PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL ÁREA METROPOLITANA DE BUCARAMANGA

Gestión Corporativa y Sistemas

ÁREA METROPOLITANA DE BUCARAMANGA
BUCARAMANGA - FLORIDABLANCA - GIRÓN - PIEDECUESTA

Bucaramanga, diciembre 21 de 2018
ÁREA METROPOLITANA DE BUCARMANGA
Avenida Los Samanes No. 9-280 Ciudadela Real de Minas.

Tabla de Contenido

1. INTRODUCCIÓN 2
2. DERECHOS DE AUTOR....3
3. OBJETIVOS 4
3.1 Objetivo general 4
3.2 Objetivos específicos 4
3.3 Objetivos estratégicos 4
4. ALCANCE DEL PLAN 5
5. ÁMBITO DE APLICACIÓN 5
6. DEFINICIONES....5
7. ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DEL RIESGO 7
8. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO 8
9. ETAPAS PARA LA ADMINISTRACIÓN DEL RIESGO 9
Contexto Estratégico 9
Identificación de los riesgos 10
Análisis de Riesgos 11
a) Calificación del riesgo 11
b) Evaluación del riesgo 13
c) Valoración de los riesgos....13
d) Identificación de controles.... 13
e) Evaluación de los controles 14
10. VALORACIÓN Y DIAGNOSTICO DEL RIESGO EN EL AMB 15
PROGRAMACIÓN, MANEJO Y SEGUIMIENTO DEL PLAN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN EL AMB....15
11. DOCUMENTOS DE REFERENCIA....17
12. MARCO LEGAL 17
13. REQUISITOS TECNICOS 17
14. RESPONSABLE DEL DOCUMENTO....18

1. INTRODUCCIÓN

El Área Metropolitana de Bucaramanga AMB como entidad Pública busca afrontar los diferentes retos con una infraestructura moderna, robusta y segura. Que sea competitiva en el nuevo mundo digital, que avanza día a día. Por ello La gestión de la seguridad de la información debe realizarse sistemáticamente por procesos completamente documentados y conocidos por toda la entidad.

Con ello se busca promover la implementación y ejecución de buenas prácticas de seguridad y privacidad de la información que constituyen un SGSI que podría llegar a llamarse como un sistema de calidad para la seguridad de la información, teniendo en cuenta el Modelo de Seguridad y Privacidad de la Información del Ministerio de las TIC.

Con el presente documento se busca crear un documento guía para la gestión de riesgos de seguridad y privacidad de la información del Área Metropolitana de Bucaramanga teniendo claro que llegar a garantizar niveles de protección total en el mundo informático es casi imposible aun cuando se cuente el suficiente presupuesto.

El objetivo principal de todo sistema de gestión de seguridad de la información el asegurarse que los riesgos en la seguridad de la información estén plenamente identificados y que los mismos sean enfrentados, asumidos y tratados de forma correcta por toda la organización a partir de una política que este ampliamente documentada y sea ejecutada de forma sistémica, estructurada, eficiente y repetible. además, que pueda adaptarse a los cambios que los sistemas de riesgos tienen con el tiempo.

Es aquí donde cobra sentido que las administraciones asignen los niveles de prioridad e importancia a todo este conjunto de planes estratégicos que comprenden el desarrollo del área de los tics en toda organización y puedan así contar con un buen y estructurado plan de tratamiento de riesgos de seguridad y privacidad de la información.

2. DERECHOS DE AUTOR

El presente documento se desarrolló teniendo en cuenta el artículo de Gestión del Riesgo y demás anexos con derechos reservados del Ministerio de las Tics como documento guía para la implementación de la estrategia de Gobierno Digital.

El contenido referenciado en el presente documento relacionado a definiciones, políticas o cualquier otro contenido como anexos fue tomado de la norma técnica colombiana NTC ISO/IEC 27001 así como los anexos con derechos reservados por parte de la ISO/ICONTEC

3. OBJETIVOS

3.1 Objetivo general

Identificar y dar prioridad a todas las actividades contempladas en el presente documento "PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÒN DEL AMB 2018 – 2020", alineados con la Política de Gobierno Digital (Estrategia de MINTIC) con fin de Mitigar oportunamente los riesgos asociados a la seguridad y privacidad de la información del Área Metropolitana de Bucaramanga y que las personas interesadas tengan la confianza en el tratamiento de la información que realiza la entidad.

3.2 Objetivos específicos

- Establecer los posibles riesgos a los que se encuentra expuesta la entidad en materias de seguridad y privacidad de la información
- Valorar los riesgos a los cuales se encuentra expuesta la información
- Concientizar a todos los colaboradores, áreas, procesos, proveedores externos en general sobre la necesidad e importancia de gestionar de manera adecuada, los riesgos inherentes a la gestión.
- Involucrar y comprometer a todos en la formulación e implementación de controles y acciones encaminadas a prevenir y administrar los riesgos.
- Establecer, mediante una adecuada administración del riesgo, una base confiable para la toma de decisiones y la planificación institucional.
- Planificar el tratamiento de cada uno de los riesgos hallados

3.3 Objetivos estratégicos

Definir el plan de tratamiento de riesgos que hace parte complementaria del plan de gestión de seguridad y privacidad de la información y de esta manera mitigar todos los riesgos hallados en la fase de Diagnostico o cualquier otro que se pueda generar, en el desarrollo de las áreas misionales de la entidad.

4. ALCANCE DEL PLAN

El alcance del presente plan comprende todas las actividades que permitan dar cumplimiento al 100% de los componentes definidos en esta etapa de diagnóstico y planeación en el Modelo de riesgos de la Seguridad y Privacidad de la Información del Ministerio de las Tics.

.

5. ÁMBITO DE APLICACIÓN

Los lineamientos definidos en esta guía, aplica para la gestión de los riesgos de seguridad de la información del área metropolitana de Bucaramanga AMB.

6. DEFINICIONES

Para la administración del riesgo, se tendrán en cuenta los siguientes términos y definiciones:

- **Aceptación del riesgo:** decisión de asumir un riesgo [Fuente 3.1 ISO/IEC 27001]
- **Activo:** Cualquier cosa que tiene valor para la organización [Fuente 3.2 ISO/IEC 27001] Gestión de Riesgos de Seguridad de la Información se consideran los siguientes tipos: información, actividades y procesos del negocio, software, hardware, personal, redes, organización y ubicación.
- **Amenaza**: situación externa que no controla la entidad y que puede afectar su operación
- **Análisis de riesgo:** uso sistemático de la información para identificar las fuentes y estimar el riesgo. [Fuente 3.3 ISO/IEC 27001]
- **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos o entidades no autorizados. [Fuente 3.4 ISO/IEC 27001]
- **Causa:** medios, circunstancias y/o agentes que generan riesgos.
- **Calificación del riesgo:** estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.

- **Compartir o transferir el riesgo:** opción de manejo que determina traspasar o compartir las pérdidas producto de la materialización de un riesgo con otras organizaciones mediante figuras como outsourcing, seguros, sitios alternos

- **Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada. [Fuente 3.6 ISO/IEC 27001]

- **Debilidad:** situación interna que la entidad puede controlar y que puede afectar su operación.

- **Evaluación del riesgo:** Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo. [Fuente 3.7 ISO/IEC 27001]

- **Gestión del Riesgo**: Actividades coordinadas para dirigir y controlar una organización en relación con el riesgo. [Fuente 3.9 ISO/IEC 27001]

- **Incidente de seguridad de la información**: Un evento o serie de eventos de seguridad de la información no deseado o inesperado, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. [Fuente 3.10 ISO/IEC 27001]

- **Integridad:** Propiedad de salvaguardad la exactitud y estado completo de los activos [Fuente 3.11 ISO/IEC 27001]

- **Riesgo:** Efecto de incertidumbre sobre los Objetivos. [Fuente ISO 31000]

- **Riesgo Residual:** Nivel relevante del riesgo después del tratamiento del riesgo. [Fuente 3.12 ISO/IEC 27001]

- **Riesgo de corrupción**: posibilidad de que, por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular.

- **Riesgo inherente**: es aquel al que se enfrenta una entidad o proceso en ausencia de controles y/o acciones para modificar su probabilidad o impacto.

- **Riesgo institucional**: Son los que afectan de manera directa el cumplimiento de los objetivos o la misión institucional. Los riesgos institucionales, son producto del análisis de los riesgos por proceso y son denominados de este tipo cuando cumplen las siguientes características:

Los riesgos que han sido clasificados como estratégicos: en el paso de identificación deben haber sido marcados como de clase estratégica, es decir, se relacionan con el cumplimiento de objetivos institucionales, misión y visión.
Los riesgos que se encuentran en zona alta o extrema: después de valorar el riesgo (identificación y evaluación de controles), el riesgo residual se ubica en zonas de riesgo alta o extrema, indicando que el grado de exposición a la materialización del riesgo aún se encuentra poco controlado.
Los riesgos que tengan incidencia en usuario o destinatario final externo: en el caso de la materialización del riesgo la afectación del usuario externo se presenta de manera directa.
Los riesgos de corrupción: todos los riesgos identificados que hagan referencia a situaciones de corrupción, serán considerados como riesgos de tipo institucional.

- **Plan de contingencia:** conjunto de acciones inmediatas, recursos, responsables y tiempos establecidos para hacer frente a la materialización del riesgo y garantizar la continuidad del servicio

- **Seguridad de la información:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información, además puede involucrar propiedades como: autenticidad, trazabilidad, no repudio y fiabilidad.

7. ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DEL RIESGO

El éxito de la administración del riesgo depende de la decidida participación de los directivos, servidores públicos y contratistas; por esto, es preciso identificar los actores que intervienen:

- Alta Dirección: aprueban las directrices para la administración del riesgo en la Entidad. La alta Dirección es la responsable del fortalecimiento de la política de administración del riesgo.
- Proceso Administración del Sistema Integrado de Gestión: Genera la metodología para la administración del riesgo de la Entidad, coordina, lidera, capacita y asesora en su aplicación.
- Responsables de los procesos: Identifican, analizan, evalúan y valoran los riesgos de la entidad (por procesos e institucionales) al menos una vez al año. Si bien los Líderes SIG apoyan la ejecución de las etapas de gestión del riesgo a nivel de los procesos, esto no quiere decir que el proceso de administración

de riesgos este solo bajo su responsabilidad. Al contrario, cada responsable de proceso se encarga de garantizar que en el proceso a su cargo se definan los riesgos que le competen, se establezcan las estrategias y responsabilidades para tratarlos y, sobre todo, que se llegue a cada funcionario que trabaja en dicho proceso. No se debe olvidar que son las personas que trabajan en cada uno de los procesos los que mejor conocen los riesgos existentes en el desarrollo de sus actividades.

- Servidores públicos y contratistas: ejecutar los controles y acciones definidas para la administración de los riesgos definidos, aportar en la identificación de posibles riesgos que puedan afectar la gestión de los procesos y/o de la entidad.
- Quien haga las veces de Control Interno: debe realizar evaluación y seguimiento a la política, los procedimientos y los controles propios de la administración de riesgos

8. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

En el área metropolitana de Bucaramanga, AMB adelantará las acciones pertinentes para la implementación y mantenimiento del proceso de Administración del Riesgo de la seguridad y privacidad de la información, y para ello todos los servidores de la entidad se comprometen a:

1. Gestión de recursos necesarios para implementación de nuevos esquemas para prevenir el riesgo de la seguridad y privacidad de la información en el AMB.
2. Dar a Conocer a todos los funcionarios del área metropolitana de Bucaramanga y hacer cumplir las normas internas y externas relacionadas con la administración de los riesgos.
3. Fortalecer dentro de la institución la cultura de administración de los riesgos para crear conciencia colectiva sobre los beneficios de su aplicación y los efectos nocivos de su desconocimiento.
4. Reportar los eventos de riesgo que se materialicen, utilizando los procedimientos e instrumentos establecidos para el efecto.
5. Presentar propuestas de mejora continua que permitan optimizar la forma de realizar y gestionar las actividades de la entidad para así aumentar nuestra eficacia y efectividad.

Para lograr lo anteriormente enunciado dependemos de una aprobación de recursos tanto humanos como presupuestales y tecnológicos necesarios, por parte de la Alta Dirección que permitan realizar el seguimiento y evaluación a la implementación y efectividad de esta política.

De igual manera, la presente guía forma parte de la política de administración del riesgo, por cuanto detalla las directrices que deben tenerse en cuenta para la gestión del mismo en la entidad y que tienen como propósito evitar la materialización del riesgo.

9. ETAPAS PARA LA ADMINISTRACIÓN DEL RIESGO

Las etapas a desarrollar durante la administración del riesgo; en la descripción de cada etapa se desplegarán los aspectos conceptuales y operativos que se deben tener en cuenta.

- Contexto estratégico: determinar los factores externos e internos del riesgo.
- Identificación: identificación de causas, riesgo, consecuencias y clasificación del riesgo.
- Análisis: Calificación y evaluación del riesgo inherente.
- Valoración: identificación y evaluación de controles; incluye la determinación del riesgo residual.
- Manejo: determinar, si es necesario, acciones para el fortalecimiento de los controles.
- Seguimiento: evaluación integral de los riesgos.

Contexto Estratégico

Definir el contexto estratégico contribuye al control de la entidad frente a la exposición al riesgo, ya que permite conocer las situaciones generadoras de riesgos, impidiendo con ello que la entidad actúe en dirección contraria a sus propósitos institucionales.

Para la definición del contexto estratégico, es fundamental tener claridad de la misión institucional del área metropolitana de Bucaramanga y sus objetivos, tener una visión sistémica de la gestión, de manera que se perciba la administración del riesgo como una herramienta gerencial y no como algo aislado del accionar administrativo. Por lo tanto, el diseño de esta primera etapa, se fundamenta en la identificación de los factores internos (debilidades) y externos (amenazas) que puedan generar riesgos que afecten el cumplimiento de los objetivos institucionales.

- Cada responsable de proceso del Sistema Integrado de Gestión, deberá identificar a los funcionarios que por su competencia pueden ser considerados claves dentro de cada una de las dependencias que participan en el proceso, serán factores de selección de estos, el conocimiento y nivel de toma de decisiones sobre el proceso.

- Los funcionarios seleccionados deberán ser convocados a una reunión inicial, en donde se presentará el propósito de esta actividad

- Se establecerán los factores internos y externos que afectan el proceso, para esto, se debe diligenciar el formato Matriz DOFA para identificación de riesgos:

Identificación de los riesgos

Es la etapa que permite conocer los eventos potenciales, estén o no bajo el control del área metropolitana de Bucaramanga, que ponen en riesgo el logro de su misión, estableciendo las causas y los efectos de su ocurrencia". Adicionalmente, en esta etapa también se realiza la clasificación del riesgo.

a) **Causas del riesgo**: Son las causas, uno de los aspectos a eliminar o mitigar para que el riesgo no se materialice; esto se logra mediante la definición de controles efectivos. Para realizar el análisis de las causas existen varias técnicas que serán analizadas a continuación.

b) **Consecuencias:** Son los efectos que se generan o pueden generarse con la materialización del riesgo sobre los objetivos de los procesos y de la entidad; generalmente se dan sobre las personas o los bienes materiales o inmateriales con incidencias importantes tales como daños físicos y fallecimiento, sanciones, pérdidas económicas, de información, de bienes, de imagen, de credibilidad y de confianza, interrupción del servicio y daño ambiental.

c) **Clasificación de los riesgos:** Durante la etapa de identificación, se realiza una clasificación del riesgo, según sus características, con el fin de orientar la formulación de un tratamiento adecuado que posibilite la mitigación del riego mediante la definición de controles y planes de manejo:

Clases de riesgo	Definición
Estratégico	Son los riesgos relacionados con la misión y el cumplimiento de los objetivos estratégicos, la definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.
Operativo	Relacionados con el funcionamiento y operatividad de los sistemas de información de la entidad: definición de procesos, estructura de la entidad, articulación entre dependencias.
Financieros	Relacionados con el manejo de los recursos de la entidad: ejecución presupuestal, elaboración estados financieros, pagos, manejos de excedentes de tesorería y manejo de los bienes.
Cumplimiento	Capacidad de cumplir requisitos legales, contractuales, ética pública y compromiso con la comunidad.
Tecnología	Capacidad para que la tecnología disponible satisfaga las necesidades actuales y futuras y el cumplimiento de la misión.
Imagen	Tienen que ver con la credibilidad, confianza y percepción de los usuarios de la entidad.

Análisis de Riesgos

El análisis del riesgo busca establecer la probabilidad de ocurrencia del mismo y sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo.

Se han establecido dos aspectos a tener en cuenta en el análisis de los riesgos identificados, probabilidad e impacto. Por la primera se entiende la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de Frecuencia, si se ha materializado, o de Factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado. Por Impacto se entiende las consecuencias que puede ocasionar a la Entidad la materialización del riesgo. La etapa de análisis de los riesgos se divide en:

a) Calificación del riesgo

Se logra a través de la estimación de la probabilidad de su ocurrencia y el impacto que puede causar la materialización del riesgo. La primera representa el número de veces que el riesgo se ha presentado en un determinado tiempo o puede presentarse, y la

segunda se refiere a la magnitud de sus efectos. Para la determinación de la calificación del riesgo, con base en la probabilidad y el impacto se debe tener en cuenta las siguientes tablas:

Escala para calificar la probabilidad del riesgo		
Nivel	Concepto	Frecuencia
Raro	El evento puede ocurrir solo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años.
Improbable	El evento puede ocurrir en algún momento.	Al menos de 1 vez en los últimos 5 años.
Moderado	El evento podría ocurrir en algún momento.	Al menos de 1 vez en los últimos 2 años.
Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias.	Al menos de 1 vez en el último año.
Casi certeza	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.

b) Evaluación del riesgo

Permite comparar los resultados de la calificación, con los criterios definidos para establecer el grado de exposición al riesgo; de esta forma, se define la zona de ubicación del riesgo inherente (antes de la definición de controles). La evaluación del riesgo se calcula con base en variables cuantitativas y cualitativas.

PROBABILIDAD	IMPACTO				
	Insignificante	Menor	Moderado	Mayor	Catastrófico
Raro	B	B	B	M	M
Improbable	B	M	M	A	A
Moderado	B	M	A	A	E
Probable	M	A	A	E	E
Casi certeza	M	A	E	E	E

Color	Zona de riesgo
B	Zona de riesgo baja
M	Zona de riesgo moderada
A	Zona de riesgo alta
E	Zona de riesgo extrema

Con la evaluación del riesgo, previa a la formulación de controles se obtiene la ubicación del riesgo en la matriz de evaluación; esto se denomina evaluación del riesgo inherente.

c) Valoración de los riesgos

Es el producto de confrontar la evaluación del riesgo y los controles (preventivos o correctivos) de los procesos. La valoración del riesgo se realiza en tres momentos: primero, identificando los controles (preventivos o correctivos) que pueden disminuir la probabilidad de ocurrencia o el impacto del riesgo; luego, se deben evaluar los controles, y finalmente, con base en los resultados de la evaluación de los controles, determinar la evaluación del riesgo residual y definir la opción de manejo del riesgo. Lo anterior de acuerdo con los formatos Identificación y evaluación de controles y Valoración del riesgo.

d) Identificación de controles

Los controles son las acciones orientadas a minimizar la probabilidad de ocurrencia o el impacto del riesgo; estos, deben estar directamente relacionados con las causas o las consecuencias identificadas para el riesgo y eliminarlas o mitigarlas. La administración del riesgo contribuirá a la gestión de la entidad, en la medida en que los controles se identifiquen, documenten, apliquen y sean efectivos para prevenir o mitigar los riesgos.

.

Causa	Riesgo	Efecto/Consecuencia	Control
Acceso a la red Privada sin ser autorizado o detectado	Perdida de información o robo de esta	Perímetro de seguridad física	Control Se deben utilizar perímetros de seguridad (barreras tales como paredes, puertas de acceso controladas con tarjeta o mostradores de recepción atendidos) para proteger las áreas que contienen información y servicios de procesamiento de información.

Clases de controles	
PREVENTIVO	CORRECTIVO
Acción o Conjunto de acciones que elimina o mitiga las causas del riesgo	Acción o conjunto de acciones que eliminan o mitigan las consecuencias
Orientación a disminuir la probabilidad de ocurrencia del riesgo	Orienta a disminuir el nivel de impacto del riesgo

e) Evaluación de los controles

Permite determinar en qué medida los controles identificados están aportando para disminuir los niveles de probabilidad e impacto del riesgo. Se evalúan verificando su documentación, aplicación y efectividad de la siguiente manera:

¿El control está documentado, incluye el responsable y la frecuencia de aplicación?	¿El control se está aplicando?	¿El control es efectivo (sirve o cumple su función?

10. VALORACIÓN Y DIAGNOSTICO DEL RIESGO EN EL AMB

Ver documento anexo DISGNOSTICO SGSI
Herramienta de Diagnostico del Ministerios de las TICS

PROGRAMACIÓN, MANEJO Y SEGUIMIENTO DEL PLAN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN EL AMB

ACTIVIDAD	TAREA A DESARROLLAR PARA EL PLAN	RESPONSABLE	FECHA INICIAL PLANIFICADA	FECHA FINAL PLANIFICADA	ESTADO
Diagnostico Riesgos de Seguridad de la información AMB	Realizar un Diagnóstico del estado actual	Ing. Fredy Varela,	30/07/2018	Finalizado, 1er Diagnostico diciembre de 2018	Gestionado
Actualizar el inventario básico de activos (software y hardware)	Actualizar el inventario actual de todos los activos de TIC de software y hardware	Ing. Fredy Varela,	1/08/2018	Si ya se tiene se coloca fecha de finalización y se adjunta documento a carpeta de anexos	Gestionado
Crear y/o actualizar políticas relacionadas con el cumplimiento del Modelo de Seguridad y Privacidad de la Información	Elaborar y/o actualizar políticas según el modelo de Seguridad y Privacidad de la Información.	Ing. Fredy Varela	1/08/2018	29/03/2019	En proceso
Crear y/o actualizar procedimientos para la clasificación de la información	Elaborar los procedimientos para clasificar la información	Ing. Fredy Varela	1/08/2018	30/05/2019	En proceso
Implementar la Ley 1581:2012 sobre protección de datos personales	Implementar la política de y requisitos de le ley de protección de datos personales	Ing. Fredy Varela	FECHA INICIO CONTRATO	FECHA FINALIZACIÒN CONTRATO	Por definir

Socializaciones políticas de Seguridad y Privacidad de la Información	Elaborar e implementar el cronograma de socialización de Políticas	Ing. Fredy Varela	2/01/2019	30/06/2019.	En proceso
Elaboración del Manual de roles y responsabilidad	Elaborar para su posterior presentación ante la Dirección del AMB	Ing. Fredy Varela	15/10/2018	26/10/2018	En proceso
Presentación manual de Roles y responsabilidades	Presentación ante la Dirección de la entidad para aprobación	Ing. Fredy Varela	2/01/2019	29/05/2019	En proceso
Clasificación de los riesgos hallados en el Diagnostico	Elaborar tabla de clasificación Según: Tipo, Amenaza y Origen	Ing. Fredy Varela	2/01/2019	29/03/2019	En proceso
Elaborar documento de registro de vulnerabilidades y controles existentes	Elaborar registro de las afectaciones recibidas y las acciones tomadas para su control	Ing. Fredy Varela	2/01/2019	31/12/2019	En proceso
Listado de consecuencias de las afectaciones recibidas y de las posibles a recibir	Elaborar documento donde se registren las consecuencias recibidas	Ing. Fredy Varela	2/01/2019	29/03/2019	En proceso
Evaluación del Riesgo	Documento de evaluación cualitativa del Riesgo	Ing. Fredy Varela	01/04/2019	30/05/2019	En Proceso
Documentación acciones de Mitigación realizadas por la entidad	Registro de acciones de Mitigación de riesgos	Ing. Fredy Varela	2/01/2019	31/12/2019	En proceso
Definición de Presupuesto	Definir Presupuesto de Ti para implementación del SGSi	Ing. Fredy Varela	2/01/2019	29/03/2019	Por definir

11. DOCUMENTOS DE REFERENCIA

MPSI Modelo de Seguridad y Privacidad de la Información del Ministerios de las TIC
ISO 27001:2013 Norma internacional emitida por la Organización Internacional de Normalización (ISO) sobre gestión de seguridad de la información.
LEY 1581:2012 Por la cual se dictan disposiciones generales para la protección de datos personales.
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.
Decreto 1078 de 2015 Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones

12. MARCO LEGAL

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.
- Decreto 612 de 4 de abril de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado.
- Decreto 1008 de 14 de junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital

13. REQUISITOS TECNICOS

- Norma técnica Colombiana NTC ISO/IEC 27001:2013 Sistemas de Gestión de la seguridad de la información.
- Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías y Sistemas de Información.
- Artículo de gestión del riesgo, Ministerio de Tecnologías y Sistemas de Información.

14. RESPONSABLE DEL DOCUMENTO

Jefe de Áreas tecnológicas y sistemas de información.

FECHA	VERSIÓN	CAMBIOS

ELABORADO POR:	REVISADO POR:	APROBADO POR: