Contenido

Índice de tablas

Índice de ilustraciones

1. INTRODUCCIÓN

Con el constante aumento de amenazas que afectan la Seguridad de la Información que podrían generar riesgos como incidentes de Seguridad de la Información en la Secretaría Distrital de la Mujer causando pérdidas económicas, de reputación o imagen, ocasionando así reprocesos para la Entidad, se hace necesario formular, documentar, implementar y monitorear controles, orientados a la adecuada gestión de riesgos de Seguridad de la Información, los cuales permitirán minimizar la probabilidad de que se materialicen riesgo y el impacto en caso de que ocurran, manteniendo los riesgos de Seguridad de la Información en un nivel aceptable para la Entidad.

Por lo anterior, el presente documento hace parte de la estrategia y actividades de implementación del Modelo de Seguridad y Privacidad de la Información – MSPI de MinTIC en la Entidad, de esta forma se prevé la identificación, valoración y tratamiento de los riesgos de Seguridad de la Información, en concordancia con las directrices para la administración de riesgos definida por el Departamento Administrativo de la Función Pública (DAFP), en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5 (Diciembre de 2020).

2. OBJETIVO

Establecer la metodología para orientar a los responsables de los activos de información en la oportuna gestión, identificación, valoración y tratamiento de los riesgos de Seguridad de la Información de la Secretaría Distrital de la Mujer, cuya finalidad es la adecuada protección de los activos de información favoreciendo la toma de decisiones respecto al adecuado tratamiento de los riesgos de Seguridad de la Información.

3. OBJETIVOS ESPECÍFICOS

- Proteger la confidencialidad, integridad y disponibilidad de la información institucional como activo de información de la Secretaría Distrital de la Mujer.
- Identificar, analizar y valorar los riesgos de Seguridad de la Información de los activos de información de las dependencias de la Secretaría Distrital de la Mujer.
- Identificar las amenazas e impacto de Seguridad de la Información a las cuales están expuestos los activos de información de la Secretaría Distrital de la Mujer.
- Identificar e implementar los controles necesarios para el tratamiento de los riesgos de Seguridad de la Información.

4. ALCANCE

El Manual de Gestión de Riesgos de Seguridad de la información define las etapas de identificación, valoración y tratamiento de los riesgos de Seguridad de la Información, aplica a todas las dependencias y procesos de la Entidad, quienes deben aplicar y realizar las actividades correspondientes a la gestión y tratamiento de riesgos de Seguridad de la Información.

5. NORMATIVIDAD

Se tomarán como marco de referencia y línea base para la identificación, clasificación y valoración del inventario de activos de información las siguientes normas y/o Leyes:

- **Ley 1266 de 2008:** por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

- **Ley 1581 de 2012:** por la cual se dictan disposiciones generales para la protección de datos personales.

- **Decreto 1377 de 2013**: por el cual se reglamenta parcialmente la Ley 1581 de 2012. Que mediante la Ley 1581 de 2012 se expidió el Régimen General de Protección de Datos Personales, el cual, de conformidad con su artículo 1, tiene por objeto "(.. .) desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

- **Ley 1712 de 2014:** por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

- **Decreto 103 de 2015**: por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones. Que para facilitar la implementación y cumplimiento de la Ley 1712 de 2014 se hace necesaria su reglamentación en los temas relacionados con la gestión de la información pública en cuanto a: su adecuada publicación y divulgación, la recepción y respuesta a solicitudes de acceso a ésta, su adecuada clasificación y reserva, la elaboración de los instrumentos de gestión de información, así como el seguimiento de la misma.

- **Decreto 1081 de 2015:** por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República, compiló el decreto 2641 de 2012, reglamentario de los artículos 73 y 76 de la ley 1474 de 2011, mediante el cual se estableció como metodología para diseñar y hacer seguimiento a la estrategia de lucha contra la corrupción y de atención al ciudadano, la establecida en el Plan Anticorrupción y de Atención al Ciudadano contenida

en el documento "Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano".

- **Decreto 1083 de 2015:** por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública, entre otros aspectos establece que, se deben tomar medidas para administrar los riesgos en la entidad pública (Artículo 2.2.21.5.4).

- **Decreto 1078 de 2015:** por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

- **Decreto 648 de 2017:** por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública, y en su Artículo 2.2.21.1.6 literal g., establece dentro de las funciones del Comité Institucional de Coordinación de Control Interno que se debe someter a aprobación del representante legal la política de administración del riesgo y hacer seguimiento, en especial a la prevención y detección de fraude y mala conducta.

- **Decreto 1008 de 2018:** por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

- **Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5-Departamento Administrativo de la Función Pública DAFP:** establece los lineamientos que deben ser utilizados por los responsables de la gestión y tratamiento de riesgos en las entidades públicas.

- **Norma NTC ISO/IEC 27001:2013:** es el referente internacional a la hora de implementar el Sistema de Gestión de Seguridad de la Información, emite lineamientos y directrices para que las organizaciones aseguren la confidencialidad, integridad y disponibilidad de la información.

6. DEFINICIONES

A continuación, se relacionan una serie de conceptos y definiciones que son necesarios para poder comprender la terminología empleada en el documento.

- **Activo de información:** un activo de información es, cualquier elemento que contenga, genere, adquiera, gestione y/o procese información, que tiene valor para uno o más procesos de la organización en razón a qué aporta al cumplimiento de su objetivo y por lo cual debe protegerse[1]. En el contexto de seguridad digital son elementos tales como aplicaciones de la

[1] Adaptado de ISO IEC 27000.

organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital[2].

- **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[3].

- **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[4].

- **Causa**: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo[5].

- **Causa Inmediata**: circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo[6].

- **Causa Raíz**: causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo[7].

- **Confidencialidad:** es la propiedad que determina que la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados[8].

- **Consecuencia**: 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[9].

- **Control**: medida que permite reducir o mitigar un riesgo[10].

---

[2] Tomado de Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5.

[3] Ibidem.

[4] Ibidem.

[5] Ibidem.

[6] Ibidem.

[7] Ibidem.

[8] Adaptado de ISO IEC 27000.

[9] Tomado de Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5.

[10] Tomado de Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5.

- **Disponibilidad:** es la propiedad de acceso y utilización de la información por parte de los individuos, entidades o procesos autorizados cuando lo requieran[11].

- **Factores de Riesgo**: Son las fuentes generadoras de riesgos[12].

- **Integridad:** es la propiedad que garantiza la exactitud y completitud de la información[13].

- **Impacto**: las consecuencias que puede ocasionar a la organización la materialización del riesgo[14].

- **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[15].

- **Probabilidad:** se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año[16].

- **Propietario de la Información:** cargo, proceso, o dependencia que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso[17].

- **Riesgo**: efecto que se causa sobre los objetivos de las entidades, debido a 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[18].

---

[11] Adaptado de ISO IEC 27000.

[12] Tomado de Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5.

[13] Adaptado de ISO IEC 27000.

[14] Tomado de Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5.

[15] Ibidem.

[16] Ibidem.

[17] Adaptado de la Guía de Gestión de Activos - MINTIC.

[18] Tomado de Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5.

- **Riesgo Inherente**: nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto, nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad[19].

- **Riesgo Residual**: el resultado de aplicar la efectividad de los controles al riesgo inherente[20].

- **Riesgo de Seguridad de la Información**: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000) [21].

- **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[22].

- **Vulnerabilidad**: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas[23].

[19] Tomado de Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5.

[20] Ibidem.

[21] Ibidem.

[22] Ibidem.

[23] Ibidem.

7. ROLES Y RESPONSABILIDADES:

Los siguientes roles serán responsables y tendrán participación directa en la implementación y ejecución de la metodología para la identificación, valoración y tratamiento de los riesgos de Seguridad de la Información de la Secretaría Distrital de la Mujer.

Rol	Responsable	Responsabilidades
ALTA DIRECCIÓN	Comité Institucional de Gestión y Desempeño.	Socializar ante la alta dirección, lideresas y líderes de políticas del Modelo Integrado de Planeación y Gestión los lineamientos frente a la gestión y tratamiento de riesgos de Seguridad de la Información.
DEPENDENCIAS Y PROCESOS	Lideresas y líderes de Proceso. Responsables de la Información.	Realizar la gestión de riesgos de Seguridad de la Información acorde a las directrices establecidas por la OAP en la presente metodología. Identificar y tratar sus riesgos de Seguridad de la Información. Designar personal de planta o contratistas, para la gestión, identificación y tratamiento de riesgos de Seguridad de la Información, teniendo en cuenta que deben ser los idóneos para el tema. Aprobar sus riesgos y realizar el tratamiento de los riesgos de Seguridad de la Información de su competencia.
OFICINA ASESORA DE PLANEACIÓN	Jefa (e) Oficina Asesora de Planeación.	Aprobar el Manual de Gestión de Riesgos de Seguridad de la Información. Gestionar los temas correspondientes al Sistema Integrado de Gestión y la publicación del Manual de Gestión de Riesgos de Seguridad de la Información. Articular y apoyar las mesas de trabajo con cada uno de los “responsables”, designados por cada dependencia para la

Rol	Responsable	Responsabilidades
		gestión, identificación, valoración y tratamiento de los riesgos de Seguridad de la Información.
GESTIÓN TECNOLÓGICA – SEGURIDAD DE LA INFORMACIÓN	Jefa (e) Oficina Asesora de Planeación. Responsable Seguridad de la Información.	Definir, revisar y/o actualizar cuando sea necesario, el Manual de Gestión de Riesgos de Seguridad de la Información. Apoyar al equipo de riesgos de la OAP y las dependencias en la identificación, valoración y tratamiento de los riesgos de Seguridad de la Información. Apoyar a la OAP frente al monitoreo de los riesgos de Seguridad de la Información.

Tabla 1. Responsables
Fuente: Elaboración propia Gestión Tecnológica - Seguridad de la Información.

8. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

La Secretaría Distrital de la Mujer, definió y aprobó la política **PG-PLT-1 - POLÍTICA ADMINISTRACIÓN DEL RIESGO**, en la cual se definen los lineamientos para la gestión de riesgos en la Secretaría Distrital de la Mujer, se abarcan los riesgos asociados a Gestión, Corrupción y Seguridad de la Información.

9. METODOLOGÍA DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Teniendo en cuenta la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5 del Departamento Administrativo de la Función Pública DAFP, se debe definir el contexto interno y externo de la Entidad como parte inicial de la identificación de los riesgos, luego se realiza la identificación y valoración de los riesgos y se determinan las acciones pertinentes para disminuir los riesgos a un nivel aceptable y se continúa con el tratamiento de los riesgos.

La aceptación del riesgo debe asegurar que los riesgos residuales sean aceptados explícitamente por el equipo directivo de la entidad. Esto es importante dado el caso en el que la implementación de los controles se omita o deba posponerse, por ejemplo, por temas presupuestales o de capacidades de la Entidad[24].

[24] Guía N°7 – Gestión de Riesgos. MinTIC.

En la siguiente tabla se presentan las actividades propias de la gestión de riesgos de Seguridad de la Información, de acuerdo con las diferentes fases que define el Modelo de Seguridad y Privacidad de la Información – MSPI.

ETAPAS DEL MSPI	PROCESO DE GESTION DEL RIESGO EN LA SEGURIDADDE LA INFORMACION
Planear	Establecer Contexto Valoración del Riesgo Planificación del Tratamiento del Riesgo Aceptación del Riesgo
Implementar	Implementación del Plan de Tratamiento de Riesgo
Gestionar	Monitoreo y Revisión Continuo de los Riesgos
Mejora Continua	Mantener y Mejorar el Proceso de Gestión del Riesgo en la Seguridad de la Información.

Ilustración 1Etapas de la Gestión del Riesgo a lo Largo del MSPI
Fuente: Tomado de Guía N° 7 – Gestión de Riesgos de MinTIC.

10. IDENTIFICACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Para realizar la adecuada gestión de riesgos de seguridad de la información, es necesario que los responsables designados por cada dependencia conozcan el objetivo de su respectiva área. Igualmente, se debe tener disponible el inventario de activos de información de su competencia, insumo que se obtiene como resultado de las actividades descritas en el procedimiento GD-PR-2 – ACTIVOS DE INFORMACIÓN. Con esta información, se procede a realizar las actividades correspondientes a la identificación, valoración y tratamiento de riesgos de Seguridad de la Información y de esta manera definir las acciones necesarias a implementar para gestionar el respectivo tratamiento y el nivel adecuado de protección de los activos de información.

Para realizar el proceso de identificación y gestión de riesgos Seguridad de la Información se requiere tener disponible:

1. Matriz de activos de Información del proceso o dependencia según corresponda (se identifican por tipo de activo).
2. Matriz de Riesgos de Seguridad de la Información (Diligenciar la información que solicita el instrumento, la cual se describe de esta sección en adelante).
3. Manual de Gestión de Riesgos de Seguridad de la Información (este documento).

10.1 Instructivo de diligenciamiento de la matriz de riesgos

Se deben diligenciar todos los campos que solicita el instrumento:

COLUMNA	DESCRIPCIÓN - LINEAMIENTOS PARA EL DILIGENCIAMIENTO
Proceso	Seleccione de la lista desplegable el nombre del proceso al cual se le identificarán y valorarán los riesgos.
Dependencia	Seleccione de la lista desplegable el nombre de la dependencia al cual se le identificarán y valorarán los riesgos.
Objetivo	Diligencie el objetivo del proceso o dependencia. Consulte la caracterización del proceso o dependencia en LUCHA.
Alcance	Diligencie el alcance del proceso o dependencia. Consulte la caracterización del proceso o dependencia en LUCHA.
Referencia	Permite definir un consecutivo de riesgos.
Tipo de Activo	Consulte la matriz de activos de su proceso o dependencia según corresponda, los activos se van a agrupar por tipo de activo (Información, Hardware, Software, Servicio, Bases de Datos Personales, Recurso Humano, Infraestructura Crítica Cibernética) para identificar los riesgos, amenazas y vulnerabilidades. En este campo en la lista desplegable seleccione el tipo de activo y consulte en la matriz de activos a qué hace referencia para definir la descripción del riesgo.
Impacto	Analice las consecuencias que puede ocasionar a la Entidad la materialización del riesgo.
Amenaza (Causa Inmediata)	Circunstancias bajo las cuales se presenta el riesgo, es la situación más evidente frente al riesgo, redacte de la forma más concreta posible. En el manual de gestión de riesgos de seguridad de la información, consulte el numeral 10.3 Amenazas, verifique en la tabla de Amenazas si hay algunas de las amenazas comunes que le aplique, o adáptela de acuerdo con su necesidad, recuerde que la información allí consignada es una guía de referencia.
Vulnerabilidad (Causa Raíz)	Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo por la falta de un control, redacte de la forma más concreta posible. En el manual de gestión de riesgos de seguridad de la información, consulte el numeral 10.4 Amenazas, verifique en la tabla de Vulnerabilidades si hay algunas de las vulnerabilidades comunes que le aplique, o adáptela de acuerdo con su necesidad, recuerde que la información allí consignada es una guía de referencia.
Tipo de Riesgo	Seleccione de la Lista desplegable el tipo de riesgo, hay 3 riesgos asociados a seguridad de la información y 4 asociados a bases de datos personales. En el manual de gestión de riesgos de seguridad de la información, consulte el numeral 10.2 Riesgos de Seguridad de la Información y Bases de Datos Personales.
Descripción del Riesgo	Consolida o resume los análisis sobre impacto + causa inmediata + causa raíz, permitiendo contar con una redacción clara y concreta del riesgo identificado. Tenga en cuenta que la descripción inicia con **POSIBILIDAD DE + Tipo de Riesgo para la entidad + "AMENAZA - Causa Inmediata (Cómo)" + "VULNERABILIDADES - Causa Raíz (Por qué)"**
Clasificación del Riesgo	Utilice la lista desplegable que se encuentra parametrizada, le aparecerán las opciones: 1) Ejecución y Administración de procesos, 2) Fraude Externo, 3) Fraude Interno, 4) Fallas Tecnológicas, 5) Relaciones Laborales, 6) Usuarios, productos y practicas organizacionales, 7) Daños Activos Físicos, seleccione la opción que corresponda.

COLUMNA	DESCRIPCIÓN - LINEAMIENTOS PARA EL DILIGENCIAMIENTO
	En el manual de gestión de riesgos de seguridad de la información, consulte el numeral 10.5 Clasificación del Riesgo, en el cual se encuentra la descripción de cada uno.
Frecuencia con la cual se lleva a cabo la actividad	Defina el número de veces que se ejecuta la actividad durante el año, (Recuerde la probabilidad u ocurrencia del riesgo se define como el número de veces que se pasa por el punto de riesgo en el periodo de 1 año). La matriz automáticamente hará el cálculo para el nivel de probabilidad inherente (Columnas J-K) En el manual de gestión de riesgos de seguridad de la información, consulte el numeral 11.1 Probabilidad, en el cual se encuentra la tabla Análisis de Probabilidad, con la descripción de cada uno, de igual forma también se encuentra en el instrumento en la hoja "Tabla Probabilidad".
Criterios de Impacto	Utilice la lista desplegable que se encuentra parametrizada, le aparecerán las opciones de la tabla de Impacto en la hoja "Tabla Impacto" del instrumento. La matriz automáticamente hará el cálculo para el nivel de impacto inherente (Columnas N-P). En el manual de gestión de riesgos de seguridad de la información, consulte el numeral 11.2 Impacto, en el cual se encuentra la tabla Análisis de Impacto.
Zona de Riesgo Inherente	Teniendo en cuenta que ingresó la información de PROBABILIDAD e IMPACTO, la matriz automáticamente hará el cálculo para la zona de riesgo inherente (Columna N)
No. Control	Permite identificar el número de controles que se van a aplicar.
Descripción del Control	Recuerde que el control se define como la medida que permite reducir o mitigar un riesgo. Defina el control (es) que atacan la VULNERABILIDAD (causa raíz) del riesgo.
Afectación	**Este campo NO se diligencia**, depende de lo que seleccione en la columna **T**(Tipo).
Atributos Eficiencia Tipo	Utilice la lista desplegable que se encuentra parametrizada, le aparecerán las opciones: 1) Preventivo, 2) Detectivo, 3) Correctivo, seleccione según corresponda.
Atributos Eficiencia Implementación	Utilice la lista desplegable que se encuentra parametrizada, le aparecerán las opciones: 1) Automático, 2) Manual, seleccione según corresponda.
Atributos Eficiencia Calificación	**Este campo NO se diligencia, l**a matriz automáticamente hará el cálculo para el control analizado (Columna V)
Atributos Informativos Documentación	Utilice la lista desplegable que se encuentra parametrizada, le aparecerán las opciones: 1) Documentado, 2) Sin documentar.
Atributos Informativos Frecuencia	Utilice la lista desplegable que se encuentra parametrizada, le aparecerán las opciones: 1) Continua, 2) Aleatoria.
Atributos Informativos Registro	Utilice la lista desplegable que se encuentra parametrizada, le aparecerán las opciones: 1) Con Registro, 2) Sin Registro.

COLUMNA	DESCRIPCIÓN - LINEAMIENTOS PARA EL DILIGENCIAMIENTO
Evaluación del Nivel de Riesgo - Nivel de Riesgo Residual • **Probabilidad Residual (Z)** • **Probabilidad Residual Final (AA)** • **% (AB)** • **Impacto Residual Final (AC)** • **% (AD)** • **Zona de Riesgo Final (AE)**	**Estos campos NO se diligencian,** la matriz automáticamente hará el cálculo, acorde con el control o controles definidos con sus atributos analizados, lo que permitirá establecer el **nivel de riesgo inherente** (Columnas Z y AB, AC - AE).
Tratamiento	Utilice la lista desplegable que se encuentra parametrizada, le aparecerán las opciones: 1) Aceptar, 2) Evitar, 3) Reducir (compartir), 4) Reducir (mitigar).
Plan de Acción Responsable, fecha implementación, fecha seguimiento, seguimiento.	Esta casilla dependerá del tratamiento establecido, si es Aceptar no se requieren acciones adicionales, en caso de escoger Reducir (mitigar) se deben diligenciar las acciones que se adelantarán como complemento a los controles establecidos, no necesariamente son controles adicionales. Para Reducir (compartir), es viable diligenciar la acción que deriva de esta (ejemplo póliza seguros, tercerización), indicando información relevante.
Estado	Utilice la lista desplegable que se encuentra parametrizada, le aparecerán las opciones: 1) Finalizado, 2) En curso, 3) Sin Iniciar, la selección en este caso dependerá de las acciones del plan que se hayan establecido en cada caso.

Tabla 2 Instructivo de diligenciamiento de la matriz de riesgos
Fuente: Adaptado del Anexo 4, lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas

10.2 Riesgos de Seguridad de la Información y Bases de Datos Personales

A continuación, se definen los riesgos de Seguridad de la Información, las vulnerabilidades y amenazas, en concordancia con la línea base indicada en el Anexo, Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas de MINTIC, que incluye el identificador tanto para seguridad como para privacidad de la información, los cuales servirán de guía en el diligenciamiento del mapa riesgos.

NOTA: La identificación de los riesgos de Seguridad de la Información, se realizará frente a los diferentes tipos de activos de información (Información, Hardware, Software, Servicios, Recurso Humano, Bases de Datos Personales, e Infraestructura Crítica) que estén clasificados en la Matriz de Activos, **con nivel de criticidad ALTO**, a estos activos se les realizará el respectivo proceso de gestión de riesgos por parte de cada uno los responsables.

Riesgos de Seguridad de la Información:

1. Posibilidad de pérdida de confidencialidad.
2. Posibilidad de pérdida de integridad.
3. Posibilidad de pérdida de disponibilidad.

Riesgos de Datos Personales:

1. Posibilidad de pérdida de confidencialidad, divulgación no autorizada o mal uso de la información de datos personales.
2. Posibilidad de pérdida de integridad, alteración, o modificación de la Información de datos personales.
3. Posibilidad de afectación de la disponibilidad de la plataforma tecnológica o aplicativos que gestionan datos personales.
4. Posibilidad de uso y/o tratamiento inadecuado de los datos personales, incumpliendo las directrices o normativas al respecto.

Los riesgos de seguridad de la información y de datos personales, se basan en la afectación de alguno de alguno de los principios de seguridad de la información que son: Integridad, Confidencialidad o Disponibilidad de los activos de información.

10.3 Amenazas

Es la circunstancia o evento que puede causar un daño o impacto negativo, cuando explota la vulnerabilidad afectando la confidencialidad, integridad o disponibilidad de la información de la Secretaría Distrital de la Mujer, quiere decir esto, que la amenaza explota las vulnerabilidades identificadas de la información, el hardware, el software, los servicios, las personas, las bases de datos personales y/o la infraestructura tecnológica.

Cuando se analice el evento es necesario determinar si este tiene origen en las personas, los equipos, activos o es de tipo natural. Si tiene origen en las personas se debe determinar si el evento es de tipo intencional o accidental. El mayor nivel de detalle provisto facilita el análisis del riesgo correspondiente.

En la Tabla 3. Amenazas, se presenta el listado de amenazas identificadas por la Secretaría Distrital de la Mujer.

AMENAZAS		
TIPO	**ID**	**AMENAZAS**
1. Personas	**1.1**	Sobrecarga laboral.
	1.2	Ingeniería social.
	1.3	Coacción.
	1.4	Sabotaje.
	1.5	Errores humanos en el cumplimiento de las labores.

AMENAZAS		
TIPO	**ID**	**AMENAZAS**
	1.6	Acciones fraudulentas.
	1.7	Entrega indebida de la información.
	1.8	Modificación indebida de la información.
	1.9	Personal de servicios generales, puede ocasionar daños accidentales o premeditados en el datacenter cuando hacen la limpieza.
	1.10	Acceso de personal externo al datacenter, sin el acompañamiento del responsable(s) de la infraestructura.
2. Infraestructura Tecnológica	**2.1**	Contaminación, polvo, corrosión.
	2.2	Niveles de temperatura o humedad por fuera de los rangos aceptables.
	2.3	Fallas de electricidad.
	2.4	Daño en instalaciones físicas.
	2.5	Fallas en el aire acondicionado.
	2.6	Fallas en las UPS.
	2.7	Fallas en la planta eléctrica.
	2.8	Desastres naturales.
	2.9	Incendio.
	2.10	Inundación.
	2.11	Asonada/Conmoción civil/Terrorismo.
	2.12	Desastre accidental.
	2.12	Daños Intencionales.
3. Sistemas de Información/Servicios informáticos/Información	**3.1**	Ataque informático para acceder a información clasificada o reservada.
	3.2	Ataque informático para modificar o eliminar datos.
	3.3	Ataques de Ingeniería social.
	3.4	Interceptación de información.
	3.5	Cifrado no autorizado de la información por algún tipo de malware o acción mal intencionada.
	3.6	Corrupción de los datos por fallas en el software.
	3.7	Suplantación de usuarios.
	3.8	Abuso de privilegios.
	3.9	Elevación de privilegios.
	3.10	Exposición de información clasificada o reservada por errores de configuración.

AMENAZAS		
TIPO	**ID**	**AMENAZAS**
	3.11	Ataques por medio de Malware.
	3.12	Denegación de servicios.
	3.13	Errores humanos voluntarios o involuntarios en la parametrización de seguridad de los sistemas de información.
4. Hardware	**4.1**	Fallas en los componentes de hardware.
	4.2	Falla de medios de respaldo y recuperación.
	4.3	Fallas en el aire acondicionado.
	4.4	Fallas en las UPS.
	4.5	Uso de equipos no autorizados como piñas, videocámaras, y grabadoras entre otros.
	4.6	Hurto de equipos, medios magnéticos o documentos.
	4.7	Fallas en el suministro de energía eléctrica.
	4.8	Acceso a información clasificada o reservada dese componentes tecnológicos reciclados o desechados.
	4.9	Daños Intencionales.
	4.9	Daños Involuntarios.
5. Datos Personales	**5.1**	No facilitar o generar mecanismos de acceso a la información en materia de datos personales a los titulares.
	5.2	Tratar datos personales inadecuados y excesivos para la finalidad del tratamiento.
	5.3	Tratar datos personales con una finalidad distinta para la cual fueron recolectados.
	5.4	No disponer de una estructura organizativa, procesos y recursos para la adecuada gestión de los datos personales en la SDCR.
	5.5	Almacenar los datos personales, por tiempos superiores a los necesarios, según su finalidad de tratamiento.
	5.6	Realizar transferencias internacionales de datos personales a países que no ofrezcan un nivel de protección adecuado.
	5.7	No tramitar o dificultar el ejercicio de los derechos de los interesados.
	5.8	Resolución indebida del ejercicio de derechos de los interesados en tiempo, formato y forma.
	5.9	Seleccionar o mantener una relación con un encargado de tratamiento sin disponer de las garantías adecuadas.

AMENAZAS		
TIPO	**ID**	**AMENAZAS**
	5.10	No disponer de una estructura organizativa, procesos y recursos para una adecuada gestión datos personales en la Secretaría Distrital de la Mujer.
	5.11	Violaciones de la confidencialidad de los datos personales por parte de los funcionarios, contratistas o proveedores externos de la Secretaría Distrital de la Mujer.
	5.12	Información no actualizada o incorrecta (Registros duplicados con información inconsistente o con campos de datos incorrectos).
	5.13	Acceso a información, servicios, aplicaciones o dispositivos de forma no autorizada, por personas no autorizadas.
	5.14	Manipulación o modificación no autorizada de la información de datos personales.
	5.15	Deficiencias en los protocolos de recolección, almacenamiento, uso, circulación o supresión de los datos personales en formato físico
	5.16	Desordenes de carácter social que atenten contra activos que contienen información personal.

Tabla 3 Amenazas

Fuente: Adaptado del Anexo 4, lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas

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[25].

10.4 Vulnerabilidades

Son debilidades que pueden ser explotadas por una amenaza, la tecnología, los activos de información, las personas y/o la infraestructura con la que se realiza el procesamiento de la información, pueden ser explotadas por las amenazas, afectando de esta forma la confidencialidad, integridad y/o disponibilidad.

La Tabla “Vulnerabilidades”, presenta un listado de posibles causas, que han sido identificadas por la Secretaría Distrital de la Mujer, las cuales sirven como guía para la identificación de los riesgos de

[25] Tomado de Anexo 4, lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas.

Seguridad de la Información, es de aclarar que la vulnerabilidad se debe redactar citando el contexto y los detalles que la sustenten de forma clara y precisa.

Es fundamental entender que las vulnerabilidades están identificadas para los activos los activos de información de tipo Hardware, Software, Personas e Infraestructura Tecnológica que contenga o administre la información y esto debe quedar claramente diferenciado, por eso al describir una vulnerabilidad se debe especificar si esta radica sobre alguno de los tipos activos mencionados.

VULNERABILIDADES		
TIPO	**ID**	**ÍTEM**
1. Personas	**1.1**	Ausencia de personal idóneo.
	1.2	Ausencia o carencia de conocimientos y habilidades en el manejo de la tecnología.
	1.3	Desconocimiento de los lineamientos de Seguridad de la Información.
	1.4	Ausencia de reporte de incidentes de Seguridad de la Información.
	1.5	Debilidad frente a la gestión y uso de herramientas de seguridad informática.
	1.6	Falta de conciencia en materia de Seguridad de la Información.
	1.7	Desconocimiento de las políticas para el buen uso de los servicios tecnológicos (Red, Correo, Internet, Sistemas de Información, equipos, otros).
	1.8	Personal inconforme.
	1.9	Desconocimiento del marco legal y regulatorio de seguridad de la información.
	1.10	Desconocimiento de los controles de seguridad informática que se pueden aplicar a la información.
	1.11	Desconocimiento del marco legal y regulatorio de la protección de los datos personales.
	1.12	Falta de conciencia en la Protección de Datos Personales.
2. Infraestructura Tecnológica	**2.1**	Inexistencia, insuficiencia o mal uso de los controles de acceso físico a cualquiera de las instalaciones de la Entidad.
	2.2	Falta de monitoreo en el control de acceso físico a las instalaciones de la Entidad.
	2.3	Falta de mantenimiento a la infraestructura de: cableado, racks, aire acondicionado, sistemas de detección de incendios, y UPS.

VULNERABILIDADES		
TIPO	**ID**	**ÍTEM**
	2.4	Ubicación en un área susceptible de inundación o deterioro físico o locativo.
	2.5	Ausencia de protección contra humedad, polvo y suciedad.
	2.6	Ausencia o deficiencia en los controles para detección y/o prevención de incendios.
	2.7	Almacenamiento de documentos impresos sin medidas de protección.
	2.8	Errores humanos.
	2.9	Error en la gestión o administración de la Infraestructura Tecnológica.
	2.10	Fallas Técnicas de cualquier Hardware de la Infraestructura Tecnológica.
3. Sistemas de Información/Servicios informáticos/Información	**3.1**	Ausencia de mantenimientos preventivos y correctivos.
	3.2	Mala identificación de los requisitos técnicos y funcionales.
	3.3	Asignación inadecuada de privilegios de acceso.
	3.4	Ausencia de parchado de los componentes tecnológicos.
	3.5	Ausencia de mecanismos de identificación y autenticación de usuario.
	3.6	Inadecuada segregación de funciones, roles y perfiles de usuario.
	3.7	Ausencia de un proceso formal para la revisión periódica de los permisos de acceso de los usuarios.
	3.8	Ausencia de documentación actualizada de los Sistemas de Información.
	3.9	Imposibilidad de actualización de los Sistemas de Información por integración con otros.
	3.10	Falta de control en el cumplimiento de actualización de software.
	3.11	Ausencia o insuficiencia de pruebas de software.
	3.12	Uso de software desactualizado o que no cumple con los requerimientos de los usuarios.
	3.13	Configuraciones por defecto.
	3.14	Los ambientes de desarrollo y producción no se encuentran separados.
	3.15	Incapacidad del sistema para atender un alto volumen de conexiones.

VULNERABILIDADES		
TIPO	**ID**	**ÍTEM**
	3.16	Permitir la ejecución de sesiones simultáneas del mismo usuario en el sistema de información o servicio.
	3.17	Uso de código con vulnerabilidades, para la protección de la información.
	3.18	Versión desactualizada de software y medios de almacenamiento para las Copias de Respaldo.
	3.19	Ausencia de Backup y pruebas de restauración.
	3.20	Ausencia de documentación de los puertos que utilizan los Sistemas de Información o Servicios.
	3.21	Errores humanos.
	3.22	Ausencia de control para "terminar sesión" luego de un tiempo determinado de inactividad.
	3.23	No activación de registros de logs.
	3.24	Habilitación de servicios de red innecesarios.
	3.25	Ausencia de pruebas de vulnerabilidad periódicas.
4. Datos personales	**4.1**	Ausencia o carencia de personal que se encargue de la implementación de los temas relacionados con protección de los datos personales.
	4.2	Ausencia de personal de respaldo para los roles y responsabilidades en protección de datos personales.
	4.3	Ausencia de una política de protección de datos personales.
	4.4	Ausencia de procedimientos para la recolección de datos personales.
	4.5	Falta de conocimiento del personal en el debido tratamiento de los datos personales descritos en la finalidad del tratamiento.
	4.6	Ausencia de evidencia de la autorización para recolección y tratamiento de datos personales.
	4.7	Ausencia o debilidades en la parte contractual para la transmisión y/o transferencia de datos personales.
	4.8	Ausencia de lineamientos para el tratamiento de datos personales.
	4.9	Ausencia de procedimientos para la eliminación de los datos personales cuando ya no se requieran.

VULNERABILIDADES		
TIPO	**ID**	**ÍTEM**
	4.10	Carencia de procedimientos y/o herramientas para la solicitud de rectificaciones, cancelaciones y demás relacionadas con los datos personales.
	4.11	Dificultar o imposibilitar el ejercicio de los derechos de los titulares de los datos personales.
	4.12	Utilizar los datos personales para finalidades diferentes a las especificadas.
	4.13	Falta de controles de acceso frente a información de datos personales en temas reservados.
	4.14	Intereses a favor de un tercero o asignación de un perfil inadecuado de los servidores públicos que intervienen en el proceso.
	4.15	Intrusión informática, manipulación, modificación, eliminación, robo o cifrado de la información.
	4.16	Fallas en la plataforma tecnológica para control y validación de los campos que registran información de datos personales.
	4.17	Falta o fallas de sincronización de reloj del servidor.
5. Hardware	**5.1**	Ausencia Mantenimiento, insuficiente o inoportuno de los componentes de hardware.
	5.2	Debilidades en la seguridad física de la red de datos.
	5.3	Arquitectura de red de datos que no cumple los requerimientos de seguridad de la información.
	5.4	Ausencia de control sobre dispositivos móviles.
	5.5	Ausencia o deficiencia en los procedimientos de monitoreo a los recursos de procesamiento de información.
	5.6	Ausencia de pruebas de vulnerabilidad.
	5.7	Ausencia de Planes de Continuidad o Planes de Recuperación de Desastres (DRP).
	5.8	Ausencia de Pruebas de los Planes de Continuidad y/o los Planes de Recuperación de Desastres (DRP).
	5.9	Ausencia de sistemas redundantes (Alta disponibilidad).
	5.10	Único proveedor de Internet.
	5.11	Ausencia o insuficiencia de ANS (Acuerdos de niveles de servicio).
	5.12	Susceptibilidad a las variaciones de voltaje.

VULNERABILIDADES		
TIPO	**ID**	**ÍTEM**
	5.13	Ausencia de copias de respaldo del firmware de los dispositivos de comunicaciones, seguridad, servidores y otros que aplique.
	5.14	Falta de pruebas de verificación de las copias de respaldo.
	5.15	Ausencia de almacenamiento externo de las copias de respaldo.
	5.16	Obsolescencia de medios de respaldo de información.
	5.17	Obsolescencia de la infraestructura tecnológica.

Tabla 4 Vulnerabilidades

Fuente: Adaptado del Anexo 4, lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas

10.5 Clasificación del Riesgo

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

CLASIFICACIÓN DEL RIESGO	DESCRIPCIÓN
Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros
Fallas tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
Daños a activos fijos/ eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

Tabla 5 Clasificación del Riesgo

Fuente: Tomado de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5

11. VALORACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

En esta fase se establece la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de identificar la zona de riesgo inherente, en otras palabras, es el riesgo antes de aplicar controles.

11.1 Probabilidad

Para determinar la probabilidad, se tiene en cuenta la exposición del proceso o la actividad al riesgo que se está analizando, es decir, es el número de veces que se pasa por el punto de riesgo durante un año, como se muestra en la siguiente tabla.

ANÁLISIS DE PROBABILIDAD

Valor Inherente	Probabilidad Inherente	Frecuencia
Muy Baja	20%	La actividad que conlleva el riesgo se ejecuta como máximo 5 veces al año.
Baja	40%	La actividad que conlleva el riesgo se ejecuta de 6 a 25 veces por año.
Media	60%	La actividad que conlleva el riesgo se ejecuta de 26 a 150 veces por año.
Alta	80%	La actividad que conlleva el riesgo se ejecuta de 151 a 300 veces por año.
Muy Alta	100%	La actividad que conlleva el riesgo se ejecuta más de 301 veces por año.

Tabla 6 Análisis de Probabilidad
Fuente: Adaptado de Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5

11.2 Impacto

Para determinar el impacto referente a afectaciones económicas y/o reputacionales los cuales contemplan afectaciones a la ejecución presupuestal, pagos por sanciones económicas, indemnizaciones a terceros, sanciones por incumplimientos de tipo legal; así como afectación a la imagen institucional por vulneraciones a la información o por fallas en la prestación del servicio como lo señala la guía del DAFP, en este sentido se tienen los siguientes criterios para definir los niveles de impacto.

ANÁLISIS DE IMPACTO

Valor Inherente	Impacto Inherente	Afectación económica	Afectación reputacional
Muy Baja	20%	Pérdida económica hasta 10 SMLMV.	El riesgo afecta la imagen de algún área de la organización.
Baja	40%	Pérdida económica de 11 hasta 20 SMLV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, a nivel interno, de directivos y/o de proveedores.
Media	60%	Pérdida económica de 20 hasta 100 SMLV	Afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Alta	80%	Pérdida económica de 100 hasta 500 SMLV	Afecta la imagen de la entidad con efecto publicitario sostenido a nivel Sectorial.
Muy Alta	100%	Pérdida económica superior a 500 SMLMV	Afecta la imagen de la entidad a nivel nacional, con efecto publicitarios a nivel Distrital.

Tabla 7 Análisis de Impacto
Fuente: Adaptado de Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5

11.3 Evaluación del riesgo

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se obtiene el resultado del riesgo inherente o inicial, es decir antes de aplicar controles, y se identifica el nivel de severidad del riesgo, que puede quedar ubicado en alguna de las 4 zonas (Extremo, Alto, Moderado, Bajo), para lo cual se tiene como referencia la siguiente matriz de calor.

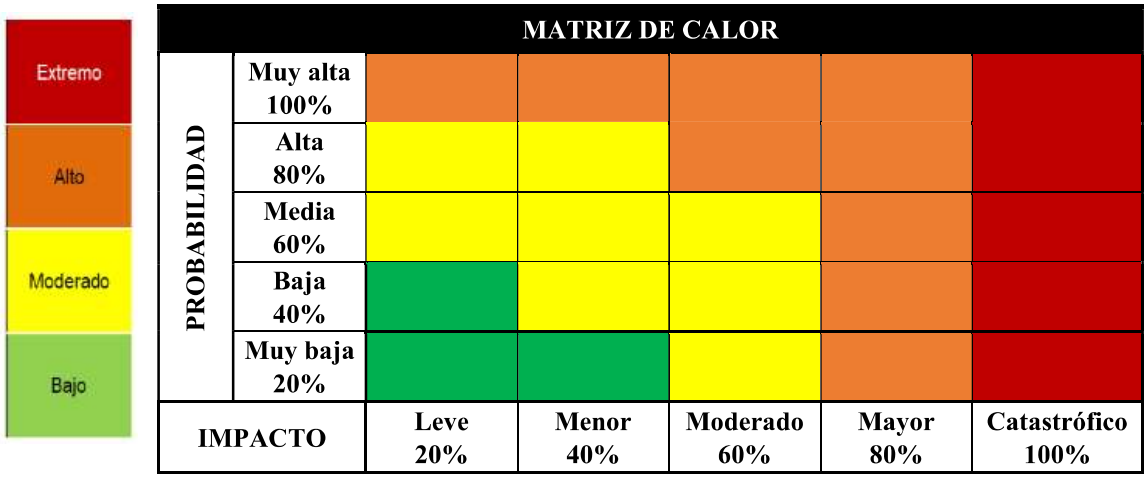

Tabla 8 Matriz de calor evaluación del riesgo
Fuente: Tomado de Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5

Es importante tener en cuenta las siguientes premisas:

- La fuente de información de los controles, son los Líderes de procesos, dependencia o funcionarios, quienes tienen el criterio experto, en concordancia con el objetivo de su proceso o dependencia.
- Los responsables de implementar y monitorear la efectividad de los controles son los Líderes de proceso con el apoyo de su equipo de trabajo.

12. TRATAMIENTO DE LOS RIESGOS

Una vez identificados y valorados los riesgos, se debe definir el tratamiento para cada uno de ellos como la decisión que se toma frente a un determinado nivel de riesgo, dicha decisión puede ser aceptar, reducir o evitar. Lo anterior teniendo en cuenta los criterios definidos en la Política de Administración del Riesgo adoptada por la Secretaría Distrital de la Mujer. Las decisiones que se toman de acuerdo con el nivel de riesgo pueden ser:

- **ACEPTAR,** cuando la Zona de Riesgo Residual es **BAJA, o MODERADA**
- **REDUCIR, EVITAR o COMPARTIR,** cuando la Zona de Riesgo Residual es **ALTA**
- **REDUCIR, EVITAR o COMPARTIR,** cuando la Zona de Riesgo Residual es **EXTREMA**

Así mismo, se definen los **niveles de aceptación del riesgo**, con el fin de determinar el máximo valor del nivel de riesgo que la entidad puede soportar y a partir del cual se considera por la alta dirección que no sería posible el logro de los objetivos de la entidad, partiendo del "**Apetito**" que es el nivel de riesgo que se puede aceptar en relación con sus objetivos, el marco legal y se define por las diferentes clasificaciones de riesgos, así mismo se establece el valor máximo de desviación y la "**Tolerancia**" Tope máximo admisible del nivel de riesgo con respecto al apetito determinado, para lo cual para los riesgos de seguridad, se define lo siguiente[26]:

Riesgo	Nivel de Aceptación	Zona de Riesgo Inherente	Gestión del Riesgo	Seguimiento Primera y Segunda línea de defensa (OAP)
SEGURIDAD DE LA INFORMACIÓN	SI	BAJA	Definir y/o mantener los controles existentes.	Se realiza seguimiento a los controles con periodicidad CUATRIMESTRAL y se registran sus avances en el instrumento definido por la Entidad.
		MODERADA		
	NO	ALTA	Se deben establecer nuevos controles o fortalecer los existentes.	
		EXTREMA		

Tabla 9 Niveles de aceptación del riesgo
Fuente: Adaptada de POLÍTICA DE ADMINISTRACIÓN DEL RIESGO - Secretaría Distrital de la Mujer

[26] ADAPTADA DE POLÍTICA DE ADMINISTRACIÓN DEL RIESGO - Secretaría Distrital de la Mujer

Ilustración 2 Estrategias para combatir el riesgo
Fuente: Tomado de Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5.

Es importante resaltar que cuando se decide reducir el riesgo es necesario definir un plan de acción o tratamiento, donde se incluya entre otros, el responsable, la fecha en la que se implementará el control y la fecha de seguimiento a este[27].

13. CONTROLES ASOCIADOS

De acuerdo a las directrices de la Guía de Administración del Riesgo del DAFP, para el tratamiento de los riesgos, es necesario aplicar como mínimo los controles del Anexo A, de la ISO/IEC 27001:2013, cuando estos se ajusten al respectivo análisis de los riesgos que se han identificado los controles se encuentran identificados en la Guía No. 8 del Modelo de Seguridad y Privacidad de la Información – MSPI, https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf .

El seguimiento a la implementación de los controles se realizará mediante el plan de tratamiento de riesgos, en este punto se indica el control aplicado, el responsable y el tiempo de implementación.

14. ANEXOS

Anexo 1. Matriz de riesgos de seguridad de la información

[27] Tomado de Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5

15. REGISTRO DE MODIFICACIONES

VERSIÓN	FECHA	DESCRIPCIÓN DE LA MODIFICACIÓN
1	16/08//2022	Primera versión del Manual de Gestión de Riesgos de Seguridad de la Información de la Secretaría Distrital de la Mujer.

	NOMBRE	CARGO
ELABORÓ	Andrés Giovanny Cadena Herrera	Contratista - OAP
REVISÓ	Mónica de la Cruz Luz Angela Andrade Sirley Yessenia Quevedo Diana Hernández Roger Ortiz Nelly García	Contratista - OAP Contratista - OAP Contratista - OAP Contratista - OAP Contratista - OAP Profesional Universitario
APROBÓ	Sandra Catalina Campos Romero	Jefa Oficina Asesora de Planeación