MANUAL DE POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 3.0

ALCALDÍA MUNICIPAL DE SOACHA

ENERO 2024

Control de cambios

Versión	Fecha	Descripción de la Modificación
1.0	30-07-2018	• Versión inicial del documento Plan de Seguridad y Privacidad en la información Link: http://www.alcaldiasoacha.gov.co/phocadownloadpap/Planes_2018/Plan%20de%20Seguridad%20y%20Privacidad%20de%20la%20Informacin.pdf
2.0	20-11-2020	• Se realiza ajuste de normalización como consecuencia de la entrada en vigor a través del decreto único reglamentario 1078 de 2015, del sector de Tecnologías de Información y Sistema de Gestión de Seguridad de la Información SGSI. • De la misma manera se ajusta a la Guía 2 - Política General MSPI (Modelo de Seguridad y Privacidad de la Información) en su versión 1 del 11/05/2016 y la Guía 3 - Procedimiento de Seguridad de la Información en su versión 1 del 25/04/2016. • Link: https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo- de-Seguridad/ • Todas las referencias a las políticas, definiciones o contenido relacionado, publicadas en la norma técnica colombiana NTC ISO/IEC 27001:2013, así como a los anexos son derechos reservados • por parte de ISO/ICONTEC.
3.0	23-01-2024	• Se ha actualizado el nombre del recurso de servicios de tickets previamente denominado "helpdesk" a "mesa de servicios". Esta modificación busca reflejar de manera más precisa y moderna el enfoque y alcance de los servicios ofrecidos. A partir de ahora, todas las referencias y documentación relacionadas con el soporte de tickets deberán utilizar el nuevo nombre "mesa de servicios" para asegurar coherencia en la comunicación y en los procesos operativos. • Se procedido a cambiar el versionamiento del software de V2 a V3. Este cambio de versión incluye mejoras significativas en la funcionalidad y en la estabilidad del sistema. Además, se han actualizado los logos correspondientes a esta nueva versión para reflejar que se aplican los lineamientos de no marca. • Se realizo una actualización en el campo de directrices del ítem 7.1, que corresponde a la Gestión de Activos. Esta actualización busca proporcionar una mayor claridad y precisión en las directrices que regulan la gestión de los activos. Las nuevas directrices reflejan las mejores prácticas actuales y las normativas vigentes, con el objetivo de mejorar la eficiencia y el control en el manejo de los activos • En el ítem 7.7, referente a Registro y Auditoría, se ha actualizado el campo de prohibiciones. Estas nuevas prohibiciones están diseñadas para fortalecer los controles y asegurar la integridad y la precisión de los registros y auditorías. Las actualizaciones

		incluyen nuevas restricciones y procedimientos que deben seguirse para evitar el mal uso de la información y garantizar una auditoría efectiva.

Metodología de elaboración	Revisó	Aprueba
El documento se elabora con base en la normatividad que regula la materia (Decreto 1078 de 2015), los profesionales de la Dirección de Gestión Tecnológica realizan los ajustes correspondientes, pasa a socialización y revisión del Comité de Desempeño y Gestión de la Entidad. Proyectó: ***Carlos Albeiro Garzón Ramírez*** Profesional Universitario	***LUIS MIGUEL ROJAS BOGOTÁ*** **DIRECCIÓN DE GESTIÓN TECNOLÓGICA**	***CARLOS ANDRÉS TOBÓN*** **SECRETARIA GENERAL**

El siguiente documento ha desarrollado el modelo plantilla para la elaboración de la política general de seguridad y privacidad de información para las entidades públicas, como parte del Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno en Línea, según lo establecido en el Decreto 1078 de 2015. Alcaldía de Soacha, 2024.

TABLA DE CONTENIDO

1. PROPÓSITO

La Alcaldía Municipal de Soacha a través de la Dirección de Gestión Tecnológica de la Secretaría General, dando cumplimiento a sus funciones en lo referente a Seguridad y Privacidad de la Información y gestión del riesgo de seguridad digital (ciberseguridad) y buscando una administración más eficiente, más transparente y participativo hacia la ciudadanía, plantea y desarrolla la siguiente política y lineamientos de Seguridad y Privacidad de la Información, para dar cumplimiento a lo establecido en el componente de seguridad y privacidad de la información y seguridad digital de la estrategia de gobierno digital y el Modelo Integrado de Planeación y Gestión-MIPG, según lo establecido en el Decreto 1078 de 2015, el Decreto 1499 de 2017, el Decreto 1008 de 2018, el Decreto Municipal 192 de 2018 y el Decreto 129 de 2021; con esto la entidad vela por la integridad, confidencialidad y disponibilidad de la información y administra el riesgo sobre todos sus activos de información.

2. INTRODUCCIÓN

La política de seguridad es un documento de política general que denota el compromiso de la alta gerencia con la seguridad de la información que contiene la definición de la seguridad de la información en la Entidad.

La protección y seguridad de los activos de información, parte del concepto fundamental de seguridad de la información la cual se desarrolla mediante el principio explícito de la gestión de riesgo, y comprende el conjunto de medidas, procedimientos y controles establecidos en cada dominio de la norma ISO27001-2022, para el correcto manejo, gestión y control de la información, en todo su ciclo de vida bajo el modelo PHVA, así como para garantizar sus propiedades fundamentales; la preservación de la confidencialidad, integridad y disponibilidad de la información que se complementan con otras propiedades como Accesibilidad, Autenticidad, No Repudio, entre otros, mediante el resguardo de datos, la protección frente a accesos no autorizados.

Conscientes de que la seguridad informática se fundamenta en la existencia de un conjunto de políticas que brinden instrucciones claras y sean el soporte tecnológico y legal de la Alta Dirección y con el objetivo que estas sean una herramienta para la definición de los estándares y procesos internos de la Entidad, la Alcaldía Municipal de Soacha a través de este documento define la política de seguridad y privacidad de la información y seguridad digital y reglamenta los lineamientos para la implementación, medición y seguimiento, los roles y responsables de su implementación y mejora continua, y la estrategia para su adopción mediante las pautas para uso y apropiación, dentro de estas políticas se consideran las planteadas en la norma ISO27001-2022: (Controles Organizacionales, Controles relativas al Personal, Controles físicos y Controles tecnológicos).

El desarrollo de la presente política conlleva a determinar y plantear las siguientes acciones que son el eje fundamental para el logro determinante de la misma:

1. Adoptar la presente Política de seguridad de la información
2. Integrar el Comité de Seguridad de la Información al Comité de Desempeño Institucional de la Entidad.
3. Desarrollar controles de la Política de Seguridad de la Información, para cada uno de los dominios de las 10 políticas planteadas.

- ✓ GESTIÓN DE ACTIVOS
- ✓ CONTROL DE ACCESO
- ✓ NO REPUDIO
- ✓ PRIVACIDAD Y CONFIDENCIALIDAD
- ✓ INTEGRIDAD
- ✓ DISPONIBILIDAD DEL SERVICIO E INFORMACIÓN y/o CONTINUIDAD DEL NEGOCIO
- ✓ REGISTRO Y AUDITORIA
- ✓ GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
- ✓ SEGURIDAD DIGITAL
- ✓ SEGURIDAD DEL PERSONAL

Lo anterior enmarcado además en los esfuerzos que la Administración Municipal de Soacha enfoca en impulsar las Tecnologías de la Información y las Comunicaciones, para garantizar una mayor y mejor interacción con la ciudadanía a través del uso adecuado de los recursos a su alcance.

Es así como la Política de Seguridad de la Información permite avanzar en la estrategia de Gobierno Digital, específicamente en las metas trazadas para la Implementación de la Estrategia de Gobierno Digital, como entidad de orden territorial.

En este componente también se describen actividades orientadas a que cada entidad cuente con una política de seguridad que es aplicada de forma transversal y mejorada constantemente; y que se garantice la incorporación del Gobierno Digital como parte de la cultura organizacional y elemento de soporte en sus actividades misionales.

Para alcanzar los objetivos de este componente, la entidad deberá desarrollar las siguientes actividades:

1. Institucionalizar la Estrategia de Gobierno Digital
2. Centrar la atención en el usuario;
3. Implementar un sistema de gestión de Tecnologías de Información;
4. Implementar un sistema de gestión de seguridad de la información (SGSI).

3. OBJETIVOS

3.1 OBJETIVO GENERAL

La presente política de Seguridad de la Información tiene como objetivo guiar el comportamiento personal y profesional de los funcionarios, contratistas o terceros sobre la información obtenida, generada o procesada por esta entidad; así mismo, permitir que la alcaldía trabaje bajo las mejores prácticas de seguridad, mediante la implementación de buenas prácticas enmarcadas en un modelo de gestión sistemático y cíclico de Seguridad y Privacidad de la Información y de riesgo de seguridad digital; para mitigar el riesgo de acceso, uso, divulgación, interrupción o destrucción no autorizada a los que puedan estar expuesta la información, los Sistemas de Información y su infraestructura al tiempo que se cumple con los requisitos legales que debe cumplir esta entidad en términos de seguridad de la información y seguridad digital.

3.2 OBJETIVOS ESPECÍFICOS

A continuación, se describen los objetivos específicos para alcanzar los resultados del presente manual de Seguridad de la Información:

1. Definir la política de seguridad y privacidad de la información y seguridad digital de la Alcaldía Municipal de Soacha Cundinamarca.
2. Definir los lineamientos para implementar y verificar el cumplimiento de la política para seguridad y privacidad de la información y seguridad digital.
3. Enmarcar los objetivos y lineamientos para implementar el modelo de gestión sistemático y cíclico de Seguridad y Privacidad de la Información y de riesgo de seguridad digital en la Alcaldía Municipal de Soacha.
4. Definir los roles y responsabilidades para la gestión de la seguridad y privacidad de la información y seguridad digital en la Alcaldía Municipal, de Soacha.
5. Definir una estrategia de continuidad de los procesos de la Alcaldía Municipal de Soacha frente a incidentes de seguridad de la Información, y Monitorear el

cumplimiento de los requisitos de seguridad de la información, mediante el uso de herramientas de diagnóstico, revisiones por parte de la Alta Dirección y auditorías internas planificadas a intervalos regulares.

6. Sensibilizar y capacitar a los servidores públicos, Contratistas, proveedores y partes interesadas acerca del Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información, de Gobierno Digital, fortaleciendo el nivel de conciencia de estos, en cuanto a la necesidad de salvaguardar los activos de información institucionales.

4. ALCANCE

La presente política de Seguridad de la Información detallada en este documento proporciona los lineamientos requeridos para normalizar la seguridad y privacidad de la información y seguridad digital en la Alcaldía Municipal de Soacha, partiendo desde el enunciado de la política, pasando por los lineamientos para la implementación de un modelo de gestión sistemático y cíclico de Seguridad y Privacidad de la Información y de riesgo de seguridad digital, la definición de los indicadores para el monitoreo de cumplimiento de la política hasta la definición de una estrategia para la adopción de la política en la alcaldía de Soacha, donde se fortalezca el nivel de conciencia para la adopción y aplicación de la misma.

5. SANCIONES POR INCUMPLIMIENTO

La desatención e inobservancia de las presentes Políticas de Seguridad de la Información plasmadas en el presente Manual, podrá acarrear según corresponda a sanciones disciplinarias y a la iniciación de las investigaciones de conformidad con las disposiciones legales vigentes en relación con la función pública.

6. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

Nombre de la Política
Seguridad, privacidad de la Información y Seguridad digital – Alcaldía Municipal de Soacha.
Enunciado
La secretaría General de la Alcaldía Municipal de Soacha, en cabeza de la Dirección de Gestión Tecnológica, se compromete a mantener acciones y estrategias orientadas a la protección de la información como principal activo de la Entidad, mediante un modelo de gestión sistemático de privacidad y seguridad digital, orientado a la administración del riesgo con el fortalecimiento de la integridad, confidencialidad y disponibilidad de la información, fomentando la cultura de seguridad en todos los niveles de la Organización, sus proveedores y la ciudadanía que demanda servicios.

Tabla 1 – Política de Seguridad y Privacidad de la Información y Seguridad Digital - Alcaldía Municipal de Soacha.

7. LINEAMIENTOS PARA LA IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

A continuación, se definen los lineamientos y directrices que se deben seguir por parte de los colaboradores y terceros de la Alcaldía Municipal de Soacha, con el fin de garantizar la disponibilidad, integridad y confidencialidad de la información, a manera de enunciados, directrices y prohibiciones; a continuación se definen 10 políticas específicas para la implementación de controles de seguridad de la información y seguridad digital; a partir de las características particulares de esta entidad de orden territorial se hacen recomendaciones en cuanto a sus activos de información, sus procesos y los servicios de información que presta esta alcaldía. A continuación, se agruparán las políticas con el objetivo de hacer una implementación transversal de Seguridad de la Información en esta Entidad.

7.1 GESTIÓN DE ACTIVOS

Enunciado:

La Alcaldía Municipal de Soacha se compromete a identificar y clasificar los activos de información de acuerdo con su nivel de criticidad y nivel de confidencialidad. Igualmente, a definir el mecanismo para la identificación, uso, administración, protección y responsabilidad de los activos de información en cada una de sus secretarías y dependencias. Por esto, la entidad protege la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta.

Directrices:

- Semestralmente se deben validar y actualizar los listados de activos de información, definiendo responsabilidades, criticidad, sensibilidad, reserva, protección adecuada y las infraestructuras criticas cibernéticas (en cada secretaría el profesional de seguridad de la información es responsable de dicha validación y actualización de este, siempre que haya lugar).
- Implementar la gestión de riesgos sobre los activos de información, teniendo en cuenta las herramientas actuales definidas en el manual de riesgo de la entidad y adecuándolas de ser necesario para que cumplan con las guías al respecto de MINTIC.
- Los funcionarios, contratistas o terceros de la entidad deben tener en cuenta estas recomendaciones cuando envíen la impresión, escaneen o saquen copias, deberán verificar y recoger de las impresoras inmediatamente los documentos confidenciales para evitar su divulgación no autorizada o mal intencionada.
- La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico las condiciones adecuadas de almacenamiento y resguardo.
- Todos los activos de información físicos de la Alcaldía Municipal de Soacha deben estar inventariados y/o identificados por la Dirección de Gestión Tecnológica, el área de inventarios de la Dirección de Recursos Físicos, por medio de códigos de barras y/o codificación de plaquetas; y al administrador de red para los equipos de infraestructura Tecnológica. Su responsabilidad será entregada a cada usuario durante su tiempo de uso, administrado mediante un sistema de asignación de inventario físico. Al inicio de su asignación en usuario y/o funcionario firmará un acta de recibido. El Área encargada establecerá el procedimiento.
- Todos los usuarios deben devolver sus activos de información, en buen estado, una vez cese su relación laboral con la Administración.

- El usuario debe velar por el cuidado de los recursos tecnológicos que se tengan asignados, sin perjuicio de la responsabilidad administrativa, fiscal disciplinaria o penal, en que se pueda incurrir por cualquier daño o pérdida.
- Los funcionarios como terceros deben asegurarse de que, en el momento de ausentarse de su puesto de trabajo, sus escritorios se encuentran libres de documentos y medios de almacenamiento, utilizados en el desempeño de sus labores, estos deben contar con la protección de seguridad necesarias, de la misma manera su herramienta de trabajo (computador) debe contar con una contraseña de usuario o cuenta, para evitar que terceros ingresen sin autorización.
- Solo el personal del área a cargo de la Dirección de Gestión Tecnológica en la Entidad está autorizado para realizar mantenimiento, cambios de partes, cambio de aplicativos, cambio de lugar y/o otra actividad que genere cambios en el hardware y/o software del equipo de propiedad de la Alcaldía Municipal de Soacha, según el requerimiento aprobado en el caso generado a través del aplicativo Mesa de Servicios, usado por la entidad.
- En caso de necesitar soporte técnico, el usuario debe crear el caso en la herramienta Mesa de Servicios a cargo de la Dirección de Gestión Tecnológica en la Entidad. No se atenderán solicitudes realizadas de manera personal.
- En el caso del personal directivo, secretarios de despacho, directores y jefes de oficina, la Dirección de Talento Humano debe solicitar la creación de credenciales de acceso al dominio, asignación de cuenta en Microsoft Office 365, correo electrónico, mesa de servicios, por medio un caso en la mesa de servicios, relacionando los nombres y apellidos, No de documento de identificación, cargo, dependencia. Si la persona está ingresando a la entidad en la modalidad de contrato de prestación de servicios, se debe adjuntar adicionalmente copia del Acta de Inicio. Si la persona está ingresando en la modalidad de planta a la Entidad, se debe adjuntar adicionalmente la copia de resolución de nombramiento.
- No hay expectativa de privacidad, los computadores y cuentas asociadas son dadas a los Usuarios para facilitarles su trabajo. Los usuarios no deben tener una expectativa de privacidad en relación con la información manejada en el equipo de cómputo, el cual pertenece a la entidad. Es decir, los usuarios renuncian expresamente a la privacidad en relación con cualquier material que ellos creen, almacenen, envíen o reciban en el computador, a través de Internet o de cualquier otra red.
- Los usuarios dan su consentimiento para que, de ser necesario, funcionarios autorizados de la entidad puedan acceder y revisar cualquier tipo de material que los usuarios creen, almacenen, envíen o reciban en el computador, a través de Internet o de cualquier otra red. Los usuarios entienden y aceptan que el área a cargo de la Dirección de Gestión Tecnológica en la Entidad puede utilizar procedimientos

y recursos manuales o automáticos para monitorear la utilización de sus Recursos Tecnológicos.

- Toda información y/o material encontrado en los recursos tecnológicos de la Administración, que no cumpla requerimientos laborales, será borrada y se reportara el usuario ante su jefe inmediato para las sanciones pertinentes.
- La Dirección de Gestión Tecnológica en la entidad mantendrá actualizado las hojas de vida de los recursos tecnológicos y avisará de los cambios pertinentes a la Dirección de Recursos Físicos de secretaría general con respecto a los recursos tecnológicos de la Administración. Se establecerá un procedimiento con su respectivo responsable.
- Los recursos tecnológicos de software y hardware (aplicativos, antivirus, cambio de partes etc.) y su mantenimiento correspondiente, solo será instalado y generado por la Dirección de Gestión Tecnológica en la entidad.
- Se prohíbe el uso de medios extraíbles como memorias USB, Discos externos entre otros por parte de los usuarios. Si el dispositivo se instala y se daña es única responsabilidad del usuario que lo instaló.
- El trabajo remoto o teletrabajo causado por el COVID-19 o en sus causas generales, sólo debe ser autorizado por el responsable de la dependencia, o superior jerárquico a la cual pertenece el usuario solicitante, conjuntamente con la Dirección de Gestión Tecnológica y se verificará que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con la política, normas y procedimientos existentes. Se implementarán procesos de auditoría específicos para los casos de accesos remotos, que deben ser revisados regularmente. Se llevará un registro de incidentes a fin de corregir eventuales fallas en la seguridad de este tipo de accesos.
- Los usuarios que acceden al dominio de la administración deberán tener copias de la información propia y relevante de su labor las plataformas de OneDrive, o SharePoint que se haya destinado para este fin, respetando las cuotas de espacio asignadas para cada uno. Todo lo anterior quedará establecido mediante un procedimiento.
- La Dirección de Gestión Tecnológica, debe garantizar que los equipos que se utilizan en la alcaldía municipal de Soacha, y que sean de su misma propiedad, estén vinculados al dominio alcaldiasoacha.local.lan.
- Mantener al día todas las solicitudes de los casos, solicitudes y requerimientos relacionados con recursos tecnológicos (sistemas de información, redes de datos, servidores, equipos de cómputo, conectividad, especificaciones técnicas) asignados en la plataforma de mesa de servicios.

- La Dirección de Gestión Tecnológica, debe garantizar que todos los usuarios se autentiquen en el dominio y estén creados en el directorio activo.
- Si conoce de alguna violación a las políticas y lineamientos, consignadas en el presente documento, se deberá reportar a la Dirección de Gestión Tecnológica.

Prohibiciones:

- **Está estrictamente prohibido** adquirir, desarrollar o contratar aplicaciones de software, equipos de hardware y todo recurso tecnológico, sin la autorización, concepto técnico de viabilidad y verificación de la Dirección de Gestión Tecnológica en la Entidad.

  La Dirección de Gestión Tecnológica en la entidad, no se hará responsable si no se pueden implementar aplicaciones de software y/o instalar equipos de hardware por falta de condiciones técnicas requerimientos funcionales de los mismos.
- **Está estrictamente prohibido** descargar, instalar software en los recursos tecnológicos de la entidad, así como la manipulación del hardware de los mismos. Solamente es autorizado el personal de soporte técnico de la Dirección de Gestión Tecnológica en la Entidad.
- **Está estrictamente prohibido** la divulgación, cambio, retiro o pérdida no autorizada de información de la entidad almacenada en medios físicos removibles, como USB, discos externos, entre otros.
- **Está estrictamente prohibido** utilizar los recursos tecnológicos de la entidad para divulgar, propagar o almacenar contenido personal o comercial de publicidad, promociones, ofertas, juegos recreativos, programas destructivos (virus), material político o cualquier otro uso que no esté autorizado.
- Está estrictamente prohibido utilizar software no licenciado en los recursos tecnológicos de la Administración. No es permitida, en ningún caso, la violación a los derechos de propiedad intelectual.
- **Está estrictamente prohibido** copiar software licenciado de la entidad para utilizar en sus computadores personales, ya sea en su domicilio o en cualquier otra instalación y/o entregarlos a terceros.
- **Está estrictamente prohibido** la utilización de la red de la entidad por parte de equipos de cómputo personales o dispositivos móviles. Estará controlado y monitoreado por el UTM (Gestión Unificada de Amenazas), desde la Dirección de Gestión Tecnológica en la Entidad.

7.2 CONTROL DE ACCESO

Enunciado:

La Alcaldía Municipal de Soacha en cabeza de la secretaría general y la Dirección de Gestión Tecnológica, se compromete a realizar control de acceso a la información, sistemas y recursos de red, así como a controlar el acceso a las instalaciones por medio de un sistema de información a terceros, el busca controlar el ingreso seguro a los activos de información, sin importar si estos accesos sean electrónicos o físicos. Igualmente protege la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos, del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores, clientes o ciudadanía en general).

Directrices:

- Crear políticas de utilización de contraseñas y buscar que sean controladas por el sistema.
- La Dirección de Gestión Tecnológica, debe garantizar la implementación y operación un sistema de información de ingreso a terceros, con el propósito de controlar y registrar en una bitácora el ingreso y salida de personal externo de las diferentes secretarías, en cada una de las sedes físicas donde operen. La alcaldía contará con un sistema de información que permita llevar a cabo dicha tarea.
- El profesional de redes y comunicaciones de la Dirección de Gestión Tecnológica, como responsable de las redes e infraestructura de datos y los recursos de red de la toda la administración, debe propender porque dichas redes sean debidamente protegidas contra accesos no autorizados a través de mecanismos de control de acceso lógico.
- La Dirección de Gestión Tecnológica, debe asegurar que las redes inalámbricas de la Alcaldía Municipal de Soacha cuenten con métodos de autenticación que evite accesos no autorizados, en cada una de sus secretarías y diferentes dependencias.
- Los Usuarios son responsables de salvaguardar sus contraseñas de acceso al sistema de cómputo. Las contraseñas individuales no deben ser impresas, almacenadas en los sistemas o suministradas a cualquier otra persona. Los usuarios son responsables de todas las transacciones efectuadas con sus contraseñas.
- La Dirección de Talento Humano, está en la obligación de avisar oportunamente el ingreso, ausencia temporal, cambio de funciones o retiro del personal, a la Dirección de Gestión Tecnológica, para la activación o inactivación de cuentas en los aplicativos, generando los casos correspondientes a través de la herramienta de mesa de servicios.

- El acceso a Internet es solo de uso estrictamente laboral. Por tal razón, está restringido de acuerdo con la necesidad de acceso según el perfilamiento de usuarios que genera el área a cargo de la Dirección de Gestión Tecnológica.
- La clave de inicio de sesión al dominio de red, debe ser solicitada en todos los computadores, se habilita al momento de configurar el equipo y es una clave que debe ser cambiada por el usuario como primer paso de inicialización después de encendido el computador.
- Las contraseñas de usuario de red y de los diferentes aplicativos, deben ser alfanuméricas e incluyendo por lo menos un signo especial, la primera letra debe ser mayúscula, con mínimo 8 caracteres. No se debe aceptar las últimas 6 claves utilizadas por el usuario y/o el nombre de usuario de la red. La vigencia máxima es de 30 días calendarios, momento en el cual debe ser cambiada, y el sistema lo solicitará.
- El intento de acceso a red y a los diferentes aplicativos será bloqueado con 5 intentos fallidos al digitar la contraseña. El desbloqueo de la contraseña será realizado por el área a cargo de la Dirección de Gestión Tecnológica.
- Todos los accesos a servidores de datos y a instalaciones de procesamiento de información, áreas de infraestructura tecnológica estarán limitados. Las áreas de informática deberán tener acceso restringido a personas no autorizadas, según el responsable del área, al igual que los centros de cableado de equipos en los centros de datos, plantas eléctricas y cuartos de UPS.
- Los equipos de cómputo de usuario externos que se conecten o deseen conectarse a las redes de datos de la Alcaldía Municipal deben cumplir con todos los requisitos o controles para autenticarse en ellas (contar con antivirus y sistema operativo debidamente licenciado) y únicamente podrán realizar las tareas para las que fueron autorizados.
- Para la conectividad a tomacorrientes de todos los equipos de propiedad de la administración deben ser de corriente regulada y con polo a tierra), no se deben conectar otros equipos que interfieran con el consumo de energía (teléfonos celulares personales, dispositivos tablet, o portátiles de usuarios externos).
- Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.
- Evitar el acceso de usuarios no autorizado a sistemas y aplicaciones, definiendo roles y permisos de acceso controlado.
- Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.
- Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.
- Todos los funcionarios, deberán portar el carnét en un lugar visible, permitiendo con esto una mejor identificación y control de las personas que ingresan y transitan en la

Entidad. Los usuarios externos deberán portar un carnet de identificación de Visitante en un lugar visible.

Prohibiciones:

- **Está estrictamente prohibido** el ingreso de usuarios externos sin que se realice un registro en el sistema de información de control de acceso a cada una de las instalaciones físicas de la Alcaldía.
- **Está estrictamente prohibido** generar varios perfiles de usuario a una sola persona en un mismo aplicativo (dominio, asignación de licencia de Microsoft, correo electrónico y demás aplicativos de software).
- **Está estrictamente prohibido,** utilizar autenticación de otros usuarios para ingresar a la información, debe utilizar única y exclusivamente la generada para cada usuario. Lo anterior, será reportado para la toma de correctivos pertinentes.
- **Está estrictamente prohibido,** Ingresar a los centros de cableado, centro de datos, área de infraestructura tecnológica, espacio de planta eléctrica y UPS de personal externo no autorizado por el área a cargo de la Dirección de Gestión Tecnológica. Se debe generar bitácora de personal autorizado en caso de que aplique.

7.3 NO REPUDIO /

Enunciado:

La Alcaldía Municipal de Soacha se compromete a generar mecanismos de control de usuarios (log de transacciones) en los sistemas de información IN-HOUSE, arrendados o adquiridos; de tal manera que quede una trazabilidad de los acontecimientos que han ido afectando a un sistema informático (programa, aplicación, servidor, etc.), así como el conjunto de cambios que estos han generado, y que se haga seguimiento a los mismos, de tal manera que un usuario no pueda negar su responsabilidad sobre un cambio en los ejercicios de intercambio electrónico de la información. En la construcción, arrendamiento o por compra de aplicaciones o sistemas de información nuevos o existentes garantiza que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

Directrices:

- El usuario final responde por la información enviada desde medios institucionales (sistemas de información, correo electrónico y etc).
- Incluir log (Bitácora de transacciones), que generen la trazabilidad en la modificación de cualquier dato o información en los sistemas de información.
- Todas las aplicaciones IN-HOUSE, arrendados o adquiridos deben cumplir dentro de la arquitectura de funcionalidad un módulo de roles y permisos, a fin de evitar desbordamiento de los datos en el sistema y poder establecer un mayor control.

- La Dirección de Gestión Tecnológica debe proveer los respectivos mecanismos de seguridad consignados para el tratamiento de mensajes electrónicos en la Ley 527 de 1999 "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las Entidades de certificación y se dictan otras disposiciones", como son entre otros, encriptación de datos y firmas digitales, y en las demás disposiciones legales que rigen la materia.

Prohibiciones:

- **Está totalmente prohibido** implementar Sistemas de Información, que no cuenten con un módulo de supervisión (log de transacciones), y módulo de administración de roles y usuarios. Y todos los sistemas de información desarrollados en la modalidad IN-HOUSE, arrendados, o comprados deberán contar con dicho módulo).
- **Está totalmente prohibido** utilizar otra máquina diferente a la asignada, para enviar correos electrónicos o procesar información en los diferentes SI, de la administración.

7.4 PRIVACIDAD Y CONFIDENCIALIDAD

Enunciado:

La Alcaldía Municipal de Soacha se compromete a definir una política de tratamiento y protección de datos personales, que deben ser aplicados, conforme a lo establecido en la normatividad vigente (Ley 1581 de 2012 – Decreto 1377 de 2013).

Directrices:

- La clave de usuario del acceso al dominio de red será la misma para el correo electrónico, Microsoft Office 365, mesa de servicios e intranet de la entidad.
- Para todas las bases de datos de la administración se debe garantizar el control del manejo de la información de datos personales frente a su tratamiento automatizado o no, en lo que respecta a su utilización, almacenamiento, organización y acceso. Como mínimo se debe atender los siguientes ítems: a) Ámbito de aplicación, b) Excepción al ámbito de aplicación de las políticas de tratamiento de datos personales, c) Los 8 Principios del tratamiento de datos personales (Legalidad, finalidad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad, confidencialidad), d) Derechos de los titulares, e) Autorización del titular, f) Deberes de los responsables del Tratamiento.
- Inscribir las bases de datos y mantenerlas actualizadas en la Superintendencia de Industria y Comercio.

- Todos los usuarios deben aceptar los acuerdos de confidencialidad pertinentes, en los casos cuando un Sistema de Información permita crear el registro por ellos mismos.
- Solicitar a la Dirección de Talento Humano y la Secretaria Jurídica los acuerdos de confidencialidad necesarios para todos los tipos de usuarios, hacia la protección de la información de la entidad. Identificar, revisar regularmente y documentar todos los requisitos para evitar la divulgación no autorizada de la información de la Entidad.
- La información laboral institucional debe ser remitida y recibida por medios institucionales (Mensajería interna electrónica, correo institucional etc).

Prohibiciones:

- **Está totalmente prohibido** generar información a terceros de usuarios que reposen dentro de las bases de datos, sin una orden legal por parte de entidades del estado (Policía, procuraduría, fiscalía, contraloría entre otros).
- **Está totalmente prohibido** el manejo de datos físicos, para el usuario inadecuado, por parte de todo funcionario de la Administración. So pena de entrar y ser vinculado a procesos disciplinarios.

7.5 INTEGRIDAD

Enunciado:

Todo usuario debe utilizar los activos de información de la administración Municipal de Soacha de manera responsable, profesional, ética y legal. En particular, la Alcaldía velará porque toda la información verbal, física o electrónica, sea entregada o transmitida integralmente, sin modificaciones ni alteraciones, al destinatario correspondiente. Igualmente, la Administración protege su información de las amenazas originadas por parte del personal.

Directrices:

- Monitorear la carga de tráfico de la red y cuando sea necesario tomar acción para proteger la integridad y operatividad de sus redes. Se debe garantizar la integridad de los datos de cada usuario dentro de los Sistemas de Información.
- Mantener la privacidad de las comunicaciones personales y un nivel de servicio apropiado, que afecten el tratamiento de datos de los usuarios.
- La información generada y recibida en la Alcaldía, debe ser usada por los usuarios únicamente para los propósitos de la misión de la entidad, por las funciones propias de su cargo y para responder por información de los entes de control o terceros (previa autorización del jefe inmediato o del jefe de la dependencia responsable de la información).

Prohibiciones:

- **Está totalmente prohibido** la modificación de datos personales de los usuarios sin plena autorización y aceptación de estos. Aplica para todas las bases de datos procesadas en los Sistemas de Información de la Alcaldía.

7.6 DISPONIBILIDAD DEL SERVICIO E INFORMACIÓN Y/O CONTINUIDAD DEL NEGOCIO

Enunciado:

La Alcaldía Municipal de Soacha adquiere el compromiso en disminuir los posibles efectos de las interrupciones en los sistemas de información o el normal funcionamiento de la infraestructura tecnológica; y asegurar los procesos críticos con los controles necesarios documentados preventivos y de auto recuperación. La Dirección de Gestión Tecnológica, debe garantizar los niveles de disponibilidad de acuerdo con los acuerdos de nivel de servicio establecidos, incluyendo la segregación de ambientes y gestión de cambios para el control de los sistemas de información. Con esto, se garantiza la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

Directrices:

- Generar un plan de la continuidad o plan de contingencia informático, por parte del profesional líder de infraestructura tecnológica.
- Generación de bitácora donde se documente los hallazgos o interrupciones para su estudio y búsqueda de mejora continua en el aspecto vulnerado y reforzar riesgos informáticos.
- Aplicar el plan de continuidad o plan de contingencia informático, a fin de restablecer los servicios que puedan afectar el acceso a la información de los clientes o ciudadanía.
- Las instalaciones de procesamiento de información se deben implementar con una estructura de arquitectura suficiente para cumplir los requisitos de disponibilidad.
- Se deben establecer niveles de servicio para todos los servicios ofrecidos y recibidos en la Dirección de Gestión Tecnológica.
- Todos los cambios en los servidores y equipos de red deben estar a cargo de la Dirección de Gestión Tecnológica, incluyendo la instalación de nuevo software, el cambio de dirección IP, la reconfiguración de routers, y switchs, cualquier novedad y/o puesta en producción de servicios tecnológicos en hardware y/o software, deben ser documentados y debidamente por la Dirección de Gestión Tecnológica. Esto es para prevenir cambios apresurados que puedan causar interrupción de los servicios de red o acceder en forma inadvertida a información confidencial.

- Se debe probar la efectividad del plan de recuperación de BD por lo menos 1 vez anual con enfoque mejora continua.
- Asegurar la protección de los activos de la organización que sean accesibles a los proveedores, clientes internos o externos y/o ciudadanía.
- Establecer la segregación de ambientes de infraestructura tecnológica y desarrollo de software, para minimizar los riesgos de puesta en funcionamiento de cambios y nuevos desarrollos con el fin de minimizar el impacto de la indisponibilidad del servicio durante las fases de desarrollo, pruebas y producción. Se deben ubicar Servidores diferentes para cada acción.

Prohibiciones:

- **Está estrictamente prohibido,** generar cambios en las configuraciones de hardware y/o software tecnológico sin la documentación de acciones de cambios.
- **Está estrictamente prohibido,** generar las pruebas en el ambiente de producción correspondiente.

7.7 REGISTRO Y AUDITORIA

Enunciado:

La Alcaldía Municipal de Soacha se compromete a realizar auditorías periódicamente a los sistemas y actividades relacionadas a la gestión de activos de información en cabeza de la Dirección de Gestión Tecnológica, así como a llevar un control de histórico de registros de cualquier evento de seguridad ocurrido. Garantiza a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

Directrices:

- Todos los Sistemas de Información instalados en la Alcaldía Municipal de Soacha, generarán registros de auditoria con la información del registro y monitoreo de eventos de seguridad.
- Se desarrollarán las auditorías a que haya lugar, según la programación informada por la Oficina de Control Interno.
- Garantizar la evaluación de los controles, la eficiencia de los sistemas, el cumplimiento de las políticas y procedimientos de la Alcaldía Municipal de Soacha; así como recomendar las deficiencias detectadas a Gobierno Digital.

- Oficina de Control Interno de Gestión tiene la responsabilidad de llevar las auditorías periódicas (mínimo una anualmente) a los sistemas de información y actividades relacionadas a la gestión de activos de información de acuerdo con la normatividad vigente.
- Anualmente revisar los niveles de riesgo de los activos de información de la Alcaldía Municipal de Soacha.
- La Dirección de Gestión Tecnológica, monitorea y registra los eventos de seguridad vulnerados. (Bitácora).
- La Oficina de Control Interno de Gestión revisará de forma independiente el cumplimiento con las políticas, normas de seguridad y cumplimiento técnico del MPSI (incluida las actividades relacionadas con los activos de información) que adopte la Alcaldía Municipal de Soacha, mínimo una vez anualmente.
- La Secretaría Jurídica de la Alcaldía Municipal de Soacha, revisará la legislación aplicable y de los requisitos contractuales, en conjunto con el manejo de los derechos de propiedad intelectual en los desarrollos de Sistemas de Información INHOUSE-ARRENDADOS-COMPRADOS.
- La Secretaria Jurídica de la Alcaldía Municipal de Soacha, será apoyo para la verificación legal de la ley de protección y privacidad de datos personales, la reglamentación de registros y criptografía interna.
- La Secretaria Jurídica incluirá dentro de las obligaciones contractuales, la responsabilidad del óptimo manejo y tratamiento de datos en los Sistemas de Información de acuerdo con la Normatividad Vigente.
- Establecer un esquema recomendado de trabajo para la Alcaldía Municipal de Soacha, para la eficaz implementación del sistema de gestión de seguridad de la información en su alcance "Proceso a cargo del área a cargo de la gestión de tecnologías de la Información en la Entidad".

Prohibiciones:

- **Está estrictamente prohibido,** la adquisición de software o desarrollo INHOUSE, sin que cumplan con los Niveles de Seguridad mínimos y tratamiento de datos según la normatividad vigente.
- **Está estrictamente prohibido**, la contratación de personal de la Dirección de Gestión Tecnológica debe permitir que se cumplan con las competencias mínimas que puedan garantizar la seguridad de Activos de Información.

7.8 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Enunciado:

La Alcaldía Municipal de Soacha documentará la gestión de eventos, incidentes y vulnerabilidades de seguridad de la información.

Directrices:

- Dirección de Gestión Tecnológica debe asegurar un enfoque coherente, eficaz y documentado (Bitácora), para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades, estará dando Informe a la Oficina de Control Interno de Gestión.
- Se deben Reportar los incidentes de seguridad por medio de la herramienta de Mesa de Servicios de la Dirección de Gestión Tecnológica, en donde se verificará la pertinencia del mismo y se mantendrá la trazabilidad al caso correspondiente. En caso de quien detecte el incidente de seguridad sea el técnico o profesional de la mesa de servicio, avisará a los interesados y reportara el seguimiento en el caso generado hasta lograr la solución.
- La trazabilidad de los casos generados, documentos o registros de seguimiento deben quedar almacenados en la herramienta Mesa de Servicios de la Dirección de Gestión Tecnológica en la Entidad.
- Todo tipo de incidente de seguridad debe ser reportado a la Dirección de Gestión Tecnológica, y este a su vez al Líder encargado del proceso de Gobierno digital de la Alcaldía Municipal de Soacha.
- Gobierno digital de la Alcaldía Municipal de Soacha, debe garantizar el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas en temas de seguridad.

Prohibiciones:

Está estrictamente prohibido, No llevar un control de incidentes presentados que afecten la seguridad de la información en la herramienta mesa de servicios de la Dirección de Gestión Tecnológica en la Entidad – Mesa de Servicios.

Está estrictamente prohibido, No informar a la Oficina de control Interno de Gestión los incidentes presentados que den lugar a la afectación de la seguridad de la información del Municipio.

7.9 SEGURIDAD DIGITAL

Enunciado:

La Alcaldía Municipal de Soacha se compromete a fortalecer la seguridad en el entorno digital, de tal manera que permita aumentar la confianza del ciudadano en sus servicios TIC. Las aplicaciones digitales que se generen buscarán la prosperidad económica y social, y la alcaldía vela por la ciberseguridad, por enfrentar nuevos tipos de crimen en tratamientos de datos, delincuencia y otros fenómenos que afecten la seguridad de la Alcaldía Municipal.

Directrices:

- Generar el autodiagnóstico anual utilizando la herramienta de MINTIC relacionado con TICs, y lograr un enfoque de mejora continua.
- Diseñar, ejecutar y medir una estrategia de comunicaciones para sensibilización y concientización de la Seguridad Digital, de acuerdo con el plan de comunicaciones establecido, a todo el personal de las diferentes dependencias de la Alcaldía Municipal de Soacha.
- Realizar trabajo interdisciplinario para identificar vulnerabilidades en seguridad digital en toda la Administración Municipal.
- Definir enfoque de gestión de riesgo en ciberseguridad y plan de tratamiento a seguir en todo lo referente a seguridad Digital.

7.10 SEGURIDAD DEL PERSONAL

Enunciado:

- La Alcaldía Municipal de Soacha mediante la Dirección de Talento Humano debe notificar al área a cargo de la Dirección de Gestión Tecnológica en la Entidad todas las novedades del personal directo e indirecto tales como ingresos, traslados, encargos, retiros y vacaciones, a fin de realizar los respectivos ajustes y actualización de datos en las plataformas correspondientes.

Directrices:

- Seguridad previa a la contratación del personal: Para toda persona que ingrese a la Alcaldía Municipal, la Dirección de Recursos Humanos debe asegurar las responsabilidades sobre seguridad de manera previa a la contratación. Esta tarea debe reflejarse en una adecuada descripción del cargo y en los términos y condiciones de la contratación.
- Seguridad Durante la Vinculación: La Dirección de Recursos Humanos debe desarrollar un programa efectivo y continúo de concientización de protección de la información para todo el personal. También se requiere de capacitación específica en administración de riesgos tecnológicos para aquellos individuos que están a cargo de responsabilidades especiales de protección y los conceptos básicos con que debe cumplir todo colaborador
- Es responsabilidad y deber de cada funcionario de la Alcaldía Municipal de Soacha asistir a las charlas de concientización en seguridad de la información que la entidad programe y aplicar la seguridad según las políticas y los procedimientos establecidos por la Alcaldía Municipal de Soacha.
- Finalización o Cambio de Puesto: La Dirección de Talento Humano debe asegurar que todos los funcionarios de planta, funcionarios contratistas, colaboradores y/o asesores, que salgan de la entidad o cambien de puesto de trabajo, hayan firmado un acuerdo de confidencialidad, cuyo cumplimiento será vigente hasta que la Alcaldía Municipal de Soacha lo considere conveniente, incluso después de la finalización del contrato. La Dirección de Recursos Humanos se asegurará que la salida o movilidad de los colaboradores, contratistas o terceros sea gestionada hasta la completa devolución de todos los activos y retirada de los derechos de acceso.

8. IMPLEMENTACIÓN DE LA POLÍTICA

El Ministerio TIC a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, dando cumplimiento a sus funciones, a través de las cuales contribuye a la construcción de un Estado más eficiente, más transparente y participativo, publica El Modelo de Seguridad y Privacidad de la Información, para dar cumplimiento a lo establecido en el componente de seguridad y privacidad de la información de la estrategia de gobierno digital. Mediante el aprovechamiento de las TIC y el modelo de seguridad y privacidad de la información, se trabaja en el fortalecimiento de la seguridad de la información en las entidades, con el fin de garantizar la protección de esta y la privacidad de los datos de los ciudadanos y funcionarios de la entidad, todo esto acorde con lo

expresado en la legislación colombiana.

El Modelo de Seguridad y Privacidad de la Información – MSPI, por medio de un compendio de buenas prácticas conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

LINEAMIENTO

La Alcaldía Municipal de Soacha, se compromete a implementar un modelo de gestión de Seguridad y Privacidad de la Información sistemático, cíclico, y de riesgo de seguridad digital, de acuerdo con los lineamientos consignados en esta política. El modelo debe evidenciar claramente las siguientes etapas:

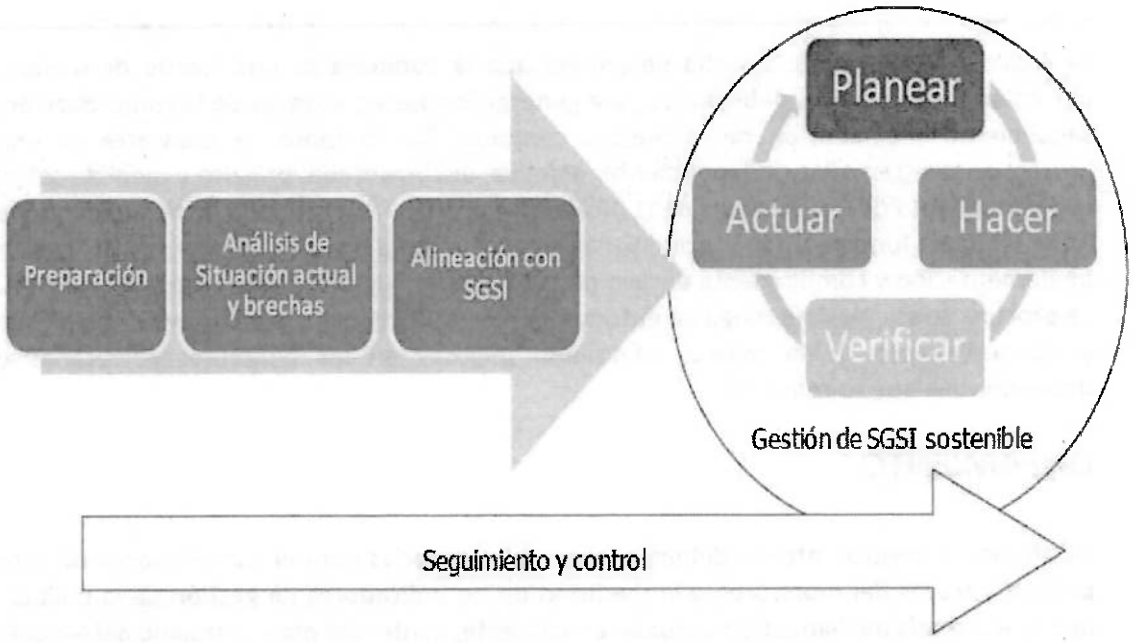

Imagen 1. Ciclo PHVA Tomado de: https://docplayer.es/5698325-Modelo-de-seguridad-de-la-informacion-luis-mauricio-vergara-jimenez-lvergara-mintic-gov-co-maovergara-enero-de-2013.html

Para la Alcaldía Municipal de Soacha, el presente modelo de Seguridad y Privacidad de la información incrementa la transparencia en la gestión pública y promueve el uso de mejores prácticas de seguridad de la información y riesgos de seguridad digital. Asegura que exista un grupo interdisciplinario y apoyo administrativo para soportar la administración y desarrollo de iniciativas sobre seguridad de la información, a través de compromisos apropiados y uso de recursos adecuados en la Alcaldía, así como de la formulación, adopción y mantenimiento de la Política de Seguridad y Privacidad de la Información y de Riesgo de Seguridad Digital de la entidad, acordes en el ciclo de implementación PHVA.

9. MEDICIÓN Y MONITOREO DEL CUMPLIMIENTO DE LA POLÍTICA

La Alcaldía Municipal de Soacha determina que la auditoria es una fuente de mejora, permitiendo conocer las debilidades para generar fortalezas, a través de la comprobación, seguimiento y evaluación de la mejora continua. Por lo tanto, se convierte en una herramienta sistemática, independiente, objetiva, documentada, práctica y medible sobre el cumplimiento de los objetivos de la Alcaldía en el SGSI y es allí donde la mejora continua tiene un papel fundamental. Las auditorias apoyan la toma de decisiones frente al nivel de implementación y complementa el ciclo de mejora continua en relación con el ciclo PHVA. Se procura que la Alcaldía tenga un enfoque de seguridad en el cual se incluya el desarrollo y mantenimiento de la misma, realizando mejoras en las diferentes secretarías y dependencias que se requiera.

LINEAMIENTO

La oficina de control interno deberá realizar las auditorías para el cumplimiento de esta política a través del monitoreo a la medición de los indicadores de gestión de la política, que la secretaría de Planeación apruebe anualmente, dentro del plan de trabajo del Modelo de seguridad y privacidad de la información y seguridad digital.

Los objetivos, metas e indicadores del Modelo de seguridad y privacidad de la información y seguridad digital de la Información, deberán estar alineados con cada uno de los lineamientos aquí escritos. De acuerdo, con la siguiente tabla:

ITEM	LINEAMIENTO	META	INDICADOR
7.1	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Oficializar el comité de seguridad y privacidad de la información y seguridad digital de la Información según el MIPG en el transcurso del año 2020 a través del recurso que maneje la secretaría de Planeación.	Creación según el MIPG del comité de seguridad y privacidad de la información y Seguridad digital de la Información.
7.2	GESTIÓN DE ACTIVOS	Se desarrollará en la Fase de ejecución.	Según el PHVA EN LA FASE **Hacer.**
7.3	CONTROL DE ACCESO	Se desarrollará en la Fase de ejecución.	Según el PHVA EN LA FASE **Hacer.**
7.4	NO REPUDIO	Se desarrollará en la Fase de ejecución.	Según el PHVA EN LA FASE **Hacer.**
7.5	PRIVACIDAD Y CONFIDENCIALIDAD	Se desarrollará en la Fase de ejecución.	Según el PHVA EN LA FASE **Hacer.**
7.6	INTEGRIDAD	Se desarrollará en la Fase de ejecución.	Según el PHVA EN LA FASE **Hacer.**
7. 7	DISPONIBILIDAD DEL SERVICIO E INFORMACIÓN Y/O CONTINUIDAD DEL NEGOCIO	Se desarrollará en la Fase de ejecución.	Según el PHVA EN LA FASE **Hacer.**
7.8	REGISTRO Y AUDITORÍA	Se desarrollará en la Fase de ejecución.	Según el PHVA EN LA FASE **Hacer.**
7.9	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.	Se desarrollará en la Fase de ejecución.	Según el PHVA EN LA FASE **Hacer.**
7.10	SEGURIDAD DIGITAL.	Se desarrollará en la Fase de ejecución.	Según el PHVA EN LA FASE **Hacer.**

Tabla 2 - Seguridad y Privacidad de la Información y Seguridad Digital – Indicadores - Alcaldía Municipal de Soacha.
Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf

10. PREPARACIÓN PARA LA CONTINUIDAD FRENTE A INCIDENTES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

La implementación de un proceso de preservación de la información pública ante situaciones súbitas de interrupción, permite minimizar el impacto y recuperación por perdida de activos de información de la toda entidad, hasta un nivel aceptable mediante la combinación de controles preventivos y de recuperación. En este proceso es conveniente identificar los procesos críticos que puedan afectar la continuidad del negocio e integrar los requisitos de la gestión de la seguridad de la información de la continuidad del negocio con otros requisitos de continuidad relacionados con aspectos tales como operaciones, personal, materiales, transporte e instalaciones. Las consecuencias de eventos disruptivos (desastres, fallas de seguridad, perdida del servicio y disponibilidad del servicio) deberían ser sometidas a un análisis del impacto del negocio (BIA – GUÍA 11 Mintic).

LINEAMIENTO

La Alcaldía Municipal de Soacha en cabeza de la Oficina de Dirección de Gestión Tecnológica -OGTI, se compromete a desarrollar e implementar un plan de continuidad o plan de contingencia informático que permita garantizar la restauración oportuna de las operaciones esenciales. La correcta implementación de la gestión de la continuidad del negocio disminuirá la posibilidad de ocurrencia de incidentes disruptivos y, en caso de producirse, la Alcaldía estará preparada para responder en forma adecuada y oportuna, de esa manera se reduce de manera

significativa un daño potencial que pueda ser ocasionado por ese incidente.
La gestión de la continuidad del negocio deberá buscar los siguientes objetivos:

- Responder al cambiante ambiente de riesgos.
- Asegurar la continuidad de las operaciones críticas del negocio soportadas por servicios de TIC.
- Estar preparado para responder antes de que una disrupción de los servicios de TIC ocurra, identificar los eventos o las series de eventos relacionados provenientes de incidentes.
- Responder y recuperarse de incidentes y/o desastres y fallas.

Para la gestión de la continuidad se deben seguir las fases del modelo de gestión sistemático y cíclico de Seguridad y Privacidad de la Información y de riesgo de seguridad digital y la preparación de las TIC para la continuidad del negocio (IRBC), la hace referencia al sistema de gestión que complementa y soporta la continuidad del negocio de la entidad. La siguiente ilustración muestra el Marco de Continuidad del negocio para Seguridad y Privacidad de la Información y de Riesgo de Seguridad Digital que se debe implementar en la Alcaldía Municipal de Soacha.

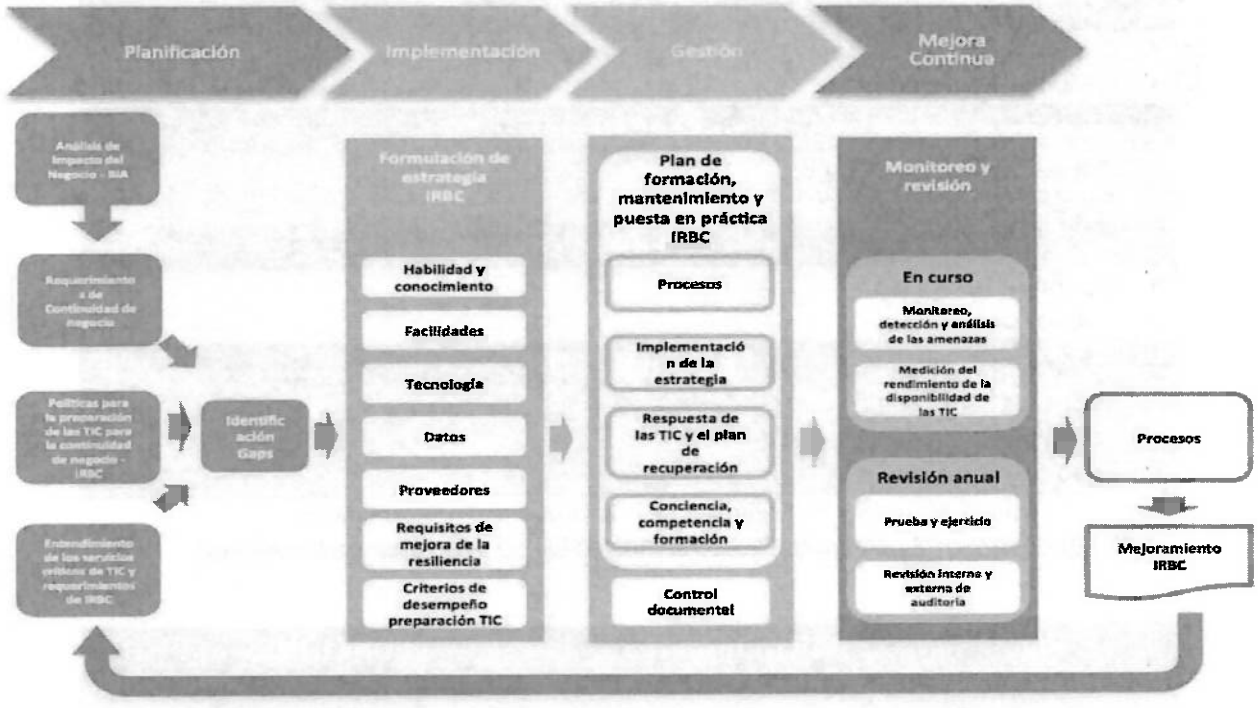

Imagen 2. Marco Continuidad del Negocio para Seguridad y Privacidad de la Información
Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_G10_Continuidad_Negocio.pdf

10. ROLES Y RESPONSABILIDADES DE LA POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

Las máximas autoridades de la Alcaldía Municipal de Soacha deben aprobar este lineamiento y son responsables de su implementación y sus modificaciones, por esta razón deben impulsarse la creación de los siguientes roles que garanticen su cumplimiento

La Imagen No.3 muestra la estructura requerida para el establecimiento de la política de seguridad y privacidad de la información y seguridad digital y en la Tabla

No.3; se encuentran descritos los principales roles y funciones en lo referente al desarrollo de esta política:

ESTRATÉGICO
▪ Comité Institucional de Gestión y desempeño o quien haga sus veces ▪ Oficial de Seguridad
TÁCTICO
▪ Oficina de Control Interno ▪ Entidades Externas
OPERATIVO
▪ Equipo del proyecto ▪ Dueños de Procesos
PARTICIPANTES
▪ Todos los Funcionarios ▪ Todos los Ciudadanos ▪ Todos los proveedores

Imagen 3. – Equipo de Gestión de Seguridad de la Información en las entidades
Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_G4_Roles_responsabilidades.pdf

ROL	PARTICIPANTES	FUNCIONES
		* Liderar el proceso de gestión de incidentes de seguridad, así como la posterior investigación de dichos eventos para determinar causas, posibles responsables y

Oficial de Seguridad	**Oficial de Seguridad**	recomendaciones de mejora para los sistemas afectados, ayudando con las cuestiones disciplinarias y legales necesarias. * Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio. * Realizar y/o supervisar pruebas de vulnerabilidad sobre los diferentes recursos tecnológicos para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información. * Definir, seguir y controlar la estrategia de la OGTI que permita lograr los objetivos y minimizar de los riesgos de la institución. 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. * Verificar el cumplimiento de las obligaciones legales y regulatorias del estado relacionadas con la seguridad de la información. * Desarrollar y supervisar los resultados del plan de formación y sensibilización establecido para la entidad, con el fin de identificar oportunidades de mejora * Generar y monitorear el cronograma de la implementación del Modelo de Seguridad y privacidad de la información.

		* Velar por el mantenimiento y actualización de la documentación del proyecto, su custodia y protección.
Oficina de Control Interno.	**Profesional(s) delegado por la Alcaldía.**	* Realizar las auditorías periódicas (mínimo una anualmente) a los sistemas y actividades relacionadas a la gestión de activos de información de acuerdo a la normatividad vigente.
Entidades Externas	**MINTIC – Subdirección de TI, Área de Seguridad y Privacidad de La información.**	* Cómo Oficina Transversal a todas las entidades del estado, brindará asesoría con base en su punto de vista sistemático en todos los procesos que la Alcaldía Municipal de Soacha genere en el Proyecto de la implementación de Seguridad de la Información.
Equipo del Proyecto	***Profesionales designados por el Comité de Seguridad de la Información de las diferentes áreas.** ***Profesional de Administración de Bases de Datos y Tratamiento de datos personales.**	* Apoyar al Oficial de Seguridad al interior de la entidad, de acuerdo al cronograma establecido * Coordinar la interacción con consultores externos * Analizar el riesgo de los activos de información de la Alcaldía Municipal de Soacha y verificar la aplicación de las medidas de seguridad necesarias para la protección de la misma. * Oficiar como consultores de primer nivel en cuanto a las dudas técnicas y de procedimiento que se puedan suscitar en el desarrollo del proyecto. * Tomar las decisiones sobre las bases de datos personales a que hubiere lugar y direccionar las actividades de los encargados de los datos personales * Generación, revisión, aprobación, seguimiento, apoyo y/o plan de mejora para el cambio de protocolo IPV4 a IPV6. Apoyado por Mintic. * Autodiagnóstico del MPSI y seguridad digital *Apoyar con el desarrollo de la documentación de seguridad * Apoyar en

		las diversas actividades del MINTIC relacionadas
Dueños del Proceso:	**Persona de planta que ejerce como responsable de un proceso de la Alcaldía y/o aplicación especializada relacionada.**	* Actúa como el "administrador del activo de información" para todos los aspectos de seguridad de la información relacionados con el procesamiento de datos dentro de este proceso particular de la organización.* Clasificar los activos de información de su proceso, de acuerdo con el grado de sensibilidad y criticidad de la misma, documentar y mantener actualizada la clasificación efectuada, y definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia.
Usuarios de la Entidad	▪ Todos los Funcionarios ▪ Todos los Ciudadanos ▪ Todos los proveedores	*Conocer y dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente

Tabla 3 - Seguridad y Privacidad de la Información y Seguridad Digital – Roles y Responsabilidades - Alcaldía Municipal de Soacha.
Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_G4_Roles_responsabilidades.pdf

11. USO Y APROPIACION DE LA POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

Las habilidades del Recurso Humano, en muchos casos, son la principal causa de los incidentes de seguridad dentro de un sistema determinado, esto debido a que no conocen sobre seguridad de la información y su rol dentro de una Entidad. Por esto debemos prestar la suficiente atención a este recurso humano que se contrata, que puede llegar a ser el eslabón más débil en la cadena de la seguridad de la información, por lo que es necesario sensibilizarlos o capacitarlos sobre la importancia de la preservación de la disponibilidad, integridad y confidencialidad de la información.

LINEAMIENTO

La Alcaldía Municipal de Soacha en cabeza del área a cargo de la Dirección de Gestión Tecnológica en la Entidad se compromete a llevar semestralmente un programa de capacitación y sensibilización del uso y Apropiación de esta política buscando la adopción de la misma en Seguridad y Privacidad de la Información y Seguridad Digital donde se explicará de manera apropiada las reglas de comportamiento adecuadas para el uso de los sistemas y la información, que generalmente están plasmadas en las políticas y procedimientos de seguridad de la información que la Entidad, requiere que sean cumplidos por parte de todos los usuarios del sistema. Cualquier incumplimiento a las políticas, debe llevar a la imposición de una sanción, siempre y cuando el usuario haya sido adecuadamente capacitado e informado sobre todo el contenido de seguridad correspondiente a su rol y responsabilidades dentro de la Alcaldía. Teniendo en cuenta lo anterior, un plan de capacitación, sensibilización y comunicación adecuado debe llevarse a cabo con base a las siguientes 4 fases:

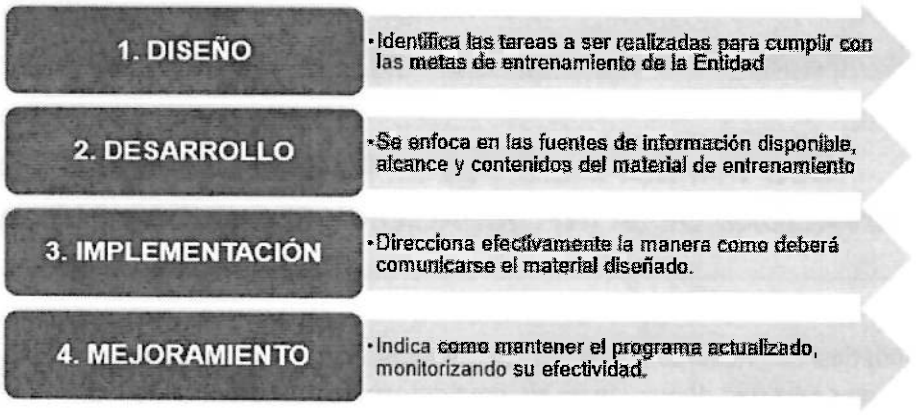

Imagen 4. – Fases Plan de sensibilización, capacitación y comunicación.
Fuente: https://www.mintic.gov.co/gestionti/615/articles-482_G14_Plan_comunicacion_sensibilizacion.pdf

Previo a la identificación de cada una de las fases, y a la aplicación de estas capacitaciones

es conveniente definir y diferenciar los siguientes términos: SENSIBILIZACIÓN, ENTRENAMIENTO, EDUCACIÓN y DESARROLLO PROFESIONAL ya que cada uno de ellos tiene un fin particular dentro del plan y dentro de la Entidad.

Imagen 5. – Relación Entre Sensibilización, Capacitación Y Educación.
Fuente: https://www.mintic.gov.co/gestionti/615/articles-482_G14_Plan_comunicacion_sensibilizacion.pdf

La alcaldía Municipal de Soacha se compromete a diseñar el Plan apropiadamente, una vez identificada las necesidades dentro de la Alcaldía en cada una de las Secretarías y/o dependencias

Es clave involucrar en el hallazgo de dichas necesidades a todo el personal, la siguiente clasificación de roles, podría ayudar a identificarlas en
toda la Entidad y cada rol tendría diferentes objetivos especiales de conocimiento:

Directivo y/o Asesor	Deben conocer y entender las leyes y directivas que forman la base del programa de seguridad, también deben comprender el liderazgo que su rol tiene y que son el ejemplo a seguir de todas las demás unidades.
Personal de Seguridad (Oficiales de seguridad)	Son los asesores expertos en seguridad, deben estar bien preparados en políticas de seguridad y buenas prácticas.

Administradores de Sistemas	Deben entender bien las políticas de seguridad, así como también conocer sobre los controles de seguridad y la relación que tienen con los sistemas que manejan.
	Estos funcionarios deben tener un buen nivel de preparación a nivel técnicos de seguridad (Implementación y prácticas de

Administradores de Sistemas y Personal de Soporte	seguridades efectivas) para soportar las operaciones críticas de la entidad de manera apropiada.
Usuarios Finales	Requieren de un alto grado de sensibilización sobre la seguridad y las reglas de comportamiento adecuadas con los sistemas que tienen a disposición.

Imagen 6. – Roles Y Necesidades En Capacitación Más Comunes
Fuente: https://www.mintic.gov.co/gestionti/615/articles-482_G14_Plan_comunicacion_sensibilizacion.pdf

12. DOCUMENTOS RELACIONADOS

DOCUMENTOS EXTERNOS

Nombre	Fecha de Publicación o versión	Entidad que lo emite	Medio de consulta
Arquitectura TI	http://www.mintic.gov.co/arquitecturati/630/w3-channel.html	MINTIC	INTERNET
Marco de referencia Arquitectura Empresarial	http://www.mintic.gov.co/arquitecturati/630/w3-propertyvalue-8114.html	MINTIC	INTERNET
Política Gobierno Digital	http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-7652.html	MINTIC	INTERNET
Detalle Política Gobierno Digital	http://mintic.gov.co/portal/604/articles-61775_recurso_2.pdf	MINTIC	INTERNET
Manual Gobierno en Línea	http://estrategia.gobiernoenlinea.gov.co/623/propertyvalues-7751_archivo_pdf_manual.pdf	MINTIC	INTERNET
Modelo Seguridad de la Información	http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html	MINTIC	INTERNET
MIPG- FURAG	http://www.funcionpublica.gov.co/web/MIPG	DNP	INTERNET

Manual de gestión de la información - GDI-TIC-MXXX	http://gaia.gobiernobogota.gov.co/sites/default/files/documentos/sig/documentos/c_gdi-tic-mxxx_manual_de_gestion_de_seguridad.docx	ALCALDÍA DE BOGOTÁ	INTERNET
Política de la seguridad de la información v1.0	http://www.alcaldiasoacha.gov.co/phocadownloadpap/Planes_2018/Plan%20de%20Seguridad%20y%20Privacidad%20de%20la%20Informacin.pdf	ALCALDÍA DE SOACHA.	INTERNET

NORMATIVIDAD VIGENTE

Norma	Año	Título	Norma
Decreto 1078	2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector TIC	http://www.mintic.gov.co/portal/604/articles-9528_documento.pdf
Decreto 1008	2018	Política Gobierno Digital	http://es.presidencia.gov.co/normativa/normativa/DECRETO%201008%20DEL%2014%20DE%20JUNIO%20DE%202018.pdf
Conpes 3854	2016	Ciberseguridad Colombia	https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf Conpes 3854
Decreto 192	2018	Por medio del cual se adopta el Sistema de Gestión – MIPG.	http://www.alcaldiasoacha.gov.co/index.php/secretarias/secretaria-de-hacienda/acuerdos/file/5761- decreto-192-de-2018.html

13. GLOSARIO DE TÉRMINOS

DERECHO DE AUTOR: "Son los derechos de los creadores sobre sus obras literarias y artísticas. Las obras que se prestan a la protección por derecho de autor van desde los libros, la música, la pintura, la escultura y las películas hasta los programas informáticos, las bases de datos, los anuncios publicitarios, los mapas y los dibujos técnicos". (OMPI, s.f.).

ENRUTADOR (ROUTER): es un dispositivo electrónico que se interconecta en la red de datos y permite que la Información, que viaja por dicha red en forma de paquetes, sea en rutada y direccionada hacia su destino.

INFRAESTRUCTURA CRÍTICA CIBERNÉTICA NACIONAL: aquella soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos, o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública.

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.

HARDWARE: Son aquellos elementos físicos (CPU, monitor, mouse, teclados, impresoras, parlantes y demás elementos que se encuentren conectados a la CPU).

POLITICAS TI: Son directrices u orientaciones que debe generar la TI y que indican la intención de la alta gerencia, con el propósito de establecer pautas para lograr los objetivos propuestos en la Estrategia de TI. Son establecidas para que perduren a largo plazo y aplican a grupos grandes de áreas o personas dentro y, muchas veces, fuera de la organización (deben ser cumplidas por los contratistas y terceros que trabajan con la organización y que por sus funciones deben tener acceso a su información y a su infraestructura). Son también

llamadas Políticas generales y/o corporativas. Para efecto de este manual, solo serán llamadas políticas.

LINEAMIENTOS TI: Son reglas que especifican una acción o respuesta que se debe seguir en una situación determinada. En sí, son especificaciones técnicas que tienen una función instrumental que responden a cómo se implementa una política. Pueden cambiar con frecuencia debido a que los procedimientos manuales, estructura organizacional, procesos del negocio y las tecnologías de la información que se mencionan cambian

rápidamente. Son también llamadas política específica o de ámbito técnico. Para efecto de este manual, solo serán llamados lineamientos.

MEJORES PRÁCTICAS: Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.

SOFTWARE LICENCIADO: Se refiere a la obtención del derecho para uso del software de computador.

SWITCH: Es un dispositivo electrónico que sirve de enlace entre las redes y subredes de datos permitiendo convertirlas en una sola red administrable.

SOFTWARE AUTORIZADO: Sistemas operacionales, paquetes de usuario final y aplicativos, que la Dirección de Tecnología de la Información ha instalado, previo visto bueno para su adquisición, actualización o renovación y con la Autorización legal del proveedor para su uso, o si se trata de licencias otorgadas con el código fuente, para generar modificaciones al mismo. El uso de Software no autorizado o adquirido ilegalmente se considera como una violación a los derechos de autor, previsto en la Ley 603 de 2000.

SEGURIDAD DIGITAL: Es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país.

SEGURIDAD DE LA INFORMACIÓN: La seguridad de la información es el conjunto de medidas técnicas, operativas, organizativas, y legales que permiten a las organizaciones resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de esta. El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos. La seguridad de la información se encarga de garantizar la integridad, confidencialidad, disponibilidad de nuestra información. Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos de información. [NTC 5411-1:2006]. Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada. [NTC 5411-1:2006]. Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos entidades o procesos no autorizados. [NTC5411- 1:2006].

SOFTWARE: Son aquellos elementos informáticos, sobre los cuales la Alcaldía Municipal de Soacha tiene el derecho de uso o de propiedad intelectual, que permiten que las labores de procesamiento de Información sirvan como herramienta de productividad y gestión. Están conformados entre otros por: A) Sistemas operativos. B) Software de ofimática, c) Software de desarrollo, D) Software comercial, E) Software de comunicaciones.

RECURSO TECNOLÓGICO: Son todos los bienes tangibles e intangibles que posee la entidad, que constituyen herramientas informáticas para el desarrollo de las labores diarias. Los recursos tecnológicos y la Información son de propiedad de la Alcaldía Municipal de Soacha y deben ser utilizados únicamente para propósitos legítimos de la entidad. Se permite que los Usuarios utilicen estos Recursos para facilitarles el desempeño de sus tareas. El uso de estos Recursos es un privilegio que puede ser revocado en cualquier momento.

USUARIO: Se refiere a todos los servidores públicos y cualquier otra persona o entidad que utilice los Recursos Tecnológicos de la Alcaldía Municipal de Soacha.

RIESGO: Es el efecto de incertidumbres sobre objetivos y puede resultar de eventos en donde las amenazas cibernéticas se combinan con vulnerabilidades generando consecuencias económicas. Riesgo de seguridad digital: es la expresión usada para describir una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital. Este riesgo puede resultar de la combinación de amenazas y vulnerabilidades en el ambiente 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. El riesgo de seguridad digital es de naturaleza dinámica. Incluye aspectos

relacionados con el ambiente físico y digital, las personas involucradas en las actividades y los procesos organizacionales que las soportan.

EDUCACIÓN: Formación destinada a desarrollar la capacidad intelectual, moral y afectiva de las personas de acuerdo con la cultura y las normas de convivencia de la sociedad a la que pertenecen.

SENSIBILIZACIÓN: Es un proceso que tiene como objetivo principal impactar sobre el comportamiento de una población o reforzar buenas prácticas sobre algún tema en particular.

ENTRENAMIENTO: Proceso utilizado para enseñar habilidades, que permitan a una persona ejecutar funciones específicas asignadas su cargo.

VIRUS: Secuencia de código que se incluye en un archivo ejecutable (llamado huésped), y cuando el archivo se ejecuta, el virus también se ejecuta, propagándose a otros programas.