Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Alcaldía municipal de San Bernardo del Viento

Presentación

La alcaldía de San Bernardo del viento debe definir las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma a través de la implementación del plan de tratamiento de riesgos de seguridad de la información, en el cual se identifica el conjunto de controles a aplicar para llevar cada uno de los riesgos a un nivel tolerable para la entidad. Es por esto que se debe lograr en el marco de 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, emitida por el DAFP.

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.

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, el Modelo Integrado de Gestión – MIG del 28 de diciembre de 2023. 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.

El Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia establece que la seguridad de la información es un elemento que apoya a las entidades de manera trasversal, habilitando el desarrollo de los componentes de la política de Gobierno Digital, desarrollado a través de lineamientos en materia de seguridad y privacidad de la información, así como de gestión de riesgos de seguridad digital, lo cuales soportan las acciones establecidas por cada entidad para proteger los activos de información, preservando la confidencialidad, integridad, disponibilidad y privacidad de los datos. El Manual de la política de Gobierno Digital expedido por el Ministerio de Tecnologías de información y de las Comunicaciones entre sus propósitos pretende lograr procesos internos seguros y eficientes a través del fortalecimiento de las capacidades de gestión de tecnologías de información, que consiste en desarrollar procesos y procedimientos que hagan uso de las tecnologías de la información, a través de la incorporación de esquemas de manejo seguro de la información y de la alineación con la arquitectura institucional de la entidad (Arquitectura misional y Arquitectura de TI), a fin de apoyar el logro de las metas y objetivos de la entidad. En ese sentido, teniendo en cuenta el nuevo concepto de Gobierno Digital acorde con lo establecido en el Modelo de Seguridad y Privacidad de la Información – MSPI, Controles de Seguridad y Privacidad de la Información, se estipulan los lineamientos del presente plan

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.
- ✓ **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.

Objetivos

Objetivo general

Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción) a los que Alcaldía de San Bernardo del viento pueda estar expuesta, y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad, privacidad y autenticidad de la información.

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.
- ✓ Cumplir con los requisitos legales, reglamentarios, regulatorios y de las normas técnicas colombianas en materia de seguridad y privacidad de la información, seguridad digital y protección de la información personal.
- ✓ Gestionar riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios, de acuerdo con los contextos establecidos en la Entidad.
- ✓ Fortalecer y apropiar conocimiento referente a la gestión de riesgos 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.

Alcance

Realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios, 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. Adicionalmente dar 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.

Junto con 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 municipal de San Bernardo del Viento.

El Plan de Tratamiento de Riesgo tendrá en cuenta los riesgos que se encuentren en los niveles Moderado, Alto y Extremo acorde con los lineamientos definidos por la alcaldía municipal de San Bernardo del Viento, los riesgos que se encuentren en niveles inferiores serán aceptados por la Entidad.

Creando así una línea base del tratamiento de riesgos en la alcaldía municipal de San Bernardo del viento, facilitando la identificación de los riesgos que se encuentran presentes en la entidad; de la misma manera los funcionarios conozca el proceso de mitigación de riesgos para lograr minimizar la pérdida de información o daños en los equipos.

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

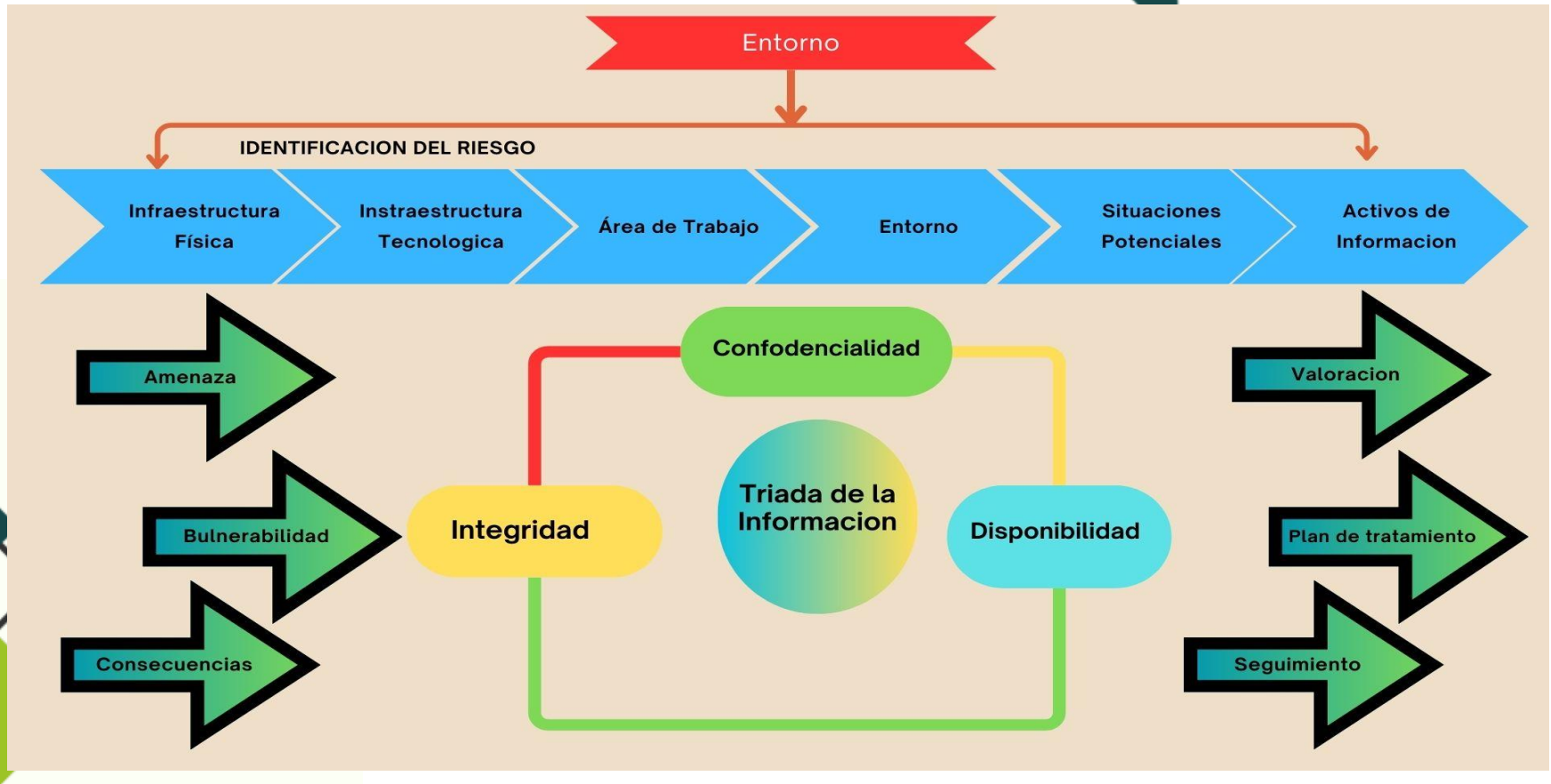
El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos de información de los diferentes procesos de la Alcaldía de San Bernardo de viento, estas actividades se estructuraron de la siguiente manera, siguiendo las recomendaciones 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	
				Inicio	**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	Oficina de sistemas	03/02/25	**28/02/25**
	Actualizar políticas y metodologías	Revisar y ajustar metodología para la gestión de Riesgo de Seguridad Digital Y lineamientos de riesgo	Oficina de sistemas	03/03/25	**31/02/25**
	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	Oficina de sistemas	01/04/25	**30/04/25**
		Realimentación, revisión y verificación de los riesgos identificados (Ajustes)	Oficina de sistemas	01/05/25	**31/05/25**
	Aceptación de Riesgos Identificados	Aceptación, aprobación riesgos identificados y planes de tratamiento	Oficina de sistemas	02/06/25	**30/06/25**
	Publicación	Publicación mapas de riesgos de los procesos en SIMIG	Oficina de sistemas	01/07/25	**31/07/25**
	Seguimiento Fase de Tratamiento	Seguimiento implementación de controles y planes de tratamiento de riesgos los identificados (verificación de evidencias)	Oficina de sistemas	01/08/25	**01/08/29**
	Planificación de controles	Medición de la eficacia de los controles, Mejoramiento	Oficina de sistemas	01/09/25	**30/09/25**
	Mejoramiento	Identificación de oportunidades de mejora acorde al seguimiento de la ejecución de los controles y de los planes de tratamiento	Oficina de sistemas	01/10/25	**31/10/25**
		Revisión y/o actualización de lineamientos de Riesgos de Seguridad y privacidad de la información de acuerdo con las observaciones identificadas.	Oficina de sistemas	03/11/25	**28/11/25**
	Monitoreo y Revisión	**Medición, presentación y reporte de indicadores**	**Oficina de sistemas**	**03/02/25**	**31/12/25**

Tabla: Actividades a desarrollar en aras de mitigar los riesgos

Desarrollo metodológico

Los controles seleccionados para mitigar los riesgos de Seguridad y Privacidad de la Información serán confrontados con los estándares ISO 27001; a fin de determinar las falencias de la alcaldía en este sentido.



Establecimiento del contexto

El contexto en términos generales relaciona los aspectos externos, internos y del proceso que se deben tener en cuenta para gestionar los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios (riesgos de interrupción) de la alcaldía. A partir del contexto es posible establecer las posibles causas de los riesgos a identificar. De esta forma para la definición del contexto se seguirán las metodologías dispuestas en la entidad para lograr establecer las posibles causas y determinar la identificación de los riesgos, además definir el contexto estratégico contribuye al control de la entidad frente a la exposición del riesgo ya que permite conocer las situaciones generadoras de riesgos, impidiendo con ello que la Entidad actúe en dirección contraria a sus propósitos institucionales

Identificación del Riesgo

La valoración de los 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 se realizará acorde a la metodología para la administración de riesgos mencionada 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 y adoptada por el Ministerio para la gestión del riesgo y las tablas de impacto definidas para el Ministerio.

Es así como en mesas de trabajo con los procesos se analiza el contexto, se identifican los riesgos y se realiza el análisis de la probabilidad e impacto como valoración preliminar para identificar el nivel del riesgo inherente, asociando sus amenazas, vulnerabilidades y consecuencias e identificando los controles asociados al anexo A de la Norma ISO 27001 para mitigarlas. A estos controles se le identifican las variables a evaluar para su adecuado diseño como son: la asignación de un responsable, segregación y autoridad del responsable, tipo de control (preventivo, defectivo o correctivo), implementación (manual o automático), periodicidad, propósito, cómo se realiza la actividad de control, qué pasa con las observaciones o desviaciones y la evidencia de la ejecución del control. Adicionalmente se evalúa que cada control se ejecute de manera consistente, de tal forma que pueda mitigar el riesgo. Esta valoración se realiza de acuerdo con las tablas y metodología establecida y mencionada en la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP.

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

MAPA DE RIESGOS											
PROCESO: ATENCIÓN AL USUARIO											
OBJETIVO: Dar trámite oportuno a las solicitudes provenientes de las diferentes partes interesadas, Permitiendo atender las necesidades y expectativas de los usuarios, todo dentro de una cultura de servicio y de acuerdo a las disposiciones legales vigentes.											
RIESGO	**CALIFICACIÓN**		**Evaluación**	**CONTROLES**	**NUEVA CALIFICACIÓN**		**Evaluación**	**Medidas de Respuesta**	**ACCIONES**	**RESPONSABL E**	INDICAD**OR**
	Prob	**Impa**	**Zona de Riesgo**		**Prob**	**Imp**			**Zona de Riesgo**		
Cambio en los datos de contacto de los usuarios	3	4	EXTR EMA	Procedimientos establecidos para la asignación de Roles y Perfiles dentro del sistema **Herramienta que permita el registro y monitoreo de acciones de los usuarios sobre sistema**	3	4	ALTA	Reducir el Riesgo Evitar Compartir o Transferir	Capacitación al nuevo personal que asigna usuarios sobre el sistema . **Inclusión de alarmas ante anomalías.**	Áreas responsables del manejo del sistema - Área de tecnología	**Nuevo personal vinculado VS Usuarios formados y conocedores de los procedimient os.** **Número de solicitudes de usuario vs Cantidad de alarmas sobre el sistema**

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 sólo deberá centrarse en los riesgos identificados, sino que este análisis o apreciación del riesgo debe ser la base para identificar oportunidades. Por lo anterior la oportunidad deberá entenderse como la consecuencia positiva frente al resultado del tratamiento del Riesgo.

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, dispone de los siguientes recursos.

RECURSOS	VARIABLE
Humanos	La Oficina de Tecnologías de la información a través de seguridad de la información es responsable de coordinar, implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos en la Entidad en lo concerniente a la seguridad y privacidad de la información lo cual contribuye a la mejora continua.
Técnicos	Guía de Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 -octubre de 2018 del DAFP. Herramienta para la gestión de riesgos (Matriz de Riesgos SGSI) , ISO 27005, Magerit
Logísticos	Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.
Financieros	Recursos para la adquisición de conocimiento, recursos humanos, técnicos para los controles producto de la gestión de riesgos

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.

Medición

La medición se realiza con un indicador de gestión, está orientada principalmente en la medición de eficacia de los componentes de implementación y gestión definidos en el modelo de operación del marco de seguridad y privacidad de la información, indicador que se alimenta de indicadores internos en el marco de la implementación del Eje de Seguridad de la Información y que servirán como insumo para el componente de mejora continua permitiendo adoptar decisiones de mejora sobre Seguridad de la informa.

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**