PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ALCALDÍA MUNICIPAL
SAN BERNARDO DEL VIENTO

Presentación

La Alcaldía de San Bernardo del Viento, en cumplimiento de sus responsabilidades institucionales y de los lineamientos de Gobierno Digital, debe establecer e implementar acciones sistemáticas para la gestión de los riesgos de seguridad de la información, con especial énfasis en aquellos riesgos que superan el nivel de aceptación definido por la entidad. Para ello, se adopta el Plan de Tratamiento de Riesgos de Seguridad de la Información, como instrumento que permite identificar, evaluar y tratar los riesgos asociados a los activos de información, mediante la definición e implementación de controles adecuados. El Plan de Tratamiento de Riesgos tiene como propósito principal reducir la probabilidad de ocurrencia y el impacto de los riesgos identificados, garantizando la protección de la información institucional, la continuidad de los servicios, la prevención de incidentes de seguridad y el fortalecimiento de la confianza ciudadana. Así mismo, contribuye al cumplimiento de los principios de confidencialidad, integridad y disponibilidad de la información que soporta los procesos estratégicos, misionales y de apoyo de la entidad; este plan se formula y ejecuta en concordancia con el CONPES 3854 de 2016, CONPES 4144 de 2025 el Modelo de Seguridad y Privacidad de la Información del MINTIC, el Decreto 1008 del 14 de junio de 2018, Decreto 338 del 2022 y demás disposiciones normativas aplicables. De igual forma, incorpora las buenas prácticas y lineamientos de los estándares internacionales ISO/IEC 27001:2022 e ISO 31000:2018, así como la Guía para la administración del riesgo y el diseño de controles en entidades públicas, emitida por el Departamento Administrativo de la Función Pública (DAFP), fortaleciendo así el modelo de gestión, control y mejora continua de la seguridad de la información en la Alcaldía.

Introducción

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios de la alcaldía municipal de San Bernardo del Viento, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la entidad en caso de materialización, adicional se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos trazados en el Entorno TIC para el Desarrollo Digital, ciudadanos y hogares empoderados del Entorno Digital, Transformación Digital Sectorial y Territorial e Inclusión Social Digital.
Por lo anterior dando cumplimiento a la normativa establecida por el estado colombiano CONPES 3854 de 2016, CONPES 4144 de 2025 el Modelo de Seguridad y Privacidad de la Información del MINTIC, el Decreto 1008 del 14 de junio de 2018, Decreto 338 del 2022 y demás disposiciones normativas aplicables. De igual forma, incorpora las buenas prácticas y lineamientos de los estándares internacionales ISO/IEC 27001:2022 e ISO 31000:2018, así como la la guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital – versión 6 emitida por el DAFP.

El Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) establece que la seguridad y privacidad de la información constituyen un elemento transversal y habilitador para el adecuado funcionamiento de las entidades públicas, en tanto soportan el desarrollo integral de los componentes de la Política de Gobierno Digital. Este enfoque se materializa a través de lineamientos específicos en materia de seguridad y privacidad de la información y de gestión de riesgos de seguridad digital, los cuales orientan a las entidades en la definición e implementación de acciones destinadas a la protección de sus activos de información, dichos lineamientos permiten a las entidades preservar de manera efectiva los principios fundamentales de la seguridad de la información: confidencialidad, integridad, disponibilidad y privacidad de los datos, asegurando que la información institucional sea utilizada, almacenada y transmitida de forma segura, confiable y conforme a la normativa vigente. En este contexto, la gestión adecuada de los riesgos de seguridad digital se convierte en un componente esencial para prevenir incidentes, minimizar impactos y garantizar la continuidad de los servicios digitales ofrecidos a la ciudadanía, por otra parte el Manual de la Política de Gobierno Digital, expedido por el MINTIC, establece dentro de sus propósitos el logro de procesos internos seguros, eficientes y confiables, mediante el fortalecimiento de las capacidades de gestión de las Tecnologías de la Información en las entidades públicas.

Este fortalecimiento implica el diseño, implementación y mejora continua de procesos y procedimientos que incorporen el uso estratégico de las tecnologías de la información, apoyados en esquemas de manejo seguro de la información y en la alineación con la arquitectura institucional, tanto en su componente misional como en la Arquitectura de TI, la articulación entre la gestión de la seguridad de la información y la arquitectura institucional permite que las soluciones tecnológicas respondan de manera coherente a las necesidades del negocio, apoyen el cumplimiento de los objetivos estratégicos y contribuyan al logro de las metas institucionales. En este sentido, la seguridad de la información deja de ser un componente aislado y se integra de manera estructural a los procesos de planeación, gestión y operación de la entidad, en concordancia con el nuevo enfoque de Gobierno Digital y con lo establecido en el Modelo de Seguridad y Privacidad de la Información (MSPI), así como en los Controles de Seguridad y Privacidad de la Información, se definen los lineamientos del presente plan, el cual orienta a la entidad en la adopción de medidas preventivas, correctivas y de mejora continua para la gestión de los riesgos de seguridad de la información, fortaleciendo así la gobernanza digital y la protección de los activos de información institucionales.

Definiciones.

- ✓ **Riesgo:** es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.
- ✓ **Ciberdefensa:** Conjunto de capacidades, estrategias, procesos y acciones coordinadas orientadas a prevenir, detectar, responder y recuperarse frente a amenazas y ataques en el ciberespacio que puedan afectar los sistemas de información, las infraestructuras tecnológicas, los servicios digitales y los activos de información críticos de una entidad o del Estado.
- ✓ **Ciberamenaza**: Evento o circunstancia potencial, de origen interno o externo, que puede materializarse en un ataque cibernético y generar afectaciones a los activos de información, sistemas o servicios digitales de una entidad.
- ✓ **Ciberriesgo**: Posibilidad de que una ciberamenaza explote una vulnerabilidad tecnológica, humana o de proceso y genere un impacto negativo sobre los activos de información, la operación institucional o la continuidad del servicio.
- ✓ **Ciberincidente**: Evento real o potencial en el ciberespacio que compromete o pone en riesgo la **confidencialidad, integridad, disponibilidad o privacidad** de la información o de los servicios digitales de una entidad.
- ✓ **Ciberdelito:** Conducta ilícita tipificada por la ley, cometida mediante el uso de tecnologías de la información, redes o sistemas informáticos, que afecta la información, los sistemas o los derechos de las personas o entidades.
- ✓ **Ciberespacio**: Entorno virtual conformado por la interconexión de redes, sistemas de información, servicios digitales y dispositivos tecnológicos, donde se generan, procesan, almacenan y transmiten datos e información.
- ✓ **Ciberresiliencia**: Capacidad de una entidad para anticiparse, resistir, responder y recuperarse frente a incidentes cibernéticos, manteniendo la continuidad de sus operaciones y la prestación de servicios esenciales.
- ✓ **Ciberhigiene**: Conjunto de buenas prácticas que deben adoptar las personas y organizaciones para reducir los riesgos en el uso de tecnologías digitales, tales como el uso de contraseñas seguras, actualizaciones periódicas y el manejo responsable de la información.
- ✓ **Ciberinteligencia**: Proceso de recopilación, análisis y uso de información relacionada con amenazas y riesgos en el ciberespacio, con el fin de anticipar ataques, fortalecer la toma de decisiones y mejorar las capacidades de prevención y respuesta.

- ✓ **Ciberprotección**:Aplicación de controles técnicos y organizacionales orientados a salvaguardar los sistemas, redes y activos de información frente a accesos no autorizados, fallas o ataques cibernéticos.
- ✓ **Ciberseguridad Digital:** Enfoque integral promovido por el Estado colombiano para la gestión de riesgos en el entorno digital, que articula la seguridad de la información, la ciberseguridad, la protección de datos personales y la continuidad de los servicios digitales.
- ✓ **Archivo:** Conjunto organizado de documentos, independientemente de su soporte, formato o fecha, producidos o recibidos por una entidad, persona natural o jurídica en el ejercicio de sus funciones, actividades o responsabilidades, y conservados como evidencia de la gestión administrativa, soporte de la memoria institucional y fuente de información para la toma de decisiones.
- ✓ **Ataque Informático:** Acción intencional y maliciosa, ejecutada por personas o sistemas, que tiene como objetivo comprometer, dañar, interrumpir, alterar o acceder de manera no autorizada a los sistemas de información, redes, servicios tecnológicos o activos de información de una entidad, afectando la confidencialidad, integridad, disponibilidad o privacidad de la información.
- ✓ **Riesgo aceptable**: Riesgo en que la organización decide que puede convivir y/o soportar dado a sus obligaciones legales, contractuales y/o intereses propios.
- ✓ **Riesgo residual**: Nivel de riesgo que permanece luego de tomar medidas de tratamiento.
- ✓ **Gestión del riesgo**: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- ✓ **Riesgo de seguridad digital**: combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.
- ✓ **Evaluación de riesgos**: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.
- ✓ **Amenaza:** es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).
- ✓ **Vulnerabilidad:** es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.
- ✓ **Probabilidad:** es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.

- ✓ **Impacto:** son las consecuencias que genera un riesgo una vez se materialice.
- ✓ **Control o Medida:** acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.
- ✓ **Administración del riesgo**: Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.
- ✓ **Activo de Información**: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.
- ✓ **Análisis de riesgos**: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.
- ✓ **Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- ✓ **Consecuencia**: Resultado de un evento que afecta los objetivos. Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.
- ✓ **Evento:** Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.
- ✓ **Contexto externo:** Ambiente externo en el cual la organización busca alcanzar sus objetivos (tecnológico, legal, regional, etc.).
- ✓ **Contexto interno**: Ambiente interno en el cual la organización busca alcanzar sus objetivos (gobierno, políticas, estructura organizacional, etc.).
- ✓ **Fuente**: Elemento que por sí solo o en combinación tiene el potencial intrínseco para dar lugar a riesgo; a fuente del riesgo puede ser tangible o intangible.
- ✓ **Acceso a la Información Pública**: El acceso a la información pública se rige por lo dispuesto en la **Ley 1712 de 2014 (Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional)** y sus normas reglamentarias, y se ejerce sin perjuicio de las restricciones legales relacionadas con la protección de datos personales, la seguridad de la información, la reserva legal y la confidencialidad, las cuales deben ser aplicadas de manera proporcional y justificada.

- ✓ **Activo Crítico** : Activo de información cuya afectación, pérdida, alteración, divulgación no autorizada o indisponibilidad puede generar un impacto alto o crítico en el cumplimiento de las funciones misionales, estratégicas u operativas de la entidad, comprometiendo la continuidad del servicio, el cumplimiento normativo, la seguridad de la información, la confianza ciudadana o la imagen institucional.
- ✓ **Alcance del Modelo de Seguridad y Privacidad de la Información (MSPI)**: El Modelo de Seguridad y Privacidad de la Información (MSPI) aplica a todos los procesos, dependencias, funcionarios, contratistas y terceros que participen en el tratamiento, gestión, administración o custodia de la información de la Alcaldía de San Bernardo del Viento, así como a los activos de información que soportan el cumplimiento de sus funciones misionales, estratégicas y de apoyo.
- ✓ **Ataque Cibernético**: Acción intencional y maliciosa, ejecutada mediante el uso de tecnologías de la información y las comunicaciones, cuyo propósito es acceder, alterar, interrumpir, destruir o divulgar de manera no autorizada sistemas de información, redes, servicios digitales o activos de información de una entidad, afectando la confidencialidad, integridad, disponibilidad o privacidad de la información.
- ✓ **BCP – Business Continuity Plan (Plan de Continuidad del Negocio):** Conjunto de estrategias, procedimientos y acciones documentadas que permiten a una entidad prepararse, responder y recuperarse ante eventos disruptivos o incidentes que puedan afectar la operación normal de sus procesos, servicios o sistemas de información, garantizando la continuidad de las funciones críticas y la prestación de servicios esenciales dentro de niveles aceptables de tiempo y calidad.

Objetivos

Objetivo general

Establecer, implementar y fortalecer los lineamientos necesarios para la gestión integral de los riesgos asociados a la Seguridad y Privacidad de la Información, la Seguridad Digital y la Continuidad de la Operación de los servicios de la Alcaldía de San Bernardo del Viento, incluyendo los riesgos de interrupción, con el propósito de garantizar el cumplimiento de los objetivos estratégicos institucionales y asegurar la protección de la información, bajo los principios de confidencialidad, integridad, disponibilidad, autenticidad y privacidad, en concordancia con los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC.

Objetivos específicos

- ✓ Establecer el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, como un instrumento que permita adoptar medidas y acciones encaminadas a controlar y minimizar los riesgos de seguridad y privacidad de la información de la Alcaldía de San Bernardo de viento.
- ✓ Identificar y clasificar los activos de información de la Alcaldía de San Bernardo del Viento, con el fin de reconocer su valor, criticidad y nivel de protección requerido, de acuerdo con su importancia para los procesos misionales, estratégicos y de apoyo.
- ✓ Identificar, analizar y evaluar los riesgos asociados a la Seguridad y Privacidad de la Información, la Seguridad Digital y la Continuidad de la Operación de los servicios institucionales, considerando amenazas internas y externas, vulnerabilidades y posibles impactos.
- ✓ Definir e implementar controles técnicos, administrativos y operativos para el tratamiento de los riesgos identificados, de manera que se reduzca su probabilidad de ocurrencia o impacto, en concordancia con los lineamientos del MinTIC y las buenas prácticas internacionales.
- ✓ Fortalecer la protección de la información y los datos personales, garantizando el cumplimiento de los principios de confidencialidad, integridad, disponibilidad, autenticidad y privacidad, así como la normatividad vigente en materia de protección de datos personales.

- ✓ Establecer y mantener mecanismos de continuidad de la operación, que permitan asegurar la prestación oportuna y continua de los servicios institucionales y la recuperación de los procesos críticos ante eventos de interrupción o incidentes de seguridad.
- ✓ Implementar un esquema de gestión de incidentes de seguridad de la información, que permita la detección, reporte, análisis, atención y cierre oportuno de eventos que afecten la información o los servicios digitales de la entidad.
- ✓ Promover la cultura de Seguridad y Privacidad de la Información, mediante programas de sensibilización, capacitación y apropiación dirigidos a servidores públicos, contratistas y terceros que tengan acceso a la información institucional.
- ✓ Monitorear, evaluar y mejorar continuamente el MSPI, a través del seguimiento de indicadores, auditorías, revisiones periódicas y acciones de mejora, garantizando su alineación con los objetivos institucionales y los lineamientos del MinTIC.
- ✓ Asegurar el cumplimiento normativo y regulatorio, relacionado con la Seguridad de la Información, la Seguridad Digital y la Protección de Datos Personales, aplicable a las entidades públicas del orden territorial.

Alcance

El presente documento tiene como propósito establecer una gestión integral y eficiente de los riesgos asociados a la Seguridad y Privacidad de la Información, la Seguridad Digital y la Continuidad de la Operación de los servicios de la Alcaldía Municipal de San Bernardo del Viento, integrando buenas prácticas de gestión de riesgos en los procesos institucionales, que apoyen la toma de decisiones y contribuyan a la prevención de incidentes que puedan afectar el cumplimiento de los objetivos estratégicos de la entidad, además se con contempla la definición y aplicación de lineamientos claros y estandarizados que permitan identificar, analizar, evaluar, tratar y monitorear los riesgos de Seguridad y Privacidad de la Información presentes en la Alcaldía Municipal de San Bernardo del Viento, en concordancia con la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC (2016) y demás normatividad vigente aplicable a las entidades públicas por otra parte El Plan de Tratamiento de Riesgos considerará aquellos riesgos clasificados en los niveles Moderado, Alto y Extremo, de acuerdo con los criterios y lineamientos definidos por la Alcaldía Municipal, los cuales deberán ser gestionados mediante la implementación de controles y acciones de mitigación, los riesgos que se ubiquen en niveles Bajo o Muy Bajo podrán ser aceptados por la entidad, previa evaluación y aprobación de las instancias competentes. Como resultado de lo anterior, se establecerá una línea base para el tratamiento de riesgos en la Alcaldía Municipal de San Bernardo del Viento, que facilite la identificación permanente de los riesgos presentes en la entidad y permita fortalecer las capacidades institucionales para su gestión, asimismo, se promoverá el conocimiento y apropiación del proceso de mitigación de riesgos por parte de los servidores públicos, con el fin de minimizar la pérdida de información, los impactos sobre los activos tecnológicos y la afectación a la prestación de los servicios institucionales.

Marco de Referencia

Política de Administración de Riesgos

La alcaldía municipal de San Bernardo del Viento a través de su Modelo Integrado de Gestión, se orienta hacia una cultura de la gestión del riesgo asociados en el desarrollo de sus procesos, en aras de cumplir con su responsabilidad de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector TIC que contribuyen al desarrollo social y económico del país, al desarrollo integral de los ciudadanos y la mejora en su calidad de vida.

Objetivo de la Política

El objetivo de la política es establecer los parámetros necesarios para una adecuada gestión de los Riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de los servicios (riesgos de interrupción) de la alcaldía procurando que no se materialicen, atendiendo los lineamientos establecidos en la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP, orientando a la toma de decisiones oportunas y minimizando efectos adversos al interior de la Entidad, con el fin de dar continuidad a la gestión institucional y asegurar el cumplimiento de los compromisos con los Grupos de interés.

Tratamiento de riesgos

El tratamiento de riesgos es la respuesta establecida por la primera línea de defensa, es decir, el líder o responsable del proceso junto con su equipo de trabajo para la mitigación de los diferentes riesgos.

El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

- ✓ **Aceptar el riesgo**: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. (Ningún riesgo de corrupción es aceptado). La aceptación del riesgo puede ser una opción viable en la alcaldía, para los riesgos bajos, pero también pueden existir escenarios de riesgos a los que no se les puedan aplicar controles y, por ende, se acepta el riesgo. En ambos escenarios debe existir un seguimiento continuo del riesgo.

- ✓ **Reducir el riesgo:** Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles. Deben seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este.

- ✓ **Evitar el riesgo:** Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.

- ✓ **Compartir el riesgo:** Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad. Los dos principales métodos de compartir o transferir parte del riesgo son: seguros y tercerización.

Gestión de Riesgos de Seguridad, Privacidad y Continuidad Operacional.

La Gestión de Riesgos de Seguridad, Privacidad y Continuidad Operacional es un enfoque integral que busca identificar, evaluar, gestionar y mitigar los riesgos asociados con estos tres aspectos fundamentales en cualquier organización.

- ✓ **Riesgos de Seguridad**

Los riesgos de seguridad están relacionados con las amenazas a los activos de información y sistemas tecnológicos de la organización. Esto puede incluir ciberataques, acceso no autorizado, fallos en la infraestructura tecnológica, y otros incidentes que puedan comprometer la integridad, confidencialidad o disponibilidad de la información.

- **Objetivo**: Proteger los sistemas de información, redes y datos sensibles contra accesos no autorizados, alteraciones, destrucción o robo.
- **Medidas**: Implementación de firewalls, cifrado, control de accesos, autenticación multifactor, monitoreo constante.

✓ **Riesgos de Privacidad**

Los riesgos de privacidad están relacionados con el manejo y protección de la información personal de los usuarios, clientes y empleados. La filtración o mal manejo de datos personales puede tener repercusiones legales, financieras y de reputación.

Objetivo: Asegurar que la alcaldía cumpla con las normativas y leyes de protección de datos personales, y que la información sensible sea tratada de manera ética y segura.

- **Medidas**: Implementación de políticas de privacidad claras, cifrado de datos personales, limitación del acceso a esta información y capacitación del personal sobre privacidad.

✓ **Riesgos de Continuidad Operacional**

Los riesgos de continuidad operacional están relacionados con la capacidad de la alcaldía para mantener sus operaciones en marcha frente a incidentes disruptivos. Esto incluye desastres naturales, fallos tecnológicos, problemas de proveedores o cualquier evento que pueda afectar la capacidad de la organización para operar normalmente.

- **Objetivo**: Minimizar el impacto de incidentes disruptivos y garantizar la continuidad de las operaciones críticas, tanto a corto como a largo plazo.
- **Medidas**: Desarrollo de planes de continuidad del negocio, planes de recuperación ante desastres (DRP), pruebas de resiliencia y establecimiento de procesos de gestión de crisis.

Por lo anterior, la gestión de riesgos en los ámbitos de seguridad, privacidad y continuidad operacional es un enfoque clave para proteger a la organización de amenazas internas y externas, asegurar el cumplimiento normativo y garantizar la continuidad de las operaciones a largo plazo.

Metodología

El Plan de Tratamiento de Riesgos establece la metodología para la definición, implementación y seguimiento de las actividades necesarias para mitigar, reducir o controlar los riesgos que puedan afectar los activos de información asociados a los diferentes procesos estratégicos, misionales, de apoyo y de evaluación y control de la Alcaldía Municipal de San Bernardo del Viento, dicha metodología se fundamenta en un enfoque sistemático y continuo de gestión de riesgos, orientado a proteger la información institucional y garantizar la continuidad de la operación de los servicios, y se desarrolla en concordancia con las recomendaciones y lineamientos establecidos en la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC (2016), así como con las buenas prácticas nacionales e internacionales en materia de seguridad de la información; las actividades del Plan de Tratamiento de Riesgos se estructuran de manera ordenada y coherente, permitiendo identificar, analizar, evaluar, tratar y monitorear los riesgos, definir responsables, establecer controles y acciones de mitigación, y realizar el seguimiento a su efectividad, con el fin de disminuir la probabilidad de ocurrencia o el impacto de los riesgos sobre la información y los servicios institucionales. Esta metodología facilita la integración de la gestión de riesgos en los procesos de la entidad, apoya la toma de decisiones informadas por parte de la alta dirección y contribuye al fortalecimiento de la cultura de Seguridad y Privacidad de la Información en la Alcaldía Municipal.

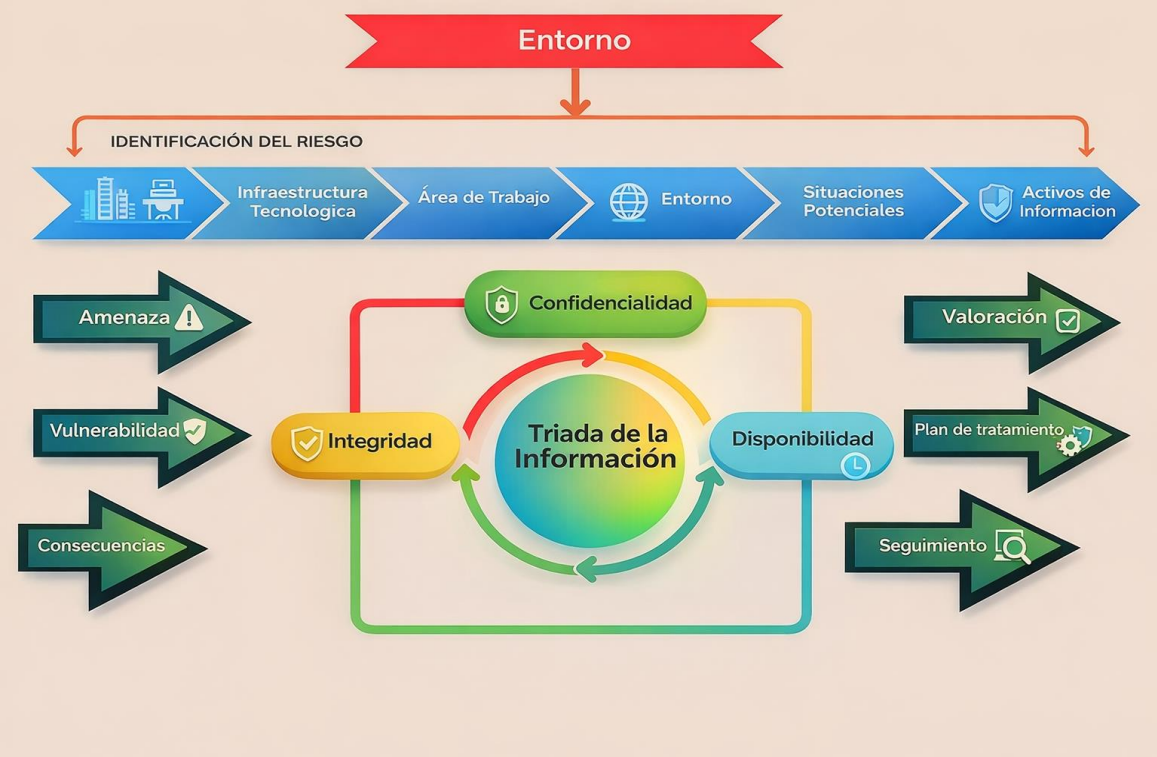
Tabla: Actividades a desarrollar en aras de mitigar los riesgos

Gestión	Actividad	Tareas	Responsable	Inicio	Fin	Productos / Evidencias	Indicadores	Observaciones
Gestión de Riesgos	Sensibilización	Socialización de lineamientos, políticas y herramienta de gestión de riesgos	Oficina de Sistemas	02/02/2026	27/02/2026	Actas, material divulgativo, listas de asistencia	Funcionarios sensibilizados	
Gestión de Riesgos	Actualización metodológica	Revisión y ajuste de la metodología y lineamientos de gestión de riesgos	Oficina de Sistemas	02/03/2026	31/03/2026	Metodología y lineamientos actualizados	Actualización realizada (Sí/No)	
Gestión de Riesgos	Identificación de riesgos	Definición de contexto, identificación, análisis y evaluación de riesgos SPI, SD y Continuidad	Oficina de Sistemas	01/04/2026	30/04/2026	Matriz de riesgos institucional	% procesos con riesgos identificados	
Gestión de Riesgos	Validación de riesgos	Revisión, retroalimentación y ajuste de los riesgos identificados	Oficina de Sistemas	04/05/2026	29/05/2026	Matriz de riesgos validada	% riesgos validados	
Gestión de Riesgos	Aceptación de riesgos	Aprobación de riesgos y planes de tratamiento	Oficina de Sistemas	01/06/2026	30/06/2026	Actas de aprobación, planes de tratamiento	% riesgos con plan aprobado	
Gestión de Riesgos	Publicación	Publicación de mapas de riesgos de los procesos en SIMIG	Oficina de Sistemas	01/07/2026	31/07/2026	Mapas de riesgos publicados	Publicación realizada (Sí/No)	

Gestión de Riesgos	Seguimiento al tratamiento	Seguimiento a la implementación de controles y planes de tratamiento (evidencias)	Oficina de Sistemas	03/08/2026	30/09/2026	Informes de seguimiento	% planes en ejecución	
Gestión de Riesgos	Evaluación de controles	Medición de la eficacia de controles y definición de acciones de mejora	Oficina de Sistemas	01/10/2026	30/10/2026	Informe de eficacia de controles	% controles efectivos	
Mejoramiento	Identificación de mejoras	Identificación de oportunidades de mejora según resultados del seguimiento	Oficina de Sistemas	02/11/2026	20/11/2026	Plan de mejora	Número de mejoras identificadas	
Mejoramiento	Actualización de lineamientos	Ajuste de lineamientos de riesgos según observaciones	Oficina de Sistemas	23/11/2026	18/12/2026	Lineamientos actualizados	Actualización realizada (Sí/No)	
Monitoreo y Revisión	Seguimiento de indicadores	Medición, análisis y reporte de indicadores del MSPI	Oficina de Sistemas	02/02/2026	31/12/2026	Reportes periódicos, tablero de control	Cumplimiento de indicadores (%)	

Desarrollo metodológico

Los controles definidos para el tratamiento y mitigación de los riesgos de Seguridad y Privacidad de la Información serán evaluados y contrastados frente a los requisitos y controles establecidos en la norma ISO/IEC 27001, con el propósito de identificar brechas, debilidades o falencias en la Alcaldía Municipal de San Bernardo del Viento, y establecer acciones de mejora que fortalezcan el nivel de madurez del Sistema de Gestión de Seguridad de la Información. A continuación se muestra el proceso que sigue la identificación de riesgo de la información.



Establecimiento del contexto

El establecimiento del contexto constituye una etapa fundamental dentro del proceso de gestión de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción) de la Alcaldía de San Bernardo del Viento, en la medida en que permite identificar y analizar los factores internos, externos y propios de los procesos que pueden incidir en la materialización de riesgos, este análisis contempla, entre otros aspectos, el entorno normativo, organizacional, tecnológico, operativo y humano, así como las condiciones del entorno externo que pueden afectar la confidencialidad, integridad, disponibilidad, privacidad y autenticidad de la información y la continuidad de los servicios institucionales. A partir de la definición del contexto, es posible establecer las posibles causas y fuentes de riesgo, facilitando una identificación y evaluación más precisa y coherente con la realidad de la Entidad. Para la definición del contexto, la Alcaldía adoptará las metodologías, lineamientos y herramientas dispuestas institucionalmente, en concordancia con la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información del MinTIC y los principios del estándar ISO/IEC 27001. Este enfoque permite asegurar la consistencia en el análisis de riesgos y su adecuada integración con los procesos misionales, estratégicos y de apoyo, adicionalmente, la definición del contexto estratégico contribuye al fortalecimiento del control institucional frente a la exposición al riesgo, al permitir la identificación de situaciones generadoras de riesgos y su alineación con los objetivos estratégicos, la misión y la visión de la Entidad, evitando que la gestión institucional se desarrolle en contravía de sus propósitos y compromisos con la ciudadanía.

Identificación del Riesgo

La identificación y valoración de los riesgos asociados a la Seguridad y Privacidad de la Información, la Seguridad Digital y la Continuidad de la Operación de los servicios (riesgos de interrupción) de la Alcaldía Municipal de San Bernardo del Viento se realizará de conformidad con la metodología para la administración de riesgos establecida en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, emitida por el Departamento Administrativo de la Función Pública (DAFP) y adoptada por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, así como con las tablas de probabilidad e impacto definidas para la gestión del riesgo institucional, en desarrollo de este proceso, se llevarán a cabo mesas de trabajo con los líderes y responsables de los procesos, en las cuales se analizará el contexto interno, externo y del proceso, se identificarán los riesgos y se realizará el análisis de probabilidad e impacto como valoración preliminar, con el fin de determinar el nivel de riesgo inherente.

Durante este ejercicio, se asociarán las amenazas, vulnerabilidades y consecuencias relacionadas con cada riesgo identificado, adicionalmente, se identificarán y relacionarán los controles aplicables, tomando como referencia el Anexo A de la Norma ISO/IEC 27001, con el propósito de mitigar los riesgos identificados. Para cada control se evaluarán las variables necesarias para asegurar su adecuado diseño e implementación, tales como: la asignación de responsables, la segregación de funciones y niveles de autoridad, el tipo de control (preventivo, detectivo o correctivo), la forma de implementación (manual o automatizada), la periodicidad, el propósito del control, el procedimiento de ejecución, el tratamiento de observaciones o desviaciones y la definición de las evidencias que soportan su ejecución. Asimismo, se verificará que cada control se ejecute de manera consistente y efectiva, de modo que contribuya de forma real a la mitigación del riesgo. Esta valoración se realizará conforme a las tablas, criterios y metodología definidos en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas del DAFP, garantizando la trazabilidad, coherencia y alineación del proceso de gestión de riesgos con los objetivos institucionales y los lineamientos normativos vigentes.

Valoración del Riesgo

La valoración del riesgo en el Plan de Riesgos de Seguridad y Privacidad de la Información es un proceso clave para identificar, evaluar y priorizar los riesgos asociados con la seguridad y la privacidad de la información de la alcaldía. Esta valoración permite tomar decisiones informadas para mitigar, transferir, aceptar o evitar dichos riesgos. A continuación, se describen los pasos y consideraciones clave para llevar a cabo una valoración de riesgos efectiva:

✓ **Identificación de activos**

Se deben identificar los activos de información que se quieren proteger, tales como bases de datos, sistemas informáticos, aplicaciones, infraestructuras tecnológicas y documentos confidenciales.

✓ Identificación de amenazas y vulnerabilidades

- **Amenazas**: Factores que pueden explotar las vulnerabilidades de un sistema, como ciberataques, errores humanos, desastres naturales, fallos tecnológicos, etc.
- **Vulnerabilidades**: Debilidades en los sistemas de protección que podrían ser aprovechadas por las amenazas, como contraseñas débiles, falta de cifrado de datos o protocolos de seguridad inadecuados.

- ✓ **Evaluación de la probabilidad de ocurrencia**

  Se evalúa la probabilidad de que una amenaza explote una vulnerabilidad. Esto se puede hacer utilizando escalas cualitativas (baja, media, alta) o cuantitativas (porcentaje de probabilidad).

- ✓ **Evaluación del impacto**

Se determina el impacto potencial de que una amenaza se materialice, es decir, el daño o perjuicio que causaría a los activos de información de la entidad. El impacto se puede clasificar en términos de confidencialidad, integridad, disponibilidad y reputación.

Un ataque a la confidencialidad de los datos personales podría tener un impacto grave en la reputación de la alcaldía y en la confianza de los usuarios.

- ✓ **Determinación del nivel de riesgo**

El nivel de riesgo se calcula combinando la probabilidad de ocurrencia y el impacto de un riesgo. Se puede utilizar una matriz de riesgos (baja, media, alta) para clasificar el nivel de riesgo.

- ✓ **Priorización de riesgos**

Con base en el nivel de riesgo determinado, se priorizan los riesgos a gestionar. Los riesgos con un alto impacto y alta probabilidad deben ser tratados con urgencia, mientras que los de bajo impacto o baja probabilidad pueden ser aceptados o mitigados en menor medida.

- ✓ **Definición de estrategias de mitigación**

  Para cada riesgo identificado, se debe establecer una estrategia para reducir la probabilidad de que ocurra o el impacto si se materializa. Esto puede incluir controles técnicos, organizacionales o físicos, así como la implementación de políticas de seguridad y privacidad.

- ✓ **Monitoreo y revisión**

La valoración del riesgo debe ser un proceso continuo, ya que los riesgos pueden cambiar con el tiempo debido a la evolución de las amenazas, cambios tecnológicos, o ajustes en los procesos de negocio.

Definición y Aprobación de Mapas de Riesgos y Planes de Tratamiento

De toda la información recolectada anteriormente se obtiene el Mapa de riesgos en el cual se presenta un resumen de las acciones empleadas para la identificación, análisis y evaluación de riesgos, así como de la evaluación y elección de los controles, tal como se presenta en el siguiente cuadro

PROCESO	OBJETIVO DEL PROCESO	RIESGO	TIPO DE RIESGO	CAUSA	CONSECUENCIA	PROB.	IMPACTO	ZONA DE RIESGO INHERENTE	CONTROLES EXISTENTES	ZONA DE RIESGO RESIDUAL
Planeación Institucional	Garantizar la correcta formulación y ejecución de planes institucionales	Deficiente planeación y seguimiento institucional	Estratégico	Falta de articulación entre dependencias y debilidades en seguimiento	Incumplimiento de metas del Plan de Desarrollo	3	4	ALTA	Seguimiento a planes, comités de planeación	MEDIA
Atención al Usuario	Garantizar atención oportuna y de calidad al ciudadano	Atención inoportuna o deficiente al ciudadano	Operativo	Falta de capacitación y alta demanda de solicitudes	Insatisfacción ciudadana y quejas	3	3	ALTA	Protocolos de atención y PQRSD	MEDIA
Atención al Usuario	Proteger la información de los ciudadanos	Modificación o uso indebido de datos personales	Seguridad de la Información	Gestión inadecuada de accesos y roles	Vulneración de datos y sanciones legales	3	4	EXTREMA	Roles y perfiles, monitoreo de accesos	ALTA
Gestión Financiera	Garantizar uso eficiente de recursos públicos	Uso inadecuado de recursos financieros	Financiero	Debilidades en control presupuestal	Hallazgos fiscales	2	4	ALTA	Control presupuestal y auditorías	MEDIA

ALCALDÍA MUNICIPAL
SAN BERNARDO DEL VIENTO

Gestión Contractual	Asegurar procesos contractuales transparentes	Irregularidades en contratación	Corrupción	Falta de controles y supervisión	Sanciones y pérdida de recursos	2	5	EXTREMA	SECOP, supervisión contractual	ALTA
Gestión TI	Garantizar continuidad de los servicios tecnológicos	Caída de sistemas o pérdida de información	Tecnológico	Infraestructura obsoleta o sin respaldo	Interrupción de servicios	3	4	EXTREMA	Backups, mantenimiento	ALTA

Talento Humano	**Garantizar personal idóneo y capacitado**	**Alta rotación o falta de competencias**	**Operativo**	**Contratación temporal y poca capacitación**	**Baja eficiencia institucional**	**3**	**3**	**ALTA**	**Plan de capacitación**	**MEDIA**
Gestión Documental	Asegurar correcta gestión de archivos	Pérdida o deterioro de documentos	Operativo	Manejo inadecuado de archivos	Pérdida de información	2	4	ALTA	TRD y archivo central	MEDIA
Continuidad del Servicio	Garantizar prestación continua de servicios	Interrupción de servicios críticos	Continuidad	Falta de planes de contingencia	Afectación a la comunidad	2	5	EXTREMA	Plan de continuidad	ALTA
Transparencia	Fortalecer acceso a la información pública	Incumplimiento de la Ley de Transparencia	Legal	Desactualización de información	Sanciones y pérdida de confianza	2	4	ALTA	Portal web y seguimiento	MEDIA

Materialización del Riesgo

La **materialización del riesgo** se refiere al momento en el que un riesgo previamente identificado y evaluado en un proceso de gestión de riesgos se convierte en un evento real, afectando a los activos, procesos u objetivos de la entidad. Este es el punto en el que las amenazas se concretan, y el impacto anticipado se vuelve una realidad. La materialización del riesgo puede tener efectos significativos, tanto en términos de pérdidas financieras, operacionales, legales, como en la reputación de la organización.

Factores Clave en la Materialización del Riesgo

Probabilidad de Ocurrencia: Aunque los riesgos son identificados de manera proactiva, no todos se materializan. La probabilidad de que un riesgo se materialice depende de factores internos y externos, como el entorno operativo, las medidas preventivas implementadas y la naturaleza del riesgo en sí.

- ✓ **Impacto Real**: El impacto de un riesgo materializado puede ser menor, igual o mayor que el estimado en la etapa de evaluación de riesgos. Un riesgo puede tener un impacto muy negativo en las operaciones, la reputación o finanza de una organización si no se gestionó adecuadamente.
- ✓ **Eficacia de las Medidas de Mitigación**: Las acciones tomadas para mitigar los riesgos tienen un papel crucial en determinar el grado en que un riesgo se materializa y su impacto. Si las medidas preventivas son eficaces, el impacto de la materialización del riesgo puede reducirse significativamente. Sin embargo, si las medidas son inadecuadas, el riesgo puede tener consecuencias mucho más graves.
- ✓ **Tiempo de Respuesta**: La rapidez con la que la entidad responde a la materialización del riesgo también afecta su magnitud. Una respuesta oportuna puede reducir las pérdidas y contener los efectos del evento. Esto es clave en la gestión de incidentes, como ciberataques, desastres naturales o crisis operacionales.

Oportunidad de mejora

La Alcaldía Municipal de San Bernardo del Viento no debe limitar la gestión institucional únicamente a la identificación, análisis y tratamiento de los riesgos, sino que debe concebir este ejercicio como un insumo estratégico para la identificación de oportunidades de mejora, orientadas al fortalecimiento de la gestión pública, la eficiencia administrativa y la generación de valor público.

En este sentido, el análisis y la valoración de los riesgos constituyen una herramienta fundamental para reconocer debilidades, optimizar procesos y potenciar capacidades institucionales, permitiendo transformar los escenarios de riesgo en resultados positivos para la entidad y para la ciudadanía. Por lo tanto, una oportunidad debe entenderse como la consecuencia favorable derivada de la implementación efectiva de las acciones de tratamiento del riesgo, que contribuye a mejorar el desempeño institucional.

La adecuada gestión de las oportunidades permite, entre otros aspectos:

- Fortalecer los mecanismos de control interno y la cultura organizacional orientada a la prevención.
- Optimizar los procesos misionales y de apoyo, incrementando la eficiencia y la calidad en la prestación de los servicios.
- Mejorar la transparencia, la confianza ciudadana y el cumplimiento normativo.
- Impulsar la innovación institucional mediante el uso estratégico de las Tecnologías de la Información y las Comunicaciones.
- Consolidar la mejora continua, en coherencia con los principios del MIPG y las buenas prácticas de gestión pública.

En consecuencia, la Alcaldía Municipal de San Bernardo del Viento deberá integrar la identificación de oportunidades como un componente transversal del proceso de administración del riesgo, asegurando que los resultados del tratamiento de los riesgos no solo mitiguen impactos negativos, sino que generen aprendizajes, fortalecimiento institucional y valor público sostenible, en concordancia con los objetivos estratégicos y la vigencia 2026.

Recursos

La alcaldía municipal de San Bernardo del Viento, en el marco de la gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios, debe disponer de los siguientes recursos, aunque algunos no se cuenta con ellos en la totalidad se está en proceso de mejora continua para estar a la vanguardia.

Tipo de Recurso	Descripción	Finalidad dentro del Plan de Riesgos y Privacidad
Recursos Humanos	Responsable de Seguridad y Privacidad de la Información (RSPI), equipo de TI, líderes de proceso, servidores públicos y contratistas.	Identificar, analizar, tratar y hacer seguimiento a los riesgos de seguridad y privacidad; garantizar el cumplimiento de políticas y buenas prácticas.
Recursos Tecnológicos	Infraestructura TI (servidores, redes, equipos), sistemas de respaldo, control de accesos, antivirus, firewall, herramientas de monitoreo y gestión documental.	Proteger la información frente a amenazas internas y externas, garantizar disponibilidad, integridad y confidencialidad de los activos de información.
Recursos Financieros	Presupuesto asignado para seguridad de la información, mantenimiento tecnológico, adquisición de software, contratación de servicios especializados y capacitaciones.	Asegurar la sostenibilidad del Plan, la implementación de controles y el tratamiento efectivo de los riesgos identificados.
Recursos Físicos	Áreas seguras para servidores, controles de acceso físico, archivadores, espacios de custodia documental, sistemas de protección ambiental.	Proteger la información y los activos físicos que la soportan frente a accesos no autorizados, daños o pérdidas.
Recursos Documentales y Normativos	Políticas, procedimientos, inventario de activos, mapa de riesgos, planes de continuidad, lineamientos MinTIC, normatividad de protección de datos personales.	Establecer el marco de referencia para la gestión del riesgo, el cumplimiento normativo y la mejora continua del MSPI.
Recursos de Capacitación y Sensibilización	Jornadas de formación, campañas de concienciación, material pedagógico en seguridad y privacidad de la información.	Reducir el riesgo humano, fortalecer la cultura organizacional y mejorar la apropiación de controles de seguridad.

Presupuesto

La estimación y asignación del presupuesto para el plan de tratamiento de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios identificados en la entidad, corresponderá al presupuesto Asignado por el año en vigencia del municipio, las diferentes dependencias serán responsables de contribuir con el seguimiento y control de la gestión, además de la implementación de los controles definidos y del plan de tratamiento, a continuación se muestra un estimado a tener en cuenta para cubrir la necesidad de dichos servicios anuales.

Rubro Presupuestal	Concepto	Descripción	Valor Estimado
Talento humano	Liderazgo y gestión MSPI	Dedicación parcial del RSPI, apoyo del equipo TI y líderes de proceso.	$8.000.000
Capacitación y sensibilización	Formación en seguridad y privacidad	Capacitaciones en MSPI, protección de datos personales, gestión de riesgos y buenas prácticas.	$6.000.000
Herramientas de seguridad informática	Software de seguridad	Antivirus corporativo, firewall básico, control de accesos, actualizaciones de seguridad.	$10.000.000
Respaldo y recuperación de información	Backups y almacenamiento	Soluciones de copias de seguridad, almacenamiento externo o en la nube y pruebas de restauración.	$7.000.000
Infraestructura tecnológica	Mantenimiento y renovación	Mantenimiento preventivo de servidores, red y equipos críticos.	$12.000.000
Servicios especializados	Auditoría y asesoría	Auditoría MSPI, análisis de riesgos, pruebas básicas de seguridad o acompañamiento especializado.	$9.000.000
Gestión documental y continuidad	Documentación y planes	Actualización de políticas, procedimientos, planes de continuidad y respuesta a incidentes.	$5.000.000
Controles físicos	Seguridad física de la información	Adecuación de áreas seguras, controles de acceso físico, archivadores y custodia documental.	$6.000.000
Total		**$63.000.000**	

Medición

La medición del Plan de Seguridad y Privacidad de la Información permite evaluar de manera sistemática el desempeño, la efectividad y el nivel de madurez de los controles implementados en la entidad, en concordancia con el Modelo de Seguridad y Privacidad de la Información – MSPI del MinTIC, la ISO/IEC 27001 y la Guía para la Administración del Riesgo del DAFP, este componente constituye un insumo fundamental para la toma de decisiones, la mejora continua y el fortalecimiento de la gestión de riesgos de seguridad y privacidad de la información en la Alcaldía Municipal de San Bernardo del Viento.

Dimensión MSPI	Indicador	Qué mide	Meta 2026	Frecuencia
Gestión del Riesgo	Riesgos de seguridad tratados	Nivel de ejecución del plan de tratamiento de riesgos	≥ 90 %	Trimestral
Incidentes	Incidentes de seguridad gestionados	Atención oportuna de incidentes reportados	≥ 95 %	Mensual
Controles	Controles de seguridad implementados	Grado de implementación de controles definidos	≥ 90 %	Trimestral
Cumplimiento	Cumplimiento normativo	Adherencia a políticas, normas y lineamientos	≥ 95 %	Semestral
Capacitación	Funcionarios capacitados	Nivel de sensibilización en seguridad	≥ 85 %	Semestral
Disponibilidad	Servicios críticos disponibles	Continuidad de los servicios de información	≥ 99 %	Mensual
Mejora continua	Acciones de mejora ejecutadas	Implementación de acciones correctivas	≥ 90 %	Anual

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 2025**	**Actualización del Plan por cambio a vigencia 2026**	**Oficina TIC**