

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN



**ALCALDÍA MUNICIPAL
SAN BERNARDO DEL VIENTO**



sanbernardodelviento-cordoba.gov.co



Introducción

La información institucional constituye un activo estratégico para la Alcaldía Municipal de San Bernardo del Viento, en tanto soporta la planeación, la toma de decisiones, la ejecución de los procesos misionales, la prestación de servicios a la ciudadanía y el cumplimiento de las funciones constitucionales y legales del municipio. Esta información se origina y gestiona a partir de múltiples fuentes y sistemas, apoyados en infraestructuras tecnológicas diversas, lo cual exige la adopción de medidas adecuadas que garanticen su protección durante todo su ciclo de vida, el crecimiento de los servicios digitales, la implementación de trámites en línea, la interoperabilidad con entidades del orden departamental y nacional, así como el uso intensivo de tecnologías de la información y las comunicaciones, han incrementado la exposición a riesgos asociados a la pérdida, alteración, indisponibilidad o uso no autorizado de la información. En este contexto, la seguridad y privacidad de la información se consolidan como un componente transversal de la gestión institucional y un factor clave para la continuidad de la operación, la transparencia administrativa y la confianza ciudadana; en concordancia con lo anterior, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), mediante el artículo 7 de la Resolución 4870 de 2023, estableció la relevancia de integrar de manera articulada los modelos y sistemas de gestión de las entidades públicas, con el fin de garantizar su sostenibilidad, coherencia y mejora continua. Dicho marco resalta la necesidad de alinear los sistemas de gestión con el Modelo Integrado de Gestión y con las políticas de Gestión y Desempeño Institucional del MIPG, entre ellas la Política de Gobierno Digital, de la cual la seguridad y privacidad de la información es un habilitador fundamental, en este sentido, el proceso de Seguridad y Privacidad de la Información se enmarca dentro de los lineamientos de la Política de Gobierno Digital, de conformidad con lo dispuesto en el artículo 2.2.9.1.2.1 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector TIC, el cual establece la obligación de los sujetos obligados de desarrollar capacidades institucionales mediante la implementación de lineamientos de seguridad y privacidad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructuras tecnológicas y activos de información, con el propósito de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.



República de Colombia
Departamento de Córdoba
Alcaldía de San Bernardo del Viento

Nit:800096804-9

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Así mismo, el Decreto 2106 de 2019 dispone que las entidades que realicen trámites y procedimientos por medios digitales deben contar con sistemas de gestión documental electrónica y archivo digital, garantizando la integridad, disponibilidad, autenticidad y conservación de la información, lo que refuerza la necesidad de adoptar una estrategia de seguridad digital alineada con los lineamientos emitidos por el MinTIC. De igual forma, la Resolución 0500 de 2021 establece los lineamientos y estándares para la Estrategia de Seguridad Digital y adopta el Modelo de Seguridad y Privacidad de la Información (MSPI) como habilitador de la Política de Gobierno Digital, señalando que las entidades obligadas deben definir e implementar los lineamientos para la gestión de riesgos de seguridad de la información y el procedimiento para la atención de incidentes de seguridad digital además en cumplimiento de lo dispuesto en el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, y particularmente de lo establecido en el artículo 2.2.22.3.14, el Plan de Seguridad y Privacidad de la Información se integra al Plan de Acción institucional de la Alcaldía Municipal de San Bernardo del Viento, asegurando su articulación con la planeación estratégica, el Sistema Integrado de Gestión y la gestión del riesgo institucional por todo lo anterior el presente Plan define los lineamientos, políticas, roles, responsabilidades y controles necesarios para la implementación de un enfoque preventivo y basado en riesgos, alineado con el MSPI y las mejores prácticas en seguridad de la información, considerando las capacidades tecnológicas actuales y el contexto territorial del municipio. De esta manera, la Alcaldía reafirma su compromiso con la protección de la información institucional, la continuidad de los servicios, la seguridad digital y el fortalecimiento de la confianza de los ciudadanos.





República de Colombia
Departamento de Córdoba
Alcaldía de San Bernardo del Viento

Nit:800096804-9

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. <u>Objetivo</u>	Pág. 5
2. <u>Alcance</u>	Pág. 6
3. <u>Normatividad</u>	Pág. 7
4. <u>Documentos asociados</u>	Pág. 10
5. <u>Estados actuales del Sistema de Gestión de Seguridad y Privacidad de la Información</u>	Pág. 11
6. <u>Desarrollo</u>	Pág. 19
1.1. <u>Proceso de seguridad y privacidad de la información</u>	Pág. 19
1.2. <u>Política general de seguridad y privacidad de la información y seguridad digital y continuidad de los servicios del ministerio/fondo de tecnologías de la información y las comunicaciones</u>	Pág. 25
1.3. <u>Objetivos específicos de la política de seguridad y privacidad de la información y seguridad digital y continuidad de los servicios del ministerio/fondo único de tecnologías de la información y las comunicaciones</u>	Pág. 26
1.4. <u>Alcance del sistema de gestión de seguridad y privacidad de la información</u>	Pág. 28
1.5. <u>Ámbito de aplicación</u>	Pág. 28
1.6. Estrategias y modelo de operación por gestiones del sistema de gestión de seguridad y privacidad de la información – SGSPI. –pág. 30	
1.7. Portafolio de proyectos / actividades	Pág. 30
1.8. <u>Plan de implementación del modelo de seguridad y privacidad de la información</u>	Pág. 32
1.9. <u>Análisis presupuestal</u>	Pág. 34
2. <u>Control de cambios</u>	pág. 35





República de Colombia
Departamento de Córdoba
Alcaldía de San Bernardo del Viento

Nit:800096804-9

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Objetivo

Definir e implementar, en la Alcaldía Municipal de San Bernardo del Viento, los mecanismos y controles requeridos por el Modelo de Seguridad y Privacidad de la Información (MSPI) de la Política de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, que permitan proteger los activos de información y los recursos tecnológicos de la entidad frente a amenazas internas y externas, garantizando la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información, así como la continuidad de la operación de los servicios institucionales.





Alcance

El presente Plan de Seguridad y Privacidad de la Información 2024–2027 aplica a todo el modelo de operación por procesos de la Alcaldía Municipal de San Bernardo del Viento, abarcando los procesos estratégicos, misionales, de apoyo y de evaluación, en cumplimiento de lo establecido en el Decreto 1083 de 2015, el Decreto 1078 de 2015 en lo relacionado con la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información (MSPI) adoptado mediante la Resolución 0500 de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, alineado con las buenas prácticas de la NTC/IEC ISO 27001, y articulado con el Sistema Integrado de Gestión y el Plan de Desarrollo Municipal 2024–2027 *“Todo por mi pueblo”*, con el propósito de gestionar de manera integral los riesgos de seguridad y privacidad de la información y seguridad digital, integrar buenas prácticas en los procesos institucionales, apoyar la toma de decisiones, prevenir incidentes de seguridad y asegurar la continuidad de la operación y el logro de los objetivos estratégicos del municipio.



Normatividad

Norma	Descripción
Constitución Política de Colombia (Arts. 15, 20, 23 y 74)	Reconoce los derechos fundamentales a la intimidad, habeas data, acceso a la información pública, libertad de expresión y derecho de petición.
Ley 23 de 1982	Establece el régimen general de derechos de autor en Colombia.
Ley 44 de 1993	Modifica y complementa la Ley 23 de 1982 en materia de derechos de autor y derechos conexos.
Decisión Andina 351 de 1993	Régimen común sobre derechos de autor y derechos conexos en la Comunidad Andina.
Ley 527 de 1999	Regula el uso de mensajes de datos, comercio electrónico y firmas digitales.
Ley 594 de 2000	Regula la función archivística del Estado y la gestión documental.
Ley 850 de 2003	Reglamenta las veedurías ciudadanas como mecanismo de control social.
Ley 962 de 2005	Establece medidas para la racionalización de trámites y procedimientos administrativos.
Ley 1221 de 2008	Regula y promueve el teletrabajo en Colombia.
Ley 1266 de 2008	Regula el habeas data financiera, crediticia y comercial.
Ley 1273 de 2009	Crea el delito de protección de la información y los datos en el Código Penal.
Ley 1341 de 2009	Define los principios de la sociedad de la información y la organización de las TIC.
Ley 1437 de 2011	Expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
Ley 1474 de 2011	Establece medidas para prevenir y sancionar actos de corrupción.
Ley 1581 de 2012	Define el régimen general de protección de datos personales.
Ley 2088 de 2021	Regula el trabajo en casa en Colombia.
Ley 1712 de 2014	Establece la Ley de Transparencia y Acceso a la Información Pública.
Ley 1755 de 2015	Regula el Derecho Fundamental de Petición.
Ley 1915 de 2018	Actualiza el régimen de derechos de autor y derechos conexos.
Ley 2052 de 2020	Expide el Código General Disciplinario.
Decreto 2364 de 2012	Reglamenta la firma electrónica.
Decreto 2609 de 2012	Reglamenta la gestión documental en las entidades públicas.



República de Colombia
Departamento de Córdoba
Alcaldía de San Bernardo del Viento

Nit:800096804-9

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Decreto 884 de 2012	Reglamenta la Ley de Teletrabajo.
Decreto 1377 de 2013	Reglamenta parcialmente la Ley 1581 de 2012.
Decreto 886 de 2014	Reglamenta el Registro Nacional de Bases de Datos.
Decreto 1078 de 2015	Decreto Único Reglamentario del sector TIC; base de la Política de Gobierno Digital.
Decreto 1081 de 2015	Decreto Reglamentario del sector Presidencia.
Decreto 103 de 2015	Reglamenta parcialmente la Ley de Transparencia.
Decreto 1068 de 2015	Decreto Único Reglamentario del sector Hacienda.
Decreto 1074 de 2015	Reglamenta la protección de datos personales en el sector comercio.
Decreto 1499 de 2017	Integra el Modelo Integrado de Planeación y Gestión – MIPG.
Decreto 728 de 2017	Fortalece el acceso público a internet y el Gobierno Digital.
Decreto 1008 de 2018	Establece los lineamientos de la Política de Gobierno Digital.
Decreto 612 de 2018	Integra los planes institucionales al Plan de Acción.
Decreto 2106 de 2019	Simplifica y racionaliza trámites administrativos.
Decreto 1287 de 2020	Regula la seguridad de documentos firmados durante el trabajo en casa.
Decreto 620 de 2020	Regula los servicios ciudadanos digitales.
Decreto 338 de 2022	Establece la gobernanza de la seguridad digital en el Estado.
Decreto 767 de 2022	Actualiza la Política de Gobierno Digital.
Decreto 88 de 2022	Reglamenta disposiciones sobre trabajo en casa.
Resolución 500 de 2021	Adopta el Modelo de Seguridad y Privacidad de la Información – MSPI.
Resolución 746 de 2022	Fortalece el MSPI y define lineamientos adicionales.
Resolución 1519 de 2020	Define estándares de acceso a la información pública y seguridad digital.
Resolución 924 de 2020	Actualiza la Política de Tratamiento de Datos Personales del MinTIC.
Resolución 0448 de 2022	Actualiza la Política General de Seguridad y Privacidad de la Información del MinTIC.
Resolución 1838 de 2022	Regula modalidades de teletrabajo y desconexión laboral.
CONPES 3701 de 2011	Lineamientos de política para ciberseguridad y ciberdefensa.





República de Colombia
Departamento de Córdoba
Alcaldía de San Bernardo del Viento

Nit:800096804-9

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CONPES 3854 de 2017	Política Nacional de Seguridad Digital.
CONPES 3995 de 2020	Política de Confianza y Seguridad Digital.
CONPES 4069 de 2022	Política Nacional de Ciencia, Tecnología e Innovación 2022–2031.
Manual MIG	Lineamientos del Modelo Integrado de Gestión.
Manual de Políticas de Seguridad y Privacidad de la Información	Define políticas institucionales de protección de la información.
Manual de Lineamientos de Protección de Datos Personales	Establece controles para el tratamiento de datos personales.
MSPI – MinTIC	Modelo base para la gestión de seguridad y privacidad de la información en entidades públicas.





República de Colombia
Departamento de Córdoba
Alcaldía de San Bernardo del Viento

Nit:800096804-9

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Documentos asociados

1. MIG-TIC-MC-001 Manual del MIG
2. SPI-TIC-MA-001 Manual de Políticas de Seguridad y Privacidad de la Información
3. SPI-TIC-MA-002 Manual de Lineamientos de Seguridad para la Protección y Tratamiento de Datos Personales.
4. Plan de Cambio, Cultura y Apropiación del Sistema Integrado de Gestión.
5. Plan de desarrollo municipal 2024 – 2027 “Todo por mi pueblo”
6. Manual de Gobierno Digital – MINTIC.





República de Colombia
Departamento de Córdoba
Alcaldía de San Bernardo del Viento
Nit:800096804-9

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Estados actuales del Sistema de Gestión de Seguridad y Privacidad de la Información.

Para la evolución de estado actual es pertinente tener en cuenta el Reporte de Cumplimiento ITA para el Periodo 2024 por lo cual anexamos imagen de la calificación de la alcaldía de San Bernardo del viento.

Informe Consolidado de Resultados

Punt N.II: Puntaje Nivel II			Punt N.I: Puntaje nivel I			Punt Anx: Puntaje Anexo		
Peso N.II: Peso Nivel II			Peso N.I: Peso nivel I			Peso Anx: Peso Anexo		
Subnivel Menú Nivel II	Punt N.II	Peso N.II	Menú – Nivel I	Punt N.I	Peso N.I	Anexo Técnico	Punt Anx.	Peso Anx.
1.1 Directrices de Accesibilidad Web	100	100%	1. Directrices de Accesibilidad Web	100	100%	ANEXO TÉCNICO 1. ACCESIBILIDAD	100	4%
2.1 Top Bar (GOV.CO)	100	6%	2. REQUISITOS SOBRE IDENTIDAD VISUAL Y ARTICULACIÓN CON PORTAL ÚNICO DEL ESTADO COLOMBIANO GOV.CO	100	8%	ANEXO TÉCNICO 2: ESTANDARIZACIÓN DE CONTENIDOS DEL MENÚ DE TRANSPARENCIA	97.9	94%
2.2 Footer o pie de página	100	55%						
2.3 Requisitos mínimos de políticas y cumplimiento legal.	100	22%						
2.4 Requisitos mínimos en menú destacado.	100	17%						
3.1 Misión, visión, funciones y deberes	100	5%	3. INFORMACIÓN DE LA ENTIDAD	85.8	15%			
3.2 Estructura orgánica - organigrama	100	3%						
3.3 Mapas y cartas descriptivas de los procesos	100	3%						
3.4 Directorio Institucional incluyendo sedes, oficinas, sucursales, o regionales, y dependencias	100	13%						
3.5 Directorio de servidores públicos, empleados o contratistas	80	26%						
3.6 Directorio de entidades	0	3%						
3.7 Directorio de agremiaciones, asociaciones y otros grupos de interés	0	3%						
3.8 Servicio al público, normas, formularios y protocolos de atención	100	11%						
3.9 Procedimientos que se siguen para tomar decisiones en las diferentes áreas	100	3%						





República de Colombia
Departamento de Córdoba
Alcaldía de San Bernardo del Viento

Nit:800096804-9

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Subnivel Menú Nivel II	Punt N.II	Peso N.II	Menú – Nivel I	Punt N.I	Peso N.I	Anexo Técnico	Punt Anx.	Peso Anx.
3.10 Mecanismo de presentación directa de solicitudes, quejas y reclamos a disposición del público en relación con acciones u omisiones del sujeto obligado	100	3%	4. NORMATIVA	100	6%			
3.11 Calendario de actividades	100	3%						
3.12 Información sobre decisiones que pueden afectar al público	100	3%						
3.13 Entes y autoridades que lo vigilan	100	18%						
3.14 Publicación de hojas de vida	0	3%						
4.1 Normativa de la entidad o autoridad	100	60%	5. CONTRATACIÓN	100	4%			
4.2 Búsqueda de normas	100	20%						
4.3 Proyectos de normas para comentarios	100	20%						
5.1 Plan Anual de Adquisiciones	100	10%						
5.2 Publicación de la información contractual	100	10%						
5.3 Publicación de la ejecución de los contratos	100	60%	6. PLANEACIÓN	100	12%			
5.4 Manual de contratación, adquisición y/o compras	100	10%						
5.5 Formatos o modelos de contratos o pliegos tipo	100	10%						
6.1 Presupuesto general de ingresos, gastos e inversión	100	4%						
6.2 Ejecución presupuestal	100	4%						
6.3 Plan de Acción	100	27%						
6.4 Proyectos de Inversión	100	4%						
6.5 Informes de empalme	100	4%						
6.6 Información pública y/o relevante	100	4%						
6.7 Informes de gestión, evaluación y auditoría	100	25%						
6.8 Informes de la Oficina de Control Interno	100	7%	7. TRÁMITES	100	3%			
6.9 Informe sobre Defensa Pública y Prevención del Daño Antijurídico	100	4%						
6.10 Informes trimestrales sobre acceso a información, quejas y reclamos	100	17%	8. PARTICIPA	100	18%			
7.1 Trámites	100	100%						
8.1 Descripción General	100	23%	9. DATOS ABIERTOS	100	14%			
8.2 Estructura y Secciones del menú "PARTICIPA"	100	77%						
9.1 Instrumentos de gestión de la información	100	97%	10. INFORMACIÓN ESPECÍFICA PARA GRUPOS DE INTERÉS	100	2%			
9.2 Sección de Datos Abiertos	100	3%						
10.1 Información para Grupos Específicos	100	100%						

Subnivel Menú Nivel II	Punt N.II	Peso N.II	Menú – Nivel I	Punt N.I	Peso N.I	Anexo Técnico	Punt Anx.	Peso Anx.
11.1 Normatividad Especial	100	100%	11. OBLIGACIÓN DE REPORTE DE INFORMACIÓN ESPECÍFICA POR PARTE DE LA ENTIDAD	100	1%			
12.1 Procesos de recaudo de rentas locales	100	27%	12. INFORMACIÓN TRIBUTARIA EN ENTIDADES TERRITORIALES LOCALES	100	5%			
12.2 Tarifas de liquidación del Impuesto de Industria y Comercio (ICA)	100	73%						
13.1 Trámites, Otros Procedimientos Administrativos y consultas de acceso a información pública	100	5%	13. MENÚ "ATENCIÓN Y SERVICIOS A LA CIUDADANÍA"	100	10%			
13.2 Canales de atención y pida una cita	100	9%						
13.3 PQRS	100	86%						
14.1 Sección de Noticias	100	100%	14. SECCIÓN DE NOTICIAS	100	2%			
15.1 Anexo 3. Condiciones de seguridad digital	100	100%	15. ANEXO 3. CONDICIONES TÉCNICAS MINIMAS Y DE SEGURIDAD DIGITAL WEB	100	100%	ANEXO 3. CONDICIONES TÉCNICAS MINIMAS Y DE SEGURIDAD DIGITAL WEB	100	2%





República de Colombia
Departamento de Córdoba
Alcaldía de San Bernardo del Viento

Nit:800096804-9

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

De acuerdo con el autodiagnóstico del Modelo de Seguridad y Privacidad de la Información de la Política Nacional de Gobierno Digital, el porcentaje de efectividad en la implementación de los controles de la Norma NTC/ISO 27001:2022 es de:

Evaluación de Efectividad de controles				
No.	DOMINIO	Calificación Actual	Calificación Objetivo	Nivel de Madurez
A.5	CONTROLES ORGANIZACIONALES	90	100	OPTIMIZADO
A.6	CONTROLES DE PERSONAS	90	100	OPTIMIZADO
A.7	CONTROLES FÍSICOS	95	100	OPTIMIZADO
A.8	CONTROLES TECNOLÓGICOS	90	100	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		91.2	100	OPTIMIZADO



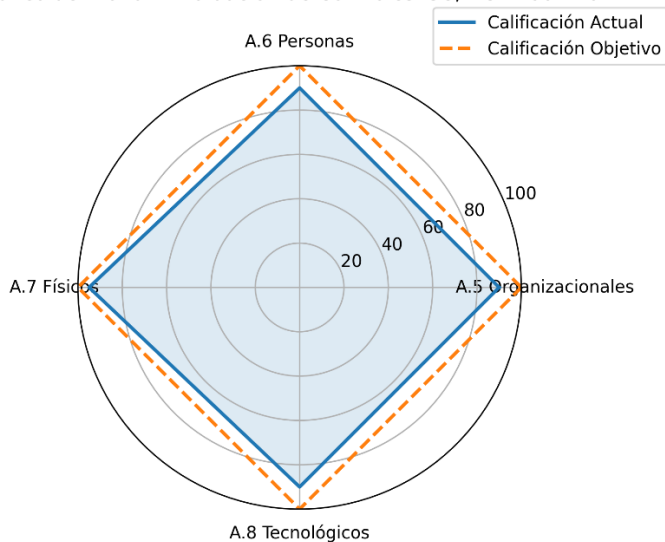


República de Colombia
Departamento de Córdoba
Alcaldía de San Bernardo del Viento

Nit:800096804-9

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Gráfico de Araña - Evaluación de Controles ISO/IEC 27001:2022



Aunque se debe seguir mejorando en muchos aspectos pero estamos caminando por el camino de la adopción e implementación de las políticas de seguridad y privacidad de la información.





ESTRATEGIA DE SEGURIDAD DIGITAL

La Entidad establecerá y adoptará una Estrategia de Seguridad Digital orientada a proteger los activos de información, garantizar la continuidad de la operación y fortalecer la confianza en el uso de los servicios digitales, integrando de manera articulada los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos necesarios para la gestión de la seguridad y privacidad de la información, teniendo como premisa fundamental la implementación, operación y mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI), así como la aplicación de la Guía para la Gestión de Riesgos de Seguridad de la Información y del Procedimiento de Gestión de Incidentes de Seguridad de la Información, conforme a lo establecido en la Resolución 500 de 2021 y demás normas que la modifiquen o sustituyan; esta estrategia se desarrollará de manera transversal, alineada con la Política de Gobierno Digital, el Modelo Integrado de Planeación y Gestión (MIPG) y las buenas prácticas internacionales que permitirán consolidar una estrategia general de seguridad digital orientada a la prevención, detección, respuesta y recuperación frente a los riesgos y amenazas que puedan afectar la confidencialidad, integridad, disponibilidad y privacidad de la información institucional.



República de Colombia
Departamento de Córdoba
Alcaldía de San Bernardo del Viento

Nit:800096804-9

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN



Fig1. Estrategias específicas





PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

A continuación, se describe cada proceso:

Proceso / Gestión	Descripción
Gestión de la Estrategia	Define, orienta y articula la estrategia de seguridad y privacidad de la información de la Alcaldía, asegurando su alineación con los objetivos institucionales, el Plan de Desarrollo, la Política de Gobierno Digital y el MIPG, y promoviendo la mejora continua del SGSPI.
Gestión de Activos de Información	Identifica, clasifica, registra y protege los activos de información de la entidad, estableciendo responsables y controles de acuerdo con su criticidad, con el fin de preservar la confidencialidad, integridad y disponibilidad de la información.
Gestión de Riesgos	Permite identificar, analizar, evaluar y tratar los riesgos asociados a la seguridad y privacidad de la información, priorizando los riesgos críticos y definiendo controles de mitigación y seguimiento conforme a los lineamientos del MSPI y la Función Pública.
Gestión del Cambio y Cultura Organizacional	Fortalece la cultura de seguridad de la información mediante acciones de sensibilización, capacitación y gestión del cambio, promoviendo comportamientos responsables y la apropiación de las políticas y controles del SGSPI.
Gestión de Incidentes de Seguridad de la Información	Establece los lineamientos para la detección, reporte, análisis, atención y cierre de incidentes de seguridad y privacidad, con el propósito de minimizar impactos, garantizar una respuesta oportuna y generar lecciones aprendidas.
Gestión de la Continuidad	Asegura la continuidad de los servicios institucionales y la disponibilidad de la información ante eventos disruptivos, mediante la definición de planes de continuidad, recuperación y pruebas periódicas.
Gestión del Cumplimiento	Garantiza el cumplimiento de la normatividad legal, reglamentaria y técnica relacionada con la seguridad de la información y la protección de datos personales, incluyendo el seguimiento a auditorías y requerimientos de entes de control.
Seguridad de la Información	Proceso transversal que establece políticas, principios y controles para proteger la información institucional frente a accesos no autorizados, alteraciones, pérdidas o divulgaciones indebidas.



República de Colombia
Departamento de Córdoba
Alcaldía de San Bernardo del Viento

Nit:800096804-9

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Privacidad y Protección de Datos Personales	Asegura el adecuado tratamiento de los datos personales, respetando los derechos de los titulares y cumpliendo la normatividad vigente, mediante la gestión de consentimientos y evaluaciones de impacto de privacidad.
Seguridad Digital	Protege los entornos digitales, la infraestructura tecnológica y los sistemas de información frente a amenazas cibernéticas, fortaleciendo la prevención, detección y respuesta a incidentes digitales.
Arquitectura de la Información	Define la estructura, organización y flujo de la información institucional durante todo su ciclo de vida, garantizando coherencia, interoperabilidad y apoyo a la toma de decisiones seguras.
Seguridad de Datos	Implementa controles técnicos y administrativos para proteger los datos institucionales, tales como control de accesos, copias de seguridad, cifrado y mecanismos de integridad.
Transparencia	Garantiza el acceso a la información pública conforme a la normativa vigente, equilibrando los principios de transparencia con los requerimientos de seguridad de la información y protección de datos personales.





Desarrollo.

En cumplimiento de lo establecido en el numeral 2.1.3 del Manual de Gobierno Digital del MINTIC, el Plan de Seguridad y Privacidad de la Información define de manera integral la forma en que se implementará la seguridad y privacidad de la información en todos los procesos de la entidad, estableciendo directrices, actividades, responsables, tiempos y recursos necesarios para garantizar una adecuada gestión, administración, evaluación y control. Su implementación es transversal a los procesos estratégicos, misionales, de apoyo y de evaluación, incorporando la seguridad de la información como un componente permanente del ciclo de vida de los activos de información, con responsabilidades claras para los líderes de proceso y el área de Tecnologías de la Información. Asimismo, el plan contempla la gestión y tratamiento de los riesgos de seguridad y privacidad de la información, así como mecanismos de seguimiento y evaluación periódica que permiten medir la efectividad de los controles, promover la mejora continua y asegurar la protección de la información, la continuidad de la operación y la alineación con los lineamientos del Modelo de Gobierno Digital y los objetivos estratégicos institucionales.

Proceso de seguridad y privacidad de la información

La Alcaldía de San Bernardo del viento adopta el proceso de Seguridad y Privacidad de la Información en el subproceso de Tecnologías de la Información y las comunicaciones en el nivel estratégico el cual permite garantizar continuamente la seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios de TI en la Alcaldía, por medio de la definición de políticas, programas, procedimientos, manuales lineamientos y estrategias.



El proceso de seguridad y privacidad de la información la alcaldía sigue una serie de principios y marcos normativos que buscan proteger la información tanto de los ciudadanos como de la institución. A continuación alguno de los pasos y consideraciones clave que deben tomarse en cuenta para cumplir con las normas de seguridad y privacidad:

1. Cumplimiento con la Ley de Protección de Datos Personales (Ley 1581 de 2012)

La Ley 1581 de 2012 regula la protección de datos personales en Colombia y establece normas claras sobre la recolección, uso, almacenamiento, y circulación de datos personales.

- ✓ Obtener **autorización explícita** de los ciudadanos para recolectar, almacenar y procesar sus datos personales.
- ✓ Cumplir con los **derechos de los titulares** de los datos, como el derecho a conocer, actualizar y rectificar la información personal.
- ✓ Registrar las bases de datos en la **Superintendencia de Industria y Comercio (SIC)**.

Políticas y Normativas Internas

La Alcaldía debe desarrollar e implementar **políticas internas de seguridad y privacidad** para proteger la información. Estas políticas deben cubrir:

- ✓ **Clasificación de la información:** Definir qué tipo de datos se maneja y cómo se debe proteger cada tipo.
- ✓ **Políticas de acceso:** Determinar quién tiene acceso a la información y bajo qué condiciones.
- ✓ **Confidencialidad:** Asegurar que los funcionarios y contratistas firmen acuerdos de confidencialidad para proteger los datos sensibles.



3. Protección de Datos Personales

Se deben implementar medidas técnicas y organizativas para proteger los **datos personales** de los ciudadanos, como:

- ✓ **Encriptación de la información:** Utilizar herramientas que cifren los datos tanto en tránsito como en reposo.
- ✓ **Control de acceso:** Garantizar que solo las personas autorizadas puedan acceder a los sistemas que contienen datos sensibles, mediante mecanismos como contraseñas seguras y autenticación multifactor.
- ✓ **Anonimización o seudonimización** de datos cuando sea posible, especialmente en el manejo de grandes volúmenes de datos.

4. Protección ante Amenazas Cibernéticas

- ✓ **Ciberseguridad:** Adoptar herramientas y tecnologías para prevenir, detectar y responder a ciberataques, como malware o ransomware.
- ✓ **Monitoreo y auditoría:** Implementar sistemas de monitoreo para detectar accesos no autorizados o actividades sospechosas en los sistemas de información.
- ✓ **Copias de seguridad:** Realizar copias de seguridad periódicas de los datos y almacenarlas de manera segura.

5. Capacitación y Sensibilización

- ✓ **Entrenamiento del personal:** Los funcionarios deben recibir capacitación regular sobre las políticas de seguridad y privacidad de la información, así como sobre cómo manejar adecuadamente los datos personales.
- ✓ **Conciencia sobre amenazas:** Educar al personal sobre los riesgos relacionados con el uso de tecnologías (por ejemplo, phishing o ingeniería social) y las buenas prácticas en ciberseguridad.

Gestión de Incidentes de Seguridad

- ✓ **Plan de respuesta a incidentes:** Desarrollar y mantener un plan de respuesta ante posibles violaciones de seguridad o filtraciones de información. Este plan debe incluir protocolos para:
 - ❖ La identificación y notificación de incidentes.
 - ❖ La investigación y mitigación de los daños.
 - ❖ La notificación a las autoridades competentes y a los titulares de los datos en caso de brechas de seguridad.



República de Colombia
Departamento de Córdoba
Alcaldía de San Bernardo del Viento

Nit:800096804-9

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

- ✓ **Notificación de violaciones de seguridad:** Según la Ley 1581, si se produce una violación de datos, la Alcaldía debe notificar a la Superintendencia de Industria y Comercio (SIC) y a los titulares de los datos personales afectados.

7. Auditoría y Revisión Periódica

- ✓ **Auditorías de seguridad:** Realizar auditorías regulares de los sistemas de información para garantizar que se están cumpliendo las políticas de seguridad y privacidad.
- ✓ **Evaluación de riesgos:** Evaluar periódicamente los riesgos asociados con el manejo de la información y adaptar las medidas de protección según las nuevas amenazas.

8. Cumplimiento con Otras Normativas Locales e Internacionales

Además de la Ley 1581 de 2012, la Alcaldía debe considerar otras normativas como:

- ✓ **Ley 1266 de 2008:** Referida al manejo de la información financiera y crediticia de las personas.
- ✓ **Política de Gobierno Digital:** Establece directrices para el uso de tecnologías en las entidades públicas y la protección de los datos de los ciudadanos en sus servicios en línea.

9. Transparencia y Acceso a la Información Pública

En el marco de la Ley de Transparencia (Ley 1712 de 2014), la Alcaldía debe garantizar el acceso a la información pública. Sin embargo, se debe hacer una clara distinción entre la información pública y la privada. La información confidencial, como datos personales, debe ser protegida adecuadamente.

Gestión de la Información y la Destrucción Segura

- ✓ **Conservación de datos:** Definir el tiempo durante el cual se almacenarán los datos personales y cuándo se eliminarán.
- ✓ **Destrucción de información:** Establecer procedimientos para la destrucción segura de documentos o soportes que contengan información sensible.





República de Colombia Departamento de Córdoba Alcaldía de San Bernardo del Viento

Nit:800096804-9

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN



Ciclo PHVA del proceso de Seguridad y Privacidad de la Información para la alcaldía de san Bernardo.

A continuación se describen los procesos PHVA.

CICLO PHVA DEL PROCESO

P – Planear

Planear la Seguridad y Privacidad de la Información, la Seguridad Digital y la Continuidad de la Operación de los servicios de TI de la Alcaldía, mediante:

- Definición y actualización de políticas, lineamientos y procedimientos de seguridad de la información.
- Identificación y clasificación de los activos de información.
- Identificación, análisis y valoración de riesgos de seguridad y privacidad de la información.
- Planeación del Plan de Seguridad y Privacidad de la Información (PSPI) y del Plan de Continuidad de los Servicios de TI.





PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

H – Hacer

Implementar los lineamientos definidos para la seguridad y privacidad de la información mediante:

- Ejecución de controles técnicos, administrativos y organizacionales.
- Implementación de medidas para la protección de datos personales.
- Acompañamiento a los procesos en la adopción de controles de seguridad.
- Implementación del Plan de Continuidad de los Servicios de TI.
- Gestión operativa de incidentes de seguridad de la información.

V – Verificar

Realizar seguimiento y evaluación al desempeño del proceso mediante:

- Monitoreo de controles de seguridad de la información.
- Seguimiento a incidentes y eventos de seguridad.
- Auditorías internas y revisiones periódicas.
- Evaluación del cumplimiento normativo y del nivel de madurez del MSPI.
- Medición de indicadores de seguridad y privacidad de la información.

A – Actuar

Adoptar acciones de mejora continua para fortalecer el proceso mediante:

- Definición e implementación de acciones correctivas, preventivas y de mejora.
- Actualización de políticas, procedimientos y controles.
- Fortalecimiento de la gestión del conocimiento en seguridad de la información.
- Ajuste del PSPI y de los planes de tratamiento del riesgo.

SALIDAS

- Lineamientos y políticas de Seguridad y Privacidad de la Información actualizados.
- Riesgos de seguridad tratados y controlados.
- Incidentes de seguridad gestionados.
- Servicios de TI con continuidad asegurada.
- Cumplimiento del MSPI y del Modelo de Gobierno Digital.



Política general de seguridad y privacidad de la información y seguridad digital y continuidad de los servicios del ministerio/fondo de tecnologías de la información y las comunicaciones

La Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los Servicios de la Alcaldía de San Bernardo del Viento tiene como objetivo garantizar la protección de la información institucional y de los datos personales, la seguridad cibernética y la continuidad operativa de los servicios digitales, reconociendo la importancia de los activos de información para el cumplimiento de la misión institucional y la generación de confianza con el Estado y la ciudadanía. En este sentido, la Alcaldía adopta e implementa el Modelo de Seguridad y Privacidad de la Información (MSPI), enmarcado en un Sistema de Gestión de Seguridad de la Información (SGSI) y alineado con el Modelo de Gobierno Digital del MINTIC, mediante el cual se protegen y administran la confidencialidad, integridad, disponibilidad, autenticidad, privacidad y no repudio de la información, a través de una gestión integral de riesgos y la aplicación de controles físicos, administrativos y tecnológicos. Esta política se desarrolla bajo un marco normativo y tecnológico robusto, alineado con la legislación nacional vigente, las mejores prácticas internacionales y las necesidades operativas de la entidad, y se operacionaliza a través de objetivos claros, medibles y verificables que permiten evaluar su eficiencia, eficacia y efectividad, asegurando que los servicios digitales sean seguros, resilientes y confiables, y que la infraestructura tecnológica y la información de los ciudadanos y de la entidad se encuentren debidamente protegidas, promoviendo la mejora continua y el fortalecimiento permanente de la gestión de la seguridad de la información.



PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Objetivos específicos de la política de seguridad y privacidad de la información y seguridad digital y continuidad de los servicios del ministerio/fondo único de tecnologías de la información y las comunicaciones

- ✓ Proteger los activos de información de la entidad garantizando la confidencialidad, integridad y disponibilidad de la información, mediante la implementación de controles técnicos, administrativos y organizacionales definidos en el Modelo de Seguridad y Privacidad de la Información y el Sistema de Gestión de Seguridad de la Información.
- ✓ Gestionar de manera integral los riesgos de seguridad y privacidad de la información, identificando, analizando, evaluando y tratando los riesgos asociados a los procesos, servicios digitales y activos de información, con el fin de reducir la probabilidad y el impacto de incidentes de seguridad.
- ✓ Garantizar la protección de los datos personales de conformidad con la Ley 1581 de 2012 y demás normas aplicables, asegurando el ejercicio de los derechos de los titulares y el cumplimiento de las obligaciones legales en materia de tratamiento de datos personales.
- ✓ Fortalecer la seguridad digital de la entidad, mediante la adopción de medidas de prevención, detección, respuesta y recuperación frente a amenazas cibernéticas, que permitan proteger la infraestructura tecnológica y los sistemas de información.
- ✓ Asegurar la continuidad de la operación de los servicios de Tecnologías de la Información y las Comunicaciones, a través de la definición, implementación y prueba de planes de continuidad y recuperación ante desastres, que minimicen los impactos de eventos disruptivos.
- ✓ Promover una cultura organizacional de seguridad y privacidad de la información, mediante programas permanentes de sensibilización y capacitación dirigidos a funcionarios, contratistas y terceros, fortaleciendo el uso seguro y responsable de la información y las tecnologías.
- ✓ Garantizar el cumplimiento de los requisitos legales, reglamentarios y normativos aplicables, así como de los lineamientos del Modelo de Gobierno Digital, el MSPI y las normas técnicas adoptadas por la entidad, mediante mecanismos de seguimiento y control.



República de Colombia
Departamento de Córdoba
Alcaldía de San Bernardo del Viento

Nit:800096804-9

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

- ✓ Monitorear y evaluar la efectividad de los controles de seguridad de la información, estableciendo indicadores de desempeño que permitan medir la eficiencia, eficacia y efectividad de la política y soportar la mejora continua del SGSI.
- ✓ Gestionar de manera oportuna y eficaz los incidentes de seguridad de la información, asegurando su identificación, registro, análisis, tratamiento y notificación a las autoridades competentes y a los titulares de la información, cuando aplique.
- ✓ Fortalecer la confianza en los servicios digitales de la entidad, garantizando que estos sean seguros, confiables y resilientes, en beneficio de la ciudadanía y del cumplimiento de la misión institucional.





Alcance del sistema de gestión de seguridad y privacidad de la información.

La implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), conforme a los requisitos legales, reglamentarios y normativos vigentes, comprende la totalidad de los procesos estratégicos, misionales, de apoyo y de evaluación de la entidad, así como los activos de información, sistemas de información, infraestructuras tecnológicas, servicios digitales, usuarios, funcionarios, contratistas y terceros que intervienen en el tratamiento de la información. El Sistema de Gestión de Seguridad y Privacidad de la Información tiene como alcance asegurar la confidencialidad, integridad y disponibilidad de la información institucional y de los datos personales, así como la seguridad digital y la continuidad de la operación en la gestión, control y prestación del Servicio Público de las Tecnologías de la Información y las Comunicaciones, garantizando el cumplimiento de la misión institucional, la protección de los derechos de los ciudadanos y la alineación con los lineamientos del Modelo de Gobierno Digital y el enfoque de mejora continua.

Ámbito de aplicación

La Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios de la Alcaldía de San Bernardo del Viento aplica a todos los niveles funcionales y organizacionales de la entidad, a sus funcionarios, contratistas, proveedores, operadores y demás terceros que, en ejercicio de sus funciones o en virtud de su relación con la Alcaldía, compartan, utilicen, recolecten, procesen, intercambien o consulten información institucional, así como a los organismos de control y demás entidades que accedan, de manera interna o externa, a cualquier activo de información, independientemente de su ubicación; igualmente, esta política es aplicable a toda la información creada, recibida, procesada, almacenada o utilizada por la Alcaldía, sin importar el medio, formato, presentación o soporte en el que se encuentre, por lo que toda dependencia, persona o usuario que tenga acceso tecnológico o maneje activos de información de la entidad está obligado a cumplir las disposiciones aquí establecidas



República de Colombia
Departamento de Córdoba
Alcaldía de San Bernardo del Viento

Nit:800096804-9

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Estrategias y modelo de operación por gestiones del sistema de gestión de seguridad y privacidad de la información – SGSPI





Portafolio de proyectos / actividades

Para cada estrategia específica, **alcaldía** define los siguientes proyectos y productos esperados, que tienen por objetivo lograr la implementación y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI):

Estrategia / Eje	Proyecto / Iniciativa	Productos esperados
Liderazgo en Seguridad de la Información	Proyecto 1: Diseñar, adoptar e implementar la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los Servicios.	Política de Seguridad y Privacidad de la Información aprobada y socializada.
	Proyecto 2: Definir, documentar y formalizar los roles y responsabilidades en Seguridad de la Información.	Matriz de roles y responsabilidades formalizada e integrada a las políticas institucionales.
Gestión de Riesgos de Seguridad de la Información	Proyecto 1: Identificar, analizar, valorar y clasificar los riesgos asociados a los activos de información.	Matriz de riesgos de seguridad y privacidad de la información actualizada.
	Proyecto 2: Definir e implementar planes de tratamiento de riesgos de seguridad y privacidad de la información.	Planes de tratamiento de riesgos definidos, aprobados y en ejecución.
Concientización y Cultura de Seguridad	Proyecto 1: Elaborar el plan anual de sensibilización en seguridad y privacidad de la información.	Plan anual de sensibilización aprobado.
	Proyecto 2: Ejecutar jornadas de sensibilización dirigidas a funcionarios, contratistas y terceros.	Evidencias de las actividades realizadas (actas, registros, material de apoyo).
	Proyecto 3: Realizar transferencia de conocimiento mediante cursos y capacitaciones especializadas.	Certificaciones de cursos y capacitaciones.
	Control 1: Definir e implementar la Política de Respaldos de Información.	Resultados de encuestas de medición del nivel de concientización.



República de Colombia
Departamento de Córdoba
Alcaldía de San Bernardo del Viento

Nit:800096804-9

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Implementación de Controles de Seguridad	Control 2: Establecer el Procedimiento de Gestión de Cambios.	Política de respaldos aprobada y operativa.
		Procedimiento de gestión de cambios documentado y aplicado.
	Control 3: Implementar la Clasificación de la Información.	Esquema de clasificación de la información adoptado.
	Control 4: Definir Políticas de Desarrollo Seguro.	Políticas de desarrollo seguro implementadas.
	Control 5: Implementar una solución de Firewall de Aplicaciones Web (WAF).	WAF desplegado, configurado y en funcionamiento.
Gestión de Incidentes de Seguridad de la Información	Proyecto 1: Definir, documentar y formalizar el procedimiento de gestión de incidentes de seguridad de la información.	Procedimiento de gestión de incidentes aprobado y divulgado.
	Proyecto 2: Capacitar al personal en la atención y reporte de incidentes de seguridad.	Registros de capacitación y simulacros realizados.





Plan de implementación del modelo de seguridad y privacidad de la información.

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos identificados en la alcaldía de San Bernardo del viento , estas actividades se estructuraron de la siguiente manera, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016)

Gestión	Actividades	Tareas	Respon sable de la tarea	Fecha inicio	Fecha final
Gestión de Riesgos	Sensibilización	Socialización de los lineamientos y herramientas para la Gestión de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación.	Equipo de Sistemas	03-feb-26	30-abr-26
	Identificación de riesgos	Contexto, identificación, análisis y evaluación de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación.	Equipo de Sistemas	02-mar-26	24-jul-26
		Retroalimentación, revisión y verificación de los riesgos identificados (ajustes).	Equipo de Sistemas	01-jun-26	31-jul-26
	Aceptación de riesgos	Aprobación de los riesgos identificados y de los planes de tratamiento.	Equipo de Sistemas	05-ago-26	21-ago-26
	Publicación	Publicación de los mapas de riesgos de los procesos en el sistema institucional (SIMIG o el que aplique).	Equipo de Sistemas	24-ago-26	30-sep-26



República de Colombia
Departamento de Córdoba
Alcaldía de San Bernardo del Viento

Nit:800096804-9

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Mejoramiento Continuo	Seguimiento fase de tratamiento	Seguimiento a la implementación de controles y planes de tratamiento de riesgos, incluyendo verificación de evidencias.	Equipo de Sistemas	15-ene-26	18-dic-26
	Identificación de oportunidades de mejora	Identificación de oportunidades de mejora con base en el seguimiento a la ejecución de controles y planes de tratamiento.	Equipo de Sistemas	15-ene-26	18-dic-26
	Actualización de lineamientos	Revisión y/o actualización de los lineamientos de Gestión de Riesgos de Seguridad y Privacidad de la Información, conforme a las observaciones y resultados del seguimiento.	Equipo de Sistemas	03-feb-26	18-dic-26
	Monitoreo y revisión	Medición, presentación y reporte periódico de indicadores de gestión del SGSPI.	Equipo de Sistemas	20-ene-26	18-dic-26





República de Colombia
Departamento de Córdoba
Alcaldía de San Bernardo del Viento

Nit:800096804-9

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Análisis presupuestal

El análisis presupuestal del Plan de Seguridad y Privacidad de la Información para la vigencia 2026 de la Alcaldía de San Bernardo del Viento se formula con base en las actividades definidas en la gestión de riesgos, sensibilización, implementación de controles, mejora continua y continuidad de la operación de los servicios, garantizando la adecuada asignación de recursos financieros, humanos y tecnológicos necesarios para el cumplimiento de los objetivos del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI). Este presupuesto se orienta a fortalecer las capacidades institucionales, mitigar los riesgos de seguridad y privacidad de la información, asegurar la protección de los activos de información y garantizar la continuidad de los servicios digitales, en concordancia con los lineamientos del Ministerio TIC, el Modelo de Seguridad y Privacidad de la Información, la Política de Gobierno Digital y las buenas prácticas de la norma ISO/IEC 27001. Los recursos presupuestales estarán destinados prioritariamente a actividades de sensibilización y capacitación del talento humano, actualización y fortalecimiento del inventario y clasificación de activos de información, identificación, análisis y tratamiento de riesgos de seguridad y privacidad de la información, implementación y mantenimiento de controles técnicos, administrativos y físicos, así como al seguimiento, monitoreo y medición de indicadores del SGSPI. De igual manera, se contempla la asignación de recursos para la elaboración, actualización, socialización y pruebas del Plan de Continuidad de la Operación (BCP), incluyendo la realización de simulacros, evaluación de resultados y ajustes necesarios para mejorar la resiliencia institucional frente a incidentes de seguridad y eventos disruptivos; el presupuesto del plan se estructurará bajo un enfoque de eficiencia y racionalización del gasto, priorizando el aprovechamiento de capacidades internas de la entidad, el uso de herramientas institucionales existentes y el apoyo de proveedores especializados únicamente cuando se requieran conocimientos técnicos específicos o soluciones tecnológicas que no puedan ser atendidas con recursos propios. Asimismo, se considerará la ejecución de los recursos bajo las modalidades de gasto de funcionamiento e inversión, de acuerdo con la naturaleza de cada actividad, garantizando el cumplimiento de la normativa presupuestal vigente y la trazabilidad de la ejecución.





República de Colombia
Departamento de Córdoba
Alcaldía de San Bernardo del Viento

Nit:800096804-9

Componente / Eje	Actividad principal	Tipo de gasto	Descripción del recurso	Presupuesto estimado
Gobernanza y liderazgo de SPI	Actualización y formalización de políticas, roles y lineamientos de seguridad	OPEX	Apoyo técnico, revisión normativa, socialización institucional	\$8.000.000
Gestión de activos de información	Inventario, clasificación y actualización de activos de información	OPEX	Jornadas de trabajo, documentación, soporte técnico interno	\$6.000.000
Gestión de riesgos SPI y Seguridad Digital	Identificación, análisis y tratamiento de riesgos	OPEX	Talleres, matrices de riesgos, seguimiento a controles	\$10.000.000
Sensibilización y capacitación	Capacitación en seguridad de la información, protección de datos y ciberseguridad	OPEX	Capacitaciones, material pedagógico, cursos virtuales/presenciales	\$12.000.000
Implementación de controles técnicos	Herramientas de seguridad (copias de seguridad, control de accesos, WAF, antivirus)	CAPEX	Adquisición o fortalecimiento de soluciones tecnológicas	\$25.000.000
Implementación de controles administrativos	Procedimientos de gestión de cambios, respaldos y desarrollo seguro	OPEX	Documentación, adopción y divulgación de procedimientos	\$6.000.000
Gestión de incidentes de seguridad	Diseño y puesta en marcha del procedimiento de gestión de incidentes	OPEX	Capacitación, simulacros, formatos y reportes	\$7.000.000





República de Colombia
Departamento de Córdoba
Alcaldía de San Bernardo del Viento

Nit:800096804-9

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Continuidad de la operación (BCP)	Actualización, socialización y pruebas del Plan de Continuidad	OPEX	Mesas de trabajo, simulacros, ajustes al plan	\$10.000.000
Protección de datos personales	Registro y actualización de bases de datos ante la SIC	OPEX	Gestión administrativa, actualización documental	\$4.000.000
Monitoreo, auditoría y mejora continua	Seguimiento a indicadores, auditorías internas y planes de mejora	OPEX	Medición, informes, ajustes al SGSPI	\$7.000.000
Total				\$ 95.000.000





Control de cambios.

Fecha	Versión	Descripción del Cambio	Autor
29 de enero de 2021	1.0 – Versión final 2021	Elaboración del Plan	Oficina TIC
24 de enero de 2022	2.0 - Versión final 2022	Actualización del Plan por cambio a vigencia 2022	Oficina TIC
30 de enero de 2023	3.0 – Versión final 2023	Actualización del Plan por cambio a vigencia 2023	Oficina TIC
27 de enero de 2024	4.0 – Versión final 2024	Actualización del Plan por cambio a vigencia 2024	Oficina TIC
30 de enero de 2025	5.0 – Versión final 2025	Actualización del Plan por cambio a vigencia 2025	Oficina TIC
30 de enero de 2026	6.0 – Versión final 2026	Actualización del Plan por cambio a vigencia 2026	Oficina TIC