ALCALDIA MUNICIPAL DE SAN BERNARDO DEL VIENTO

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

Tabla de versiones

Versión	Fecha	Autor
1.0 – Versión final 2021	29 de enero de 2021	Oficina TIC

TABLA DE CONTENIDO

INTRODUCCIÓN

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, frente a los riesgos que sufre la información. Desde la alcaldía de San Bernardo del Viento, promovemos la protección de nuestros activos de información en cualquiera de sus estados ante una serie de posibles amenazas que atenten contra la confidencialidad, integridad y su disponibilidad, a través de la implementación de medidas de control de seguridad de la información, que permitan gestionar y reducir los riesgos e impactos a que está expuesta.

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información 2021 - 2023, busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad.

Lo anterior dando cumplimiento a la normativa establecida por el estado colombiano, CONPES 3854 de 2016, Modelo de Seguridad y Privacidad de MINTIC y lo establecido en el decreto 1008 de 14 de junio 2018, adoptando las buenas prácticas y los lineamientos de los estándares ISO 27001:2013, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 emitida por el DAFP.

La Alcaldía de San Bernardo del Viento 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 Entidad confidencial, integra y disponible, a través de su ciclo de vida desde su captura, almacenamiento, explotación, hasta su eliminación.

Objetivo General

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, tiene como objetivo brindar a la Alcaldía de San Bernardo del Viento una herramienta que proporcione las pautas necesarias para el adecuado tratamiento de los riesgos a los que están expuestos los activos de información, que permitan una adecuada gestión de los riesgos que en materia de seguridad y privacidad de la información sea necesario sobre los activos de información y la toma de decisiones para disminuir la probabilidad que se materialice una amenaza o bien reducir la vulnerabilidad del sistema o el posible impacto en la Entidad, así como permitir la recuperación del sistema y la estabilidad operativa y funcional del mismo.

Objetivos Específicos

- Consolidar una administración de riesgos acorde con las necesidades de la Alcaldía de San Bernardo del Viento como entidad pública.

- Definir los principales activos a proteger en la Alcaldía de San Bernardo del Viento

- Proteger los activos de información de acuerdo a su clasificación y criterios de Confidencialidad, Integridad y Disponibilidad

- Crear conciencia a nivel institucional de la importancia y la necesidad de una correcta gestión del riesgo de seguridad de la información.

Alcance del documento

El alcance del Plan de Seguridad y Privacidad de la Información 2021 – 2023 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 2020 - 2023 “Comprometidos contigo”. 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. Teniendo como base la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016): se dan los lineamientos para poder identificar, analizar, tratar, evaluar y monitorear los riesgos de seguridad y privacidad de la información en la alcaldía de San Bernardo del Viento.

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.

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. Además de los de seguridad y privacidad de la Información y Seguridad Digital de manera Integral.

Se deben tener en cuenta alguna de las siguientes opciones, las cuales pueden considerarse independientemente, interrelacionadas o en conjunto:

- **Evitar**: es eliminar la probabilidad de ocurrencia o disminuir totalmente el impacto, lo que requiere la eliminación de la actividad o fuente de riesgo, eliminar la exposición y su expresión máxima es dejar una actividad. Por ejemplo, para evitar perdida de documentación se prohíbe el ingreso a un área.
- **Prevenir**: corresponde al área de planeación, esto es, planear estrategias conducentes a que el evento no ocurra o que disminuya su probabilidad. Un ejemplo de ello son las inspecciones el mantenimiento preventivo, las políticas de seguridad o las revisiones periódicas a los procesos.
- **Reducir o mitigar**: corresponde a la protección en el momento en que se presenta el riesgo se encuentra en esta categoría los planes de emergencia planes de continencia equipos de protección personal, ambiental, de acceso mantener copias de respaldo.

El incumplimiento de la política de Seguridad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la entidad, en cuanto a Seguridad de la Información se refiere.

Metodología de evaluación de riesgos de seguridad de la información

La metodología de gestión de riesgos de seguridad de la información está alineada con la norma ISO/IEC 31000 y en la ISO 27005. Las actividades que hacen parte de la metodología, son las siguientes:

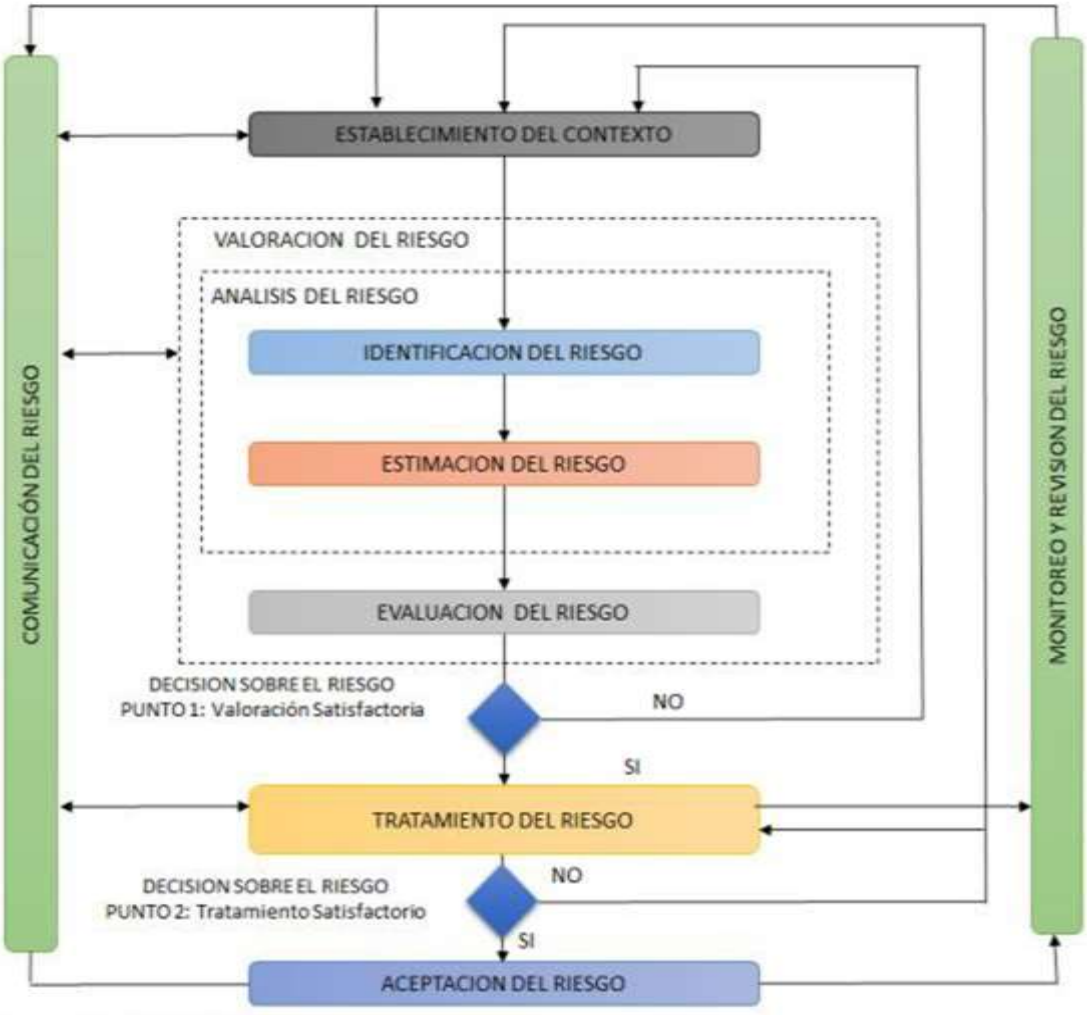

Imagen 1: VISION PROCESO DE RIESGOS DE SEGURIDAD

Tomado de la norma ISO/IEC 27005

Identificación de riesgos

El objetivo de esta etapa es identificar los principales riesgos críticos a los cuales se encuentran expuestos los procesos de la Agencia. Los encargados de Riesgos identificarán, para los procesos de su responsabilidad, los riesgos críticos que pudieran afectar los objetivos y/o estrategias definidas para el área. Dicha identificación puede ser realizada a través de los siguientes

métodos:

- Reuniones o con el equipo de trabajo.
- Encuestas a los distintos participantes del equipo de trabajo.
- Bases de datos o matices de riesgo de ejercicios previos.
- Una vez Identificados los riesgos críticos, estos se deben documentar en una matriz de riesgos, clasificándolos por tipo de riesgo de acuerdo con lo siguiente:
- Estratégico: Riesgo relacionado con los objetivos estratégicos, alineados con la misión de la
- Agencia.
- De Imagen: Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la
- Agencia.
- Financieros: Riesgo relacionado con el uso eficaz y eficiente de los recursos financieros.
- Operacional: Riesgo resultante de deficiencias o fallas en procesos, personas, sistemas o eventos externos.
- Tecnológicos: Están relacionados con la capacidad tecnológica de la Alcaldía de San Bernardo del Viento para
- satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.
- Cumplimiento: Riesgo relacionado con el cumplimiento de leyes y regulaciones, especialmente concierne al cumplimiento de aquellas leyes y normas a las cuales la Alcaldía de San Bernardo del Viento está sujeta.

Valorización de los riesgos

El objetivo de este paso es generar una lista completa de los riesgos sobre la base de los acontecimientos que puedan crear, mejorar, prevenir, degradar, acelerar o retrasar la consecución de los objetivos de la Agencia. Las debilidades de los procesos en cuanto a seguridad de la información, los riesgos a los cuales se encuentran expuestos y las causas que podrían comprometer la confidencialidad, integridad y disponibilidad de los procesos de la ANI deben ser identificadas y evaluadas teniendo en cuenta los criterios de evaluación definidos. En este proceso se debe realizar las siguientes actividades:

- Identificar el flujo de información de cada uno de los procesos
- Identificar las vulnerabilidades que existen en el proceso.
- Identificar las amenazas que podrían materializarse, dadas las vulnerabilidades existentes.
- Definir las escalas a utilizar

Proceso → Objetivo Proceso → Identificación de Activo → Riesgo

↓

Causa (Amenazas y Vulnerabilidades)

↓

Descripción del Riesgo

↓

Efectos de la Materialización del Riesgo

De acuerdo con los Lineamientos para la gestión de riesgos digital en entidades públicas emitida por el DAFP, se podrán identificar los siguientes

tres (3) riesgos inherentes de seguridad digital:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Para cada riesgo, se deben asociar el grupo de activos o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. A continuación, se mencionan un listado de amenazas y vulnerabilidades que podrían materializar los tres (3) riesgos previamente mencionados:

- **Identificación de Amenazas**

Se plantearán un listado de amenazas, que representan situaciones o fuentes que pueden hacer daño a los activos y materializar los riesgos.

AMENANA	TIPO
Polvo, Corrosión	**Evento natural**
Inundación	**Evento natural**
Incendios	**Evento natural**
Fenómenos Sísmicos	**Evento natural**
Perdida en el suministro de energía	**Daño Físico**
Espionaje remoto	**Acciones no autorizadas**
Ingeniería social	**Acciones no autorizadas**
Intrusión	**Acciones no autorizadas**
Acceso forzado al sistema	**Acciones no autorizadas**
Manipulación del Hardware	**Acciones no autorizadas**
Manipulación con Software	**Acciones no autorizadas**
Fallas del equipo	**Fallas técnicas**
Saturación del sistema de información	**Fallas técnicas**

Identificación de las Vulnerabilidades.

VULNERABILIDADES	DESCRIPCIÓN
Fácil acceso a las dependencias o Secretarías.	**No existe un control para el acceso de las personas no autorizadas a las secretarías.**
Falta de dispositivos de seguridad biométrica para acceso a las secretarias de alto riesgo.	**El dispositivo de seguridad biométrica reduce el riesgo de robo de información o equipos electrónicos por fácil acceso.**
Falta de Aplicación de la Política de escritorio limpio	**La política de escritorio limpio, es implementada para que los funcionarios no dejen expuestos: documentos, equipos electrónicos u objetos de valor, sobre los escritorios, que pueden ser robados fácilmente.**
Falta de máquina trituradora de papel	**La máquina trituradora de papel, evita que las personas arrojen documentos importantes con información personal a la basura, que puedan ser usados para crear perfiles de ataque.**
Falta de Capacitación de los funcionarios en temas de seguridad Informática.	**El eslabón más débil en términos de seguridad informática son los funcionarios, dado que no tienen conocimiento sobre las amenazas y riesgos que enfrentan y como poder mitigarlos.**
Falta de equipos electrónicos para copias de respaldo.	**El no contar con un HDD externo, impide a los realizar copias de respaldo o Back ups**
Falta de equipos institucionales.	**El no contar con suficientes equipos institucionales, lleva a los funcionarios a traer equipo personal que pueden afectar el funcionamiento de la red o infectarla. Adicionalmente promueve el compartir cuentas de usuarios y claves que pueden afectar al prestador**
Red	**Tráfico sensible sin protección**

Análisis del Riesgo de Seguridad de la Información

El análisis está basado en los flujos de información de cada uno de los procesos y los requerimientos de seguridad, tomando en cuenta los controles existentes. En esta etapa se definen los criterios que se deben utilizar para evaluar la importancia del riesgo. Los criterios reflejarán los valores de la Alcaldía de San Bernardo del

Viento, los objetivos y los recursos existentes.

TABLA DE PROBABILIDAD			
NIVEL	**PROBABILIDAD**	**DESCRIPCIÓN**	**FRECUENCIA**
5	Siempre	El evento ocurrirá en la mayor parte de las circunstancias	**Ocurre más de una vez al mes**
4	Muy probable	Se espera que el evento ocurra en la mayor parte de las circunstancias	**Ocurre más de una vez al año**
3	Probable	El evento debe ocurrir en algún momento	**Ocurre menos de una vez al año**
2	Poco Probable	El evento debería ocurrir en algún momento	**Ocurre más de una vez cada cinco años**
1	**Raro**	**El evento debe ocurrir, pero solo en circunstancias excepcionales**	**El evento ocurre rara vez**

TABLA DE IMPACTO		
NIVEL	**DESCRIPTOR**	**DESCRIPC ION**
5	Catastrófico	**Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad**
4	Mayor	**Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad**
3	Moderado	**Si el hecho llegara a presentarse, tendría medianas consecuencias o efecto sobre la entidad**
2	Menor	**Si el hecho llegara a presentarse, tendría bajo impacto o efecto mínimos sobre la entidad**
1	**Insignificante**	**Si el hecho llegara a presentarse, tendría consecuencias mínimas sobre la entidad**

Actividades

ACTIVIDAD	DESCRIPCIÓN	FECHA
Diagnóstico	Realizar diagnóstico del estado actual	**Enero a Marzo 2021**
Actualización de lineamientos de riesgos	Actualizar política y metodología de gestión del riesgo	**Marzo a Diciembre 2021**
Sensibilización	Socialización de gestión de riesgos de seguridad y privacidad de la información	**Abril a Mayo 2021**
Actualización de riesgos identificados	Identificación y actualización de los riesgos de seguridad y privacidad de la información	**Abril a Septiembre 2021**
Aceptación de riesgos identificados	Aceptación de riesgos identificados y planes de tratamiento	**Junio a Noviembre 2021**
Seguimiento a tratamientos	Seguimiento de estado de planes de tratamiento de riesgos identificados	**Junio a Diciembre 2021**
Evaluación de riesgos residuales	Evaluación de riesgos residuales	**Julio a Diciembre 2021**
Mejoramiento	Identificación de oportunidades de mejoras acorde a los resultados obtenidos en la evaluación	**Julio a diciembre 2021**
Monitoreo y revisión	**Generación, presentación y reporte de indicadores**	**Julio a diciembre 2021**

Estrategias en el tratamiento de riesgos

Las estrategias en el tratamiento de riesgos consisten en minimizar la probabilidad de materialización del riesgo. Para ello, se puede evidenciar cuatro opciones

Transferir	Son procedimientos que permiten eliminar el riesgo por medio de la transferencia.
Mitigar	**Permite reducir la probabilidad de ocurrencia del riesgo o reducir sus consecuencias. La probabilidad de ocurrencia de un riesgo puede reducirse a través de controles de gestión, políticas y procedimientos encaminados a reducir la materialización del riesgo.**
Evitar	**Puede evitarse el riesgo no procediendo con la actividad que incorporaría el riesgo, o escoger medios alternativos para la actividad que logren el mismo resultado y no incorporen el riesgo detectado.**
Aceptar	**consiste en hacer frente a un riesgo (positivo o negativo) o porque no se ha identificado ninguna otra estrategia de respuesta adecuada.**

Términos y definiciones

Activo: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

Aceptación de riesgo: Decisión de asumir un riesgo

Amenazas: situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

Análisis de Riesgo: Uso sistemático de la información para identificar fuentes y estimar el riesgo (Guía ISO/IEC 73:2002). Apetito al riesgo: magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener.

Causa: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

Confidencialidad: propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

Consecuencia: los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Control: medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

Disponibilidad: propiedad de ser accesible y utilizable a demanda por una entidad.

Dueño del riesgo sobre el activo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

Evaluación del riesgo: Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

Factor de riesgo: Agente ya sea humano o tecnológico que genera el riesgo.

Gestión del riesgo: proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Impacto: Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Integridad: propiedad de exactitud y completitud.

Mapa de riesgos: documento con la información resultante de la gestión del riesgo.

Probabilidad: se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.

Riesgo: Efecto de la incertidumbre sobre el cumplimiento de los objetivos.

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.

Riesgo Inherente: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.

Riesgo residual: Nivel restante de riesgo después del tratamiento del riesgo.

Tratamiento del riesgo: Proceso de selección e implementación de acciones de mejorar que permitan mitigar el riesgo.

Tolerancia al riesgo: son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable.

Valoración del riesgo: Proceso de análisis y evaluación del riesgo.

Vulnerabilidad: La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.