CONCEJO MUNICIPAL DE COVEÑAS SUCRE

ALICIA SOFIA MUENTES DIAZ
Presidente 2023

"Coveñas Es De Todos"

Plan de Seguridad y Privacidad de la Información

Vigencia 2023

Coveñas es de todos

CONCEJO MUNICIPAL DE COVEÑAS
NIT: 823004035-1

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VIGENCIA 2023

CONCEJO MUNICIPAL DE COVEÑAS - SUCRE

“UN CONCEJO PARA TODOS”

ENERO DE 2023

HONORABLES CONCEJALES

MESA DIRECTIVA DEL CONCEJO MUNICIPAL AÑO 2023

PRESIDENTE - ALICIA MUENTES DÍAZ

PRIMER VICEPRESIDENTE- CARLOS MORALES CASTELLANOS

SEGUNDO VICEPRESIDENTE SADDAM FERIA MERCADO

MERLY MARTINEZ OSORIO
Secretaria general

CONFORMACIÓN DEL CONCEJO MUNICIPAL
PLENARIA DEL CONCEJO

- KEBIN ANDRES ZUBIRIA PEROZA -PARTIDO CENTRO DEMOCRATICO
- SADDAM ALBERTO FERIA MERCADO -PARTIDO CENTRO DEMOCRATICO
- ERIS HERNANDEZ JULIO -PARTIDO CAMBIO RADICAL
- PEDRO ELIECER REVUELTAS -PARTIDO ASI
- JOHN JAIRO MARTÍNEZ -PARTIDO ASI
- LUZ HELENA URANGO -PARTIDO ASI
- JAVIER SEGUNDO NUÑEZ RINCO -PARTIDO ASI
- CARLOS JOSE MORALES CASTELLANOS -PARTIDO CONSERVADOR
- MARTA ISABEL RIOS REVUELTA -PARTIDO LIBERAL
- ALICIA SOFIA MUENTES DIAZ -PARTIDO LIBERAL
- SORAIDA MARQUEZ LOPEZ -PARTIDO DE LA U

Coveñas Enero de 2023

Contenido

PRESENTACIÓN

La seguridad y privacidad de la Información como habilitador transversal de la Política de Gobierno Digital se desarrolla a través del Modelo de Seguridad y Privacidad de la Información -MSPI, orientando la gestión e implementación del Sistema de Gestión de Seguridad de la Información – SGSI, con el fin de incorporar la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información del Concejo Municipal de Coveñas, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.
El Plan de Seguridad Informática es importante en la corporación ante la posible pérdida, destrucción, robo y otras amenazas, teniendo en cuenta que cualquier Sistema de Redes de Computadoras (ordenadores, periféricos y accesorios) están expuestos a riesgo y puede ser fuente de problemas.

El Hardware y Software están expuestos a diversos Factores de Riesgo Humano y Físicos. Estos problemas menores y mayores sirven para retroalimentar nuestros procedimientos y planes de seguridad en la información. Pueden originarse pérdidas catastróficas a partir de fallos de componentes críticos (el disco duro), bien por grandes desastres (incendios, terremotos, sabotaje) o por fallas técnicas (errores humanos, virus informáticos, entre otros) que producen daño físico irreparable.

Por lo anterior es importante contar con un Plan de Seguridad y privacidad de la información basado en el Modelo de seguridad y Privacidad de la Información – MSPI, que hace parte integral de la Estrategia de Gobierno digital de tal forma que ayude a la Entidad a recobrar rápidamente el control y capacidades para procesar la información y restablecer la marcha normal de la corporación

Teniendo en cuenta lo anterior, se formula el presente Plan, en cumplimiento de la normativa aplicable vigente, y en particular, como parte de los planes institucionales establecidos en el Decreto 612 de 2018.

1. INTRODUCCION

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la Corporación en caso de materialización, adicional se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos trazados en el Entorno TIC para el Desarrollo Digital, ciudadanos y corporación empoderada del Entorno Digital. 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 del negocio. 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 el documento con el diagnóstico del sistema actual de la el Concejo Municipal de Coveñas, donde se conoce la situación actual de la organización 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.

2. OBJETIVO GENERAL

Garantizar la confidencialidad, integridad y disponibilidad de la información, mediante la formulación e implementación de actividades y controles de seguridad alineadas con las Política de Gobierno Digital y la Política de Seguridad Digital, de acuerdo con el alcance definido por el Concejo Municipal de Coveñas

1.1 OBJETIVOS ESPECIFICOS

- Identificar los riesgos asociados a los procesos que hacen parte del alcance del Modelo Integrado de Planeación y Gestión y Gobierno Digital.
- Identificar las principales amenazas que afectan los activos de información del Concejo Municipal de Coveñas
- Proteger los activos de información del Concejo Municipal de Coveñas, con base en los criterios de confidencialidad, integridad y disponibilidad.
- 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.
- Administrar los riesgos de seguridad de la información para mantenerlos en niveles aceptables.
- Sensibilizar y capacitar a los servidores públicos, funcionarios, contratistas y partes interesadas acerca del Sistema de Gestión de Seguridad y Privacidad de la Información, de gobierno digital, fortaleciendo el nivel de conciencia de los mismos, en cuanto a la necesidad de salvaguardar los activos de información institucionales.
- Monitorear el cumplimiento de los requisitos de seguridad de la información, mediante el uso de herramientas de diagnóstico, revisiones por parte de la Alta Dirección y auditorías internas planificadas a intervalos regulares.
- Implementar acciones correctivas y de mejora para el Sistema de Gestión del Modelo de Seguridad y Privacidad de la Información.

- Evaluar y comparar el nivel de riesgo actual con el impacto generado después de implementar el plan de gestión de seguridad de la información.

3. ALCANCE

El presente Plan comprende la descripción y programación de las actividades a realizar por el Concejo Municipal de Coveñas durante la vigencia 2023, como parte de la Implementación del Sistema de Gestión de la Seguridad de la Información (SGSI), de acuerdo con el Modelo de Seguridad y Privacidad de la Información - MSPI emitido por el Ministerio de las Tecnologías de la Información y las Comunicaciones – MINTIC Este Plan de Seguridad y Privacidad de la Información y su política, son aplicables a todos los funcionarios del Concejo Municipal de Coveñas, a sus recursos, procesos y procedimientos tanto internos como externos, así mismo al personal vinculado y terceras partes, que usen activos de información que sean propiedad de la corporación.

4. DEFINICIONES

Activo: En cuanto a la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

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.

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo.

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.

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.

Confidencialidad: La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

Contratistas: Entenderemos por contratista aquella persona natural o jurídica que ha celebrado un contrato de prestación de servicios o productos con una entidad.

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.

Disponibilidad: Acceso y utilización de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

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.

Guía: documento técnico que describe el conjunto de normas a seguir en los trabajos relacionados con los sistemas de información.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Norma: Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.

Parte interesada: (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

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.

Política del SGSI: Manifestación expresa de apoyo y compromiso de la alta dirección con respecto a la seguridad de la información.

Política: Es la orientación o directriz que debe ser divulgada, entendida y acatada por todos los miembros de la entidad.

Privacidad de datos: La privacidad de datos, también llamada protección de datos es el aspecto de la tecnología de la información (TI) que se ocupa de la capacidad que una organización o individuo tiene para determinar qué datos en un sistema informático pueden ser compartidos con terceros

Procedimiento: Los procedimientos constituyen la descripción detallada de la manera como se implanta una política.

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.
Rol: Papel, función que alguien o algo desempeña.

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

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

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

5. POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

De acuerdo con lo estipulado en el numeral 2.1.3 del Manual de Gobierno Digital del MINTIC, el Plan de Seguridad y Privacidad de la Información debe establecer los detalles de cómo se realizará la implementación de la seguridad de la información en cada uno de los procesos de la entidad, estipulando directrices, tiempo y responsables para lograr un adecuado proceso de gestión, administración, evaluación y resultados del plan desarrollado El concejo municipal de Coveñas ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades de la Entidad, y a los requerimientos regulatorios. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores o terceros.

Esta actualización de la política de seguridad y privacidad de la información se basa en la existe mediante resolución No. 96 DE 2016, que se derogara cuando sea aprobada.

5.1. OPERACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

Su operativización busca establecer, implementar, monitorear, revisar, mantener y mejorar el sistema en El concejo municipal de Coveñas, reportando su estado de avance, de manera que fomente la consulta y cooperación con organismos especializados para la obtención de asesoría en dicha materia para garantizar la aplicación de medidas de seguridad adecuadas, en los accesos a la información de la Entidad.

5.2. POLÍTICA INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN

El concejo municipal de Coveñas, en el marco de sus funciones, se compromete a proteger y asegurar la información tanto física como digital, a través de acciones, estrategias y recursos necesarios, con el fin de cumplir con los requisitos legales y de la entidad, en pro del fortalecimiento y mejora del sistema de gestión de seguridad de la información y sus objetivos. Preservando los

activos de información y tecnológicos del Concejo, para asegurar la confidencialidad, integridad y disponibilidad de la información; con el fin de apoyar el cumplimiento de la gestión de la entidad y promover la confianza en la ciudadanía.

5.3 IDENTIFICACIÓN DEL RIESGO

Teniendo en cuenta que el riesgo de seguridad de información es la 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), se procede, posterior a la identificación de los activos de información a la identificación de los riesgos inherentes a la seguridad de información, clasificándolos, pérdida de la información, pérdida de la integridad y pérdida de la disponibilidad, así mismo se identificaron las amenazas y vulnerabilidades, como se detalla a continuación:

IDENTIFICACIÓN DEL RIESGO	RIESGO	ACTIVO	TIPO	AMENAZA	VULNERABILIDAD
Perdida de confidencialidad, integridad y disponibilidad	Posibilidad de daño o pérdida de Base de Datos por baja seguridad, eventos de desconexiones no controladas, Discos duros con demasiado uso	Base de Datos de	Información	Daño, robo o pérdida de la Base de Datos	seguridad conlleva a acceso no autorizado
					Desconexiones no controladas
					Discos duros con demasiado uso, apagones de forma imprevista, golpes al equipo
Perdida de integridad y disponibilidad	Posibilidad de pérdida o daño de la información multimedia generada en las sesiones por causa de Discos duros con demasiado uso, apagones de	Posibilidad de pérdida o daño de la información multimedia generada en las sesiones por causa de Discos duros con demasiado	Posibilidad de pérdida o daño de la información multimedia generada en las sesiones por causa de Discos duros con demasiado	Posibilidad de pérdida o daño de la información multimedia generada en las sesiones por causa de Discos duros con demasiado	Posibilidad de pérdida o daño de la información multimedia generada en las sesiones por causa de Discos duros con demasiado uso, apagones de forma imprevista, golpes al equipo

	forma imprevista, golpes al equipo	uso, apagones de forma imprevista, golpes al equipo	uso, apagones de forma imprevista, golpes al equipo	uso, apagones de forma imprevista, golpes al equipo	

6. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para llevar a cabo la implementación del Plan de Seguridad y Privacidad de la Información en el Concejo Municipal de Coveñas, toma referencia Modelo de Seguridad y Privacidad de la Información en su versión 3.0.2 publicado por el Ministerio de Tecnologías de la Información y las Comunicaciones.

En este punto es pertinente presentar el ciclo de funcionamiento del modelo de operación, a través de la descripción detallada de cada una de las cinco (5) fases que lo comprenden. Estas, contienen objetivos, metas y herramientas (guías) que permiten que la seguridad y privacidad de la información sea un sistema de gestión sostenible dentro del Concejo Municipal de Coveñas

La seguridad y privacidad de la información, como componente transversal a la Estrategia de Gobierno digital, permite alinearse al componente de TIC para la Gestión al aportar en el uso estratégico de las tecnologías de la información con la formulación e implementación del modelo de seguridad enfocado a preservar la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento de la misión y los objetivos estratégicos del Concejo Municipal de Coveñas.

La Seguridad y Privacidad de la Información se alinea al componente de TIC para Servicios apoyando el tratamiento de la información utilizada en los trámites y servicios que ofrece la Corporación, observando en todo momento las normas sobre protección de datos personales, así como otros derechos garantizados por la Ley que exceptúa el acceso público a determinada información.

El componente de TIC para Gobierno Abierto se alinea con el componente de Seguridad y Privacidad de la Información que permite la construcción de un estado más transparente, colaborativo y participativo al garantizar que la información que se provee tenga controles de seguridad y privacidad de tal

forma que los ejercicios de interacción de información con el ciudadano, otras entidades y la empresa privada sean confiables.

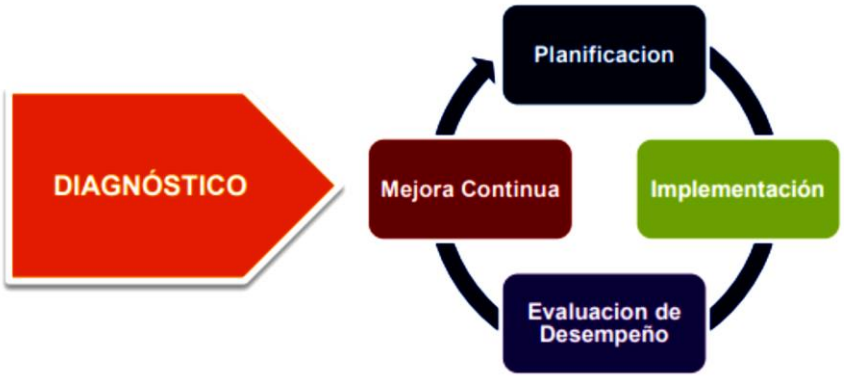
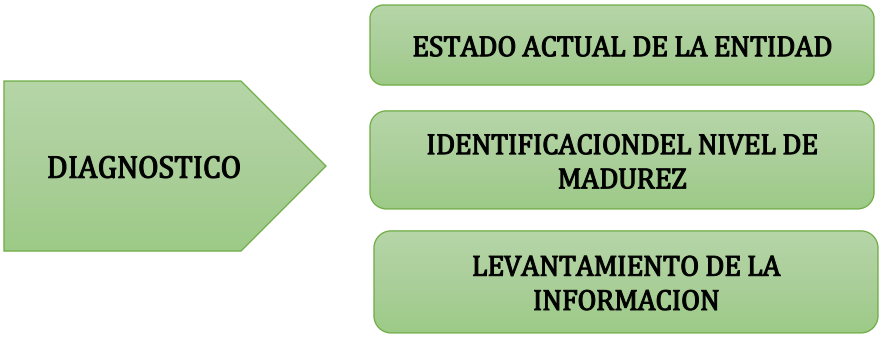


Figura 1. Ciclo de operación del modelo de seguridad y privacidad de la información

6.1. FASE DE DIAGNÓSTICO - ETAPAS PREVIAS A LA IMPLEMENTACIÓN

En esta fase se pretende identificar el estado actual del Concejo Municipal de Coveñas con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.



En la fase de diagnóstico se pretende alcanzar las siguientes metas:

• Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior del Concejo Municipal de Coveñas.

• Determinar el nivel de madurez de los controles de seguridad de la información.

• Identificar el avance de la implementación del ciclo de operación al interior de la entidad.

• Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.

• Identificación del uso de buenas prácticas en ciberseguridad. Para ello se recomienda utilizar los siguientes instrumentos:

• Herramienta de diagnóstico.

• Instructivo para el diligenciamiento de la herramienta.

• Guía No 1 - Metodología de Pruebas de Efectividad.

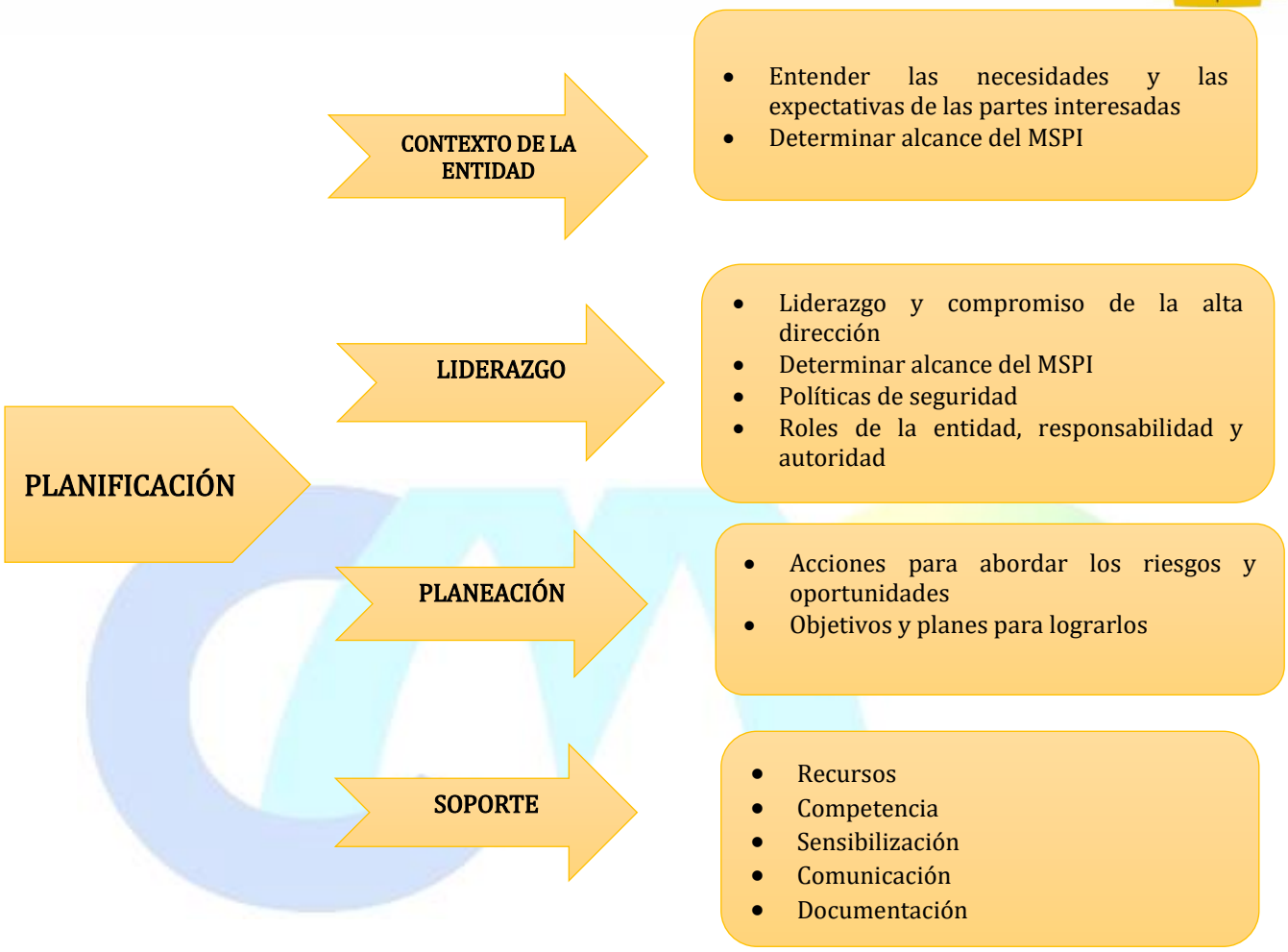
Para realizar dicha fase el Concejo Municipal de Coveñas debe efectuar la recolección de la información con la ayuda de la herramienta de diagnóstico y la metodología de pruebas de efectividad. Una vez se tenga el resultado del diagnóstico inicial y se haya determinado el nivel de madurez de la entidad se procede al desarrollo de la fase de Planificación. Los resultados asociados a la fase de Diagnostico previas

6.3. FASE DE PLANIFICACIÓN

Para el desarrollo de esta fase la entidad debe utilizar los resultados de la etapa anterior y proceder a elaborar el Plan de Seguridad y Privacidad de la Información alineado con el objetivo misional de la entidad, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo.

El alcance del MSPI permite a la Corporación definir los límites sobre los cuales se implementará la seguridad y privacidad. Este enfoque es por procesos y debe extenderse a todo el Concejo Municipal de Coveñas.

Para desarrollar el alcance y los límites del Modelo se deben tener en cuenta las siguientes recomendaciones: Procesos que impactan directamente la consecución de objetivos misionales, procesos, servicios, sistemas de información, ubicaciones físicas, terceros relacionados, e interrelaciones del Modelo con otros procesos.



A continuación se explica de manera general los productos esperados en la fase de planificación del Modelo de Seguridad y Privacidad de la Información:

6.3.1. Política de seguridad y privacidad de la información.

Actualizar la Política de Seguridad y Privacidad de la información contenida en un documento de alto nivel que incluye la voluntad de la Alta Dirección del Concejo Municipal de Coveñas para apoyar la implementación del Modelo de Seguridad y Privacidad de la Información la cual será divulgada al interior del Concejo.

6.3.2. Políticas Operativas de Seguridad y Privacidad de la Información.

Desarrollar un Manual de políticas a nivel operativo, donde se describe los objetivos, alcances y el nivel de cumplimiento, que garanticen el adecuado uso de los Activos de información al interior del Concejo Municipal de Coveñas; definiendo las responsabilidades generales y específicas para la gestión de la seguridad de la información.

6.3.3. Procedimientos de Seguridad de la Información.

Desarrollar y formalizar procedimientos que permitan gestionar la seguridad de la información. Para desarrollar esta actividad, la Guía No 3 del MSPI- describe los procedimientos mínimos que se deberían tener en cuenta para la gestión de la seguridad al interior del Concejo Municipal de Coveñas.

6.3.4. Roles y Responsabilidades de Seguridad y Privacidad de la Información.

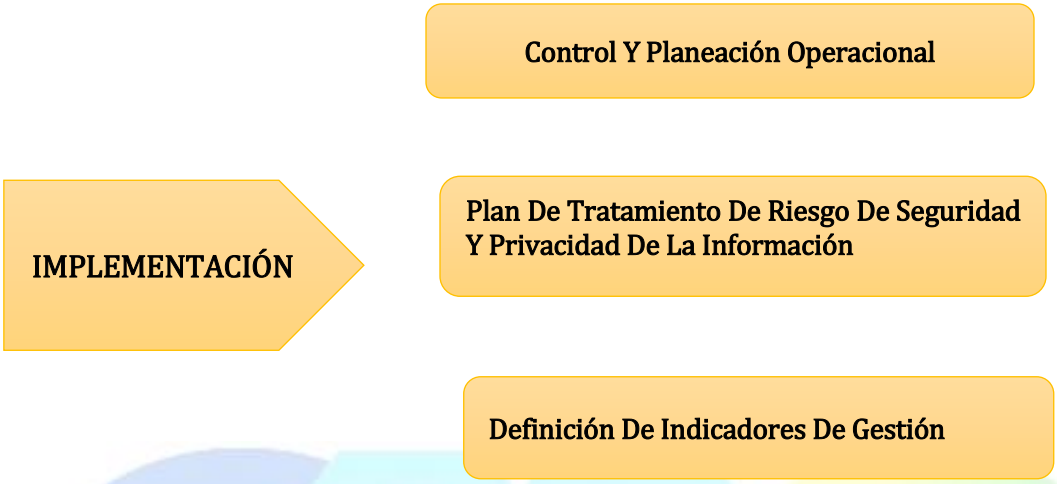
Concejo Municipal de Coveñas debe definirá mediante un acto administrativo (Resolución, circular, decreto, entre otros) los roles y las responsabilidades de seguridad de la información en los diferentes niveles (Directivo, De procesos y Operativos) que permitan la correcta toma de decisiones y una adecuada gestión que permita el cumplimiento de los objetivos en el Concejo.

6.3.5. Inventario de activos de información.

Desarrollar una metodología de gestión de activos que le permita generar un inventario de activos de información exacto, actualizado y consistente, que a su vez permita definir la criticidad de los activos de información, sus propietarios, custodios y usuarios.

6.4. FASE DE IMPLEMENTACIÓN

Esta fase le permitirá al Concejo Municipal de Coveñas, llevar acabo la implementación de la planificación realizada en la fase anterior del MSPI.



A continuación, se explica de manera general los productos esperados en la fase de Implementación del Modelo de Seguridad y Privacidad de la Información en el Concejo Municipal de Coveñas.

6.4.1. Implementación del plan de tratamiento de riesgos.

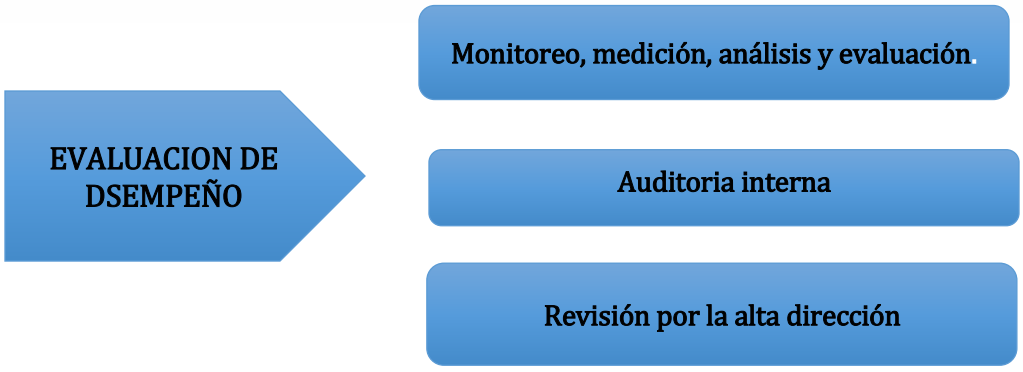
Desarrollar Informes de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso. Es decir, del estado de implementación y efectividad de los controles escogidos para la mitigación de cada riesgo identificado en los activos de información.

6.4.2. Indicadores De Gestión.

Definir indicadores que le permitan medir la efectividad, la eficiencia y la eficacia en la gestión y las acciones implementadas en seguridad de la información.

6.5. FASE DE EVALUACIÓN DE DESEMPEÑO

El proceso de seguimiento y monitoreo del MSPI se hace con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas



7. PLAN DE REVISIÓN Y SEGUIMIENTO A LA IMPLEMENTACIÓN DEL MSPI.

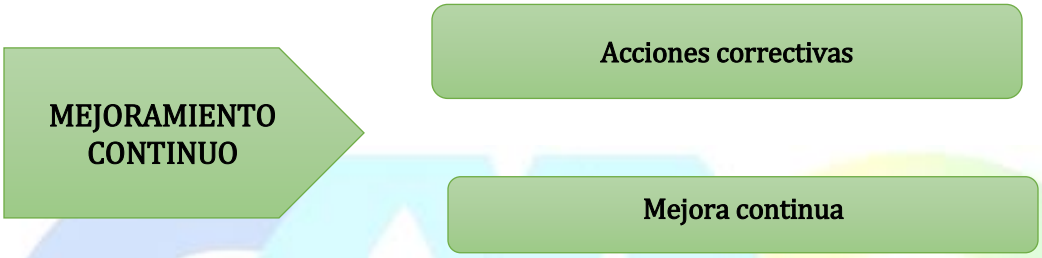
En esta actividad el Concejo Municipal de Coveñas debe crear un plan que contemple las siguientes actividades:

- Revisión de la efectividad de los controles establecidos y su apoyo al cumplimiento de los objetivos de seguridad.
- Revisión de la evaluación de los niveles de riesgo y riesgo residual después de la aplicación de controles y medidas administrativas.
- Seguimiento a la programación y ejecución de las actividades de autorías internas y externas del MSPI.
- Seguimiento al alcance y a la implementación del MSPI.
- Seguimiento a los registros de acciones y eventos / incidentes que podrían tener impacto en la eficacia o desempeño de la seguridad de la información al interior de la entidad.
- Medición de los indicadores de gestión del MSPI
- Revisiones de acciones o planes de mejora (solo aplica en la segunda revisión del MSPI)

Este plan deberá permitir la consolidación de indicadores periódicamente y su evaluación frente a las metas esperadas; deben ser medibles permitiendo analizar causas de desviación y su impacto en el cumplimiento de las metas y objetivos del MSPI.

8. FASE DE MEJORA CONTINUA

En esta fase el Concejo Municipal de Envigado debe consolidar los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas



En esta fase es importante que la Corporación defina y ejecute el plan de mejora continua con base en los resultados de la fase de evaluación del desempeño. Este plan incluye:

- Resultados de la ejecución del plan de seguimiento, evaluación y análisis para el MSPI.
- Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI.

Utilizando los insumos anteriores, la Corporación puede efectuar los ajustes a los entregables, controles y procedimientos dentro del MSPI. Estos insumos tendrán como resultado un plan de mejoramiento y un plan de comunicaciones de mejora continua, revisados y aprobados por la Alta Dirección de la entidad. La revisión por la Alta Dirección hace referencia a las decisiones, cambios, prioridades etc. tomadas en sus comités y que impacten el MSPI.

A. Protección de la información y de los bienes informáticos

El secretario del Concejo deberá reportar de forma inmediata a la Mesa Directiva cuando detecte riesgo alguno real o potencial sobre equipos de cómputo de comunicaciones, tal como caídas de agua, choques eléctricos, caídas o golpes o peligro de incendio.

El funcionario tiene la obligación de proteger las unidades de almacenamiento que se encuentre bajo su responsabilidad, aun cuando no se utilicen y contengan información confidencial o importante.

Es responsabilidad del usuario o funcionario evitar en todo momento la fuga de información de la entidad que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

B. Controles de acceso físico

Cualquier persona que tenga acceso a las instalaciones del Concejo Municipal de Coveñas, deberá registrar al momento de su entrada, el equipo de cómputo y equipos audiovisuales en el área de recepción o la secretaria del concejo. Los computadores de escritorio, portátiles y cualquier activo de tecnología de información podrán ser retirados de las instalaciones del Concejo Municipal de Coveñas únicamente con la autorización de salida del área de recursos físicos, siguiendo el debido proceso.

C. Protección y ubicación de los equipos

Los usuarios de los equipos tendrán en cuenta para la protección de los equipos lo siguiente:

- Los usuarios no deben mover o reubicar los equipos de cómputos o de comunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos, sin autorización de la mesa directiva.

- El equipo de cómputo asignado, deberá ser de uso exclusivo de las funciones de los funcionarios o servidores del Concejo Municipal de Coveñas.

- Es responsabilidad de los usuarios almacenar su información únicamente en la partición del disco duro diferente a la destinada para archivos de programa y sistemas operativos, o unidades de almacenamiento externas.

- Mientras se opere el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos.

- Se debe evitar colocar objetos encima del equipo de cómputo u obstruir las salidas de ventilación del monitor o de la CPU.

- Se debe mantener el equipo de cómputo en un lugar limpio sin humedad.

- El usuario debe asegurarse que los cables de conexión no sean pisados al colocar otros objetos encima a contra ellos en caso de que no se cumpla solicitar la reubicación de los cables al proceso de TIC.

- Se prohíbe rigurosamente al usuario o funcionario distinto al personal de la oficina de sistemas abrir o destapar los equipos de cómputo.

D. Mantenimiento de equipos:

Únicamente el personal autorizado por el Presidente del Concejo podrá llevar a cabo los servicios y reparaciones al equipo informático.

Los usuarios deberán asegurarse de respaldar en copias de seguridad la información que consideren relevante cuando el equipo sea enviado a reparación, y borrar aquella información sensible que se encuentre en el equipo, previniendo así la perdida involuntaria de información derivada del proceso de reparación.

El mantenimiento preventivo de los equipos de cómputo de la corporación (Planta telefónica, servidores, computadores de escritorio, computadores portátiles, computadores todo en uno, impresoras, escáner, se hará 1 vez al año, según el cronograma.

E. Pérdida de equipo:

El funcionario que tenga bajo su responsabilidad o asignado algún equipo de cómputo, será responsable de su uso y custodia; en consecuencia, responder por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravió o pérdida del mismo.

El servidor o funcionario deberá dar aviso inmediato a la mesa directiva de la desaparición, robo o extravío de equipos de cómputo, periféricos o accesorios

bajo su responsabilidad, a su vez en caso de robo deberá dar entrega del oficio de denuncia por parte de la Policía Nacional.

9. IDENTIFICACION DE PROCESOS Y SERVICIOS

Principales procesos de Software identificados en el concejo.

Apolo Ultra

Es uno del poco software desarrollado bajo web. Esta versión le permite seguir funcionando en una red local. Pero, si la entidad quiere permitir tener acceso a sus funcionarios de forma remota, el aplicativo se puede instalar en el hosting que tenga la entidad, permitiendo con esto que se pueda tener acceso desde un servidor web (Internet).

Los módulos adquiridos por el software Apolo Ultra son:

- Contabilidad General.
- Presupuesto.
- Compromisos.
- Recurso Físico.
- Recurso Humano (Nómina).
- Cuentas Por Cobrar.
- Tesorería.
- Secretaría.
- Rendición de Cuentas.

10. RESPALDO DE LA INFORMACION

Las copias de seguridad que están disponibles en la Corporación son las siguientes:

a) **DISCOS DUROS:** Son aquellos dispositivos de almacenamiento asignados al Funcionario o servidor público, este Backus lo hará manualmente el usuario cada vez que crea necesario y reposara bajo su custodia, allí el usuario almacenara la información que el considere vital. Se destina l disco duro en el área de sistemas, para que diariamente haga una copia desde el servidor donde se almacenan las carpetas compartidas, este disco duro estará bajo la custodia Únicamente del Presidente del Concejo.

b) **CARPETAS COMPARTIDAS:** Es el espacio que se destina de Correo Electrónico o Espacio en la nube, donde se crea una carpeta por cada usuario con el mismo nombre de usuario de red y solamente este usuario tendrá todos los permisos para guardar directamente la información que considere necesaria.

Para realizar un análisis de todos los elementos de riesgos a los cuales están expuesto los equipos informáticos y la información procesada del Concejo Municipal de Coveñas, se iniciara describiendo los activos que se pueden encontrar dentro de las tecnologías de información y la comunicación de La Corporación:

11. ACTIVOS SUSCEPTIBLES DE DAÑO.

El Personal, Hardware, Software, Periféricos, Datos, información, Documentación Física y magnética, Suministro de energía eléctrica y Suministro de telecomunicaciones

11.1.1. Posibles daños

- Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones.
- Imposibilidad de acceso a los recursos informáticos, sean estos por cambios involuntarios o intencionales, tales coma cambios de claves de acceso, eliminación o borrado físico/lógico de información.
- Divulgación de información a instancias fuera de la institución y que afecte su patrimonio estratégico, sea mediante Robo o Infidencia.

11.1.2 Fuentes de daño

- Acceso no autorizado.
- Ruptura de las claves de acceso al sistema informático.
- Desastres Naturales (Movimientos telúricos, Inundaciones, Fallas en los equipos de soporte causadas por el ambiente, la red de energía eléctrica o el no acondicionamiento atmosférico necesario).
- Fallas de Personal (Enfermedad, Accidentes, Renuncias, Abandono de su puesto de trabajo).

•Fallas de Hardware (Falla en los Servidores o Falla en el hardware de Red Switches,
cableado de la Red, Router, FireWall).
•Falla en el servicio del proveedor de Internet.

11.1. IDENTIFICACION DEL RIESGO

RIESGO:
Perdida de la confidencialidad e integridad de la información por faltas en la seguridad informática en beneficio de un particular.

CAUSAS:

- Generación de información confusa a errada sobre los temas de la Corporación.
- Falta de unidad de criterio sobre el manejo de los temas.
- Incumplimiento en la entrega de los productos finales.

RIESGO:
Perdida de información.

CAUSAS:

- Falta de capacitación para implementar actualizaciones normativas y procedimentales.
- Cambio de la normatividad relacionada con TIC que impliquen modificación de las actividades.
- Falencias en la generación de copias de seguridad de los equipos servidores.
- Falencias en los controles de seguridad informática.
- Fallas en la infraestructura tecnológica.
-

Una vez realizada la identificación de riesgos, se tiene que es posible la presencia de:
• Incendios.
•Robo común de equipos y archivos.
•Falla en los equipos.
•Virus informático.
•Fenómenos naturales.

•Accesos no autorizados.
•Ausencia del personal de sistemas.
•Bajas Eléctrica

11.2.1. Minimización del riesgo

Teniendo en cuenta, corresponde al presente Plan de Seguridad Informática del Concejo Municipal de Coveñas minimizar estos índices con medidas preventivas y correctivas sobre los riesgos más relevantes:

Es de tener en cuenta que en lo que respecta a Fenómenos naturales, as Lluvias fuertes producen mayores estragos, originando filtraciones de agua en las estructuras físicas, produciendo cortes de luz, cortos circuitos que podrían desencadenar en incendios; Factores de impacto de riesgo a las instalaciones de equipos, redes y otros.

FALLA EN LOS EQUIPOS

GRADO DE IMPACTO: MODERADO SITUACION ACTUAL	**ACCION PREVENTIVA**
La falla en los equipos pocas veces se debe a falta de mantenimiento y limpieza.	Realizar mantenimiento preventivo de equipos de cómputo anualmente, según cronograma.
El daño de equipos por fallas en la energía eléctrica, algunos equipos no cuentan con dispositivos que amplíen tiempo para apagar correctamente el equipo.	Los equipos de escritorio cuentan con Estabilizador, algunos con UPS, y el cuarto de telecomunicaciones cuenta con una UPS principal.

EQUIVOCACIONES EN EL MANEJO DEL SISTEMA

GRADO DE IMPACTO: MODERADO SITUACION ACTUAL	**ACCION PREVENTIVA**
Equivocaciones que se producen de forma involuntaria, con respecto at manejo de información, software y equipos.	Realizar capacitaciones en el ambiente de trabajo presentando las políticas

	informáticas establecidas para el manejo de sistemas.
Algunas veces el usuario que tiene conocimiento en informática intenta navegar por sistemas que no están dentro de sus funciones y/o competencia.	La Mesa Directiva o el administrador de la red debe asignar permisos y privilegios a cada usuario de acuerdo a sus funciones y/o competencias.
Se presentan equivocaciones en el manejo de información debido a que no conocen las políticas de informática claras y precisas.	Capacitar en políticas de informática y seguridad a los funcionarios at igual que cualquier modificación a las mismas.

ACCION DE VIRUS INFORMATICO

GRADO DE IMPACTO: MODERADO SITUACION ACTUAL	**ACCION PREVENTIVA**
Se cuenta con un software antivirus kaspesky Internet Security para la corporación, pero su actualización no se realiza de forma inmediata a su expiración.	Se debe evitar que las licencias de antivirus expiren, se requiere renovación con Anterioridad del nuevo antivirus.
Únicamente la persona que se contrate para tal fin es la encargada de realizar la instalación de software en cada uno de los equipos de acuerdo a su necesidad.	Se cumple.
Los antivirus a veces no se actualizan periódicamente en cada equipo.	Informar la política informática de Actualización de antivirus a cada funcionario y su responsabilidad frente a esto.

ACCESOS NO AUTORIZADOS

GRADO DE IMPACTO: MODERADO SITUACION ACTUAL	**ACCION PREVENTIVA**
Se controla el acceso al sistema mediante la definici6n de un administrador con su respectiva clave	Se cumple

Se cancelan los usuarios del personal que se retira de la entidad de forma inmediata, recurriendo en algunos casos a utilizar la contraseña del funcionario ausente.	Se cumple

12. PLAN DE RECUPERACION Y RESPALDO DE LA INFORMACION

Actividades previas al desastre

Se considera las actividades de resguardo de la información, en busca de un proceso de recuperación con el menor costo posible para la Entidad. Se establece los procedimientos relativos a: Sistemas e Información, Equipos de Computo, Obtención y almacenamiento de los Respaldos de Información (BACKUPS).

a) Sistemas de Información

La Entidad cuenta con una relación de los Sistemas de Información de software de datos, para respaldarla con backups.

b) Equipos de Cómputo

Se debe tener en cuenta el inventario de Hardware, impresoras, scanner, circuito cerrado de televisión y otros, detallando su ubicación (software que usa, ubicación y nivel de use institucional).

Se debe emplear los siguientes criterios sobre identificación y protección de equipos:

• Pólizas de seguros comerciales, como parte de la protección de los activos institucionales y considerando una restitución por equipos de mayor potencia, teniendo en cuenta la depreciación tecnológica.

• Socialización o etiquetamiento de las computadoras de acuerdo a la importancia de su contenido y valor de sus componentes, para dar prioridad en caso de evacuación o buscar información importante, en este caso aplica los servidores de aplicaciones y carpetas compartidas.

• Mantenimiento actualizado del inventario de los equipos de cómputo requerido como mínima para el funcionamiento permanente de cada sistema en la corporación.

13.SOLO ACTIVIDADES PREVIAS AL DESASTRE Y EL RESTO

13.1.1 CONTROLES PARA LA GENERACION Y RESTAURACION DE COPIAS DE RESPALDO (BACKUPS)

En el procedimiento de generación y restauración de copias de respaldo para salvaguardar la información crítica de los procesos significativos de la entidad. Se deberán considerar como mínimo los siguientes aspectos:

• Establecer como medida de seguridad informática la necesidad de realizar copias de respaldo backups periódicamente en los equipos de cómputo administrativos y servidores, estas copias de seguridad deben realizarse al menos una vez a la semana.

- Cada funcionario es responsable directo de la generación de los backups o copias de respaldo, asegurándose de validar la copia.

• Almacenamiento interno o externa de las copias de respaldo, o verificar si se cuenta con custodia para ello.

- Se utilizará el programa WINRAR en la opción añadir para comprimir el listado de archivos a carpetas a respaldar.

14.RECOMENDACIONES GENERALES

14.1. RELACIONADAS CON LOS EQUIPOS DE CÓMPUTO

- Poner especial atención a las actualizaciones del navegador web, el sistema operativo como Windows es propenso a fallos, riesgo que puede ser aprovechado por delincuentes informáticos, frecuentemente se liberan actualizaciones que solucionan dichos fallos.

- Estar al día con las actualizaciones, así coma aplicar los parches de seguridad recomendados por los fabricantes, nos ayudara a prevenir la posible intrusión de hackers y la aparición de nuevos virus.

- Los usuarios no deberán alterar o eliminar las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas par el proceso de Gestión de TIC en antivirus, Outlook, office, navegadores y otros programas.

- Tener el antivirus actualizado con frecuencia. Escanear con el antivirus todos los dispositivos de almacenamiento de datos que utilice y todos los archivos nuevos, especialmente aquellos archivos descargados par internet.

- Estar pendiente de la fecha de caducidad de la licencia con el fin de renovarla inmediatamente tan pronto esta se cumpla.

- Es recomendable tener instalado en los equipos algún tipo de software anti-spyware para evitar que se introduzcan en el equipo programas espías destinados a recopilar información confidencial sobre el usuario.

- Para prevenir infecciones por virus informático, los usuarios del Concejo Municipal de Coveñas no deben hacer use de software que no haya sido proporcionado y validado par el proceso Gestión de TIC.

- Los usuarios del Concejo Municipal de Coveñas deben verificar que la información y los medios de almacenamiento, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado antes de ejecutarse.

- Ningún usuario, funcionario, empleado o personal externo, podrá descargar software, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización de la oficina de sistemas.

14.2. RELACIONADOS CON LA NAVEGACION EN INTERNET Y LA UTILIZACION DE CORREO ELECTRONICO:

- Navegue por páginas web seguras y de confianza, para identificarlas verifique si dichas páginas tienen algún sello o certificado que garanticen su calidad y fiabilidad, extreme la precaución si va a facilitar información

confidencial a través de internet. En estos casos reconocerá como paginas seguras aquellas que cumplan dos requisitos:

a) Empezar por https:// en lugar de http.
b) En la barra del navegador deben aparecer el icono de candado cerrado. A través de este icono se puede acceder a un certificado que confirma la autenticidad en la pagina.

- Utilizar contraseñas seguras, es decir aquellas compuestas par ocho caracteres, coma mínimo y que combinen letras, números y símbolos. Es conveniente además que modifique sus contraseñas con frecuencia. En especial, le recomendamos que cambie la clave de su cuenta de correo si accede con frecuencia a este desde equipos públicos.

- Sea cuidadoso al utilizar programas de acceso remoto. A través de internet y mediante estos programas (Teamviewer), es posible acceder a un ordenador, desde otro situado a kilómetros de distancia. Aunque esto supone una gran ventaja, puede poner en peligro la seguridad de su sistema.

- Ponga especial atención en el tratamiento de su correo electrónico, ya que este se ha convertido en una de las formas más utilizadas para introducir código malicioso, llevar a cabo estafas, introducir virus, etc. Por' ello le recomendamos que:

a) No abra mensajes de correo de remitentes desconocidos.
b) Desconfié de aquellos e-mails en los que entidades bancarias, compañías de subastas o sitios de venta online, le solicitan contraseñas, información confidencial, etc.
c) No propague aquellos mensajes de correo con contenido dudoso y que le pidgin ser reenviados a todos sus contactos. Este tipo de mensajes, conocidos coma hoaxes, pretenden avisar de la aparición de nuevos virus, transmitir leyendas urbanas o mensajes solidarios, difundir noticias impactantes, etc. Estas cadenas de a-mails se suelen crear can el objetivo de captar las direcciones de correo de usuarios a los que posteriormente se les enviaran mensajes con virus, phishing o todo tipo de spam.

d) Utilice algún tipo de software Anti-Spam para proteger su cuenta de correo de mensajes no deseados.

En general, es fundamental estar al día de la aparición de nuevas técnicas que amenazan la seguridad de su equipo informático, para tratar de evitarlas a de aplicar la solución más efectiva posible.

14.3. RELACIONADA CON EL USO DE DISPOSITIVOS EXTRAIBLES

• El funcionario o usuario que tenga asignados estos tipos de dispositivos serán responsable de la buena usa de ellos.

• La persona encargada de administrar cada equipo deberá velar por el uso adecuado de dispositivos de almacenamiento externo, como Pen Drives, Discos portátiles, Unidades de Cd y DVD Externos, para el manejo y traslado de información o realización de copias de seguridad o Backups.

• Cada vez que se inserte un dispositivo externo a la red de la corporación, deberá ser analizado con el software del antivirus.

14.4. RELACIONADA CON CONEXIONES REMOTAS

En el Concejo Municipal de Coveñas solo están disponibles una forma de conexión remota:

10.4.1 CONEXION A ESCRITORIO REMOTO (TEAMVIEWER)

Con Conexión a Escritorio remoto, puedes conectarse a un equipo que ejecute Windows desde otro equipo que ejecute Windows que esté conectado a la misma red o a Internet. Par ejemplo, puedes usar todos los programas, archivos y recursos de red del equipo del trabajo desde el equipo de tu casa, como si estuvieras sentado delante del equipo del trabajo.

Escritorio remoto es una utilidad de Windows que permite usar y manejar completamente una conmutadora desde otra ubicación, ya sea distante o cercana, siempre que exista algún tipo de conexión entre ellas. Antiguamente fue Llamada Terminal Services, hoy forma parte del sistema operativo.

La conexión puede ser de cualquiera de las siguientes formas:

•Un cable de red

•Una conexión inalámbrica o Wi-Fi
•Internet

Escritorio remoto nos muestra en el monitor el escritorio de la computadora conectada, ya sea en una ventana con las dimensiones reducidas, las medidas originales de equipo, o a pantalla completa, esto permite sentirnos exactamente igual que si estuviéramos sentados frente a dicho equipo.

Mediante escritorio remoto se pueden usar todos los programas, aplicaciones, archivos y recursos del equipo remoto.

Utilizar escritorio remoto puede ser muy útil en varias situaciones, puede facilitarnos tareas que de otra forma solo puedan ser posibles, accediendo directamente al equipo remoto, algunos ejemplos prácticos que permite su use son los siguientes:

• Utilizar una PC de escritorio desde una laptop en el mismo lugar conectado ambos por un cable de red.

• Acceder a un equipo que está en el hogar desde el trabajo, aunque sea en una localización distante utilizando internet.

• Lo inverso, acceder a la PC de nuestro trabajo desde un equipo en el hogar u otra ubicación diferente usando internet.

Requisitos para utilizar Escritorio remoto entre dos equipos:

Los requisitos indispensables para usar Escritorio remoto entre dos equipos son los siguientes:

- Debe existir una conexión de red funcional.
- Escritorio remoto debe estar habilitado en ambos equipos.
- El equipo que se conecte debe tener permiso para conectarse, para obtener dicho permiso debe aparecer en la lista de usuarios, a no ser que sea Administrador.
- El equipo que recibirá la conexión debe estar encendido, no puede estar en estado de suspensión ni de hibernación, por lo que debe configurarse

las Opciones de energía en el Panel de control, pare que no entre en ninguno de dichos estados de forma automática

14.4.2 CARACTERISTICAS DE TEAMVIEWER

Multiplataforma: Multiplataforma de PC a PC, móvil a PC, PC a móvil e incluso móvil a conexiones compatibles con Windows, macOS, Linux, Chrome OS, DS, Android, Windows Universal Platform y BlackBerry.

Máxima compatibilidad: TeamViewer funciona en el mas amplio espectro de sistemas operativos, desde sistemas vanguardistas con lo Último en OS hasta dispositivos más antiguos y sistemas operativos heredados.

Sin configuración: TeamViewer funciona incluso detrás de firewalls y detecta autocráticamente cualquier configuración proxy.

Fácil de entender: Disfrutar de una interfaz de usuario avanzada, ordenada de forma clara, sencilla, de manejo rápido y fácil de operar.

Alto rendimiento: La configuración y ruta de la conexión inteligente, el uso eficiente del ancho de banda, la transmisión de datos rápida, la velocidad de hasta 60 bps, la aceleración de hardware y los ajustes de calidad automáticos garantizan una experiencia de usuario optimizada.
Gran seguridad: TeamViewer emplea el intercambio de claves publicas/privadas RSA 2048, codificación de sesión AES (256 bits) de punto a punto, contraseñas aleatorias para acceso puntual, autenticación opcional de dos factores y controles de acceso mediante dispositivos de confianza, así como mediante listas blancas y negras.

Internacional: TeamViewer está disponible en más de 30 idiomas y es compatible con teclados internacionales, lo que lo convierte en la solución ideal pare utilizarlo en todo el mundo.

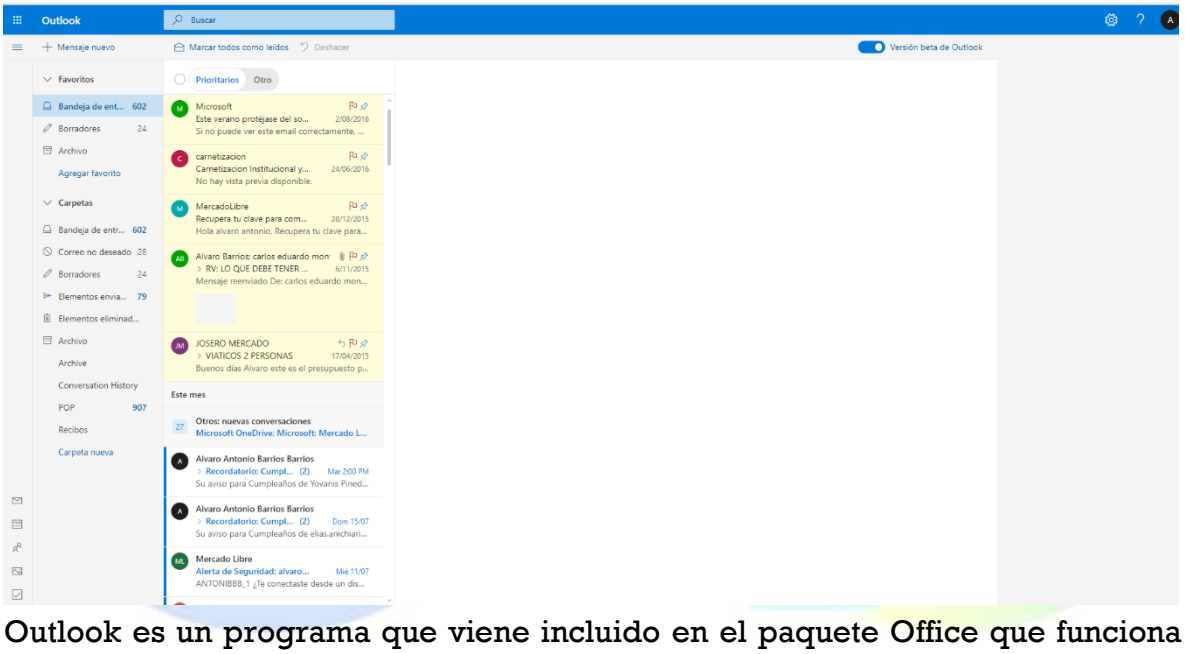
Gratis para pruebas y Uso personal: TeamViewer es de forma gratuita sin tener que facilitar ninguna información personal. También puede utilizar el software en casa para uso particular de forma gratuita.

Maltica: Teamviewer da la posibilidad de interactuar chat individual o grupal en la Corporación

14.5. CORREO ELECTRONICO

En el Concejo Municipal de Coveñas hay OUTLOOK y GMAIL

a) **MICROSOFT OUTLOOK**



Outlook es un programa que viene incluido en el paquete Office que funciona bajo la plataforma de Windows y ha sido desarrollado por la compañía Microsoft para dar soporte a gente que necesitaba un gestor de correo electrónico.

La función de este programa es recibir y enviar correos electrónicos así como la de almacenar localmente los mensajes recibidos y enviados mediante un archivo.

Una de sus múltiples características es:

- **Clutter:** Clutter ayuda al usuario a ordenar su bandeja de entrada, clasificando los mensajes y separándolos según su importancia. Cuanto mas se use Outlook.com, Clutter se ajustara aun mas a las necesidades del usuario.

- Búsqueda **de sugerencias y Filtros:** a través de las Sugerencias, los contactos y contenidos favoritos del usuario serán más accesibles a la hora de buscar entre tus correos. Los Filtros, por su parte, ofrecen una búsqueda más ajustada por remitente, archivos, fecha de recibo y contenido adjunto.

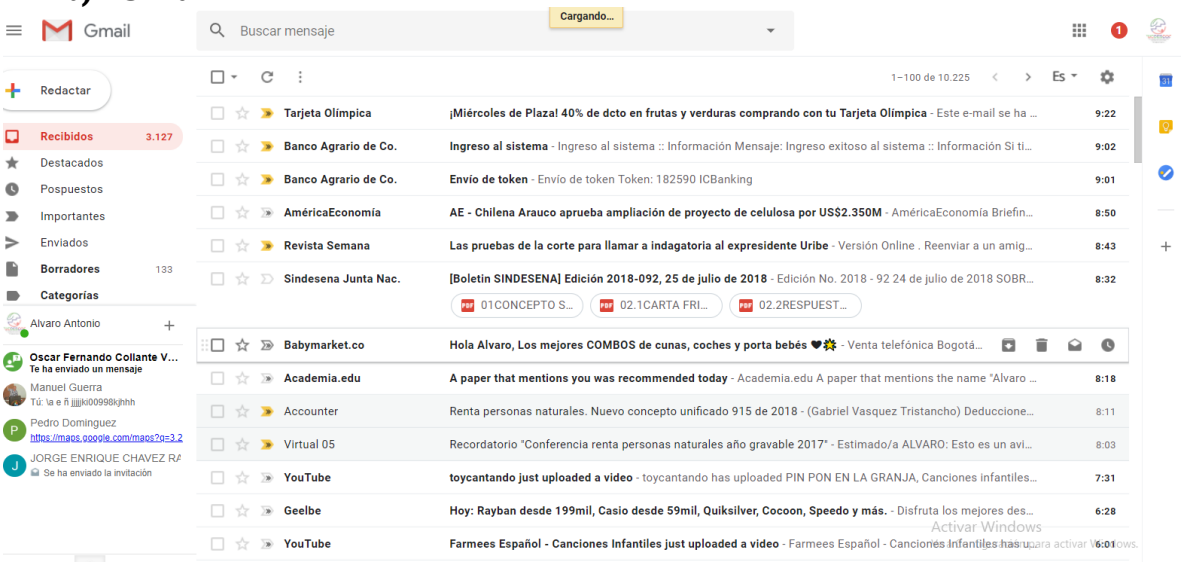
- Escritura y lectura Pop-out: esta característica facilita la multitarea, ya que los mensajes pueden aparecer en nuevas ventanas.

- Pins y Banderas: los usuarios podrán destacar sus emails más relevantes con pins y podrán marcar otros como no leídos mediante las banderas.

- Administrar varias cuentas de correo electrónico desde un Único lugar. Puede administrar fácilmente los mensajes de correo electrónico de varias buzones. Sincronice varias cuentas de correo electrónico de servicios como Hotmail, Gmail de prácticamente cualquier otro proveedor con Outlook 2010.

- Administrar fácilmente grandes volúmenes de correo electrónico y Personalizar tareas comunes en comandos de un solo clic.

b) Gmail



Gmail es un servicio gratuito de correo electrónico proporcionado par Google que combina las mejores funciones del correo electrónico tradicional con la tecnología de búsqueda de Google. Al igual es una herramienta en la que se puede visualizar sincronizar el correo corporativo para ser visualizado por fuera de las instalaciones del Concejo Municipal de Coveñas.

Gmail ofrece una capacidad de almacenaje de mensajes de 15 GB compartido can Drive y Fotos de Google +. Gracias a esta gran capacidad de almacenamiento no necesitaras eliminar mensajes para liberar espacio, sino que los podrás tener siempre disponibles, y localizarlos fácilmente.

Tiene integrado un servicio de chat para poder comprobar qua usuarios están online y conectarse con ellos en tiempo real. Las conversaciones de chat pueden guardarse y buscarse en Gmail, igual que las del correo electrónico.

Dentro de las características de Gmail están:

a) **Almacenamiento de 1GB:** Gmail innovo desde sus inicios al ofrecer lo que otros servicios de correo no ofrecían: 1GB de espacio de almacenamiento. Aunque en hoy en día, 1GB suene a poco, en 2004, la competencia tenia a disposición de sus usuarios apenas de 2 a 6MB, por lo que muchos debían borrar correos para hacer mas espacio. Hoy, Gmail da al menos 15 GB gratis.

b) **Búsqueda:** Gmail fue el primer servicio de e-mail en integrar una barra de búsqueda para permitir encontrar correos de forma rápida y sencilla, por palabras clave.

c) **Mensajería (GTalk, Hangouts):** Fue el primer servicio de correo electrónico en integrar un chat a su interface. Los usuarios podían enviar mensajes a sus contactos sin utilizar otra plataforma de mensajería externa. Estas herramientas permiten también las video llamadas.

d) **Organización de correo electrónico:** Gmail innovo en la manera de organizar los correos. Un mismo tema entre varias personas fue catalogado como "conversaciones". En 2013, introdujo las categorías: Principal, Social y Promociones, permitiendo al usuario clasificar sus

correos de forma ordenada, y agregar mas categorías según su preferencia.

e) **Herramientas (Drive, Docs):** Gmail esta integrado a otras herramientas desarrolladas por Google. Permite trabajar de forma colectiva documentos que se guardan en Google Docs.

f) **Labs:** En Configuración > Labs es posible encontrar algunas funciones: detener un envió en los 30 segundos siguientes a que un mensaje sali6 de la casilla. También una lista de opciones para personalizar la interface de correo.

g) **Android e IOS:** La integración con el teléfono celular marco también innovación en Gmail. Se lanzaron las apps para móviles y se han convertido en una extensión importante del correo versión escritorio.

h) **Cuentas delegadas:** Es de especial utilidad para quienes manejan Gmail en el ámbito empresarial. Permite un acceso delegado desde la bandeja personal. Para una cuenta corporativa, se puede designar a otras personas para escribir en nombre de esta.

i) **Configuración visual:** En 2011, Gmail lanzo el ostión de ponerle una imagen de fondo al correo, en su mayoría paisajes, lo que llevo a una mayor personalización.

15. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

Las funciones del comité de Seguridad de la Información son asumidas por el Comité del Modelo Integrado de Gestión (MIG).

16. DOCUMENTOS DE REFERENCIA

• Constitución Política de Colombia. Artículo 15. Ley 44 de 2093. Por la cual se modifica y adiciona la Ley 23 de 2082 y se modifica la Ley 29 de 2044 y Decisión Andina 351 de 2015 (Derechos de autor).
• Ley 527 de 2099. Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
• Ley 594 de 2000. Por medio de la cual se expide la Ley General de Archivos.
• Ley 850 de 2003. Por medio de la cual se reglamentan las veedurías ciudadanas
• Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
• Ley 1221 del 2008. Por la cual se establecen normas para promover y regular el Teletrabajo 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 - TICSe crea la agencia Nacional de espectro y se dictan otras disposiciones.
• Ley 1437 de 2011. Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.
• Ley 1474 de 2011. Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
• Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
• Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
• Ley 2015 de 2018. Por la cual se modifica la Ley 23 de 2082 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
• Ley 2052 de 2020. Por medio de la cual se expide el código general disciplinario

• Ley 2055 de 2020. Por el cual se expide el Plan Nacional de Desarrollo 2018-2022. "Pacto por Colombia, Pacto por la Equidad".
• Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000,
parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
• Decreto 0884 del 2012. Por el cual se reglamenta parcialmente la Ley 1221 del 2008.
• Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
• Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
• Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto 1074 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
• Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
• Decreto 1080 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Cultura.
• Decreto 1081 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
• Decreto 728 de 2017. Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico
• Decreto 1499 de 2017. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
• Decreto 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 2106 de 2019. Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.

• CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.

• CONPES 3854 de 2016. Política Nacional de Seguridad digital.