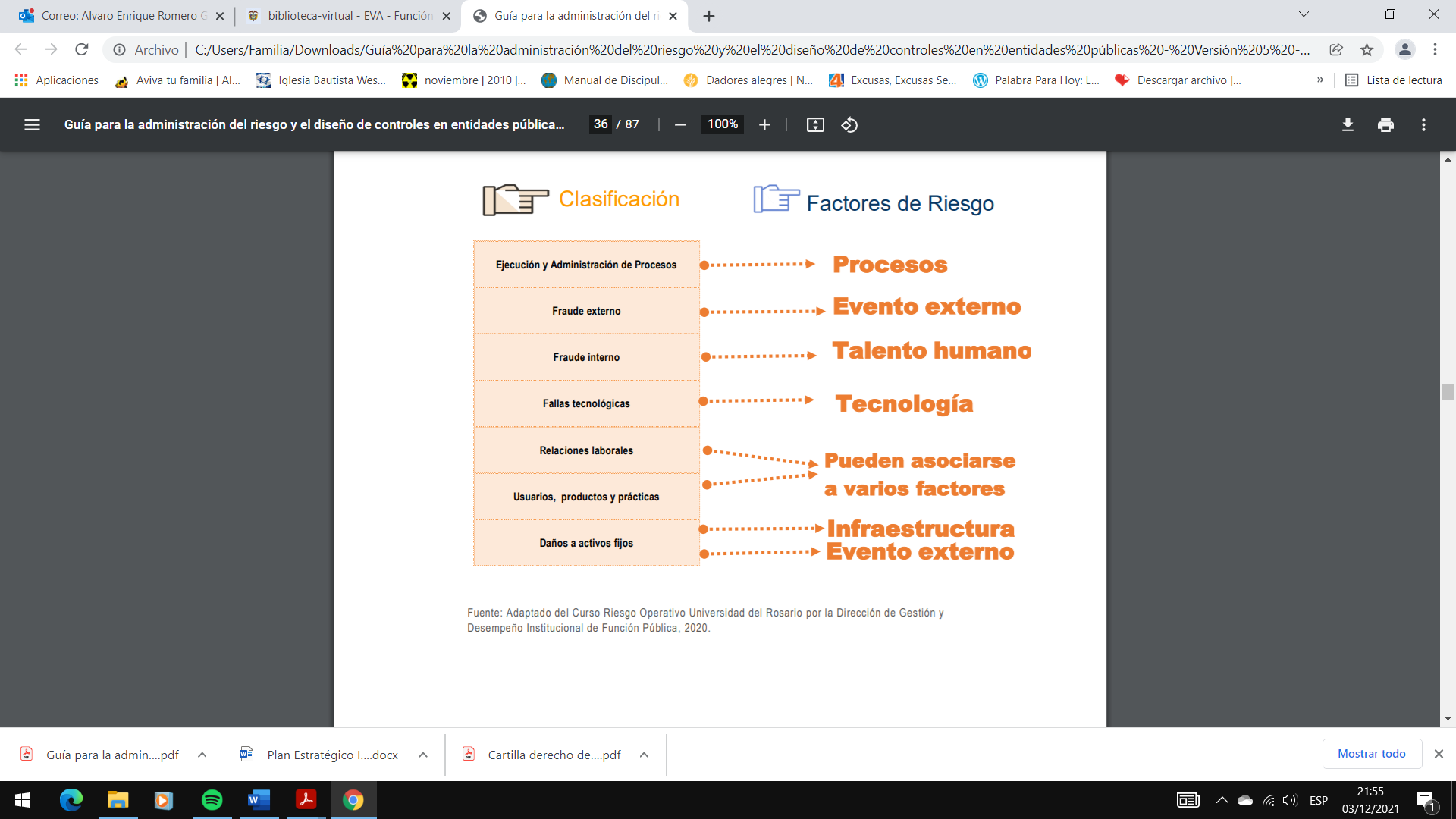
### **Identificación de áreas de factores de riesgo**

Es importante tener en cuenta los agentes generadores de riesgo que son el resultado del análisis del contexto estratégico, por lo tanto, son el insumo para determinar las causas; por esta razón cada una de estas, se debe asociar a un agente externo o interno de riesgo, según corresponda.

En la siguiente tabla encontrará un listado de factores de riesgo aplicable a la entidad.

| **NOMBRE** | **DESCRIPCIÓN** | **TIPO DE FACTOR** | **ESTADO** |
| --- | --- | --- | --- |
| Tecnológico | Cambios, avances o exposiciones tecnológicas relacionadas con: -Evoluciones tecnológicas -Modificación de plataformas tecnológicas -Interrupciones en las redes de comunicación -Vulnerabilidad en los sistemas de seguridad de la información -Cambios tecnológicos que generen obsolescencia de los sistemas y modelos con que cuenta la Entidad. | Externo | Activo |
| Social | Condiciones sociales de los habitantes de la ciudad. Algunas conductas asociadas a este agente generador son: -Políticas migratorias o emigración -Desplazamiento -Asonadas -Secuestros -Extorsión -Vandalismo -Delincuencia común -Corrupción social -Terrorismo. | Externo | Activo |
| Político | Cambios de gobierno, legislación, planes, políticas públicas, decisiones de gobernantes. Algunas conductas asociadas a este agente generador son: -Decisiones políticas que afecten la operación institucional -Influencias políticas que pueden afectar la operación institucional -Cambios de gobierno. -Decisiones administrativas nacionales y/o distritales -Respaldo deficiente del Concejo -Reformas. | Externo | Activo |
| Legal | Cambios en las normas que rigen la operación de la Entidad. Algunas conductas asociadas a este agente generador son: -Nuevos criterios jurisprudenciales -Cambios normativos nacionales o distritales. | Externo | Activo |
| Interinstitucional | Relaciones interinstitucionales con las entidades del sector, gobierno y demás partes interesadas. Algunas conductas asociadas a este agente generador son: -Reglamentación y/o capacidad operativa de las entidades -Disponibilidad de información de Entidades con las que el IDPAC debe operar de manera articulada -Disposición de Entidades Públicas y/o partes interesadas. | Externo | Activo |
| Imagen | Credibilidad, interpretación de conceptos, percepciones de la realidad y del funcionamiento u operación de la entidad y de lo público. Algunas conductas asociadas a este agente generador son: -Poca o nula credibilidad en la gestión institucional -Percepción negativa de la gestión institucional por parte de las partes interesadas -Publicidad negativa -Acciones, decisiones y trámites errados -Inadecuada atención al usuario. | Externo | Activo |
| Económico | Disponibilidad y lineamientos para la administración de recursos económicos. Algunas conductas asociadas a este agente generador son: -Disponibilidad de capital para la operación institucional -Aspectos y directrices a tener en cuenta para la administración de recursos financieros asignados a la Entidad. | Externo | Activo |
| Cultural | Condiciones de interacción y relación con los usuarios y partes interesadas de la Entidad. Algunas conductas asociadas a este agente generador son: Malinterpretación de conceptos -Percepciones equivocadas de la operación institucional -Coordinación interinstitucional -Convenios interinstitucionales. | Externo | Activo |
| Ambiental | Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible. Algunas conductas asociadas a este agente generador son: -Terremotos -Inundaciones -Cambios climáticos -Contaminación -Gestión de residuos. | Externo | Activo |
| Talento Humano | Disponibilidad de personal, estabilidad, capacidad operativa y de respuesta de los servidores y contratistas del IDPAC en el desarrollo de sus funciones y obligaciones, competencias y capacitación. Algunas conductas asociadas a este agente generador son: -Capacidad del Talento Humano disponible para dar respuesta a las funciones asignadas -Demoras en los procesos a causa del desconocimiento de las funciones -Falencias en la habilidades y capacidades de los servidores públicos -Debilidad de programas de bienestar laboral y capacitación -Acciones u omisiones de los servidores que intervienen en la gestión -Alta rotación de contratistas o poca continuidad de equipos de trabajo existentes -Falta de personal con los conocimientos y/o habilidades para adelantar la gestión institucional. | Interno | Activo |
| Sistemas Tecnológicos | Operación, disponibilidad, vigencia, pertinencia y estado de los sistemas de información y comunicación de la Entidad. Algunas conductas asociadas a este agente generador son: -Obsolescencia o insuficiencia de los sistemas tecnológicos y modelos para la administración de la información con los que cuenta la Entidad -Sistemas tecnológicos que no se adaptan a la naturaleza institucional -Lentitud y caídas en los sistemas. -Sistemas no integrados o sin interface. -Congestión en los sistemas por demandas en el servicio. -Falta o inadecuado mantenimiento preventivo y correctivo de sistemas de información -Retrasos en la modernización de sistemas de información -Fugas de información. | Interno | Activo |
| Sistemas de gestión | Operación, aplicación, adaptación y mejoramiento de los modelos de planeación y gestión adoptados por el IDPAC para el fortalecimiento de su gestión. Algunas conductas asociadas a este agente generador son: -Definición inadecuada del Direccionamiento Estratégico Institucional -Planeación institucional que no corresponde con las necesidades del gobierno o con las condiciones de la entidad -Falta de continuidad en planes y proyectos institucionales -Operación inadecuada de los modelos de gestión -Incumplimiento de lineamientos de gestión establecidos por el gobierno. -Deficiencia en la planeación estratégica. -Debilidad institucional en la interpretación y aplicación de normas. -Vigencia de lineamientos de gestión establecidos -Desarticulación de requisitos de los modelos de gestión -Pertinencia de los lineamientos. | Interno | Activo |
| Seguridad y salud en el trabajo | Condiciones de trabajo producto de las emociones de los integrantes de un equipo o de toda la Entidad; contempla aspectos físicos y emocionales, e influye de manera directa en la motivación de los empleados. Algunas conductas asociadas a este agente generador son: -Espacio físico, instalaciones, temperatura -Conflictos en los equipos de trabajo -Debilidad en las relaciones interpersonales -Estabilidad laboral -Remuneración laboral -Política de ascenso -Bajo nivel de participación de los servidores en procesos de formación y capacitación -Organización inadecuada del trabajo -Planeación inadecuada del tiempo de trabajo -Carga mental elevada -Resistencia al cambio -Desinterés de los servidores o equipos de trabajo -Acoso laboral. | Interno | Activo |
| Mecanismos de Control | Estado, características y disponibilidad de los mecanismos de seguimiento y medición institucionales. Algunas conductas asociadas a este agente generador son: -Insuficientes, deficientes o inadecuados mecanismos de seguimiento y control -Sobrestimación de los mecanismos de control dispuestos sin ser adecuados con las condiciones institucionales -Interpretación errónea de normas que implican la implementación de mecanismos de control -Observaciones erradas por parte de los actores de evaluación y seguimiento -Falta de aplicación de los mecanismos de control establecidos -Definición desmedida de mecanismos de control que dificultan la gestión institucional. | Interno | Activo |
| Gestión por procesos | Operación, articulación e interrelación de los procesos, procedimientos y metodologías que orientan la gestión institucional. Algunas conductas asociadas a este agente generador son: -Falencias en la definición del modelo de operación por procesos institucional -Objetivo y alcance de los procesos inadecuado o impreciso -Inconvenientes en la operación de los procesos institucionales -Pertinencia de los documentos asociados a los procesos y falta de claridad frente a la operación -Falta de efectividad en la interrelación de procesos o relaciones entre procesos con inconsistencias -Desconocimiento del modelo de operación por procesos (Documentos, políticas, prácticas de gestión). | Interno | Activo |
| Financiero | Capacidad financiera de la entidad y administración de los recursos disponibles. Algunas conductas asociadas a este agente generador son: -Inadecuada programación presupuestal -Inadecuados procesos de planeación y ejecución presupuestal -Políticas internas de austeridad del gasto -Inadecuado seguimiento presupuestal. | Interno | Activo |
| Ético | Compromiso y comportamiento ético (principios y valores) de los trabajadores. Algunas conductas asociadas a este agente generador son: -Deficiencias en el proceso de selección al validar las competencias comportamentales -Falta de ética de los servidores y/o contratistas en el desempeño de su labor. | Interno | Activo |
| Estructura organizacional | Organización de la entidad, distribución de roles y responsabilidades, cambios en los directivos. Algunas conductas asociadas a este agente generador son: -Multiplicidad de funciones concentradas en un solo cargo o dependencia -Cambios en la estructura y funcionamiento de las dependencias -Asignación de nuevas funciones -Ausencia de criterios para la definición de niveles de responsabilidad y autoridad -Alta rotación en el nivel directivo -Falencias de liderazgo por parte de los gerentes públicos. | Interno | Activo |
| Dirección | Resultados y decisiones de los diferentes comités de la Entidad, lineamientos y políticas institucionales. Algunas conductas asociadas a este agente generador son: -Decisiones de la alta dirección, toma de decisiones sin atención de las condiciones institucionales y las recomendaciones de los equipos de trabajo (Toma de decisiones no sustentadas en evidencias) - Falta de apoyo de los Gerentes Públicos para adelantar iniciativas institucionales. | Interno | Activo |
| Comunicación e información | Flujos de información y comunicación formales e informales de la Entidad. Algunas conductas asociadas a este agente generador son: -Integridad de la información -Debilidades en la disposición y consulta de la información interna como insumo para la gestión de los procesos -Calidad, vigencia y pertinencia de la información interna que se requiere para generar resultados. -Debilidad en la implementación de las estrategias de comunicación informativa y organizacional -Debilidad o ausencia de canales de comunicación internos. | Interno | Activo |

De acuerdo a lo anterior, su interrelación es la siguiente:

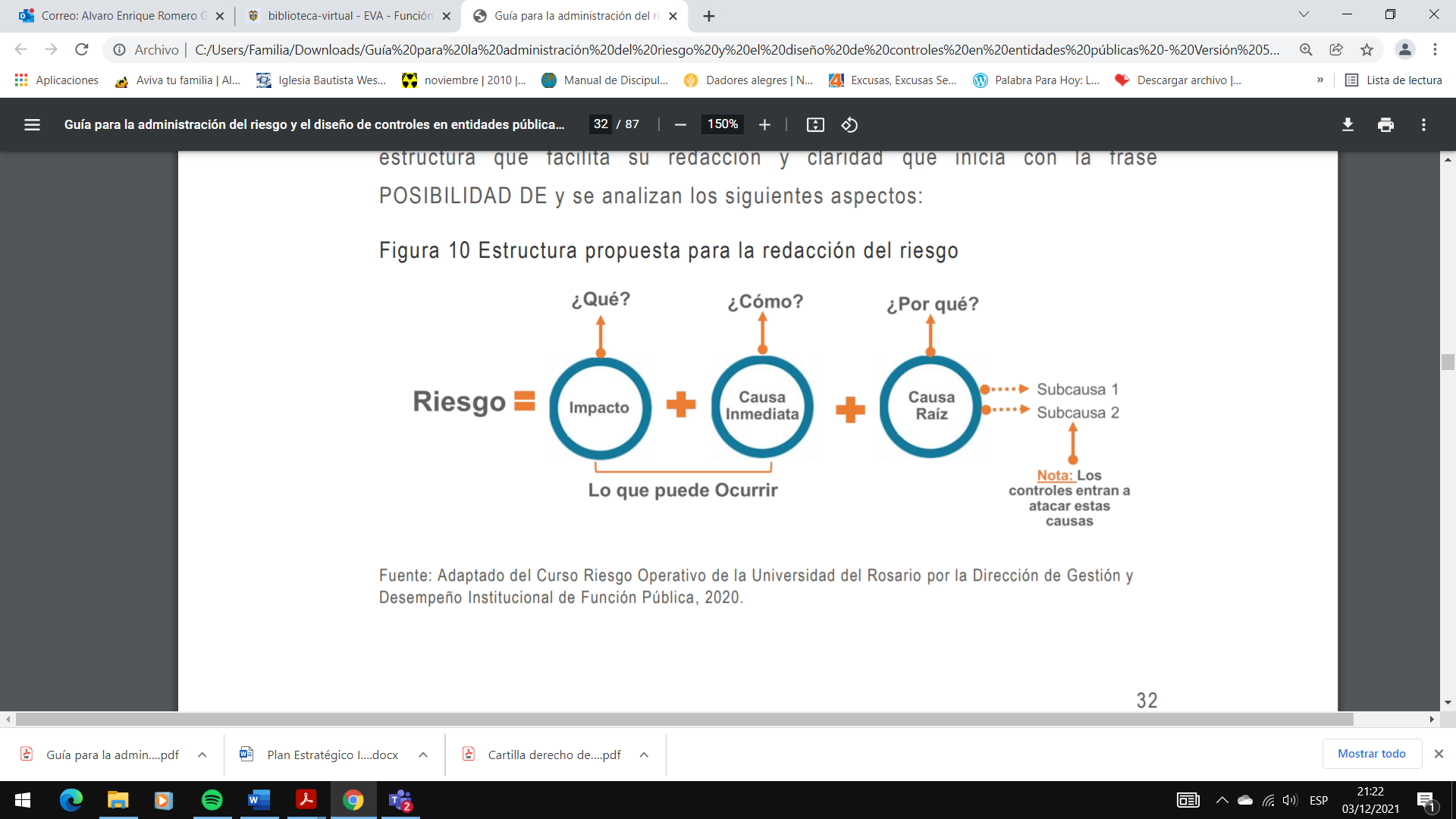


**Fuente:** *Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5*

### **Descripción del riesgo**

Debe contener todos los detalles que sean necesarios y de fácil entendimiento, tanto para el líder del proceso como para personas ajenas al mismo.

La estructura que facilita su redacción y claridad inicia con la frase “P**osibilidad de”** y se complementa con los siguientes elementos:



**Fuente:** *Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5*

La descripción del riesgo debe cumplir con los criterios de redacción para lograr una adecuada imagen del evento. Para describir el riesgo será importante 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….

Desglosando la estructura propuesta tenemos:

***Impacto:*** Son las consecuencias que puede ocasionar a la entidad la materialización del riesgo del proceso.

***Causa inmediata*:** Circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.

***Causa raíz:*** Es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas.

***Por ejemplo:*** Si el objetivo del proceso de Gestión Contractual es “*Adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación”.*

La redacción del riesgo sería:

*RIESGO DEL PROCESO: “Inoportunidad en la adquisición de los bienes y servicios requeridos por la entidad”. RIESGO DE CORRUPCIÓN: “Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato”.*

**1**

**Premisas para una adecuada redacción del riesgo**

No describir como riesgos omisiones ni desviaciones del control.

*Ejemplo***:** errores en la liquidación de la nómina por fallas en los procedimientos existentes.

No describir causas como riesgos

*Ejemplo*: inadecuado funcionamiento de la plataforma estratégica donde se realiza el seguimiento a la planeación.

No describir riesgos como la negación de un control.

*Ejemplo***:** retrasos en la prestación del servicio por no contar con digiturno para la atención.

No existen riesgos transversales, lo que pueden existir son causas transversales.

*Ejemplo***:** pérdida de expedientes. Puede ser un riesgo asociado a la gestión documental, a la gestión contractual o jurídica y en cada proceso sus controles son diferentes.

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

### **Tipos de riesgos**

La tipología de riesgos está asociada a la misión de la entidad, a las normas que regulan la operación, al sistema de gestión implementado, entre otros aspectos.

**Nota**: Para la identificación de los riesgos tenga en cuenta la tipología que se presenta a continuación:

* ***Riesgos Estratégicos*:** Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la entidad.
* ***Riesgos Gerenciales*:** Posibilidad de ocurrencia de eventos que afecten los procesos estratégicos de la entidad.
* ***Riesgos Operativos*:** Posibilidad de ocurrencia de eventos que afecten el cumplimiento del objetivo de procesos misionales de la entidad.
* ***Riesgos Financieros:*** Posibilidad de ocurrencia de eventos que afecten los recursos de la entidad y todos aquellos temas relacionados con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, ejecución presupuestal, estados financieros, pagos, manejos de excedentes de tesorería y manejo de los bienes.
* ***Riesgos Tecnológicos*:** Posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.
* ***Riesgos de cumplimiento:*** Posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la entidad, debido a su incumplimiento o desacato a la normatividad legal y las obligaciones contractuales.
* ***Riesgos de Contratación****:* Se considera la identificación de estos riesgos a través del Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación: https://www.colombiacompra.gov.co/sites/default/ files/manuales/ cce\_manual\_riesgo\_web.pd
* ***Riesgos de corrupción:*** 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:*** Posibilidad de 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.
* ***Riesgo de Imagen*:** Posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización ante sus clientes y partes interesadas.
* ***Riesgos de SST:*** Incluyen las condiciones de seguridad y salud o las necesidades y expectativas de las partes interesadas que pueden afectar la capacidad de la organización para lograr los resultados previstos en el Sistema Integrado de Gestión, esta identificación sigue los lineamientos establecidos en la Guía para la identificación de los peligros y la valoración de los riesgos en seguridad y salud ocupacional (GTC 45).

**Nota:** Para la identificación de los riesgos de seguridad y salud en el trabajo, se debe realizar una descripción y clasificación de los peligros. Los peligros pueden clasificarse de acuerdo con los siguientes criterios (Biológicos, condiciones de seguridad, fenómenos naturales, físicos, psicosociales, químicos, biomecánicos y/o ergonómicos).

* ***Riesgos Ambientales:*** Incluyen las condiciones ambientales o las necesidades y expectativas de las partes interesadas que pueden afectar la capacidad de la organización para lograr los resultados previstos en el Sistema Integrado de Gestión.

A continuación, se presentan algunos ejemplos de descripción del riesgo:

| **RIESGO** | **DESCRIPCIÓN** | **TIPO** | **CAUSAS** | **CONSECUENCIAS** |
| --- | --- | --- | --- | --- |
| 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. | Operativo | 1.Carencia de controles en el procedimiento de contratación  2.Insuficiente capacitación del personal de contratos  3.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 |

La descripción de los peligros está relacionada con el tipo de peligro (Biológicos, Condiciones de seguridad, Fenómenos naturales, Físicos, Psicosociales, Químicos, Biomecánicos y/o Ergonómicos que se haya documentado en la etapa de identificación de la causa, para el caso de los riesgos de SST lo denominamos peligro:

| **RIESGO** | **DESCRIPCIÓN** | **TIPO** | **CAUSAS** | **CONSECUENCIAS** |
| --- | --- | --- | --- | --- |
| Biológico | Contagio a causa del COVID 19, en las actividades que requieren trabajo de campo y contacto con la comunidad durante las medidas de aislamiento preventivo. | Seguridad y Salud en el trabajo | 1. No implementación del protocolo de bioseguridad. 2. Mal uso de los elementos de protección personal como tapabocas, guantes, careta, entre otros. 3. No cumplir con medidas de preventivas de lavado de mano y distanciamiento social. | 1. Aumento de contagio de coronavirus en la entidad. 2. Pérdida de la capacidad laboral o hasta la muerte a causa de la enfermedad. 3. Demandas y demás acciones jurídicas 4. Investigaciones disciplinarias |

La descripción de los riesgos ambientales está asociada al análisis del contexto interno y externo que no permita el logro de los objetivos, así como a las situaciones de emergencia que se presenten y que afecten la capacidad administrativa y operativa de la entidad.

| **RIESGO** | **DESCRIPCIÓN** | **TIPO** | **CAUSAS** | **CONSECUENCIAS** |
| --- | --- | --- | --- | --- |
| Ausencia de planificación en la gestión ambiental asociada con los aspectos ambientales identificados en la ejecución de los proyectos de la entidad | Corresponde al posible incumplimiento por la no identificación de los aspectos y posibles impactos ambientales generados por las actividades que adelanta el IDPAC relacionados con sus proyectos. | Ambiental | 1.Ausencia en la identificación de los aspectos e impactos ambientales  2. Debilidad en la definición de controles y oportunidad en la gestión del riesgo. | Afectación ambiental e incumplimiento de requisitos legales.  Imposición de multas y procesos sancionatorios ambientales |

PASO 3

## **Valoración de Riesgos**

Consiste en establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto con el fin de estimar la zona de riesgo inicial.

### **Análisis del riesgo**

Se debe establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto.

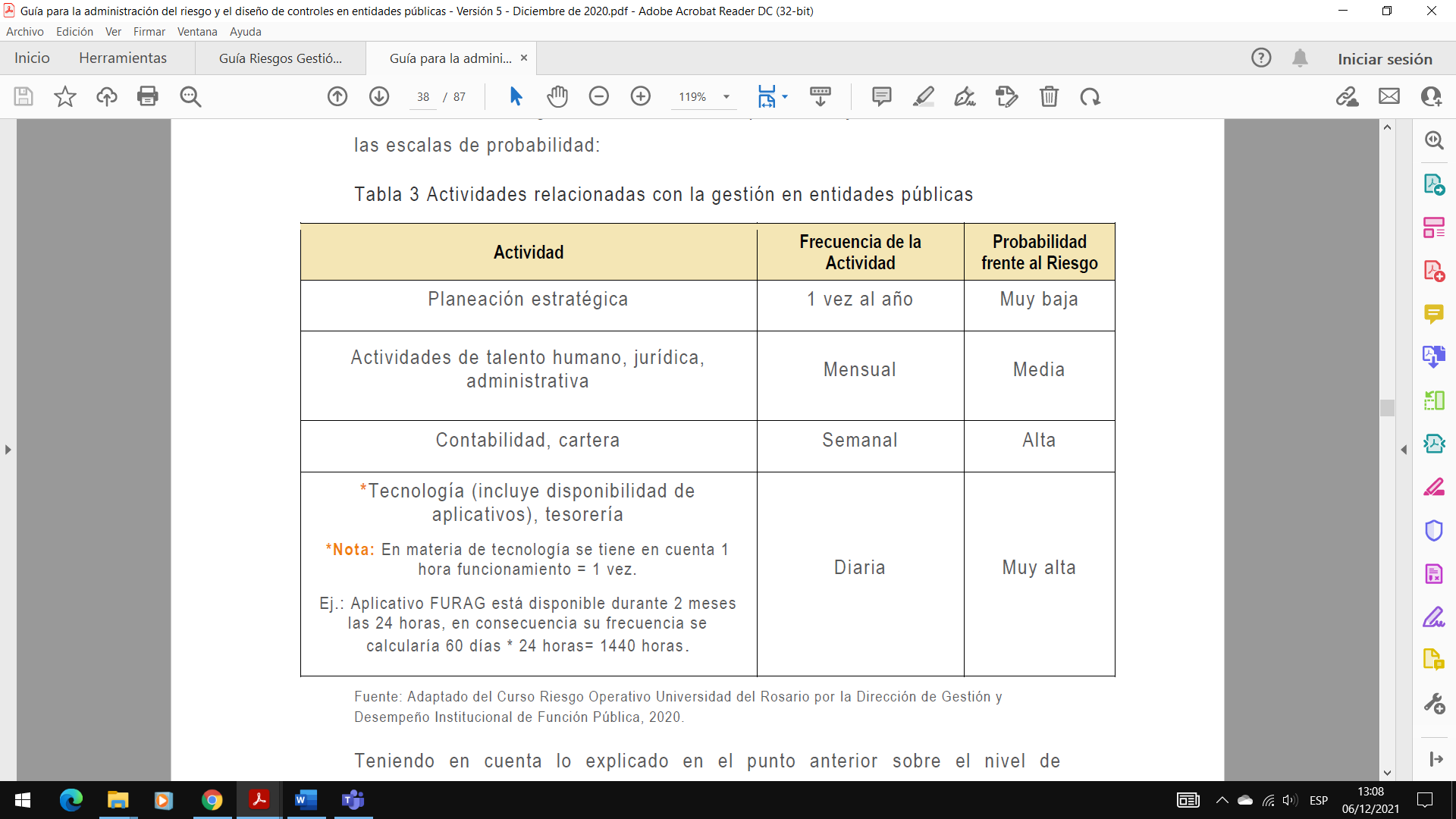
**Nota**: La calificación del riesgo se logra a través de la estimación de la probabilidad de su ocurrencia y el impacto que puede causar su materialización.

### **Determine la probabilidad del riesgo**

La probabilidad representa la posibilidad de ocurrencia del riesgo y esta a su vez estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando, por lo tanto, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de un (1) año.

De este modo, al realizar este tipo de análisis se podrá determinar con claridad la frecuencia con la que se lleva a cabo una actividad, en vez de considerar los posibles eventos que pudiesen haberse dado en el pasado, esto nos dice que, si nunca se han presentado eventos, todos los riesgos tendrán la tendencia a quedar ubicados en niveles bajos, situación que no es realmente usual.

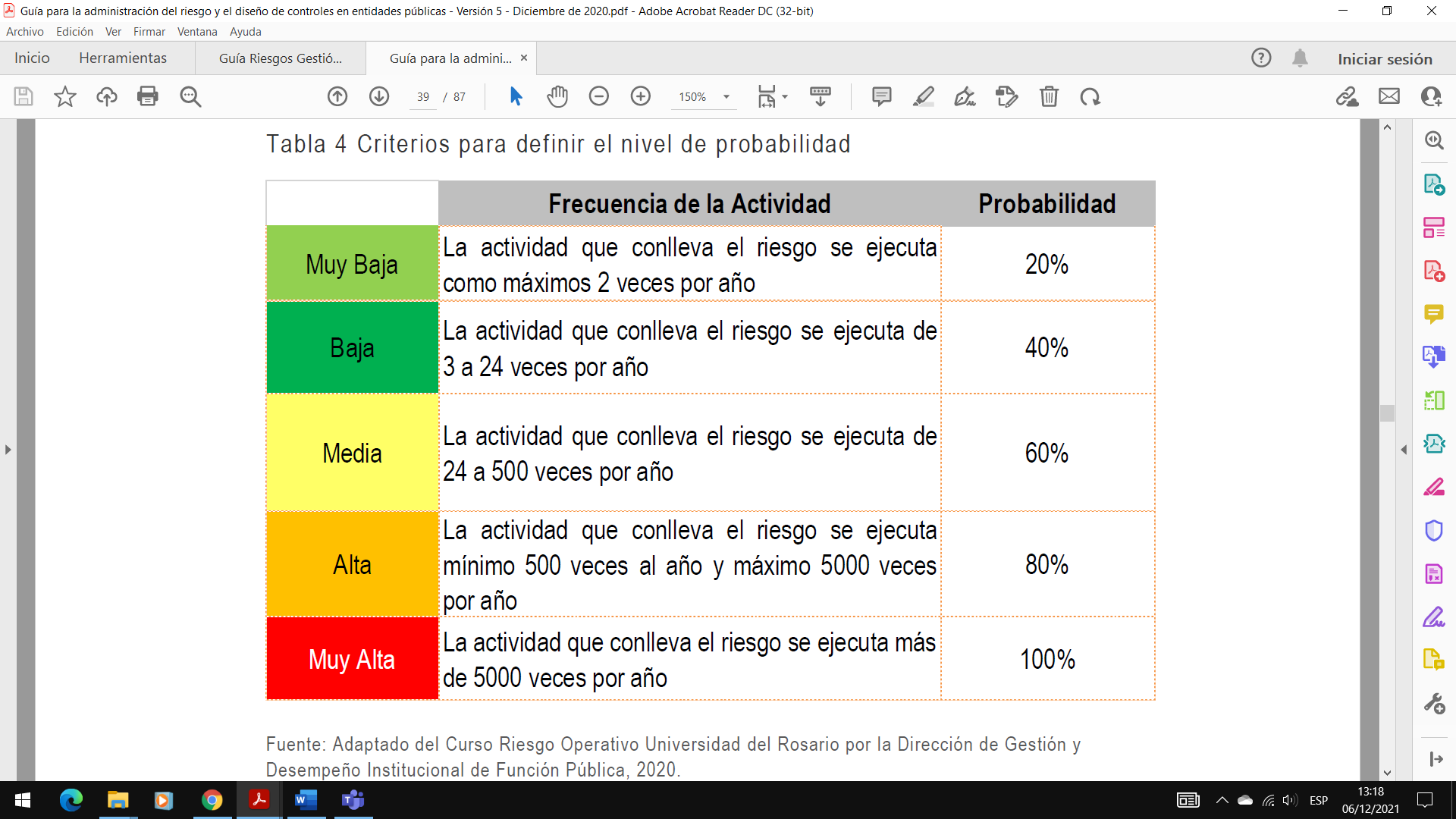
Como ejemplo a continuación, se muestra una tabla de actividades típicas relacionadas con la gestión de una entidad pública, bajo las cuales se definen las escalas de probabilidad:



**Fuente:** *Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5*

No olvidando, lo explicado en el punto anterior sobre el nivel de probabilidad, la exposición al riesgo estará asociada al proceso o actividad que se esté analizando, es decir, **“Al número de veces que se pasa por el punto de riesgo en el periodo de un (1) año”.**

Veamos la tabla donde se establecen los criterios para valorar el nivel de probabilidad.



**Fuente:** *Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5*

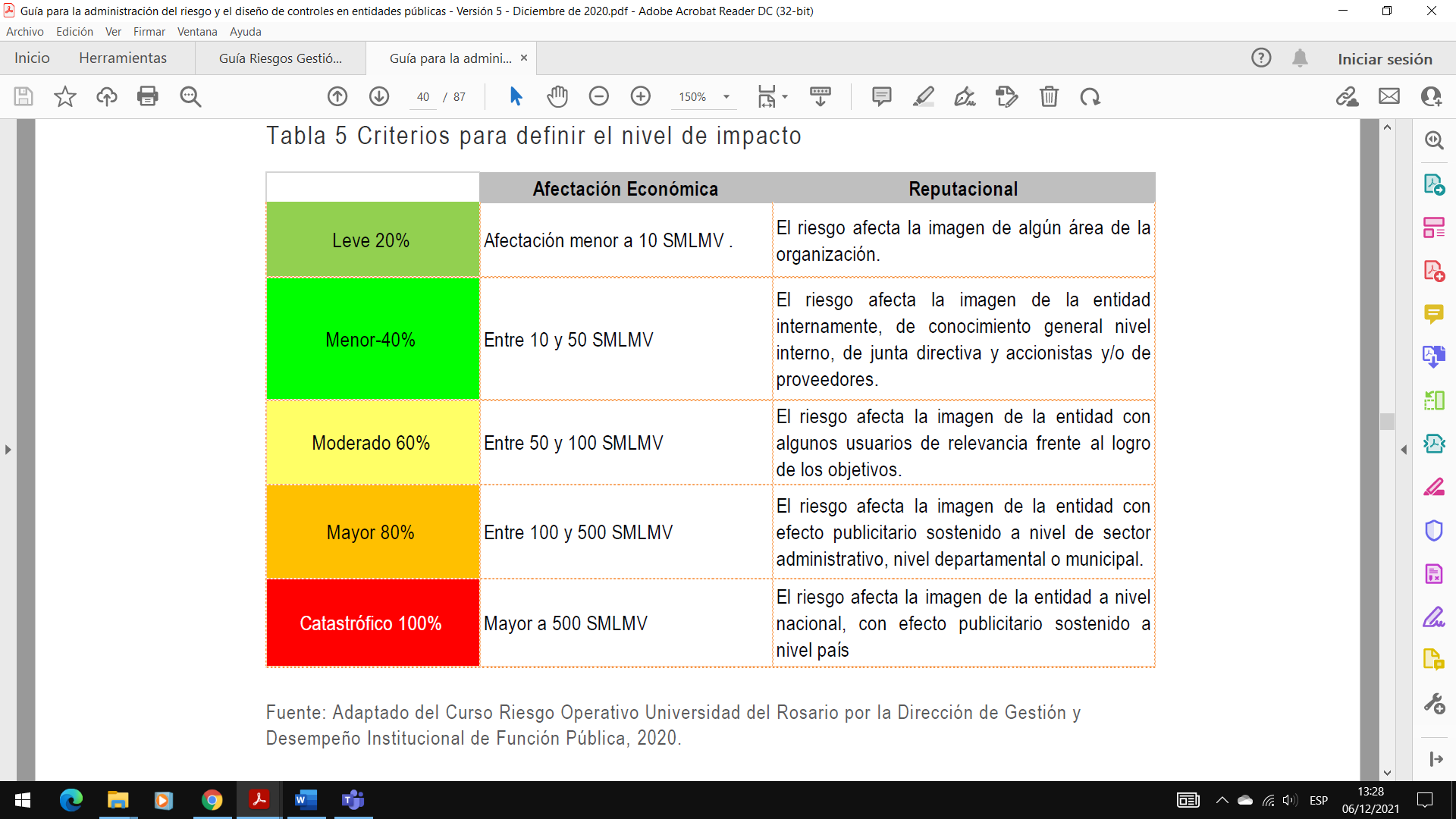
### **Determine el impacto del riesgo**

De acuerdo con la tabla que se presenta en este apartado, se debe determinar el impacto del riesgo, comprobando los criterios que definen el nivel de este, teniendo como variables principales los impactos económicos y reputacionales.

Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional con diferentes niveles se debe tomar el nivel más alto, por ejemplo, para un riesgo identificado se define un impacto económico en nivel “**insignificante”** e impacto reputacional en nivel “**moderado”**, se tomará el más alto, en este caso sería el nivel “**moderado”.**

Bajo este esquema se facilita el análisis para el líder del proceso, dado que se puede considerar información objetiva para su establecimiento, eliminando la subjetividad que usualmente puede darse en este tipo de análisis.

Ahora se presenta la tabla a usar para establecer los criterios para definir el nivel de impacto:



**Fuente:** *Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5*

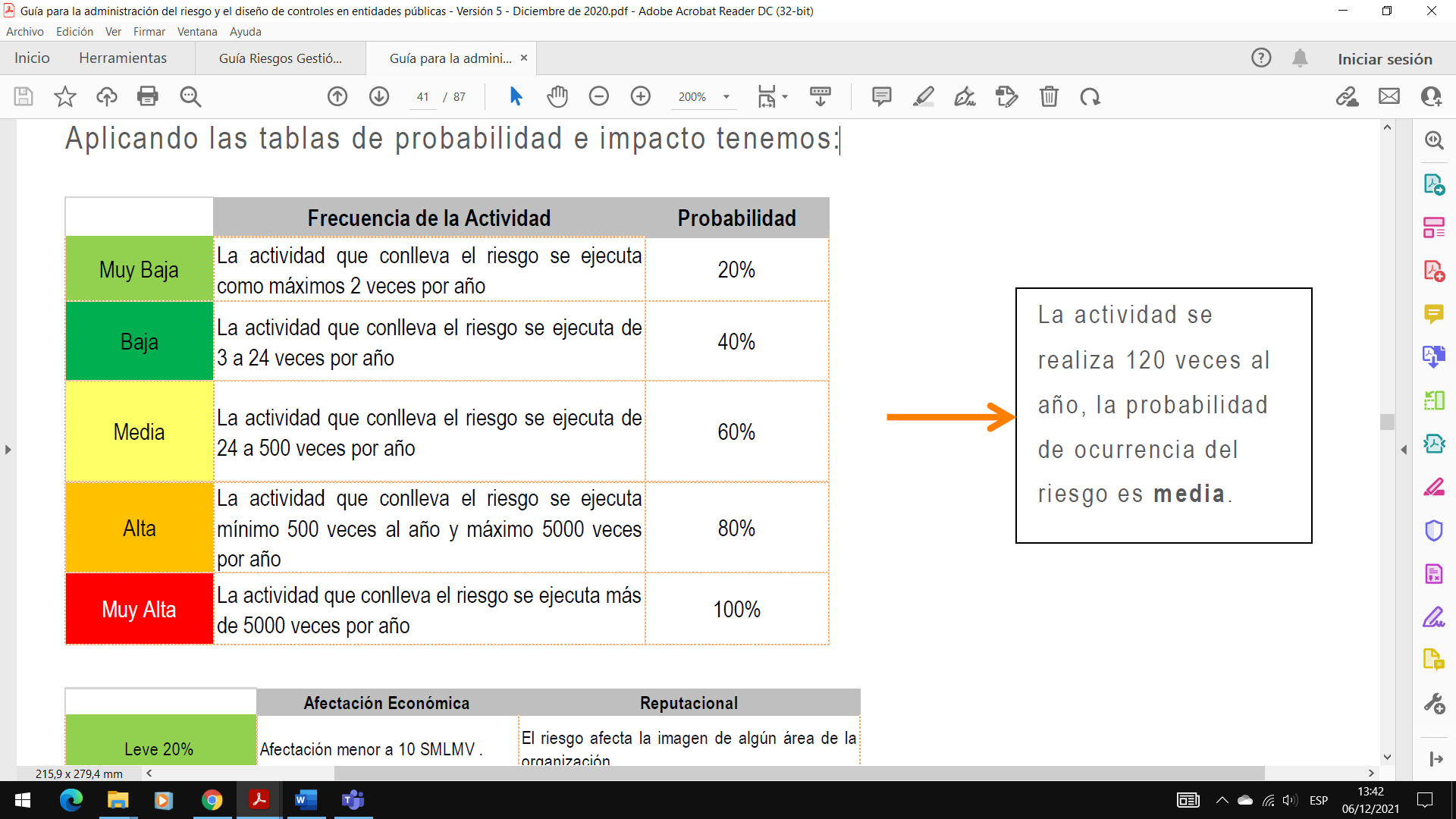
**IMPORTANTE:** Frente al análisis de probabilidad e impacto no se utiliza el criterio experto, esto quiere decir que el líder del proceso, como conocedor de su quehacer, define cuántas veces desarrolla la actividad.

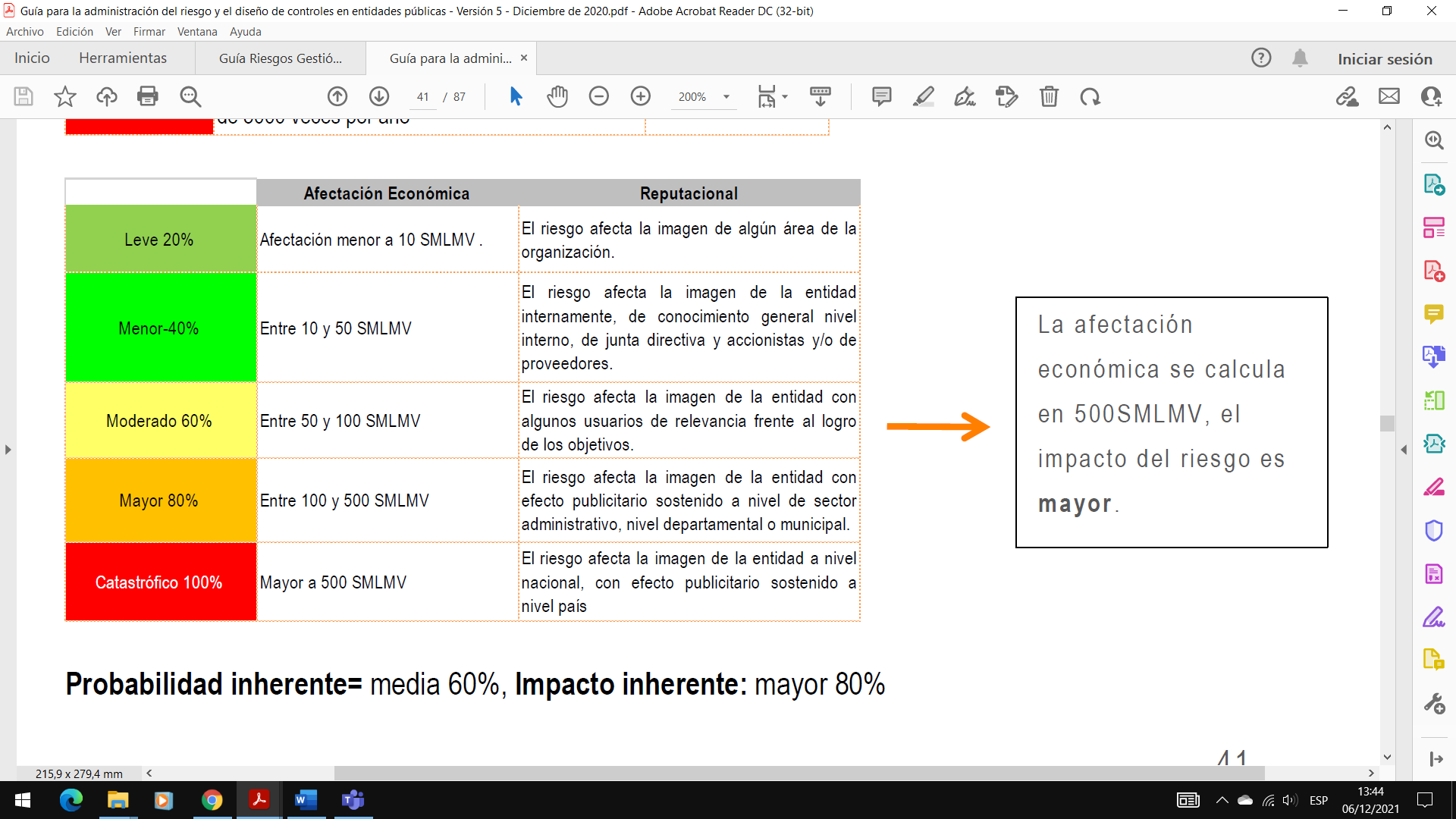
Veamos un ejemplo de cómo aplicar los criterios de las tablas de probabilidad e impacto, tanto de frecuencia como de valoración económica:

***Proceso*:** Gestión de recursos físicos

* ***Objetivo*:** Adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación
* ***Riesgo identificado*:** posibilidad de afectación económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.
* ***Nº de veces que se ejecuta la actividad*:** la actividad de contratos se lleva a cabo 10 veces en el mes = 120 contratos en el año.
* ***Cálculo afectación económica*:** De llegar a materializarse, tendría una afectación económica de 500 SMLMV.

Aplicando las tablas de probabilidad e impacto tenemos:



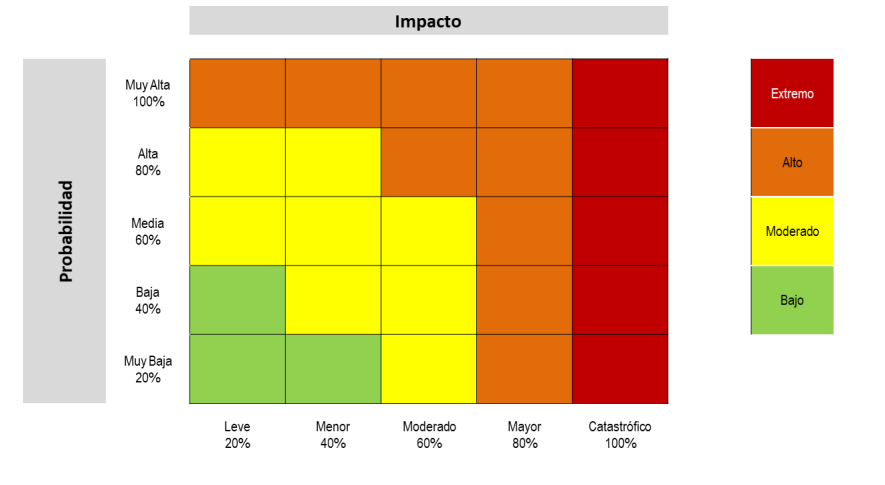


**Fuente:** *Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5*

El resultado es el siguiente: **Probabilidad** **inherente**= media 60%, **Impacto** **inherente:** mayor 80%

### **Evaluación de riesgos preliminar**

Ahora se determina la zona de riesgo inicial - RIESGO INHERENTE; el cual es un análisis preliminar. Se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor.



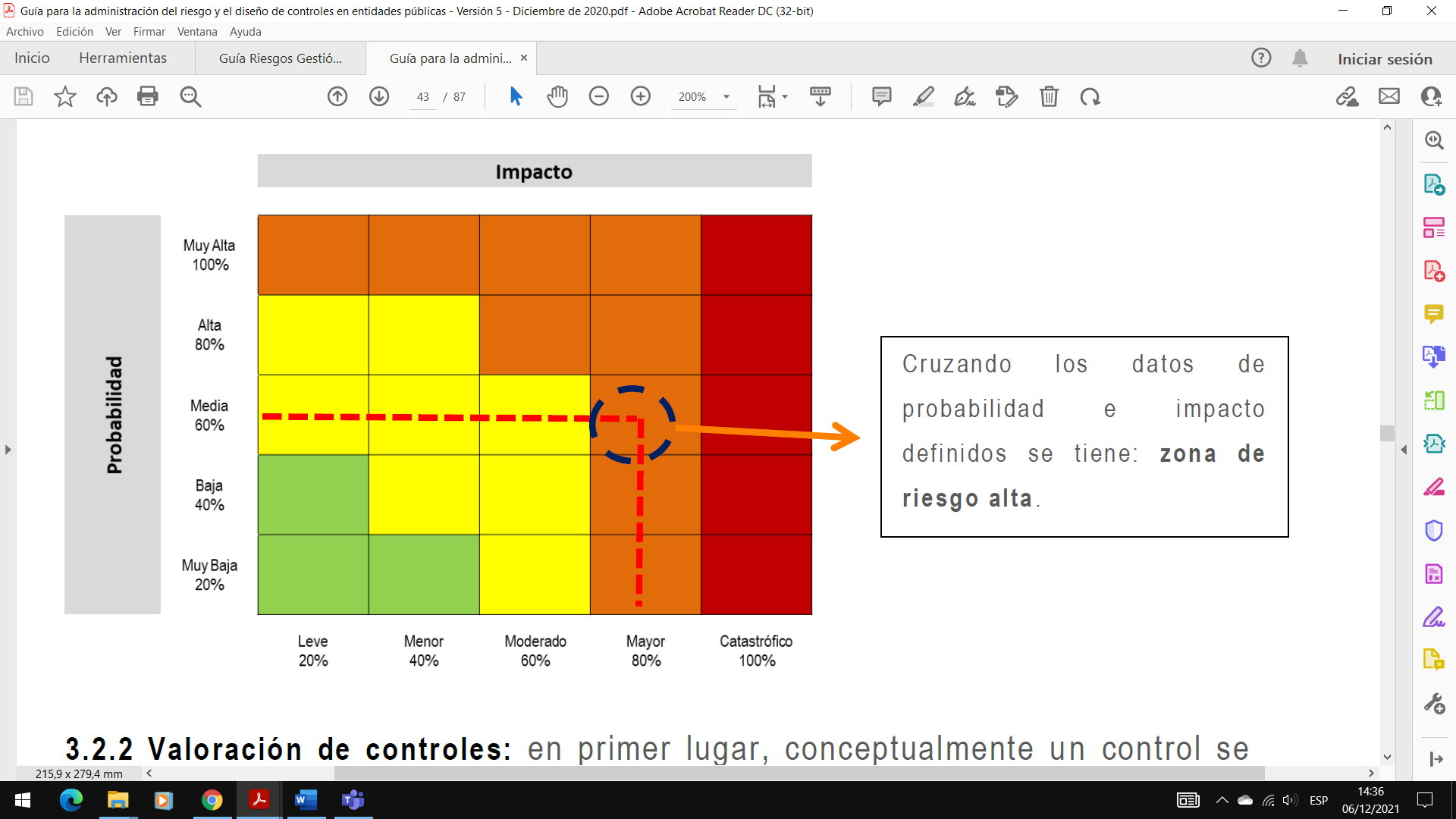
**Fuente:** *Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5*

**Ejemplo** (continuación del ejemplo anterior):

***Proceso*:** Gestión de recursos físicos

* ***Objetivo*:** Adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación
* ***Riesgo identificado*:** posibilidad de afectación económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos
* ***Probabilidad Inherente*** = moderada 60%
* **Impacto Inherente:** mayor 80%

Al aplicar la matriz de calor tenemos:



**Fuente:** *Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5*

**Nota:** Esta evaluación se realiza de manera automática al registrar los datos en el aplicativo SIGPARTICIPO – Módulo: Gestión del Riesgo.

### **Valoración de controles**

Un control se define como la medida que permite reducir o mitigar el riesgo.

Para la valoración de controles se debe tener en cuenta:

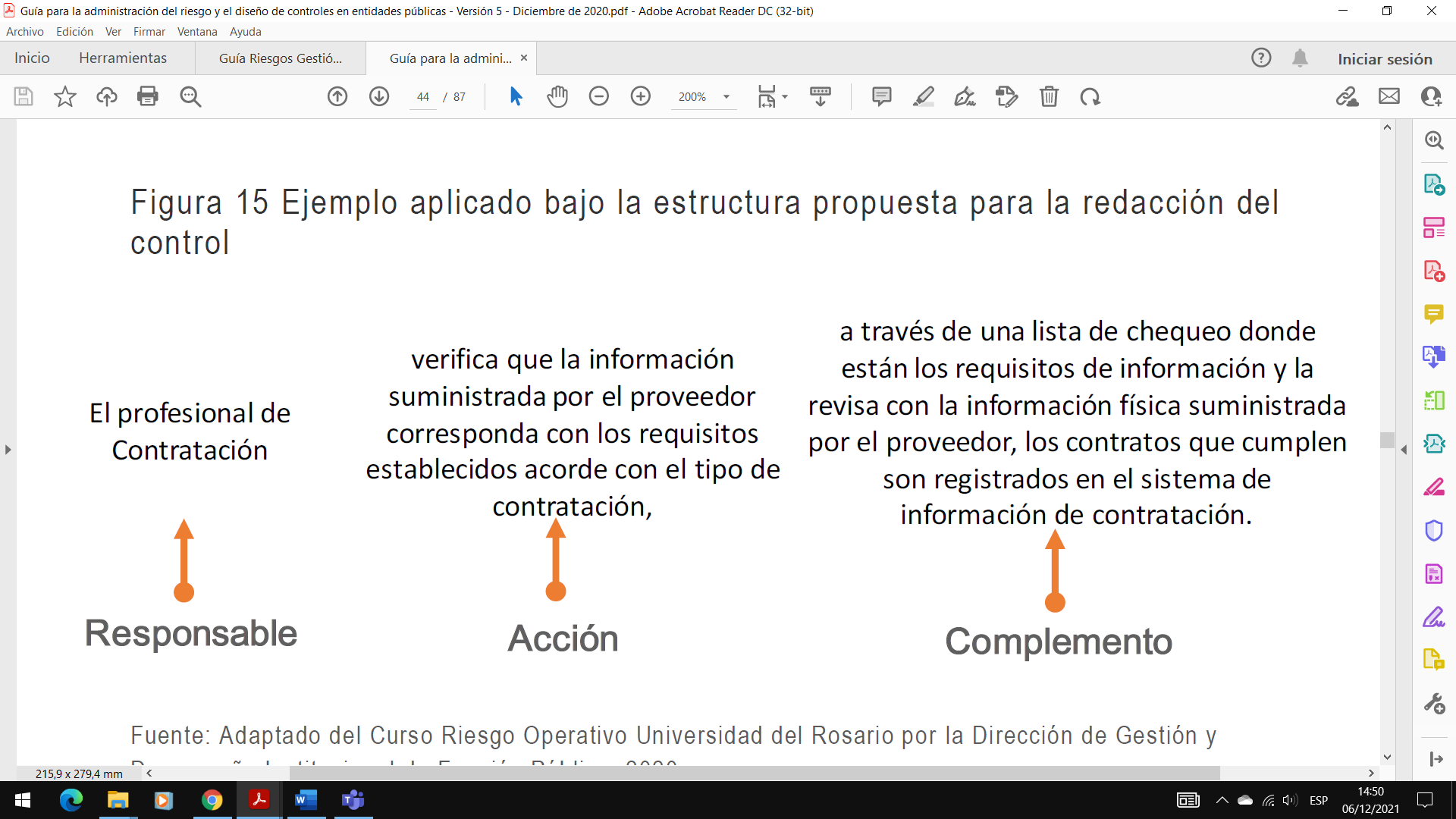
* La identificación de controles se debe realizar a “**Cada”** riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. Estos estarán documentados en los procedimientos y/o políticas de operación, en este caso si aplica el criterio experto.
* Los responsables de implementar y monitorear los controles son los líderes de proceso, apoyándose en su equipo de trabajo.

### **Estructura para la descripción del control**

Debe tener la siguiente estructura:

* **Responsable de ejecutar el control:** Identifica el cargo del servidor de cualquier nivel que ejecuta el control y está definido en el respectivo procedimiento, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.
* **Acción:** Se determina mediante verbos que indican la acción que deben realizar como parte del control.
* **Complemento:** Corresponde a los detalles que permiten identificar claramente el objeto del control.

Veamos un ejemplo aplicado bajo la estructura propuesta para la redacción del control:

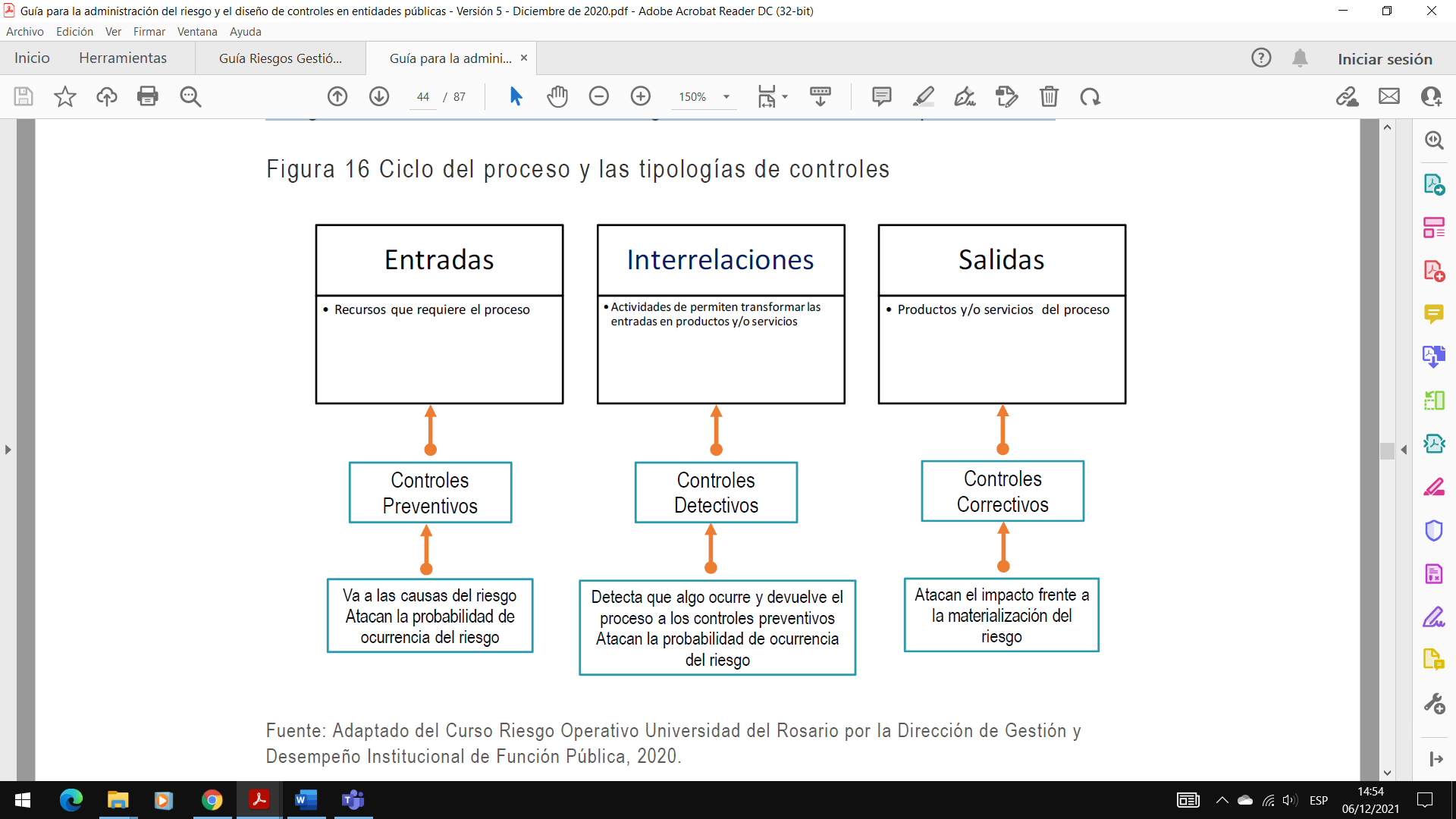


**Fuente:** *Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5*

### **Tipología de controles y los procesos**

A través del ciclo del proceso es posible establecer cuándo se activa un control y por lo tanto, establecer su tipología con mayor precisión.

Para comprender esta estructura conceptual, en la figura siguiente se consideran tres (3) etapas globales del ciclo de un proceso así:



**Fuente:** *Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5*

Derivado de lo anterior, tenemos las siguientes tipologías de controles:

* **Control preventivo:** Es accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.
* **Control detectivo:** Es accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.
* **Control correctivo:** Es accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

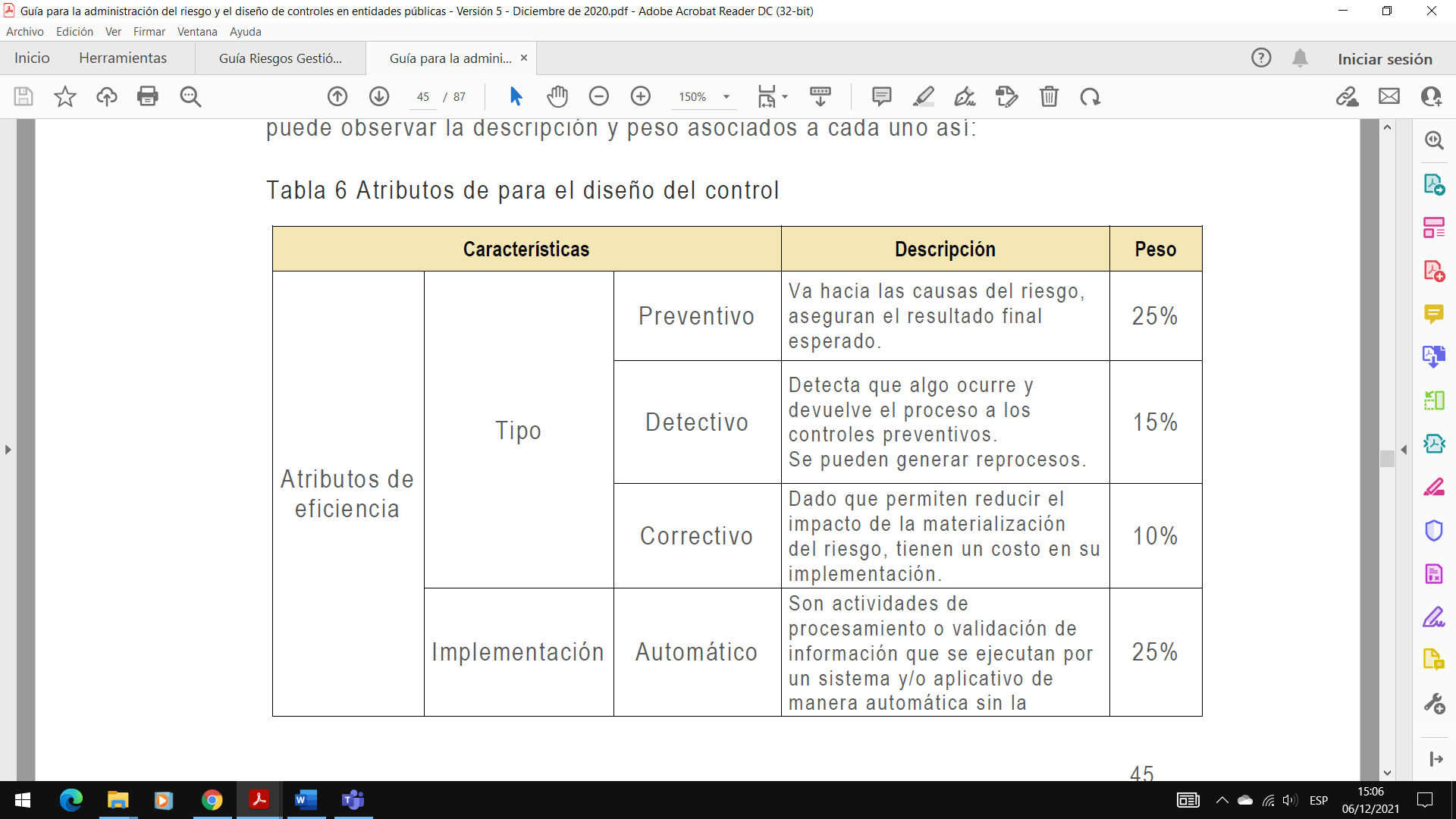
Dependiendo la forma como se ejecutan los controles, tenemos:

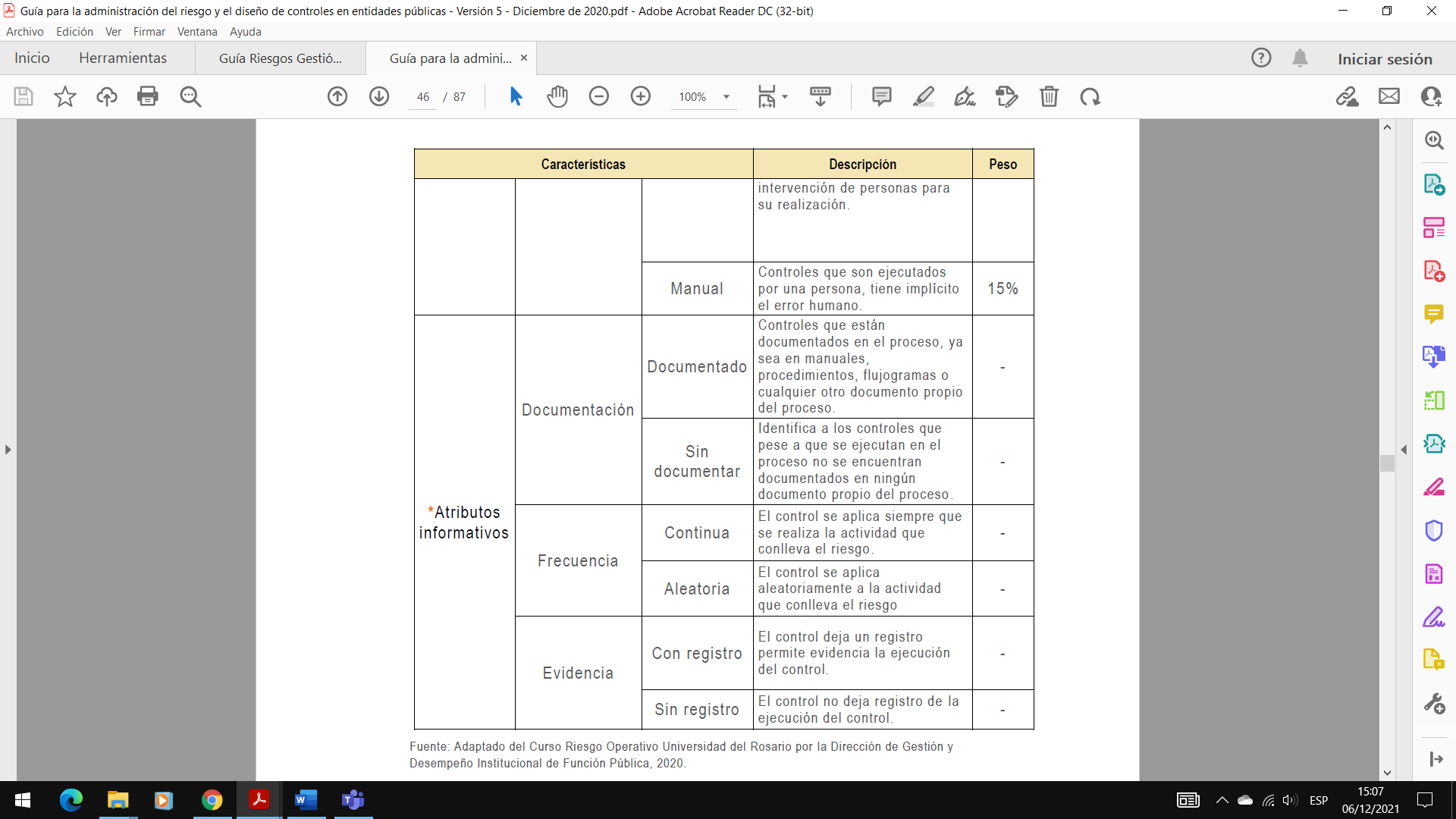
* **Control manual:** Son ejecutados por personas.
* **Control automático:** Son ejecutados por un sistema o aplicación informática

### **Análisis y evaluación de los controles – Atributos**

A continuación, se analizan los “**Atributos”** para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización.

En la siguiente tabla se observa la descripción y peso asociados a cada uno así:

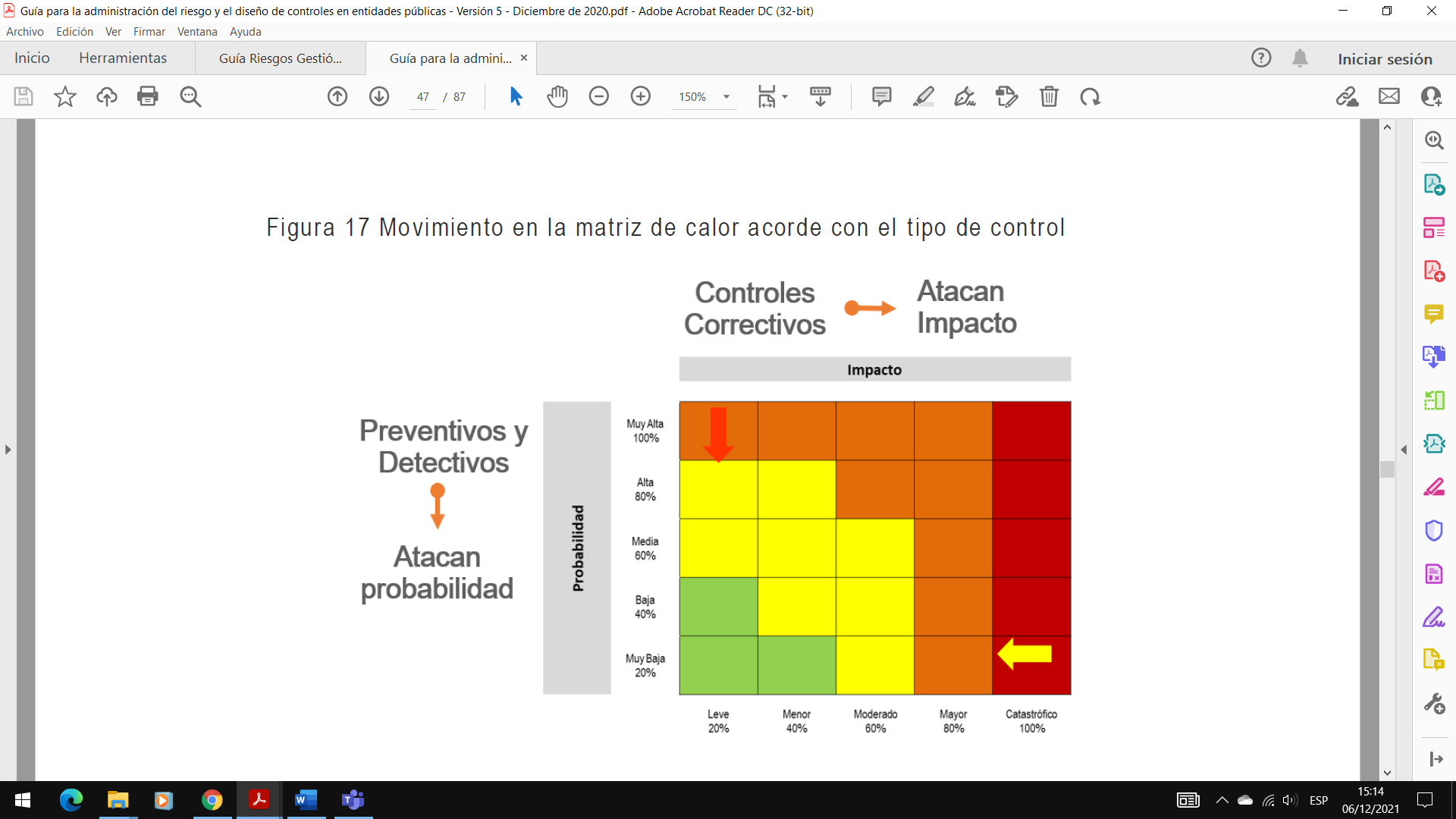




**Fuente:** *Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5*

Los atributos **informativos** solo permiten darle formalidad al control y su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos; sin embargo, estos no tienen una incidencia directa en su efectividad.

**Tenga en cuenta**: Es a partir de los controles que se dará el movimiento en la matriz de calor que se muestra en la siguiente figura donde se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.



**Fuente:** *Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5*

***Ejemplo*** *(continuación del ejemplo gestión de recursos físicos):*

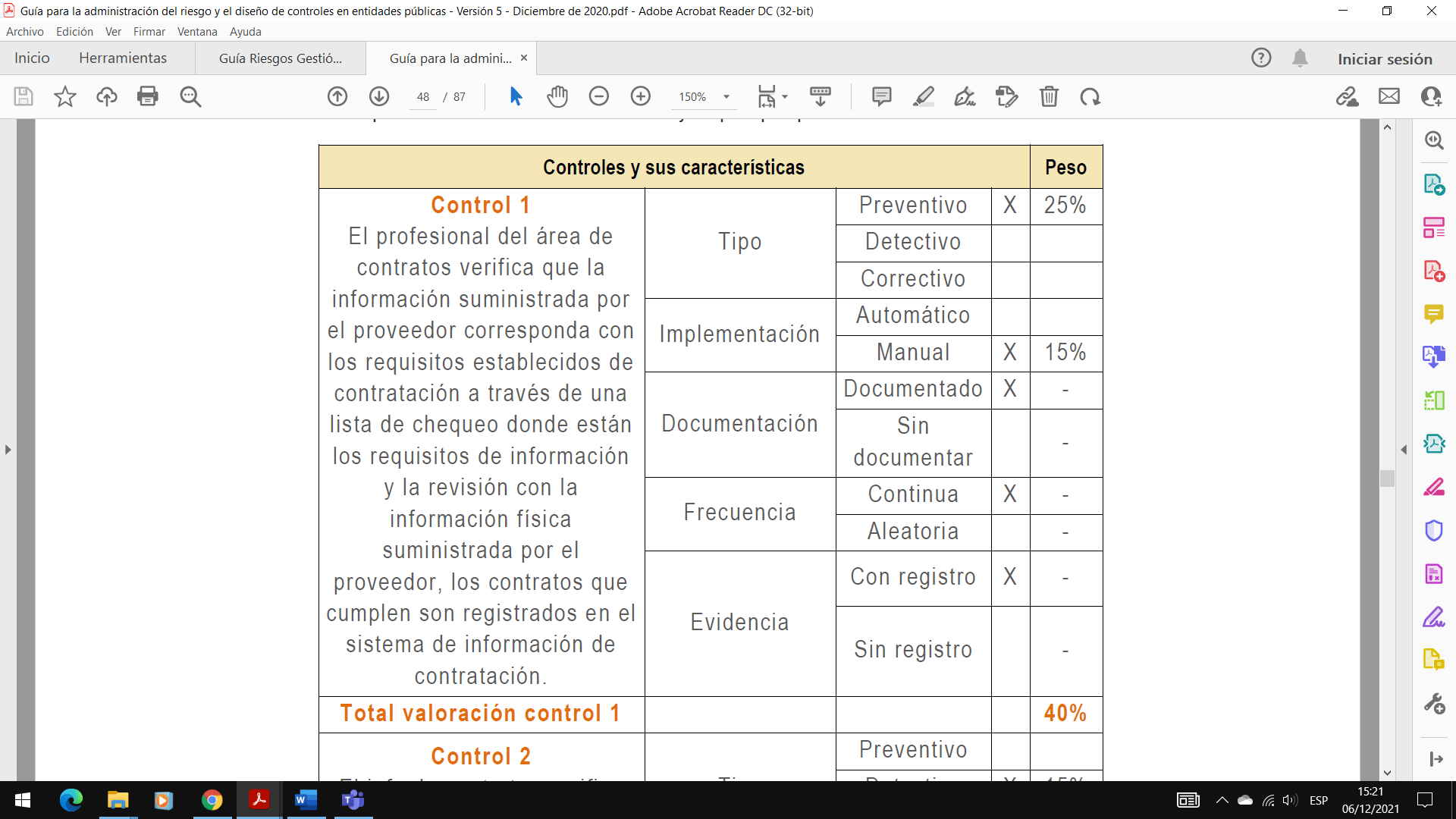
***Proceso***: gestión de recursos físicos

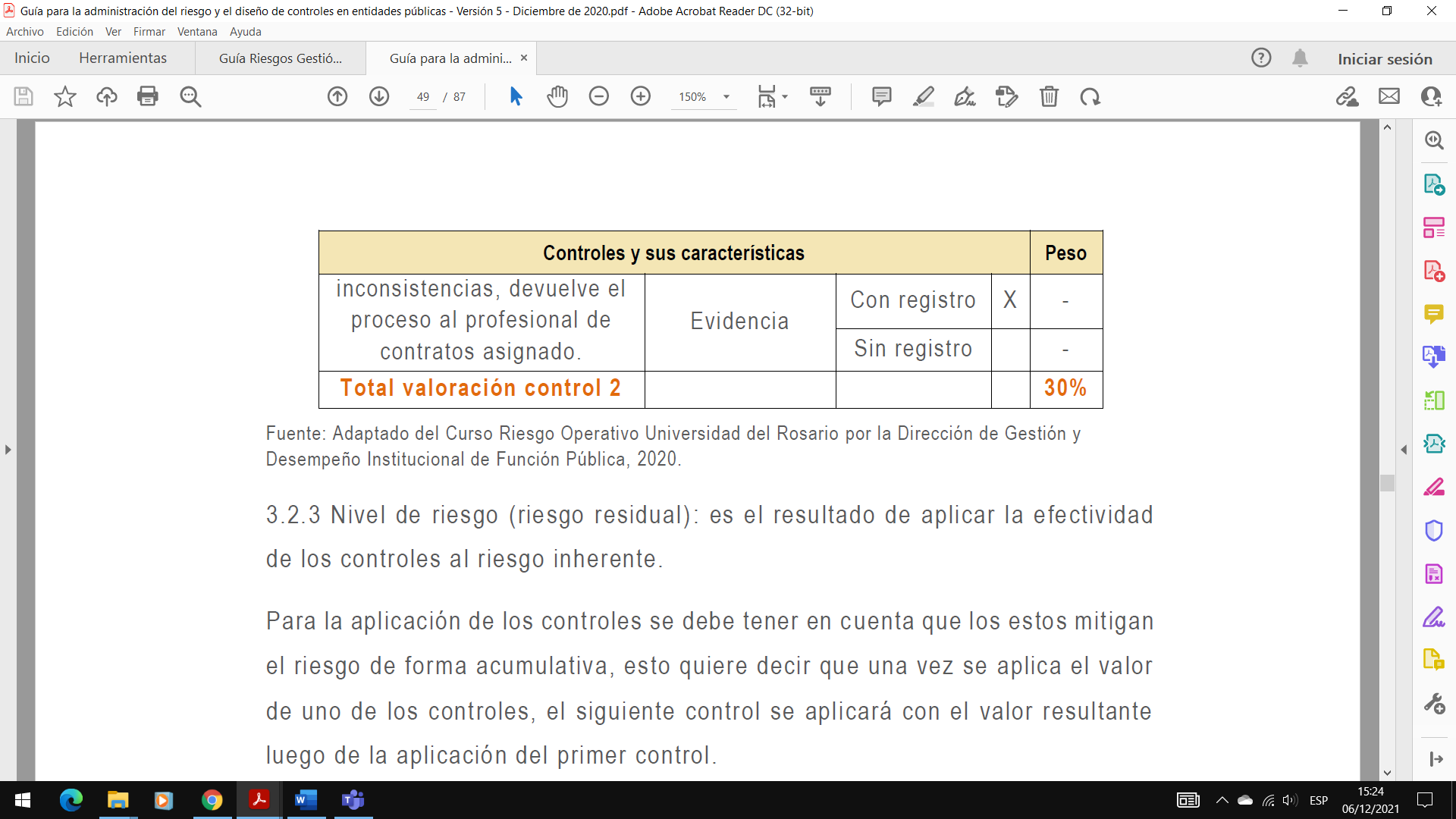
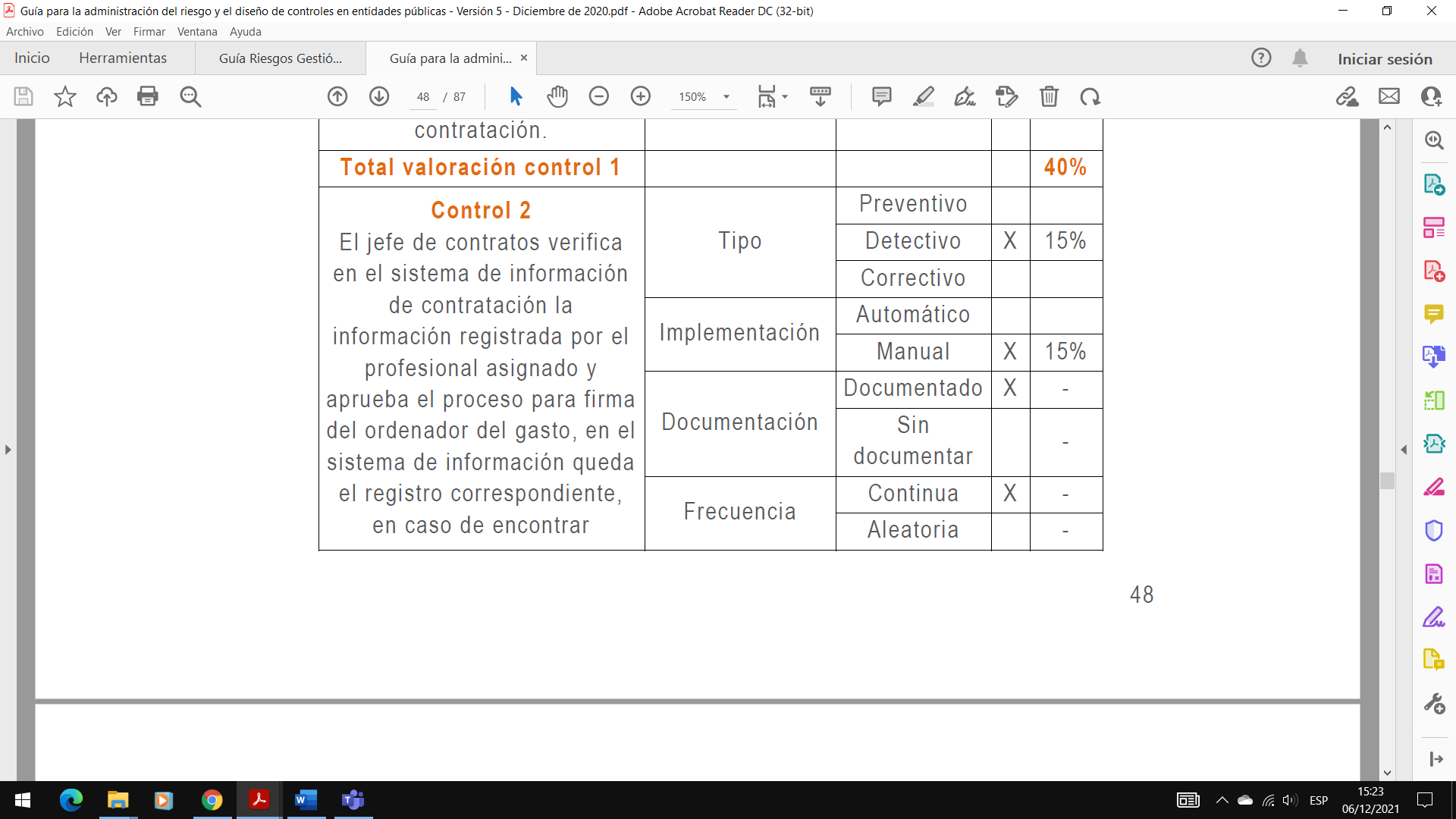
* ***Objetivo****:* adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación
* ***Riesgo identificado*:** posibilidad de afectación económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos
* ***Probabilidad Inherente***= moderada 60%
* ***Impacto Inherente***: mayor 80%
* ***Zona de riesgo***: alta
* ***Controles identificados***:

***Control 1*:** El profesional del grupo de contratos 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, los contratos que cumplen son registrados en el sistema de información de contratación.

***Control 2*:** El coordinador del grupo de contratos verifica en el sistema de información de contratación la información registrada por el profesional asignado y aprueba el proceso para firma del ordenador del gasto. En el sistema de información queda el registro correspondiente, en caso de encontrar inconsistencias, devuelve el proceso al profesional de contratos asignado.

En la siguiente tabla, se observa la aplicación de la tabla de atributos, esta le servirá como ejemplo para el análisis y valoración de los dos controles propuestos.





**Fuente:** *Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5*

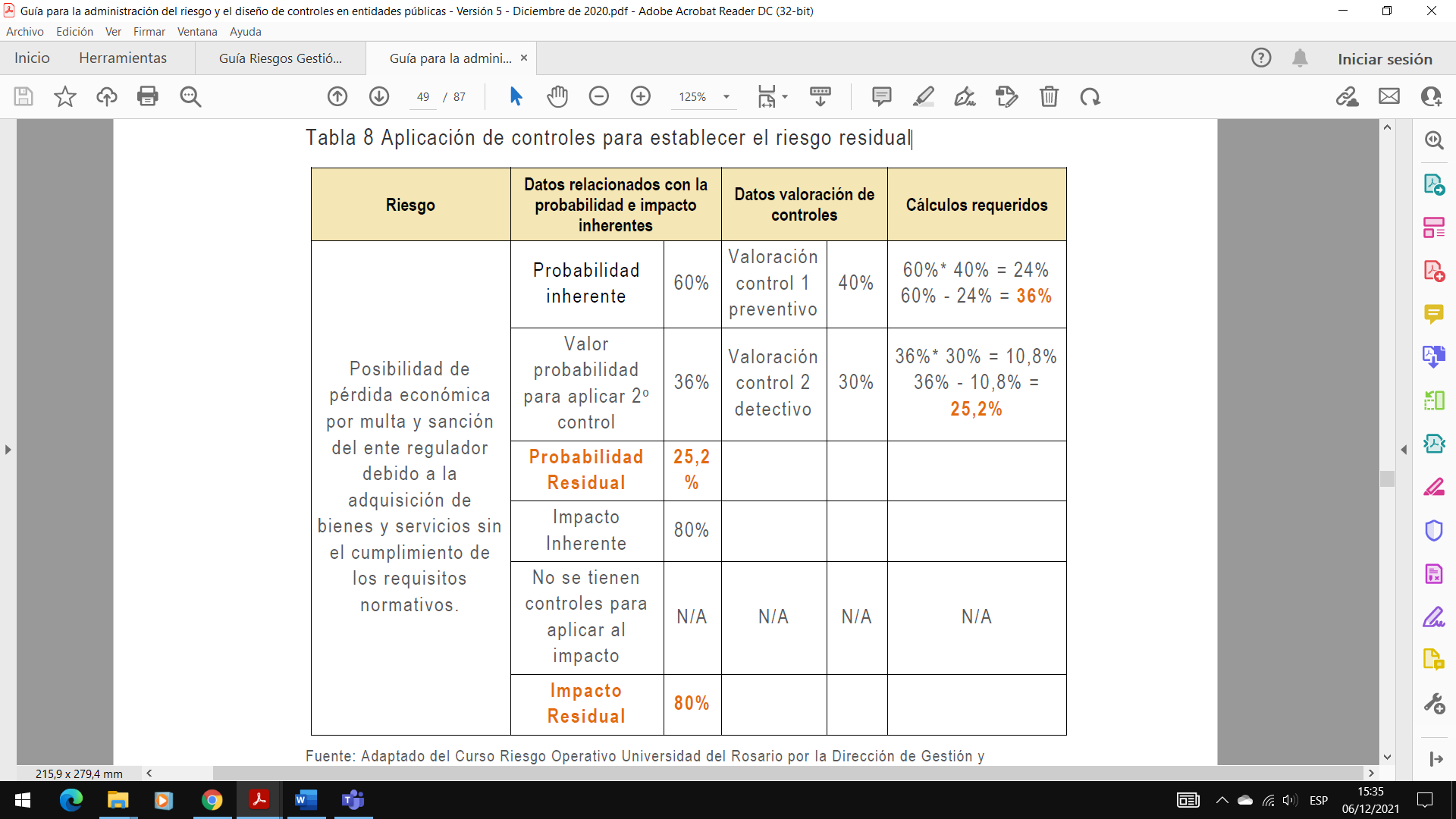
**Nota**: Para la adecuada mitigación de los riesgos no basta con que un control esté bien diseñado, el control debe ejecutarse por parte de los responsables tal como se diseñó. Un control que no se ejecute, o un control que se ejecute y esté mal diseñado, no van a contribuir a la mitigación del riesgo.

### **Nivel de riesgo (riesgo residual)**

Es el resultado de aplicar la “**EFECTIVIDAD”** de los controles al riesgo inherente.

Para la aplicación de los controles se debe tener en cuenta que estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control.

En la siguiente tabla, se observan los cálculos requeridos para la aplicación de los controles para obtener el riesgo residual:



**Fuente:** *Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5*

**Ejemplo** (continuación del ejemplo):

***Proceso*:** Gestión de recursos físicos

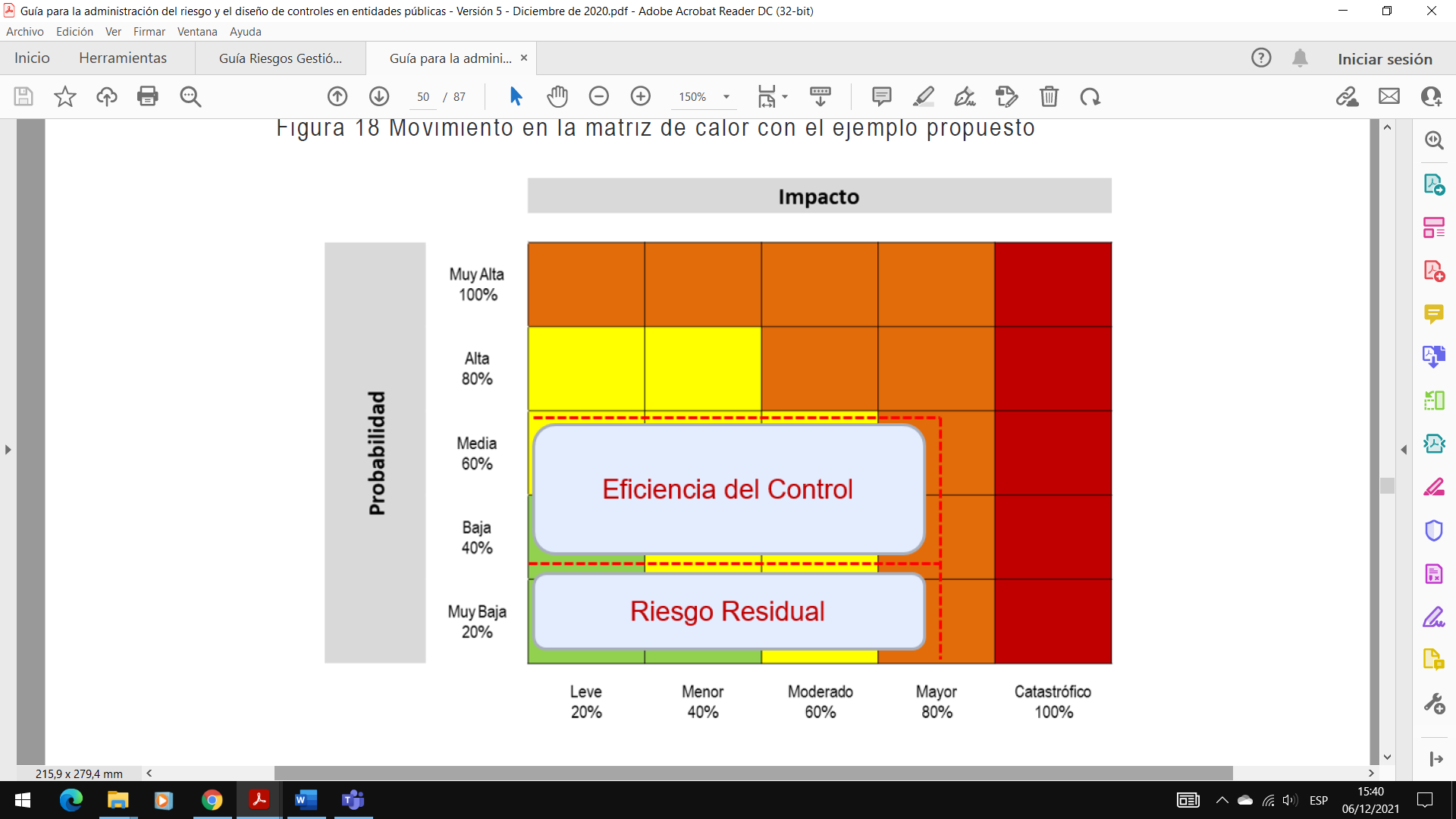
* ***Objetivo*:** adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación
* ***Riesgo identificado*:** posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.

*Probabilidad residual* = baja 26.8%

* ***Impacto Residual***: mayor 80%
* ***Zona de riesgo residual*:** alta

Para este caso, si bien el riesgo se mantiene en zona alta, se bajó el nivel de probabilidad de ocurrencia del riesgo.

En la siguiente figura se observa el movimiento en la matriz de calor.



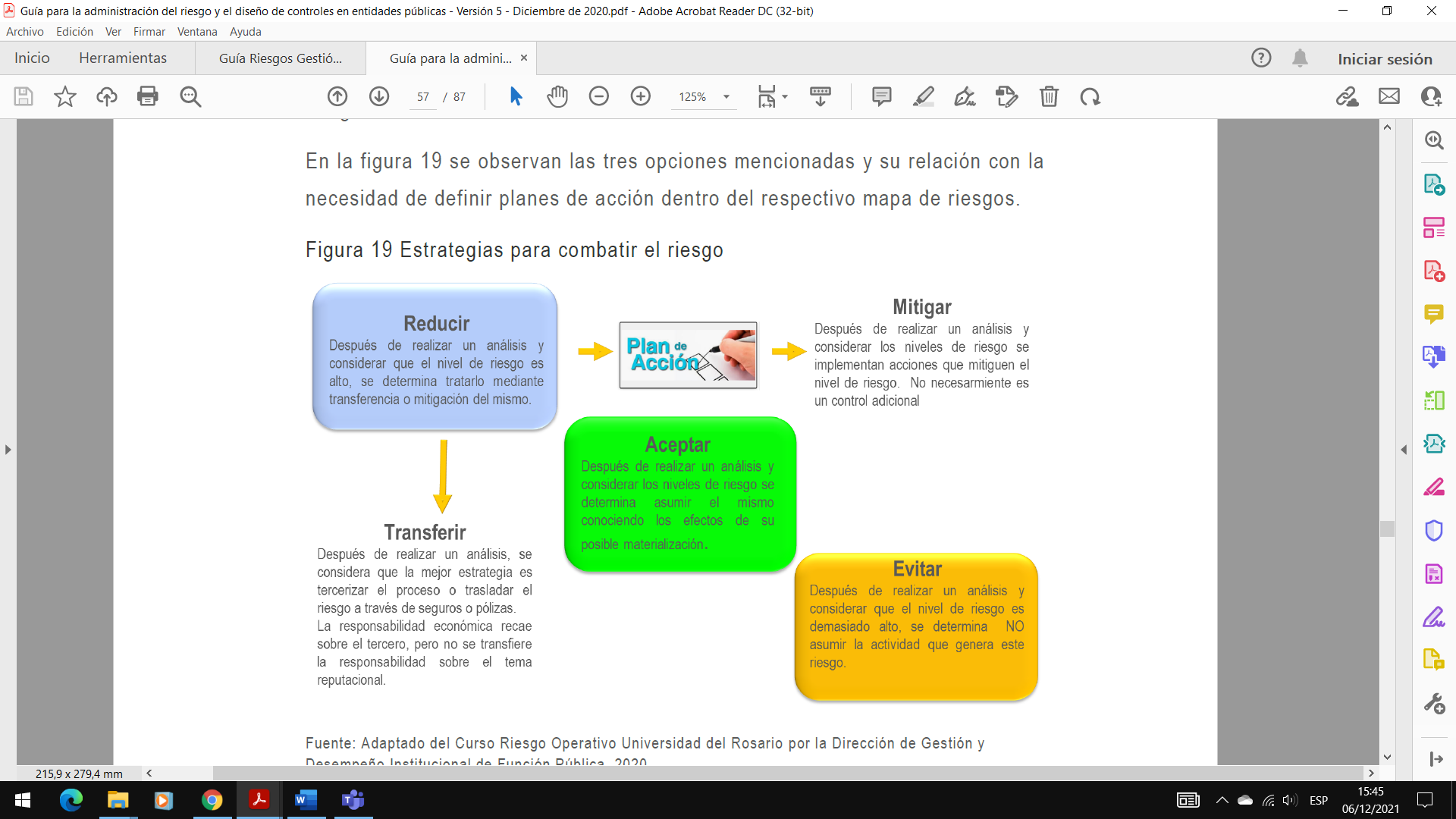
**Fuente:** *Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5*

**Nota:** En caso de **NO** contar con controles correctivos, el impacto residual es el mismo calculado inicialmente, es importante señalar que no será posible su movimiento en la matriz para el impacto.

### **Estrategias para combatir el riesgo**

Decisión que se toma frente a un determinado nivel de riesgo: Reducir (transferir o mitigar), Aceptar y Evitar.

**Nota:** Se analiza frente al riesgo residual, esto para procesos en funcionamiento, cuando se trate de procesos nuevos, se procede a partir del riesgo inherente.



**Fuente:** *Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5*

Frente al plan de acción referido para la opción de reducir, es importante mencionar que, conceptualmente y de manera general, se trata de una herramienta de planificación empleada para la gestión y control de tareas o proyectos.

Para efectos del mapa de riesgos, cuando se define la opción de reducir, se requerirá la definición de un plan de acción que especifique: i) responsable, ii) fecha de implementación, y iii) fecha de seguimiento.

**Nota**: El plan de acción antes referido es diferente a un plan de contingencia, el cual se enmarca en el Plan de Continuidad de Negocio y se consideraría un control correctivo.

## **Herramientas para la gestión del riesgo**

Como producto de la aplicación de la metodología se contará con los mapas de riesgo y otras herramientas, como son:

### **Gestión de eventos de materialización**

Un evento es un riesgo materializado, se puede considerar incidentes que generan pérdidas a la entidad, se debe contar con una base histórica de eventos que permita revisar si el riesgo fue identificado y qué sucedió con los controles. En caso de que el riesgo no se hubiese identificado, se debe incluir y dar el tratamiento correspondiente de acuerdo con la metodología.

Algunas fuentes para establecer una base histórica de eventos pueden ser:

* Mesa de ayuda
* Las PQRSD (peticiones, quejas, reclamos, solicitudes, denuncias)
* Oficina jurídica
* Líneas internas de denuncia

Este mecanismo genera información para que el evento no se vuelva a presentar, así mismo, es posible establecer el desempeño de los controles así:

Desempeño del control = # eventos / frecuencia del riesgo (# veces que se hace la actividad)

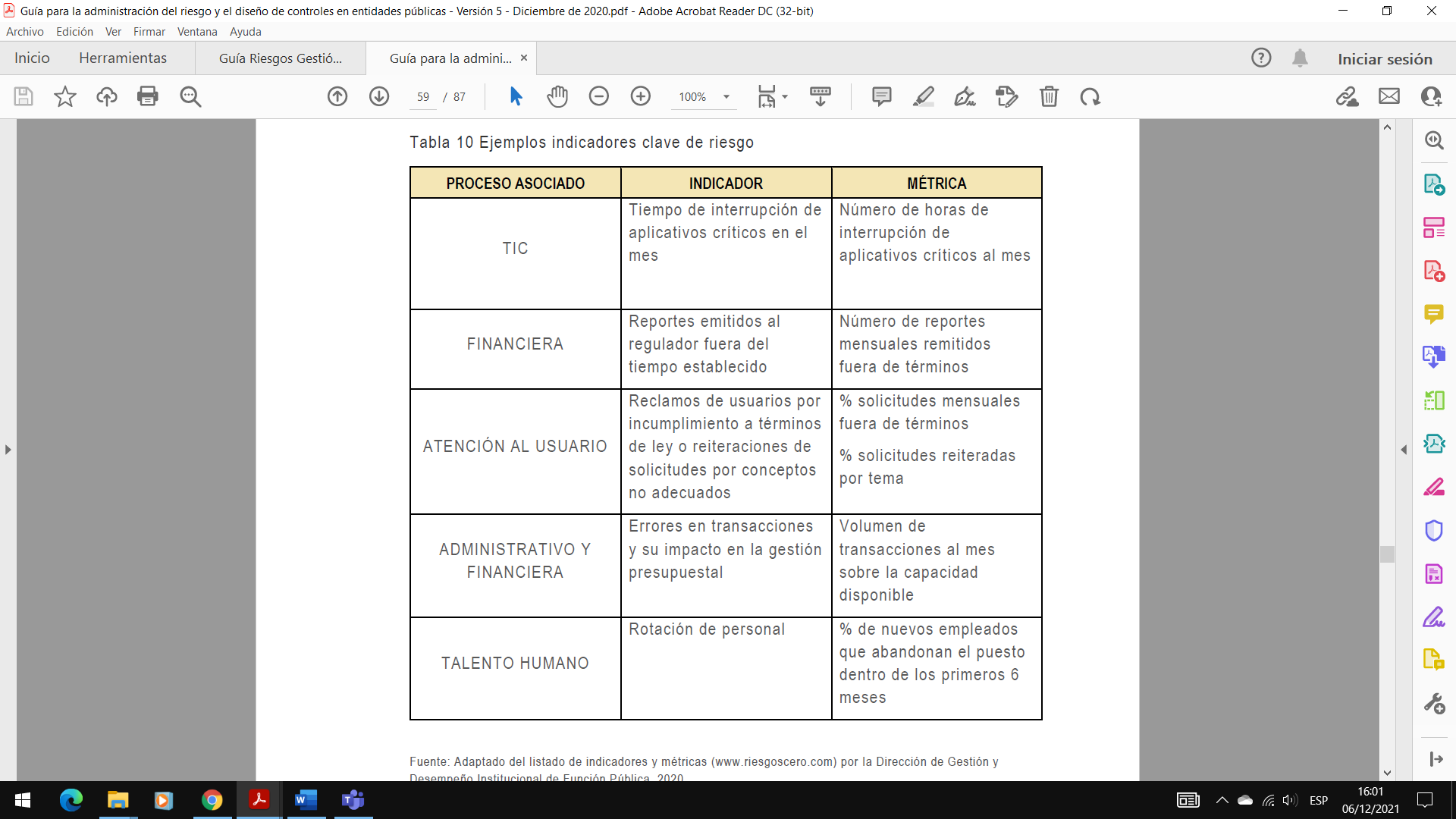
En el evento de materializarse un riesgo, es necesario que el líder del proceso realice los ajustes necesarios con acciones, tales como:

* Revisar el Riesgo, si en necesario reformularlo, revisar sus controles y acciones de tratamiento.
* Verificar si se tomaron las acciones de tratamiento y se actualizó el mapa Institucional de riesgos.
* Llevar a cabo un monitoreo permanente y seguimientos a las acciones definidas para resolver materializaciones de riesgo detectadas.

### **Indicadores clave de riesgo**

Hace referencia a una colección de datos históricos, por periodos de tiempo, relacionados con algún evento cuyo comportamiento puede indicar una mayor o menor exposición a determinados riesgos. No indica la materialización de los riesgos, pero sugiere que algo no funciona adecuadamente y, por lo tanto, se debe investigar.

Un indicador clave de riesgo, o KRI, por su sigla en inglés (Key Risk Indicators), permite capturar la ocurrencia de un incidente que se asocia a un riesgo identificado previamente y que es considerado alto, lo cual permite llevar un registro de ocurrencias y evaluar a través de su tendencia la eficacia de los controles que se disponen para mitigarlos. En la siguiente tabla se muestran algunos ejemplos de estos indicadores.



**Fuente:** *Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5*

### **Diseño de controles**

Es importante considerar que los controles estén bien diseñados, es decir, que efectivamente estos mitigan las causas que hacen que el riesgo se materialice.

Importante:

* 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).
* Un control puede ser tan eficiente que me ayude a mitigar varias causas, en estos casos se repite el control, asociado de manera independiente a la causa específica.

Estos, deben estar directamente relacionados con las causas identificadas para el riesgo con el fin de eliminarlas o mitigarlas. La administración del riesgo contribuirá a la gestión de la entidad en la medida en que los controles se diseñen, documenten, apliquen y sean efectivos para prevenir o mitigar los riesgos.

Lo primero que se debe hacer es definir:

* **Nombre del control:** asignar un nombre al control que debe tener explicita la ejecución de una acción; ejemplo: Realizar la tabulación mensual de las encuestas de satisfacción de usuarios.
* **Descripción:** definir de manera detalladacómo se ejecuta el control. Ejemplo: Para un control denominado validar el cumplimiento de los bienes a recibir, la descripción es: El profesional de almacén revisa las características de los bienes a recibir de acuerdo con la orden del pedido y las características definidas en el contrato, diligenciando el formato de recepción de bienes.
* **Donde está documentado el control:** Indique el documento del proceso en el cual está definido y aprobado el control. Ejemplo: en el procedimiento de administración de bienes y servicios.No es una opción válida para este campo indicar de forma genérica que se encuentra en los documentos del proceso.

A continuación, se presentan las variables “M**ínimas”** que debe tener un control desde la “**Redacción del control”**:

1. **Responsable de llevar a cabo la actividad de control:** persona asignada en un procedimiento del proceso u otro documento para ejecutar el control; la persona asignada, 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, para reducir así el riesgo de error o de actuaciones irregulares o fraudulentas (Riesgos de corrupción). Es importante establecer el cargo responsable de su realización; cuando el control lo hace un sistema o una aplicación de manera automática a través de un sistema programado, es importante establecer como responsable de ejecutar el control al sistema o aplicación.
2. **Periodicidad:** el control debe tener una periodicidad específica para su realización (diario, mensual, trimestral, anual, etc.) y su ejecución debe ser consistente y oportuna para la mitigación del riesgo. Hay controles que no tienen una periodicidad específica como, por ejemplo, los controles que se ejecutan en el proceso de contratación de proveedores solo se ejecutan cuando se contratan proveedores. La periodicidad debe quedar redactada de tal forma que indique: que cada vez que se desarrolla la actividad se ejecuta el control.
3. **Propósito:** El control debe tener un propósito que indique para qué se realiza, y que ese propósito conlleve a prevenir las causas que generan el riesgo (verificar, validar, conciliar, comparar, revisar, cotejar) o detectar la materialización del riesgo, con el objetivo de llevar a cabo los ajustes y correctivos en el diseño del control o en su ejecución. El solo hecho de establecer un procedimiento o contar con una política por sí sola, no va a prevenir o detectar la materialización del riesgo o una de sus causas.
4. **Como se realiza el control:** El control debe indicar el cómo se realiza, de tal forma que se pueda evaluar si la fuente u origen de la información que sirve para ejecutar el control es confiable para la mitigación del riesgo. Cuando estemos evaluando el control debemos preguntarnos si la fuente de información utilizada es confiable. Ejemplo: Cada vez que se va a realizar un contrato el profesional de contratación 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.
5. **Qué pasa con las observaciones o desviaciones resultantes de ejecutar el control:** Al momento de evaluar si un control está bien diseñado para mitigar el riesgo, si como resultado de un control preventivo se observan diferencias o aspectos que no se cumplen, la actividad no debería continuarse hasta que se subsane la situación o si es un control que detecta una posible materialización de un riesgo, deberían gestionarse de manera oportuna los correctivos o aclaraciones a las diferencias presentadas u observaciones. Ejemplo: En caso de encontrar información faltante, requiere al proveedor a través de correo para el suministro de la información y poder continuar con el proceso de contratación.
6. **Evidencias de aplicación del control:** El control debe dejar evidencia de su ejecución. Esta evidencia ayuda a que se pueda revisar la misma información por parte de un tercero y llegue a la misma conclusión de quien ejecutó el control y se pueda evaluar que el control realmente fue ejecutado de acuerdo con los parámetros establecidos y descritos anteriormente:

1. Fue realizado por el responsable que se definió.

2. Se realizó de acuerdo con la periodicidad definida.

3. Se cumplió con el propósito del control.

4. Se dejó la fuente de información que sirvió de base para su ejecución.

5. Hay explicación a las observaciones o desviaciones resultantes de ejecutar el control.

## **Monitoreo y revisión**

La entidad debe asegurar el logro de sus objetivos anticipándose a los eventos negativos relacionados con su gestión. El Modelo Integrado de Planeación y Gestión-MIPG, desarrollada en la dimensión 7 Control Interno las líneas de defensa para identificar la responsabilidad de la gestión del riesgo y control que está distribuida en diversos servidores de la entidad como fue definido en el numeral 4.1. Responsabilidades – líneas de Defensa de esta guía.

* **Línea Estratégica**

Define el marco general para la gestión del riesgo, el control y supervisa su cumplimiento, está a cargo de la alta dirección y el Comité Institucional de Coordinación de Control Interno - CICCI.

Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora.

* **Primera Línea de Defensa**

Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora.

* **Segunda Línea de Defensa**

Asegura que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende.

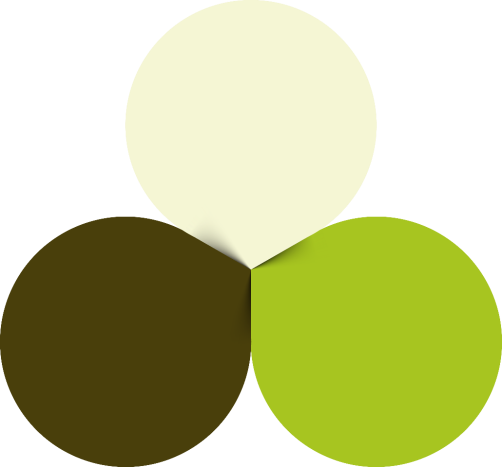
* **Tercera Línea de Defensa**

Proporciona información sobre la efectividad del Sistema de Control Interno - SCI, a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa.

En esta etapa debe hacerse un seguimiento periódico a la gestión de los riesgos sobre la operación adecuada de los controles atendiendo la periodicidad establecida para cada uno, mediante el reporte de información relacionada con:

* **Estado de aplicación del control**: descripción de la operación para cada control durante el periodo, de acuerdo con los cortes de monitoreo establecidos.
* **Evidencias de operación del control:** se deben adjuntar los soportes que evidencien la operación del control durante el periodo o citar la URL donde se encuentran ubicadas.
* **Efectividad del control:** se debe indicar si el control ha sido efectivo o no en la gestión del riesgo durante el periodo; en caso de identificar un control no efectivo; se deben realizar los ajustes correspondientes en la etapa de valoración.

A partir de la información registrada por los líderes de proceso en el monitoreo, la Oficina Asesora de Planeación realizará seguimiento trimestral al estado de aplicación de los controles. Posteriormente, la Oficina de Control Interno, de acuerdo con los ciclos establecidos en el plan de auditoría, realizará la evaluación independiente de los riesgos identificados y gestionados en la entidad.



**AUTOCONTROL.** Cada cuatro meses los responsables deberán registrar el monitoreo de los riesgos identificados.

**PLANEACIÓN.** Realiza el informe de seguimiento cuatrimestral con base en la información reportada por los responsables.

**CONTROL INTERNO.** Realiza la evaluación independiente para determinar

### **Definición del semáforo del riesgo.**

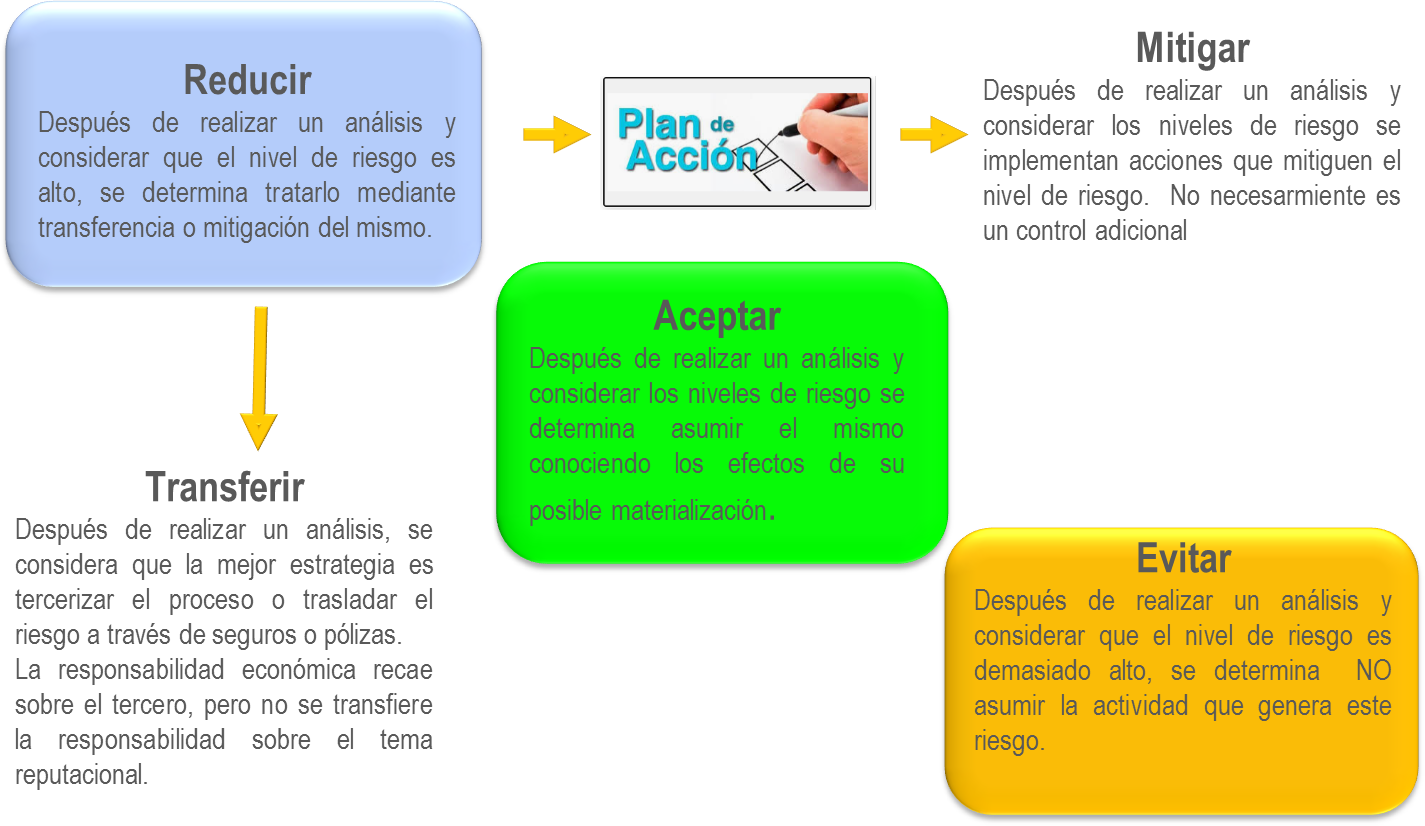
El SIGPARTICIPO presentará los riesgos y su semáforo; las opciones disponibles en el sistema son:

* Sobre el estado y documentación oportuna de las acciones que se asocien para el manejo del riesgo.
* Sobre el estado y reporte que se realice de los indicadores que se asocien al riesgo.
* Sobre el cumplimiento de las fechas de monitoreo establecidas en la Entidad para que cada responsable.
* A partir de la evaluación residual del riesgo.

De acuerdo con los lineamientos institucionales, el semáforo de todos los riesgos se debe calcular con la opción de evaluación residual del riesgo.

### **Determinación de la opción de tratamiento para el riesgo**

Para esta etapa deberán tenerse en cuenta las siguientes opciones:



**Fuente:** *Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5*

* **Aceptar el riesgo**: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo.
* **Reducir el riesgo**: Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles.
* **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 de este. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad.

Estas opciones se determinan teniendo en cuenta la ubicación del riesgo residual y la calificación del conjunto de controles:

| **ZONA DE RIESGO** | **OPCIONES DE MANEJO** |
| --- | --- |
| BAJA | Asumir el riesgo / Reducir el riesgo |
| MODERADA | Reducir el riesgo / Evitar el riesgo / Compartir o transferir el riesgo |
| ALTA | Reducir el riesgo / Evitar el riesgo / Compartir o transferir el riesgo |
| EXTREMA | Reducir el riesgo / Evitar el riesgo / Compartir o transferir el riesgo |

**Fuente:** *Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5*

# LINEAMIENTOS SOBRE LOS RIESGOS RELACIONADOS CON POSIBLES ACTOS DE CORRUPCIÓN

Recuerde que un riesgo de corrupción es “la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado. “Esto implica que las prácticas corruptas son realizadas por actores públicos y/o privados con poder e incidencia en la toma de decisiones y la administración de los bienes públicos” (Conpes N° 167 de 2013)”.

**Por ejemplo:** Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.

Tenga en cuenta en la identificación de estos riesgos:

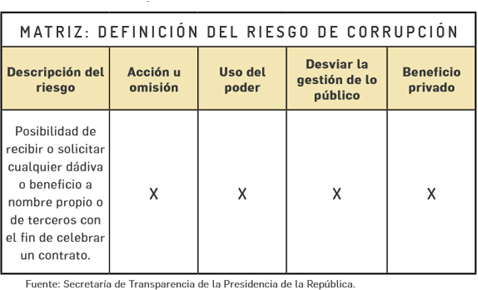
* Los riesgos de corrupción se establecen sobre el proceso
* Los riesgos de corrupción siempre deben gestionarse.
* El riesgo debe estar descrito de manera clara y precisa.
* Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos.

Con el fin de facilitar la identificación de riesgos de corrupción y evitar que se presenten confusiones entre un riesgo de gestión y uno de corrupción, se sugiere la utilización de la matriz de definición de riesgo de corrupción, que incorpora cada uno de los componentes de su definición.

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

***Acción U Omisión + Uso del Poder + Desviación de la Gestión de lo Público + El Beneficio Privado.***

Usando la siguiente matriz de comprobación, si se marca con una X en la descripción del riesgo que aparece en cada casilla quiere decir que se trata de un riesgo de corrupción:



**Fuente:** *Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5*

A continuación, se presenta un ejemplo de un riesgo de corrupción:

| **RIESGO** | **DESCRIPCIÓN** | **TIPO** | **CAUSAS** | **CONSECUENCIAS** |
| --- | --- | --- | --- | --- |
| Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de 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 | 1. 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.  2. Presiones indebidas.  3. Carencia de controles en el procedimiento de contratación.  4. Falta de conocimiento y/o experiencia del personal que maneja la contratación  5. Excesiva discrecionalidad  6. Adendas que modifican las condiciones generales del proceso de contratación para favorecer a un proponente. | 1. Pérdida de la imagen institucional.  2. Demandas contra el Estado.  3. Pérdida de confianza en lo público.  4. Investigaciones penales, disciplinarias y fiscales.  5. Detrimento patrimonial.  6. Obras inconclusas.  7. Mala calidad de las obras. 8. Enriquecimiento ilícito de contratistas y/o servidores públicos. |

## **Valoración de los riesgos de corrupción**

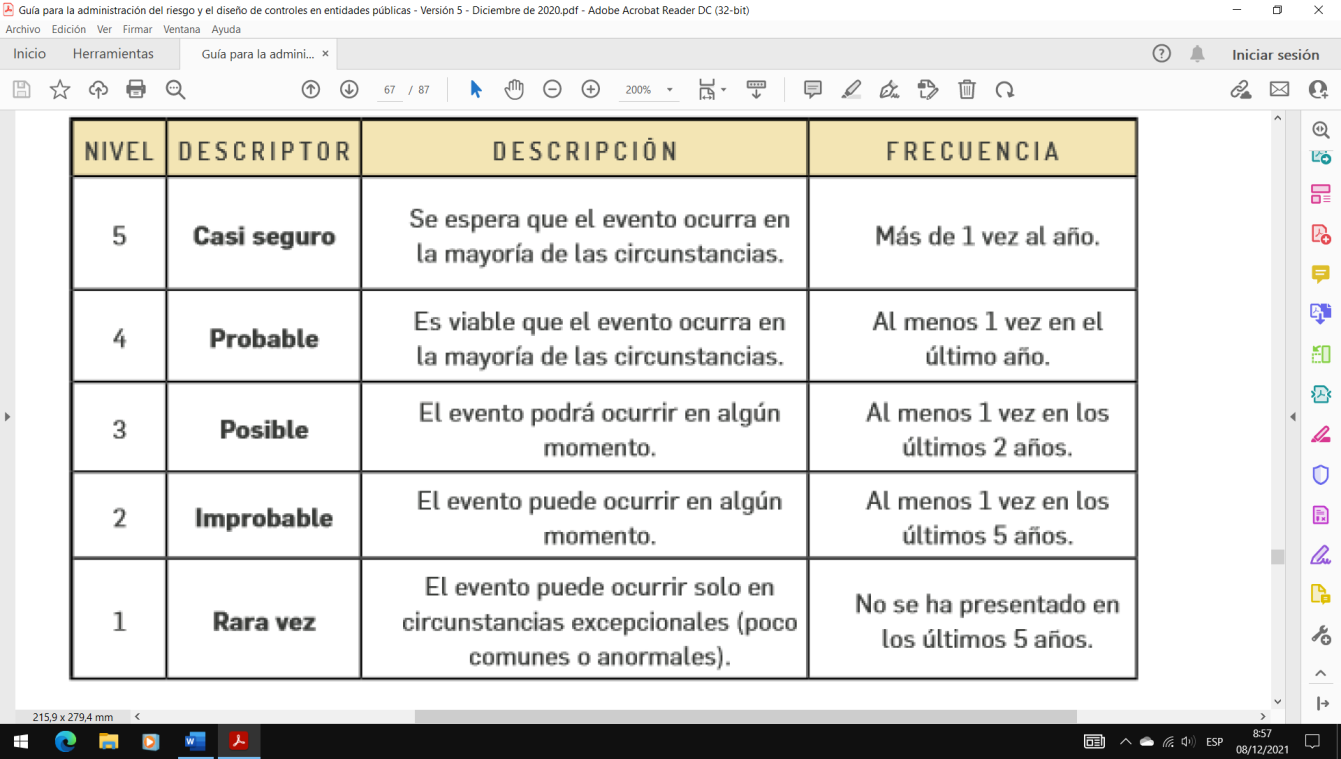
Una vez definido el riesgo de corrupción y comprobado que concurren los cuatro componentes, se procede a calcular la probabilidad e impacto.

## **Análisis de la probabilidad**

Se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de frecuencia o factibilidad.

* **Frecuencia:** Implica analizar el número de 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:** Implica analizar 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 suceda.

Veamos los criterios a usar para calificar la probabilidad.



**Fuente:** *Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5*

## **Análisis de impacto**

El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo. Debe realizarse respondiendo de manera afirmativa o negativa en el siguiente cuestionario que contiene los criterios:

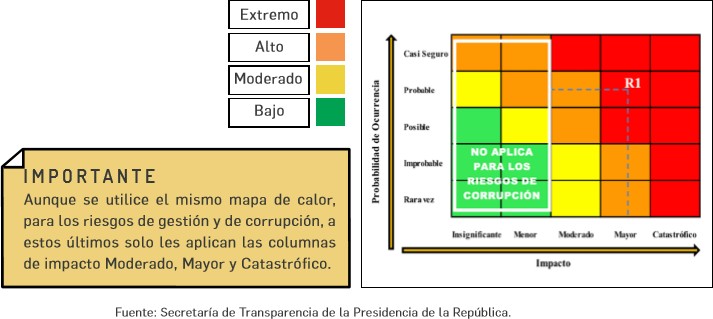
| ***Nº*** | ***PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...*** | ***SI*** | ***NO*** |
| --- | --- | --- | --- |
| ***1*** | *¿Afectar al grupo de funcionarios del proceso?* | *X* |  |
| ***2*** | *¿Afectar el cumplimiento de metas y objetivos de la dependencia?* | *X* |  |
| ***3***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

**Fuente:** *Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5*

**Importante:**

* Si la respuesta a la pregunta 16 es afirmativa, el riesgo se considera CATASTRÓFICO.
* Por cada riesgo de corrupción identificado por el proceso, se debe responder el cuestionario.
* Para los riesgos de corrupción, el análisis de impacto se realizará teniendo en cuenta solamente los niveles “**moderado**”, “**mayor**” y “**catastrófico**”, dado que estos riesgos siempre serán significativos; en este orden de ideas, no aplican los niveles de impacto insignificante y menor, que sí aplican para los demás riesgos.

Ahora, ubique en el mapa de calor el punto de intersección resultante de la **probabilidad** y el **impacto** para establecer el nivel del “**Riesgo inherente”.**

****

**Fuente:** *Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5*

*Es importante resaltar que cuando hablamos de Riesgos de Corrupción únicamente hay disminución de probabilidad. Es decir, para el impacto no opera el desplazamiento.*

Recuerde, que el **riesgo inherente** es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto, y se obtiene comparando los resultados de la calificación, con los criterios definidos para establecer el grado de exposición al riesgo; de esta forma, se define la zona de ubicación del riesgo inherente; esta evaluación se realiza de manera automática por SIG participo.

El **riesgo residual** está relacionado con el desplazamiento del riesgo inherente en el mapa de riesgos, es decir, dado que ningún riesgo con una medida de tratamiento se puede evitar o eliminar, se deberá tener en cuenta el desplazamiento de un riesgo inherente (antes de formular controles) en su probabilidad o impacto para el cálculo del riesgo residual (después de formulados los controles). Es importante precisar que, para los riesgos de corrupción únicamente hay disminución de probabilidad, pero nunca de impacto.

## **Valoración de los controles – diseño de controles**

El diseño de los controles de los riesgos de corrupción se realizará conforme a los lineamientos establecidos en el numeral 5.2.4.3., de la presente guía.

Es importante comprobar que los controles estén bien diseñados, es decir, que efectivamente estos mitigan las causas que hacen que el riesgo se materialice; por tanto, su valoración se realiza de acuerdo con lo definido en el numeral 6.2.12 de esta guía.

## **Generalidades acerca de los riesgos de corrupción**

* **El mapa de riesgos de corrupción se elabora anualmente** por cada líder de proceso al interior de la entidad junto con su equipo.
* **Consolidación:** La Oficina Asesora de Planeación, le corresponde liderar el proceso de administración de estos. Adicionalmente, esta misma oficina será la encargada de consolidar el mapa de riesgos de corrupción.
* **Publicación del mapa de riesgos de corrupción:** se debe publicar en el portal web de la entidad, en la sección de transparencia y acceso a la información pública o en un medio de fácil acceso al ciudadano, a más tardar el 31 de enero de cada año. La publicación será fundamentada en la elaboración del índice de información clasificada y reservada. En dicho instrumento la entidad debe establecer las condiciones de reserva y clasificación de algunos de los elementos constitutivos del mapa de riesgos en los términos dados en los artículos 18 y 19 de la Ley 1712 de 2014.

En este caso se deberá anonimizar esa información. Es decir, la parte clasificada o reservada, aunque se elabora, no se hace visible en la publicación. Recuerde que las excepciones solo pueden estar establecidas en la ley, un decreto con fuerza de ley o un tratado internacional ratificado por el Congreso o en la Constitución.

* **Socialización**: Los servidores públicos y contratistas de la entidad deben conocer el mapa de riesgos de corrupción antes de su publicación; lo cual se hace mediante el envío de correos masivos y jornada de socialización con los enlaces de los procesos.
* **Ajustes y modificaciones:** se podrán llevar a cabo los ajustes y modificaciones necesarias orientadas a mejorar el mapa de riesgos de corrupción después de su publicación y durante el respectivo año de vigencia. En este caso deberán dejarse por escrito los ajustes, modificaciones o inclusiones realizadas.

## **Tratamiento del riesgo**

Es la respuesta establecida por la primera línea de defensa 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, y partiendo de lo que establezca la política de administración del riesgo, los líderes de los procesos tendrán en cuenta la importancia del riesgo, para lo cual, tendrán en cuenta el efecto que puede tener la materialización del riesgo para la entidad, así como su probabilidad e impacto y la relación costo-beneficio de las medidas identificadas para su tratamiento.

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, reducir o compartir el riesgo. Para la entidad se tendrán en cuenta los siguientes criterios dentro del tratamiento de riesgo:

Para esta etapa deberán tenerse en cuenta las siguientes opciones:

* **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 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 de este. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad.

Estas opciones se determinan teniendo en cuenta la ubicación del riesgo residual y la calificación del conjunto de controles:

| **ZONA DE RIESGO** | **OPCIONES DE MANEJO** |
| --- | --- |
| BAJA | Asumir el riesgo / Reducir el riesgo |
| MODERADA | Reducir el riesgo / Evitar el riesgo / Compartir o transferir el riesgo |
| ALTA | Reducir el riesgo / Evitar el riesgo / Compartir o transferir el riesgo |
| EXTREMA | Reducir el riesgo / Evitar el riesgo / Compartir o transferir el riesgo |

**Fuente:** *Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5*

## **Monitoreo de riesgos de corrupción**

En concordancia con la cultura del autocontrol al interior de la entidad, los líderes de los procesos junto con su equipo realizarán monitoreo y evaluación permanente a la gestión de riesgos de corrupción.

Le corresponde, igualmente, a la Oficina Asesora de Planeación adelantar el monitoreo (segunda línea de defensa), para este propósito se elaborará un documento que consolide el monitoreo realizado. Dicho monitoreo será con periodicidad trimestral y presentado al Comité Institucional de Gestión y Desempeño – CIGD.

Su importancia radica en la necesidad de llevar a cabo un seguimiento constante a la gestión del riesgo y a la efectividad de los controles establecidos. Teniendo en cuenta que la corrupción es, por sus propias características, una actividad difícil de detectar. Para tal efecto deben atender a los lineamientos y las actividades descritas en la primera y segunda línea de defensa.

## **Seguimiento**

La Oficina de Control Interno debe adelantar seguimiento a la gestión de riesgos de corrupción. En este sentido es necesario que en sus procesos de auditoríainterna analice las causas, los riesgos de corrupción y la efectividad de los controles incorporados en el mapa de riesgos de corrupción.

La Oficina de Control Interno, deberá adelantar las siguientes actividades:

1. Verificar la publicación del Mapa de Riesgos de Corrupción en el portal web de la entidad.
2. Seguimiento a la gestión del riesgo.
3. Revisión de los riesgos y su evolución.
4. Asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma adecuada.

* **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.

El seguimiento adelantado por la Oficina de Control Interno se deberá publicar en el portal web de la entidad en el link de Transparencia y Acceso a la Información Pública.

## **Acciones para seguir en caso de materialización de riesgos de corrupción**

En el evento de materializarse un riesgo de corrupción, es necesario que el líder del proceso realice los ajustes necesarios con acciones, tales como:

1. Informar a las autoridades de la ocurrencia del hecho de corrupción.
2. Revisar el mapa de riesgos de corrupción, en particular, las causas, riesgos y controles.
3. Verificar si se tomaron las acciones y se actualizó el mapa de riesgos de corrupción.
4. Llevar a cabo un monitoreo permanente.

La Oficina de Control Interno debe adelantar las siguientes acciones:

* Determinar la efectividad de los controles.
* Mejorar la valoración de los riesgos.
* Mejorar los controles.
* Analizar el diseño e idoneidad de los controles y si son adecuados para prevenir o mitigar los riesgos de corrupción.
* Determinar si se adelantaron acciones de monitoreo.
* Revisar las acciones del monitoreo.

# LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La política de seguridad digital se vincula al Modelo de Seguridad y Privacidad de la Información (MSPI); por tanto, se recomienda conocerla antes de iniciar la identificación de los riesgos de seguridad digital.

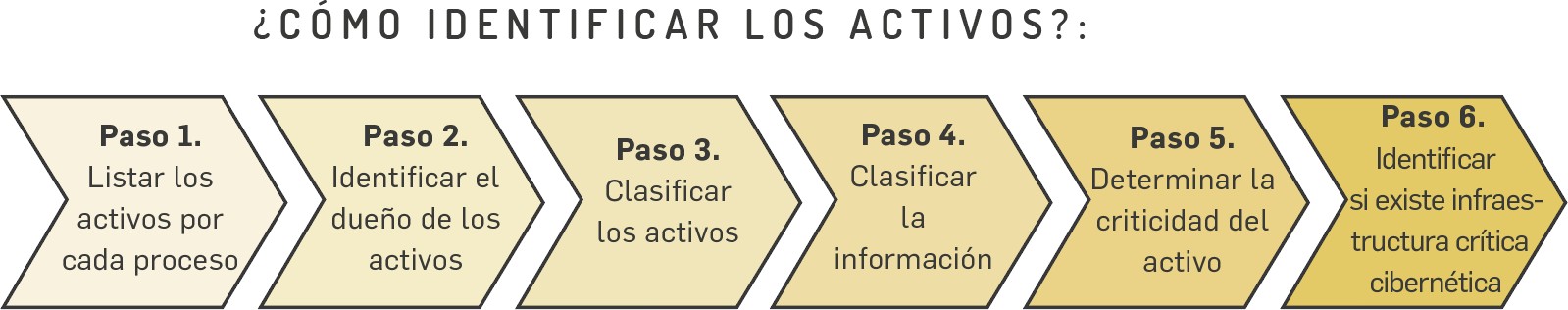
## **Identificación de los activos de seguridad de la información**

Se deben identificar los activos de información del proceso, para lo cual dará aplicación al procedimiento definido para tal fin. Un activo es cualquier elemento que tenga valor para el proceso, sin embargo, en el contexto de seguridad digital, son activos:

* Aplicaciones de la organización
* Servicios web
* Redes
* Información física o digital
* Tecnologías de información -TI
* Tecnologías de operación -TO.

El inventario de activos permite determinar qué es lo más importante que el proceso posee; sean bases de datos, archivos, servidores web o aplicaciones claves para que el proceso pueda prestar sus servicios.

El proceso debe tener claridad qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano o partes interesadas, aumentando así su confianza en el uso del entorno digital.

Para identificar estos ACTIVOS, el proceso debe cumplir con seis (6) pasos: 

**Fuente:** *Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5*

**Nota:** Para la identificación de activos deberá remitirse a la sección 3.1.6 del anexo 4 “Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en entidades públicas”.

La identificación de los activos de seguridad de la información del proceso se consolida en una matriz y contiene como mínimo los siguientes ítems:

* Nombre del activo
* Descripción del activo
* Tipo de activo
* Clasificación según Ley 1712 de 2014
* Clasificación Ley 581 de 2012
* Criticidad respecto a su confidencialidad
* Criticidad respecto a completitud o integridad
* Criticidad respecto a su disponibilidad
* Nivel de criticidad

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. Las amenazas representan situaciones o fuentes que pueden hacer daño a los activos y materializar los riesgos. Existen amenazas comunes cuyo origen puede ser deliberado (D), fortuito (F) o Ambiental (A) como el mal funcionamiento del equipo, el fuego y/o la saturación del sistema de información y otras serán amenazas dirigidas por el hombre como por ejemplo: ataques contra el sistema y/o hurto de información. Con respecto a las vulnerabilidades, estas últimas pueden ser: mantenimiento insuficiente, conexión deficiente de cableado y/o red eléctrica inestable.

***NOTA:*** *La sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.*

**1**

## **Identificación del riesgo**

Se pueden identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

1. Pérdida de la confidencialidad
2. Pérdida de la integridad
3. Pérdida de la disponibilidad

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. Para este efecto, es necesario consultar el **Anexo 4**. Modelo Nacional de Gestión de Riesgos de Seguridad de la Información para entidades públicas, donde se encuentran las siguientes tablas necesarias para este análisis:

* Tabla 5. Tabla de amenazas comunes
* Tabla 6. Tabla de amenazas dirigida por el hombre
* Tabla 7. Tabla de vulnerabilidades comunes

La identificación y valoración de activos debe ser realizada por la primera línea de defensa – líderes de proceso, en aquellos que aplique la gestión del riesgo de seguridad digital, siendo debidamente orientados por el responsable de seguridad digital o de seguridad de la información de la entidad.

A continuación, se presenta la tabla de amenazas y vulnerabilidades de acuerdo con el tipo de activo, ejemplo textual de la guía de administración del riesgo, versión 5

| Tipo de activo | Ejemplos de vulnerabilidades | Ejemplos de amenazas |
| --- | --- | --- |
| Hardware | Almacenamiento de medios sin protección | Hurto de medios o documentos |
| Software | Ausencia de parches de seguridad | Abuso de los derechos |
| Red | Líneas de comunicación sin protección | Escucha encubierta |
| Información | Falta de controles de acceso físico | Hurto de información |
| Personal | Falta de capacitación en las herramientas | Error en el uso |
| Organización | Ausencia de políticas de seguridad | Abuso de los derechos |

Ejemplo de identificación del riesgo sobre un activo como es la base de datos de nómina.

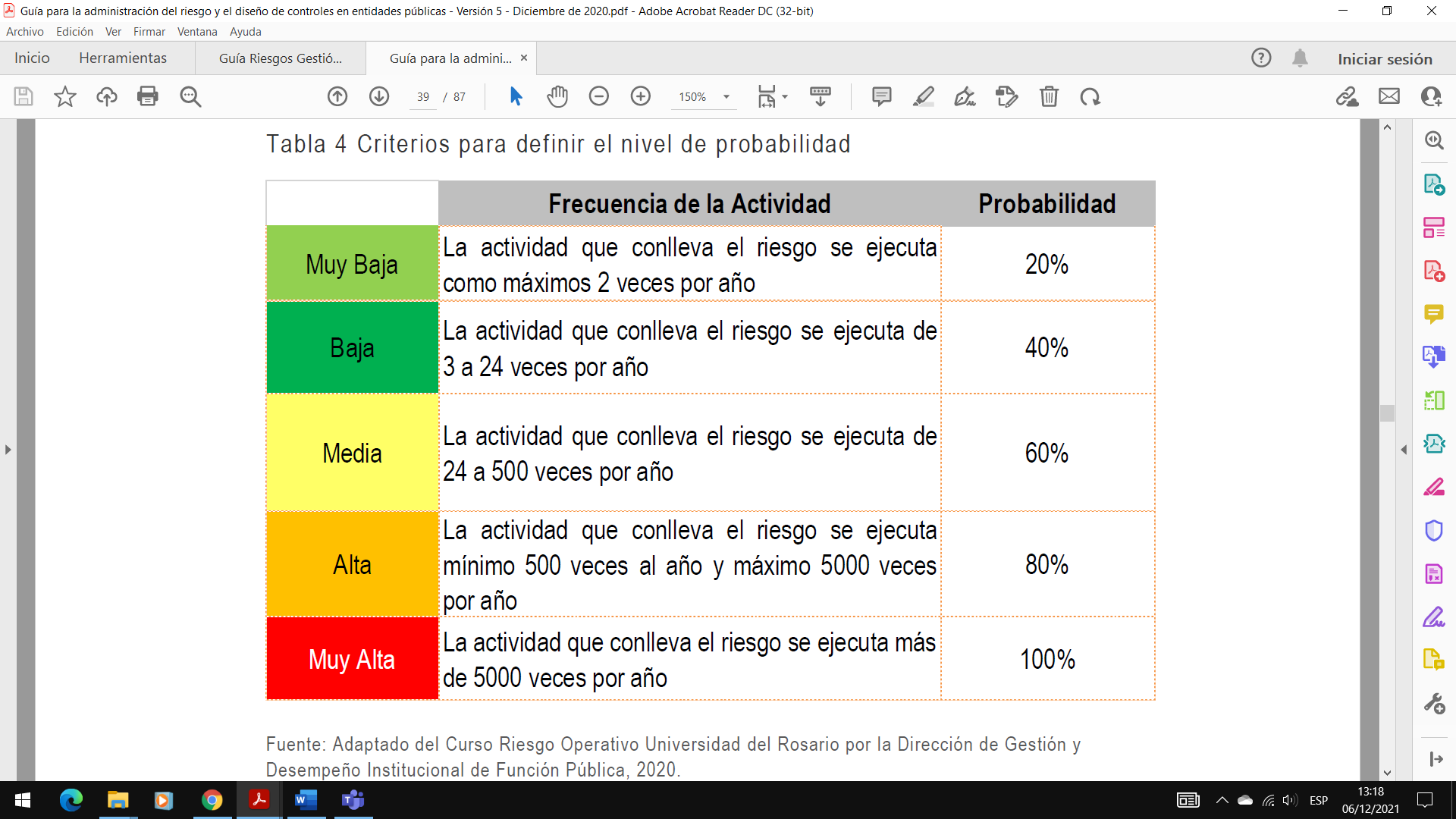
| **RIESGO** | **ACTIVO** | **DESCRIPCIÓN DEL RIESGO** | **AMENAZA** | **TIPO** | **CAUSAS/**  **VULNERABILIDADES** | **CONSECUENCIAS** |
| --- | --- | --- | --- | --- | --- | --- |
| Base de datos de nómina | Pérdida de la integridad | La falta de políticas de seguridad digital, ausencia de políticas 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. | Modificación no autorizada | Seguridad digital | Falta de políticas de seguridad digital  Ausencia de políticas de control de acceso  Contraseñas sin protección  Autenticación débil | 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. |

## **Valoración del riesgo de seguridad de la información**

Para esta etapa se asociarán las tablas de probabilidad e impacto definidas en la guía.

### **Análisis de la probabilidad del riesgo de seguridad de la información**

La determinación de la probabilidad se debe llevar de acuerdo con:



**Fuente:** *Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5*

### **Análisis del impacto de seguridad de la información**

La determinación del impacto se debe llevar a cabo de acuerdo con:



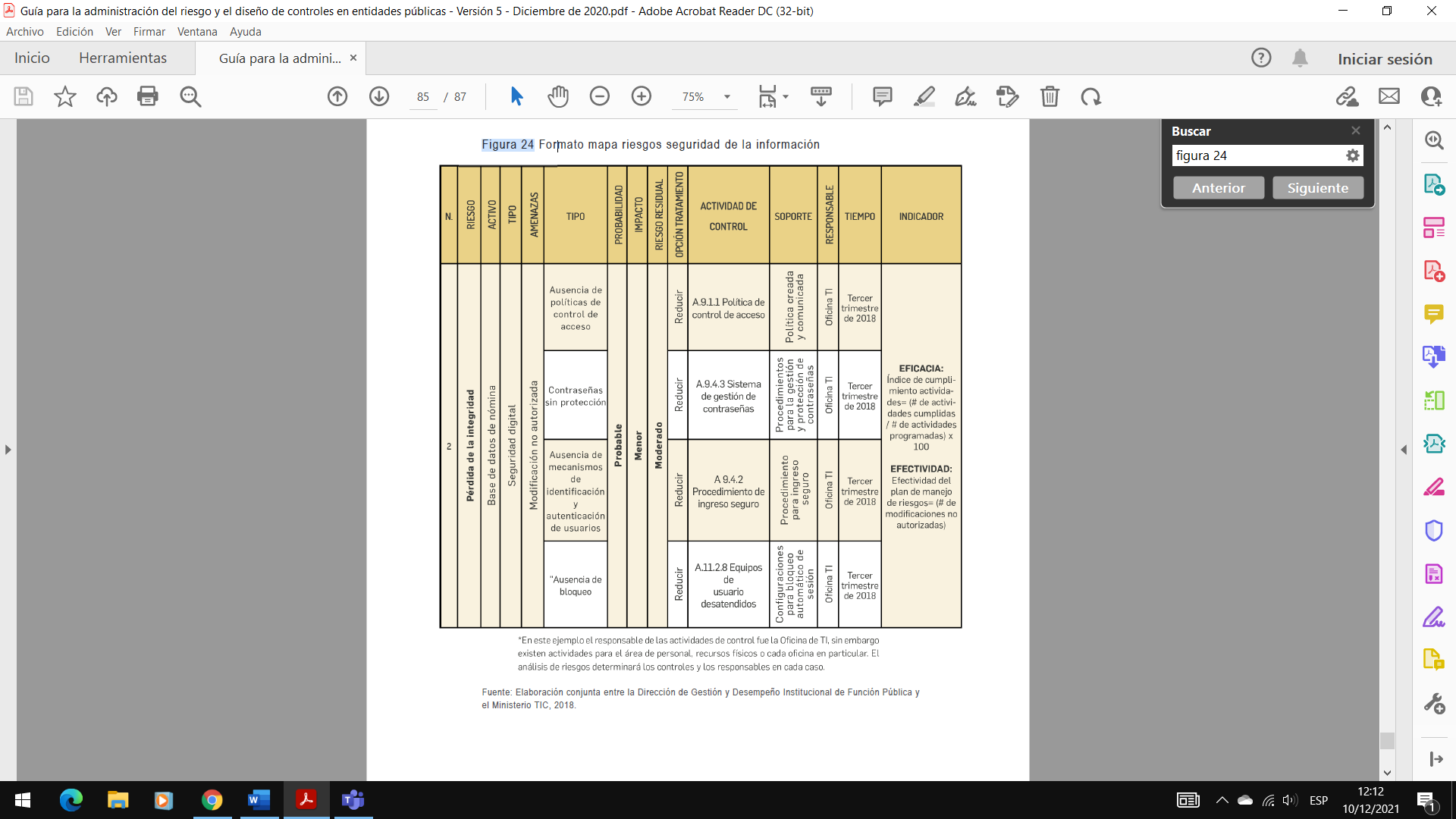
**Fuente:** *Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5*

Entendiendo que el impacto se define como la consecuencia económica y reputacional que se genera por la materialización del riesgo. Para el análisis preliminar (riesgo inherente), en esta etapa se define el nivel de severidad para el riesgo de seguridad de la información identificado, para ello, se aplica la siguiente matriz de calor:



**Fuente:** *Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5*

En la siguiente ilustración, se observa un ejemplo aplicando la etapa de valoración del riesgo, sobre un ACTIVO como es la base de datos de nómina.

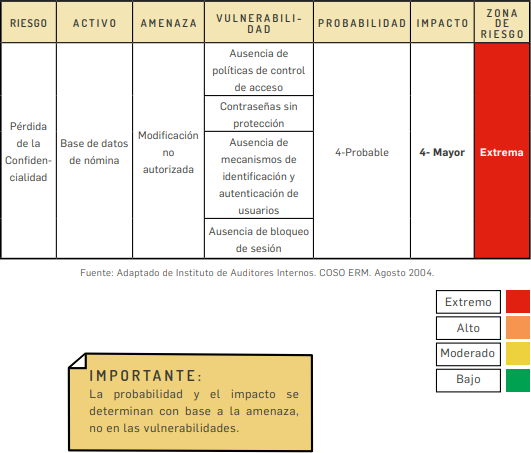


**Fuente:** *Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5*

En este ejemplo el responsable de ejecutar las actividades de control es la Oficina de TI, no obstante, existen actividades bajo la responsabilidad de ejecución de otros procesos o dependencias, el análisis de riesgos determina los controles y los responsables de ejecutarlos en cada caso.

**Nota:** El nivel de impacto debe ser determinado con la presencia de cualquiera de los criterios establecidos, tomando el criterio con mayor nivel de afectación, ya sea cualitativo o cuantitativo.

Las variables CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD se definen de acuerdo al MSPI, de la estrategia de Gobierno Digital del Ministerio de Tecnologías de la Información.



**Fuente:** *Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5*

## **Controles para riesgos de seguridad de la información**

La entidad debe mitigar/tratar los riesgos de seguridad de la información empleando como mínimo los controles de la ISO/IEC 27001:2013, estos controles se encuentran en el Anexo 4. *“Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas”*, siempre y cuando se ajusten al análisis de riesgos.

Así mismo se presentan algunos ejemplos de controles y los dominios a los que pertenecen:

| **Procedimientos operacionales y**  **responsabilidades** | **Objetivo: asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información** |
| --- | --- |
| Procedimientos de operación  documentados | Control: los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten. |
| 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. |
| Gestión de capacidad | Control: para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, llevar a cabo los ajustes y las proyecciones de los requisitos sobre la capacidad futura. |
| 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. |
| Protección contra códigos maliciosos | Objetivo: asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos. |
| Controles contra códigos maliciosos | Control: se deberían implementar controles de detección, prevención y recuperación, combinados con la toma de conciencia apropiada por parte de los usuarios para protegerse contra códigos maliciosos. |
| Copias de respaldo | Objetivo: proteger la información contra la perdida de datos. |
| Respaldo de información | Control: se deberían hacer copias de respaldo de la información, del *software* y de las imágenes de los sistemas, ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada. |

**Fuente:** *Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5*

# MAPA DE RIESGOS

El mapa de riesgos estará disponible por parte de la Oficina Asesora de Planeación para la consulta de todos los servidores en el aplicativo SIGPARTICIPO. Los líderes de procesos y sus equipos de trabajo deben garantizar que la información de los riesgos sea adecuada, coherente, pertinente y vigente. Cualquier ajuste que se deba realizar de esta información, debe ser tramitada con la Oficina Asesora de Planeación.

Será la Oficina Asesora de Planeación la responsable de la publicación del mapa de riesgos de corrupción en el portal web de la Entidad; esta publicación se realizará cada vez que se ajuste la información registrada por los procesos y debe estar disponible en datos abiertos (Archivo de Excel) para facilitar la consulta por las partes interesadas.

# SOLICITUD DE CREACIÓN, AJUSTES O ELIMINACIÓN

Cuando el proceso requiera crear un nuevo riesgo, hacer ajustes en la información documentada, o eliminar un riesgo existente, se deberá registrar la solicitud correspondiente en el aplicativo SIGPARTICIPO:

| ***TIPO DE SOLICITUD*** | ***DESCRIPCIÓN*** | ***TIEMPOS DE GESTIÓN*** |
| --- | --- | --- |
| ***Crear riesgos*** | Registrar la solicitud con la justificación correspondiente en el flujo de solicitudes del SIG. | Los tiempos de gestión para dar respuesta a esta solicitud, se encuentran estandarizados en el flujo de solicitudes.  **Nota:** se debe tener en cuenta que para crear riesgos es importante generar mesas de trabajo con el fin de registrar la información de cada etapa. Estas reuniones y el cierre de la solicitud dependerán de la programación que se realice en las mesas de trabajo. |
| ***Ajustar la información del riesgo*** | Registrar en SIGPARTICIPO la solicitud de la devolución de la etapa indicando los ajustes a realizar con la justificación correspondiente. | De acuerdo con la justificación, la Oficina Asesora de Planeación tendrá cinco días hábiles para verificar cada caso y aprobar la devolución a la etapa del riesgo, según la solicitud.  Una vez aprobada la devolución de la etapa, el responsable tendrá diez días hábiles para registrar los ajustes en la información de las etapas del riesgo. |
| ***Eliminar riesgos*** | Mediante la opción disponible en el módulo de riesgos, registrar la solicitud con la justificación correspondiente | Una vez registrada la solicitud debidamente justificada; la Oficina Asesora de Planeación tendrá cinco días hábiles para inactivar el riesgo en el aplicativo o pronunciarse al respecto. |

# ANEXOS

* Instructivo para el manejo del Módulo de Riesgos – SIGPARTICIPO
* https://www.participacionbogota.gov.co/transparencia/gestion-del-riesgo-institucional