Concejo Municipal
de Coveñas

PLAN DE TRATAMIENTO DE RIESGO 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 TRATAMIENTO DE RIESGO 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

1. Introducción

El Concejo Municipal de Coveñas - Sucre, en su compromiso con la transparencia, la protección de la información y la mejora continua de sus procesos, presenta el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2026. Este documento constituye una herramienta fundamental para la identificación, análisis y mitigación de los riesgos asociados al manejo de la información, asegurando la confidencialidad, integridad y disponibilidad de los datos que gestiona la entidad.

En un contexto donde la transformación digital y la gestión eficiente de la información son pilares fundamentales para el buen funcionamiento de las instituciones públicas, resulta indispensable contar con estrategias claras que garanticen un entorno seguro tanto en el ámbito digital como en el físico. El presente plan está alineado con las normativas nacionales e internacionales vigentes en materia de seguridad de la información, así como con las políticas internas del Concejo Municipal.

El plan se fundamenta en el ciclo PHVA (Planear-Hacer-Verificar-Actuar), un enfoque que permite no solo la implementación de medidas preventivas y correctivas, sino también la evaluación constante de su efectividad y la adaptación a nuevos desafíos y amenazas. A través de este ciclo, se promueve la mejora continua en la gestión de la seguridad y privacidad de la información.

Este documento está dirigido a todos los grupos de interés, incluyendo servidores públicos, contratistas, proveedores y ciudadanía en general, quienes desempeñan un papel crucial en la protección de la información. La participación activa y la adopción de buenas prácticas en el manejo de los datos contribuirán al fortalecimiento de una cultura organizacional orientada a la seguridad y la confianza.

Con la implementación de este plan, el Concejo Municipal de Coveñas reafirma su compromiso con la protección de la información pública, el cumplimiento de la normativa vigente y la generación de un entorno confiable que respalde la gestión administrativa y la toma de decisiones en beneficio de la comunidad.

Este plan se alinea con la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, la cual proporciona un marco metodológico para identificar, evaluar y mitigar los riesgos que puedan afectar la gestión de la información en el sector público. Asimismo, se ajusta a lo establecido en el Decreto 1008 del 14 de junio de 2018, que regula la Política de Gobierno Digital en Colombia, promoviendo la adopción de tecnologías que fortalezcan la eficiencia, transparencia y seguridad en la gestión pública.

De acuerdo con este decreto, se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, conocido como el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. Esta normativa establece los lineamientos generales para el uso adecuado de las tecnologías en las entidades del Estado, fomentando la innovación, la protección de la información y la prestación de servicios digitales eficientes.

En este contexto, se resaltan los Habilitadores Transversales definidos para las entidades públicas, que son pilares fundamentales para la implementación de la política de Gobierno Digital:

a) Seguridad de la Información: Garantiza la protección de los datos y activos digitales de la entidad frente a amenazas internas y externas, asegurando la confidencialidad, integridad y disponibilidad de la información.

b) Arquitectura de Tecnologías de la Información (TI): Establece un marco estructurado para la integración y gestión eficiente de los sistemas tecnológicos, facilitando la interoperabilidad, la optimización de recursos y la adopción de soluciones innovadoras.

c) Servicios Ciudadanos Digitales: Promueve la digitalización de los servicios públicos, facilitando el acceso de la ciudadanía a trámites y servicios en línea, fortaleciendo la transparencia y mejorando la interacción entre el Estado y los ciudadanos.

La incorporación de estos habilitadores en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Concejo Municipal de Coveñas - Sucre, garantiza una gestión integral y coherente con las políticas nacionales, contribuyendo a un entorno digital más seguro, eficiente y orientado al servicio de la comunidad.

2. Elementos Estratégicos Corporativos

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.

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. Objetivo Estratégico

Fortalecer la capacidad y efectividad administrativa y la innovación organizacional, para la modernización del Concejo Municipal de Coveñas y el incremento de la confianza ciudadana en la Entidad.

4. Objetivos del Plan de Tratamiento de Riesgo de Seguridad y Privacidad de la Información

a. Objetivos Generales

- Fortalecer la seguridad y privacidad de la información en todos los procesos administrativos y operativos del Concejo Municipal de Coveñas - Sucre, garantizando la protección de los datos frente a amenazas internas y externas.
- Determinar las acciones de tratamiento de riesgos de seguridad y privacidad de la información, mediante la identificación, análisis, valoración y tratamiento de los riesgos de pérdida de confidencialidad, disponibilidad e integridad de la información; con la finalidad de prevenir su materialización y/o reducir los impactos negativos en la gestión del Concejo Municipal de Coveñas.

b. Objetivos Específicos

- Identificar, evaluar y mitigar los riesgos asociados al manejo de la información, mediante la implementación de controles adecuados que aseguren la confidencialidad, integridad y disponibilidad de los datos.

- Alinear la gestión de la seguridad de la información con las normativas vigentes, incluyendo el *Decreto 1008 de 2018*, la *Política de Gobierno Digital*, y la *Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas*, asegurando el cumplimiento de los estándares nacionales e internacionales.

- Promover una cultura organizacional de seguridad de la información, a través de la capacitación continua del personal, la sensibilización sobre buenas prácticas y la adopción de políticas claras para el manejo adecuado de la información.

- Planificar la evaluación y hacer seguimiento de la gestión de los riesgos de seguridad de la información, con el fin de asegurar la disponibilidad de los servicios críticos de TIC y mitigar las interrupciones, que aportan a la eficiencia operativa del Concejo Municipal de Coveñas - Sucre.

- Optimizar la infraestructura tecnológica y los procesos digitales del Concejo, garantizando la implementación de herramientas y tecnologías seguras que faciliten la interoperabilidad y la eficiencia en la gestión de la información.

- Establecer mecanismos de monitoreo, control y mejora continua mediante la aplicación del ciclo PHVA (Planear-Hacer-Verificar-Actuar), que permitan evaluar la efectividad de las medidas implementadas y realizar ajustes oportunos frente a nuevos riesgos o cambios en el entorno tecnológico.

- Fomentar la transparencia y la confianza ciudadana mediante la protección adecuada de la información pública y la garantía de acceso seguro y confiable a los servicios digitales ofrecidos por el Concejo Municipal.

5. Alcance del Plan de Tratamiento de Riesgo.

El alcance del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Concejo Municipal de Coveñas – Sucre para la vigencia 2026 aplica para todos los procesos identificados en el modelo de operación institucional, a todos sus funcionarios, contratistas, proveedores y aquellas personas o terceros que para el cumplimiento de sus funciones y las de la entidad, compartan, utilicen, recolecten, procesen, intercambien o consulten cualquier activo de información de su propiedad. Su objetivo es identificar, evaluar y mitigar los riesgos que puedan comprometer la confidencialidad, integridad y disponibilidad de la información, asegurando el cumplimiento de las normativas vigentes y la protección de los datos manejados.

6. Alcance Específico.

- **Procesos y Procedimientos**: Incluye la revisión y mejora de todos los procesos administrativos y operativos que involucren el manejo de información, garantizando que se realicen bajo estándares de seguridad y privacidad adecuados.

- **Sistemas de Información**: Comprende la evaluación y fortalecimiento de las plataformas tecnológicas utilizadas para la gestión de datos, asegurando su resiliencia frente a posibles amenazas cibernéticas.

- **Infraestructura Tecnológica**: Abarca la infraestructura de TI, incluyendo hardware, software y redes de comunicación, asegurando su protección y correcto funcionamiento.

- **Personal**: Involucra a todos los funcionarios y colaboradores del Concejo Municipal, promoviendo una cultura de seguridad de la información a través de capacitaciones y sensibilizaciones continuas.

- **Proveedores y Terceros**: Extiende las políticas de seguridad y privacidad a los proveedores y terceros que tengan acceso o manejen información del Concejo, asegurando que cumplan con los estándares establecidos.

- **Cumplimiento Normativo**: Garantiza la alineación con las leyes y regulaciones aplicables en materia de seguridad y privacidad de la información, incluyendo el Decreto 1008 de 2018 y el Decreto 1078 de 2015.

- **Gestión de Incidentes**: Establece procedimientos para la identificación, reporte y manejo de incidentes de seguridad de la información, minimizando su impacto y previniendo futuras ocurrencias.

Este plan se aplicará de manera transversal en toda la organización, asegurando que cada área y proceso esté alineado con los objetivos de seguridad y privacidad establecidos, y promoviendo una cultura organizacional comprometida con la protección de la información.

7. Lineamientos conceptuales

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

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceso a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000).

Activos de Información y recursos: se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 de 20116).

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o Entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo. (ISO/IEC 27000).

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

Ciberseguridad: Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las Entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

Datos Personales Mixtos: Para efectos de este documento es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos Personales Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información–SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC27000).

Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

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

Encargado del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3).

Evaluación de Desempeño: Seguimiento a los resultados, de manera que se pueda verificar la efectividad, la eficiencia y la eficacia de las acciones que se implementaron.

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Impacto: Las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

Ley de Habeas Data: Se refiere a la Ley Estatutaria 1266 de 2008.

Ley de Transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria 1712 de 2014.

Mecanismos de protección de datos personales: Lo constituyen las distintas alternativas con que cuentan las Entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

Partes interesadas (Stakeholder): Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Probabilidad: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.

Registro Nacional de Bases de Datos: Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25).

Responsabilidad Demostrada: Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

Responsable del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art. 3).

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Riesgo Inherente: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.

Riesgo Residual: El resultado de aplicar la efectividad de los controles al riesgo inherente.

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).

Seguridad digital: Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.

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, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Titulares de la información: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).

Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

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. (ISO/IEC 27000).

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

8. Marco Normativo

8.1.Del Orden Constitucional

- **Constitución Política de 1991.**

- *Artículo 15:* Derecho a la intimidad personal y familiar, y protección de datos.
- *Artículo 74:* Derecho de acceso a documentos públicos, salvo excepciones legales.

8.2.Del Orden Legal.

- **Ley 527 de 1999**. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

- **Ley 1266 de 2008**. Por la cual se dictan las disposiciones generales del Habeas 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 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 del Espectro y se dictan otras disposiciones.

- **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 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 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.

8.3.Decretos Nacionales.

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

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

- **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. 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 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.

8.4.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.

8.5.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"

8.6.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.

- **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.

- **Plan Estratégico** del Concejo Municipal de Coveñas para el periodo 2024 -2027.

9. Modelo de Operación por Procesos

En el Concejo Municipal de Coveñas se trabaja mediante la Gestión por procesos, teniendo en cuenta el Modelo Estándar de Control Interno (MECI 1000: 2014). El Sistema de Gestión Corporativo se compone de ocho procesos:

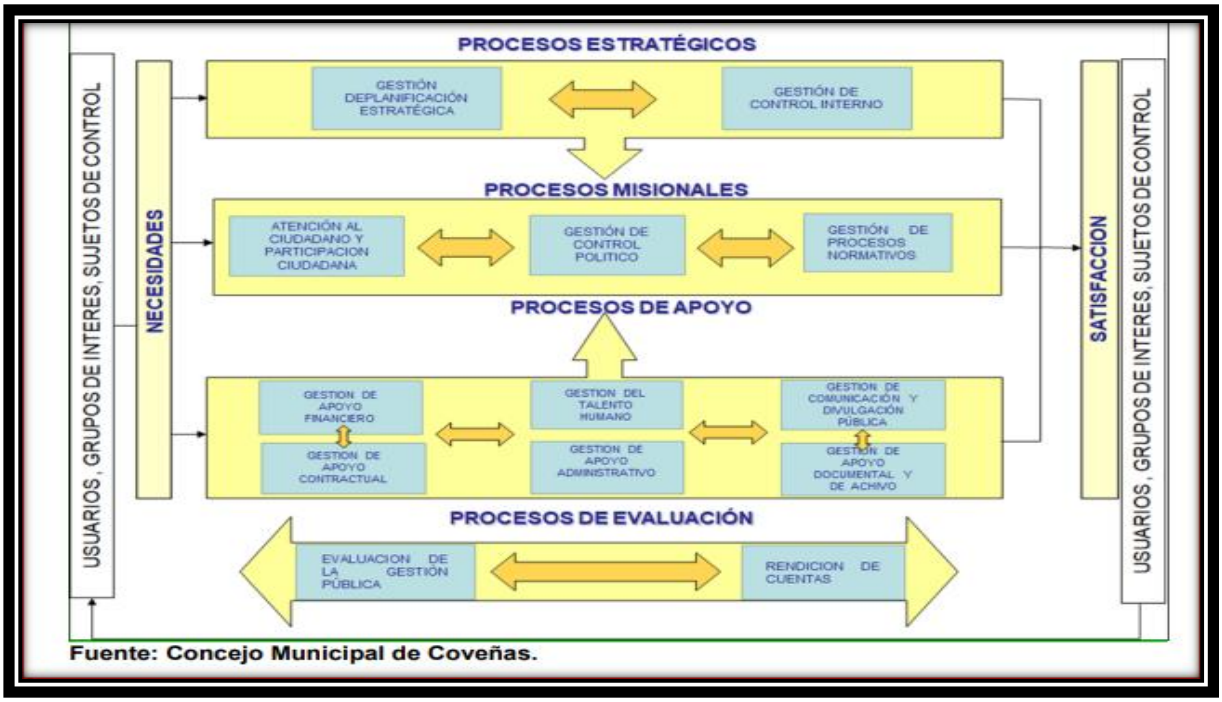
- **Un proceso misional**, Debate Temático Público, que se desarrolla mediante tres líneas estratégicas: control político, participación ciudadana y proyectos de acuerdo.

- **Dos procesos estratégicos**, Gestión Estratégica y Planeación y Comunicaciones y Relaciones Corporativos.

- **Tres procesos de apoyo**; Gestión de la Información, Gestión de Bienes y Servicios y Gestión del Talento Humano.

- **Dos procesos de evaluación**, Evaluación Independiente y Mejora Continua

9.1. Mapa de Procesos



Fuente: Manual de Procesos y Procedimientos. -Concejo Municipal de Coveñas.

9.2.Descripción de los Procesos.

9.2.1. Procesos estratégicos.

ID	Nombre	Objetivo
001	Gestión estratégica y planeación	Garantizar la generación de valor público en la Corporación mediante la orientación e implementación de políticas y estrategias institucionales y la gestión eficiente de los recursos, en el marco del Sistema de Gestión Corporativo (SGC).
002	Comunicaciones y relaciones corporativas	Desarrollar estrategias y acciones comunicacionales y de relaciones interinstitucionales que faciliten el cumplimiento de los objetivos corporativos y el posicionamiento de la imagen institucional, ante los grupos de valor y de interés, conforme a los lineamientos de la comunicación pública.

9.2.2. Procesos misionales.

ID	Nombre	Objetivo
001	Debate Temático Público	Estudiar y aprobar propuestas para el desarrollo del Municipio, realizando control político a las decisiones y actuaciones de la Administración Central y Descentralizada; promoviendo y facilitando la participación de la comunidad en los asuntos del Municipio.

9.2.3. Procesos de apoyo.

ID	Nombre	Objetivo
001	Gestión del talento humano	Fortalecer las competencias del talento humano mediante el desarrollo de estrategias, planes, y programas, con el fin de mejorar el desempeño laboral, contribuyendo al logro de los objetivos corporativos y promoviendo en el empleado la apropiación de valores y principios para generar valor público.
002	Gestión de bienes y servicios	Gestionar y disponer de los recursos logísticos relacionados con los bienes y servicios requeridos para los procesos de la corporación.
003	Gestión de la información	Liderar la gestión de la información para maximizar el valor y los beneficios derivados de su uso, contribuyendo a la gestión del conocimiento organizacional y la preservación de la memoria histórica.

9.2.4. Procesos de evaluación y control.

ID	Nombre	Objetivo
001	Evaluación independiente	Contribuir a la mejora y eficacia del Sistema de Gestión Corporativo mediante la evaluación del Control Interno, a través de metodologías y procedimientos previamente establecidos, en el marco de la normatividad legal aplicable.

002	Mejora continua	Asegurar la conveniencia, adecuación y eficacia del Sistema de Gestión Corporativo, mediante el diseño e implementación de metodologías para el seguimiento, la medición, la evaluación, el análisis y la mejora continua de los procesos.

10. Gestión de Riesgos

10.1. Importancia de la gestión de riesgos.

En el ámbito empresarial se está dando mayor prioridad a salvar, proteger y custodiar el activo de la información, debido a que los sistemas de información y los avances tecnológicos están siendo implementados en todas las empresas del mundo.

El Concejo Municipal de Coveñas, sigue los lineamientos trazados por el gobierno nacional, en cumplimiento de la Ley de transparencia 1712 de 2014 y gobierno en línea, que viene impulsando actividades dentro de las entidades públicas, para que se ajusten a modelos y estándares que permitan brindar seguridad a la información dando cumplimiento al Decreto 1078 de 2015.

Los riesgos por desastres naturales, riesgos inherentes relacionados con procesos no adecuados en el tratamiento de la misma información, desconocimiento de normas y políticas de seguridad y el no cumplimiento de estas, suelen ser los temas más frecuentes, de mayor impacto, presentes en las empresas. Una entidad sin un plan de gestión de riesgos está expuesta a perder su información.

Todas las organizaciones deberían implementar planes para gestionar los riesgos que afectan a los sistemas de información, tecnologías de información y activos informáticos. Considerando que en la actualidad los riesgos más comunes son generados por ataques dirigidos al software empresarial, afectando la disponibilidad e integridad de la información, almacenada o transportada a través de los equipos de comunicación.

Por esta razón hay que estar preparados para prevenir todo tipo de ataques o desastres, ya que cuando el costo de recuperación supera al costo de prevención, es preferible tener implementados planes de gestión de riesgos que permitan la continuidad del negocio tras sufrir alguna perdida o daño en la información de la entidad.

Considerando la situación actual del Concejo Municipal de Coveñas, para reducir los niveles de riesgo, es indispensable diseñar un plan para iniciar las prácticas de las normas y políticas de seguridad e implementar procesos que aseguren la continuidad de los servicios.

10.2. Definición gestión de riesgo.

La definición estandarizada de riesgo proviene de la organización internacional de normalización (ISO), definiéndolo como "*la posibilidad de que una amenaza determinada explote las vulnerabilidades de un activo o grupo de activos y por lo tanto causa daño a la organización*".

10.3. Visión general para la administración del riesgo de seguridad de la información.

10.4. Identificación del riesgo.

1. **Riesgo estratégico:** se asocia con la forma en que se administra la entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la gerencia.

2. **Riesgos de imagen:** están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

3. **Riesgos operativos:** comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional de la definición de procesos de la estructura de la entidad y de la articulación entre dependencias.

4. **Riesgos financieros:** se relacionan con el manejo de recurso de la entidad que incluyen: la ejecución presupuestal, la elaboración de estados financieros, los pagos, los manejos de excedentes de tesorería y el manejo sobre los bienes.

5. **Riesgos de cumplimiento:** se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales de ética pública y en general con su compromiso ante la comunidad de acuerdo con su misión.

6. **Riesgos de tecnología:** están relacionados con la capacidad tecnológica de la entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

10.5. Situación no deseada.

- Hurto de información o equipos informáticos.
- Hurto de información durante el cumplimiento de las funciones laborales, por intromisión.
- Incendio en las instalaciones de la empresa por desastre natural o de manera intencional.
- Alteración de claves y de información.
- Perdida de información.
- Baja cobertura de internet.
- Daño de equipos y de información.
- Atrasos en la entrega de información.
- Fuga de información.
- Manipulación indebida de información.

11. Marco Referencial.

11.1. Política de Administración de Riesgos.

El objetivo de la política es establecer los parámetros necesarios para una adecuada gestión de los riesgos de gestión, corrupción, seguridad y privacidad de la información, seguridad digital y continuidad de los servicios del Concejo de Coveñas procurando que no se materialicen, atendiendo los lineamientos establecidos en el plan de tratamientos de riesgos orientando a la toma de decisiones oportunas y minimizando efectos adversos al interior de la entidad, con el fin de dar continuidad a la gestión institucional y asegurar el cumplimiento de los compromisos.

Se orienta hacia una cultura de la gestión del riesgo asociados en el desarrollo de sus procesos, en aras de cumplir con su responsabilidad de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector TIC que contribuyen al desarrollo social y económico del país, al desarrollo integral de los ciudadanos y la mejora en su calidad de vida.

El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías: defensa, es decir, el líder o responsable del proceso junto con su equipo de trabajo para la mitigación de los diferentes riesgos.

El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

- **Aceptar el riesgo**: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. (Ningún riesgo de corrupción es aceptado). La aceptación del riesgo puede ser una opción viable en la entidad, para los riesgos bajos, pero también pueden existir escenarios de riesgos a los que no se les puedan aplicar controles y, por ende, se acepta el riesgo. En ambos escenarios debe existir un seguimiento continuo del riesgo.

- **Reducir el riesgo**: Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles. Deben seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este.

- **Evitar el riesgo**: Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.

- **Compartir el riesgo**: Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad. Los dos principales métodos de compartir o transferir parte del riesgo son: seguros y tercerización.

La gestión de riesgos de seguridad y privacidad de la Información, seguridad digital y continuidad de la operación de los servicios le permite al Concejo de Coveñas realizar una identificación, análisis y tratamiento de los riesgos que puedan generar afectación al cumplimiento de los objetivos de sus procesos, contribuyendo en la toma de decisiones, y en la prevención de la materialización de estos. La administración de riesgos de seguridad y privacidad de la información se encuentra enfocada en identificar, analizar, valorar y tratar las amenazas y vulnerabilidades de los activos de información de la entidad, teniendo presente su criticidad y protección. Las etapas presentes en la gestión de riesgos permiten alinearlas con los objetivos, estrategias y políticas corporativas, logrando un nivel de riesgo que pueda aceptar o asumir la alta dirección.

12. Metodología

El Plan de Tratamiento de riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos, estas actividades se estructuraron de la siguiente manera, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016) estos documentos tiene como objetivo generar un lineamiento para la gestión del riesgo del Concejo de Coveñas, que permita la mejora continua y el cumplimiento de los objetivos institucionales mediante el tratamiento de controles fortaleciendo el desempeño de los procesos y la transparencia en la gestión Institucional y aplica para todos los procesos de la Corporación.

Gestión	Actividad	Tarea	Responsable	Fecha Inicio	Fecha Fin
Gestión de Riesgos	Sensibilización.	Socialización guía y herramienta, gestión de riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación	Presidente Secretaria General	mayo	junio
	Identificación de riesgos y seguridad de la información, seguridad digital y continuidad de la operación.	Identificación, análisis y evaluación de riesgos y seguridad y privacidad de la información, seguridad digital y continuidad de la operación.	Presidente Secretaria General	mayo	julio
	Aceptación de riesgos identificados.	Aceptación, aprobación de riesgos identificados y planes de tratamientos.	Presidente Secretaria General	julio	septiembre
	Seguimiento fase de tratamiento.	Seguimiento estado de planes de tratamientos de riesgos identificados y verificación de evidencias.	Presidente Secretaria General	julio	octubre
	Evaluación de riesgos residuales.	Evaluación de riesgos residuales.	Presidente Secretaria General	julio	octubre
	Mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales Actualización guía de gestión de riesgos, seguridad de la información de acuerdo a los cambios solicitados.	Presidente Secretaria General	octubre	diciembre
	Monitoreo y revisión.	Generación, presentación y reportes de indicadores.	Presidente Secretaria General	octubre	diciembre

13. Desarrollo Metodológico

Fase 1: Análisis de la información

En esta etapa se evaluarán los resultados de las entrevistas con los colaboradores del proceso Tic, se desarrollarán las siguientes actividades:

- Aplicar las políticas de tratamiento de riesgos.

- Determinar los controles (se desprenden de las medidas) aplicados en el Ministerio TIC.
- Determinar los riesgos que van a ser incluidos en el Plan de Tratamiento de Riesgos.

Fase 2: Desarrollo de los proyectos

En esta fase se realizarán las actividades que permitan la estructuración de las medidas:

- Determinar el nombre de la medida.
- Definir los responsables de cada medida.
- Establecer el objetivo de cada medida.
- Elaborar la justificación de la medida.
- Definir las actividades a realizar para el desarrollo de la medida.

Fase 3: Análisis de los proyectos

- Definición de los controles relacionados con cada medida.
- Validar los riesgos mitigados por cada medida.
- Análisis de la aplicabilidad de las medidas.
- Priorización de las medidas.

Fase 4: Definición del organigrama de responsabilidad.

En esta fase se realizará un organigrama y se definirán responsabilidades respecto a la administración y gestión del riesgo, esta etapa deberá ser definida por el Concejo Municipal de Coveñas, teniendo en cuenta su estructura organizacional para la gestión de riesgos.

- Identificación de las funciones del Concejo de Coveñas en materia de seguridad de la información.
- Definición del grupo de trabajo de gestión de riesgo por parte del Concejo Municipal de Coveñas.
- Definición de las funciones del grupo de trabajo referente a la aplicación y gestión de las medidas.

Fase 5: Ciclo de vida del tratamiento de riesgos.

Definir las actividades a realizar por cada uno de los elementos del ciclo de vida del Plan de Tratamiento de Riesgos.

- **Planear**: Dentro de esta etapa se desarrollan las actividades definidas en la fase 1 de la metodología de tratamiento de riesgos.

- **Hacer**: En este paso del ciclo de vida se desarrollarán las actividades enmarcadas en la fase 2 de la metodología del tratamiento de riesgos.

- **Verificar**: En esta etapa se desarrollarán las actividades que permiten hacer seguimiento o auditorías a la ejecución de cada una de las medidas.

- **Actuar**: Dentro de esta etapa se realizarán las mejoras teniendo en cuenta el seguimiento y los resultados de las auditorías de la ejecución de los proyectos.

14. **Plan de Tratamiento de Riesgos de Seguridad de la Información**.

14.1. **Factores de Riesgos**.

Para la vigencia 2026 se priorizan los siguientes factores de riesgo digital en el Plan de Tratamiento de Riesgos:

- Nivel de conocimiento del personal en amenazas digitales, políticas y controles de seguridad.
- Disponibilidad permanente de servicios esenciales como telecomunicaciones, energía e infraestructura.
- Mejora locativa del Concejo Municipal de Coveñas.
- Identificación y protección de los datos de carácter personal.
- Adecuada clasificación de la información bajo custodia del Concejo Municipal de Coveñas de acuerdo con el marco legal vigente.

15. **Valoración del Riesgo**.

El análisis del riesgo busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y valorándolos con el fin de obtener información para establecer el nivel de riesgo y las posibles acciones a implementar.

El análisis de riesgos influye las fuentes, así como los factores que generan las consecuencias y aumentan la probabilidad de que ocurran. En la etapa de análisis se identifican los controles existentes ya sean administrativos, técnicos y/o procedimientos implementados en la entidad. Por lo tanto, se analiza el riesgo combinando estimaciones de impacto y probabilidades en el contexto de las medidas de control existente.

La aplicación de análisis cualitativo facilita la calificación y evaluación de los riesgos al aplicar formas descriptivas para presentar la magnitud de las consecuencias potenciales y la posibilidad de ocurrencia (consecuencia y probabilidad). La siguiente tabla describe la valoración de los riesgos definidos por el Concejo Municipal de Coveñas.

16. **Estrategia de Tratamiento de Riesgo**.

Las estrategias en el tratamiento de riesgos consisten en minimizar la probabilidad de materialización del riesgo. Para ello, se evidencian cuatro opciones:

- **Transferir**: Son procedimientos que permiten eliminar el riesgo por medio de la transferencia.

- **Mitigar**: Permite reducir la probabilidad de ocurrencia del riesgo o reducir sus consecuencias. La probabilidad de ocurrencia de un riesgo, puede reducirse a través de controles de gestión, políticas y procedimientos encaminados a reducir la materialización del riesgo.

- **Evitar**: Puede evitarse el riesgo no procediendo con la actividad que incorporaría el riesgo, o escoger medios alternativos para la actividad que logren el mismo resultado y no incorporen el riesgo detectado.

- **Aceptar**: Consiste en hacer frente al riesgo (positivo o negativo) o porque no se ha identificado ninguna otra estrategia de respuesta adecuada.

La estrategia de control de riesgos para la vigencia 2026, contempla cuatro ejes que son: conocimiento, continuidad, control de acceso y controles tecnológicos, así:

ESTRATEGÍAS DE CONTROL DE RIESGOS 2026			
CONOCIMIENTO	CONTINUIDAD DEL SERVICIO	CONTROL DE ACCESO	CONTROLES TECNOLOGÍCOS.
Habeas Data	Servicios esenciales	Inventario de activos de la información	Detección de eventos
Transparencia y Acceso	Planes alternos de operación		Seguridad en la nube
Políticas de Seguridad		Roles y privilegios	Copias de respaldo
Amenazas Informáticas	Anticipación de eventos de riesgo.	Acuerdos de confidencialidad.	Parches de seguridad.

- **Estrategias orientadas al conocimiento**: Mediante actividades de inducción, sensibilización y capacitación periódica, se busca que todos los servidores y contratistas, apropien conocimientos en materia de:

i. Ley de protección de datos personales.
ii. Ley de transparencia y acceso a la información.
iii. Políticas institucionales de seguridad digital.
iv. Modalidades y control de ataques informáticos.

- **Estrategias orientadas a la continuidad del servicio**: Para afrontar escenarios de riesgo asociados a la pérdida de continuidad, el Concejo Municipal de Coveñas en la vigencia 2026, realizará acciones específicas en materia de:

i. Mejora locativa,
ii. Actualización de planes articulados con las políticas institucionales y la planeación institucional en consonancia con la nueva visión.
iii. Mejoramiento de las capacidades de detección oportuna de eventos adversos de seguridad de la información.

- **Estrategias orientadas al control de acceso**: Con la finalidad de prevenir y controlar el acceso no autorizado a activos de información clasificados y reservados, la Corporación emprenderá en la vigencia 2026 acciones específicas para:

i. Revisar y/o actualizar los instrumentos de acceso a la información pública.
ii. Reforzar los controles de acceso a activos de información con roles y privilegios más precisos.
iii. Reforzar el cumplimiento de las políticas institucionales de gestión y desempeño adoptadas en la entidad.

- **Estrategias de fortalecimiento de controles técnicos**: Ante el aumento del tipo y complejidad de amenazas informáticas, el Concejo Municipal de Coveñas, implementará estrategias específicas en:

i. Identificación de eventos potencialmente nocivos.
ii. Reforzamiento de controles de acceso a servicios en la nube.
iii. Verificación y control de copias de respaldo.
iv. Control de cambios en plataformas tecnológicas.
v. Aplicación de parches de seguridad y actualización de equipos de procesamiento de datos, de ser necesario.

HOJA DE RUTA VIGENCIA 2026

PRODUCTO	VIGENCIA 2026											
	E	F	M	A	M	J	J	A	S	O	N	D
Estrategias de fortalecimiento en el conocimiento asociado a la seguridad digital y prevención de riesgos.		X	X				X				X	
Estrategias orientadas a la continuidad del servicio.		X	X	X			X				X	
Estrategias de fortalecimiento de controles técnicos.		X	X				X				X	

17. **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 en 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)

18. **Cronograma**.

Para dar cumplimiento al ciclo de gestión de riesgos, el cronograma se define y actualiza anualmente, incluyendo las etapas de identificación, análisis, evaluación y tratamiento de los riesgos. Los riesgos de seguridad digital identificados se reflejarán en el Mapa de Riesgos Institucional, donde se establecerán las acciones de control necesarias, junto con las fechas previstas para su implementación. La oficina de sistemas e informática, o el despacho delegado, proporcionará apoyo en la definición y diseño de estos controles, trabajando de forma coordinada con los líderes de cada grupo o dependencia responsable.

Según lo expuesto en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, emitida por el Departamento Administrativo de la Función Pública, el tratamiento de riesgos constituye la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos. En este contexto, la planeación hace referencia específica al tratamiento de riesgos de Seguridad y Privacidad de la Información, enfocándose en la protección de los activos de información a cargo de la Secretaría General. Para este fin, se ejecuta un conjunto de actividades durante la vigencia anual, orientadas a implementar los controles requeridos y priorizados según la criticidad de los riesgos identificados.

En atención a lo anterior, a continuación, se describen las actividades más relevantes orientadas al tratamiento de riesgos de Seguridad y Privacidad de la Información:

1. **Identificación y Actualización del Inventario de Activos de Información**: Catalogar y mantener actualizado el inventario de activos de información, incluyendo datos, sistemas, aplicaciones y dispositivos.

2. **Evaluación de Riesgos**: Realizar análisis periódicos para identificar vulnerabilidades y amenazas que puedan afectar la confidencialidad, integridad y disponibilidad de la información.
3. **Definición y Priorización de Controles**: Establecer controles técnicos, administrativos y físicos, priorizando aquellos que mitiguen riesgos de mayor impacto.
4. **Capacitación y Concienciación**: Desarrollar programas de formación continua para el personal sobre buenas prácticas en seguridad de la información y manejo de datos sensibles.
5. **Monitoreo y Seguimiento**: Implementar mecanismos de monitoreo constante para evaluar la eficacia de los controles y realizar ajustes cuando sea necesario.
6. **Gestión de Incidentes de Seguridad**: Establecer procedimientos claros para la detección, reporte y respuesta a incidentes de seguridad de la información.
7. **Revisión y Actualización del Mapa de Riesgos**: Realizar revisiones periódicas del Mapa de Riesgos Institucional para incorporar nuevos riesgos identificados y ajustar los controles existentes.

El objetivo es mantener implementado los lineamientos a nivel de seguridad de la información en la entidad, que esté protegida frente a las amenazas cibernéticas cumplir con los estándares y normas establecidas de seguridad y privacidad de la información.

Estas actividades permiten fortalecer la postura de seguridad de la información en la entidad, garantizando la protección de los datos y el cumplimiento de la normatividad vigente en materia de seguridad digital y privacidad.

19. **Recursos**.

La estimación y asignación de los recursos necesarios para la ejecución del plan de tratamiento de riesgos de seguridad de la información, identificados en la entidad, será responsabilidad directa del dueño del riesgo. Este rol implica no solo la identificación y priorización de los riesgos, sino también la evaluación de los recursos financieros, tecnológicos y humanos requeridos para mitigar o eliminar dichos riesgos. El dueño del riesgo deberá garantizar que estos recursos sean suficientes y adecuados para la implementación efectiva de los controles definidos en el plan de tratamiento. Asimismo, será responsable de contribuir activamente en el seguimiento y control continuo de la gestión de riesgos, asegurando que las acciones correctivas se lleven a cabo conforme a los plazos establecidos y que los controles implementados sean revisados periódicamente para verificar su eficacia. Esta gestión incluye la documentación y reporte de los avances a las instancias correspondientes, así como la toma de decisiones oportunas en caso de que se identifiquen desviaciones o nuevas amenazas.

20. **Indicadores**.

La medición se realiza con un indicador de gestión que está orientado principalmente a disminuir el número de riesgos identificados con nivel alto y externo a través de la implementación y evaluación de controles.

El número de riesgos identificados como no aceptables no debe ser superior al 20% del total de riesgos identificados.

21. **Consideraciones Generales**.

El desarrollo de las actividades necesarias para la consecución de los objetivos establecidos estará condicionado a la disponibilidad y adecuada asignación de diversos tipos de recursos, incluyendo recursos humanos, técnicos, tecnológicos y financieros. La ejecución efectiva de estas actividades dependerá no solo de la cantidad de recursos disponibles, sino también de su calidad, pertinencia y oportunidad. Este proceso estará alineado con la disponibilidad presupuestal aprobada y asignada de manera oportuna, lo cual garantiza que las actividades puedan llevarse a cabo sin interrupciones ni retrasos significativos.

Adicionalmente, la planificación y ejecución de estas actividades deberán enmarcarse en el apetito de riesgo institucional, es decir, el nivel de riesgo que la entidad está dispuesta a aceptar en el cumplimiento de sus metas. Este apetito de riesgo será definido y ajustado por la alta dirección, quienes proporcionarán directrices claras sobre los límites y tolerancias aceptables frente a los riesgos asociados a cada actividad. Dichas orientaciones permitirán priorizar acciones y tomar decisiones estratégicas en caso de limitaciones de recursos o aparición de contingencias.

De este modo, cualquier ajuste en la ejecución de las actividades deberá considerar tanto la capacidad presupuestal como el enfoque institucional frente al riesgo, asegurando un equilibrio entre la eficiencia operativa y la protección de los intereses y activos de la entidad.

Para el desarrollo de las actividades contempladas en este Plan, la Secretaría General asumirá un papel fundamental, contando con un equipo humano calificado y comprometido, que estará encargado de liderar y ejecutar las acciones necesarias para su correcta implementación. Este equipo estará conformado por profesionales con experiencia en las áreas pertinentes, quienes serán responsables de diseñar y llevar a cabo actividades de sensibilización, capacitación y atención de inquietudes dirigidas a las diferentes dependencias adscritas al Concejo Municipal en el nivel central.

Las actividades de sensibilización tendrán como objetivo principal generar conciencia sobre la importancia del cumplimiento del Plan, destacando su impacto en la gestión institucional y en el logro de los objetivos estratégicos. Por su parte, las capacitaciones estarán orientadas a fortalecer las competencias del personal, asegurando que cuenten con el conocimiento y las herramientas necesarias para aplicar adecuadamente las directrices establecidas en el Plan. Además, se establecerán canales de comunicación eficientes para la atención oportuna de dudas e inquietudes que puedan surgir durante el proceso, promoviendo un ambiente de colaboración y apoyo constante.

Todas estas actividades serán planificadas y organizadas mediante cronogramas definidos, que permitirán un seguimiento riguroso y garantizarán la cobertura adecuada de todas las dependencias involucradas. Estos cronogramas incluirán fechas específicas, responsables asignados, y recursos necesarios para cada actividad, facilitando una ejecución ordenada y eficiente.

Se recomienda el seguimiento constante a los procesos y la implementación del plan de mitigación de riesgo de seguridad de la información el cual deben ser ejecutados, monitoreados, actualizados frecuentemente y será integrado y divulgado a más tardar el 31 de enero de cada año según el Decreto 612 de 2018.

Es indispensable implementar el plan de gestión de riesgo que permitirá prevenir las posibles amenazas encontradas en la infraestructura tecnológica de la entidad.

Las políticas de seguridad de la información del Concejo Municipal de Coveñas deben ser revisadas y actualizadas conforme al crecimiento, cambios de la estructura organizacional, exigencias del gobierno y los mismos procesos dentro de la entidad.

La secretaria del concejo también será responsable de evaluar periódicamente el impacto de estas acciones, realizando los ajustes necesarios para mejorar continuamente el proceso y asegurar el cumplimiento de los objetivos del Plan.

DARWIN CHICA TIRADO
Presidente

MARÍA P. MENDOZA VEGA
Primer vicepresidente

MARTA RIOS REVUELTA
Segunda vicepresidenta

KELLY J. MENA OROZCO
secretaria

Concejo Municipal de Coveñas

Anexo N°.01

PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2026

No.	Actividades	Meta	Hitos	Fecha de Inicio	Fecha fin	Responsable
01	Documentar y actualizar la información de seguridad de la información alineada a los objetivos estratégicos del Concejo Municipal.	Documentación actualizada del sistema de seguridad de la información.	1. Actualizar la política general de seguridad de la información enfocando: * Mejoramiento ciberseguridad * Protección de datos personales * Protección contra malware y ransomware	2026/02/01	2026/11/30	Oficina de Tecnologías de la Información y las Comunicaciones.
02	Diseñar, aplicar y comunicar un programa de concientización en seguridad de la información.	Programa de concientización en seguridad de la información.	1-. Definir la temática sobre seguridad de la información. 2. socialización a través de capacitaciones.	2026/02/01	2026/11/30	Oficina de Tecnologías de la Información y las Comunicaciones.
03	Documentar y actualizar los procedimientos, políticas, estrategias de aseguramiento de datos.	Procedimientos, políticas, estrategias de aseguramiento de datos, documentos y actualizados.	1-. Actualizar la declaración de aplicabilidad 2. Actualizar los activos de información de Función Pública 3. Desarrollar los lineamientos de la	2026/02/01	2026/11/30	Oficina de Tecnologías de la Información y las Comunicaciones.

			política de control de acceso 4. Actualizar el procedimiento para la gestión de incidentes 5. Actualizar el procedimiento de continuidad de negocio.			
04	Aplicar la mejora continua al Sistema de Gestión de Seguridad de la Información.	Mejora continua al Sistema de Gestión de Seguridad de la Información aplicada.	Realizar análisis de los riesgos actuales para la seguridad de la información 2. Realizar el procedimiento actualizado de respuesta ante incidentes de seguridad y ciberataques.	2026/02/01	2026/11/30	Oficina de Tecnologías de la Información y las Comunicaciones.

Concejo Municipal de Coveñas

Anexo N°.02

Matriz de Vulnerabilidad y Mitigación del Riesgo

Vulnerabilidad	Descripción	Causa	Efecto	Clasificación	Evaluación	Mitigación del Riesgo	Vigencia
Las políticas y normas de seguridad no se están cumpliendo	Algunos funcionarios de la entidad, desconocen algunas normas de seguridad con respecto a la información que se maneja en el concejo	Los funcionarios del concejo cumplen su contrato e ingresa un nuevo a reemplazar sus funciones.	Incumplimiento de confidencialidad	Riesgo Humano	Riesgo moderado.	Capacitar a los funcionarios nuevos	2026
No hay la suficiente cantidad de equipos de cómputo.	En algunos casos los funcionarios se ven obligados a pedir prestados los equipos para terminar su labor.	Algunos de los equipos tienen fallas físicas por el uso.	Retrasar las labores de los funcionarios.	Riesgo físico. Riesgo Humano	Riesgo moderado.	Habilitar a los funcionarios computadores de gran capacidad y desempeño.	2026
Uso de memorias extraíbles.	La información es llevada en memorias o discos duros portátiles personales y se desconoce el uso de la misma, tampoco se hace el uso de antivirus para evitar virus y daños en los equipos.	No se lleva un control de qué información guardan en sus memorias o discos duros portátiles personales	Incumplimiento de confidencialidad	Riesgo Humano	Riesgo alto	Capacitar a los funcionarios, para evitar daños en los equipos y para que conozcan las políticas de confidencialidad.	2026
Documentos importantes de la entidad no se encuentra digitalizados.	Muchos de los informes, acuerdos, entre otros archivos, no se encuentran digitalizados.	No se ha digitalizado con eficiencia los documentos.	Perdida de información importante para la entidad.	Riesgo físico	Riesgo alto.	Digitalizar todos los documentos y crear copia de seguridad de ellos.	2026