PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Instituto de Desarrollo Municipal de Dosquebradas
Vigencia 2022

TABLA DE CONTENIDO

1. DERECHOS DE AUTOR 5
2. INTRODUCCIÓN 6
3. OBJETIVO 7
3.1. OBJETIVOS ESPECIFICOS 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 20
6.40. Partes interesadas (Stakeholder) 21
7. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 22
7.1. FASE UNO - DIAGNÓSTICO 24
7.2. FASE DOS - PLANIFICACIÓN 25
7.2.1. Política de seguridad y privacidad de la información 25
7.2.2. Políticas Operativas de Seguridad y Privacidad de la Información 25
7.2.3. Procedimientos de Seguridad de la Información 26
7.2.4. Roles y Responsabilidades de Seguridad y Privacidad de la Información 26
7.2.5. Inventario de activos de información 26
7.2.6. Identificación, Valoración Y Tratamiento de Riesgos 27
7.2.7. Plan de tratamiento de riesgos 27
7.2.8. Plan de Comunicaciones 28
7.2.9. Plan de transición de IPv4 a IPv6 28
7.3. FASE DE IMPLEMENTACIÓN 29
7.3.1. Implementación del plan de tratamiento de riesgos 29
7.3.2. Indicadores De Gestión 29
7.4. FASE DE EVALUACIÓN DE DESEMPEÑO 30
7.4.1. Plan de Ejecución de Auditorias 30
7.5. FASE DE MEJORA CONTINUA 30
7.5.1. Plan de mejoramiento 31
7.6. PLAN DE IMPLEMENTACION – VIGENCIA 2022 32
8. 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, **actualizado para la vigencia 2022**

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 las acciones necesarias que aseguren la implementación del Modelo de Seguridad y Privacidad de la Información de acuerdo a la política de Gobierno Digital en el **Instituto de Desarrollo Municipal de Dosquebradas (IDM)** bajo el enfoque de mejoramiento continuo **actualizado para la vigencia 2022.**

3.1. OBJETIVOS ESPECIFICOS

- Identificar las actividades necesarias para garantizar la implementación del MSPI de acuerdo a la Política de Gobierno Digital.

- Estableces un cronograma de trabajo para la implementación del MSPI de acuerdo a las fases recomendadas en el Modelo de seguridad y privacidad de la información.

4. ALCANCE

Aplica a todos los procesos, a todos sus funcionarios, contratistas y terceros que en razón del cumplimiento de sus funciones compartan, utilicen, recolecten, procesen, intercambien o consulten su información, así como a los Entes de Control, Entidades relacionadas que accedan, ya sea interna o externamente a cualquier archivo de información, independientemente de su ubicación. Así mismo, este documento será aplicable a toda la información creada, procesada o utilizada por la entidad, sin importar el medio, formato o presentación o lugar en el cual se encuentre.

5. MARCO LEGAL Y NORMATIVO

5.1. DECRETOS Y LEYES

- **LEY 527/99** Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos.
- **LEY 594/00** Por medio de la cual se dicta la Ley General de Archivo y se dictan otras disposiciones.
- **CONPES 3701 DE 2011** Lineamientos de política para ciberseguridad y Ciberdefensa
- **LEY 1581/12** Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales.
- **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 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".
- **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.

- **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".
- **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".
- **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.

5.2. BASES METODOLÓGICAS

- Norma ISO/IEC 27001:2013.
- Modelo de Seguridad y Privacidad de la Información de Gobierno Digital – MSPI
- 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. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La seguridad de la información, como habilitador transversal de la política de Gobierno en Digital, permite alinearse con sus dos componentes denominados TIC para el estado y TIC para la sociedad aportando en el uso estratégico de las tecnologías de la información y las comunicaciones con la formulación e implementación del modelo de seguridad, el cual se enfoca en preservar la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento de la misión y los objetivos estratégicos de la entidad.

El Habilitador Transversal de Seguridad de la información busca que las entidades públicas implementen los lineamientos de seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad y disponibilidad y privacidad de los datos. Este habilitador se soporta en el Modelo de Seguridad y Privacidad de la Información - MSPI.

El modelo de seguridad y privacidad de la información entregada por el ministerio de las TIC dentro del marco de la política de Gobierno Digital contempla un ciclo de operación que consta de cinco (5) fases, las cuales permitirán que el **Instituto de Desarrollo Municipal de Dosquebradas - IDM** pueda gestionar adecuadamente la seguridad y privacidad de sus activos de información.

A continuación se especifican las fases y los productos a desarrollar para la implementación del MSPI en el **Instituto de Desarrollo Municipal - IDM**:

7.1. FASE UNO - DIAGNÓSTICO

En esta fase se pretende identificar el estado actual del **Instituto de Desarrollo Municipal de Dosquebradas (IDM)** con respecto a los requerimientos del MSPI.

En la fase de diagnóstico del MSPI se pretende alcanzar las siguientes metas:

- Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior del **Instituto de Desarrollo Municipal de Dosquebradas (IDM)**.
- Determinar el nivel de madurez de los controles de seguridad de la información.
- Identificar el avance de la implementación del ciclo de operación al interior de la entidad.

Para realizar esta fase se debe efectuar la recolección de la información con la ayuda de la herramienta de diagnóstico.

Una vez se tenga el resultado del diagnóstico inicial y se haya determinado el nivel de madurez de la entidad se procede al desarrollo de la fase de Planificación.

Herramienta : Herramienta de diagnóstico MinTIC
https://www.mintic.gov.co/gestionti/615/articles-5482_Instrumento_Evaluacion_MSPI.xlsx

Producto : Herramienta de diagnóstico diligenciada.

7.2. FASE DOS - PLANIFICACIÓN

En esta fase se debe modificar el plan seguridad y privacidad de la información manteniendo alineado con el objetivo misional del **Instituto de Desarrollo Municipal de Dosquebradas (IDM)**, con el propósito de definir las acciones a implementar dentro del contexto de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo.

A continuación se explica de manera general los productos esperados en la fase de planificación del Modelo de Seguridad y Privacidad de la Información

7.2.1. Política de seguridad y privacidad de la información

Actualizar la Política de Seguridad y Privacidad de la información contenida en un documento de alto nivel que incluye la voluntad de la Alta Dirección del **Instituto de Desarrollo Municipal de Dosquebradas (IDM)** para apoyar la implementación del Modelo de Seguridad y Privacidad de la Información la cual será divulgada al interior del Instituto.

7.2.2. Políticas Operativas de Seguridad y Privacidad de la Información

Desarrollar un Manual de políticas a nivel operativo, donde se describe los objetivos, alcances y el nivel de cumplimiento, que garanticen el adecuado uso de los Activos de información al interior del **Instituto de Desarrollo Municipal de Dosquebradas (IDM)**; definiendo las responsabilidades generales y específicas para la gestión de la

seguridad de la información.

7.2.3. Procedimientos de Seguridad de la Información

Desarrollar y formalizar procedimientos que permitan gestionar la seguridad de la información.

Para desarrollar esta actividad, la Guía No 3 del MSPI describe los procedimientos mínimos que se deberían tener en cuenta para la gestión de la seguridad al interior del **Instituto de Desarrollo Municipal de Dosquebradas (IDM)**.

Guía 3 : https://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf

7.2.4. Roles y Responsabilidades de Seguridad y Privacidad de la Información

El **Instituto de Desarrollo Municipal de Dosquebradas (IDM)** deberá definir mediante un acto administrativo (Resolución, circular, decreto, entre otros) los roles y las responsabilidades de seguridad de la información en los diferentes niveles (Directivo, De procesos y Operativos) que permitan la correcta toma de decisiones y una adecuada gestión que permita el cumplimiento de los objetivos en el Instituto.

7.2.5. Inventario de activos de información

Desarrollar una metodología de gestión de activos que le permita generar un inventario

de activos de información exacto, actualizado y consistente, que a su vez permita definir la criticidad de los activos de información, sus propietarios, custodios y usuarios.

La Guía No 5 del MSPI - Gestión De Activos, brinda información relacionada para poder llevar a cabo esta actividad.

Guía 5 : https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

7.2.6. Identificación, Valoración Y Tratamiento de Riesgos

El **Instituto de Desarrollo Municipal de Dosquebradas (IDM)** dispondrá de una política de gestión de riesgos la cual debe ser proyectada en tal sentido que permita identificar, evaluar, tratar y dar seguimiento a los riesgos de seguridad de la información a los que estén expuestos los activos de información, así como la declaración de aplicabilidad.

7.2.7. Plan de tratamiento de riesgos

La metodología definida en la política de riesgos será aplicada para la identificación, valoración y tratamiento de riesgos de los activos de información relacionados a seguridad de la información una vez se tengan identificados y clasificados todos los activos de información del **Instituto de Desarrollo Municipal de Dosquebradas (IDM)**.

Una vez se tengan identificados los riesgos, se definiran los controles de acuerdo a la

Guía No 8 - Controles de Seguridad del MSPI que mitigarán los riesgos identificados y se procede a realizar el plan de tratamiento de riesgos y la declaración de aplicabilidad

Guía 8 : https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

7.2.8. Plan de Comunicaciones

Definir un Plan de comunicación, sensibilización y capacitación que incluya la estrategia para que la seguridad de la información se convierta en cultura organizacional, al generar competencias y hábitos en todos los niveles (directivos, funcionarios, terceros) del **Instituto de Desarrollo Municipal de Dosquebradas (IDM)**.

Este plan será ejecutado, con el aval de la Alta Dirección, a todas las áreas del Instituto.

Para estructurar dicho plan se podrá utilizar la Guía No 14 del MSPI – plan de comunicación, sensibilización y capacitación.

Guía 14 : https://www.mintic.gov.co/gestionti/615/articles-5482_G14_Plan_comunicacion_sensibilizacion.pdf

7.2.9. Plan de transición de IPv4 a IPv6

Desarrollar el diagnóstico de IpV4 a IpV6 y el plan para llevar a cabo el proceso de transición de IPv4 a IPv6 en la entidad, orientado por la Guía No 20 - Transición de IPv4 a IPv6 para Colombia que indica las actividades específicas a desarrollar.

Guía 20 : https://www.mintic.gov.co/gestionti/615/articles-5482_G20_Transicion_IPv4_IPv6.pdf

7.3. FASE DE IMPLEMENTACIÓN

En esta fase se llevara a cabo la implementación de la estrategia trazada en la fase de planificación haciendo especial énfasis en la implementación de los controles que mitigan los riesgos, es decir el plan de mitigación de riesgos.

A continuación se explica de manera general los productos esperados en la fase de Implementación del Modelo de Seguridad y Privacidad de la Información en el **Instituto de Desarrollo Municipal de Dosquebradas (IDM)**.

7.3.1. Implementación del plan de tratamiento de riesgos

Desarrollar Informes de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso. Es decir del estado de implementación y efectividad de los controles escogidos para la mitigación de cada riesgo identificado en los activos de información.

7.3.2. Indicadores De Gestión

Definir indicadores que le permitan medir la efectividad, la eficiencia y la eficacia en la gestión y las acciones implementadas en seguridad de la información.

7.4. FASE DE EVALUACIÓN DE DESEMPEÑO

En esta fase, la oficina de control interno deberá contemplar dentro del proceso de auditorías, la planificación y desarrollo de ejercicios auditores para el seguimiento y monitoreo del MSPI

A continuación se explica de manera general los productos esperados en la fase de Evaluación de desempeño del Modelo de Seguridad y Privacidad de la Información en el **Instituto de Desarrollo Municipal de Dosquebradas (IDM).**

7.4.1. Plan de Ejecución de Auditorias

El **Instituto de Desarrollo Municipal de Dosquebradas (IDM)** desarrollará un documento donde se especifique el plan de auditorías para el MSPI, el cual estipulara la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la elaboración de informes.

Se debe llevar a cabo auditorías y revisiones a intervalos planificados que permitan identificar si el MSPI es conforme con los requisitos, está implementado adecuadamente y se mantiene de forma eficaz; así mismo es necesario difundir a las partes interesadas, los resultados de la ejecución de las auditorías.

7.5. FASE DE MEJORA CONTINUA

En esta fase el **Instituto de Desarrollo Municipal de Dosquebradas (IDM)** deberá

consolidar los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.

A continuación se explica de manera general los productos esperados en la fase de Evaluación de desempeño del Modelo de Seguridad y Privacidad de la Información en el **Instituto de Desarrollo Municipal de Dosquebradas (IDM)**

7.5.1. Plan de mejoramiento

Definir y ejecute el plan de mejora continua con base en los resultados de la fase de evaluación del desempeño

7.6. PLAN DE IMPLEMENTACION – VIGENCIA 2022

			Vigencia 2022												
N°	Actividad	Producto / Resultado	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Sept.	Oct.	Nov.	Dic.	Responsable
1	Actualización del plan del seguridad y privacidad de la información.	Plan de seguridad y privacidad de la información actualizado para la vigencia 2022.	100%												Tecnología
2	Revisión de las Políticas de seguridad informática.	Políticas actualizadas para la vigencia 2022.		100%											Tecnología
3	Revisión del inventario activos de información	Inventario activos de información actualizado vigencia 2022.		100%											Tecnología
4	Revisión del plan mitigación de riesgos.	Plan mitigación de riesgos actualizado para la vigencia 2022.			50%	100%									Tecnología
5	Política de tratamiento de datos personales	Documento generado			50%	100%									Tecnología Dirección Jurídica
6	Política de privacidad y condiciones de uso del Portal Web	Documento generado				50%	100%								Tecnología Dirección Jurídica
7	Esquema de publicaciones web	Documento generado				50%	100%								Tecnología Dirección Jurídica

8	Diseñar modulo para el curso de inducción virtual en plataforma de capacitaciones.	Modulo inducción al plan de seguridad y privacidad.		25%	50%	75%	100%								
9	Ejecutar un plan comunicación, sensibilización en seguridad, privacidad de la información y buenas practicas digitales.	Acciones de socialización y recordación permanente por canales virtuales como intranet, grupos whatsapp, entre otros.			10%	20%	30%	40%	50%	60%	70%	80%	90%	100%	Tecnología Comunicaciones

8. BIBLIOGRAFIA

Plan de seguridad y privacidad de la información, Concejo de Cali 2020.

http://www.concejodecali.gov.co/descargar.php?idFile=18571

Herramienta de diagnóstico, Ministerio TIC.

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

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

Guía N° 8 - Controles de Seguridad y Privacidad de la Información, Ministerio TIC

https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.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

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

PROYECTÓ:	REVISÓ Y APROBÓ:
HUGO ANDRES OROZCO Ingeniero de Apoyo TIC	Comité Institucional de Gestión y Desempeño
Enero 25 de 2022	Acta No. 1 de Enero 27 de 2022