Alcaldía Municipal de California, Santander 2024 – 2027
Secretaria de Gobierno
Email: gobierno@california-santander.gov.co
Carrera 6 No. 4 - 22
Tel: 3102182681 - 3112190854

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

DANILO VALBUENA PABÓN
ALCALDE MUNICIPAL

CALIFORNIA, SANTANDER
2026

Tabla de Contenido

1 INTRODUCCIÓN

La era digital ha transformado significativamente la forma en que los municipios gestionan, comparte y resguardan la información. En este contexto, la implementación de un robusto Plan de Seguridad y Privacidad de la Información se presenta como una imperiosa necesidad para el Municipio. Este plan busca establecer un marco integral que garantice la confidencialidad, integridad y disponibilidad de la información, al tiempo que salvaguarda la privacidad de los datos y cumple con las regulaciones vigentes.

En un entorno donde la tecnología avanza rápidamente y las amenazas cibernéticas evolucionan constantemente, es imperativo que el Municipio adopte medidas proactivas y estratégicas para proteger los activos de información crítica y preservar la confianza de la comunidad. Este plan no solo se enfoca en la seguridad técnica, sino también en la concientización y el compromiso de todos los miembros del municipio para fortalecer una cultura de seguridad de la información.

A través de este documento, se abordarán las distintas áreas críticas que involucran la gestión de información, desde la infraestructura tecnológica hasta la capacitación del personal y la disposición segura de datos. Al promover la seguridad y privacidad de la información, La alcaldía Municipal no solo protegerá sus activos, sino que también garantizará una administración eficiente y transparente que responde a las expectativas de sus ciudadanos.

Este plan es un compromiso continuo con la mejora constante. Se someterá a revisiones periódicas para adaptarse a los cambios tecnológicos, regulaciones y amenazas emergentes. La colaboración de todos los departamentos y empleados será esencial para su éxito. Juntos, trabajaremos para construir y mantener un entorno seguro y confiable para la información municipal.

2 JUSTIFICACIÓN

La creciente digitalización de los procesos administrativos y la ampliación de servicios en línea han colocado al Municipio en un escenario donde la seguridad de la información y la privacidad de los datos se han vuelto esenciales para preservar la integridad y la confianza tanto de la administración municipal como de los ciudadanos. La justificación para la implementación de este Plan de Seguridad y Privacidad de la Información se fundamenta en los siguientes puntos clave:

Protección de la Información Sensible: En la gestión diaria, el municipio maneja información confidencial y sensible, incluyendo datos personales de los ciudadanos y detalles administrativos. La implementación de medidas de seguridad garantizará la protección de esta información contra amenazas internas y e*x*ternas.

Cumplimiento de Regulaciones y Normativas: La existencia de regulaciones y leyes específicas relacionadas con la privacidad y seguridad de la información exige que el municipio implemente medidas claras y efectivas. Cumplir con estas normativas no solo es

un requisito legal, sino también una muestra de compromiso con la protección de los derechos de privacidad de los ciudadanos.

Amenazas Cibernéticas en Evolución: El aumento constante de amenazas cibernéticas, como malware, ransomware (secuestro de datos) y ataques dirigidos, implica la necesidad de fortalecer las defensas para prevenir intrusiones y proteger la infraestructura tecnológica municipal.

Construcción de Confianza Ciudadana: La seguridad y privacidad de la información son fundamentales para construir y mantener la confianza de la comunidad. Los ciudadanos deben tener la seguridad de que la información que comparten con el municipio se manejará de manera segura y ética.

Respaldo de la Continuidad Operativa: Un enfoque integral en seguridad de la información contribuye directamente a la continuidad operativa. La prevención de incidentes y la rápida recuperación frente a posibles brechas garantizan la continuidad de los servicios municipales sin interrupciones significativas.

Inversión Responsable de Recursos: La implementación de medidas de seguridad y privacidad de la información representa una inversión responsable de los recursos municipales. Evitar posibles incidentes de seguridad ayuda a evitar costos asociados con la recuperación y reparación de sistemas afectados.

Fomento de una Cultura de Concientización: Al establecer un plan de seguridad y privacidad de la información, se fomenta una cultura de concientización y responsabilidad entre los empleados municipales. La capacitación y la educación continua son elementos clave para fortalecer las defensas contra amenazas internas.

Adaptación a un Entorno Tecnológico Cambiante: La rápida evolución tecnológica y las cambiantes amenazas en línea requieren una estrategia de seguridad dinámica. Este plan permitirá al municipio adaptarse eficientemente a los cambios y mitigar nuevas amenazas a medida que surgen.

En conjunto, estas justificaciones resaltan la importancia de establecer una sólida infraestructura de seguridad y privacidad de la información para garantizar la protección, integridad y disponibilidad de los datos municipales en el entorno digital actual. Este plan no solo se erige como un escudo protector, sino como un compromiso fundamental con la transparencia, la confianza y la eficiencia en la administración municipal.

3 ALCANCE

El Alcance del Plan de Seguridad y Privacidad de la Información buscando una alta adopción del El Modelo de Seguridad y Privacidad de la Información (MSPI) para el Municipio abarca de manera integral todas las dimensiones y aspectos críticos relacionados con la protección de la información y la preservación de la privacidad en el entorno municipal. Este plan se centra en las siguientes áreas clave:

Gestión de Riesgos:

- Identificación y evaluación de riesgos asociados con la información confidencial y datos sensibles del municipio.
- Desarrollo de estrategias para mitigar, transferir o aceptar los riesgos identificados.

Protección de Datos Personales:

- Implementación de medidas específicas para garantizar la privacidad y seguridad de los datos personales manejados por el municipio.
- Cumplimiento de regulaciones y normativas relacionadas con la protección de datos personales.

Seguridad de la Infraestructura Tecnológica:

- Evaluación y fortalecimiento de la infraestructura tecnológica para prevenir accesos no autorizados y ataques cibernéticos.
- Implementación de controles de acceso, cifrado de datos y firewalls para proteger la integridad y confidencialidad de la información

Gestión de Acceso y Control de Identidad:

- Establecimiento de un sistema de gestión de accesos que garantice que los usuarios solo tengan acceso a la información necesaria para sus funciones.
- Implementación de controles de identidad robustos y autenticación multifactor para fortalecer la seguridad.

Prevención de Amenazas Cibernéticas:

- Implementación de herramientas y políticas para prevenir y detectar amenazas cibernéticas, incluyendo malware, ransomware (secuestro de datos) y ataques dirigidos.
- Respuesta inmediata ante incidentes de seguridad para minimizar el impacto.

Formación y Concientización:

- Desarrollo de programas de formación y concientización en seguridad de la información para todos los empleados municipales.
- Promoción de una cultura de seguridad que fomente prácticas seguras y la rápida identificación de posibles amenazas.

Gestión de Incidentes:

- Establecimiento de procedimientos claros y eficientes para la gestión de incidentes de seguridad.
- Designación de un equipo de respuesta y coordinación con entidades externas en caso de brechas significativas.

Seguridad Física de la Información:

- Evaluación y mejora de la seguridad física de la información almacenada en dispositivos físicos y centros de datos.
- Implementación de controles de acceso físico y protección contra riesgos ambientales.

Respaldo y Recuperación de Datos:

- Establecimiento de procedimientos robustos de respaldo de datos, asegurando la disponibilidad y recuperación rápida en caso de pérdida de información.
- Pruebas periódicas para verificar la efectividad de los procedimientos de recuperación.

Privacidad en Proyectos y Desarrollos Tecnológicos:

- Integración de principios de privacidad desde la concepción en proyectos y desarrollos tecnológicos.
- Evaluación de impacto en la privacidad antes de la implementación de nuevas tecnologías.

Cumplimiento Legal y Normativo:

- Aseguramiento de que el plan cumple con todas las regulaciones y normativas locales y nacionales en materia de seguridad y privacidad de la información.
- Monitoreo continuo de cambios en regulaciones y ajuste del plan en consecuencia.

Este alcance aborda de manera exhaustiva la seguridad y privacidad de la información en el municipio, asegurando una protección integral y sostenible. Cada área identificada contribuirá a la creación de un entorno confiable y seguro para la información municipal y los ciudadanos.

4 OBJETIVOS

4.1 Objetivo General

Garantizar la seguridad integral y la privacidad de la información manejada por el Municipio, estableciendo un marco robusto y sostenible que proteja la confidencialidad, integridad y disponibilidad de los datos, y que cumpla con las normativas y regulaciones aplicables.

4.2 Objetivos Específicos

Protección Integral de Datos: Asegurar la protección de datos críticos mediante la implementación de medidas técnicas y procedimentales que minimicen los riesgos de pérdida o acceso no autorizado.

Cumplimiento Normativo: Evaluar, adaptar y mantener el plan para garantizar el cumplimiento continuo con las regulaciones y normativas locales y nacionales relacionadas con la seguridad y privacidad de la información.

Cultura de Seguridad: Desarrollar programas de formación y concientización que promuevan una cultura de seguridad, involucrando a todos los empleados en prácticas seguras y conscientes.

Gestión Efectiva de Riesgos: Identificar y gestionar proactivamente los riesgos asociados con la seguridad de la información, implementando estrategias efectivas de mitigación.

Prevención de Amenazas Cibernéticas: Implementar medidas preventivas y de detección para prevenir amenazas cibernéticas, reduciendo la vulnerabilidad de la infraestructura tecnológica.

Seguridad en el Acceso y Control de Identidad: Establecer y fortalecer sistemas de gestión de accesos y controles de identidad para garantizar que el acceso a la información sea autorizado y seguro.

Gestión Efectiva de Incidentes: Establecer procedimientos eficientes para la gestión de incidentes, garantizando respuestas rápidas y coordinadas para minimizar el impacto.

Respaldo y Recuperación de Datos: Establecer procedimientos sólidos de respaldo y recuperación para garantizar la disponibilidad continua y la rápida recuperación de datos críticos.

Integración de Privacidad en Desarrollos Tecnológicos: Incorporar principios de privacidad desde la concepción en proyectos y desarrollos tecnológicos, evaluando su impacto en la privacidad antes de la implementación.

Seguridad Física de la Información: Mejorar la seguridad física de la información almacenada, implementando controles de acceso físico y protección contra riesgos ambientales.

Concientización Ciudadana: Involucrar activamente a la comunidad en iniciativas de concientización sobre seguridad de la información, promoviendo la colaboración y la retroalimentación positiva.

5 DEFINICIÓNES

Información Pública: Definición según la **Ley 1712 de 2014 (Artículo 4) "***Cualquier contenido, documento, dato, material, objeto o información, que sea de propiedad o esté bajo la custodia de una entidad, y que haya sido creada, adquirida, recibida, procesada, poseída o controlada por ella*".

Seguridad de la Información: Definición según **ISO/IEC 27000 "***Preservación de la confidencialidad, integridad y disponibilidad de la información al aplicar un enfoque de gestión de riesgos y dando cumplimiento a los requisitos legales y reglamentarios*".

Gestión de Riesgos de la Seguridad de la Información: Definición según **ISO/IEC 27000 "***Coordinación sistemática y aplicada de actividades para dirigir y controlar una organización con respecto a la seguridad de la información*".

Documento: Definición según la **Ley 594 de 2000 (Artículo 3)** "*Toda expresión que conste en un material susceptible de ser leído o visualizado, como libros, mapas, grabaciones, fotografías, grabaciones audiovisuales, publicaciones en cualquier medio, documentos escritos, manuscritos, textos, planos, planillas, dibujos, croquis, diseños y, en general, cualquier representación de hechos, ideas o conceptos que tenga un soporte físico*".

Privacidad de la Información: Definición según **ISO/IEC 27000 "***La preservación de la confidencialidad, integridad y disponibilidad de la información en el contexto de la privacidad*".

Gestión de Identidad y Accesos: Definición según **ISO/IEC 27000 "***La gestión de identidades y accesos asegura que solo personas autorizadas tengan acceso a la información y que los sistemas validen y autentiquen adecuadamente a los usuarios*".

Política de Seguridad de la Información: Definición según **ISO/IEC 27001 "***Documento que proporciona una declaración formal de la intención y dirección de la alta dirección con respecto a la seguridad de la información*".

La **seguridad y privacidad de la información** constituyen un conjunto de principios, procesos y medidas diseñadas para preservar la confidencialidad, integridad y disponibilidad de los datos. Este enfoque, respaldado por normativas como la Ley 1712 de 2014 y estándares como ISO/IEC 27000, busca garantizar que la información, ya sea pública o privada, sea manejada de manera segura y conforme a los requisitos legales. Incluye la gestión de riesgos, la protección contra amenazas cibernéticas, la preservación de la privacidad en el manejo de datos personales, y la implementación de controles que aseguren un acceso autorizado y seguro a la información. Este marco integral se orienta a fortalecer la confianza, eficiencia y responsabilidad en el tratamiento de la información, tanto en el ámbito público como privado.

6 ANÁLISIS DE LA SITUACIÓN ACTUAL

La Alcaldía Municipal de California completó el proceso de cumplimentar la "Herramienta de Diagnóstico", conocida como "INSTRUMENTO DE IDENTIFICACIÓN DE LA LÍNEA BASE DE SEGURIDAD", proporcionada por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC). Este instrumento tiene como objetivo evaluar el grado de progreso en la planificación y desarrollo del Modelo de Privacidad y Seguridad de la Información, fundamentado en la normativa de seguridad informática ISO 27001.

La realización de este proceso permite a la entidad obtener una evaluación integral de sus puntos fuertes y áreas de mejora. Utilizando como referencia la ISO 27001, que establece estándares para la seguridad de la información, la Alcaldía puede identificar de manera detallada tanto las deficiencias como los aspectos positivos. Este análisis proporciona una visión directa de los recursos tecnológicos y humanos que se deben asignar para elevar la calidad de los procesos tecnológicos. El objetivo final es prevenir posibles filtraciones de información y garantizar la preservación óptima de la misma en la entidad.

7 MARCO NORMATIVO

Este plan se enmarca dentro de una amplia gama de legislaciones y normativas que salvaguardan la seguridad y privacidad de la información, asegurando el cumplimiento de estándares rigurosos y la protección de los derechos asociados. A continuación, se detallan un conjunto adicional de leyes y regulaciones que contribuyen al respaldo normativo del presente plan:

Ley 1437 de 2011, Capítulo IV, "utilización de medios electrónicos en el procedimiento administrativo". "*Los procedimientos y trámites administrativos podrán realizarse a través de medios electrónicos. Para garantizar la igualdad de acceso a la administración, la autoridad deberá asegurar mecanismos suficientes y adecuados de acceso gratuito a los medios electrónicos, o permitir el uso alternativo de otros procedimientos*".

Ley 1581 de 2012, Principio de seguridad "*La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento*".

Ley 1581 de 2012, Artículo 17, ítem d "*Conservar al información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento*".

Ley 1712 de 2014 Articulo 3, "principio de transparencia"' "*Principio conforme la cual toda la información en poder de los sujetos obligados definidos en esta ley se presume pública, en consecuencia, de lo cual dichos sujetos están en el deber de proporcionar y facilitar el acceso a la misma en los términos más amplios posibles y a través de los medios y procedimientos que al efecto establezca la ley, excluyendo solo aquello que esté sujeto a*

las excepciones constitucionales y legales y bajo el cumplimiento de los requisitos establecidos en esta ley".

Ley 1712 de 2014, artículo 7, "Disponibilidad de la información" "*En virtud de los principios señalados, deberá estar a disposición del público la información a la que hace referencia la presente ley, a través de medios físicos, remotos o locales de comunicación electrónica. Los sujetos obligados deberán tener a disposición de las personas interesadas dicha información en la web, a fin de que estas puedan obtener la información, de manera directa o mediante impresiones. Asimismo, estos deberán proporcionar apoyo a los usuarios que lo requieran y proveer todo tipo de asistencia respecto de los trámites y servicios que presten*".

Ley 1712 de 2014 -Título III, Articulo 18 "Excepciones acceso a la información "*Información exceptuada por daño de derechos a personas naturales o jurídicas. Es toda aquella información pública clasificada, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito*".

Decreto 2573 de 2014 "*Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea*" donde se encuentra como componente el modelo de Seguridad y Privacidad de la Información.

Decreto 1413 de 2017, artículo 2.2.17.6.6, "Seguridad de la información." "*Los actores que traten información, en el marco del presente título, deberán adoptar medidas apropiadas, efectivas y verificables de seguridad que le permitan demostrar el correcto cumplimiento de las buenas prácticas consignadas en el modelo de seguridad y privacidad de la información emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones, o un sistema de gestión de seguridad de la información certificable. Esto con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información*".

Decreto 1413 de 2017, artículo 2.2.17.6.1, "responsable y encargado del tratamiento": "*Los operadores de servicios ciudadanos digitales serán responsables del tratamiento de los datos personales que los ciudadanos el suministren directamente y encargados del tratamiento respecto de los datos que otras entidades le proporcionen*".

Decreto 1413 de 2017, artículo 2.2.17.6.3. Responsabilidad demostrada y programa integral de gestión de datos. los operadores de servicios ciudadanos digitales deberán adoptar medidas apropiadas, efectivas y verificables que le permitan demostrar el correcto cumplimiento de las normas sobre tratamiento de datos personales. Para el efecto, deben crear e implementar un Programa Integral de Gestión de Datos (PIGD), como mecanismo operativo para garantizar el debido tratamiento de los datos personales.

Decreto 1413 de 2007, artículo 2.2.17.6.5, "Privacidad por diseño y por defecto" "*Los operadores de servicios ciudadanos digitales deberán atender las buenas prácticas y principios desarrollados en el ámbito internacional en relación con la protección y tratamiento de personales que adicionales a la Accountability, y que se refieren al Privacy by design (PbD) y Privacy Impact Assessment (PIA), cuyo objetivo se dirige a que la*

protección de la privacidad y de los datos no puede ser asegurada únicamente a través del cumplimiento de la normativa, sino que debe ser un 'modo de operar de las organizaciones, y aplicarlo a los sistemas de información, modelos, prácticas de negocio, diseño físico, infraestructura e interoperabilidad, que permita garantizarla privacidad al ciudadano y a las empresas en relación con la recolección, uso, almacenamiento, divulgación y disposición de los mensajes de datos para los servicios ciudadanos digitales gestionados por el operador".

Decreto 1413 de 2017, artículo 2.2.17.5.10, "*Derechos de los usuarios de los servicios ciudadanos digitales*" tendrán derecho a:

1. *"Registrarse de manera gratuita eligiendo al operador de servicios ciudadanos digitales de su preferencia entre aquellos que estén vinculados por el articulador".*
2. *"Aceptar, actualizar y revocarlas autorizaciones para recibir información, comunicaciones y notificaciones electrónicas desde las entidades públicas a su elección a través de los servicios ciudadanos digitales".*
3. *"Hacer uso responsable de los servicios ciudadanos digitales a los cuáles se registre".*
4. *"Interponer peticiones, quejas, reclamos y solicitudes de información en relación con la prestación a los servicios ciudadanos digitales".*
5. *"Elegir y cambiar libremente el operador de servicios ciudadanos digitales".*
6. *"Solicitar en cualquier momento, y a través de cualquiera de los medios de atención al usuario, su retiro de la plataforma de servicios en· cuyo caso podrá descargar su información a un medio de almacenamiento propio".*

Decreto 1413 de 2017, artículo 2.2.17.2.1.1 "*Descripción de los servicios ciudadanos digitales, 1.5. servicio de interoperabilidad Cualquier desarrollo en el marco de los servicios ciudadanos digitales especiales deberá hacer uso de o estar soportado en los servicios ciudadanos digitales básicas cuando lo requieran*".

Decreto 612 de 2018, artículo 1 "Integración de planes institucionales y estratégico. Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web."

Conpes 3854 de 2016, Objetivo general "*Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, un marco de cooperación, colaboración y asistencia*."

Con el objetivo de potenciar el desarrollo de la economía digital a nivel nacional, lo que, a su vez, se traducirá en un impulso para la prosperidad económica y social en el país, la Alcaldía se encuentra comprometida con emprender acciones estratégicas. Estas acciones están orientadas hacia la salvaguarda de la información que gestiona, requiriendo la identificación y el tratamiento de los riesgos asociados a los activos críticos que sustentan sus operaciones.

En este contexto, se establecen y ejecutan acciones específicas en consonancia con el plan de acción y el Sistema Integrado de Gestión. Este enfoque proactivo busca no solo mitigar riesgos potenciales sino también garantizar la integridad, confidencialidad y disponibilidad de la información. Al adoptar un marco de gestión de riesgos de la información, la Alcaldía busca fortalecer sus procesos y procedimientos, asegurando la resiliencia de sus activos digitales frente a posibles amenazas.

El propósito fundamental de estas iniciativas es crear un entorno seguro y confiable para la gestión de la información, lo que a su vez contribuirá al florecimiento de la economía digital a nivel local. Además, se busca mantener un equilibrio entre la facilitación del acceso a los servicios digitales y la implementación de medidas robustas de seguridad, garantizando así la confianza de los ciudadanos y usuarios en las plataformas y servicios digitales proporcionados por la Alcaldía.

Decreto 1008 del 2018. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1del título 9 de al parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

8 FASES PARA IMPLEMENTAR E INSTRUMENTAR MSPI.

8.1 Preparación y Planificación:

- Objetivos:
- Definir los objetivos específicos del MSPI.
- Identificar los recursos necesarios.
- Establecer un equipo de trabajo y roles.
- Realizar un análisis inicial de riesgos y vulnerabilidades.
- Incluir la preparación para la transición a IPv6, tanto a nivel de infraestructura como en la página web de la alcaldía.
- Identificar indicadores clave de gestión (KPIs) relacionados con la página web y la seguridad informática.
- Evaluar la integración con el Sistema de Gestión Documental (SGD) y sus implicaciones en la página web.

8.2 Diagnóstico y Evaluación:

- Objetivos:
- Evaluar la situación actual de la seguridad y privacidad de la información.
- Identificar activos críticos y datos sensibles.
- Realizar un análisis de riesgos detallado.
- Evaluar el cumplimiento normativo y legal.
- Evaluar la infraestructura actual de IPv4 y preparar el terreno para IPv6, considerando la página web de la alcaldía.
- Analizar la documentación existente en el SGD relacionada con la página web.

8.3 Diseño del MSPI:

- Objetivos:
- Desarrollar políticas y procedimientos de seguridad.
- Definir controles de seguridad específicos.
- Diseñar el marco organizativo del MSPI.
- Identificar métricas y KPIs para la evaluación del MSPI y la página web.
- Incluir diseño y políticas para la transición IPv4 a IPv6, considerando la página web.
- Integrar políticas de gestión documental en el MSPI, con enfoque en la página web.

8.4 Implementación y Despliegue:

- Objetivos:
- Introducir las políticas y procedimientos.
- Implementar controles técnicos y organizativos.
- Realizar capacitación y concienciación del personal.
- Desplegar tecnologías de seguridad, como firewalls, cifrado, etc.
- Iniciar el proceso de transición a IPv6, implementando cambios en la página web.
- Integrar indicadores de gestión en los procesos, particularmente aquellos relacionados con la página web.

8.5 Monitoreo y Evaluación Continua:

- Objetivos:
- Establecer un sistema de monitoreo constante.
- Realizar auditorías y revisiones periódicas.
- Evaluar la eficacia de los controles implementados.
- Actualizar el MSPI según sea necesario.
- Monitorear y gestionar la transición IPv4 a IPv6, con especial atención a la página web.
- Evaluar la efectividad de la gestión documental en el SGD, centrada en la documentación web.

8.6 Gestión de Incidentes y Respuesta:

- Objetivos:
- Desarrollar un plan de respuesta a incidentes.
- Establecer un equipo de respuesta.
- Realizar simulacros de respuesta a incidentes.
- Mejorar el MSPI en base a lecciones aprendidas.
- Integrar la gestión de incidentes en la transición IPv4 a IPv6, considerando la página web.
- Mejorar la gestión documental en respuesta a incidentes, particularmente en documentos web.

8.7 Mejora Continua:

- Objetivos:
- Evaluar las tendencias y desarrollos en seguridad y privacidad.
- Incorporar nuevas tecnologías y mejores prácticas.
- Recoger feedback del personal y partes interesadas.
- Ajustar el MSPI según cambios en el entorno operativo.
- Optimizar la transición a IPv6 en base a experiencias anteriores, centrándose en la página web.
- Mejorar la gestión documental según los resultados de auditorías, especialmente en documentos vinculados a la página web.

Estas fases detallan la implementación de IPv6, la integración de indicadores de gestión y la conexión efectiva del MSPI con el Sistema de Gestión Documental, con un enfoque específico en la página web de la alcaldía. Cada fase se entrelaza para proporcionar una implementación coherente y eficiente.

9 ADOPCIÓN DEL PROTOCOLO IPV6

La adopción del Protocolo IPv6 para la página web de la alcaldía es un proceso crucial para garantizar la continuidad y la eficiencia de las operaciones en un entorno digital en constante evolución. Aquí te presento un enfoque paso a paso para la adopción de IPv6:

9.1 Evaluación de la Infraestructura Actual:

- Realiza una auditoría de la infraestructura de red actual de la alcaldía para determinar la compatibilidad con IPv6.
- Identifica los equipos, servicios y aplicaciones que necesitan ser actualizados o modificados para admitir IPv6.
- Evalúa la capacidad de los proveedores de servicios de Internet y los proveedores de alojamiento web para brindar soporte IPv6.

9.2 Desarrollo de un Plan de Transición a IPv6:

- Establece un plan detallado que incluya los pasos específicos para la transición de IPv4 a IPv6.
- Define un cronograma que considere la minimización de tiempos de inactividad y el impacto mínimo en los usuarios finales.
- Incluye una estrategia de comunicación para informar a los usuarios y partes interesadas sobre los cambios planificados.

9.3 Capacitación del Personal:

- Proporciona capacitación al personal de TI y a otros departamentos relevantes sobre los conceptos y procedimientos asociados con IPv6.

- Asegúrate de que el personal sea consciente de las diferencias clave entre IPv4 e IPv6 y cómo gestionar la red en el nuevo entorno.

9.4 Configuración de Equipos y Dispositivos:

- Configura los routers, firewalls y otros dispositivos de red para admitir IPv6.
- Asegúrate de que los servidores web, bases de datos y otros servicios en línea estén listos para IPv6.
- Actualiza o reemplaza hardware y software obsoleto que no sea compatible con IPv6.

9.5 Pruebas Exhaustivas:

- Realiza pruebas exhaustivas en un entorno de prueba para garantizar que todos los sistemas y servicios funcionen correctamente con IPv6.
- Identifica y resuelve cualquier problema de interoperabilidad antes de implementar la transición a nivel de producción.

9.6 Implementación Gradual:

- Adopta un enfoque gradual para la implementación de IPv6, comenzando con segmentos de red o servicios específicos.
- Supervisa de cerca el rendimiento durante cada fase de implementación para abordar cualquier problema de manera proactiva.

9.7 Monitoreo Continuo:

- Establece un sistema de monitoreo continuo para supervisar el tráfico IPv6 y detectar posibles problemas.
- Implementa herramientas de monitoreo de red que admitan IPv6 y que permitan la visibilidad completa de la red.

9.8 Optimización y Mejora Continua:

- Realiza ajustes y optimizaciones según sea necesario después de la implementación.
- Recoge comentarios de usuarios y realiza mejoras continuas en la infraestructura IPv6.
- Mantén actualizadas las políticas y procedimientos relacionados con IPv6.

La adopción de IPv6 para la página web de la alcaldía debe ser un proceso cuidadosamente planificado y ejecutado para garantizar una transición suave y efectiva. Este enfoque paso a paso debería ayudar a abordar los desafíos comunes asociados con la migración a IPv6.

10 PLAN DE COMUNICACIONES

El plan de comunicaciones es esencial para asegurar una transición suave y efectiva durante la implementación de iniciativas como la adopción del Protocolo IPv6 para la página

web de la alcaldía. Aquí te proporciono un esquema para desarrollar un plan de comunicaciones sólido:

10.1 Objetivos del Plan de Comunicaciones:

10.1.1 Difusión a funcionarios

Informar a todos los funcionarios de la administración sobre el nuevo Plan de Seguridad y Privacidad de la Información.

10.2 Estrategias de Comunicación:

10.2.1 Portal Web Territorial:

- Publicar el plan en el canal de transparencia y acceso a la información en el Portal Web Territorial.
- Garantizar accesibilidad para que todos los usuarios, internos y externos, puedan revisar el documento.

10.2.2 Correo Electrónico:

- Enviar una comunicación oficial a través del correo electrónico a todos los funcionarios de la entidad.
- Incluir enlaces directos al documento y proporcionar instrucciones claras sobre su implementación.

10.3 Mensajes Clave:

10.3.1 Compromiso con la Transparencia:

- Resaltar el compromiso de la alcaldía con la transparencia al compartir el plan a través del Portal Web Territorial.

10.3.2 Accesibilidad para Todos:

- Asegurar que el plan esté al alcance de todos, tanto internos como externos, a través del portal web.

10.3.3 Implementación Integral:

- Enfatizar la importancia de que todos los funcionarios conozcan y sigan las directrices establecidas en el plan.

10.4 Evaluación y Retroalimentación:

10.4.1 Seguimiento en el Portal Web:

- Monitorear la frecuencia de acceso al plan a través del Portal Web Territorial.
- Analizar cualquier retroalimentación o preguntas de los usuarios externos.

10.4.2 Confirmación de Lectura:

- Solicitar confirmación de lectura a los funcionarios a través del correo electrónico.
- Establecer un canal para preguntas y comentarios adicionales.

Este plan asegura una amplia difusión del Plan de Seguridad y Privacidad de la Información, utilizando medios accesibles y canales efectivos para garantizar la comprensión y la implementación adecuada por parte de todos los involucrados.

11 CRONOGRAMA ANUAL PARA LA EJECUCIÓN DEL MSPI

Año: 2026

Preparación y Planificación (Febrero - Abril):

- Sesiones de planificación con el equipo y identificación de recursos (Febrero).
- Análisis inicial de riesgos y preparación para IPv6 (Marzo).
- Definición de objetivos específicos y evaluación de integración con SGD (Abril).

Diagnóstico y Evaluación (Mayo - Julio):

- Evaluación de seguridad y privacidad de la información, identificación de activos críticos (Mayo).
- Análisis de riesgos detallado y evaluación del cumplimiento normativo (Junio).
- Evaluación de la infraestructura IPv4 (Julio).

Diseño del MSPI (Agosto - Octubre):

- Desarrollo de políticas de seguridad y diseño organizativo del MSPI (Agosto).
- Definición de controles de seguridad y diseño de políticas para transición IPv4 a IPv6 (Septiembre).
- Integración de políticas de gestión documental (Octubre).

Implementación y Despliegue (Noviembre - Enero):

- Introducción de políticas y procedimientos, implementación de controles técnicos (Noviembre).
- Capacitación y concienciación del personal, despliegue de tecnologías de seguridad (Diciembre).

- Inicio del proceso de transición a IPv6 (Enero).

Monitoreo y Evaluación Continua (Febrero - Abril del siguiente año):

- Establecimiento de sistema de monitoreo y gestión de la transición IPv4 a IPv6 (Febrero).
- Auditorías y revisiones periódicas, evaluación de la eficacia de los controles (Marzo).
- Monitoreo continuo y ajuste según sea necesario (Abril).

Gestión de Incidentes y Respuesta (Mayo - Julio):

- Desarrollo del plan de respuesta a incidentes y establecimiento de equipo de respuesta (Mayo).
- Simulacros de respuesta a incidentes y mejora del MSPI en base a lecciones aprendidas (Junio).
- Integración de gestión de incidentes en la transición IPv4 a IPv6 (Julio).

Mejora Continua (Agosto - Octubre):

- Evaluación de tendencias y desarrollos, incorporación de nuevas tecnologías (Agosto).
- Recolección de feedback del personal, ajuste del MSPI según cambios (Septiembre).
- Optimización de la transición a IPv6 y mejora de la gestión documental según auditorías (Octubre).

Este plan de implementación del MSPI para la Alcaldía presenta una estrategia sólida y práctica, adaptada a las necesidades específicas del entorno municipal. La rapidez y la eficiencia del plan están alineadas con la dinámica operativa de la alcaldía, abordando de manera integral la seguridad de la información y la transición a IPv6.

Es crucial destacar la importancia de la participación activa del personal municipal en todo el proceso. La capacitación y concienciación del personal, así como la retroalimentación continua, son aspectos esenciales para garantizar una transición fluida y la adopción efectiva de las nuevas políticas y tecnologías de seguridad.

Se firma en el Municipio de California, Santander a los veintisiete (27) días del mes de enero de 2026.

DANILO VALBUENA PABÓN
ALCALDE MUNICIPAL

Realizó: Gerardo Arias Garcia – Secretario General y de Gobierno