PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

OBJETIVO

Establecer desde la Oficina de las Tecnologías de la Información y Comunicación TIC las medidas, actividades y controles de seguridad contempladas en el Anexo A de la norma NTC/IEC ISO 27001:2013 que ayudarán, mediante su implementación, a preservar la confidencialidad, integridad y disponibilidad de la información que permitirá garantizar continuamente la seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios en la alcaldía de Sabaneta, por medio de la definición de políticas, programas, lineamientos, estrategias y actividades.

ALCANCE

Aplica a todos los niveles de la administración Municipal de Sabaneta, sus funcionarios, contratistas, proveedores y aquellas personas o terceros que debido al cumplimiento de sus funciones compartan, utilicen, recolecten, procesen, intercambien o consulten cualquier tipo de información, ya sea interna o externamente independientemente de su ubicación, así mismo las actividades pertinentes que se consideren fundamentales para determinar la estrategia de implementación de los controles de seguridad requeridos para el funcionamiento adecuado de la alcaldía de Sabaneta.

¿Qué son los activos?	¿Por qué identificar los activos?
-Servicios web -Redes -Información física o digital -Tecnologías de información TI -Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital	La entidad puede saber **qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano**, aumentando así su confianza en el uso del entorno digital

ROLES Y RESPONSABILIDADES

La Oficina de las Tecnologías de la Información y Comunicación TIC por medio de sus profesionales en cabeza de su director serán los responsables de los controles técnicos de seguridad de la información

- ✓ Cierre de vulnerabilidades técnicas
- ✓ Seguimiento al cierre de vulnerabilidades técnicas
- ✓ Seguimiento de indicadores
- ✓ Seguimiento al cierre de eventos e incidentes de seguridad de la información
- ✓ Seguimiento del plan de tratamiento de riesgos de seguridad de la información del proceso Gestión Tics.
- ✓ Establecer controles de seguridad de la información con el fin de mitigar los riesgos que puedan afectar la confidencialidad, disponibilidad e integridad de la información y/o servicios que presta la dirección de informática.
- ✓ Notificar a la cuenta de correo electrónico mesadeayuda@sabaneta.gov.co, los eventos o incidentes de seguridad de información, así como cualquier eventualidad sospechosa que pueda poner en riesgo la continuidad de las operaciones de la alcaldía de Sabaneta.

Administrador del SGSI

El rol del administrador del SGSI, es el responsable de:

- ✓ Realizar seguimiento al cumplimiento de los lineamientos y políticas del SGSI
- ✓ Revisar y aprobar políticas, planes, programas, procedimientos en materia de seguridad de la información para la aplicación de controles en el sistema
- ✓ Realizar revisiones al SGSI periódicamente y definir acciones a seguir
- ✓ Velar por el cumplimiento de las políticas, normas, procedimientos y demás documentos relacionados con el SGSI

Líderes de procesos

El rol de los líderes de procesos en la ejecución del plan de revisión y seguimiento al SGSI, es fundamental dado que es el responsable de:

- ✓ Seguimiento a la ejecución de los planes de tratamiento de riesgos en seguridad de la información.
- ✓ Actualización de activos de información
- ✓ Revisión y cumplimiento de los procedimientos, controles y políticas del SGSI

Funcionarios y Contratistas

- ✓ Mantener y garantizar la confidencialidad e integridad de la información que reciben, generan y procesan en la alcaldía de Sabaneta
- ✓ Hacer buen uso de los activos de información de la entidad.
- ✓ Respetar la legislación y regulación vigente.

Crear comité de seguridad de la información

Para poder cumplir con este ítem es necesario reunirnos con los encargados o los que pertenecen dichos procesos de control (antes de publicar se hace necesario).

ACTIVIDADES

El Plan de implementación de Seguridad de la Información de la alcaldía de Sabaneta comprende las siguientes actividades.

ID	CONTROLES	ACTIVIDAD	ACTIVIDAD	ACTIVIDAD	RESPONSABLE
1	Política general de seguridad de la información	Revisión anual Del cumplimiento de la política general de seguridad de la información	Revisar y/o ajustar la política de seguridad de la información al menos cada año	Hacer seguimiento a las evidencias de actualización y revisión del cumplimiento de la política de seguridad	Alta Dirección, Planeación Integral
2	Manual de seguridad de la información	Revisión del Manual de seguridad de la Información	Actualización del Manual de Seguridad de la Información	Realizar seguimiento del Manual de Seguridad de la Información	Dirección de informática
3	Procedimiento de seguridad de la información	Realizar seguimiento y control del procedimiento, formatos, instructivos, políticas, etc.	Revisar y/o actualizar los documentos asociados al procedimiento Seguridad de la información	Solicitar a Planeación la actualización de los documentos y publicación de los mismos	Dirección de informática Planeación
4	Gestión de activos de Información	Levantamiento y/o actualización de los Activos de Información	**Identificar nuevos activos de información en cada área **Validarla actualización de los activos de información en el formato actualizado	** Verificación y aprobación de los activos de información para su publicación en Intranet	Planeación

			comparado con la vigencia anterior	** Publicar los activos de información consolidado	
5	Gestión de vulnerabilidades	** Definir lineamientos para ejecutar las pruebas de vulnerabilidades **Ejecución de pruebas de seguridad (análisis de vulnerabilidades) al menos una vez al año.	** Ejecutar el plan de remediación sobre los sistemas y plataforma de acuerdo con los resultados del análisis de vulnerabilidades ** Realizar seguimiento al cierre de vulnerabilidad técnicas de acuerdo con su nivel de criticidad	** Verificar la ejecución del re- test de pruebas de seguridad ** Documentar las actualizaciones cuando ocurra un cambio importante en los activos de información producto del retest.	Dirección de informática
6	Indicadores de seguridad de la información	Formular, implementar y actualizar los indicadores del SGSI	**Realizar Seguimientos a las acciones correctivas planteadas para los indicadores que no cumplen las metas **Realizar seguimiento al cumplimiento de las metas de los indicadores del SGSI	Hacer Seguimiento a las evidencias de ejecución de acciones correctivas o de mejora	Planeación Dirección de informática
7	Gestión de riesgos (Identificación, Análisis y Evaluación de Riesgos)	Realizar seguimiento trimestral de los Planes de Tratamiento de Riesgos	Realizar valoración trimestral del riesgo residual	Realizar seguimiento a la documentación y evidencia de la ejecución del plan de tratamiento de Riesgos	Planeación Dirección de informática Líderes de los procesos misionales
8	Plan de contingencia y continuidad de negocio de TI	** Actualización del documento ** Identificación y/o valoración de Riesgos de interrupción de la operación de la entidad	** Realizar seguimiento y revisión de la ejecución de las pruebas del plan ** Realizar seguimiento a la documentación y lecciones aprendidas de los resultados de las pruebas del Plan	Revisión de las acciones de mejora Identificadas en las pruebas del Plan	Dirección de informática
9	Plan de comunicación, socialización y sensibilización	** Elaborar y ejecutar el Plan de comunicación en temas	Realizar evaluación de conocimientos de seguridad posterior	Hacer seguimiento a las evidencias de	Planeación Líderes de los procesos

		relacionados con seguridad de la información ** Realizar mínimo 2 jornadas de sensibilización en seguridad de la información en las jornadas de inducción y reinducción durante el año	a las capacitaciones (Encuestas)	socialización del SGSI	
10	Auditoria (Internas – Externas)	Realizar auditorías internas y externas de la norma ISO 27001:2013	Realizar seguimiento al cierre de las no conformidades producto de las auditorías internas y externas al SGSI.	Hacer seguimiento a las evidencias del cierre de las no conformidades por proceso	Planeación Control interno
11	Gestión de incidentes de seguridad	Gestionar los Incidentes de Seguridad de la Información identificados	**Realizar el seguimiento a la gestión de incidentes de seguridad de la información incluyendo cierre **Realizar seguimiento a las lecciones aprendidas producto de la gestión del incidente	Realizar seguimiento de los reportes de eventos de seguridad de la información y tomar acciones.	Dirección de informática
12	Declaración de aplicabilidad – Anexo A	Revisión de los controles de la norma ISO 27001:2013	Actualizar declaración aplicando acciones y controles para la implementación del control	Seguimiento a La aplicación de los controles	Dirección de informática

DOCUMENTOS DE REFERENCIA

Constitución política de Colombia

Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

Ley 1978 de 2019. Por la cual se moderniza el sector de las Tecnologías de la Información y las Comunicaciones TIC), se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones

Decreto 1064 de 2020. Por el cual se modifica la estructura del Ministerio de Tecnologías de la Información y las Comunicaciones

Resolución 924 de 2020. Por la cual se actualiza la política de tratamiento de datos personales del Ministerio/Fondo Único de TIC y se deroga la resolución 2007 de 2018.

Resolución 2256 de 2020. Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones y se definen lineamientos frente al uso y manejo de la información y se deroga la resolución 1124 de 2020.

CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.

CONPES 3854 de 2016. Política Nacional de Seguridad digital.

CONPES 3905 de 2020. Política Nacional de Confianza y Seguridad Digital

CONTROL DE CAMBIOS

FECHA	VERSION	DESCRIPCION DEL CAMBIO
29-12-2021	V.1	Elaboración del plan

Elaboro: Andrés Felipe García Henao

Reviso: Diego Alejandro Montoya

Aprobó: