POLITICA GENERAL DEL SISTEMA DE GESTION Y SEGURIDAD DE LA INFORMACION

CONTENIDO

1. INTRODUCCIÓN

La Política General de Seguridad y Privacidad de la Información, como parte del Modelo de Seguridad y Privacidad de la Información, es la manifestación de la Alcaldía de Ibagué que materializa el propósito de garantizar la protección de los activos de información que soportan los procesos y el cumplimiento de las metas institucionales.

La Alcaldía de Ibagué reconoce la información como un activo fundamental en el desarrollo de los procesos, razón por la cual determina la necesidad de generar una política que contenga los lineamientos para la protección de los activos de información (Hardware, Software, Datos, Usuarios), de los procesos, los cuales se complementan con las políticas específicas y controles establecidos para garantizar la integridad, confidencialidad y disponibilidad de la información.

La estructura de este documento está basado en los lineamientos establecidos por el Ministerio de las Tecnologías de la Información y las Comunicaciones, los cuales son concordantes con la Norma Técnica NTC ISO/IEC 27001:2013

2. OBJETIVO

Establecer lineamientos para el control efectivo de la información de los procesos de la Alcaldía de Ibagué, con el propósito de minimizar los riesgos asociados a los activos de información, establecer una cultura de seguridad y asegurar el cumplimiento de la misión y objetivos institucionales de la Entidad.

3. TERMINOS Y DEFINICIONES

Activo: Cualquier cosa que tiene valor para la organización. [Guía ISO/IEC 73:2002]

Amenaza: Causa potencial de un incidente o deseado, que puede ocasionar daño a un sistema u organización. [NTC 5411-1:2006]

Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. [NTC 5411-1:2006]

Continuidad de Negocio: describe los procesos y procedimientos que una organización pone en marcha para garantizar que las funciones esenciales puedan continuar durante y después de un desastre.

Control: Medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

Directriz: Descripción que aclara lo que se debería hacer y cómo hacerlo, para alcanzar los objetivos establecidos en las políticas. [NTC 5411-1:2006]

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada. [NTC 5411-1:2006]

Gestión de riesgos de seguridad digital

Es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en

un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego. (CONPES 3854, pág. 24).

Incidente de Seguridad de la información: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. [ISO/IEC TR 18044: 2004]

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos. [NTC 5411-1:2006]

Monitoreo: Verificación, supervisión, observación crítica o determinación continúa del Estado con el fin de identificar cambios con respecto al nivel de desempeño exigido o esperado. (NTC ISO 31000:2011).

Política: Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

Probabilidad: Oportunidad de que algo suceda. (NTC ISO 31000:2011).

Procedimiento: Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico.

Riesgo: Combinación de la probabilidad de un evento y sus consecuencias. [ISO/IEC GUÍA 73:2002]

Seguridad de la información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad. [NTC ISO/IEC 17799:2006]

SGSI: Sistema de gestión de seguridad de la información.

Sistema de gestión de la seguridad de la información SGSI. parte del sistema de gestión global, basado en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información. Incluye la estructura organizacional, políticas, actividades de planificación, responsabilidades, prácticas, procedimientos, procesos y recursos.

Vulnerabilidad Debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas. [NTC 5411-1:2006]

4. POLITICA GENERAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION

La Alcaldía de Ibagué, considerando que la información es un activo fundamental para el desarrollo de los procesos, la prestación de los servicios y la toma de decisiones oportunas y asertivas, se ha comprometido con la implementación del sistema de gestión de seguridad de la información, para asegurar su integridad, confidencialidad y disponibilidad, como parte de una estrategia orientada a la mejora continua y a garantizar la continuidad del negocio, al fortalecimiento de la cultura de la seguridad y la gestión del riesgo, el cumplimiento del marco legal, reglamentario y requisitos de las partes interesadas y las obligaciones de seguridad contractuales; en concordancia con la planeación estratégica de la entidad y la norma ISO27001.

En la Alcaldía de Ibagué la gestión de los riesgos de seguridad digital a los cuales se encuentran expuestos los activos de información, busca minimizar la probabilidad de ocurrencia de incidentes de seguridad y el impacto operativo, financiero, ambiental y legal, que puedan afectar el normal desarrollo de los procesos de la Entidad y de los servicios que presta al ciudadano

La política de Administración del Riesgo define la metodología y lineamientos para la gestión del Riesgo.

5. OBJETIVOS DE SEGURIDAD DE LA INFORMACION

La Alcaldía de Ibagué, para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y con los siguientes objetivos de seguridad de la información.

- Minimizar el riesgo de los procesos de la entidad.
- Cumplir con los principios de seguridad de la información.
- Mantener la confianza de los servidores públicos, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los servidores públicos, terceros, aprendices, practicantes, proveedores y clientes de los procesos de la Alcaldía de Ibagué
- Garantizar la continuidad del negocio frente a incidentes.

6. ALCANCE DE LA POLÍTICA

El Sistema de Gestión de Seguridad de la Información aplica a todos los servidores públicos, personal externo, proveedores y demás grupos de interés que tengan responsabilidad y manejo sobre los activos de información de todos los procesos de la Alcaldía de Ibagué y las sedes donde opera.

Este alcance está fundamentado en el plan de tratamiento de riesgos de la información, el modelo de seguridad y privacidad de la información y la norma ISO 27001.

Nivel de cumplimiento: Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

7. POLÍTICAS DE SEGURIDAD QUE SOPORTAN EL SGSI

- La Alcaldía de Ibagué, ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.

- En la Alcaldía de Ibagué, Las responsabilidades frente a la seguridad de la información serán definidas por la Alta Dirección, compartidas, publicadas y aceptadas por cada uno de los Servidores Públicos, personal externo, proveedores y demás grupos de interés.

- La Alcaldía de Ibagué protegerá la información generada, procesada o resguardada por los procesos y activos de información que hacen parte de los mismos.

- La Alcaldía de Ibagué protegerá la información creada, procesada, transmitida o resguardada por sus procesos, con el fin de minimizar impactos operativos, financieros, ambientales o legales, debido a un uso incorrecto de esta. Para ello aplicará controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- La Alcaldía de Ibagué protegerá los activos de información de las amenazas originadas por parte del personal.

- La Alcaldía de Ibagué protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta los procesos.

- La Alcaldía de Ibagué, controlará la operación de los procesos garantizando la seguridad de los recursos tecnológicos y las redes de datos.

- La Alcaldía de Ibagué, implementará control de acceso a la información, sistemas y recursos de red.

- La Alcaldía de Ibagué, garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

- La Alcaldía de Ibagué, garantizará la mejora efectiva de su Sistema de seguridad, a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información.

- La Alcaldía de Ibagué, garantizará la disponibilidad de los procesos y la continuidad de su operación basada en el impacto que pueden generar los eventos de seguridad.

- La Alcaldía de Ibagué, garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a las políticas de seguridad y privacidad de la información traerá consecuencias legales que apliquen a la normatividad de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno Nacional y territorial en cuanto a Seguridad y Privacidad de la información

8. ROLES Y RESPONSABILIDADES

La Alcaldía de Ibagué ha definido las siguientes roles y responsabilidades para la implementación, aplicación, seguimiento y autorización de la política.

RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN

El responsable de Seguridad de la información será el líder del proyecto y tendrá las siguientes responsabilidades:

Con relación al proyecto:

1. Aplicar conocimientos, habilidades, herramientas, y técnicas a las actividades propias del proyecto, de manera que cumpla o exceda las necesidades y expectativas de los interesados en el mismo.

2. Identificar la brecha entre el Sistema de Gestión de Seguridad de la información y la situación de la entidad.

3. Generar el cronograma de la implementación del Sistema de Gestión de Seguridad y privacidad de la información.

4. Planear, implementar y hacer seguimiento a las tareas, fechas, costos y plan de trabajo de los objetivos específicos del cronograma definido.

5. Gestionar el equipo de proyecto de la entidad, definiendo roles, responsabilidades, entregables y tiempos.

6. Coordinar las actividades diarias del equipo y proporcionar apoyo administrativo

7. Encarrilar el proyecto hacia el cumplimiento de la implementación del Modelo de Seguridad y privacidad de la Información para la entidad.

8. Realizar un seguimiento permanente a la ejecución de los planes de trabajo, monitoreando los riesgos del proyecto para darle solución oportuna y escalar al Comité de seguridad en caso de ser necesario.

9. Monitorear el estado del proyecto en términos de calidad de los productos, tiempo y los costos.

10. Trabajar de manera integrada con el grupo o áreas asignadas.

11. Asegurar la calidad de los entregables y del proyecto en su totalidad.

12. Velar por el mantenimiento de la documentación del proyecto, su custodia y protección.

13. Contribuir al enriquecimiento del esquema de gestión del conocimiento sobre el proyecto en cuanto a la documentación de las lecciones aprendidas.

14. Liderar la programación de reuniones de seguimiento y velar por la actualización de los indicadores de gestión del proyecto.

Con relación al Dominio Servicios Tecnológicos:

15. Liderar la gestión de riesgos de seguridad sobre la gestión de TI y de información de la institución.
16. Gestionar el desarrollo e implementación de políticas, normas, directrices y procedimientos de seguridad de gestión de TI e información.
17. Definir mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de implantación de las medidas de seguridad.
18. Supervisar la respuesta a incidentes, así como la investigación de violaciones de la seguridad, ayudando con las cuestiones disciplinarias y legales necesarias.
19. Trabajar con la alta dirección y los dueños de los procesos dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio.
20. Realizar y/o supervisar pruebas de vulnerabilidad sobre los diferentes servicios tecnológicos para detectar vulnerabilidades y oportunidades de mejora a nivel de

seguridad de la información

Con relación al Dominio Estrategia TI

21. Definir la estrategia informática que permita lograr los objetivos y minimizar de los riesgos de la institución.
22. Es el encargado de guiar la prestación del servicio y la adquisición de bienes y servicios relacionados y requeridos para garantizar la seguridad de la información.

Con relación al Dominio Gobierno TI

23. Seguir y controlar la estrategia de TI, que permita el logro de los objetivos y la minimización de los riesgos del componente de TI. Encargado monitorear y gestionar la prestación del servicio y la adquisición de bienes y/o servicios relacionados y requeridos para garantizar la seguridad de información

Con relación a los Sistemas de información:

24. Establecer los requerimientos mínimos de seguridad que deberán cumplir los sistemas de información a desarrollar, actualizar o adquirir dentro de la entidad.
25. Apoyar la implementación segura de los sistemas de información, de acuerdo con el modelo de seguridad y privacidad de la información del estado colombiano.
26. Desarrollar pruebas periódicas de vulnerabilidad sobre los diferentes sistemas de información para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información.

27. Liderar el proceso de gestión de incidentes de seguridad, así como la posterior investigación de dichos eventos para determinar causas, posibles responsables y recomendaciones de mejora para los sistemas afectados.
28. Trabajar con la alta dirección y los dueños de los procesos dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio.

Con relación a la información

29. Supervisar que se garantice la confidencialidad, integridad y disponibilidad de la información a través de los distintos componentes de información implementados.
30. Verificar el cumplimiento de las obligaciones legales y regulatorias del estado relacionadas con la seguridad de la información.

Con relación al uso y apropiación

31. Desarrollar el plan de formación y sensibilización de la entidad incorporando el componente de seguridad de la información en diferentes niveles.
32. Supervisar los resultados del plan de formación y sensibilización establecido para la entidad, con el fin de identificar oportunidades de mejora.
33. Participar en la elaboración de los planes de gestión de cambio, garantizando la inclusión del componente de seguridad de la información en la implementación de los proyectos de TI.

RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES:

Tiene decisión sobre las bases de datos que contengan datos personales, responsable de direccionar las actividades de los encargados de datos personales, es decir de quienes realizan directamente el tratamiento de los datos, y tiene establecidas las siguientes responsabilidades:

1. Informar y garantizar el ejercicio de los derechos de los titulares de los datos personales.
2. Tramitar las consultas, solicitudes y reclamos.
3. Utilizar únicamente los datos personales que hayan sido obtenidos mediante autorización, a menos que los mismos no la requieran.
4. Respetar las condiciones de seguridad y privacidad de información del titular.
5. Cumplir instrucciones y requerimientos impartidos por la autoridad administrativa competente.

COMITÉ INSTITUCIONAL DE GESTION Y DESEMPEÑO

1. Aprobar la Política de Seguridad de la Información de la Alcaldía de Ibagué
2. Asegurar que se establezca los objetivos y planes del Sistema de Gestión de Seguridad de la Información (SGSI).
3. Asegurar los recursos para la implementación de esta política del Sistema de Gestión de Seguridad de la Información
4. Establecer y aprobar la documentación el SGSI.
5. Definir los criterios de aceptación de riesgos de seguridad digital.
6. Comunicar a todos los empleados de la Alcaldía de Ibagué y partes interesadas, la importancia de la aplicación de las políticas de seguridad y demás elementos del SGSI.

7. Definir los criterios y niveles de aceptación de riesgos.
8. Asegurar que se realicen las auditorías internas al SGSI
9. Efectuar las revisiones del SGSI

COMITÉ DE SEGURIDAD

El Comité de Seguridad de la información estará integrado así:

1. El Directivo del área de TIC o su delegado.
2. El Directivo del área de Planeación o su representante.
3. El Directivo del área Jurídica o su delegado.
4. El Directivo encargado de los sistemas de Gestión de Calidad o su delegado
5. El encargado de la Gestión Documental o su delegado.
6. El Jefe de la Oficina de Control Interno o su delegado.
7. El responsable de Seguridad de la información de la entidad.

Responsabilidades del Comité de Seguridad

1. Coordinar la implementación del Sistema de Gestión de Seguridad y privacidad de la Información al interior de la Alcaldía de Ibagué.
2. Revisar los diagnósticos del estado de la seguridad de la información en Nombre de la Alcaldía de Ibagué.
3. Acompañar e impulsar el desarrollo de proyectos de seguridad.
4. Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de la Alcaldía de Ibagué.

5. Recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información.
6. Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.
7. Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.
8. Realizar revisiones periódicas del SGSI (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes.
9. Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad.
10. Poner en conocimiento de la entidad, los documentos generados al interior del comité de seguridad de la información que impacten de manera transversal a la misma.
11. Las demás funciones inherentes a la naturaleza del Comité.

LIDERES DE LOS PROCESOS:

1. Aplicar los lineamientos del Sistema de Gestión de Seguridad de la Información (SGSI) al interior del área correspondiente, transmitiendo los objetivos de la seguridad de la información para cada uno de los roles que aplique.
2. Liderar y apoyar la aplicación del Sistema de Gestión de Seguridad de la Información (SGSI) al interior de su proceso.
3. Apoyar la capacitación y entrenamiento requerido para que los funcionarios asignados a su área cumplan con el Sistema de Gestión de Seguridad de la Información (SGSI)
4. Revisar los controles establecidos en el mapa de riesgos de seguridad digital definido por la entidad, de acuerdo a la periodicidad definida.

5. Definir la clasificación de la información de su proceso y determinar los niveles de acceso.
6. Autorizar la asignación de permisos de acceso a la información, de conformidad con las políticas específicas establecidas.
7. Apoyar a la Secretaría de las TIC en la generación de controles necesarios para el almacenamiento, procesamiento, distribución y uso de la información.

COMUNICACIÓN Y APROPIACION:

1. La Oficina de Comunicaciones se encargará de la difusión de la Política de Seguridad de Información de conformidad con el plan de Comunicación del Sistema de Gestión de Seguridad de la información establecido por la Secretaría de las TIC y el responsable de la Seguridad.
2. La Dirección encargada del Sistema de Gestión Integral SIGAMI será la responsable de promover el uso y apropiación de la política de seguridad de la información
3. La Dirección de Talento Humano incluirá en el plan de inducción, reinducción y capacitación, la temática de seguridad de la información.

MONITOREO Y SEGUIMIENTO:

La Oficina de Control Interno es la responsable de Realizar revisiones independientes para verificar el cumplimiento de las políticas y normas de seguridad de la información.

RESPONSABLE DE LA SEGURIDAD FÍSICA Y EL ENTORNO

La Dirección de Recursos Físicos es la responsable de garantizar áreas seguras (Perímetro de seguridad física, áreas de despacho y carga, visita al centro de cómputo)

USUARIOS DEL SISTEMA DE INFORMACION

1. Conocer y aplicar los procedimientos, controles y políticas de seguridad adoptadas por la Entidad dentro del marco del SGSI.
2. Reportar los incidentes de seguridad de conformidad con el procedimiento de manejo de incidentes.

9. REVISION Y APROBACION

El procedimiento de revisión y aprobación de la política se realizará de conformidad con el procedimiento de control de documentos PRO-GIC-01 del proceso Gestión Integral de la Calidad.model9

10. CONTROL DE CAMBIOS

VERSION	VIGENTE DESDE	OBSERVACION
01	08/10/2018	SIGAMI
02	25/04/2019	CAMBIO DE NOMBRE DEL PROCESO
03	01/12/2020	Actualización nombre Dependencia de Dirección Informática a Secretaría TIC, Política, Alcance, Objetivos
04	29/10/2021	Cambio de proceso: Pasa de Gestión de Infraestructura Tecnológica a Sistema integrado de Gestión Actualización del nombre de la política: pasa de ser la política del Modelo de Seguridad y Privacidad de la Información para ser la política del Sistema de Gestión de Seguridad de la información
05	24/08/2022	Actualización de la política, el alcance y los objetivos. Se amplió el alcance a todos los procesos por lo tanto se elimina la palabra misionales en todo el contenido del documento.

Elaboró	Revisó	Aprobó
Profesional Universitario	Asesor	Secretario(a) de Tic