Concejo Municipal Villamaría

CONCEJO VILLAMARIA-CALDAS

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

VIGENCIA 2025

CLAUDIA JULIANA TRUJILLO SAAVEDRA
PRESIDENTA CONCEJO MUNICIPAL DE VILLAMARIA-CALDAS. -

Concejo Municipal Villamaría

INTRODUCCIÓN

El Plan de Seguridad y Privacidad de la Información del Concejo Municipal de Villamaría, Caldas, es un documento estratégico que define las políticas, procedimientos y controles necesarios para proteger la información que se genera, almacena, procesa y transmite dentro de la entidad. Este plan tiene como propósito garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información, asegurando su cumplimiento con las normativas legales y estándares aplicables.

OBJETIVO GENERAL

Establecer un marco de gestión integral que permita prevenir, detectar y mitigar riesgos relacionados con el acceso no autorizado, pérdida, manipulación o divulgación indebida de la información, protegiendo tanto los datos públicos como privados gestionados por el Concejo

OBJETIVOS ESPECIFICOS

1. Identificar y clasificar la información según su nivel de confidencialidad, criticidad y valor, garantizando una gestión adecuada de los diferentes tipos de datos manejados (públicos, reservados, confidenciales).

2. Implementar políticas y procedimientos de seguridad para prevenir accesos no autorizados, alteraciones, pérdidas o divulgaciones indebidas de la información.

3. Establecer controles físicos y tecnológicos que protejan la infraestructura informática, los archivos físicos y los sistemas de información del Concejo.

4. Capacitar al personal en buenas prácticas de seguridad de la información, sensibilizándolos sobre su responsabilidad en la protección de datos y la privacidad.

5. Cumplir con la normativa legal vigente relacionada con la protección de datos personales (Ley 1581 de 2012), la gestión documental (Ley 594 de 2000) y la transparencia en la información pública.

6. Desarrollar planes de contingencia y recuperación para garantizar la continuidad de las operaciones en caso de incidentes de seguridad, desastres o fallos tecnológicos.

Concejo Municipal Villamaría

7. Monitorear y evaluar los riesgos asociados a la gestión de la información mediante auditorías internas y procesos de mejora continua.

8. Promover la transparencia y la confianza pública asegurando el manejo ético y responsable de la información en el Concejo.

9. Proteger los datos personales y sensibles de los ciudadanos y empleados, garantizando su uso únicamente para los fines autorizados y con el consentimiento correspondiente.

10. Fomentar la implementación de tecnologías seguras y actualizadas que respalden los procesos administrativos y la toma de decisiones.

CARACTERÍSTICAS PRINCIPALES

1. Confidencialidad: Garantizar que solo las personas autorizadas puedan acceder a la información.

2. Integridad: Proteger la exactitud y completitud de los datos, evitando su alteración no autorizada.

3. Disponibilidad: Asegurar que la información esté accesible para los usuarios cuando sea necesario, dentro de los límites establecidos.

4. Cumplimiento legal: Alinear las acciones del Concejo con las leyes colombianas aplicables (Ley 1581 de 2012, Ley 594 de 2000, entre otras).

BENEFICIOS ESPERADOS

Fortalecer la confianza de los ciudadanos y partes interesadas en la gestión del Concejo.

Reducir la exposición a riesgos legales, financieros y reputacionales asociados con la vulneración de información.

Mejorar la eficiencia operativa mediante el uso adecuado de tecnologías y buenas prácticas en seguridad de la información.

Concejo Municipal Villamaría

Este plan es un compromiso integral del Concejo para manejar la información con ética, responsabilidad y en pro del bienestar de la comunidad

MARCO LEGAL

- Constitución Política. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data; Artículo 20. Libertad de Información.

- Ley 527 de 1999. "Por medio de la cual se define y se reglamenta el acceso y uso de los mensajes de datos, comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones"

- Ley 962 de 2005. "Simplificación y Racionalización de Trámite. Atributos de seguridad en la información electrónica de entidades públicas;"

- Ley 1150 de 2007. "Seguridad de la información electrónica en contratación en línea"

- Ley 1266 de 2008. "Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países

- Ley 1273 de 2009. "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". Art. 199. Espionaje; Art. 258. Utilización indebida de información; Art. 418. Revelación de Secreto; Art. 419. Utilización de asunto sometido a secreto o reserva; Art. 420. Utilización indebida de información oficial; Artículo 431. Utilización indebida de información obtenida en el ejercicio de la función pública; Artículo 463. Espionaje.

- Ley 1341 de 2009. "Tecnologías de la Información y aplicación de seguridad".

Concejo Municipal Villamaría

- Ley 1437 de 2011. "Procedimiento Administrativo y aplicación de criterios de seguridad".

- Ley 1581 de 2012. "Por la cual se dictan disposiciones generales para la Protección de Datos Personales".

- Decreto Ley 019 de 2012. "Racionalización de trámites a través de medios electrónicos.

- Ley 1621 de 2013. "Por medio de la cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal y se dictan otras disposiciones".

- NTC-ISO 27001:2013: Sistema de Gestión de Seguridad de la Información.

- NTC-ISO 9001:2015: Sistema de Gestión de la Calidad, aplicable a la gestión de procesos documentales y de información.

GLOSARIO

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)

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).

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.

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

Concejo Municipal Villamaría

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

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

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

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)

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

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

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).

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).

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.

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

Concejo Municipal Villamaría

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)

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

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)

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)

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

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)

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).

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

Concejo Municipal Villamaría

cultural (Jurisprudencia Corte Constitucional).

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)

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).

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)

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)

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.

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, amonificación o cifrado.

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 2700

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles

Concejo Municipal Villamaría

necesarios para proteger la misma. (ISO/IEC 27000).

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.

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)

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.

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).

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)

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

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).

Concejo Municipal Villamaría

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

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).

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).

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

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.

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Habilitador Transversal de Seguridad de la información, como habilitador transversal de la política de Gobierno en digital, permite alinearse a los 2 componentes de la Política de Gobierno digital que son TIC para el estado y TIC para la sociedad al aportar en el uso estratégico de las tecnologías de la información con la formulación e implementación del modelo de seguridad enfocado a 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 Concejo del Municipio de Villamaría Caldas gestionar adecuadamente la seguridad y

Concejo Municipal Villamaría

privacidad de sus activos de información.
-

FASE DE DIAGNÓSTICO

1. Objetivo del diagnóstico

Evaluar el estado actual de la seguridad de la información y la gestión documental del Concejo, identificando fortalezas, debilidades, riesgos y oportunidades de mejora para garantizar la protección de la información y el cumplimiento normativo.

2. Metodología del diagnóstico

1. Recolección de información:

Identificar los tipos de información que gestiona el Concejo (pública, confidencial, sensible).

Revisar los procedimientos actuales para el manejo de datos y documentos.

Entrevistar al personal clave involucrado en la gestión de información.

Analizar los sistemas tecnológicos y físicos utilizados para almacenar y procesar la información.

2. Análisis de vulnerabilidades:

Evaluar las medidas de seguridad implementadas (contraseñas, control de accesos, sistemas de respaldo, etc.).

Identificar posibles brechas en la protección de datos personales y confidenciales.

Verificar si existen documentos o sistemas sin clasificar o sin protección adecuada.

3. Cumplimiento normativo:

Comparar las prácticas actuales con las exigencias legales (Ley 1581 de 2012, Ley 594 de 2000, Ley 1712 de 2014).

Concejo Municipal Villamaría

Evaluar si se cuenta con políticas claras para la protección de datos personales y la gestión documental.

4. Evaluación de riesgos:

Identificar riesgos asociados a la pérdida, robo o alteración de información.

Analizar las posibles consecuencias de un incidente de seguridad en términos legales, operativos y reputacionales.

5. Evaluación del personal:

Revisar el nivel de conocimiento del personal sobre buenas prácticas de seguridad de la información.

Verificar si existen capacitaciones regulares sobre protección de datos y manejo documental.

3. Resultados esperados

Mapa de riesgos: Identificación de las principales amenazas y vulnerabilidades en la gestión de información.

Análisis de brechas: Diferencias entre la situación actual y las mejores prácticas o requerimientos legales.

Fortalezas y debilidades: Identificación de aspectos que ya funcionan bien y áreas que necesitan mejora.

Recomendaciones iniciales: Propuestas para mitigar riesgos y fortalecer la seguridad de la información.

4. Instrumentos utilizados

Listas de verificación o checklists basados en normativas legales y estándares internacionales (ISO 27001).

Entrevistas y encuestas al personal administrativo y operativo.

Concejo Municipal Villamaría

Revisión documental (políticas, procedimientos, TRD, TVD, etc.).

Herramientas de análisis de sistemas de información (auditorías de TI)

FASE DE PLANIFICACION

La fase de planificación en el desarrollo de un Plan de Seguridad y Privacidad de la Información para el Concejo Municipal de Villamaría, Caldas, establece las estrategias, recursos y actividades necesarias para mitigar los riesgos identificados durante el diagnóstico y garantizar el cumplimiento normativo y operativo. Esta etapa es clave para estructurar el plan y definir las acciones a implementar.

1. Objetivo de la fase de planificación

Diseñar un plan detallado que permita implementar políticas, procedimientos y controles para proteger la información gestionada por el Concejo, alineado con los resultados del diagnóstico y las normativas vigentes.

2. Actividades principales de la fase de planificación

1. Definición de objetivos específicos:

Establecer metas concretas para la seguridad de la información, como proteger datos personales, implementar controles de acceso, mejorar la gestión documental y garantizar la continuidad de las operaciones.

2. Priorización de riesgos:

Identificar los riesgos más críticos detectados en la fase de diagnóstico.

Priorizar acciones en función del impacto y la probabilidad de ocurrencia.

Concejo Municipal Villamaría

3. Diseño de políticas y procedimientos:

Formular políticas de seguridad de la información, como:

Políticas de acceso a la información.

Políticas de protección de datos personales.

Políticas de uso de tecnologías de la información.

Diseñar procedimientos específicos para el manejo, almacenamiento, transferencia y eliminación de información.

4. Asignación de roles y responsabilidades:

Definir un equipo encargado de implementar y supervisar el plan.

Establecer responsables en áreas clave, como el tratamiento de datos personales, la administración de sistemas y la gestión documental.

5. Definición de controles técnicos y físicos:

Planificar la implementación de medidas de seguridad como:

Sistemas de contraseñas y autenticación.

Controles de acceso físico a archivos y equipos.

Copias de seguridad periódicas.

Uso de software de protección contra malware y otras amenazas.

Concejo Municipal Villamaría

6. Plan de capacitación y sensibilización:

Diseñar un programa para formar al personal en buenas prácticas de seguridad, protección de datos personales y gestión documental.

7. Planificación del presupuesto:

Estimar los recursos financieros, tecnológicos y humanos necesarios para implementar el plan.

Considerar la adquisición de herramientas tecnológicas, como software de gestión documental o sistemas de seguridad.

8. Establecimiento de indicadores de desempeño:

Definir métricas para medir el progreso y la efectividad de las acciones, como:

Número de incidentes de seguridad reportados.

Porcentaje de personal capacitado.

Nivel de cumplimiento normativo.

9. Diseño del cronograma de implementación:

Elaborar un calendario detallado con las actividades a realizar, los responsables y los plazos establecidos.

PRODUCTOS DE LA FASE DE PLANIFICACIÓN

Plan estratégico de seguridad de la información: Documento que define las acciones a implementar, los responsables, los plazos y los recursos requeridos.

Concejo Municipal Villamaría

Políticas y procedimientos escritos: Lineamientos claros para la gestión de la información.

Plan de capacitación: Cronograma y contenidos para formar al personal.

Indicadores de desempeño: Herramientas para evaluar la efectividad del plan.

Presupuesto preliminar: Estimación de costos para la implementación.

Resultados esperados

Un plan detallado y estructurado para fortalecer la seguridad y privacidad de la información.

Identificación de responsables y recursos necesarios para la implementación.

Alineación de las estrategias con los objetivos del Concejo y las normativas vigentes.

Esta fase permite organizar y dirigir los esfuerzos de manera eficiente, garantizando que el plan sea factible, sostenible y efectivo.

FASE DE IMPLEMENTACIÓN

La fase de implementación es donde se ejecutan las acciones definidas en el plan de seguridad y privacidad de la información del Concejo Municipal de Villamaría, Caldas. En esta etapa se materializan las políticas, controles y procedimientos, garantizando la protección de la información y el cumplimiento de los objetivos establecidos.

1. Objetivo de la fase de implementación

Poner en marcha las estrategias y controles planificados para garantizar la seguridad, confidencialidad, integridad y disponibilidad de la información gestionada por el Concejo.

Concejo Municipal Villamaría

2. Actividades principales de la fase de implementación

1. Adopción de políticas y procedimientos:

Formalizar e implementar las políticas de seguridad de la información y gestión documental aprobadas en la fase de planificación.

Comunicar las políticas a todo el personal del Concejo.

2. Despliegue de controles técnicos y físicos:

Configurar sistemas de seguridad tecnológica, como:

Sistemas de autenticación (contraseñas robustas, doble factor de autenticación).

Software de protección contra malware y amenazas (antivirus, firewalls).

Sistemas de respaldo y recuperación de datos.

Implementar controles físicos, como:

Restricciones de acceso a áreas de archivo.

Uso de dispositivos de seguridad (cámaras, cerraduras electrónicas).

3. Capacitación del personal:

Realizar talleres y sesiones de formación para que el personal conozca:

Las políticas de protección de datos personales.

Procedimientos para la gestión documental.

Buenas prácticas en ciberseguridad y manejo de información.

4. Clasificación y organización de la información:

Aplicar las Tablas de Retención Documental (TRD) y Tablas de Valoración Documental (TVD) para clasificar, organizar y custodiar los archivos físicos y

Concejo Municipal Villamaría

electrónicos.

Asegurar la implementación de herramientas tecnológicas para la gestión documental.

5. Pruebas y validación de sistemas:

Verificar que los sistemas tecnológicos implementados funcionan correctamente.

Realizar simulacros de recuperación de datos ante incidentes.

6. Comunicación interna y sensibilización:

Crear campañas internas para sensibilizar al personal sobre la importancia de la seguridad de la información.

Asegurar que todos comprendan los procedimientos y sepan a quién reportar incidentes.

7. Gestión de riesgos e incidentes:

Implementar el plan de respuesta ante incidentes de seguridad.

Configurar mecanismos para la detección y reporte de vulnerabilidades o amenazas.

8. Monitoreo inicial de indicadores:

Medir el cumplimiento de las actividades y evaluar el impacto de las acciones implementadas.

Realizar ajustes si se identifican fallas en los controles o procedimientos.

RESULTADOS ESPERADOS

Políticas y procedimientos implementados y en uso por el personal.

Controles tecnológicos y físicos operativos para proteger la información.

Concejo Municipal Villamaría

Personal capacitado en buenas prácticas de seguridad y gestión documental.

Información organizada y clasificada según la normativa (TRD y TVD).

Sistemas de respuesta activa ante incidentes de seguridad.

Indicadores iniciales que permitan evaluar el desempeño del plan.

Retos comunes durante la implementación

Resistencia al cambio por parte del personal.

Falta de recursos tecnológicos o presupuestales.

Problemas técnicos en la integración de sistemas.

Dificultad en la sensibilización sobre la importancia de la seguridad de la información.

Factores de éxito

Compromiso de la alta dirección del Concejo para apoyar las acciones del plan.

Participación activa del personal en las actividades de capacitación y sensibilización.

Supervisión continua durante la implementación para garantizar el cumplimiento de los plazos y objetivos.

La fase de implementación asegura que el plan pase del diseño a la acción, fortaleciendo la gestión segura y eficiente de la información en el Concejo Municipal.

FASE DE EVALUACIÓN DE DESEMPEÑO

El Plan de Desempeño dentro del contexto de un Plan de Seguridad y Privacidad de la Información para el Concejo Municipal de Villamaría, Caldas, tiene como objetivo medir, supervisar y mejorar continuamente la efectividad de las acciones implementadas. Este plan garantiza que las metas se alcancen y que las

Concejo Municipal Villamaría

actividades se ajusten a los objetivos estratégicos del Concejo.

Objetivo del Plan de Desempeño

Definir un sistema de medición y evaluación continua que permita verificar el cumplimiento de las políticas, procedimientos y controles de seguridad, así como identificar oportunidades de mejora en la protección de la información.

Componentes del Plan de Desempeño

Indicadores de Desempeño (KPI)

Definir métricas claras para evaluar la eficacia del plan, como:

Indicadores de Seguridad:

Número de incidentes de seguridad reportados.

Tasa de cumplimiento de las políticas de acceso a la información.

Porcentaje de datos respaldados periódicamente.

Indicadores de Capacitación:

Porcentaje de personal capacitado en seguridad de la información y gestión documental.

Evaluaciones de conocimiento post-capacitación.

Indicadores de Gestión Documental:

Porcentaje de documentos clasificados según las Tablas de Retención Documental (TRD).

Cumplimiento en los tiempos de actualización de documentos.

Indicadores de Cumplimiento Normativo:

Auditorías aprobadas relacionadas con protección de datos y gestión documental.

Número de recomendaciones legales implementadas.

Plan de Monitoreo y Seguimiento

Establecer un cronograma para realizar revisiones periódicas de desempeño

Concejo Municipal Villamaría

(mensual, trimestral o semestral).

Supervisar las actividades del personal para verificar el cumplimiento de los procedimientos establecidos.

Analizar el funcionamiento de los sistemas de seguridad tecnológica y ajustar configuraciones según sea necesario.

Auditorías Internas

Realizar auditorías internas periódicas para evaluar la efectividad de las políticas de seguridad de la información.

Identificar desviaciones y áreas críticas que requieran atención inmediata.

Evaluación del Personal

Aplicar evaluaciones prácticas al personal para medir el nivel de comprensión y aplicación de las políticas de seguridad.

Identificar necesidades de capacitación adicional.

Plan de Mejora Continua

Diseñar un plan de acción para corregir desviaciones detectadas durante el monitoreo y las auditorías.

Priorizar acciones según la criticidad de los riesgos identificados.

Incorporar nuevas tecnologías o ajustes en los procedimientos según las tendencias de seguridad y los cambios normativos.

Cronograma del Plan de Desempeño

El cronograma debe definir:

Periodicidad de las mediciones e informes (mensuales, trimestrales, anuales).

Fechas específicas para capacitaciones, auditorías internas y revisiones de políticas.

Plazos para implementar mejoras tras la detección de fallas.

Roles y Responsabilidades

Concejo Municipal Villamaría

Responsable de Seguridad de la Información: Supervisar y garantizar el cumplimiento del plan.

Equipo de Gestión Documental: Monitorear la correcta implementación de las TRD y TVD.

Personal Administrativo: Cumplir con las políticas establecidas y reportar incidentes.

Auditores Internos: Realizar revisiones periódicas y emitir recomendaciones.

Productos del Plan de Desempeño

Informes de desempeño: Resumen de indicadores clave, logros alcanzados y áreas de mejora.

Reporte de auditorías internas: Resultados detallados de las revisiones realizadas.

Plan de acción de mejora continua: Estrategias para abordar las brechas detectadas.

Resultados esperados

Reducción en el número de incidentes de seguridad.

Mejora en el cumplimiento normativo y de los procedimientos.

Mayor nivel de conocimiento y compromiso del personal.

Información más protegida y gestionada de forma eficiente.

Mejora continua en las operaciones del Concejo.

Este plan asegura que el Concejo evalúe regularmente su desempeño en seguridad y privacidad, promoviendo una gestión eficaz y adaptable a nuevos retos o regulaciones.

FASE DE MEJORA CONTINUA

La fase de mejora continua en un Plan de Seguridad y Privacidad de la Información para el Concejo Municipal de Villamaría, Caldas, es fundamental para mantener la efectividad del plan a largo plazo, adaptándose a nuevos desafíos, tecnologías y normativas. Esta etapa permite perfeccionar los procesos y controles mediante un ciclo de retroalimentación constante.

Concejo Municipal Villamaría

1. Objetivo de la fase de mejora continua

Garantizar la sostenibilidad y evolución del plan mediante la identificación de áreas de mejora, la implementación de cambios necesarios y la evaluación continua de su efectividad, asegurando el cumplimiento normativo y la protección de la información.

2. Enfoque metodológico

La mejora continua se basa en el Ciclo PHVA (Planear, Hacer, Verificar, Actuar):

1. Planear: Identificar oportunidades de mejora a partir de los resultados de auditorías, monitoreo e incidentes reportados.

2. Hacer: Implementar las acciones correctivas o preventivas.

3. Verificar: Evaluar la efectividad de las acciones implementadas mediante indicadores de desempeño.

4. Actuar: Ajustar y optimizar los procesos según los hallazgos.

3. Actividades principales de la fase de mejora continua

1. Monitoreo constante de indicadores:

Revisar periódicamente los indicadores definidos en el plan de desempeño, como la cantidad de incidentes de seguridad, el cumplimiento de capacitaciones y la efectividad de los controles implementados

2. Análisis de incidentes y riesgos:

Investigar incidentes de seguridad, identificar las causas raíz y proponer medidas para evitar que se repitan.

Revaluar los riesgos identificados en la fase de diagnóstico, considerando nuevos escenarios.

Concejo Municipal Villamaría

3. Auditorías internas y externas:

Realizar auditorías programadas para identificar desviaciones en las políticas y procedimientos.

Contratar auditorías externas, si es necesario, para obtener una visión imparcial y especializada.

4. Actualización de políticas y procedimientos:

Revisar y ajustar las políticas de seguridad y privacidad de la información, alineándolas con cambios normativos o tecnológicos.

Incorporar nuevas buenas prácticas o estándares internacionales relevantes (como ISO 27001).

5. Capacitación continua del personal:

Actualizar periódicamente al personal sobre nuevas amenazas, normativas o cambios en los procedimientos.

Sensibilizar constantemente sobre la importancia de la seguridad y privacidad de la información.

6. Innovación tecnológica:

Evaluar e implementar tecnologías más seguras y eficientes para la gestión de información.

Reemplazar sistemas obsoletos y actualizar herramientas de seguridad informática.

7. Evaluación de cumplimiento normativo:

Revisar el plan para asegurar que sigue alineado con las leyes aplicables (Ley 1581 de 2012, Ley 594 de 2000, entre otras).

Identificar y corregir posibles incumplimientos detectados en las auditorías.

Concejo Municipal Villamaría

8. Retroalimentación del personal:

Recopilar sugerencias y observaciones de los empleados para identificar problemas operativos y oportunidades de mejora.

Crear canales de comunicación abiertos para que el personal reporte vulnerabilidades o incidentes.

Herramientas para la mejora continua

Indicadores de desempeño: Permiten medir el impacto de las acciones correctivas.

Análisis de brechas: Comparar el estado actual con los objetivos establecidos.

Planes de acción: Documentar y priorizar las mejoras necesarias.

Talleres y capacitaciones: Mejorar las habilidades del personal continuamente.

Resultados esperados

Incremento en la efectividad de las medidas de seguridad y privacidad.

Reducción de incidentes de seguridad y violaciones de datos.

Mejor adaptación a cambios normativos y tecnológicos.

Mayor compromiso del personal con la protección de la información.

Incremento en la confianza de la ciudadanía respecto a la gestión de la información.

Factores de éxito

Compromiso de la dirección del Concejo Municipal para apoyar las acciones de mejora.

Disponibilidad de recursos tecnológicos, humanos y financieros.

Concejo Municipal Villamaría

Monitoreo constante y comunicación efectiva entre los equipos responsables.

La fase de mejora continua asegura que el Plan de Seguridad y Privacidad de la Información no sea estático, sino un proceso dinámico capaz de evolucionar frente a los retos actuales futuros.