

# PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Instituto de Desarrollo Municipal de Dosquebradas  
**Vigencia 2021**

## TABLA DE CONTENIDO

1.	DERECHOS DE AUTOR .....	5
2.	INTRODUCCIÓN .....	6
3.	OBJETIVO .....	7
4.	ALCANCE .....	8
5.	MARCO LEGAL Y NORMATIVO .....	9
5.1.	DECRETOS Y LEYES .....	9
5.2.	BASES METODOLÓGICAS .....	10
6.	GLOSARIO .....	11
6.1.	Acceso a la Información Pública .....	11
6.2.	Activo .....	11
6.3.	Activo de Información .....	11
6.4.	Archivo .....	11
6.5.	Amenazas .....	12
6.6.	Análisis de Riesgo .....	12
6.7.	Auditoría .....	12
6.8.	Autorización .....	12
6.9.	Bases de Datos Personales .....	13
6.10.	Ciberseguridad .....	13
6.11.	Ciberespacio .....	13
6.12.	Control .....	13
6.13.	Datos Abiertos .....	14
6.14.	Datos Personales .....	14

6.15.	Datos Personales Públicos.....	14
6.16.	Datos Personales Privados .....	15
6.17.	Datos Personales Mixtos .....	15
6.18.	Datos Personales Sensibles .....	15
6.19.	Declaración de aplicabilidad .....	15
6.20.	Derecho a la Intimidad .....	16
6.21.	Encargado del Tratamiento de Datos .....	16
6.22.	Gestión de incidentes de seguridad de la información.....	16
6.23.	Información Pública Clasificada .....	16
6.24.	Información Pública Reservada .....	17
6.25.	Ley de Habeas Data.....	17
6.26.	Mecanismos de protección de datos personales .....	17
6.27.	Plan de continuidad del negocio.....	18
6.28.	Plan de tratamiento de riesgos.....	18
6.29.	Privacidad.....	18
6.30.	Registro Nacional de Bases de Datos.....	18
6.31.	Responsabilidad Demostrada .....	19
6.32.	Responsable del Tratamiento de Datos .....	19
6.33.	Riesgo.....	19
6.34.	Seguridad de la información .....	19
6.35.	Sistema de Gestión de Seguridad de la Información SGSI.....	20
6.36.	Titulares de la información .....	20
6.37.	Tratamiento de Datos Personales .....	20
6.38.	Trazabilidad.....	20
6.39.	Vulnerabilidad.....	21

6.40.	Partes interesadas (Stakeholder).....	21
<b>7.</b>	<b>METODOLOGIA.....</b>	<b>22</b>
7.1.	Criterios de Frecuencia.....	22
7.2.	Criterios De Impacto .....	23
7.2.1.	Insignificante .....	23
7.2.2.	Menor.....	23
7.2.3.	Moderado.....	23
7.2.4.	Mayor.....	23
7.2.5.	Catastrófico.....	24
7.3.	Mapa de Calor de Riesgos.....	24
7.4.	Tratamiento del Riesgo .....	25
7.5.	Criterios para el tratamiento del riesgo .....	26
7.5.1.	Mitigar .....	26
7.5.2.	Prevenir.....	26
7.5.3.	Dispersar .....	26
7.5.4.	Transferir .....	26
7.5.5.	Asumir .....	27
<b>8.</b>	<b>PLAN DE TRATAMIENTO DE RIESGOS.....</b>	<b>28</b>
8.1.	PLAN DE TRABAJO .....	33
9.	BIBLIOGRAFIA .....	34

## 1. DERECHOS DE AUTOR

El documento ha sido elaborado por el **INSTITUTO DE DESARROLLO MUNICIPAL DE DOSQUEBRADAS – RISARALDA** para la implementación del componente de seguridad y privacidad de la información.

Contiene información de la apropiación de la estrategia de Gobierno en Línea y de la política de Gobierno Digital del Ministerio de Tecnologías de la Información y Comunicaciones de Colombia (MinTIC), puede ser reproducido siempre y cuando se cite la fuente.

## 2. INTRODUCCIÓN

El **Instituto de Desarrollo Municipal de Dosquebradas (IDM)**, en cumplimiento a las Políticas y Directrices establecidas por el Ministerio de Tecnologías de la Información y las Comunicaciones, el Decreto 612 del 4 de Abril de 2018, Decreto 1078 de 2015 y la NTC/IEC ISO 27001:2013, implementará actividades de planeación estratégica para el control y administración efectiva de los riesgos y las necesidades de seguridad de la información de la entidad.

Una vez socializado el presente plan, los funcionarios, contratistas y terceros de la entidad adoptarán los controles de seguridad y privacidad de la información en sus procesos, con el fin de minimizar los riesgos que puedan afectar la seguridad y privacidad de la información.

### 3. OBJETIVO

Establecer los lineamientos de buenas prácticas de seguridad y privacidad de la información, que permita salvaguardar la integridad, confidencialidad y disponibilidad de la información en el **Instituto de Desarrollo Municipal de Dosquebradas (IDM)**.

#### 4. ALCANCE

El presente Plan de Tratamiento aplica para toda el **Instituto de Desarrollo Municipal de Dosquebradas (IDM)**, funcionarios, contratistas y terceros, que tengan acceso, usen, produzcan o manejen información de los procesos estratégicos, misionales, de apoyo y de evaluación, del este Ente Territorial.



## 5. MARCO LEGAL Y NORMATIVO

### 5.1. DECRETOS Y LEYES

- **LEY 1712 DE 2014** | Ley de transparencia y del derecho de acceso a la Información pública nacional.
- **LA LEY 1581 de 2012 y Decreto 1377 de 2013** | Ley de protección de datos personales.
- **LEY 1273 DE 2009** | Ley de delitos informáticos y la protección de la información y de los datos.
- **LEY 1221 DE 2008** | Promover y regular el teletrabajo como un instrumento de generación de empleo y autoempleo mediante la utilización de tecnologías de la información y las telecomunicaciones.
- **LEY 594/00** | Por medio de la cual se dicta la Ley General de Archivo y se dictan otras disposiciones.
- **LEY 527/1999** | Acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
- **CONPES 3854 de 2016** | Política de Seguridad Digital del Estado Colombiano.
- **CONPES 3701 DE 2011** | Lineamientos de política para ciberseguridad y Ciberdefensa

- **DECRETO 1078 del 26 de mayo de 2015** | Por medio del cual se expide el “Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”, se define el componente de seguridad y privacidad de la información, como parte integral de la estrategia GEL.
- **DECRETO 1008 del 14 de junio de 2018** | Por el cual se establecen los lineamientos generales de la política Gobierno Digital
- **DECRETO 884 de 2012** | Por medio del cual se reglamenta la Ley 1221 de 2008 y se dictan otras disposiciones.
- **DECRETO 612 del 4 de abril de 2018** | Por el cual se fijan directrices para la integración de planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado.

## 5.2. BASES METODOLÓGICAS

- **Norma ISO/IEC 27001:2013** | Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).
- **NTC/ISO 31000:2009** | Gestión de Riesgos. Principios y directrices.
- Modelo de Seguridad y Privacidad de la Información de Gobierno Digital – MSPI
- Guía No. 7, MINTIC, Guía de gestión de riesgos, Seguridad y privacidad de la información.
- Instrumento de Evaluación MSPI MINTIC

## **6. GLOSARIO**

### **6.1. Acceso a la Información Pública**

Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

### **6.2. Activo**

En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).

### **6.3. Activo de Información**

En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

### **6.4. Archivo**

Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como

testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)

#### **6.5. Amenazas**

Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

#### **6.6. Análisis de Riesgo**

Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

#### **6.7. Auditoría**

Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

#### **6.8. Autorización**

Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)

## **6.9. Bases de Datos Personales**

Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

## **6.10. Ciberseguridad**

Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

## **6.11. Ciberespacio**

Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

## **6.12. Control**

Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

### **6.13. Datos Abiertos**

Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)

### **6.14. Datos Personales**

Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

### **6.15. Datos Personales Públicos**

Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

#### **6.16. Datos Personales Privados**

Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

(Ley 1581 de 2012, art 3 literal h)

#### **6.17. Datos Personales Mixtos**

Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

#### **6.18. Datos Personales Sensibles**

Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

#### **6.19. Declaración de aplicabilidad**

Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la

justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

#### **6.20. Derecho a la Intimidad**

Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

#### **6.21. Encargado del Tratamiento de Datos**

Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3)

#### **6.22. Gestión de incidentes de seguridad de la información**

Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

#### **6.23. 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 semiprivado 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 de 2014. (Ley 1712 de 2014, art 6)

#### **6.24. 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 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

#### **6.25. Ley de Habeas Data**

Se refiere a la Ley Estatutaria 1266 de 2008.

Ley de Transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria 1712 de 2014.

#### **6.26. Mecanismos de protección de datos personales**

Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

#### **6.27. Plan de continuidad del negocio**

Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

#### **6.28. Plan de tratamiento de riesgos**

Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

#### **6.29. Privacidad**

En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

#### **6.30. Registro Nacional de Bases de Datos**

Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)

### **6.31. Responsabilidad Demostrada**

Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

### **6.32. Responsable del Tratamiento de Datos**

Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

### **6.33. Riesgo**

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).

### **6.34. Seguridad de la información**

Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

### **6.35. Sistema de Gestión de Seguridad de la Información SGSI**

Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

### **6.36. Titulares de la información**

Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)

### **6.37. Tratamiento de Datos Personales**

Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

### **6.38. Trazabilidad**

Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

#### **6.39. Vulnerabilidad**

Debilidad de un activo o control que puede ser explotada por una o más amenazas.

(ISO/IEC 27000).

#### **6.40. Partes interesadas (Stakeholder)**

Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

## 7. METODOLOGIA

El **Instituto de Desarrollo Municipal de Dosquebradas (IDM)** al unísono con este documento, adopta el plan de seguridad y privacidad de la información, los cuales se encontraran dentro del Proceso Gestión de Recursos Físicos y Tecnológicos y para 2021 en el nuevo proceso Gestión de Tecnologías de la Información, en ellos se establecen esquemas adaptados e integrados a los procesos de la entidad aportando al logro de los objetivos y facilitando la mejora continua a través del uso de información y conocimiento para la toma de decisiones acertadas frente a posibles eventos y sus efectos adversos.

Adicionalmente en este plan, se contempla la política e administración de riesgos de seguridad digital.

Dentro de esta metodología para la valoración de los riesgos se tienen en cuenta los siguientes criterios:

### 7.1. Criterios de Frecuencia

- **Excepcional** | Puede ocurrir sólo en circunstancias excepcionales y bajo condiciones muy puntuales.
- **Improbable** | Puede ocurrir en algún momento, pero su probabilidad de ocurrencia es casi nula.
- **Posible** | Puede ocurrir en algún momento bajo circunstancias normales.

- **Probable** | La probabilidad de que ocurra bajo condiciones normales alta.
- **Casi Seguro** | Se espera que ocurra en la mayoría de las circunstancias.

## 7.2. Criterios De Impacto

### 7.2.1. Insignificante

El riesgo no conlleva a consecuencias significativas, la afectación es insignificante en temas referentes al cumplimiento de objetivos.

### 7.2.2. Menor

El riesgo conlleva a consecuencias mínimas, la afectación en temas referentes al cumplimiento de objetivos presenta niveles bajos.

### 7.2.3. Moderado

La materialización de este riesgo conllevaría a consecuencias y afectaciones moderadas, de no darse un manejo adecuado, puede verse comprometido el cumplimiento de objetivos de los procesos.

### 7.2.4. Mayor

La materialización de este riesgo conlleva a afectaciones mayores, contempla tratamiento médico en vidas humanas y compromete el cumplimiento de los objetivos de los diferentes procesos.

### 7.2.5. Catastrófico

El Riesgo afecta negativamente la vida y/o bienes inmuebles y representa una enorme pérdida financiera. Si el riesgo es de un proceso de apoyo, estratégico o de evaluación, su materialización impide el cumplimiento del objetivo del proceso.

### 7.3. Mapa de Calor de Riesgos

Una vez determinado el nivel de frecuencia y consecuencia del riesgo se debe estimar el nivel de riesgo a través de la ubicación en la siguiente matriz de Nivel de Riesgo. Así se determinará el nivel de riesgo al que está expuesto el proceso por la materialización de los factores identificados previamente.

		Impacto				
		Insignificante	Menor	Moderado	Mayor	Catastrófico
Frecuencia	Excepcional	Bajo	Bajo	Medio	Alto	Alto
	Improbable	Bajo	Bajo	Medio	Alto	Extremo
	Posible	Bajo	Medio	Alto	Extremo	Extremo
	Probable	Medio	Alto	Alto	Extremo	Extremo
	Casi seguro	Alto	Alto	Extremo	Extremo	Extremo

De acuerdo con los resultados obtenidos en la valoración de riesgos podemos obtener los siguientes resultados:

- **Extremo** | Zona de nivel de riesgo en la que es aconsejable eliminar el factor que genera el riesgo en la medida que sea posible. Se deben implementar acciones



de prevención para tratar de eliminar la frecuencia del riesgo y/o disminuir el Impacto mediante acciones de mitigación.

- **Alto** | Zona de nivel de riesgo en que las consecuencias deben ser controladas con acciones. En este nivel de riesgo se deben tomar Acciones y controles que lleven en lo posible al riesgo a zonas moderada y baja.
- **Medio** | Zona de nivel de riesgo en que posible asumirlo, es decir, el riesgo se encuentra en un nivel que puede ser aceptado tras la implantación de algunas medidas de control diferentes a las que se poseen.
- **Bajo** | Estos riesgos son los de menor frecuencia de ocurrencia y más bajo impacto, sin embargo, representan una posible alteración al normal desarrollo de las labores de la entidad, por lo tanto, pueden asumirse.

#### 7.4. Tratamiento del Riesgo

Para dar desarrollo de este importante componente de la administración de riesgos, es prioritario resaltar que en la definición de las metas se contemple la fácil medición y por ende la realización de estas en un periodo de tiempo determinado. De esta manera se debe fijar una meta obligatoria para cada riesgo identificado y clasificado en la zona de riesgo como Altos o Extremos, teniendo en cuenta los siguientes aspectos:

- El límite de tiempo para la ejecución de la acción será de un año a partir de la aprobación del Mapa de Riesgos.
- Tener en cuenta aspectos de viabilidad jurídica, técnica, institucional y financiera.

## **7.5. Criterios para el tratamiento del riesgo**

### **7.5.1. Mitigar**

Se desarrolla mediante la generación de cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas. Un ejemplo de esto puede ser el control de calidad, manejo de los insumos, mantenimiento preventivo de los equipos, desarrollo tecnológico, etc.

### **7.5.2. Prevenir**

La prevención del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Se consigue mediante la optimización de los procedimientos y la implementación de controles. Ejemplo: Planes de contingencia.

### **7.5.3. Dispersar**

Se logra mediante la distribución o localización del riesgo en diversos lugares. Es así como, por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar.

### **7.5.4. Transferir**

Hace referencia a buscar respaldo y compartir con otra parte del riesgo como por

ejemplo tomar pólizas de seguros, esta técnica es usada para eliminar el riesgo de un lugar y pasarlo a otro o de un grupo a otro. Así mismo, el riesgo puede ser minimizado compartiéndolo con otro grupo o dependencia.

#### **7.5.5. Asumir**

Luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso el responsable del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo.

## 8. PLAN DE TRATAMIENTO DE RIESGOS

Los riesgos de seguridad de la información y privacidad de la información se basan en la afectación de tres (3) criterios en un activo o un grupo de activos dentro del proceso:

- Integridad
- Confidencialidad
- Disponibilidad

El **Instituto de Desarrollo Municipal - IDM**, se compromete a gestionar los riesgos, identificando y administrando los eventos potenciales que pueden afectar la plataforma estratégica, los objetivos institucionales y los procesos de la entidad. Para la adecuada gestión integral del riesgo en la CVP, se presenta los siguientes lineamientos:

1. Se adoptará las metodologías para gestionar los riesgos de la entidad a través del análisis del contexto, entendido como el entorno externo e interno, y la valoración de los mismos, es decir, su identificación, análisis y evaluación, y su posterior tratamiento, todo esto manteniendo comunicación y consulta constante y permanente monitoreo y revisión, para evitar así su materialización.

2. Los riesgos que se gestionan en el **Instituto de Desarrollo Municipal de Dosquebradas (IDM)** son los siguientes:

- Riesgos Estratégicos: Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública y por tanto impactan toda la

entidad.

- Riesgos gerenciales: Posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o la alta dirección.
- Riesgos operativos: Posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad.
- Riesgos financieros: Posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas dependencias involucradas con el proceso financiero.
- Riesgos tecnológicos: Posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de la entidad.
- Riesgos de cumplimiento: Posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal y las obligaciones
- Contractuales.
- Riesgo de imagen o reputacional: 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 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 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.

3. Se deben identificar los activos de información por cada proceso.
4. Se deben identificar los dueños de los activos.
5. Se deben clasificar los activos.
6. Se debe determinar la criticidad de los activos.
7. Se deben identificar las vulnerabilidades de los activos.
8. Se deben identificar las amenazas de los activos.
9. Se deben identificar los riesgos de los activos.
10. Se debe realizar una descripción de los riesgos.
11. Se debe revisar la probabilidad y el impacto de ocurrencia de los riesgos.
12. Se debe calcular el riesgo inherente.
13. Se deben aplicar los controles a los riesgos identificados.
14. Los controles deben tener una frecuencia de aplicación.
15. La tolerancia es el nivel del riesgo que la entidad puede o está dispuesta a soportar, que corresponden a los riesgos que se encuentren en zona residual Baja y los que se encuentran en otra zona se trataran de acuerdo a lineamientos establecidos.
16. La entidad revisará y actualizará la política de Gestión de Riesgos de acuerdo con los cambios del entorno, las nuevas metodologías y los resultados de los indicadores de gestión asociados a la materialización de riesgos definidos.
17. Los riesgos identificados en la entidad deberán ser monitoreados permanentemente, para asegurar que los controles sean eficaces y eficientes, y obtener

información para mejorar la evaluación y gestión de los riesgos e identificar la materialización oportuna de los riesgos.

18. Los niveles de responsabilidad sobre periodicidad de seguimiento y evaluación de los riesgos se llevarán a cabo de acuerdo a procedimientos.

Las opciones del tratamiento a los riesgos que se evalúan en la entidad son:

a) **Evitar el riesgo:** Se logra cuando al interior de los procesos se genera cambios sustanciales por rediseño, eliminación o cancelación de una actividad o conjunto de actividades que causan el riesgo, resultado de unos adecuados controles y acciones emprendidas.

Por ejemplo: el control de calidad, manejo de los insumos, mantenimiento preventivo de los equipos, desarrollo tecnológico, etc.

b) **Reducir el riesgo:** Implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección).

La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles.

Por ejemplo: a través de la optimización de los procedimientos y la implementación de controles.

c) **Compartir el riesgo:** Reduce su efecto a través del traspaso de las pérdidas a otras organizaciones o dependencias, como en el caso de los contratos de

seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido.

Por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar, la tercerización.

- d) **Asumir el riesgo:** Después de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso, el líder del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo. No aplica para los riesgos de corrupción, estos siempre deben conducir a un plan de acción o de tratamiento para mitigarlo.



## 8.1. PLAN DE TRABAJO

			Vigencia 2021						
N°	Actividad	Producto / Resultado	Enero	Febrero	Marzo	Abril	Mayo	Junio	Responsable
1	Actualización del plan de tratamiento de riesgos de seguridad y privacidad de la información	Plan de tratamiento de riesgos de seguridad y privacidad de la información							Tecnología
2	Revisión de la matriz de activos de información con las dependencias de la CVP	Matriz de activos de información actualizada							Tecnología
3	Identificación de riesgos de seguridad digital	Matriz de riesgos de seguridad digital							Tecnología
4	Tratamiento de riesgos de seguridad digital	Matriz de riesgos de seguridad digital							Tecnología
5	Oficialización de la matriz de riesgos de seguridad digital	Matriz de riesgos de seguridad digital							Tecnología

## 9. BIBLIOGRAFIA

*Plan de tratamiento de riesgos de seguridad y privacidad de la información, Caja de Vivienda Popular, Bogotá 2020.*

<https://www.cajaviviendapopular.gov.co/sites/default/files/208-TIC-Mn-09%20-%20PLAN%20TRATAMIENTO%20RIESGOS%20SPI%20V2.pdf>

*Plan de tratamiento de riesgos de seguridad y privacidad de la información, Alcaldía de Candelaria, Candelaria (Valle) 2020.*

<http://www.candelaria-valle.gov.co/Transparencia/PlaneacionGestionControl/Plan%20de%20Tratamiento%20de%20Riesgos%20de%20Seguridad%20y%20Privacidad%20de%20la%20Informaci%C3%B3n.pdf>

*Plan de tratamiento de riesgos de seguridad y privacidad de la información, Universidad Pedagógica y Tecnológica de Colombia, Tunja (Boyacá) 2020.*

[http://www.uptc.edu.co/export/sites/default/gel/documentos/plan\\_trata\\_rie\\_seg\\_inf2020.pdf](http://www.uptc.edu.co/export/sites/default/gel/documentos/plan_trata_rie_seg_inf2020.pdf)

*Herramienta de diagnóstico, Ministerio TIC.*

[https://www.mintic.gov.co/gestionti/615/articles-5482\\_Instrumento\\_Evaluacion\\_MSPI.xlsx](https://www.mintic.gov.co/gestionti/615/articles-5482_Instrumento_Evaluacion_MSPI.xlsx)

*Guía N° 3 - Procedimientos De Seguridad De La Información, Ministerio TIC.*

[https://www.mintic.gov.co/gestionti/615/articles-5482\\_G3\\_Procedimiento\\_de\\_Seguridad.pdf](https://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf)

*Guía N° 5 - Guía para la Gestión y Clasificación Activos de Información, Ministerio TIC.*

[https://www.mintic.gov.co/gestionti/615/articles-5482\\_G5\\_Gestion\\_Clasificacion.pdf](https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf)

*Guía N° 7 – Gestión de Riesgos, Ministerio TIC*

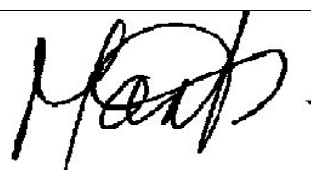

[https://www.mintic.gov.co/gestionti/615/articles-5482\\_G7\\_Gestion\\_Riesgos.pdf](https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf)

*Guía N° 14 - Plan de Capacitación, Sensibilización Y Comunicación De Seguridad De La Información, Ministerio TIC*

[https://www.mintic.gov.co/gestionti/615/articles-5482\\_G14\\_Plan\\_comunicacion\\_sensibilizacion.pdf](https://www.mintic.gov.co/gestionti/615/articles-5482_G14_Plan_comunicacion_sensibilizacion.pdf)

*Guía N° 20 - Guía de Transición de IPv4 a IPv6 para Colombia, Ministerio TIC*

[https://www.mintic.gov.co/gestionti/615/articles-5482\\_G20\\_Transicion\\_IPv4\\_IPv6.pdf](https://www.mintic.gov.co/gestionti/615/articles-5482_G20_Transicion_IPv4_IPv6.pdf)

PROYECT Ó: Hugo Andrés Orozco Contratista	REVISÓ: Marta Contreras Correa-Subdirectora Administrativa	APROBÓ: Ernesto Valencia - Director general
		
Diciembr e 16 de 2020	Enero 26 de 2021	Acta No. 11 de Diciembre 16 de 2021 Comité Institucional de Gestión y Desempeño