



Coveñas
es de todos

**PLAN DE TRATAMIENTO
DE RIESGOS DE SEGURIDAD
Y PRIVACIDAD DE LA
INFORMACIÓN 2020**



**KEBIN ZUBIRIA PEROZA
PRESIDENTE DEL CONCEJO
2020**

Un concejo para todos

CONCEJO MUNICIPAL DE COVEÑAS - SUCRE

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2020

EDUCACIÓN

ENERO DE 2020

RIQUEZAS

CONFORMACIÓN DEL CONCEJO MUNICIPAL

PLENARIA DEL CONCEJO	
KEBIN ANDRES ZUBIRIA PEROZA	PARTIDO CENTRO DEMOCRATICO
SADDAM ALBERTO FERIA MERCADO	PARTIDO CENTRO DEMOCRATICO
ERIK HERNANDEZ JULIO	PARTIDO CAMBIO RADICAL
KEVIN DANIEL MONTERROZA PANTOJA	PARTIDO ASI
NETSKY FERIA MORENO	PARTIDO ASI
SEBASTIAN ROMERO GONZALEZ	PARTIDO ASI
JAVIER SEGUNDO NUÑEZ RINCO	PARTIDO ASI
CARLOS JOSE MORALES CASTELLANOS	PARTIDO CONSERVADOR
MARTA ISABEL RIOS REVUELTA	PARTIDO LIBERAL
ALICIA SOFIA MIENTES DIAZ	PARTIDO LIBERAL
SORAIDA MARQUEZ LOPEZ	PARTIDO DE LA U

EDUCACIÓN

Y

RIQUEZAS

MESA DIRECTIVA DEL CONCEJO MUNICIPAL AÑO 2020

KEBIN ANDRES ZUBIRIA PEROZA

PRESIDENTE

CARLOS MORALES CASTELLANOS

PRIMER VICEPRESIDENTE

SEBASTIAN ROMERO

SEGUNDO VICEPRESIDENTE

MERLY MARTINEZ OSORIO

SECRETARIA GENERAL

EDUCACIÓN

Y

RIQUEZAS

Contenido

PRESENTACION	6
1. REFERENCIA NORMATIVA.....	6
2. OBJETIVOS DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.....	8
2.1 Objetivo General	8
2.2 Objetivos Específicos.....	8
3. ALCANCES.....	8
4. NATURALEZA DE LA CORPORACIÓN CONCEJO MUNICIPAL DE COVENAS.....	9
a. Naturaleza Jurídica.....	9
b. Identificación De La Entidad	9
c. Función Social – Cometido estatal.....	9
5. DEFINICIONES.....	10
6. GESTION DE RIESGOS.....	13
a. Importancia de la gestión de riesgos.....	13
7. DIAGNOSTICO DE SISTEMAS DE INFORMACIÓN	14
APOLO ULTRA VERSIÓN NET:	15
8. ARQUITECTURA DE PROCESAMIENTO Y ALMACENAMIENTO	15
a. Arquitectura de red.....	15
9. ESTADO DE LA SEGURIDAD DE LA INFORMACIÓN.....	15
10. RIESGOS ENCONTRADOS	16
11. RECURSOS.....	18
12. RESPONSABLES.....	18
13. SEGUIMIENTO Y EVALUACIÓN.	18

EDUCACIÓN

Y

RIQUEZAS

PRESENTACION

La gestión de los riesgos de seguridad de la información son aquellos procesos que reducen las pérdidas y brindan protección de la información, permitiendo conocer las debilidades que afectan durante todo el ciclo de vida del servicio.

Es muy importante que las organizaciones cuenten con un plan de gestión de riesgos para garantizar la continuidad de las funciones misionales, por este motivo, se ha visto la necesidad de desarrollar un análisis de riesgo de seguridad de la información aplicado en el Concejo Municipal de Coveñas, antes de iniciar con este plan de gestión se ha revisado la situación actual de la entidad y la identificación de los activos con sus respectivas amenazas, para continuar con la medición de riesgos existentes y sugerir las protecciones necesarias que podrían formar parte del plan de gestión de riesgos en la seguridad de la información.

El aporte que arroja este plan permite identificar el nivel de riesgo en que se encuentran los activos mediante el nivel de madurez de la seguridad existente y sobre todo incentivar al personal a seguir las respectivas normas y procedimientos referentes a la seguridad de la información y recursos.

1. REFERENCIA NORMATIVA

El marco jurídico en el cual se fundamenta el plan de previsión de recursos humanos, para los empleos es el siguiente:

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	Atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos
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.	Regulación para tener en cuenta en la creación de cadenas de servicio en sistemas de información

<p>Ley 1266 de 2008</p>	<p>Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones</p>	<p>Derecho constitucional que tienen todas las personas a 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.</p>
<p>Ley 1712 de 2014</p>	<p>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.</p>	<p>Acceso a la información pública, Publicación de información.</p>
<p>Decreto 2573 de 2014</p>	<p>Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones y que son de obligatorio cumplimiento para las entidades que conforman la administración pública en Colombia</p>	<p>Gobierno en línea</p>



2. OBJETIVOS DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

2.1 Objetivo General

Desarrollar un plan de gestión de seguridad y privacidad que permita minimizar los riesgos de pérdida de activos, el manejo de medios, control de acceso y gestión de usuarios. De la información en el Concejo Municipal de Coveñas.

2.2 Objetivos Específicos.

- Plantear modelos de reportes para su posterior uso en cada incidencia presentada en el Concejo Municipal de Coveñas.
- Gestionar los eventos de seguridad de la información para detectar y tratar con eficiencia, en particular identificar si es necesario o no clasificarlos como incidentes de seguridad de la información.
- Determinar el alcance del plan de gestión de riesgos de la seguridad y privacidad de la información.
- Identificar las necesidades en materia de seguridad de la información de la entidad, presentes y futuras derivadas del ejercicio de sus competencias.
- Determinar los riesgos y amenazas que se puedan presentar y sus efectos.
- Definir la forma de cubrir dichos eventos y las posibles contingencias.
- Proponer soluciones para minimizar los riesgos a los que está expuesto cada activo.
- Formular el plan de acción con las medidas para la Planeación Sistema de Gestión de Seguridad de la Información, documentación, procedimientos y requerimientos pertinentes a la seguridad de la información, establecidos por El Ministerio de las Tecnologías de La información.
- Identificar las necesidades de capacitación e incluirlas en el plan de capacitación institucional.
- Ejecutar el plan de acción con las medidas para la reducción de los riesgos en la entidad.

3. ALCANCES

- Lograr el compromiso del Concejo Municipal para emprender la implementación del plan de gestión del riesgo en la seguridad de la información.
- Designar funciones de liderazgo para apoyar y asesorar el proceso de diseño e implementación del plan de gestión.
- Capacitar al personal de la entidad en el proceso de plan de gestión del riesgo de la seguridad de la información.

4. NATURALEZA DE LA CORPORACIÓN CONCEJO MUNICIPAL DE COVEÑAS

a. Naturaleza Jurídica.

El Concejo Municipal de Coveñas, es una entidad pública sin personería Jurídica, definida bajo el contexto de los artículos 21 y 22 de la Ley 136 de 1994, cuenta con autonomía independiente, adscrita al Municipio de Coveñas, departamento de sucre, regulada por el Acuerdo 005 de agosto 28 de 2016, tiene su domicilio en el municipio de Coveñas, y ejerce sus operaciones en las instalaciones del Palacio Municipal. El presidente de la mesa directiva es el representante legal de la corporación, por el periodo respectivo.

b. Identificación De La Entidad

Razón Social:	Concejo Municipal de Coveñas
NIT:	823.004.035-1
Dirección	Calle 3B No. 4-16. Urb. Alicante.
Municipio	Coveñas
Departamento	Sucre
Naturaleza Entidad	Pública
Carácter de Entidad	Corporación.

c. Función Social – Cometido estatal.

El Concejo Municipal de Coveñas, debe cumplir con las funciones establecidas en la constitución, en la ley, y en su reglamento interno, en especial las establecidas en el artículo 313 de la constitución nacional.

Además de las funciones que se le señalan en la Constitución y la ley, son atribuciones de los concejos las siguientes, de acuerdo a lo establecido en la ley 1551 de 2012 y 136 de 1994.

5. DEFINICIONES

Para la ejecución de este plan, se tendrán en cuenta los siguientes términos y definiciones en relación a la administración del riesgo:

identificados asociados	Acciones	son las acciones que se deben tomar posterior a determinar las opciones de manejo del riesgo (asumir, reducir, evitar compartir o transferir), dependiendo de la evaluación del riesgo residual, orientadas a fortalecer los controles
Administración de riesgos		conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.
Amenaza		situación externa que no controla la entidad y que puede afectar su operación
Análisis del riesgo		etapa de la administración del riesgo, donde se establece la probabilidad de ocurrencia y el impacto del riesgo antes de determinar los controles (análisis del riesgo inherente).
Asumir el riesgo		Opción de manejo donde se acepta la pérdida residual probable, si el riesgo se materializa.
Bases de Datos Personales		Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).
Ciberseguridad:		Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).
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).
Causa		Medios, circunstancias y/o agentes que generan riesgos.
Calificación del riesgo		Estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.
Compartir o transferir el riesgo		opción de manejo que determina traspasar o compartir las pérdidas producto de la materialización de un riesgo con otras organizaciones mediante figuras como outsourcing, seguros, sitios alternos
Consecuencia		efectos que se pueden presentar cuando un riesgo se materializa.
Contexto estratégico		son las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución.
Control		Acción o conjunto de acciones que minimiza la

	probabilidad de ocurrencia de un riesgo o el impacto producido ante su materialización
Control preventivo	Acción o conjunto de acciones que eliminan o mitigan las causas del riesgo; está orientado a disminuir la probabilidad de ocurrencia del riesgo.
Control correctivo	Acción o conjunto de acciones que eliminan o mitigan las consecuencias del riesgo; está orientado a disminuir el nivel de impacto del 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.
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.
Debilidad	situación interna que la entidad puede controlar y que puede afectar su operación.
Evaluación del riesgo	resultado del cruce cuantitativo de las calificaciones de probabilidad e impacto, para establecer la zona donde se ubicará el riesgo
Evitar el riesgo:	Opción de manejo que determina la formulación de acciones donde se prevenga la materialización del riesgo mediante el fortalecimiento de controles identificado.
Frecuencia	Ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.
Identificación del riesgo	etapa de la administración del riesgo donde se establece el riesgo con sus causas (asociadas a factores externos e internos de riesgo), consecuencias y se clasifica de acuerdo con los tipos de riesgo definidos
Impacto	Medida para estimar cuantitativa y cualitativamente el posible efecto de 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).
Mapa de riesgos	Documento que, de manera sistemática, muestra el desarrollo de las etapas de la administración del riesgo.
Materialización del riesgo	Ocurrencia del riesgo identificado
Opciones de manejo	posibilidades disponibles para administrar el riesgo posterior a la valoración de los controles definidos (asumir, reducir, evitar, compartir o transferir el riesgo residual).
Plan de contingencia	conjunto de acciones inmediatas, recursos, responsables y tiempos establecidos para hacer frente a la materialización del riesgo y garantizar la continuidad del servicio
Probabilidad	medida para estimar cuantitativa y cualitativamente la posibilidad de ocurrencia del riesgo.
Procedimiento	Conjunto de especificaciones, relaciones, responsabilidades, controles y ordenamiento de las actividades y tareas requeridas para cumplir con el proceso.
Proceso	Conjunto de entradas tangibles o intangibles, suministradas por un proveedor, a estas entradas se les asigna recursos y se aplican controles, obteniendo salidas tangibles o intangibles, destinadas a un usuario, generando un impacto en estos. Se clasifican en estratégicos, misionales, de apoyo y de evaluación.
Riesgo	Eventualidad que tendrá un impacto negativo sobre los objetivos institucionales o del proceso
Riesgo de corrupción	Posibilidad de que por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular.
Riesgo inherente	Es aquel al que se enfrenta una entidad o proceso en ausencia de controles y/o acciones para modificar su probabilidad o impacto.
Riesgo institucional	Son los que afectan de manera directa el cumplimiento de los objetivos o la misión institucional. Los riesgos institucionales, son producto del análisis de los riesgos por proceso y son denominados de este tipo cuando cumplen las siguientes características: - Los riesgos clasificados como estratégicos: en el paso

	<p>de identificación deben haber sido marcados como de clase estratégica, es decir, se relacionan con el cumplimiento de objetivos institucionales, misión y visión.</p> <ul style="list-style-type: none"> - Los riesgos en zona alta o extrema: después de valorar el riesgo (identificación y evaluación de controles), el riesgo residual se ubica en zonas de riesgo alta o extrema, indicando que el grado de exposición a la materialización del riesgo aún se encuentra poco controlado. - Los riesgos que tengan incidencia en usuario o destinatario final externo: en el caso de la materialización del riesgo la afectación del usuario externo se presenta de manera directa.
Riesgo residual	Nivel de riesgo que permanece luego de determinar y aplicar controles para su administración.
Seguridad de la información	Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
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).
Valoración del riesgo	Establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización. En la etapa de valoración del riesgo se determina el riesgo residual, la opción de manejo a seguir, y si es necesita.

6. GESTION DE RIESGOS

a. Importancia de la gestión de riesgos

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 la transformación digital de la administración pública a través de 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 y 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 deberán 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, 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 de la entidad tras sufrir alguna pérdida o dañen 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.

7. DIAGNOSTICO DE SISTEMAS DE INFORMACIÓN

El Inventario de equipos de cómputo, periféricos y sistemas de Información del Concejo municipal de Coveñas, es el siguiente:

EQUIPOS DE OFICINA:	CANTIDAD	LICENCIA DE WINDOWS	LICENCIA DE ANTIVIRUS	LICENCIA DE OFFICE 365
Computadores de mesa completos	2	SI	SI	SI
Equipo de Computo tipo portátil,	4	SI	SI	SI
Impresoras	3	N/A	N/A	N/A
Escáner	1	N/A	N/A	N/A
Video beam	1	N/A	N/A	N/A
Fotocopiadora	2	N/A	N/A	N/A

a. Análisis de los sistemas de información Aplicativo de Producción

APOLO ULTRA VERSIÓN NET:

Sistema de información administrativo y financiero consta de los siguientes módulos:

Presup
uesto
Tesorer
ía
Contabi
lidad
Almacé
n

El sistema opera vía Web y utiliza una base de datos en SQL.

8. ARQUITECTURA DE PROCESAMIENTO Y ALMACENAMIENTO

En la actualidad no se cuenta con servidores, el almacenamiento se realiza en una unidad de disco duro externo de 500 Gb.

a. Arquitectura de red.

En la actualidad se cuenta con la infraestructura de redes inalámbricas para comunicaciones de datos proporcionada por la administración municipal.

La corporación cuenta con el portal web <http://www.concejodecovenas.gov.co>, teniendo como principal objetivo facilitar al máximo los procesos de publicidad e interrelación de la información que genera la entidad, con los usuarios en los espacios de información y participación definidos.

La corporación cuenta con el Correo electrónico concejo@covenas-sucre.gov.co

La corporación cuenta con los tipos de extintores adecuados para cada emergencia.

No se cuenta con una planta de energía suspendiendo los procesos laborales de todas las oficinas en caso de falla de la energía eléctrica.

No existen unidades UPS para los equipos de cómputo.

No existen estabilizadores eléctricos de los equipos de cómputo.

El mantenimiento Preventivo y correctivo a los equipos y sus dispositivos periféricos se realizan a través de contratos de mantenimiento con terceros.

9. ESTADO DE LA SEGURIDAD DE LA INFORMACIÓN

Del Plan de Seguridad y Privacidad de la Información, se desprenden las acciones

conducentes a reducir los riesgos detectados y ejecutar las acciones que faciliten el fortalecimiento de la seguridad de la información:

10. RIESGOS ENCONTRADOS

Hurto de equipos

informáticos. Hurto de

información.

Pérdida de información.

Alteración de claves y de información.

Fuga de información

Manipulación indebida de

información Baja calidad de internet.

Daño de equipos y de información

Incendio en las instalaciones de la corporación por desastre natural o de manera intencional.

Atrasos en la entrega de información

Escasa en asistencia técnica

Vulnerabilidad física de los equipos ante cambios, o corte de energía.

DEBILIDADES

- Existe escaso conocimiento de la gestión de seguridad y privacidad de la información.
- No existe una cultura en cuanto a la generación periódica de Backup de los documentos office, lo cual genera riesgos ante la pérdida de archivos digitales.
- Los procesos que requieren el servicio de internet, se tornan muy lentos debido al ancho de banda insuficiente.
- Operación de los equipos con Vulnerabilidad física ante cambios, o corte de energía.
- Inexistencia de una red de internet propia, utilizada y administrada por la corporación en forma exclusiva.
- Presupuesto limitado e insuficiente.

<p>OPORTUNIDADES</p>	<ul style="list-style-type: none"> • Realización de un estudio detallado de las condiciones que se deben cumplir, con el objetivo de definir las medidas correctivas, tendientes a mejorar la seguridad física de la sala y optimizar la disponibilidad de los servicios de TIC. • Formulación de la política de SGSI para facilitar el fortalecimiento de la seguridad de la información. • Implementación del plan de acción que permita la utilización de sistemas de información de forma confiable y segura. • Digitalización de toda la información que se encuentra en los documentos físicos que se manejan en la entidad. • Adquisición de equipos de protección para un Sistema de alimentación interrumpida, mediante una UPS y estabilizadores electrónicos que minimicen los riesgos de daños a los equipos de sistemas.
<p>FORTALEZAS</p>	<ul style="list-style-type: none"> • Compromiso de la Mesa directiva en el mejoramiento continuo de la entidad. • Se cuenta con el aplicativo del Sistema Apolo, el área Financiera el cual ha permitido incrementar la eficacia y eficiencia en los procesos que les corresponde, de tal forma que la información se maneja de forma segura. • Existencia de cuentas de usuario y claves para el acceso de los recursos informáticos, para los funcionarios. • Se cuenta con el portal web http://www.concejodecovenas.gov.co, permitiendo facilitar al máximo los procesos de publicidad e interrelación de la información que genera la entidad. • Equipos de cómputo en buen estado, con sistemas operativos actualizados. • Se cuenta con sistemas de climatización, por medio de aires acondicionado, los cuales son suficientes para su operatividad actual.
<p>AMENAZAS</p>	<ul style="list-style-type: none"> • Posibilidad de fuga de información por Manipulación indebida de los equipos informáticos, alteración de claves y de información. • Posibilidad de pérdida de información por hurto de los equipos informáticos, hurto de información, pérdida de información, alteración de claves y de información. • La red de internet implementada no es la más adecuada teniendo en cuenta que la red es de propiedad, utilizada y administrada por la alcaldía compartida con la corporación. • Baja señal y debilidad en la conexión WiFi. Existen cuentas de usuario y

claves para el acceso de los recursos informáticos, para los funcionarios, pero no existen para los concejales en los equipos compartidos.

- En la entidad está instalado el paquete ofimático Microsoft Office 2016, en la actualidad tres equipos presentan las licencias vencidas.
- No se ha digitalizado la totalidad de los documentos físicos que se manejan en la entidad, existiendo la posibilidad de daños físicos, perdidas, o extravíos por falta de sitios adecuados de almacenamiento.
- No se realizan copias de seguridad de los archivos.

11. RECURSOS

- ❖ Humano: presidente, Personal de Planta, Profesional contratista, Personal Externo
- ❖ Físico: PC y equipos de comunicación
- ❖ Financieros: Presupuesto de la vigencia 2020

12. RESPONSABLES

Presidente, Mesa Directiva, secretario del Concejo, Contratistas.

Para ello se establece el plan de tratamiento de riesgos de seguridad y privacidad de la información como se establece en el formato anexo que sigue a continuación.

13. SEGUIMIENTO Y EVALUACIÓN.

Al finalizar cada etapa se realizará una reunión con la mesa directiva y la Secretaría General para presentar el informe del avance del proyecto y de esta manera evaluar todos los pasos se han ido realizado.

EDUCACIÓN

Y

RIQUEZAS

CONCEJO MUNICIPAL DE COVEÑAS

PLAN DE TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2020

Riesgo	Logro	Actividad	Producto / Meta	Responsable	Fecha programada	Recursos
Físicos	Seguridad de los equipos Informáticos (Hardware)	Actualizar las medidas para el uso y el acceso a los equipos informáticos de la entidad	Acta de entrega y Recibo de Equipos	Secretaría General	hasta Dic 31 de 2020	Recursos técnicos y humanos
			Póliza de Seguros con Cobertura del riesgo de hurto o perdida	Secretaría General	hasta Dic 31 de 2020	Recursos técnicos, humanos, y Financieros
Seguridad de la Información	Seguridad de los equipos Informáticos (Software)	Actualizar las medidas para el acceso seguros de los equipos informáticos de la entidad	Establecimiento de Contraseñas a los usuarios de los equipos informáticos	Secretaría General	hasta Dic 31 de 2020	Recursos técnicos, humanos, y Financieros
		Actualización de los Software de los equipos	Actualización de Antivirus	Secretaría General	hasta Dic 31 de 2020	Recursos técnicos, humanos, y Financieros
			Actualización de licencias de sistemas operativos	Secretaría General	hasta Dic 31 de 2020	Recursos técnicos, humanos, y Financieros
			Actualización de licencias de paquetes ofimáticos	Secretaría General	hasta Dic 31 de 2020	Recursos técnicos, humanos, y Financieros
			Implementación de Copias de seguridad	Secretaría General	hasta Dic 31 de 2020	Recursos técnicos, humanos, y Financieros
Fuga de la Información	Seguridad de la Información	Actualización de un protocolo de Acceso a la Información	Implementación de Protocolo de acceso a la información y a Copias de seguridad	Secretaría General	hasta Dic 31 de 2020	Recursos técnicos, humanos, y Financieros

Vulnerabilidad física de los equipos ante cambios, o corte de energía (Eléctricos)	Seguridad de los equipos Informáticos (Instalaciones eléctricas y accesorios)	Actualizar las medidas para el uso seguro de los equipos informáticos de la entidad	Instalación de Equipos de protección eléctrica (reguladores, Ups)	Secretaria general	hasta Dic 31 de 2018	Recursos técnicos, humanos y financieros
		Mantenimiento a las redes eléctricas	Mantenimientos realizados	Secretaria general	hasta Dic 31 de 2018	Recursos técnicos, humanos y financieros
		Mantenimiento a las redes de Datos y Equipos de Internet y wifi	Mantenimientos realizados	Secretaria general	hasta Dic 31 de 2018	Recursos técnicos, humanos y financieros
Arquitectura de Redes	Seguridad de los Redes Informáticas	Instalación de Equipos	Equipos Instalados	Secretaria general	hasta Dic 31 de 2018	Recursos técnicos, humanos y financieros
		Actualización y Mantenimiento a las redes y arquitectura de Datos y Equipos de Internet y wifi	Arquitectura de Datos y Actualizada	Secretaria general	hasta Dic 31 de 2018	Recursos técnicos y humanos
Incendio en las instalaciones de la corporación por desastre natural o de manera intencional.	Seguridad física de las Instalaciones	Mantenimiento de Equipos Contra incendios	Mantenimiento a equipos extintores	Secretaria general	hasta Dic 31 de 2018	Recursos técnicos, humanos y financieros
Baja calidad de internet.	Mejora en la calidad del servicio	Mantenimiento a las redes de Datos y Cambio de Equipos de Internet y wifi	Mantenimiento y/o Cambio de equipos y redes	Secretaria general	hasta Dic 31 de 2018	Recursos técnicos, humanos y financieros
Deterioro o daño de Información en formato físico	digitalización de la totalidad de los documentos físicos	Mantenimiento a las redes de Datos y Cambio de Equipos de Internet y wifi	Mantenimiento y/o Cambio de equipos y redes	Secretaria general	hasta Dic 31 de 2018	Recursos técnicos, humanos y financieros