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

ALCALDÍA DE SIBATÉ

2024

TABLA DE CONTENIDO

INTRODUCCIÓN

En línea con la política digital del Estado colombiano que tiene como objetivo fomentar la utilización y aprovechamiento de las tecnologías de la información y las comunicaciones, con el fin de fortalecer el Estado promoviendo ciudadanos competitivos, proactivos e innovadores, capaces de generar valor público en un entorno basado en la confianza digital. La Alcaldía Municipal de Sibaté el presente plan de gestión de riesgos de Seguridad y Privacidad de la Información engloba las medidas diseñadas para mitigar los riesgos de Seguridad Digital que exceden el umbral aceptable de la Alcaldía Municipal de Sibaté. Su efectividad se determina mediante el producto de la probabilidad de ocurrencia y el impacto causado o potencial de las amenazas que explotan las vulnerabilidades de los activos de seguridad digital de la Alcaldía.

1. GLOSARIO

- Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)
- Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).
- Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- Confidencialidad: Propiedad que determina que la información está disponible ni sea revelada a quien no esté autorizado (2.13 ISO 27000)
- Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o

privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

- Disponibilidad: Propiedad que la información sea accesible y utilizable por solicitud de los autorizados (2.10 ISO 27000)
- Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
- Integridad: Propiedad de salvaguardar la exactitud y el estado completo de los activos (2.36 ISO 27000)
- Partes interesadas (Stakeholder): Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad
- Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación
- Procedimiento: Sucesión cronológica de acciones concatenadas entre sí, para la realización de una actividad o tarea específica dentro del ámbito de los controles de Seguridad de la Información.
- Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

2. OBJETIVO

Definir un conjunto de directrices para contribuir a la mitigación y manejo de los riesgos asociados a la seguridad y privacidad de la información en relación con los activos de información que maneja la Alcaldía Municipal de Sibaté. Estas directrices están orientadas a preservar la confidencialidad, integridad y disponibilidad de la información institucional, considerando el contexto organizacional, las capacidades y recursos disponibles. Con el fin de fortalecer la confianza de los ciudadanos, usuarios, socios y otras partes interesadas.

2.1 OBJETIVOS ESPECIFICOS

- Generar una cultura organizacional sobre la importancia de la adopción del plan de tratamiento de riesgos de seguridad y privacidad de la información
- Desarrollar un plan de trabajo para la implementación del plan de tratamiento de riesgo de seguridad y privacidad de la información.
- Aplicar las metodologías del Departamento Administrativo de la Función Pública – DAFP, específicamente en la aplicación en seguridad y riesgo de la información.

3. RECURSOS NECESARIOS (Humanos, técnicos y financieros)

- **Humano**: Disponibilidad de apropiación e integración por parte del alcalde municipal, secretarios de despacho, jefes de oficinas, líderes de procesos y personal de la oficina TICs.
- **Físico**: Servidores, Firewall, PC y equipos de comunicación.
- **Financiero**: Inclusión de recursos en el Plan Anual de Adquisiciones.

4. RESPONSABLES

- Alcalde municipal
- Secretarios de despacho y jefes de oficina
- Líderes de los proceso
- Personal de la oficina TICs

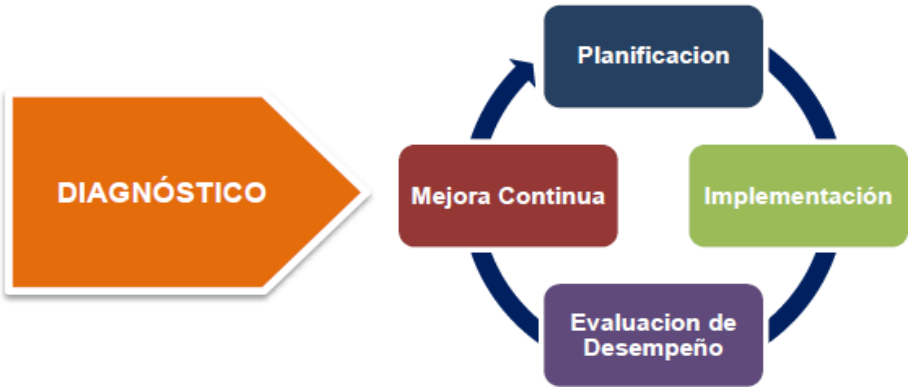
5. METODOLOGÍA DE IMPLEMENTACIÓN

Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información en la Alcaldía Municipal de Sibaté, se toma referencia la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Modelo de Implementación (versión 3.02) del Ministerio de Tecnologías de la Información y las Comunicaciones – MSPI – y la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas emitida por el DAFP

Se definieron las fases de implementación que se deben aplicar para asegurar una correcta mitigación de riesgos de exposición de información.

1. Diagnosticar
2. Planear
3. Hacer
4. Verificar
5. Actuar

Ilustración ciclo de operación del Modelo de Seguridad y Privacidad de la Información



Fuente: Manual Modelo de seguridad y Privacidad de la Información – MINTIC, consultado en https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

6. ACTIVIDADES PARA LA IMPLEMENTACIÓN

1. Realizar un diagnóstico del nivel de seguridad y riesgos de exposición de información.
2. Implementar políticas enfocadas a la seguridad de la información orientadas en el presente plan.
3. Revisar y establecer el alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información
4. Realizar un inventario de activos de Información con los líderes de cada proceso. Es válido aclarar que se cuenta con el inventario de activos de las bases de datos que hacen parte de la Administración Municipal.
5. Realizar la valoración de los activos de información con los líderes de cada proceso
6. Formular el Plan de tratamiento de los riesgos (Riesgo Inherente y Riesgo Residual)
7. Socializar el Plan de Tratamiento de Riesgo de seguridad y privacidad de la información
8. Realizar seguimiento del Plan de Tratamiento de Riesgo de seguridad y privacidad de la información.

Ítem	Nombre sistema de información y/o aplicativo	Usuario y/o área	Nombre de los reportes que genera el sistema y/o documentos	Destinatario y/o usuario de los reportes
1	Ventilla única de correspondencia municipal	Archivo y Correspondencia	Reporte de correspondencia recibida por terceros y planilla de distribución de correspondencia	Toda la administración municipal de Sibaté
2	Correspondencia interna	Sec. General y oficina de las Tic	Reporte de correspondencia enviada y recibida	Usuarios de la Secretaría General
3	Asignación de citas comisaria de familia	Comisaría de familia	Cuantifica por días y por mes la cantidad de citas asignadas en un determinado turno y con clasificaciones	Usuarios de atención a la Comisaria de Familia
4	Soporte Web Control de Ingresos	Sistemas	Reporte de la cantidad de ingresos registrados por los usuarios	Funcionarios de la Alcaldía de Sibaté
5	Predial	Área de impuestos	* Estado de cuenta para el contribuyente. * Informe detallado de ingresos por punto de recaudo y fecha. * Informe consolidado de ingresos por fecha * Cartera detallada por contribuyente * Cartera acumulada por vigencias	• Contribuyente de Predial • Área Financiera • Profesional Universitario • Secretario/a de Hacienda
6	Recaudos	Área de impuestos	• Informe de pagos realizados por los contribuyentes • Informe detallado de ingresos por punto de recaudo y fecha • Informe consolidado de ingresos por fecha	• Contribuyente de predial • Área Financiera • Director de Tesorería e Impuestos • Secretario/a de Hacienda
7	Contabilidad	Área Financiera	• Órdenes de pago • Comprobantes de Egreso Certificaciones de retenciones	•Terceros •Área Financiera •Profesional

Ítem	Nombre sistema de información y/o aplicativo	Usuario y/o área	Nombre de los reportes que genera el sistema y/o documentos	Destinatario y/o usuario de los reportes
			* Resumen de cuentas movidas Informes mensuales (Certificados Rete fuente, Industria y Comercio, Certificado de Rete IVA, relación de Egresos, Certificado de Ingresos y Retenciones, Relación de Estampillas, Declaración de Retención en la Fuente) * Informes anuales auxiliar contable • Informes Ocasionales (Plan de cuentas, Documentos sin CC, Movimientos sin afectación presupuestal, indicadores de Tesorería) • Caja Diarios • Relación de documentos presupuestales • Trazabilidad presupuestal • Informe Balance (Libro Mayor y Balance, Balance General, Estado de Resultados, Balance de prueba por tercero)	* Secretario/a de Hacienda * Entes de control y vigilancia

8	Presupuesto	Área Financiera	* Ejecución Presupuestal * Libro Ordenador del Gasto * Relación documentos presupuestales * Resumen de pagos por rubros * Certificado de disponibilidad presupuestal.	* Terceros * Área Financiera * Profesional Universitario * Secretario de Hacienda * Entes de control y vigilancia.

Ítem	Nombre sistema de información y/o aplicativo	Usuario y/o área	Nombre de los reportes que genera el sistema y/o documentos	Destinatario y/o usuario de los reportes
9	Tesorería	Área Financiera	* Libros Auxiliares * Conciliaciones * Relación de Comprobantes de Ingresos - Egresos * Informe de recaudos de terceros * Informe traslado de fondos * Informe de notas de contabilidad y bancarias	* Terceros * Área Financiera * Profesional Universitario * Secretario de Hacienda * Entes de control y vigilancia
10	Complementarios	Área de impuestos	* Reporte de la liquidación emitida por las diferentes dependencias * Informe detallado por fecha de los ingresos * Informe consolidado por fecha de los ingresos.	* Terceros * Entidad Financiera * Área Financiera * Profesional Universitario * Secretario de Hacienda
11	Industria y Comercio	Área de impuestos	* Estado de cuenta para el contribuyente * Informe detallado por fecha de los ingresos * Informe detallado de cartera	* Contribuyente de industria y comercio * Entidad Financiera * Área Financiera * Profesional Universitario * Secretario de Hacienda

7. CUMPLIMIENTO DE IMPLEMENTACIÓN

De acuerdo con las fases mencionadas anteriormente, se describe a continuación los dominios que se deben desarrollar y los plazos de implementación de acuerdo a lo establecido por la Alcaldía Municipal de Sibaté

- Implementar la Política de Seguridad de la información.
- Implementar la Política de Administración de datos.
- Implementar la Políticas de Comunicaciones.
- Aspectos organizativos de la seguridad de la información
- Seguridad de la Información enfocada a los recursos humanos
- Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas
- Revisión de los Controles de acceso
- Seguridad Física y del entorno
- Seguridad en las telecomunicaciones
- Gestión de Incidentes de Seguridad de la Información
- Aspectos de seguridad de la información en la gestión de continuidad del negocio

8. CRONOGRAMA

No.	ACTIVIDAD	RESPONSABLE	FECHA DE IMPLEMENTACIÓN
1	Realizar diagnóstico	Profesional Universitario y/o apoyo	Septiembre de 2024
2	Implementar políticas enfocadas a la seguridad de la información.	Profesional Universitario TICS	Octubre de 2024
3	Elaborar el alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información	Contratista de apoyó TICs	Octubre de 2024
3	Realizar Inventario de Activos de Información con los líderes de cada proceso	Líderes de proceso	Octubre de 2024
4	Realizar la Valoración de los Activos de Información con los líderes de cada Proceso	Líderes de proceso	Noviembre de 2024
5	Realizar el Plan de tratamiento de los riesgos (Riesgo Inherente y Riesgo Residual)	Contratista de apoyó TICs	Diciembre de 2024
6	Socializar el Plan de Tratamiento de Riesgo	Contratista de apoyó TICs	Diciembre de 2024
7	Realizar seguimiento del Plan de Tratamiento de Riesgo	Contratista de apoyó TICs	Diciembre de 2024

9. SEGUIMIENTO Y EVALUACIÓN

Al finalizar cada etapa se realizará una reunión con el alcalde municipal, los secretarios, jefes de oficina y el equipo de trabajo para presentar el informe de avance a la implementación del PTR y de esta manera evaluar todas las actividades propuestas en dicho plan. La reunión podrá ser reemplazada por un informe vía correo electrónico con el avance de la implementación, en caso de ser necesario.

10. ENTREGABLES

- Informe de avance al PTR
- Actas de Reunión.
- Plan de tratamiento de riesgo aprobado por los líderes
- Políticas de Seguridad de la información
- Productos de cada etapa

Ernesto Forero Clavijo
Secretario General

Luis Manuel González Ramírez
Alcalde Municipal de Sibaté