Concejo Municipal
de Coveñas

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Concejo Municipal
de Coveñas

Enero 2026

CONCEJO MUNICIPAL DE COVEÑAS, SUCRE
NIT: 823.004.035-1 · Carrera 25 N° 9 - 79 Guayabal - Coveñas · Código Postal 706050
www.concejodecovenas.gov.co · concejo@concejodecovenas.gov.co - Celular: 3244115713

Concejo Municipal
de Coveñas

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

MESA DIRECTIVA - 2026

DARWIN CHICA TIRADO
Presidente

MARÍA P. MENDOZA V
Primer vicepresidente

MARTA RIOS REVUELTA
Segundo vicepresidente

KELLY J. MENA O.
Secretaria General

HONORABLES CONCEJALES

NOMBRES DE CONCEJALES	*PARTIDO POLÍTICO (BANCADA)*
CHICA TIRADO DARWIN	CENTRO DEMOCRÁTICO
DIAZ BLANCO JAVIER JOSÉ	PARTIDO FUERZA DE LA PAZ
FERIA MERCADO SADDAN ALBERTO	CENTRO DEMOCRÁTICO
HERNANDEZ JULIO ERIS RAFAEL	PARTIDO CAMBIO RADICAL
MÁRQUEZ LÓPEZ SORAIDA	PARTIDO DE LA UNIÓN POR LA GENTE
MENDOZA VEGA MARÍA PATRICIA	PARTIDO INDEPENDIENTES
NUÑEZ RINCO JAVIER SEGUNDO	PARTIDIO ALIANZA SOCIAL INDEPENDIENTE "ASI"
OLASCOAGA CUELLO LUIS EDUADO	PARTIDO CONSERVADOR COLOMBIANO.
REVUELTA AGUIRRE PEDRO ELIECER	PARTIDIO ALIANZA SOCIAL INDEPENDIENTE "ASI"
RIOS REVUELTA MARTA ISABEL	PARTIDO LIBERAL COLOMBIANO
ZUBIRIA PEROZA KEBIN ANDRÉS	CENTRO DEMOCRÁTICO

Tabla de contenido

PRESENTACIÓN

La dirección del Concejo Municipal de Coveñas, en aras de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para el Concejo Municipal de Coveñas, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

La Corporación cuenta con la Política de Seguridad y Privacidad de la Información, donde se define la normatividad y las herramientas que protegen la información de la entidad con respecto a la protección de activos de información. Asimismo, dicta los lineamientos de la información, los procesos, las tecnologías de información, hardware y software, que soportan los procesos de la entidad, apoyando la implementación del Modelo de Seguridad y Privacidad de la Información.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes del Concejo Municipal de Coveñas.
- Garantizar la continuidad del negocio frente a incidentes.

1. Introducción.

La Estrategia de Gobierno en Línea, liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), busca maximizar el uso de las TIC para fortalecer la construcción de un Estado más participativo, eficiente y transparente.

En este marco, la planificación e implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) en el Concejo Municipal de Coveñas responde a las necesidades y objetivos institucionales, los requisitos de seguridad de la información, así como a los procesos misionales y la estructura organizacional de la Corporación edilicia. Esta implementación garantiza que la protección de la información se alinee con las mejores prácticas y estándares, asegurando la confidencialidad, integridad y disponibilidad de los datos manejados por la entidad.

El Modelo de Seguridad y Privacidad de la Información (MSPI) tiene como objetivo garantizar la confidencialidad, integridad y disponibilidad de la información, asegurando la privacidad de los datos. Esto se logra mediante la implementación de un proceso de gestión del riesgo, que permite identificar, evaluar y mitigar posibles amenazas. De esta manera, el MSPI brinda confianza a las partes interesadas sobre la adecuada gestión de los riesgos asociados al manejo de la información.

El Decreto Único Reglamentario 1078 de 2015, del sector de Tecnologías de la Información y las Comunicaciones (TIC), establece el componente de Seguridad y Privacidad de la Información como parte integral de la Estrategia de Gobierno en Línea (GEL). Para el desarrollo de este componente, se ha elaborado un conjunto de documentos asociados al Modelo de Seguridad y Privacidad de la Información (MSPI), los cuales han sido utilizados por diversas entidades, tanto a nivel nacional como territorial, con el objetivo de mejorar sus estándares de seguridad de la información.

El MSPI es un modelo dinámico, que se actualiza periódicamente para mantenerse alineado con las buenas prácticas de seguridad y adaptarse a los cambios técnicos y normativos. Estas actualizaciones consideran la Ley de Protección de Datos Personales, la Ley de Transparencia y Acceso a la Información Pública, entre otras normativas relevantes para la gestión de la información.

En síntesis, el presente documento describe el Plan de Seguridad y Privacidad del Concejo Municipal de Coveñas, alineado con los objetivos, metas, procesos, procedimientos y estructura organizacional, establecidos en el **Plan Estratégico Institucional 2024 – 2027**, cuyo principal objetivo es proteger los derechos de los usuarios de la entidad y mejorar los niveles de confianza en los mismos a través de la identificación, valoración, tratamiento y mitigación de los riesgos de los sistemas de información.

2. Elementos Estratégicos Corporativos

2.1. Misión

El concejo municipal de Coveñas, es una corporación político – administrativa pública, que representa democráticamente las necesidades de la comunidad, a través del ejercicio de control político eficaz y oportuno a la administración municipal, mediante la expedición de acuerdos municipales; seguimiento y evaluación de programas y proyectos; promoviendo espacios de participación ciudadana que contribuyan al desarrollo sostenible del municipio, a través del uso adecuado de las tecnologías y equipo de trabajo competente.

2.2. Visión

El Concejo Municipal de Coveñas, en el año 2027 será reconocida corporación política – administrativa pública por ejercer un control político eficaz, oportuno y de impacto, con enfoque participativo y social, coadyuvante del desarrollo integral y el bienestar de sus habitantes.

3. **Objetivos del Plan de seguridad y Privacidad de la Información**.

3.1. **Objetivo General**.

Establecer las actividades orientadas a fortalecer el tratamiento de la información que es generada, tratada y custodiada por la entidad; con el fin de elevar su nivel de confianza con sus grupos de interés, mediante la preservación de su confidencialidad, integridad y disponibilidad, así como también la adopción de las buenas prácticas, el cumplimiento de la política de Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información y el marco legal que le sea aplicable.

3.2. **Objetivos específicos**.

- Identificar, valorar, tratar y mitigar los riesgos de los sistemas de información con el fin de proteger los activos de información, el manejo de medios, el control de acceso y la gestión de los usuarios.

- Fortalecer la seguridad de la información, además de promover y mantener la confianza de los funcionarios, contratistas y terceros, mediante el desarrollo, implementación y cumplimiento de la política general de seguridad y privacidad de la información.

- Cumplir con los principios de confidencialidad, disponibilidad e integridad de la información, garantizando la protección de los activos de información del Concejo Municipal de Coveñas – Sucre.

- Incentivar la cultura de la seguridad de la información del Concejo Municipal de Coveñas, fortaleciendo las buenas prácticas y la conciencia de los funcionarios, contratistas y terceros.

- Garantizar la continuidad mediante la implementación de planes y controles que sean necesarios de desarrollar frente a la existencia de incidentes de seguridad de la información.

- Apoyar el cumplimiento de los principios de la función administrativa correspondientes a la legalidad, economía, eficacia, contradicción y publicidad, a través de los lineamientos establecidos por la política general de seguridad y privacidad de la información.

- Garantizar la protección de la información institucional, tanto en medios físicos como digitales, mediante la implementación de controles de acceso, cifrado, autenticación, monitoreo y auditoría, asegurando que solo las personas autorizadas puedan acceder, modificar o utilizar los datos sensibles.

4. Alcance del Plan de seguridad y Privacidad de la Información.

El propósito de estas políticas es asegurar que servidores públicos, utilicen correctamente los recursos tecnológicos que la entidad pone a su disposición para el desarrollo de las funciones institucionales, dichas políticas son de obligatorio cumplimiento, el servidor público que incumpla las políticas de seguridad informática, responderá por sus acciones o por los daños causados a la infraestructura tecnológica de la empresa de conformidad con las leyes penales, fiscales y disciplinarias.

Este plan se extiende a funcionarios, contratistas, proveedores y cualquier persona o entidad que tenga acceso o realice tratamiento de la información dentro del Concejo Municipal. Asimismo, contempla la adopción de controles, normativas y buenas prácticas en materia de seguridad y privacidad, alineadas con el Marco de Referencia de Arquitectura TI, la Ley de Protección de Datos Personales y demás regulaciones aplicables.

5. Lineamientos conceptuales

A los efectos del presente plan se deberán atender los siguientes lineamientos conceptuales:

Activo de Información: Toda la información que maneja con la que cuenta una organización para un correcto funcionamiento.

Amenazas: Cualquier evento, persona, situación o fenómeno que pueda causar daño.

Análisis de Brechas: es una herramienta de análisis para comparar el estado y desempeño real de una organización, estado o situación en un momento dado.

Análisis de Riesgo: Método empleado para evaluar los riesgos informáticos y obtener respuesta de peligro.

Autenticación: acto o proceso de confirmar que algo o alguien es quien dice ser.

Autenticidad: propiedad de que una entidad es lo que afirma ser.

Ciberespacio: es una realidad simulada que se encuentra implementada dentro de los ordenadores y de las redes digitales de todo el mundo.

Confidencialidad: propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

Controles: Conjunto de mecanismos que regulan el funcionamiento de un sistema.

Disponibilidad: propiedad de ser accesible y utilizable a demanda por una entidad.

Datos abiertos: son datos primarios o sin procesar, puestos a disposición de cualquier ciudadano, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.

Dato privado: es el dato que por su naturaleza intima o reservada, y es solo relevante para el titular.

Dato público: es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas.

Estándar: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. En este documento se habla de las Norma Técnica Colombiana ISO27001:2013 e ISO31000:2013.

Gestión del riesgo: proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Incidente de seguridad de la información: Resultado de intentos intencionales o accidentales de romper las medidas de seguridad de la información impactando en la confidencialidad, integridad o disponibilidad de la información.

Información: Es un conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno. Indicación o evento llevado al conocimiento de una persona o de un grupo. Es posible crearla, mantenerla, conservarla y transmitirla.

Integridad: propiedad de exactitud y completitud.

Internet: Conjunto de redes conectadas entre sí, que utilizan el protocolo TCP/IP para comunicarse entre sí.

Intranet: Red privada dentro de una empresa, que utiliza el mismo software y protocolos empleados en la Internet global, pero que solo es de uso interno.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

LAN: (Local Área Network). (Red de Área Local). Red de computadoras ubicadas en el mismo ambiente, piso o edificio.

Log: Registro de datos lógicos, de las acciones o sucesos ocurridos en los sistemas aplicativos u operativos, con el fin de mantener información histórica para fines de control, supervisión y auditoría.

MSPI: Modelo de seguridad y privacidad de la información

Política de seguridad de información: Es el instrumento que adopta una entidad para definir las reglas de comportamiento aceptables en el uso y tratamiento de la información.

Probabilidad: Posibilidad de que una amenaza se materialice.

Riesgo: Es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o de los procesos del Concejo. Se expresa en términos de probabilidad y consecuencias.

Riesgo de seguridad y privacidad: Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización. Se mide en términos de probabilidad y consecuencias.

Seguridad informática: Se ocupa de la implementación técnica y de la operación para la protección de la información.

Seguridad de la información: Se Ocupa de evaluar el riesgo y las amenazas, traza el plan de acción y esquemas normativos. Es la línea estratégica de las Seguridad.

SGSI: Sistema de Gestión de seguridad de la Información.

Sistema de Gestión de Seguridad de la Información (SGSI): conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basando en un enfoque de gestión y de mejora a un individuo o entidad.

Trazabilidad: cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

Vulnerabilidades: Falla o debilidad en un sistema que puede ser explotada por quien la conozca.

6. Marco Normativo

6.1.Del Orden Constitucional

- **Constitución Política de 1991.** Artículos 15, 20, 23 y 74.

6.2.Del Orden Legal.

- **Ley 23 de 1982**. Sobre derechos de autor.
- **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 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 850 de 2003**. Por medio de la cual se reglamentan las veedurías ciudadanas.
- **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 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.

- **Ley 1273 de 2009**. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

- **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 1437 de 2011**. Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.

- **Ley 1450 de 2011**. Por la cual se expide el Plan Nacional de Desarrollo, 2010-2014.

- **Ley 1474 de 2011**. Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

- **Ley 1581 de 2012**. Por la cual se dictan disposiciones generales para la protección de datos personales.

- **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 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 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 2080 de 2021**. Por medio de la cual se reforma el Código de Procedimiento Administrativo y de lo Contencioso Administrativo -Ley 1437 de 2011- y se dictan otras disposiciones en materia de descongestión en los procesos que se tramitan ante la jurisdicción.

- **Ley 2088 de 2012**. Por la cual se regula el trabajo en casa y se dictan otras disposiciones.

- **Ley 2108 de 2021**. Ley de Internet como servicio público esencial y universal o "por medio de la cual se modifica la Ley 1341 de 2009 y se dictan otras disposiciones".

- **Ley 2294 de 2023** – Plan Nacional de Desarrollo 2022- 2026 "Colombia potencia mundial de la vida". Artículo 143. Transformación digital como motor de oportunidades e igualdad. Numeral 4. Promover estrategias para la identificación, prevención y control de todo tipo de violencias en entornos digitales, en coordinación con el Ministerio de Educación Nacional, con énfasis en mujeres, grupos étnicos y niñas, niños y adolescentes. Numeral 5. Implementar iniciativas de transformación digital como herramienta para la productividad, la generación de empleo, la dinamización de la economía en las regiones y la potencialización de la economía popular. Numeral 6. Fortalecer el Gobierno Digital para tener una relación eficiente entre el Estado y el ciudadano, que lo acerque y le solucione sus necesidades, a través del uso de datos y de tecnologías digitales para mejorar la calidad de vida.

6.3.Decretos de orden Nacional

- **Decreto 1377 de 2013** compilado en el Decreto 1074 de 2015. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

- **Decreto 886 de 2014**. compilado en el Decreto 1074 de 2015. Por el cual se reglamenta el Registro Nacional de Bases de Datos.

- **Decreto 103 de 2015**. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

- **Decreto 1078 de 2015** modificado por el Decreto 1008 de 2018 - Política de Gobierno Digital que contiene el Modelo de Seguridad y Privacidad - MSPI de MINTIC.

- **Decreto 1081 de 2015**. Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia. Parte 1 - Disposiciones reglamentarias generales. Título 1 - Disposiciones generales en materia de transparencia y del derecho de acceso a la información pública nacional.

- **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. financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

- **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. Artículos 1 y 2 relacionados con el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y el Plan de Seguridad y Privacidad de la Información.

- **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 Presidencial 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 338 de 2022** - Ministerio de Tecnologías de la Información y las Comunicaciones. Por el cual se adiciona el Título 21 a la Decreto 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** - Presidencia de la República. 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.

6.4.Circulares.

- **Circular 01 de 2022** - Departamento Administrativo de la Presidencia de la República. Recomendaciones de uso de servicios en la nube como medida para mitigar riesgos de seguridad digital.

6.5.Directivas Presidenciales.

- **Directiva Presidencial 03 de 2021**. Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos

- **Directiva 02 de 2022** - Presidencia de la República. Reiteración de la política pública en materia de seguridad digital.

6.6.Resoluciones.

- **Resolución N°. 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 460 de 2022** - Ministerio de Tecnologías de la Información y las Comunicaciones. Por la cual se expide el Plan Nacional de Infraestructura de Datos y Su hoja de ruta en el desarrollo de la Política de Gobierno Digital, y se dictan los lineamientos generales para su implementación.

- **Resolución 746 de 2022** - Ministerio de Tecnologías de la Información y las Comunicaciones. 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 N°.500 de 2021.

- **Resolución 01117 de 2022** - Ministerio de Tecnologías de la Información y las Comunicaciones. Por la cual se establecen los lineamientos de transformación digital para las estrategias de ciudades y territorios inteligentes de las entidades territoriales, en el marco de la Política de Gobierno Digital.

- **Resolución N°.02277 de 2025**. "Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia"

- **CONPES 3975 de 2019**. Política nacional para la transformación digital e inteligencia artificial

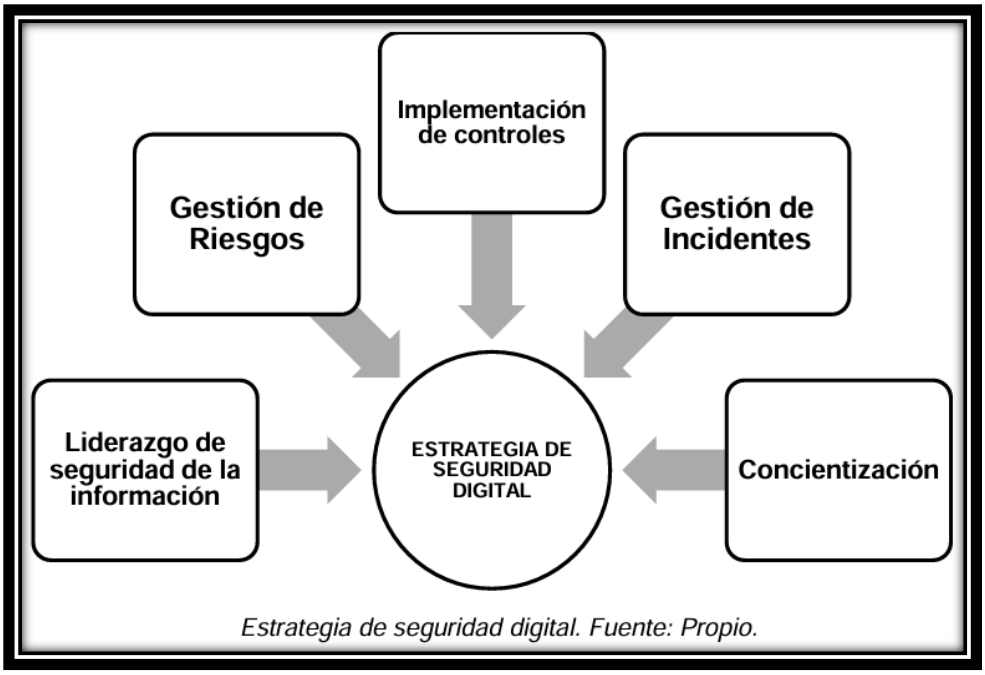
- **CONPES 3995 DE 2020**. Política nacional de confianza y seguridad digital.

- Guía para la administración del riesgo y el diseño de controles en entidades públicas V.7, 2025, publicado por el DAFP.

7. Estrategia de Seguridad Digital.

El Concejo de Coveñas establecerá una estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, teniendo como premisa que dicha estrategia gira en torno a la implementación del Modelo de Seguridad y Privacidad de la Información MSPI, así como de la guía de gestión de riesgos de seguridad de la información y del procedimiento de gestión de incidentes que debe establecerse (Ver Resolución 500 de 2021).

Por tal motivo, el Concejo de Coveñas define las siguientes cinco estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad digital:



Estrategia de seguridad digital. Fuente: Propio.

7.1.Descripción de las estrategias especificas (EJES)

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar, alineando las actividades a lo descrito dentro del MPSI y la resolución 500 de 2021:

ESTRATEGÍA / EJE	DESCRIPCIÓN/OBJETIVO
Liderazgo de seguridad de la información	Asegurar que se establezca el Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de la política general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes dependencias y/o procesos de la Corporación a través del establecimiento de los roles y responsabilidades en seguridad de la información.
Gestión de riesgos	Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados tendiendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.

Concientización	Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que se convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.
Implementación de controles	Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos del Concejo de Medellín. Se pueden subdividir en controles tecnológicos y/o administrativos.
Gestión de incidentes	Garantizar una administración de incidentes de seguridad de la información con base en un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Corporación.

7.2.Actividades.

Para cada estrategia especifica, el Concejo Municipal de Coveñas define los siguientes proyectos y productos esperados, que tienen por objetivo lograr la implementación y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI).

ESTRATEGÍA /EJE	PROYECTO	PRODUCTOS ESPERADOS
Liderazgo de seguridad de la información	Apropiar por parte del Comité Institucional de Gestión y Desempeño la implementación y desarrollo de la política de seguridad digital y de la información.	Actas de comité institucional de gestión y desempeño donde se evidencie que se abordan aspectos de desarrollo e implementación de la política de seguridad digital y de la información.
Gestión de riesgos	Gestionar los riesgos de TI aplicando la metodología adoptada en la Corporación, especialmente la de riesgos de seguridad y privacidad de la información.	Matriz de riesgos de seguridad digital. Definir planes de tratamiento de riesgos.
Concientización	Realizar jornadas de sensibilización a todo el personal.	Evidencias de las actividades desarrolladas (Registros de asistencia, convocatorias)

Implementación de controles	Gestionar la implementación de los controles identificados y asociados a los riesgos para minimizar su impacto y ocurrencia.	Evaluación de riesgos con el registro de materialización de riesgos.
Gestión de incidentes	Definir y formalizar un procedimiento de Gestión de Incidentes de seguridad de la información.	Procedimiento de gestión de incidentes de seguridad formalizado.

7.3.Cronograma de Actividades / Proyectos:

PROYECTO	2026	2027
Apropiar por parte del Comité Institucional de Gestión y Desempeño la implementación y desarrollo de la política de seguridad digital y de la información.		
Gestionar los riesgos de TI aplicando la metodología adoptada en la Corporación, especialmente la de riesgos de seguridad y privacidad de la información.		
Realizar jornadas de sensibilización a todo el personal.		
Gestionar la implementación de los controles identificados y asociados a los riesgos para minimizar su impacto y ocurrencia.		
Definir y formalizar un procedimiento de Gestión de Incidentes de seguridad de la información.		

Al finalizar cada vigencia, el Concejo de Coveñas realizará una actualización del cronograma, incorporando el estado del avance de los proyectos formulados y si en efecto se cumplieron o se plantean aplazamientos para las vigencias posteriores. Así mismo, el cronograma podrá ser modificado o ajustado de acuerdo con las necesidades o situaciones que surjan en la Corporación.

8. Responsables.

El **Concejo Municipal de Coveñas - Sucre** ha designado los siguientes responsables para garantizar la implementación, cumplimiento y mantenimiento de la Política de Seguridad y Privacidad de la Información:

- **Presidente del Concejo Municipal de Coveñas - Sucre**: Responsable de garantizar el cumplimiento de la política, velando por su correcta aplicación en la entidad.

- **Secretaría General**: Actúa como el puente entre la Mesa Directiva y la ejecución técnica. Supervisa que el personal y los contratistas cumplan con las normativas de seguridad y transparencia (Ley 1712 de 2014).

- **Profesional universitario o asesor externo como unidad de apoyo normativo del Concejo enfocado en el área de comunicaciones y tecnologías de la información TIC**: Responsable de desarrollar la implementación de la política, aplicando estrategias y acciones que permitan su adecuada ejecución en el Concejo Municipal y debe garantizar que se adopten los lineamientos y controles necesarios para su ejecución.

- **Funcionarios, contratistas y demás partes interesadas**: Tienen la responsabilidad de cumplir de manera obligatoria con la Política de Seguridad y Privacidad de la Información. En caso de incumplimiento, el Concejo Municipal se reserva el derecho de aplicar las medidas correspondientes según la normativa vigente.

- **Oficina de Control Interno (o quien haga sus veces):** Es la encargada de realizar auditorías periódicas para verificar que las medidas de seguridad se estén aplicando y que se cumplan con el marco legal (Decreto 1078 de 2015).

- **Comité Institucional de Gestión y Desempeño:** Es el órgano colegiado que revisa y aprueba los lineamientos de la Política de Seguridad Digital. En este comité se discuten los avances y fallas en la seguridad de la información.

9. Políticas de Seguridad y Privacidad de la Información.

El Concejo Municipal de Coveñas se encarga de divulgar los objetivos y alcances de la seguridad de la información dentro de la entidad, asegurando que estos sean efectivos a través de la implementación de controles de seguridad. Estos controles tienen como propósito mantener, gestionar y mitigar los riesgos conforme a lo establecido en el Plan de Tratamiento de Riesgos. De esta manera, se garantiza la continuidad de los servicios y se disminuye la probabilidad de amenazas que puedan afectar los procesos internos, contribuyendo al cumplimiento eficiente de la prestación del servicio público.

- **Identificación, clasificación y valoración de activos de información:**

Cada proceso en el Concejo Municipal de Coveñas, bajo supervisión y conforme al inventario de activos de la entidad, debe actualizarse de manera constante. Este inventario

incluirá la clasificación, valoración, ubicación y acceso de la información, así como otras características identificadas por la Alta Dirección. De este modo, se garantizará una administración eficiente de cada proceso, asegurando la disponibilidad, integridad y confidencialidad de la información en todo momento.

- **Seguridad de la información en el Talento Humano**

Todos los servidores públicos del Concejo Municipal de Coveñas, independientemente de su tipo de vinculación laboral o contractual, el área en la que desempeñen sus funciones o el nivel de actividades que realicen, deben contar con un perfil de uso de los recursos de información, que incluye tanto el hardware como el software asociado a su rol.

Para ello, es esencial contar con un directorio completo y actualizado de los perfiles creados. Además, la responsabilidad de la custodia de cualquier documento o archivo generado dentro del Concejo, que haya sido usado o producido por algún funcionario o contratista que se retire o cambie de cargo, recae en la Secretaría General o el supervisor del contrato.

Es importante señalar que el proceso de cadena de custodia de la información debe formar parte integral de los procedimientos de terminación de la relación contractual o de cambio de cargo, asegurando que los documentos e información sean debidamente gestionados durante este proceso.

- **Usuarios invitados y servicios de acceso público.**

El acceso a los recursos de información institucional por parte de usuarios no registrados deberá ser autorizado únicamente por la presidencia, y se limitará a la información institucional. Además, el servicio de internet al que puedan acceder debe estar protegido con una contraseña y contar con una restricción de acceso a sitios web no autorizados.

En caso de que los usuarios invitados no hayan completado el debido proceso de registro, no se le permitirá el acceso a cualquier otro tipo de recurso de información, aplicación o herramienta TIC.

- **Seguridad Física y del entorno**

Seguridad en los equipos:

Los servidores o equipos de cómputo que contengan información institucional deben estar ubicados en un ambiente seguro y protegido, cumpliendo, como mínimo, con los siguientes requisitos:

- Controles de acceso y seguridad física, que restrinjan el acceso no autorizado a los dispositivos y equipos.

- Sistemas eléctricos regulados, respaldados por fuentes de potencia ininterrumpida (UPS), para garantizar la continuidad operativa en caso de cortes de energía.

Toda información institucional en formato digital debe ser almacenada únicamente en los servidores y/o unidades extraíbles aprobados por la Secretaría General. Estos servidores y dispositivos deben estar adecuadamente protegidos y deben contar con mecanismos de control de acceso que aseguren que solo personas autorizadas tengan acceso a la información.

La infraestructura tecnológica debe contar con un mantenimiento y soporte adecuado para garantizar la operatividad continua tanto del hardware como del software. Es fundamental que las estaciones de trabajo sean operadas exclusivamente por los funcionarios de la Corporación edilicia, quienes deben estar capacitados sobre el contenido de esta política y las responsabilidades personales que conlleva el uso y administración de la información institucional. Esta capacitación debe incluir el conocimiento de las mejores prácticas de seguridad de la información, el manejo adecuado de los recursos tecnológicos y las consecuencias de un manejo indebido de los datos.

En cuanto al manejo de copias de seguridad, los medios de almacenamiento que alojan estas copias deben ser conservados de manera segura y protegidos contra accesos no autorizados. Las copias de seguridad deben almacenarse en lugares físicamente seguros y, preferiblemente, en entornos distintos a los de producción para evitar pérdidas catastróficas. Además, deben seguirse las políticas y estándares establecidos en cuanto a la frecuencia de las copias de seguridad, los procedimientos de restauración de datos y la auditoría periódica de los procesos relacionados.

- **Administración de las comunicaciones y operaciones**

Reporte y revisión de incidentes de seguridad:

El personal vinculado al Concejo Municipal de Coveñas tiene la responsabilidad de reportar de manera eficiente y responsable cualquier presunta violación de seguridad que detecten. Estos reportes deben ser dirigidos a la presidencia o, en casos especiales, cuando la situación lo amerite, podrán ser realizados directamente por la persona que detecte el incidente o la novedad.

Es fundamental que el procedimiento de reporte sea claro y accesible, permitiendo a los empleados y contratistas reportar incidentes de manera rápida y segura. El reporte debe

incluir detalles clave sobre el incidente, como la hora de detección, la descripción del incidente, los recursos afectados, y cualquier acción preliminar tomada.

Además, se debe diseñar, mantener y difundir las normas, procesos y guías para el reporte y revisión de incidentes de seguridad. Esto incluye la elaboración de procedimientos escritos que aseguren la correcta operación de estas actividades. Los procedimientos deben detallar los siguientes pasos:

1. **Identificación y clasificación del incidente**: Cada incidente reportado debe ser clasificado según su gravedad y tipo (e.g., acceso no autorizado, pérdida de datos, malware). Esto ayudará a priorizar la respuesta.

2. **Notificación y escalamiento**: En casos de alta gravedad, como filtraciones de datos sensibles, se debe escalar el incidente inmediatamente a las autoridades pertinentes y tomar acciones inmediatas para mitigar el daño.

3. **Investigación y análisis**: El equipo responsable debe investigar la causa del incidente, analizando los registros, el comportamiento del sistema y los recursos afectados, para determinar el alcance y la naturaleza del problema.

4. **Remediación**: Una vez identificada la causa, se deben implementar acciones correctivas para resolver el problema, como la eliminación de malware, el fortalecimiento de las medidas de seguridad o la restauración de sistemas a partir de copias de seguridad.

5. **Seguimiento y reporte**: Después de la resolución, se debe hacer un seguimiento para verificar que el incidente no se repita y se deben elaborar informes detallados sobre el incidente, las acciones tomadas y las lecciones aprendidas.

6. **Revisión de políticas y medidas preventivas**: Como medida a largo plazo, se debe revisar y, si es necesario, ajustar las políticas de seguridad para prevenir futuros incidentes similares, así como mejorar la capacitación del personal en aspectos clave de seguridad.

Este proceso debe llevarse a cabo sin afectar el desarrollo normal de la prestación del servicio y asegurando la confiabilidad de la información en todo momento, manteniendo la continuidad operativa y el cumplimiento de las normativas vigentes.

- **Protección contra software malicioso y hacking**

Es fundamental proteger todos los sistemas de información mediante un enfoque integral que incluya controles humanos, físicos, técnicos y administrativos para evitar daños. Para

ello, se elaborará y mantendrá un conjunto de políticas, normas, estándares y procedimientos que garanticen la mitigación de riesgos asociados a amenazas de software malicioso y técnicas de hacking que puedan comprometer la prestación del servicio.

Como medida de control básico, todas las estaciones de trabajo del Concejo Municipal deben estar protegidas con software antivirus que cuente con capacidad de actualización automática para asegurar que las firmas de virus estén siempre al día y que los sistemas estén protegidos frente a las amenazas emergentes. Además, el software antivirus debe incluir funcionalidades de detección en tiempo real para identificar y bloquear cualquier actividad sospechosa de forma inmediata.

Se debe implementar una política de actualización de software que asegure que todos los sistemas operativos, aplicaciones y herramientas de seguridad sean actualizados de forma periódica. Las actualizaciones de seguridad deben ser aplicadas de manera automática, siempre que sea posible, para garantizar que se aborden vulnerabilidades conocidas de manera oportuna. Asimismo, se deberán llevar a cabo pruebas de compatibilidad para evitar que las actualizaciones afecten el funcionamiento normal de los sistemas y servicios.

Para garantizar la efectividad de estas medidas, se implementará un sistema de monitoreo continuo que permita evaluar la actividad de los sistemas y detectar cualquier anomalía o vulnerabilidad en tiempo real. Este monitoreo incluirá la revisión periódica de los registros de eventos de seguridad y pruebas de penetración para asegurar que los sistemas se mantengan protegidos contra nuevas amenazas. Además, se deben realizar auditorías regulares para evaluar el cumplimiento de las políticas de seguridad y detectar posibles áreas de mejora.

Es esencial que todos los funcionarios del Concejo Municipal estén capacitados en seguridad informática. Se implementará un programa de formación continua sobre las mejores prácticas en ciberseguridad, incluyendo temas como el manejo seguro de contraseñas, el reconocimiento de phishing y otras amenazas, y el uso adecuado de herramientas de protección. Además, los funcionarios de TI deberán recibir formación especializada para mantenerse al día con las últimas tendencias en amenazas y tecnologías de protección.

- **Copias de Seguridad**

Toda información contenida en el inventario de activos de información o que sea relevante para un proceso debe estar respaldada mediante copias de seguridad. Estas copias deben tomarse siguiendo los procedimientos documentados y validados por el Sistema de Gestión Pública - MIPG.

El procedimiento de respaldo debe incluir actividades relacionadas con el almacenamiento, administración y custodia de las copias de seguridad, asegurando que estas se guarden en lugares seguros y que se lleve un control adecuado de los registros. Dentro de este procedimiento, se debe establecer la realización de auditorías aleatorias para garantizar el correcto funcionamiento de los procesos de copia de seguridad y asegurar que se mantengan alineados con los estándares establecidos.

Las auditorías de las copias de seguridad deben llevarse a cabo de manera periódica y no programada, con el objetivo de asegurar que se esté cumpliendo con los protocolos establecidos. Estas auditorías deben evaluar la integridad de los datos, verificar que las copias sean exactas y completas, y comprobar que los medios de almacenamiento estén funcionando correctamente.

Además, debe existir un procedimiento documentado que verifique la correcta restauración de los datos, lo que permitirá probar la efectividad de las copias de seguridad y garantizar que la información pueda ser recuperada en caso de un incidente.

Las auditorías también deben incluir pruebas de recuperación de datos en un entorno controlado para asegurar que no haya fallos durante el proceso de restauración.

Es importante tener en cuenta que la responsabilidad de crear copias de seguridad de archivos utilizados, custodiados o producidos por usuarios individuales recae exclusivamente en cada uno de los usuarios. Los usuarios deben ser conscientes de su responsabilidad en asegurar la actualización continua de las copias de seguridad de la información que manejan.

Los dueños de los activos de la información deben verificar regularmente la validez y accesibilidad de las copias de seguridad y asegurarse de que están almacenadas de acuerdo con los procedimientos establecidos. En caso de que los usuarios encuentren dificultades en la actualización o almacenamiento de sus copias, deberán informar inmediatamente a los responsables de la gestión de TI para que se tomen las acciones correctivas necesarias.

En cuanto al intercambio de información con entidades externas, cualquier petición o solicitud de información por parte de entes externos debe ser aprobada por la Alta Dirección. La Alta Dirección debe revisar cuidadosamente la solicitud para asegurarse de que la información solicitada sea relevante, esté completa y sea accesible conforme a las normas de confidencialidad y seguridad establecidas. Una vez aprobada la solicitud, la Alta Dirección designará a los responsables del manejo de esa información, quienes se encargarán de procesarla de acuerdo con los procedimientos internos y entregarla a la entidad solicitante.

El proceso de aprobación debe ser documentado y el registro de la solicitud debe ser almacenado de manera segura para garantizar la trazabilidad de la solicitud, permitiendo un seguimiento adecuado del uso y destino de la información institucional.

La solicitud deberá incluir detalles como el remitente, el asunto, la fecha y la naturaleza de la información solicitada, de forma que se pueda identificar claramente su origen y garantizar que no se viole ninguna normatividad vigente.

Además, toda información institucional debe ser manejada de acuerdo con la normatividad legal vigente, asegurando el cumplimiento de leyes como la protección de datos personales, la transparencia y el acceso a la información pública. Las solicitudes de entidades externas también deben cumplir con los protocolos de seguridad establecidos, asegurando que la información no se comparta con personas no autorizadas y que se mantenga la integridad y confidencialidad de los datos.

- **Instalación de Software**

Las instalaciones de software que se realicen sobre los sistemas operativos previamente instalados en el Concejo Municipal de Coveñas, deben contar con la aprobación expresa de la Alta Dirección. Esta aprobación debe basarse en una evaluación exhaustiva del software, que no solo contemple la compatibilidad con los sistemas existentes, sino también una revisión detallada de los aspectos de seguridad, eficiencia, y su adecuación al marco normativo de tecnologías de la información aplicable. Para ello, se deben seguir los procedimientos establecidos para la instalación de software, que incluyen la verificación de su origen legítimo, licencia válida, funcionalidad y que no represente ninguna amenaza a la seguridad de la información.

Los procedimientos de instalación deben también incluir una evaluación de riesgos que considere los impactos potenciales del software en los procesos internos, en la protección de datos personales y en la integridad de la infraestructura tecnológica. El procedimiento también debe establecer que el software solo puede ser instalado por personal capacitado en el área de gestión de TIC, siguiendo un protocolo que permita verificar la compatibilidad técnica con las aplicaciones existentes y asegurando que la instalación no afecte el rendimiento de los sistemas operativos ni de las estaciones de trabajo.

Es imperativo que la Alta Dirección asegure que el software instalado sea de fuentes confiables y aprobadas, evitando así la instalación de aplicaciones que puedan comprometer la seguridad, tales como software pirata o aplicaciones no verificadas. Esta política no solo asegura la legalidad del software, sino que también minimiza el riesgo de vulnerabilidades que puedan ser aprovechadas por ciberataques o malware.

El funcionario encargado de la gestión de las Tecnologías de la Información (TIC) en el Concejo Municipal tiene la responsabilidad inmediata de desinstalar cualquier software ilegal o no autorizado que sea detectado. La detección de software no autorizado debe ser considerada un incidente de seguridad, y debe ser registrada y gestionada a través de un sistema de gestión de incidentes. Este sistema debe estar diseñado para clasificar, priorizar y hacer un seguimiento de los incidentes, lo que permitirá una respuesta rápida y eficaz.

El proceso de investigación de incidentes debe incluir varias etapas. Primero, se debe llevar a cabo un análisis forense para determinar el origen y el alcance de la instalación del software no autorizado, lo que permitirá identificar cómo y cuándo fue instalado y por quién. Se debe analizar si este software ha causado algún daño o afectación a los sistemas, si ha generado brechas en la seguridad de la información o si ha comprometido la confidencialidad de los datos institucionales.

El resultado de la investigación debe ser documentado detalladamente, y deben tomarse las acciones correctivas necesarias. Estas acciones pueden incluir la eliminación del software, la actualización de las medidas de seguridad, y, si fuera necesario, la capacitación adicional del personal para evitar que se repita la instalación de software no autorizado.

Adicionalmente, el funcionario encargado de las TIC debe mantener un inventario detallado y actualizado del software autorizado para su uso institucional. Este inventario debe ser revisado de manera periódica para garantizar que todos los programas que se están utilizando son legítimos y han sido debidamente aprobados por la Alta Dirección.

El inventario debe incluir detalles como el nombre del software, la versión, el tipo de licencia, los responsables de su instalación y uso, y cualquier otra información relevante que permita hacer un seguimiento adecuado del software autorizado. Además, el inventario debe estar disponible para auditorías internas y debe ser utilizado para realizar verificaciones periódicas de la legalidad del software instalado en los sistemas del Concejo Municipal.

- **Control de Claves y Nombres de Usuario**

Las claves de administrador de los diferentes sistemas deben ser conservadas por la Secretaría General y el funcionario encargado de la Gestión de las TIC. Estas claves deberán cambiarse en intervalos regulares y, de manera obligatoria, cada vez que se presente un cambio en el personal adscrito al cargo.

Adicionalmente, se debe elaborar, mantener y actualizar un procedimiento que defina claramente el uso, la complejidad y las buenas prácticas para la gestión segura de las claves de usuario.

- **Suspensión y Cancelación de Cuentas**

Al finalizar la relación contractual o laboral de un funcionario con el Concejo Municipal de Coveñas, se deberá expedir un certificado de suspensión y/o cancelación de las cuentas asociadas al usuario en todos los sistemas de información donde estuviera activo, incluyendo correo electrónico y sistemas automatizados.

Se establecerá un tiempo prudencial para la posible renovación de la relación laboral. Si dicha renovación no se materializa al término de ese período, se procederá con la baja definitiva de las cuentas correspondientes.

- **Uso Adecuado de Internet**

Política de Gestión del Servicio de Internet

El Concejo Municipal de Coveñas reconoce la importancia del servicio de Internet como una herramienta esencial para el desarrollo eficiente y seguro de las actividades institucionales. El acceso a este recurso permite optimizar procesos, facilitar la comunicación y garantizar la prestación efectiva de los servicios públicos. Por tal razón, la entidad se compromete a proporcionar los recursos necesarios para su disponibilidad, asegurando el acceso a los servidores públicos y a otras partes interesadas que lo requieran para el desempeño de sus funciones.

Para el cumplimiento de este objetivo, el proceso de Tecnologías de la Información y las Comunicaciones (TIC) deberá implementar las siguientes acciones:

1. **Asignación de recursos:**

El proceso de TIC será responsable de gestionar, proveer y distribuir los recursos necesarios para la correcta implementación, administración y mantenimiento del servicio de Internet. Esta gestión se realizará garantizando su disponibilidad, estabilidad y seguridad, bajo las restricciones definidas según los perfiles de acceso establecidos. Se procurará la adquisición de tecnologías actualizadas que optimicen el rendimiento y la seguridad de la conexión.

2. **Continuidad del servicio:**

Se deberá diseñar, documentar e implementar mecanismos que permitan garantizar la continuidad o el restablecimiento oportuno del servicio de Internet en caso de presentarse una contingencia interna. Para tal fin, se realizarán análisis de riesgos periódicos y se desarrollarán planes de contingencia que incluyan la definición de procedimientos de respuesta ante fallos y el establecimiento de mecanismos alternativos de conectividad.

3. **Monitoreo constante:**

Se establecerá un monitoreo continuo de los canales de acceso a Internet con el objetivo de detectar, analizar y corregir de manera oportuna cualquier anormalidad que pueda afectar el funcionamiento del servicio. Este monitoreo incluirá la medición de indicadores clave de desempeño, como la velocidad de conexión, la disponibilidad del servicio y el consumo de ancho de banda, permitiendo así una gestión proactiva.

4. **Registro y control de accesos:**

El proceso de TIC deberá generar, almacenar y custodiar registros detallados sobre la navegación y los accesos realizados por los usuarios a través del servicio de Internet. Estos registros serán gestionados conforme a las disposiciones legales vigentes en materia de protección de datos y privacidad, y se utilizarán para identificar posibles usos indebidos, garantizar el cumplimiento de las políticas internas y contribuir a la mejora continua del servicio.

5. **Sensibilización y formación:**

Se desarrollarán programas de sensibilización y capacitación dirigidos a los servidores públicos y demás usuarios autorizados, con el fin de promover el uso responsable, eficiente y seguro del servicio de Internet. Estas actividades incluirán lineamientos sobre el manejo adecuado de la información, la gestión segura de las credenciales de acceso y las buenas prácticas en el entorno digital.

- **Cumplimiento y Mejora Continua:**

El Concejo Municipal de Coveñas, a través del proceso de TIC, establecerá mecanismos de auditoría y revisión periódica para evaluar el cumplimiento de esta política y realizar los ajustes necesarios que permitan su mejora continua. Asimismo, se mantendrá una actualización constante en las tecnologías y procedimientos utilizados, garantizando la eficiencia y seguridad del servicio en el marco de las necesidades institucionales y las disposiciones legales aplicables.

10. Desarrollo del Plan.

10.1. Metodología de Implementación del Plan de Seguridad y Privacidad.

La metodología de implementación del Plan de Seguridad y Privacidad del Concejo Municipal de Coveñas se fundamenta en el ciclo PHVA (Planificar-Hacer-Verificar-Actuar) y en las directrices establecidas en el Modelo de Seguridad y Privacidad del

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), según lo dispuesto en la **Resolución 00500 del 21 de marzo de 2021**. Esta metodología permite una gestión sistemática y continua de los riesgos asociados a la información, garantizando su confidencialidad, integridad, disponibilidad y privacidad.

1. **Fase de Planificación (Planificar):**

En esta fase se realiza un análisis exhaustivo del estado actual de la seguridad de la información, identificando activos críticos, posibles vulnerabilidades y amenazas potenciales. Se definen los objetivos, las estrategias y las acciones necesarias para mitigar riesgos, alineándolos con las necesidades institucionales y el marco normativo vigente. Adicionalmente, se elaboran políticas, procedimientos y planes de acción que orienten el proceso de implementación de las medidas de seguridad y privacidad.

2. **Fase de Implementación (Hacer):**

Durante esta etapa se ejecutan las acciones planificadas, aplicando las medidas técnicas, administrativas y operativas necesarias para proteger la información institucional. Esto incluye la configuración de mecanismos de control de acceso, la instalación de herramientas de seguridad, la capacitación del personal en buenas prácticas de gestión de la información y la implementación de procesos para la gestión segura de datos. Asimismo, se documentan las acciones realizadas para facilitar su seguimiento y evaluación posterior.

3. **Fase de Verificación (Verificar):**

En esta fase se evalúa la eficacia de las medidas implementadas a través de auditorías, revisiones y análisis de incidentes. Se miden los resultados obtenidos en comparación con los objetivos definidos y se identifican posibles desviaciones o fallas. Este proceso permite comprender el impacto de las acciones realizadas y determinar las mejoras necesarias para fortalecer el sistema de seguridad y privacidad de la información.

4. **Fase de Mejora Continua (Actuar):**

Finalmente, se toman las decisiones necesarias para corregir las deficiencias detectadas y optimizar los procesos de gestión de la seguridad y privacidad. Se ajustan las políticas, procedimientos y controles establecidos, incorporando lecciones aprendidas y mejores prácticas identificadas durante la fase de verificación. La mejora continua garantiza la adaptabilidad y resiliencia del sistema frente a nuevos riesgos y exigencias tecnológicas.

Compromiso Institucional: El Concejo Municipal de Coveñas, reafirma su compromiso con la protección de la información institucional, adoptando las mejores prácticas en

materia de seguridad y privacidad, conforme a la normativa aplicable y las recomendaciones de MinTIC. La aplicación rigurosa del ciclo PHVA permite una gestión efectiva de los riesgos, contribuyendo a la confianza de los ciudadanos y al fortalecimiento de la transparencia y eficiencia institucional.

Hasta la fecha, se han realizado las actividades de planificación, las cuales abarcan el análisis del contexto institucional, la definición de objetivos, la planeación estratégica, el soporte requerido y la evaluación del estado actual de la información.

En el marco de la implementación, se ha trabajado en la elaboración de procedimientos, guías y manuales, así como en el establecimiento de controles y la planificación operacional. Adicionalmente, se diseñó un plan de sensibilización para promover la cultura de seguridad de la información dentro de la entidad.

11. CUMPLIMIENTO DE LA IMPLEMENTACIÓN

El Concejo Municipal de Coveñas en su modelo de seguridad y privacidad de la información se encuentra en la fase de implementación de acuerdo con el diagnóstico realizado en MIPG en vigencias anteriores.

12. NIVEL DE MADUREZ

El modelo de seguridad y privacidad de la información, establecido por el Ministerio de Tecnologías de la Información, ofrece una guía para garantizar que las entidades públicas gestionen adecuadamente la información que poseen, protegiendo tanto la privacidad de los ciudadanos como la seguridad de los datos. En este contexto, el Concejo Municipal de Coveñas, se encuentra en la fase inicial, es decir, en el nivel incipiente de implementación de este modelo.

El nivel incipiente se refiere a la etapa temprana en la que las acciones definidas en la fase de planeación aún no se han puesto en práctica de manera efectiva, pero se cuenta con una visión clara de las medidas que deben implementarse. Por lo tanto, el Concejo debe centrarse en ejecutar las acciones ya delineadas en esa etapa previa, lo que implica diseñar un modelo de privacidad acorde con los requisitos establecidos, asegurando que cumpla con las normativas legales mínimas, como la Ley Estatutaria de Protección de Datos Personales (Ley 1581 de 2012) y las disposiciones relacionadas con el manejo de información pública.

El proceso requiere que el Concejo también desarrolle y ponga en marcha una política de privacidad específica. Esta política será fundamental para la correcta gestión de la información, ya que establecerá procedimientos y protocolos claros sobre cómo se recoge,

almacena, protege, utiliza y comparte la información dentro de la entidad. Adicionalmente, esta política debe contemplar la formación y sensibilización del personal encargado de la gestión de datos, asegurando que se actúe con la debida diligencia en el manejo de la información.

Implementar un modelo de privacidad robusto y cumplir con las regulaciones en vigor permitirá al Concejo no solo proteger los datos personales y confidenciales, sino también fortalecer la confianza de la ciudadanía en la administración pública, garantizando que se cumpla con los estándares más altos de seguridad y privacidad en la gestión de la información.

MAPA DE RUTA VIGENCIA 2026

EJE/ ÁREA	DESCRIPCIÓN	ENTREGABLE	VIGENCIA 2026											
			E	F	M	A	M	J	J	A	S	O	N	D
Modelo de Seguridad y privacidad de la información	Actualización del instrumento de identificación de la línea base de seguridad	Instrumento diligenciado y plan de acción.							X					
Transformación Digital	Actualizar los riesgos de seguridad digital y los controles de seguridad necesarios para garantizar la seguridad digital y la protección de los datos personales en el marco de la normatividad aplicable.	Matriz de Riesgos de Seguridad.		X										
Riesgos	Acompañar los procesos institucionales en la identificación, valoración, evaluación y formulación de planes de tratamiento de riesgo de seguridad digital. Así como,	Plan de Tratamiento de riesgos de seguridad Digital. Y seguimiento a			X									

	hacer seguimiento a la implementación de los planes de tratamiento de riesgos de seguridad digital que adopten los procesos.	la implementación del Plan por parte del CIGD.												
Sensibilización	Revisar los contenidos de sensibilización y divulgación de los componentes de la seguridad de la información institucional y apoyar su publicación en la página institucional para su correcto reporte.	Instrumentos de gestión de la información pública (Registro de activos de información, Registro de publicaciones, Índice de información clasificada y reservada, Esquema de publicación de información).			X						X			
Sistema de Gestión Integrado de Calidad y Ambiental.	Diseñar estrategias que permitan la implementación de las políticas de seguridad de la información en los procesos institucionales. Realizar la actualización del documento de contexto de seguridad de la información institucional. Medición del Desempeño. *Lo anterior bajo el cumplimiento de los parámetros	Adopción del Plan de Seguridad y Privacidad de la información. Actualización del documento conforme a la planeación estratégica institucional de mediano plazo, articulada con el Plan de Acción de la vigencia. Medición de desempeño a través del FURAG y/o Autodiagnóstico.			X	X		X						

	establecidos por las normas de calidad adoptadas en la entidad.													
Seguridad Operativa.	Acompañar al área de las Tecnologías de información y las comunicaciones en la gestión, evaluación e implementación de acciones de respuesta frente a eventos e incidentes de seguridad de la información.	A través del Comité institucional de Gestión y Desempeño. Actas de reuniones.	X			X			X			X		

13. Evaluación y Seguimiento.

El Plan de Seguridad y Privacidad de la información, estará en cabeza de la Mesa Directiva de la Corporación, con el apoyo del profesional especializado del área de gestión tecnológica (Tic) y comunicaciones. El seguimiento y la evaluación de riesgos y manejo de las situaciones que comprometan posibles prácticas corruptas, estará a cargo del Comité Institucional de Gestión y Desempeño, con el acompañamiento de los líderes de proceso.

Se tendrá como herramienta de medición, la matriz de autodiagnóstico MIPG, a través de la herramienta dispuesta en el sitio web del Modelo Integrado de Planeación y Gestión del Departamento Administrativo de Función Pública.

Se realizará el reporte oficial a la implementación del Plan de Seguridad y Privacidad de la información a través del FURAG II (Formulario Único Reporte de Avances de la Gestión)

DARWIN CHICA TIRADO
Presidente

MARÍA P. MENDOZA VEGA
Primer vicepresidente

MARTA RIOS REVUELTA
Segunda vicepresidenta

KELLY J. MENA OROZCO
secretaria