**Plan Tratamiento de Riesgos de Seguridad y Privacidad de la Información**

UNIDAD ADMINISTRATIVA ESPECIAL DE SERVICIOS PUBLICOS

Bogotá D.C. Enero de 2020

Tabla de contenido

[1. OBJETIVO DEL DOCUMENTO 3](#_Toc30690918)

[2. METODOLOGÍA DE GESTIÓN DE RIESGO 3](#_Toc30690919)

[2.1 Identificación y Valoración de los Activos de Información 3](#_Toc30690920)

[2.1.1 Identificación de Activos de Información 3](#_Toc30690921)

[2.1.2 Identificación de Propietario, custodio, responsable y ubicación 4](#_Toc30690922)

[2.1.3 Categorización de la Información 5](#_Toc30690923)

[2.1.4 Valoración de los Activos de Información 5](#_Toc30690924)

[2.2 ANÁLISIS Y EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 7](#_Toc30690925)

[2.2.1. Identificación de las amenazas 7](#_Toc30690926)

[2.2.2. Identificación de la Vulnerabilidades 8](#_Toc30690927)

[2.2.3. Identificación de Riesgos 8](#_Toc30690928)

[2.2.4. Análisis de la Probabilidad 9](#_Toc30690929)

[2.2.5. Determinar el Impacto de los Activos de Información 10](#_Toc30690930)

[2.2.6. Riesgos antes y después de los Controles (Inherente) 10](#_Toc30690931)

[2.2.7. Identificación de Controles Existentes 11](#_Toc30690932)

[3.TRATAMIENTO DE RIESGO 12](#_Toc30690933)

[3.1. Opciones de Tratamiento de Riesgo 12](#_Toc30690934)

[3.2. Apetito del Riesgo 12](#_Toc30690935)

[3.3. Planes de Tratamiento 13](#_Toc30690936)

[3.4. Monitoreo 13](#_Toc30690937)

[3.41. Riesgo Residual 13](#_Toc30690938)

[4. REVISIONES PERIÓDICAS DE LA EVALUACIÓN Y EL TRATAMIENTO DE RIESGOS 14](#_Toc30690939)

# OBJETIVO DEL DOCUMENTO

Definir los lineamientos mediante los cuales se realizará la gestión de riesgos de seguridad de la información en la Unidad Administrativa Especial de Servicios Públicos (UAESP), la cual debe incluir amenazas, vulnerabilidades, riesgos, controles, niveles aceptables de riesgo y el tratamiento de riesgos.

# METODOLOGÍA DE GESTIÓN DE RIESGO

La metodología para la administración y gestión de riesgos está basada en las directrices definidas por el Departamento Administrativo de la Función Pública - DAFP el cual plantea las directivas de gestión, definición, aplicación, desarrollo e implantación de los sistemas de calidad y gestión a partir del enfoque de riesgos.

De esta manera, la etapa inicial propuesta por el DAFP, arranca con un análisis relacionado con el estado actual de los riesgos y su gestión dentro de la Entidad, haciendo especial énfasis en el conocimiento de ésta, desde un punto de vista estratégico, pero teniendo en mente todo el modelo de riesgos que busque la disminución de los impactos en el caso de materialización de alguno de ellos y propendiendo por la continuidad del negocio.

La gestión de riesgos ofrece para la UAESP un método sistemático para analizar los riesgos derivados de los procesos que la componen con un especial énfasis en las tecnologías de la información y comunicaciones usadas dentro de la Entidad, con el objetivo de descubrir, valorar, planificar y adelantar el tratamiento oportuno que busque mantener los riesgos en niveles óptimos de control y así preparar a la entidad para una posible materialización de alguno de los riesgo y dentro de la misma línea, poder adelantar procesos de evaluación, auditoría, certificación o acreditación, según corresponda.

# Identificación y Valoración de los Activos de Información

# Identificación de Activos de Información

De acuerdo con la norma ISO/IEC 27000, “activo de información” se define como cualquier elemento que tenga valor para la organización y, en consecuencia, deba ser protegido. Por consiguiente, la primera actividad en la Gestión de Riesgos es identificar los activos de

información bajo las consideraciones que la Entidad defina, actividad que debe realizarse sin perder de vista el alcance definido y aprobado por la alta dirección para el Sistema de Gestión de Seguridad de la Información (SGSI) o en el caso de la UAESP el Modelo de Seguridad y Privacidad de Información - MSPI.

En este sentido, las actividades necesarias para la identificación de los activos de información y su formalización dentro de la entidad son:

1. Definir el instrumento de captura de información identificando las variables que se deben capturar.
2. Identificar los procesos y agendar las entrevistas con sus responsables.
3. Recolectar la información necesaria bajo las consideraciones definidas por la Entidad.
4. Realizar los cruces necesarios con otras fuentes de información como inventarios, Tablas de Retención Documental, entre otros, para completar información.
5. Consolidar la información.

Para adelantar esta primera etapa se debe tener en cuenta la definición de la siguiente información, con el fin de poder tener parámetros precisos frente a la captura y consolidación de la herramienta de trabajo.

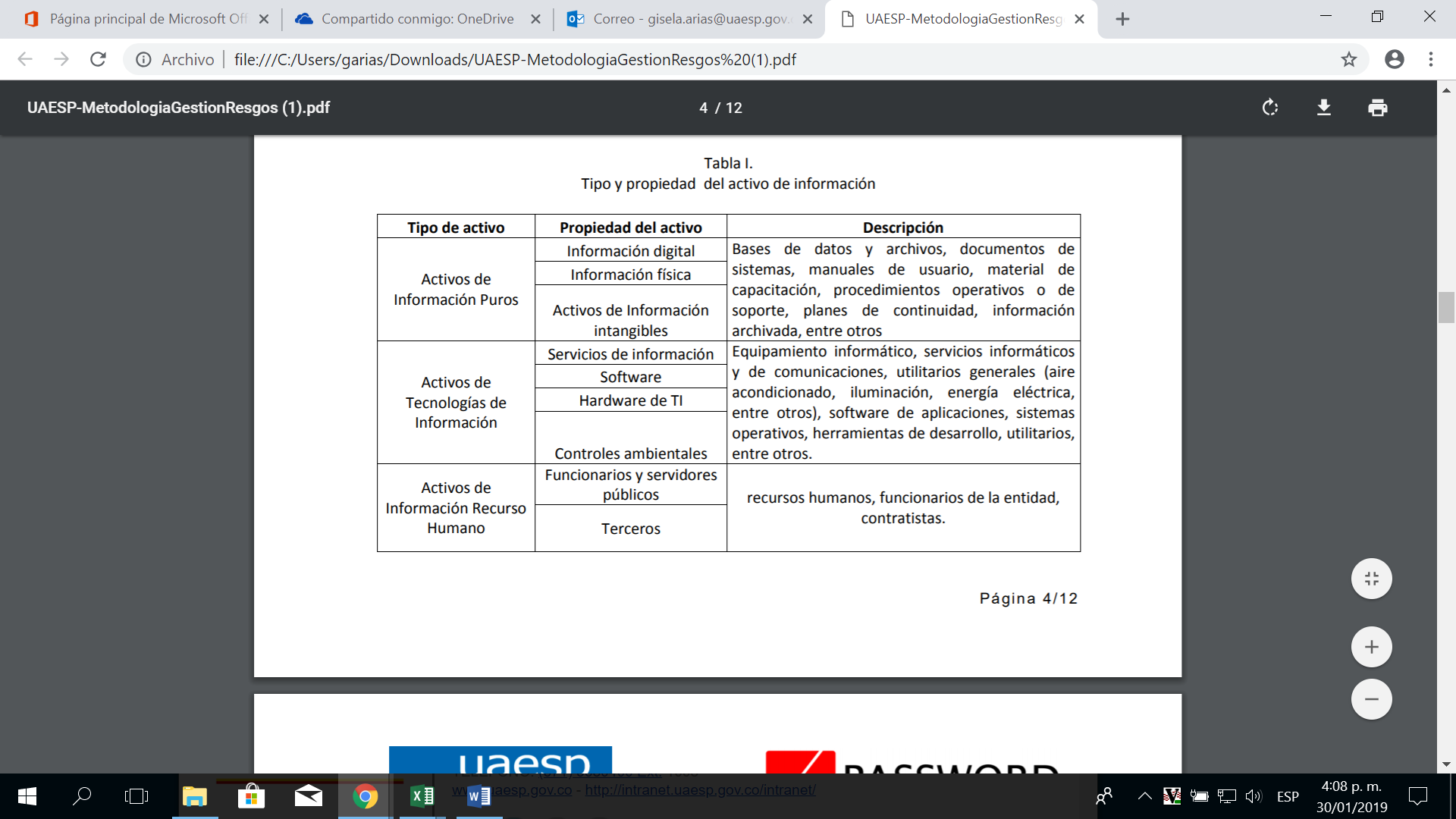
# Identificación de Propietario, custodio, responsable y ubicación

Los activos de información previamente identificados en el paso anterior deben tener su respectivo propietario, definido como la dependencia o proceso donde se crea o custodia dicho activo. Así mismo, definir el custodio de la información el cual, puede ser el mismo propietario o en su defecto el proceso o la persona que la Entidad haya definido para adelantar dicha tarea.

El responsable es el jefe y/o subdirector de cada dependencia o proceso de uno o un grupo de activos de información y es quien debe velar porque los controles de seguridad sean implementados de manera satisfactoria.

En esta medida la tipología de activos de información está definida en la siguiente tabla:

**Tabla I. Tipología del Activo**



# Categorización de la Información

Se cuenta con una categorización para el etiquetado de la información, la cual se ha establecido al interior de la entidad con los siguientes criterios:

**Información pública:** Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de Entidad y debe estar a disposición de cualquier persona natural o jurídica del estado colombiano.

**Información pública clasificada:** "Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semi-privado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la ley 1712 del 2014."

**Información pública reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada, de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 18 de la ley 1712 del 2014.

**Datos Personales**: Cualquier información vinculada o que pueda asociarse con los datos públicos y no públicos de una o varias personas naturales o jurídicas, de acuerdo con la ley estatutaria 1581 de 2012.

# Valoración de los Activos de Información

Los activos de información deben ser valorados de acuerdo a su impacto en términos de la pérdida de las tres (3) propiedades básicas de la seguridad de la información que son la confidencialidad, integridad y disponibilidad, definidos a partir de la norma ISO/IEC 27000:2013.

**Confidencialidad:** Es la propiedad de que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

**Integridad:** Es la propiedad de salvaguardar la exactitud y estado completo de los activos de información.

**Disponibilidad:** Es la propiedad de que la información sea accesible y utilizable por solicitud de un individuo o entidad autorizada cuando se requiera.

Dada las anteriores definiciones, se establecen las escalas para la confidencialidad, integridad y disponibilidad respectivamente.

**Tabla II. Valoración de la Confidencialidad**

|  |  |  |
| --- | --- | --- |
| **Escala Cuantitativa** | **Escala Cualitativa** | **Descripción** |
| 1 | Muy Bajo | Se puede acceder por cualquier usuario dentro y fuera de la entidad |
| 2 | Bajo | Se puede acceder solo por personal de la entidad |
| 3 | Medio | Se puede acceder por subdirecciones especificas y proveedores y/o contratistas directamente definidos |
| 4 | Alto | Solo es posible acceder por el personal que preparo la información, subdirectores, jefes de oficina y/o Dirección General |
| 5 | Muy Alto | Acceso exclusivo para el director(a) y Subdirectores |

**Tabla III. Valoración de la Integridad**

|  |  |
| --- | --- |
| Alta | Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad |
| Media | Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad |
| Baja | Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos |
| No clasificada | Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad ALTA |

**Tabla IV. Valoración de la Disponibilidad**

|  |  |
| --- | --- |
| Alta | La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos |
| Media | La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad |
| Baja | La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen |
| No clasificada | Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA |

# 2.2 ANÁLISIS Y EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

# 2.2.1. Identificación de las amenazas

Las amenazas son de origen natural o humano y pueden ser accidentales o deliberadas, algunas amenazas pueden afectar a más de un activo generando diferentes impactos. A continuación, se definen algunas de las amenazas detectadas dentro de la entidad o que son genéricas para este tipo de proceso. A continuación se presentan algunas amenazas en relación con la Norma ISO 27005.

**Desastres Naturales:** Este grupo de amenazas comprende los eventos que tienen su origen en las fuerzas de la naturaleza, estos desastres afectan a la información e integridad del sistema.

**Ataques Maliciosos:** Estas amenazas están enfocadas a los ataques maliciosos de destrucción como el uso de explosivos y armas químicas o de acceso como el acceso a servicios.

**Fallas eléctricas:** Este tipo de amenazas está enfocada a las fallas de energía como por ejemplo subidas de voltaje, carga electrostática, entre otros.

**Daños Accidentales:** Esta clase representa las amenazas que se generan por la acción ajena a la voluntad del usuario, ya que se presentan de forma no intencionada, pero sin las previsiones requeridas.

**Fallas de Comunicaciones:** Esta clase reúne las amenazas dirigidas a los sistemas de comunicaciones.

**Software:** Las amenazas de software incluyen posibles fallas dentro del diseño, desarrollo e implementación del software.

**Comunicaciones:** Las principales amenazas que se presentan en esta categoría son la no disponibilidad de red, y la infiltración a las comunicaciones.

**Hardware:** Dentro de esta clase se encuentran las amenazas de componentes de hardware dadas por defecto de fabricación o mal diseño de hardware, y por uso inadecuado y descuido en el mantenimiento del hardware.

**Datos:** Las principales amenazas que se presentan en esta categoría son la extracción de información y la alteración de esta.

Cabe resaltar que la anterior lista no es una verificación exhaustiva y por ende en cada una de las revisiones que se adelanten frente a la gestión de los riesgos, se entrará a revisar y evaluar nuevas amenazas que puedan afectar a la Entidad.

# 2.2.2. Identificación de la Vulnerabilidades

Las vulnerabilidades de los activos de información son debilidades que son aprovechadas por amenazas y generan un riesgo. Una vulnerabilidad que no tiene una amenaza asociada puede no requerir de la implementación de un control; sin embargo, es necesario identificarla y monitorearla.

Es importante tener en cuenta que un control mal diseñado e implementado puede constituir una vulnerabilidad.

La identificación de las vulnerabilidades se basa en los resultados de las pruebas de hacking ético, entrevistas con los responsables de los activos de información y serán registradas en la matriz de riesgos.

# 2.2.3. Identificación de Riesgos

Los riesgos en seguridad de la información se identifican mediante las pruebas de seguridad, identificación por parte de los funcionarios quienes tienen claridad y han experimentado la materialización de algunos riesgos en sus procesos y finalmente por la experiencia del personal que gestiona los riesgos o el sistema.

Los riesgos se relacionan con las vulnerabilidades y amenazas de cada activo de información los cuales se encuentran listados en la matriz de riesgos, bajo la tipología definida a continuación:

**Tabla V. Tipos de riesgos**

|  |
| --- |
| **Tipo de riesgo** |
| Lógico |
| Físico |
| Locativo |
| Legal |

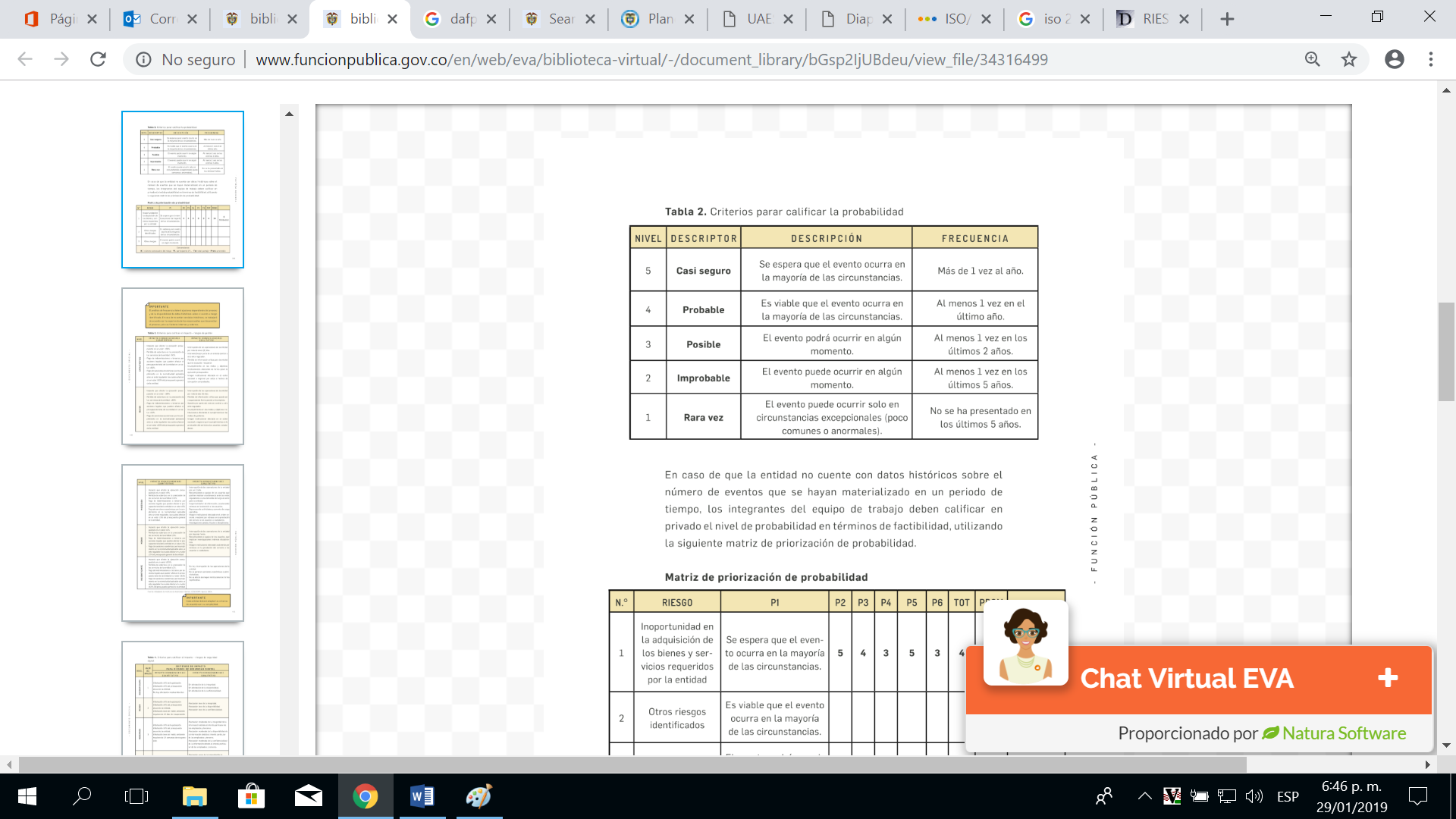
# 2.2.4. Análisis de la Probabilidad

Se realiza el análisis de la posibilidad de ocurrencia de un riesgo y se expresa en términos de frecuencia o factibilidad, donde frecuencia implica analizar el número de eventos ocurridos en un período determinado, tratando los hechos que se han materializado o que se cuente con un historial de situaciones o eventos asociados al riesgo (información historica); factibilidad por su lado, implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, tratándose en este caso, de un hecho que no se han presentado pero es posible que suceda.

Para poder adelantar la valoración de la probabilidad en los casos que no haya información dentro de la entidad, se puede entrar a definir a partir de datos de referencias externas (otras entidades o mercado) o finalmente por el criterio de una persona experta en riesgos o en seguridad de información. Cabe resaltar que dicha probabilidad debe ser determinada por el responsable del proceso de acuerdo a su experiencia y asociado a la vulnerabilidad detectada sobre un activo de información específico y de acuerdo a la amenaza definida.

Los criterios para calificar la probabilidad se describen a continuación:

**Tabla VI. Criterios para calificar la probabilidad**



**Fuente: DAFP**

En caso de que la entidad no cuente con datos históricos sobre el número de eventos que se hayan materializado en período de tiempo los integrantes de equipo de trabajo deben calificar en privado el nivel de probabilidad en términos de factibilidad, utilizando la siguiente matriz de priorización de probabilidad.

**Tabla VII. Matriz de priorización de probabilidad**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| N°. | RIESGO | DESCRIPCIÓN | P1 | P2 | P3 | P4 | P5 | P6 | TOT | PROM |
| 1 | Inoportunidad en la adquisición de los bienes y servicios requeridos por la entidad | Se espera que el evento ocurra en la mayoría de las circunstancias. | 5 | 4 | 3 | 5 | 3 | 4 | 24 | 4 probable |
| 2 | Otros riesgos identificados | Es viable que el evento ocurra en la mayoría de las circunstancias |  |  |  |  |  |  |  |  |
| 3 | Otros riesgos | El evento podrá ocurrir en algún momento |  |  |  |  |  |  |  |  |

**Fuente: DAFP**

No. Numero consecutivo del riesgo, P1…P6: Participante 1…Participante 6, Tot: total puntaje, PROM: Promedio

El análisis de frecuencia deberá ajustarse dependiendo del proceso y de la disponibilidad de datos históricos sobre el evento o riesgo identificado. En caso de no contar con datos históricos, se trabajará de acuerdo con la experiencia de los responsables que desarrollan el proceso y de sus factores internos y externos.

# 2.2.5. Determinar el Impacto de los Activos de Información

El impacto está determinado por el valor máximo de la calificación registrada en términos de la seguridad de la información (Confidencialidad, Integridad y Disponibilidad) de los activos de información.

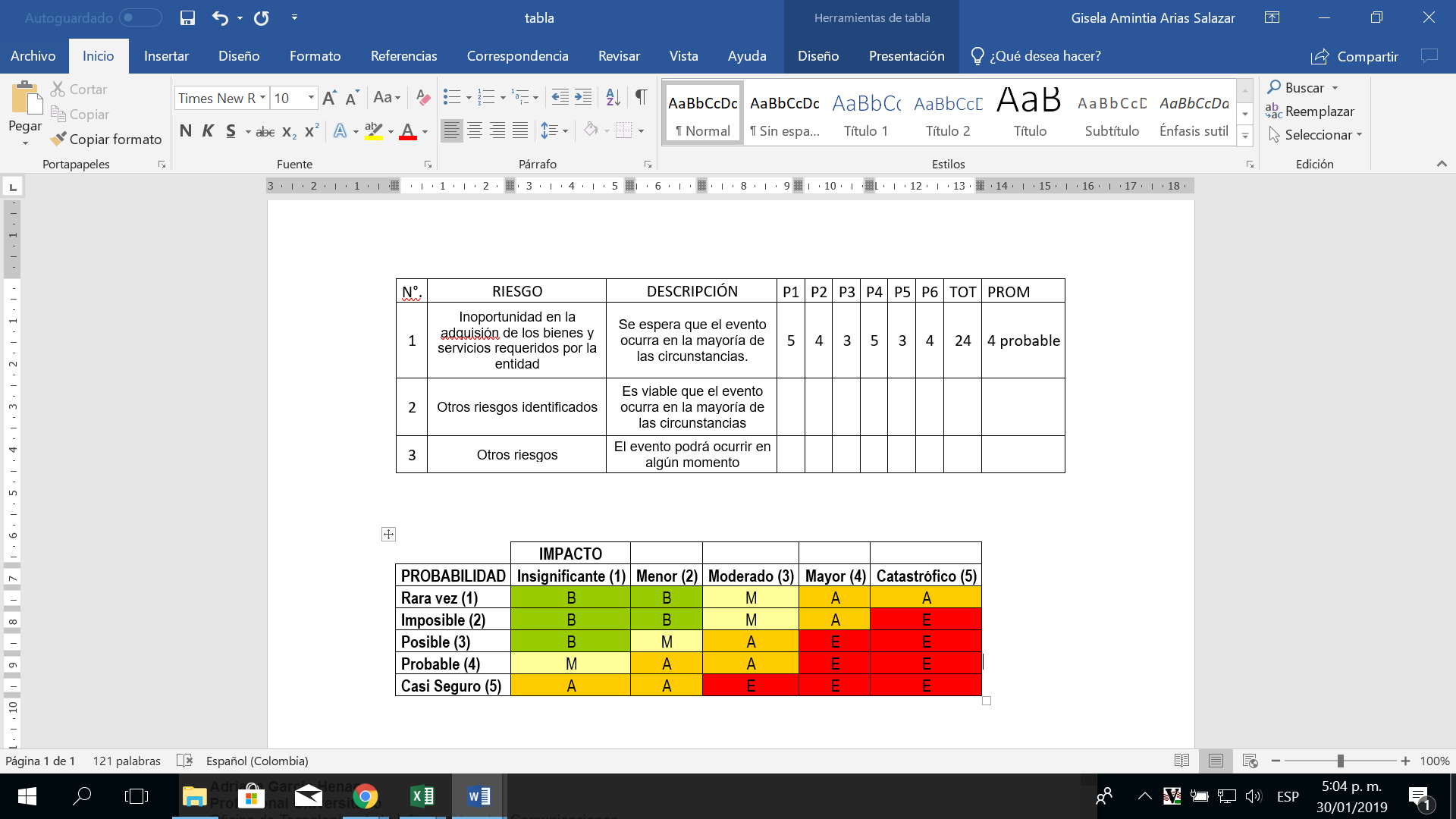
# 2.2.6. Riesgos antes y después de los Controles (Inherente)

Al momento de definir las actividades de control por parte de la primera línea de defensa, es importante considerar que los controles estén bien diseñados, es decir, que efectivamente estos mitiguen las causas que hacen que el riesgo se materialice.

Dado que se va a adoptar la matriz de riesgo se deberán adaptar los criterios a la realidad.

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

**Tabla VII Medición Riesgos Inherentes**

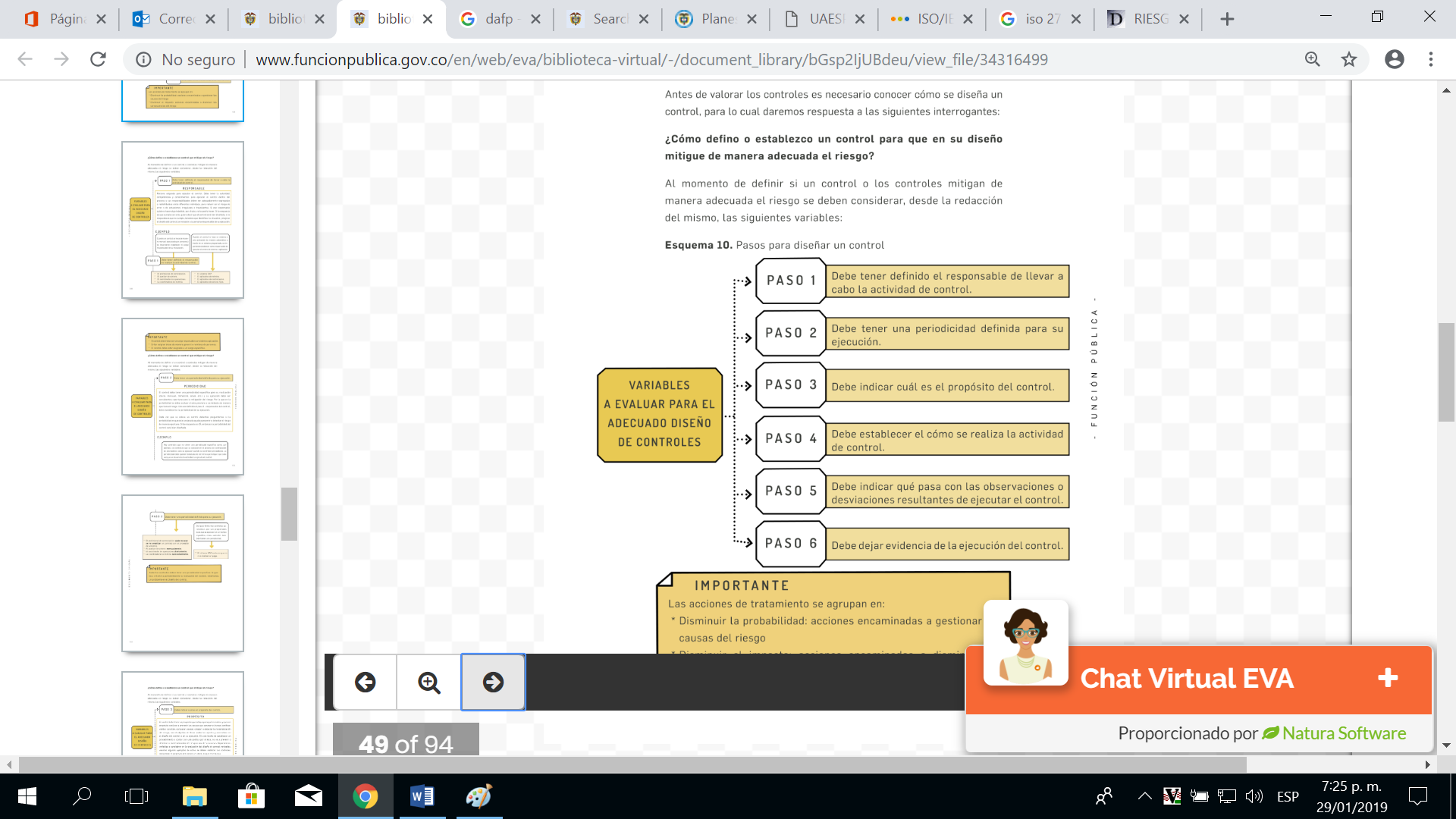


La probabilidad y el impacto se determinan con base a la amenaza, no en las vulnerabilidades.

# 2.2.7. Identificación de Controles Existentes

Se realiza identificación de controles documentados, implementados y monitoreados por la entidad para la gestión del riesgo, posteriormente es necesario verificar el valor del riesgo residual y determinar si es posible aplicar un plan de tratamiento.

**Tabla VIII. Pasos para evaluar el diseño de los controles**



**Fuente: DAFP**

# 3.TRATAMIENTO DE RIESGO

# 3.1. Opciones de Tratamiento de Riesgo

Es la respuesta establecida por la primera línea 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 dueños de los procesos tendrán en cuenta la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la entidad, la probabilidad impacto de este y la relación costo-beneficio de las medidas de tratamiento. Pero en caso de que una respuesta ante el riesgo derive en un riesgo residual que supere los niveles aceptables para la dirección, se deberá volver analizar y revisar dicho riesgo.

El tratamiento o respuesta dada al riesgo se marca en las siguientes categorías:

**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.

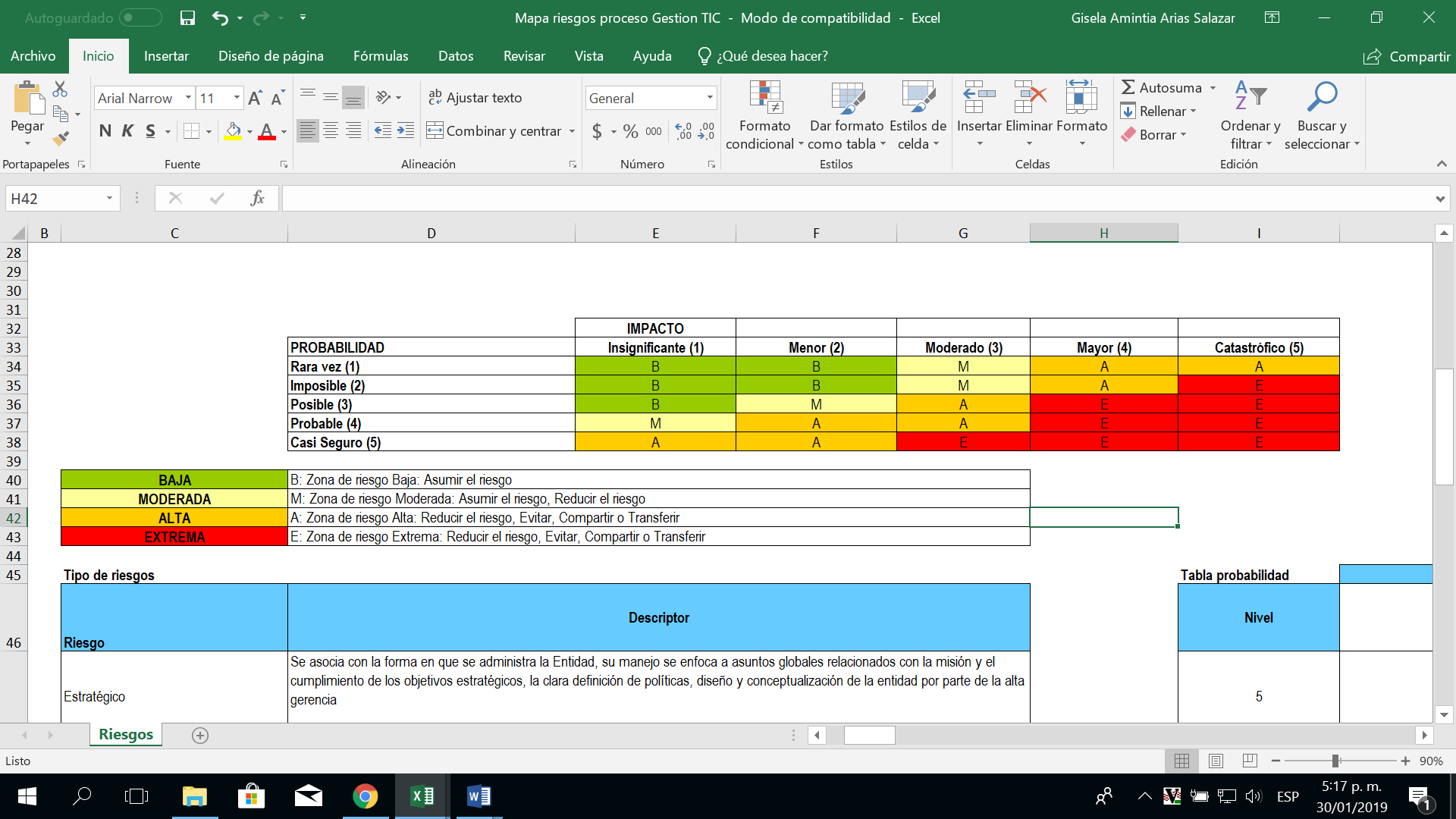
**Compartir el riesgo:** se reduce la probabilidad o el impacto del riesgo transferido o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir, pero no se pueden transferir su responsabilidad.

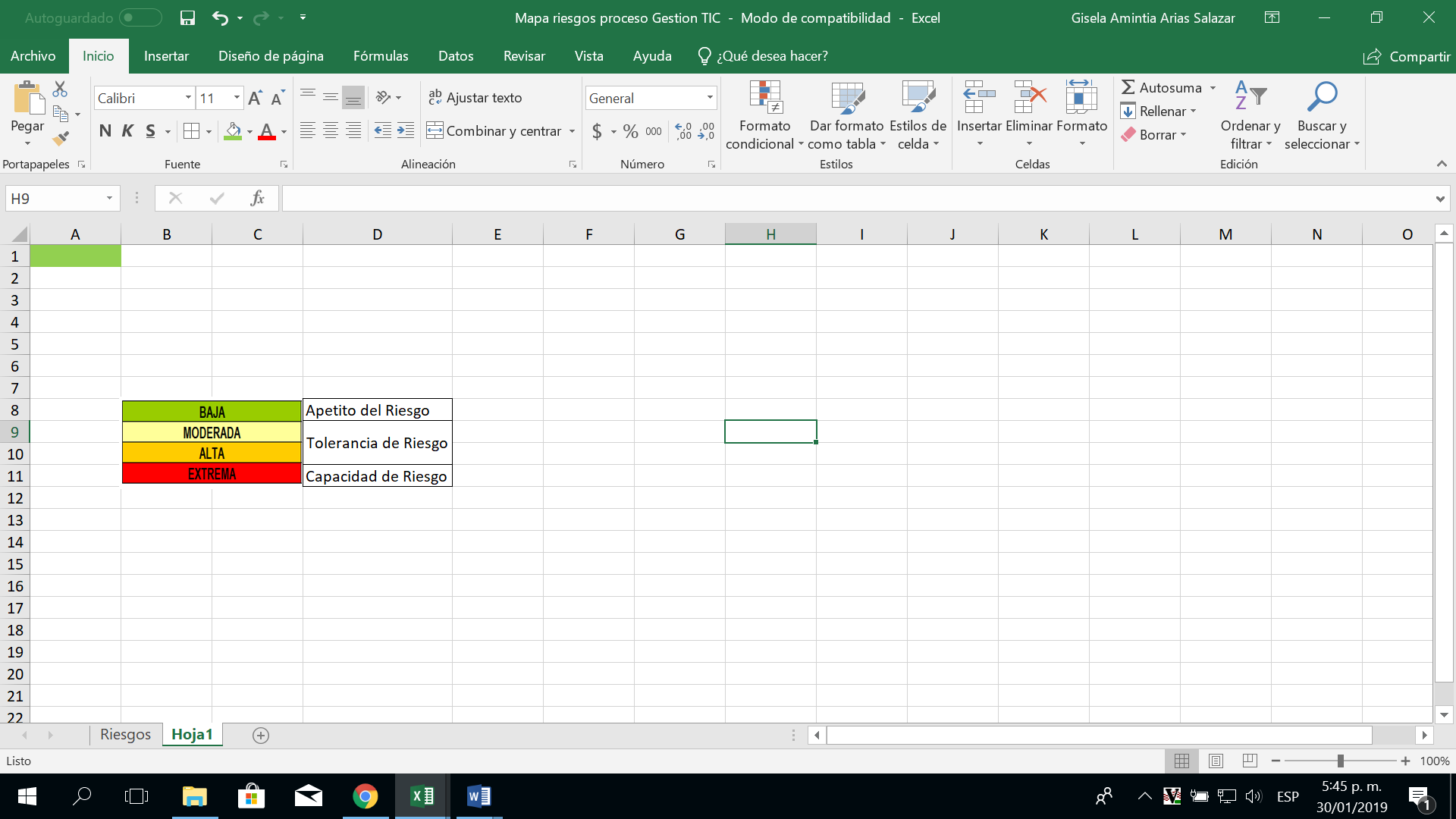
# 3.2. Apetito del Riesgo

Es la cantidad de exposición al riesgo o impacto adverso potencial de un evento que la organización está dispuesta a aceptar/retener para el logro de sus objetivos de largo plazo.

Se basa en la interacción entre los diferentes riesgos asociados a sus objetivos estratégicos y sus capacidades internas y externas para manejar dichos riesgos.

**Tabla IX Clasificación del Riesgo**



****

**Fuente:** [**Mapa riesgos proceso Gestión TIC.xls**](file:///\\apolo\UAESP_Docs\garias\Mis%20documentos\2019\Gobierno%20Digital\Mapa%20riesgos%20proceso%20Gestion%20TIC.xls)

Teniendo en cuenta lo mencionado anteriormente se tiene la siguiente matriz como referencia: [Mapa riesgos proceso Gestión TIC.xls](file:///\\apolo\UAESP_Docs\garias\Mis%20documentos\2019\Gobierno%20Digital\Mapa%20riesgos%20proceso%20Gestion%20TIC.xls)

# 3.3. Planes de Tratamiento

Los planes de tratamiento de riesgos de seguridad de la información toman como punto de partida la descripción del riesgo asociado a la vulnerabilidad identificada, para así, seleccionar la opción de tratamiento y la descripción del control a ejecutar, estableciendo los recursos (Personal y económico) necesarios para la implementación.

Es necesario identificar de manera única que los controles correspondan con los descritos en el anexo A de la norma ISO/IEC 27001:2013, y finalmente establecer las fechas de inicio y fecha límite de la implementación.

# 3.4. Monitoreo

Se considera la última fase de la gestión de riesgos de seguridad de la información, por ser aquí donde se verifica la eficacia de los controles implementados, se debe calificar nuevamente los riesgos identificados en la matriz y obtener el riesgo residual. En general, el monitoreo de los controles debe ser continuo y periódico de acuerdo a la forma de medición establecida por la UAESP.

# 3.41. Riesgo Residual

Es aquel riesgo que subsiste, después de haber implementado controles. Es importante advertir que el nivel de riesgo al que está sometida la entidad nunca puede erradicarse. Por ello, se debe buscar un equilibrio entre el nivel de recursos y mecanismos que es

preciso dedicar para minimizar o mitigar estos riesgos y un cierto nivel de confianza que se puede considerar suficiente (nivel de riesgo aceptable). El riesgo residual puede verse como aquello que separa a la entidad de la seguridad absoluta.

El riesgo residual es aquél que permanece después de que la dirección desarrolle sus respuestas a los riesgos. El riesgo residual refleja el riesgo remanente una vez se han implantado de manera eficaz las acciones planificadas por la dirección para mitigar el riesgo inherente.

# 4. REVISIONES PERIÓDICAS DE LA EVALUACIÓN Y EL TRATAMIENTO DE RIESGOS

La valoración de los riesgos (Matriz de Riesgos) será revisada al menos una vez al año y/o teniendo en cuenta los cambios en:

* La entidad
* La tecnología
* Los procesos de la Entidad
* Aplicación de controles.

Todo control aplicado con el fin de reducir el valor de riesgo calculado debe ser medible a través de su eficacia. La aplicación de un control no necesariamente implica la reducción total del valor de riesgo esperado sino la reducción a los niveles de riesgo aceptables establecidos por la entidad.

La funcionalidad de los controles debe ser constantemente evaluada; en caso de no obtener los resultados esperados se debe aplicar mejoras de acuerdo a la aplicación de la metodología PHVA (Planear, Hacer, Verificar, Actuar).