Plan de Seguridad y Privacidad de la Información

Alcaldía municipal de San Bernardo del Viento

Introducción

Los grandes volúmenes de información institucionales se originan desde diversas fuentes y con estándares tecnológicos heterogéneos en hardware, software, comunicaciones que requieren de una infraestructura de red adecuada, funcional y confiable para su transmisión y almacenamiento. En el caso del Municipio de San Bernardo del viento, las soluciones de conectividad y servicios informáticos fueron diseñadas fundamentalmente para soportar aplicaciones de procesamiento de datos. El crecimiento exponencial de nuevos servicios y aplicaciones ha generado en un conjunto de necesidades en la operación de la red y en la gestión de la seguridad de la información, elementos que han estado en una arriesgada prioridad en el dimensionamiento tecnológico institucional. Además mediante el artículo 7 de la Resolución 4870 de 2023, - "Por la cual se establecen el Modelo Integrado de Gestión (MIG) y el Sistema Integrado de Gestión (SIG) del Ministerio de Tecnologías de la Información y las Comunicaciones/Fondo Único de Tecnologías de la Información y las Comunicaciones y se deroga la Resolución 2175 de 2022 y sus modificatorias.", definió la relevancia de integrar los modelos y sistemas de gestión de la entidad de manera articulada con el Modelo Integrado de Gestión. Por otro lado, la resolución 0500 de marzo 10 del 2021 expedida por el Ministerio de Tecnologías de Información y las Comunicaciones, que tiene como "objeto establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, la guía de gestión de riesgos de Seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y establecer los lineamientos y estándares para la estrategia de seguridad digital". Por otra parte adoptar la estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital, e incluirla en el plan de seguridad y privacidad de la información que se integra al Plan de Acción en los términos del artículo 2.22.22.3.14 del capítulo 3 del título 22 de la parte 2 del libro 2 del decreto 1083 de 2015". Por todo lo anterior se hace necesaria la implementación de estrategias de seguridad y privacidad de la información para preservar los servicios disponibles y garantizar la confidencialidad e integridad de los datos en las aplicaciones. Existen algunos estándares de seguridad informática que sugieren, como primera medida realizar análisis de vulnerabilidades para responder corrigiendo posibles fallos y apuntando a modelos preventivos. Estos esfuerzos son inocuos, sin la implementación de un Sistema Integral de la

Seguridad de la Información. El presente documento pretende exponer una serie de lineamientos para implementar las mejores prácticas de Seguridad Informática en la Alcaldía Municipal de San Bernardo del viento, con el fin de optimizar la disponibilidad, la integridad, la confidencialidad/privacidad, entre otros principios relevantes, teniendo en cuenta la infraestructura y limitaciones actuales. La entidad decide vincular el modelo de administración de los riesgos de seguridad de la información y las actividades de valoración de mismos riesgos en cumplimiento de la política de seguridad de la información aprobada por la Alta Dirección, y como medio o herramienta para el logro de los objetivos de mantener la información de la alcaldía sea confidencial, integra y disponible, a través de su ciclo de vida desde su captura, almacenamiento, explotación, hasta su eliminación.

Objetivo

Definir los mecanismos y todas las medidas necesarias teniendo en cuenta el modelo de Seguridad y Privacidad de la Información – MSPI de la política de Gobierno Digital del MinTIC en el Municipio de San Bernardo del viento, tanto técnica, lógica, física, legal y ambiental para la protección de los activos de información, los recursos y la tecnología de la entidad, con el propósito de evitar accesos no autorizados, divulgación, duplicación, interrupción de sistemas, modificación, destrucción, pérdida, robo, o mal uso, que se pueda producir de forma intencional o accidental, frente a amenazas internas o externas, asegurando el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información, además garantizar los criterios de Continuidad de la operación de los servicios, que permitan mantener la seguridad y privacidad de la información que circula en los procesos.

Alcance

El alcance del Plan de Seguridad y Privacidad de la Información 2024 – 2027 se aplica a los procesos de la Alcaldía de San Bernardo del Viento, en concordancia con el Sistema de Gestión de la Seguridad de la Información y el Plan de Desarrollo 2024 - 2027 “Todo por mi pueblo” y teniendo en cuenta el Modelo de Seguridad y Privacidad de la Información - MSPI emitido por el Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC, para el desarrollo de la misión institucional y cumplimiento de sus objetivos estratégicos. En este se pretende realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital, que permita integrar en los procesos de la entidad, buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos.

El Plan de Tratamiento de Riesgo tendrá en cuenta los riesgos que se encuentren en los niveles Alto y Extremo acorde con los lineamientos definidos por el Ministerio TIC, los riesgos que se encuentren en niveles inferiores serán aceptados por la Entidad.

Las estrategias en el tratamiento del riesgo La Alcaldía de San Bernardo del Viento, se compromete a mantener una cultura de la gestión del riesgo asociados con la responsabilidad de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector TIC, regulando los riesgos de los procesos y proyectos, mediante mecanismos, sistemas y controles enfocados a la prevención y detección; y fortaleciendo las medidas de control.

Normatividad

Norma	Descripción
Ley 1581 de 2012 - Protección de Datos Personales	Regula el tratamiento de datos personales por parte de entidades públicas y privadas, estableciendo derechos de los titulares de los datos y las obligaciones de los responsables del tratamiento.
Decreto 1377 de 2013	Este decreto reglamenta la Ley 1581 de 2012, específicamente en relación con el tratamiento de los datos personales de los ciudadanos en casos en los que no haya sido otorgado el consentimiento expreso para su tratamiento.
Ley 1266 de 2008 - Habeas Data en el Sector Financiero	Esta ley establece normas relacionadas con la protección de datos personales en el contexto de la información financiera y crediticia. Regula la recolección, tratamiento, y circulación de datos de carácter financiero y crediticio.
Ley 1273 de 2009 - Delitos Informáticos	Esta ley penaliza los delitos informáticos, tales como la interceptación de comunicaciones, la violación de la privacidad en entornos digitales y el acceso no autorizado a sistemas informáticos.
Ley 1341 de 2009 - Ley TIC (Tecnologías de la Información y las Comunicaciones)	Regula las actividades relacionadas con las tecnologías de la información y las comunicaciones en Colombia, estableciendo normas de seguridad y privacidad en la infraestructura digital.
Decreto 1074 de 2015 - Decreto Único Reglamentario del Sector Comercio, Industria y Turismo	Este decreto establece normas sobre la protección de la información y la privacidad en el contexto de las actividades comerciales, incluyendo el comercio electrónico
Ley 1621 de 2013 - Ley de Inteligencia y Contrainteligencia	Regula el manejo de la información de inteligencia y contrainteligencia en Colombia, con medidas de seguridad sobre datos sensibles y estratégicos en el contexto de la seguridad nacional.
Decreto 889 de 2017 - Seguridad en la Información en el Estado	Establece los lineamientos y disposiciones para garantizar la seguridad de la información en los organismos del Estado. Establece las bases para implementar un sistema de gestión de la seguridad de la información (SGSI) en las entidades públicas.
Ley 1757 de 2015 - Derecho de Acceso a la Información Pública	Regula el acceso de los ciudadanos a la información pública del Estado, garantizando la transparencia, pero también protege los datos personales sensibles.

Ley 1527 de 2012 - Ciberseguridad y Ciberdefensa	Esta ley busca mejorar la seguridad en el ciberespacio en Colombia, protegiendo tanto la infraestructura crítica como los sistemas de información del Estado y las entidades privadas.
Resolución 3110 de 2018 - Seguridad en la Información en Entidades Públicas	Esta resolución, emitida por el Departamento Administrativo de la Función Pública (DAFP), establece directrices sobre cómo las entidades públicas deben garantizar la seguridad en la gestión de la información.
Ley 1712 de 2014	"Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".
Resolución MINTIC 746 de 2022	Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021
Decreto 1083 de 2015	Decreto 1499 de 2017. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015
Ley 1231 de 2008 - Protección de la Privacidad en Internet	Regula la protección de la privacidad en los servicios de Internet, incluyendo la recolección de datos personales a través de plataformas digitales.

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. Modelo De Seguridad Y Privacidad De La Información – MSPI de la política de Gobierno Digital del MinTIC.
6. Plan de desarrollo municipal 2024 – 2027 “Todo por mi pueblo”
7. Decreto 612 de 2018, “Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado”, donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa.
8. Resolución 500 de 2021. “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”.
9. Manual de Gobierno Digital – MINTIC.

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%						

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%						
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%	4. NORMATIVA	100	6%			
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. CONTRATACIÓN	100	4%			
5.2 Publicación de la información contractual	100	10%						
5.3 Publicación de la ejecución de los contratos	100	60%						
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. PLANEACIÓN	100	12%			
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%						
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%						
7.1 Trámites	100	100%	7. TRÁMITES	100	3%			
8.1 Descripción General	100	23%	8. PARTICIPA	100	18%			
8.2 Estructura y Secciones del menú "PARTICIPA	100	77%						
9.1 Instrumentos de gestión de la información	100	97%	9. DATOS ABIERTOS	100	14%			
9.2 Sección de Datos Abiertos	100	3%						
10.1 Información para Grupos Específicos	100	100%	10. INFORMACIÓN ESPECÍFICA PARA GRUPOS DE INTERÉS	100	2%			

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 PQRSD	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 MÍNIMAS Y DE SEGURIDAD DIGITAL WEB	100	100%	ANEXO 3. CONDICIONES TÉCNICAS MÍNIMAS Y DE SEGURIDAD DIGITAL WEB	100	2%

Aunque se deber 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 una estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, teniendo como premisa que dicha estrategia gira entorno a la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI, así como de la guía de gestión de riesgos de seguridad de la información y del procedimiento de gestión de incidentes que debe establecerse según Resolución 500 de 2021. En la cual se definen las 5 estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad digital:

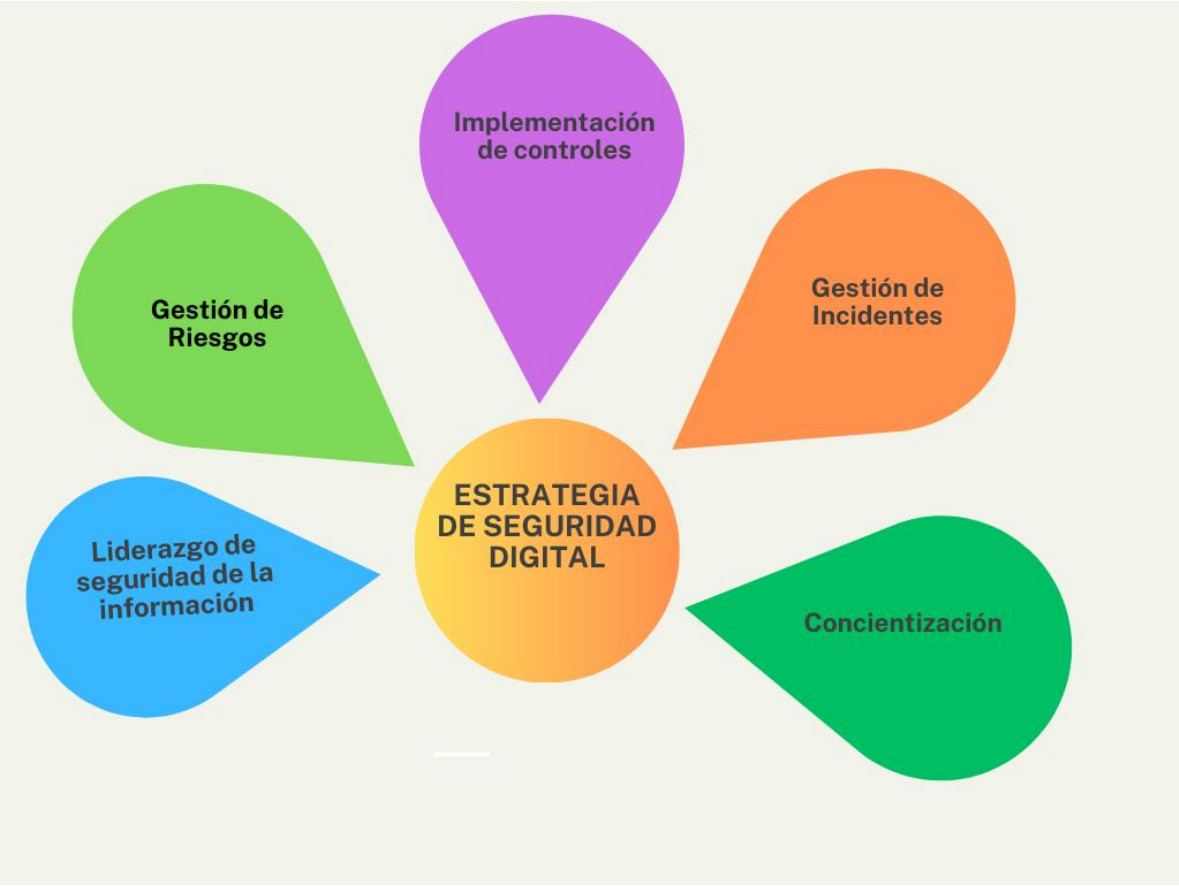


Fig1. Estrategias específicas

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar, alineando las actividades a lo descrito dentro del MPSI y la resolución 500 de 2021:

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
Liderazgo de seguridad de la información	Asegurar que se establezca el Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de la política general y demás lineamientos encontrados buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes dependencias y/o secretarias de la alcaldía a través del establecimiento de los roles y responsabilidades en seguridad de la información.
Gestión de riesgos	Se Determinan los riesgos de seguridad de la información a través de la planificación y valoración buscando prevenir o reducir los efectos indeseados tendiendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.
Concientización	Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la alcaldía en seguridad y privacidad de la información.
Implementación de controles	Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la alcaldía, se pueden subdividir en controles tecnológicos y/o administrativos.
Gestión de incidentes	Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la alcaldía.

Desarrollo.

Teniendo en cuenta lo estipulado en el numeral 2.1.3 del Manual de Gobierno Digital del MINTIC, el Plan de Seguridad y Privacidad de la Información debe establecer los detalles de cómo se realizará la implementación de la seguridad de la información en cada uno de los procesos de la entidad, estipulando directrices, tiempo y responsables para lograr un adecuado proceso de gestión, administración, evaluación y resultados del plan desarrollado.

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.

- ✓ **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:

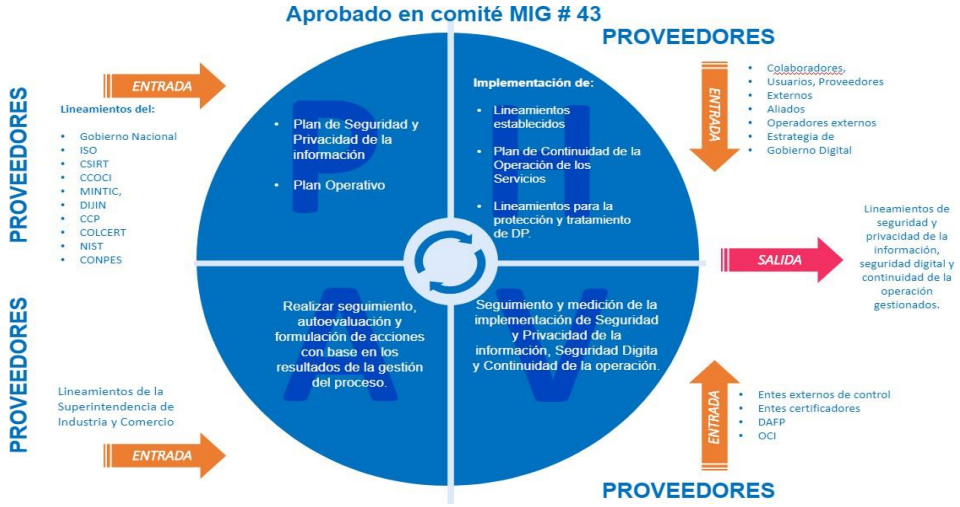
- ✓ **Ley 1266 de 2008**: Referida al manejo de la información financiera y crediticia de las personas.
- ✓ **Política de Gobierno Digital**: Establece directrices para el uso de tecnologías en las entidades públicas y la protección de los datos de los ciudadanos en sus servicios en línea.

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.



Ciclo PHVA del proceso de Seguridad y Privacidad de la Información

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

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 y la Seguridad Digital y Continuidad de los Servicios**,** tiene como objetivo garantizar la protección de la información sensible, la seguridad cibernética y la continuidad operativa en la prestación de servicios digitales. Esta política se debe desarrollar conforme a un marco normativo y tecnológico robusto que permita salvaguardar tanto los datos de los ciudadanos como la infraestructura tecnológica de la entidad, deben ser claras, robustas y estar alineadas con las mejores prácticas internacionales, leyes nacionales y necesidades operativas. La implementación efectiva de estas políticas garantizará que los servicios digitales se mantengan seguros, resilientes y confiables, protegiendo tanto a los ciudadanos como la integridad de los sistemas tecnológicos de la alcaldía.

La alcaldía de san Bernardo del viento entendiendo la importancia de sus activos de información para el cumplimiento de su misión institucional, se ha comprometido con la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) buscando proteger la confidencialidad, integridad y disponibilidad de los activos de información y además establecer un marco de confianza en el ejercicio de su misión con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes aplicables.

La alcaldía de san Bernardo del viento en su propósito de dar cumplimiento con la política de seguridad y privacidad de la información, establece los siguientes objetivos: (*recordar que los objetivos que se definan deben CUMPLIRSE y deben ser medibles de alguna forma, para que permitan determinar si en efecto son eficientes, efectivos o eficaces*)

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

- ✓ Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la alcaldía.
- ✓ Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- ✓ Minimizar el riesgo de todos los procesos de la entidad.
- ✓ Mejorar continuamente el sistema de gestión de seguridad de la información.
- ✓ Implementar los controles tecnológicos necesarios para la protección de los activos de la entidad y para la reducción de los riesgos.

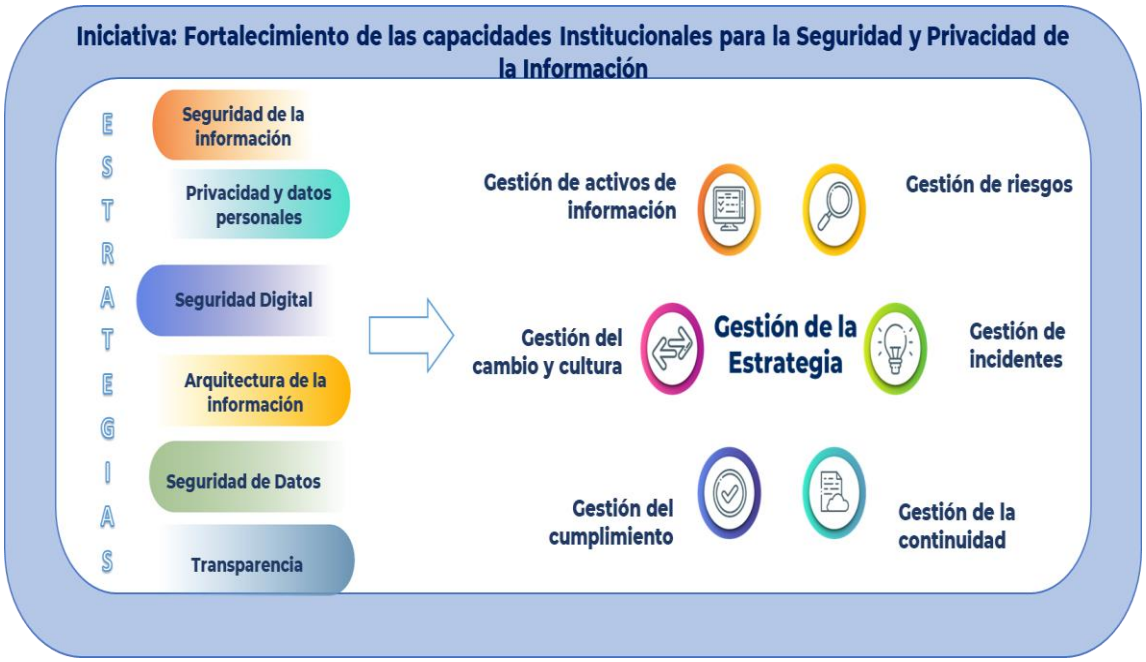
Alcance del sistema de gestión de seguridad y privacidad de la información.

La implementación del Modelo de Seguridad y Privacidad de la Información conforme a los requisitos normativos comprende a todos los procesos de la entidad y debe asegurar la confidencialidad, integridad y disponibilidad de la información en la gestión y control de la prestación del Servicio Público de las Tecnologías de la Información y las Comunicaciones.

Ámbito de aplicación

La Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios del Ministerio/Fondo Único de TIC, aplica a todos los niveles funcionales y organizacionales del Ministerio/Fondo Único de TIC, a todos sus funcionarios, contratistas, proveedores, operadores, entidades adscritas y del sector de las Tecnologías de la Información y las Comunicaciones, así como aquellas personas o terceros que en razón del cumplimiento de sus funciones y las del Ministerio de TIC compartan, utilicen, recolecten, procesen, intercambien o consulten su información, al igual que a la entidades de control, demás entidades relacionadas que accedan, ya sea interna o externamente a cualquier activo de información, independientemente de su ubicación. De igual manera, esta política aplica a toda la información creada, procesada o utilizada por el Ministerio/Fondo Único de TIC, sin importar el medio, formato, presentación o lugar en el cual se encuentre. Por lo tanto toda dependencia, persona o usuario que maneje o tenga acceso tecnológico en la alcaldía le es aplicada la norma.

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



Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

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	PRODUCTOS ESPERADOS
Liderazgo de seguridad de la información	PROYECTO 1: Desarrollar e implementar una política de seguridad PROYECTO 2: Definición de Roles y Responsabilidades de Seguridad de la Información.	Política de Seguridad Formalizada e Implementada. Definición de los Roles y Responsabilidades en Seguridad de la Información formalizados dentro de las políticas de seguridad.
Gestión de riesgos	PROYECTO 1: Identificar, valorar y clasificar los riesgos asociados a los activos de información PROYECTO 2: Definir planes de tratamiento de riesgos de seguridad	Matriz de riesgos de seguridad digital Definir planes de tratamiento de riesgos

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
Concientización	PROYECTO 1: Establecer desde el inicio de cada año la planeación de sensibilización para todo el año. PROYECTO 2: Realizar jornadas de sensibilización a todo el personal. PROYECTO 3: Realizar trasferencia de conocimiento a colaboradores de la Entidad a través de cursos especializados en diferentes temas. Medir el grado de sensibilización a toda la Entidad.	1. Plan de Sensibilización 2. Evidencias de las actividades desarrolladas 3. Certificaciones de cursos 4. Resultado de las encuestas de medición
Implementación de controles	CONTROL 1 Política de respaldos de información. CONTROL 2 Procedimiento de Gestión de Cambios. CONTROL 3 Clasificación de la información. CONTROL 4 Políticas de Desarrollo Seguro CONTROL 5 Implementación de solución WAF	Política de respaldos de información. Procedimiento de Gestión de Cambios. Clasificación de la información. Políticas de Desarrollo Seguro WAF desplegado y funcional.
Gestión de incidentes	**PROYECTO 1:** Definir y formalizar un procedimiento de Gestión de Incidentes de seguridad de la información. **PROYECTO 2:** Capacitar al personal en la gestión de incidentes de seguridad de la información.	1. Procedimiento de gestión de incidentes de seguridad formalizado. 2. Sesiones de capacitación desarrolladas.

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	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
Gestión de Riesgos	Sensibilización	Socialización de lineamientos y herramienta para la Gestión de Riesgos de Seguridad y privacidad de la Información y Seguridad Digital	Secretarias junto a equipo de sistemas	3-feb-25	**30-abril-25**
	Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación	Contexto, Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información y Seguridad Digital	Secretarias junto a equipo de sistemas	3-mar-25	**25-jul-25**
		Realimentación, revisión y verificación de los riesgos identificados (Ajustes)	Secretarias junto a equipo de sistemas	1-mar-25	**28-jul-25**
	Aceptación de Riesgos Identificados	Aceptación, aprobación riesgos identificados y planes de tratamiento	Secretarias junto a equipo de sistemas	5-may-25	**21-jul-25**
	Publicación	Publicación mapas de riesgos de los procesos en SIMIG	Secretarias junto a equipo de sistemas	2-jun-25	**31-jul-25**
	Seguimiento Fase de Tratamiento	Seguimiento implementación de controles y planes de tratamiento de riesgos los identificados (verificación de evidencias)	Secretarias junto a equipo de sistemas	15-ene-25	**26-dic-25**
	Mejoramiento	Identificación de oportunidades de mejora acorde al seguimiento de la ejecución de los controles y de los planes de tratamiento	Secretarias junto a equipo de sistemas	15-ene-25	**26-dic-25**
		Revisión y/o actualización de lineamientos de Riesgos de Seguridad y privacidad de la información de acuerdo con las observaciones identificadas.	Secretarias junto a equipo de sistemas	3-feb-25	**26-dic-25**
	Monitoreo y Revisión	**Medición, presentación y reporte de indicadores**	**Secretarias junto a equipo de sistemas**	**20-ene-25**	**26-dic-25**

Análisis presupuestal

Con base a los proyectos definidos en el cronograma de actividades, se debe generar el presupuesto aproximado por cada vigencia según los proyectos establecidos y presentarlo a la Alta Dirección para las consideraciones y viabilidad pertinentes.

<table>
<tr><th>RECURSOS</th><th>VARIABLE</th></tr>
<tr><td>Humanos</td><td>

El Grupo Interno de Trabajo de Seguridad y Privacidad de la Información
Profesional de riesgos del Grupo Interno de Trabajo de Transformación Organizacional
Líderes y gestores de procesos
Dimensión de Seguridad informática de la Oficina de TI
Grupo Interno de Trabajo de Respuesta a Emergencias Cibernéticas de Colombia - COLCERT
Equipo de Trabajo de Seguridad y Privacidad de la Información de la Dirección de Gobierno Digital.

</td></tr>
<tr><td>Técnicos</td><td>Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital del DAFP
Herramienta para la gestión de riesgos (Matriz de Riesgos SGSPI)</td></tr>
<tr><td>Logísticos</td><td>Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.</td></tr>
<tr><td>Financieros</td><td>Recursos para la adquisición de conocimiento, recursos humanos, técnicos, y desarrollo de auditorías en el GIT de Seguridad y Privacidad de la Información
<table>
<tr><th></th><th>Iniciativa</th><th>Proyecto</th><th>Presupuesto</th></tr>
<tr><td></td><td>Fortalecimiento de las capacidades institucionales para la seguridad y Privacidad de la Información</td><td>P1 - Fortalecimiento del Modelo de gestión de Seguridad y privacidad de la información.</td><td>$ 167.780.000.oo</td></tr>
</table>
</td></tr>
</table>

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 2024	**5.0 – Versión final 2025**	**Actualización del Plan por cambio a vigencia 2025**	**Oficina TIC**