PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

SECRETARIA GENERAL – SERVICIOS TECNOLÓGICOS
MUNICIPIO DE NEIVA

NEIVA, ENERO DE 2025

TABLA DE CONTENIDO

GLOSARIO

Activos: Recursos del sistema de información (datos, hardware, software, redes, soportes, instalaciones, personal y servicios)

Amenazas: Elementos de varios tipos, que pueden atacar un sistema de información, aprovechando las vulnerabilidades del mismo para causarle graves daños.

Ataques: Materialización de una amenaza contra un sistema de información.

Autenticación: Verificación de identidad de usuarios de un sistema de información.

Ciberataque: Acción organizada o premeditada de una o más agentes para causar daño o problemas a un sistema a través del Ciberespacio.

Ciberdefensa: Es el empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales

Ciberdelincuente: Individuo que realiza acciones ilícitas cometidas mediante la utilización de un bien o servicio informático.

Ciberseguridad: conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el Ciberespacio.

Confidencialidad: Protección contra revelación accidental o intencionada de información en una comunicación.

Control de acceso: Acceso concedido a recursos del sistema de información solo a usuarios autorizados.

Disponibilidad: La información estará disponible cuando un usuario autorizado la requiera.

Integridad: Invariabilidad de la información por personas no autorizadas.

Impacto: Consecuencia de la materialización de amenazas sobre los activos, aprovechando las vulnerabilidades de los sistemas de información.

ISO 27001: Norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

Malware: Programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras, y utiliza herramientas de comunicación populares para difundirse. También se propaga a través de descargas inadvertidas y ataques a las vulnerabilidades de seguridad en el software.

Riesgos: Es la probabilidad de que se materialice una amenaza, aprovechando una vulnerabilidad del sistema de información.

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información.

Vulnerabilidades: Es la probabilidad de que se materialice una amenaza contra un activo del sistema de información.

INTRODUCCIÓN

La información es el activo más importante de cualquier organización, ya que es la materia prima para proveer servicios y/o productos, y poder cumplir con las exigencias y expectativas de los clientes. Vemos que, desde los ámbitos cotidianos y académicos, hasta en compañías, multinacionales y grandes corporaciones, se hacen siempre grandes esfuerzos porque la información sea mantenida y administrada de la mejor forma posible.

Con los avances tecnológicos que se desarrollan a diario, las personas tienen muchas más herramientas tecnológicas, lo que permite reducir el tiempo para acceder a cualquier tipo de información. De esta forma, se puede aplicar eficientemente en cualquier medio para mejorar las condiciones de quienes la aprovechan de buena forma. Sin embargo, esto trae consigo amenazas, que generalmente hacen uso de vulnerabilidades lo que pone en riesgo la información, los sistemas de información y la infraestructura tecnológica que lo soporta. (Ejemplo: Ingeniería social, phishing)

Para evitar al mínimo que se presenten estas situaciones, el concepto de seguridad se convierte en una herramienta que las personas, instituciones académicas, empresas, compañías, corporaciones, o cualquier tipo de organización, utilizan para lograr que la información que poseen o que les ha sido suministrada y confiada por parte de sus clientes y/o usuarios, sea destinada para los fines descritos y empleada de forma responsable, y que no se vean afectados los diferentes procesos que con ésta se desarrollan.

Teniendo en cuenta lo anterior, las organizaciones tienden a adoptar y/o desarrollar lineamientos, reglas o políticas para propiciar el uso responsable de la información y de las herramientas que disponen para acceder a ella, y evitar que sea usada para las situaciones antes descritas. De esta forma, garantizan a sus clientes la calidad tanto de sus procesos, como de los productos y/o servicios que se ofrecen.

Si bien, las áreas de TI de las organizaciones y empresas han liderado la generación e implementación de acciones de seguridad enmarcadas en sus estrategias de TI, para preservar las cualidades de sus datos, esto no indica que solo se abarquen los activos de dichas áreas. También se cubren los procesos, trámites, servicios, sistemas de información, infraestructura, arquitectura y en general, todos los activos de las entidades. Para esto, la Gestión de la Seguridad de la Información proporciona un marco para preservar la confidencialidad, la

integridad y la disponibilidad de la información, mediante la aplicación de un proceso de gestión del riesgo, generando confianza a las partes interesadas, y manteniendo los procesos y actividades que permiten la oferta de productos y servicios.

Al igual que cualquier otra organización, la Alcaldía de Neiva es sumamente dependiente de las tecnologías de la información y las comunicaciones, para la prestación de sus servicios a la ciudadanía y la ejecución de actividades misionales, pero debido a la ejecución y apropiación de un plan estratégico de modernización en TI (en el momento existen serios riesgos en materia de seguridad de la información en todos sus niveles de la entidad, que pueden desencadenar incidentes potencialmente peligrosos y desastrosos.

Tal es la importancia, que dentro del Modelo Integral de Planeación y Gestión Institucional de la Función Pública -lineamiento general adoptado por la Alcaldía de Neiva-, los planes y políticas relacionados con seguridad de la información están inmersos en la dimensión de Direccionamiento Estratégico y Planeación, alineándolos para facilitar la gestión de las entidades públicas hacia la orientación a resultados, y a su vez articulando dichos lineamientos a los establecidos por parte del Ministerio TIC, a través de la Política de Gobierno Digital.

Esta política, antes llamada Gobierno en Línea, tiene como objetivo el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital. Aquí, la Seguridad y Privacidad corresponde a uno de los tres habilitadores transversales con lo que se soporta el desarrollo de las líneas de acción de dicha política, para cumplir con los propósitos establecidos, garantizando el buen uso de los activos de información de las entidades estatales y la privacidad de los datos, permitiendo el cumplimiento de metas de gestión de TI, y por consiguiente de las metas organizacionales, manteniendo la prestación de servicios de la entidad, y el cumplimiento las políticas y objetivos estratégicos.

Lo anterior, mediante el establecimiento e implementación del presente plan de seguridad y privacidad de la información para la entidad, promoviendo la participación de los funcionarios para que conozcan, asuman, gestionen y minimicen los riesgos de seguridad, disminuyendo las probabilidades e impactos de incidentes de seguridad, mejorando la calidad en los servicios, la confianza y satisfacción en los usuarios, cumplimiento de aspectos legales y estándares internacionales, y ahorro de costos operativos.

Sin el desarrollo de esta iniciativa al interior de la entidad, se pueden llegar a presentar situaciones como pérdida de información de ciudadanos, usuarios y/o contribuyentes, procesos y procedimientos internos; inhabilidad de servicios financieros, documentales, de planeación estratégica, web y de red; siendo éstas mitigables y corregibles, lo que puede generar estrategias de gestión de riesgos que sean replicables en otras

entidades públicas, y faciliten la identificación de elementos y aspectos comunes para su integración a otros sistemas de gestión institucional de la Administración Municipal.

Igualmente la necesidad de implementar un Sistemas de Gestión de Seguridad de la Información (SGSI), deberá estar inmersa en el presente Plan de Seguridad y Privacidad de la Información, producto del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, y teniendo en cuenta que, para su cumplimiento se requiere en gran medida la financiación con recursos de funcionamiento de la entidad, dicha implementación se establecerá por fases, garantizando así el menor impacto posible en el presupuesto anual de la entidad

El presente plan es formulado para la vigencia 2025 y se encuentra enmarcado en los planes de desarrollo nacional y departamental, así como en los lineamientos del Modelo Integrado de Planeación y Gestión y la política de Gobierno Digital.

1. PLANTEAMIENTO DEL PROBLEMA

La Alcaldía de Neiva se encuentra ubicada en el centro de la ciudad, en un edificio con más de 50 años de antigüedad, en el que inicialmente funcionaba la estación de bomberos de la ciudad, y el cual se ha ido adaptando a las necesidades, requerimientos y avances que, con el paso del tiempo, se han ido desarrollando en materia de tecnología, con el fin de brindar la mejor atención posible a la comunidad en general.

En los últimos años, y por diferentes causas de índole política y administrativa, como la falta de directrices claras y objetivas, a la falta de institucionalidad, políticas e inversión en materia de Tecnologías de la Información y las Comunicaciones - TIC establecidas al interior de la Alcaldía de Neiva, entre otras causas, la actualización y renovación de la infraestructura tecnológica de la Administración (hardware, software, datos, redes, telecomunicaciones, etc.) se ha visto estancada, o en el mejor de los casos, se ha desarrollado sin un criterio unificado, estandarizado y/o centralizado, a tal punto que al día de hoy por parte de la Administración Municipal se reconocen problemas tales como el cableado estructurado, el cual en su mayoría está implementado bajo categoría 5e, hoy ya en desuso, los problemas de administración y configuración de la red inalámbrica instalada, la disposición de servidores sin el cumplimiento de las normas técnicas para tal fin, la no existencia de un único centro de datos, y la falta de interconexión de las diferentes sedes de la Alcaldía de Neiva. Esto, entre otros aspectos, afecta la conectividad tanto a los servicios y aplicaciones que se manejan al interior de la Alcaldía como hacia servicios externos (Internet).

Teniendo en cuenta lo anterior, y ante la imposibilidad en la que se ve el personal encargado de realizar seguimiento y soporte a la infraestructura tecnológica del Municipio, al tratar de solucionar las necesidades diarias de los clientes de los diferentes procesos que se llevan a cabo en la entidad, muchas dependencias recurren a la contratación de personal de soporte y mantenimiento técnico, quienes con el ánimo de mejorar las condiciones de trabajo en las diferentes dependencias, degradan las redes híbridas existentes (redes cableadas y redes inalámbricas), mediante la conexión de equipos (Switch, Routers, Access Point, entre otros) sin posibilidad de administración y gestión organizada, con bajos niveles de protección y sin establecer políticas de control de acceso a usuarios, incluso en algunos casos, algunas de las dependencias instalan centros de datos en sus propias áreas (Secretaria de Educación y Secretaria de Hacienda). Con esto solucionan algunos de los inconvenientes existentes, pero no se articulan criterios ni acoplan soluciones que faciliten la centralización de la gestión y administración de los diferentes sistemas de información y redes estructuradas de datos.

Con base en las situaciones descritas, se hace necesario diseñar lineamientos claros bajo un Sistema de Gestión de Seguridad de la Información (SGSI) en la Administración Municipal de Neiva, basadas en estándares nacionales e internacionales, que cuenten

con el reconocimiento y aprobación por parte de la Administración, para que sean de obligatorio cumplimiento por parte de los funcionarios y servidores públicos de la Entidad, con el fin de proteger la información y los demás activos de la entidad territorial de posibles amenazas y vulnerabilidades existentes, garantizando de esta forma, los principios de seguridad de los sistemas de información: confidencialidad, integridad y disponibilidad, así como la autenticidad y trazabilidad de la misma.

2. JUSTIFICACIÓN

Al trazar lineamientos claros de administración y operación de la infraestructura tecnológica de la Administración Municipal, a través de las políticas de seguridad informática requeridas, se hace necesario previamente identificar, analizar y valorar detalladamente todos los activos de la entidad (información de los ciudadanos, aplicativos, equipos, redes de datos, mecanismos de respaldo, instalaciones, servicios y personal). De esta forma, se conocen a fondo las necesidades, amenazas, vulnerabilidades, y riesgos existentes, y se determinan los controles, medidas y acciones de mejora continua a implementar, con el fin de mitigarlos.

Es necesario además que este documento y todos sus derivados, sea de fácil entendimiento para todos los clientes, tanto internos como externos, de los diferentes procesos que se desarrollan en la Administración Municipal de Neiva, de modo que puedan apropiarse de los lineamientos a describir, e incorporarlos en sus labores cotidianas.

Teniendo en cuenta lo anterior, el Plan de Acción/Implementación que se definan a través de este proyecto, buscan garantizar la continuidad de los procesos que se desarrollan en la Administración Municipal, optimizar recursos y costos vinculados a incidentes que se puedan presentar, así como también mejorar los niveles de confianza e imagen institucional ante clientes externos e internos, a través de la implementación de controles sobre los riesgos identificados, y la definición de acciones de mejoramiento.

Así mismo, debido a que estas políticas deben estar ligadas al cumplimiento de estándares internacionales como ISO 27001, y de guías o lineamientos de buenas prácticas como ITIL y COBIT, se busca que la Alcaldía de Neiva emplee buenas prácticas aprobadas a nivel internacional, gestione la seguridad de sus procesos, procedimientos y actividades, promueve la participación y motivación de los funcionarios públicos por mantener y mejorar las políticas al interior de la entidad territorial, a sabiendas de que así mejoran sus entornos laborales, y mejora la calidad y optimización de los trámites y servicios que ofrece a la comunidad neivana.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Establecer las actividades que permitan mantener la seguridad y privacidad de la información, sistemas de información y plataforma tecnológica que circula en los procesos de la Alcaldía Municipal de Neiva, fortaleciendo el enfoque preventivo referente a la seguridad y privacidad de la Información, y garantizando su confidencialidad, integridad y disponibilidad, alineados al Modelo de Seguridad y Privacidad de la Información – MSPI de la política de Gobierno Digital del MinTIC, la norma NTC/IEC ISO 27001, la Política pública de Seguridad Digital, y los criterios de Continuidad de la operación de los servicios.

fortaleciendo el enfoque preventivo referente a la seguridad y privacidad de la Información, y garantizando su confidencialidad, integridad y disponibilidad.

3.2 OBJETIVOS ESPECÍFICOS

- Identificar, analizar y valorar los activos de información de la Administración Municipal de Neiva, sus vulnerabilidades y amenazas, para determinar los dominios que serán evaluados de acuerdo con la norma ISO/IEC 27001.

- Realizar el proceso de análisis, evaluación y tratamiento de riesgos de la información en la Alcaldía Municipal de Neiva.

- Definir las políticas y procedimientos de seguridad de la información para la Alcaldía municipal de Neiva de acuerdo con los estándares internacionales ISO/IEC 27002.

- Generar medidas que permitan garantizar los criterios de confidencialidad, integridad y disponibilidad para la información de la Alcaldía municipal de Neiva.

- Fomentar una cultura organizacional orientada hacia la seguridad y la privacidad de la información al interior de la Alcaldía Municipal de Neiva.

- Dar cumplimiento a las obligaciones legales y regulatorias del estado en materia de seguridad y privacidad de la información gestionada por la Alcaldía Municipal de Neiva.

4. ALCANCE

El Plan de Seguridad y Privacidad de la Información cobija todos los activos de información (equipos, servidores, redes de datos, cableado estructurado, instalaciones, etc.) ubicados en todas las sedes de la Alcaldía de Neiva, así como también las actividades y procesos misionales que permitan adoptar políticas y procedimientos que se establezcan sobre dichos activos, enmarcadas en un ciclo PHVA, de modo que se mejore la calidad de los servicios que se ofrecen a la comunidad neivana.

5. NORMATIVIDAD

- Constitución Política de Colombia. Artículos 15, 20, 23 y 74.
- Ley 2088 de 2012. Por la cual se regula el trabajo en casa y se dictan otras disposiciones
- Ley 2052 de 2020. Por medio de la cual se expide el código general disciplinario
- Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
    - Ley 1755 de 2015. Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
    - Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
    - Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
    - Ley 1437 de 2011. Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.
    - Ley 1341 de 2009. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones – TIC Se crea la agencia Nacional de espectro y se dictan otras disposiciones.
    - Ley 1221 del 2008. Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
    - Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
    - Ley 962 de 2005. Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.
    - Ley 594 de 2000. Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
    - Ley 527 de 1999. Por 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.
    - Ley 44 de 1993. Por la cual se modifica y adiciona la Ley 23 de 2082 y se modifica la Ley 29 de 2044 y Decisión Andina 351 de 2015 (Derechos de autor).
    - Ley 23 de 1982. Sobre derechos de autor
    - Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para

fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones. Decreto 767 de 2022. Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

- Decreto 88 de 2022. Por el cual se adiciona el Título 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los artículos 3, 5 Y 6 de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea
- Decreto 1287 de 2020. Por el cual se reglamenta el Decreto Legislativo 491 del 28 de marzo de 2020, en lo relacionado con la seguridad de los documentos firmados durante el trabajo en casa, en el marco de la Emergencia Sanitaria.
- Decreto 2106 de 2019. Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.
- Decreto 1008 del 2018. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 612 de 2018. Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
- Decreto 1499 de 2017. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- Decreto 728 de 2017. Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico
- Decreto 1074 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- Decreto 2364 de 2012. Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.

- Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- Decreto 884 de 2012 Por medio del cual se reglamenta la Ley 1221 de 2008 y se dictan otras disposiciones.
- Resolución 1838 de 2022. Por la cual se reglamentan las modalidades de teletrabajo, se establecen las condiciones de trabajo en casa y se definen los lineamientos de desconexión laboral en el MINTIC, y se deroga la resolución 1151 del 16 de mayo de 2019.
- Resolución 746 de 2022. Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021
- Resolución 500 de 2021. Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital
- Resolución 1519 de 2020. Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.

6. MARCO DE REFERENCIA

6.1 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

La Alcaldía de Neiva, cuenta con la Política General de Seguridad de la Información, aprobada mediante Resolución 0279 del 28 de diciembre de 2017, en la que se establecen los doce principios de seguridad que soportan el Sistema de Gestión de Seguridad de la Información de la Alcaldía de Neiva.

De manera general, se debe propender por una cultura de seguridad y privacidad de la información en donde se aplique las políticas, procedimiento y buenas prácticas para gestionar la información, tales como:

- Todo el personal será informado y responsable de la seguridad de la información, según sea relevante para el desempeño de su trabajo.
- El uso aceptable de los activos de información.
- Escritorio limpio y claro de la pantalla.
- La transferencia de información.
- Las restricciones a la instalación de software y el uso.
- Bloqueo de pantalla cuando se ausente temporalmente de su lugar de trabajo.
- Copia de seguridad.
- La transferencia de información.
- La protección contra el malware.
- La gestión de vulnerabilidades técnicas.
- Las comunicaciones de seguridad.
- La intimidad y la protección de la información personal identificable.

Así mismo, mediante Circular 206 del 12 de abril de 2018, se indican consideraciones y recomendaciones para el manejo adecuado de equipos e información de la entidad, difundiendo así las políticas adoptadas en materia de seguridad y privacidad de la información física y digital entre los servidores públicos de la Alcaldía de Neiva.

De igual manera se debe identificar matricialmente bajo una Metodología DOFA, las debilidades, fortalezas, oportunidades y amenazas en seguridad que actualmente posee el Municipio de Neiva a nivel tecnológico.

6.2 INVENTARIO DE ACTIVOS DE INFORMACIÓN

Durante los años 2020 - 2023, se avanzó en la identificación de inventario de activos físicos (equipos de cómputo), plataforma tecnológica y sistemas de información, mediante varias herramientas disponibles para ello, obteniendo diferentes resultados en cantidades de activos para cada una de las clasificaciones identificadas. Esto denota fallas en el proceso de eliminación y/o devolución de activos. Sin embargo, es posible

realizar clasificación y valoración de activos, que sirva de base para efectuar actualizaciones periódicas, y remitir a los entes de control cuando sea requerida dicha información.

Sin embargo, no se tiene identificado un inventario de activos de información que cumpla los parámetros de las Guías del Modelo de Seguridad y Privacidad de la Información, teniendo como referencia que un activo de información es todo aquello que genera valor a la entidad, lo que indica la falta de identificación de activos de información relacionados con información de tablas de retención documental y demás actividades y documentos de cada uno de los procesos de la entidad.

6.3 NIVEL DE MADUREZ INICIAL DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI)

La Administración Municipal realizó un autodiagnóstico sobre la implementación del Modelo de Seguridad y Privacidad de la Información en la entidad, utilizando para ello el instrumento de evaluación provisto por el Ministerio TIC, en el marco de la estrategia de Gobierno Digital, a través del cual se busca incentivar y acelerar el cumplimiento de los diferentes lineamientos de esta iniciativa entre las diferentes entidades territoriales y públicas. Este autodiagnóstico dio como resultado un promedio del 18% en la implementación de controles dispuestos en el Anexo A de la norma ISO 27001:2013.

Figura 1. Anexo A ISO27001:2013 Aplicado en la Alcaldía de Neiva.

Fuente: Evaluación MSPI Alcaldía Neiva A 30-06-2018, por Comité Institucional de Gestión y Desempeño Alcaldía de Neiva, 2018.

Esto denota un nivel de madurez inicial del MSPI en la Alcaldía de Neiva, nivel que demuestra la necesidad de consolidar los procesos de identificación de activos y de gestión de riesgos. Es importante mencionar, que se debe realizar durante la vigencia del presente plan una actualización de la medición del autodiagnóstico, pues tal como se observa en la fuente de la imagen, la última versión con la que cuenta la entidad data del año 2018, imposibilitando determinar el verdadero estado de seguridad y privacidad de la información con el que cuenta la entidad.

6.4 MATRIZ Y PLAN DE TRATAMIENTO DE RIESGOS

La Alta Dirección a través del Comité Institucional de Gestión y Desempeño aprobó en Acta del 25 de Julio de 2018 la matriz y el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información. En la matriz de riesgos se identificaron 23 riesgos extremos, y con base en estos se realizó la declaración de aplicabilidad (SoA) de controles de seguridad relevantes para la Alcaldía de Neiva, según la norma ISO27001:2013. Teniendo esto, se realizó el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, en el cual se establecen actividades a realizar para el cumplimiento de cada uno de los controles, la prioridad, el estado actual de cumplimiento, los responsables al interior de la entidad, y el plazo para la implementación de dichas actividades. Para vigencia 2023 se han identificado 33 riesgos de seguridad y privacidad de la información, siguiente la metodología de riesgos del Departamento Administrativo de Planeación.

6.5 PLAN DE CAMBIO, CULTURA Y APROPIACIÓN

Una vez aprobado el presente Plan de Seguridad y Privacidad de la Información, se diseñará el Plan de cambio, cultura y apropiación, el cual deberá ser aprobado por el Comité Institucional de Gestión y Desempeño, y en compañía del Programa de Talento Humano y el Programa de Prensa y Comunicaciones, se coordinarán diseños y medios de socialización, teniendo en cuenta los diferentes públicos objetivo: usuarios finales internos (circulares y charlas de sensibilización), usuarios finales externos (redes sociales y página web), administradores de sistemas y profesionales especializados (capacitaciones y cursos especializados), directivos (charlas de sensibilización a nivel directivo). Lo cual permita que las diseñar estrategias para socializar, apropiar, preservar e impulsar la cultura en los colaboradores de la entidad, contribuyendo al cambio organizacional para reducir los riesgos asociados y fortalecer el Sistema de Seguridad y Privacidad de la Información de la Alcaldía de Neiva.

7. PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

A continuación, se observan actividades derivadas de los controles a aplicar para la implementación del Modelo de Seguridad y Privacidad de la Información en la Alcaldía de Neiva, de acuerdo con las fechas límite para cada una de éstas, al cual se le hará seguimiento mes a mes:

Tabla 1. Cronograma de Actividades

Gestión	Actividades	Tareas	Responsable de la Tarea	Evidencia	Fechas Programación Tareas	
					Fecha Inicio	Fecha Final
Activos de Información	Definir lineamientos para el levantamiento de activos de información	Actualizar la metodología o la documentación de la gestión de levantamiento de activos de información, en el caso que aplique	Gestión Documental - Secretaria General - Gestión de Servicios Tecnológicos	Documentación actualizada	17-feb-25	31-mar-25
		Validar activos de información en el instrumento con el que cuenta la entidad	Gestión Documental - Secretaria General - Gestión de Servicios Tecnológicos	Documentación revisada	01-abril-25	04-abr-25
		Identificar nuevos activos de información en cada dependencia	Gestión Documental - Secretaria General - Gestión de Servicios Tecnológicos	Acta de Reunión	07-abril-25	30-mayo-25

	Publicación de Activos de Información	Validar y aceptar los activos de información para su publicación en sistema de gestión de la entidad	Gestión Documental - Secretaria General - Gestión de Servicios Tecnológicos	Oficio de aprobación	1-junio-25	30-junio-25
Gestión de Riesgos	Actualización de lineamientos de riesgos	Apoyar cuando se requiera la actualización de la política, metodología y lineamientos de la gestión de riesgos	Secretaria General - Gestión de Servicios Tecnológicos - MIPG	Correos electrónicos, Documentación actualizada en Sistema de Gestión Página web	17-feb-25	31-mar-25
	Identificación de Riesgos de Seguridad y Privacidad de la Información	Contexto, Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información y Seguridad Digital	Secretaria General - Gestión de Servicios Tecnológicos - MIPG	Correos electrónicos Mapas de riesgos	1-julio-25	30-sep-25
		Realimentación, revisión y verificación de los riesgos identificados (Ajustes)	Secretaria General - Gestión de Servicios Tecnológicos - MIPG	Correos electrónicos Mapas de riesgos	1-julio-25	30-sep-25
	Aceptación de Riesgos Identificados	Aceptación, aprobación riesgos identificados y planes de tratamiento	Secretaria General - Gestión de Servicios Tecnológicos - MIPG	Memorandos de aceptación mapas de riesgos	1-oct-25	31-oct-25
	Publicación	Publicación mapas de riesgos de los procesos Sistema de Gestión	Secretaria General - Gestión de Servicios Tecnológicos	Mapas de riesgos publicados Sistema de Gestión	03-nov-25	28-nov-25

	Seguimiento Fase de Tratamiento	Seguimiento implementación de controles y planes de tratamiento de riesgos los identificados (verificación de evidencias)	Secretaria General - Gestión de Servicios Tecnológicos	Seguimiento mapas de riesgo	03-nov-25	28-nov-25
Gestión de Incidentes de Seguridad y Privacidad de la Información	Publicar y Socializar el procedimiento actualizado de incidentes de seguridad de la información	Revisión, actualización y publicación cuando se requiera el procedimiento de incidentes de seguridad de la información basado en la norma ISO 27035	Secretaria General - Gestión de Servicios Tecnológicos	Documentación actualizada	14-mar-25	18-abr-25
		Socializar el procedimiento a los especialistas de atención de soportes en sitio, Mesa de Servicios	Secretaria General - Gestión de Servicios Tecnológicos	correos electrónicos, listados de asistencia	21-abr-25	30-may-25
	Gestionar los incidentes de Seguridad de la Información identificados	Seguimiento a los incidentes de seguridad de la información reportados a la mesa de servicio de acuerdo a lo establecido en el procedimiento definido.	Secretaria General - Gestión de Servicios Tecnológicos	Correos electrónicos, seguimiento al reporte de incidentes	21-abr-25	31-dic-25

Plan de Cambio y Cultura de Seguridad y Privacidad de la Información	Elaborar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información	Elaborar la documentación del Plan de Cambio, Cultura y Apropiación de Seguridad y Privacidad de la Información	Secretaria General - Gestión de Servicios Tecnológicos	Documentación actualizada en Sistema de Gestión	02-jun-25	1-jul-25
	Ejecutar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información	Implementar las estrategias del Plan de Cambio, Cultura y Apropiación de Seguridad y Privacidad de la Información	Secretaria General - Gestión de Servicios Tecnológicos	Correo electrónico, listados de asistencia	2-jul-25	31-dic-25
Matriz de verificación de Requisitos Legales de Seguridad de la Información	Elaborar la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Elaborar la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Secretaria General - Gestión de Servicios Tecnológicos - Dirección Jurídica	Documentación actualizada en Sistema de Gestión	1-oct-25	03-nov-25
Planeación	Revisión Manual Políticas de Seguridad de la Información y Resolución de Seguridad de la Información	Actualizar cuando se requiera los Manuales, Políticas, Resoluciones, documentación del SGSPI y la documentación estratégica del procesos de Seguridad y privacidad de la Información.	Secretaria General - Gestión de Servicios Tecnológicos - Dirección Jurídica - MIPG - Comité de Gestión y Desempeño	Documentación actualizada en Página Web	03-feb-25	30-dic-25
Gobierno Digital	Gobierno Digital	Actualizar el documento de autodiagnóstico de la entidad en la implementación de Seguridad y Privacidad de la Información.	Secretaria General - Gestión de Servicios Tecnológicos	Documento de Diagnostico de MINTIC para Medición del MSPI	03-feb-25	30-jun-25

Revisión de los controles de la norma ISO 27001:2013	Revisión de los controles de la norma ISO 27001:2013,	Aplicar la herramienta diseñada para realizar la validación del cumplimiento de la Política General de Seguridad y Privacidad de la Información	Secretaria General - Gestión de Servicios Tecnológicos	Herramienta diligenciada	03-feb-25	30-jun-25

Fuente: Elaboración Propia

Control de Cambios

Versión	Fecha	Descripción
1.0	17/06/2018	Versión Inicial Ing. Brayan Alexander Beleño García - Contratista Secretaría TIC y Competitividad. Revisión: Ing. Oscar Hernando Motta Valencia – Asesor TIC del Despacho.
1.1	24/01/2020	Actualización. Ing. German Yobany Beltrán Rondón, Líder de TIC – Asesor de Despacho. Ing. Juan Carlos – Contratista Secretaría de TIC y Competitividad.
1.2	30/12/2020	Actualización. Ing. German Yobany Beltrán Rondón, Secretario de TIC. Ing. Jorge Esneider Henao González – Contratista Secretaría de TIC.
1.3	28/01/2022	Actualización. Ing. German Yobany Beltrán Rondón, Secretario de TIC. Ing. Luis Ernesto Arias Méndez – Contratista Secretaría de TIC.
1.4	25/01/2023	Actualización. Ing. German Yobany Beltrán Rondón, Secretario de TIC.
1.5	26/01/2024	Actualización. Secretaría de Competitividad – Equipo TIC
1.6	13/01/2025	Actualización. Secretaria General - Gestión de Servicios Tecnológicos