TABLA DE CONTENIDO

Pág.

1 INTRODUCCIÓN 2

2 MARCO LEGAL 2

3 ALCANCE 3

4 OBJETIVOS 3

4.1 Objetivo general 3

4.2 Objetivos específicos 3

5 IMPLEMENTACIÓN 3

5.1 Actividades de Implementación 4

5.2 Cumplimiento en la Implementación 4

6 CRONOGRAMA 5

7 SEGUIMIENTO Y EVALUACIÓN 5

8 BIBLIOGRAFIA 6

1 INTRODUCCIÓN

La interconexión generalizada de diversos sistemas y redes de internet, ha propiciado una infraestructura operativa que abarca diversos sectores públicos y privados intercambiando grandes volúmenes de información, causando que los sistemas y redes individuales sean más vulnerables ya que están expuestos a una gran variedad de amenazas que pueden ocasionar pérdida, alteración o propagación no autorizada de la información. Lo anterior genera la necesidad de definir e implementar un conjunto de políticas y procedimientos que, mediante la evaluación del riesgo informático al cual el sistema está expuesto, los anticipe y minimice la posibilidad de ocurrencia de incidentes informáticos. Es de resaltar que gran parte de los incidentes de seguridad de la información ocurren por el desconocimiento o descuido de los usuarios que intervienen en el sistema o por la ausencia de mecanismos de control de riesgos informáticos.

2 MARCO LEGAL

CRITERIO	NORMAS
Plan Nacional de Desarrollo	Ley 1753 de 2015
Reglamentación TIC	Decreto 1008 de 2018 Decreto 0415 de 2016
Delitos Informáticos	Ley 1273 de 2009
Acceso a la información Pública	CONPES 3654 de 2012 – Política de Rendición de Cuentas de la Rama Ejecutiva a los ciudadanos. Ley 1712 de 2014 – Transparencia de la información. Decreto 0103 de 2015 – Reglamenta Ley 1712
Plan de Seguridad y Privacidad de la Información	Ley 1581 de 2012 Decreto 1377 de 2013 Decreto 886 de 2014
Rendición de Cuentas	Lineamientos para la Rendición de Cuentas por Medios Electrónicos - MinTIC. Manual Único de Rendición de Cuentas - Comité Técnico de la Política de Rendición de Cuentas
Datos Abiertos	Ley 1712 de 2014
Alistamiento para la Participación por medios Electrónicos	Anexo para ejercicios de participación electrónica Ley 1757 de 2015. Participación ciudadana
Acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales	Ley 527 de 1999 Decreto 1747 de 2000.
Ley General de Archivos	Ley 594 de 2000.

Racionalización de trámites y procedimientos Administrativos	Ley 962 de 2005.

3 ALCANCE

El presente plan se elabora con el fin de dar a conocer cómo se realizará la implementación y socialización del habilitador de Gobierno Digital de seguridad y privacidad de la información, el cual busca proteger la información de la entidad generada por los activos. Con base en estas políticas que aquí se establecen se realizaran los procedimientos que se aplican a la seguridad informática de los servidores y sitios web del Municipio de Armenia. Las directrices aquí definidas aplican también a los usuarios de los servidores y sitios web del Municipio de Armenia.

4 OBJETIVOS

4.1 Objetivo general

Controlar y minimizar los riesgos generados por los activos asociados a los procesos tecnológicos existentes, en la Alcaldía de Armenia con el fin de salvaguardar los activos de información, el manejo de medios, control de acceso y gestión de usuarios.

4.2 Objetivos específicos

Adoptar y ejecutar un conjunto de lineamientos para establecer buenas prácticas de uso de la infraestructura tecnológica con el que se minimice la probabilidad de ocurrencia de incidentes informáticos (control del riesgo informático) de los servidores y sitios web del Municipio de Armenia y se pueda responder a eventos inesperados e indeseados.

Concienciar a los usuarios sobre la necesidad e importancia de comprender los riesgos de seguridad informática.

5 IMPLEMENTACIÓN

Para realizar la implementación del Modelo de Seguridad y Privacidad de la Información en el Municipio de Armenia, se toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, a través de los decretos emitidos.

De acuerdo con esto, se definen las siguientes fases de implementación:

- Diagnosticar
- Planear
- Hacer
- Verificar
- Actuar

5.1 Actividades de Implementación

Realización del Diagnóstico

Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información

Realizar la Identificación de los Riesgos con los líderes del Proceso.

Entrevistar con los líderes del Proceso

Valorar del riesgo inherente y del riesgo residual

Realizar Mapas de calor donde se ubican los riesgos

Plantear al plan de tratamiento de riego aprobado por los lideres

5.2 Cumplimiento en la Implementación

De acuerdo a las fases mencionadas anteriormente, se describe a continuación los dominios que se deben desarrollar y los plazos de implementación de acuerdo a lo establecido por el Municipio de Armenia.

- Revisión y/o Modificación de la actual Política de Seguridad.
- Aspectos organizativos de la seguridad de la información
- Seguridad Ligada a los recursos humanos
- Revisión del Control de acceso
- Seguridad en la operativa
- Seguridad en las telecomunicaciones
- Gestión de Incidentes de Seguridad de la Información
- Aspectos de seguridad de la información en la gestión de continuidad del negocio.

6 CRONOGRAMA

ítem	Actividad	Producto	Fecha de Inicio	Fecha de Terminación	Responsable
1	Revisión del Contexto del Sistema de Gestión de Seguridad y Privacidad de la Información. (SGSI)	Documento con Misión, Visión, Objetivos del Negocio y Procesos seleccionados.	01/06/2025	31/12/2026	Secretaría TIC
2	Identificación y Valoración de Activos de Información.	Matriz con la identificación y clasificación de activos de información.	01/03/2025	30/08/2025	Líder Infraestructura Tecnológica
3	Identificación de amenazas y vulnerabilidades en la Infraestructura tecnológica y los Sistemas de Información	Documento diagnostico	01/09/2025	31/12/2025	Líder Infraestructura Tecnológica
4	Establecimiento de los escenarios de riesgos	Documento con escenarios de riesgos y las diferentes probabilidades de ocurrencia e impactos en la entidad.	01/11/2025	28/02/2026	Líder Infraestructura Tecnológica
4	Valoración de los Riesgos	Matriz con valor de activo, probabilidad e impacto.	01/12/2025	30/03/2026	Líder Infraestructura Tecnológica
4	Identificación, Valoración y tratamiento de riesgo	Estrategias de tratamiento y Mapa de Calor.	01/12/2025	30/03/2026	Líder Infraestructura Tecnológica
4	Identificación de los controles existentes	Documento con la identificación de riesgos inherentes y residuales.	01/03/2026	31/05/2026	Líder Infraestructura Tecnológica
4	Selección de las opciones para el tratamiento de riesgos	Plan de Tratamiento de riesgos	01/03/2026	31/05/2026	Secretaría TIC
4	Elaboración la declaración de aplicabilidad (SOA)	Matriz basada en el anexo A de la NTC ISO 27001:2013	31/05/2025	30/06/2026	Secretaría TIC
6	Implementación del plan de control operacional	Documento de seguimiento al cumplimiento de los requisitos establecidos para el cumplimiento del Plan	01/06/2026	31/12/2026	Secretaría TIC
7	Elaboración de los Indicadores De Gestión	Documento con los Indicadores de Gestión	01/01/2026	31/12/2026	Líder Infraestructura Tecnológica

7 SEGUIMIENTO Y EVALUACIÓN

El proceso de seguimiento y evaluación del Plan de Riesgos de Seguridad y Privacidad de la Información se realizará con los resultados que arrojen los indicadores de Gestión propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas, lo cual contempla las siguientes actividades:

.

- Revisión de la evaluación de los niveles de riesgo y riesgo residual después de la aplicación de controles y medidas administrativas.
- Seguimiento al alcance y a la implementación de los planes de manejo de riesgos.
- Seguimiento a los registros de acciones y eventos / incidentes que podrían tener impacto en la eficacia o desempeño de la seguridad de la información al interior de la entidad.
- Medición de los indicadores de gestión.
- Revisiones de acciones o planes de mejora
- Seguimiento a las autorías internas y externas del Plan.

8 BIBLIOGRAFIA

G.INF.01 Guía del dominio de información

Normas NTC-ISO-IEC 27001:2013, GTC-ISO-IEC 27002:2015, NTC-ISO-IEC 27005:2008

MSPI: Modelo de Seguridad y Privacidad de la Información para Gobierno Digital (Marco de Referencia de Arquitectura Empresarial para la gestión de TI) –MinTIC.

MIPG Modelo Integrado de Planeación y Gestión