Descripción

La Alcaldía de Villamaria, está comprometida en proporcionar un entorno seguro para el tratamiento de la información, preservando las características esenciales de confidencialidad, integridad, disponibilidad y privacidad de los activos de información, así como de la información vital para la sostenibilidad de la administración pública. Para lograrlo, se implementarán las mejores prácticas de seguridad y privacidad de la información, garantizando la protección de los datos y el cumplimiento de las normativas vigentes.

De acuerdo con la Política de Gobierno Digital, liderada por la division tics de la Alcaldía de Villamaría, cuyo objetivo es garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones (TIC), se busca contribuir a la construcción de una administración más participativa, eficiente y transparente. El área de Recursos Tecnológicos ha venido recopilando las mejores prácticas para proporcionar los requisitos necesarios para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo del Modelo de Seguridad y Privacidad de la Información, con el fin de diseñar, adoptar y promover políticas de seguridad digital en la entidad. La planificación e implementación de este modelo en la Alcaldía están determinadas por las necesidades y objetivos, los requisitos de seguridad, los procesos misionales, así como por el tamaño y la estructura de la administración pública. El Modelo de Seguridad y Privacidad de la Información se orienta a preservar la confidencialidad, integridad y disponibilidad de la información, garantizando la privacidad de los datos mediante la aplicación de un proceso de gestión de riesgos. Esto brinda confianza a las partes interesadas sobre la adecuada gestión de dichos riesgos en la entidad.

Con la expedición del decreto 1499 de 2017 y el manual del MODELO INTEGRADO DE PLANEACIÓN Y GESTION(MIPG) se debe elaborar e implementar la Política de Gestión del conocimiento y la innovación para las entidades públicas, la cual hace parte de la dimensión de gestión del conocimiento y la innovación.

La generación de herramientas para la utilización y apropiación del conocimiento busca identificar procesos que permitan obtener, organizar, sistematizar, guardar y compartir fácilmente datos e información a través de herramientas tecnológicas confiables su rol principal es poner a disposición el conocimiento para su uso por parte de las personas al interior y fuera de la entidad.

Objetivo

Definir e implementar las estrategias y mecanismos necesarios para desarrollar la Política de Seguridad Digital de la Alcaldía de Villamaría, garantizando los tres (3) pilares fundamentales de la seguridad de la información: confidencialidad, integridad y disponibilidad. La alcaldía se compromete a gestionar y controlar la seguridad digital mediante la definición de roles y responsabilidades, la separación de deberes, el contacto con autoridades y grupos de interés, y la integración de la seguridad digital en la gestión de proyectos. Además, establecerá controles para mitigar riesgos, todo ello en alineación con la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información.

Alcance

Esta política aplica a todos los procesos de la Alcaldía de Villamaría, Caldas, abarcando tanto los documentos físicos como electrónicos, los datos en los sistemas de información y los datos personales que la Alcaldía reconoce como activos de información. La clasificación de estos activos se realiza conforme a la normatividad vigente, ya que son vitales para el funcionamiento de la administración y la prestación eficiente de servicios a la ciudadanía.

Marco normativo

1. Ley 1341 de 2009. "Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC-, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones". Congreso de Colombia.

2. Ley 1581 de 2012. "Por la cual se dictan disposiciones generales para la protección de datos personales". Congreso de Colombia.

3. Ley 1712 de 2014. "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones". Congreso de Colombia.

4. Decreto 1499 de 2017. "Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015". Presidencia de la República.

5. 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". Ministerio de Tecnologías de la Información y las Comunicaciones

Definiciones

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.

AMENAZAS: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

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

LINEAMIENTOS: Directriz o disposición establecida por el Ministerio TIC, que debe ser implementada por las entidades públicas para el desarrollo de la Política de Gobierno Digital y se desarrolla a través de estándares, guías, recomendaciones o buenas prácticas.

ESTÁNDAR: Es el conjunto de características y requisitos que se toman como referencia o modelo y son de uso repetitivo y uniforme. Un estándar se construye a través de consenso y refleja la experiencia y las mejores prácticas en un área en particular, implican uniformidad y normalización y es de obligatorio cumplimiento.
ARQUITECTURA: Este habilitador busca que las entidades apliquen en su gestión un enfoque de Arquitectura Empresarial para el fortalecimiento de sus capacidades institucionales y de gestión de TI. El habilitador de

Arquitectura soporta su uso e implementación en el Marco de Referencia de Arquitectura Empresarial del Estado, que es el instrumento que establece la estructura conceptual, define lineamientos, incorpora mejores prácticas y traza la ruta de implementación que una entidad pública debe realizar.

SEGURIDAD DE LA INFORMACIÓN: Este habilitador busca que las entidades públicas incorporen la 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, disponibilidad, y privacidad de la información, así como la protección de los datos personales que tratan las entidades públicas en cumplimiento de la normatividad de protección de datos personales.

Lineamientos generales

1. Declaración de Alto Nivel: Establecer una declaración que defina la postura de la Alcaldía en cuanto a la protección de la seguridad y privacidad de la información. Esta declaración debe reflejar el compromiso institucional con la protección de la información y guiar todas las actividades relacionadas con la seguridad digital.

2. Requisitos Integrales: Incluir en la política los requisitos del negocio, legales y reglamentarios, así como las obligaciones de seguridad establecidas contractualmente. Esto asegura que la política no solo cumpla con las normativas vigentes, sino que también satisfaga las necesidades operativas y contractuales específicas.

3. Alineación Estratégica: Asegurar que la política esté alineada con el contexto organizacional y estratégico de la Alcaldía, integrándose adecuadamente en el marco de gestión del riesgo. Esto implica establecer y mantener un Sistema de Gestión de Seguridad de la Información (SGSI) que esté en sintonía con los objetivos estratégicos de la entidad.

4. Coherencia de Principios: Garantizar que la política mantenga coherencia entre los principios de seguridad de la información y la gestión documental. La integración de estos principios debe apoyar la protección integral de la información, asegurando que las prácticas de seguridad y la gestión documental trabajen en conjunto para resguardar los activos de información.

Roles y responsabilidades

Todos los funcionarios y/o colaboradores de la Alcaldia / Jefe de recursos tecnologicos

Primera línea de defensa: Definir los criterios de protección y buen uso de los activos de información, para lo cual deberá:

1. Acatar la política de seguridad y privacidad de la información de la Alcaldía y los procedimientos relacionados. Esto incluye adherirse a los acuerdos de uso y confidencialidad a los que se comprometan.

2.Proteger y utilizar adecuadamente los activos de información según la clasificación aprobada por el área correspondiente.

3. Informar de inmediato a la instancia encargada sobre cualquier incumplimiento de la política de seguridad y privacidad de la información o de los procedimientos corporativos, y asegurar que esta información sea comunicada al Comité de Gestión y Desempeño Institucional.

4. Aplicar las prácticas y controles de seguridad establecidos para la protección y gestión de los activos de información en su posesión.

5. Definir, aprobar y divulgar las pautas de protección y uso de los activos de información de acuerdo con los riesgos identificados y en alineación con la política de seguridad de la Alcaldía.

6.Desarrollar y mantener planes de continuidad para los procesos críticos, asegurando la operatividad de los sistemas y servicios esenciales.

7. Supervisar y gestionar la implementación de controles de seguridad, vigilando y reportando desviaciones e incidentes, y tomando las acciones correctivas necesarias.

8. Identificar y clasificar los activos de información en las herramientas de gestión de riesgos de la Alcaldía, asegurando que todos los riesgos sean adecuadamente gestionados.

9. Realizar el autocontrol de la gestión de seguridad y privacidad de la información, y reportar el estado de los indicadores relevantes a la dirección de la Alcaldía.

10.Asegurar que la política de seguridad y privacidad de la información y los procedimientos corporativos sean implementados correctamente, y que todos los funcionarios y colaboradores cumplan con estas directrices.

11. Informar a la instancia correspondiente sobre cualquier incumplimiento de las políticas y procedimientos de seguridad, y asegurar que se comunique al Comité de Gestión y Desempeño Institucional."

SEGUNDA LINEA DE DEFENSA:

1. Formalizar, divulgar, analizar y hacer cumplir el gobierno del Sistema de Gestión de Seguridad de la Información (SGSI), junto con cada uno de sus componentes, para garantizar su correcta implementación.

2. Asegurar, aprobar y verificar la correcta implementación de las directrices en materia de seguridad digital y de la información, y sus respectivos componentes, para el uso y la protección adecuada de la información.

3. Diseñar, desarrollar, implementar, monitorear, mejorar, evaluar y reportar a la organización sobre el funcionamiento del sistema de Seguridad y Privacidad de la Información, asegurando su eficacia y cumplimiento.

4. Acompañar y asesorar a las áreas responsables de la protección y uso de la información para que cumplan con las actividades del SGSI, garantizando su correcta gestión y protección de los activos de información.
5. Apoyar al líder del Sistema de Gestión de Seguridad de la Información en la planificación, ejecución y seguimiento de los planes y actividades del sistema, asegurando su operatividad y mejora continua.

Control Interno

Verificar que las áreas y funcionarios de la Alcaldía de Villamaría cumplan con sus responsabilidades en relación con el Sistema de Gestión de Seguridad de la Información (SGSI) y con la política de seguridad y privacidad de

la información, asegurando que se apliquen correctamente los controles y las medidas de seguridad establecidas.

Seguimiento, evaluación y mejora

EJE TEMATICO	DESCRIPCIÓN
Seguridad de la Información	Proteger los activos de información de la Alcaldía, garantizando su confidencialidad, integridad y disponibilidad.
Cumplimiento Normativo	Garantizar que todos los funcionarios y colaboradores de la Alcaldía cumplan con la política de seguridad y privacidad de la información.
Monitoreo y Mejora Continua	Asegurar el monitoreo constante y la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) de la Alcaldía.
Planes de Continuidad	Garantizar que los servicios críticos de la Alcaldía sigan funcionando en caso de incidentes o desastres.
Gestión de Riesgos	Identificar, evaluar y mitigar los riesgos tecnológicos que puedan afectar a los sistemas y servicios de la Alcaldía.

Indicador

NOMBRE	PROCESO	CATEGORIA	FUENTE
Porcentaje de Activos de Información Clasificados	Gestión de Activos de Información	Seguridad de la Información	Reportes de clasificación de activos
Número de Incidentes de Seguridad Reportados	Monitoreo de Seguridad y Gestión de Incidentes	Cumplimiento de la Seguridad	Plataforma de gestión de incidentes o reportes de la division tics

Porcentaje de Funcionarios Capacitados en Seguridad de la Información	Capacitación y Sensibilización en Seguridad	Cumplimiento Normativo	Registros de capacitación de Recursos Humanos	
Número de Incumplimientos a la Política de Seguridad	Monitoreo y Seguimiento de Cumplimiento Normativo	Cumplimiento de Políticas	Reportes de auditoría interna	
Porcentaje de Riesgos Tecnológicos Gestionados	Gestión de Riesgos Tecnológicos	Gestión de Riesgos	Matriz de riesgos tecnológicos	
Tiempo Promedio de Respuesta ante Incidentes de Seguridad	Respuesta y Recuperación ante Incidentes	Tiempo de Respuesta	Plataforma de monitoreo y gestión de incidentes	
Número de Auditorías Internas Realizadas	Auditoría y Monitoreo del SGSI	Auditoría Interna	Informes de auditoría interna	
Porcentaje de No Conformidades Corregidas	Gestión de No Conformidades	Mejora Continua	Informes de auditoría y acciones correctivas	
Porcentaje de Servicios Críticos con Planes de Continuidad Implementados	Gestión de Continuidad del Negocio	Continuidad Operativa	Planes de continuidad aprobados y registros de pruebas	
Número de Pruebas de Continuidad Realizadas	Pruebas y Simulacros de Continuidad del Negocio	Pruebas de Continuidad	Registros de pruebas de continuidad y simulacros	

Registro de modificaciones

Fecha	Versión

Fecha de aprobación	15/08/2025	
Elaboró:	José Ignacio Cuervo Asesor TICs	
Revisó:	John Edison Osorio Ramírez Secretario de Planeación	
Aprobó:	Jonier Alejandro Ramírez Zuluaga Alcalde	