PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION BASADOS EN LA NORMA ISO/IEC 27001:2013

EMPRESA REGIONAL AGUAS DEL TEQUENDAMA
S.A. E.S.P. DE LA MESA

WILLIAM TEJEDOR BAYONA
Gerente General

ELABORADO
ING. JHON ALEXANDER CORDOBA QUINTERO
Profesional Universitario

LA MESA ENERO DE 2022

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El presente documento describe el plan de seguridad y privacidad, junto con el de privacidad de la Información, alineada con los objetivos, metas, procesos, procedimientos y estructura organizacional.

La Política de Gobierno Digital han definido dos (2) componentes: TIC para el Estado y TIC para la sociedad, tres (3) habilitadores transversales Arquitectura, Seguridad y Servicios Ciudadanos Digitales, como podemos ver en el siguiente esquema:

Política de Gobierno Digital
Fuente MinTIC

Donde los componentes permiten mejorar el funcionamiento de las entidades públicas; su relación con otras entidades y el fortalecimiento de su relación con la sociedad. Los habilitadores por su parte contribuyen al logro de los objetivos definidos en los componentes

El habilitador de Seguridad y Privacidad permite a la Empresa Regional Aguas del Tequendama S.A. E.S.P.garantizar la confidencialidad, disponibilidad e integridad de la información para la cual se hace indispensable diseñar este plan

Empresa Regional Aguas del Tequendama S.A. E.S.P., está comprometida con la protección, preservación, y aseguramiento de la confidencialidad, Integridad, disponibilidad, accesibilidad, legalidad, confiabilidad y no repudio de los activos de información, en todo su ciclo de vida, mediante la Gestión del Riesgo, en las etapas de implementación, monitoreo y mejora continua. De igual forma, tiene un compromiso con el fortalecimiento de la cultura de la Seguridad de la Información, en los/as

servidores/as públicos/as y el cumplimiento de los requisitos legales relacionados con la misma, todo lo anterior, enmarcado en el Sistema Integrado de Gestión de la Entidad.

Empresa Regional Aguas del Tequendama S.A. E.S.P.debe cumplir con el objetivo de seguridad de la información que es proteger los activos de información de la organización, el plan deberá está alineado con los objetivos estratégicos, la gestión de riesgos de la información, optimización de recursos, entrega de valor, medición del desempeño y la integración del aseguramiento del proceso.

A continuación, se relacionan los objetivos específicos a cumplir en la elaboración del plan estratégico de seguridad de la información:

- Realizar un diagnóstico de la situación actual de seguridad de la información.
- Desarrollar un análisis de los riesgos de la información
- Definir los decretos, políticas y manuales para el modelo de gestión de seguridad de la información
- Elaborar el plan estratégico de seguridad de la información con la mitigación de riesgos

2. ALCANCE DEL DOCUMENTO

Este documento describe las estrategias, planes, políticas y manuales que ejecutará Empresa Regional Aguas del Tequendama S.A. E.S.P., durante los años 2020 al 2023 en materia de Seguridad de la información, con el fin de concretar el logro de objetivos misionales; de igual forma establece la organización en el cual se apoyará para lograrlo y establece sus respectivos planes de acción.

Por lo tanto, en el desarrollo de este documento, se requiere inicialmente hacer la diagnostico, el cual está basado en el instrumento suministrado por el Ministerio TIC en cual nos da una visión general del estado que se encuentra la administración, para identificar sus debilidades y fortalezas amenazas y oportunidades con el fin de concretar las estrategias para estructurar el Plan de seguridad de la información

3. MARCO NORMATIVO

En las siguientes normas se identifica el marco legal a través del cual se establece y obliga a las entidades públicas a tener y desarrollar un Modelo de Gestión de seguridad de la Información con el análisis de los riesgos que se tiene de este tema.

Tabla 1 Marco Normativo

NORMA	DESCRIPCION
Documento CONPES N° 3854	Política Nacional de Seguridad Digital
Decreto 415 de 2016	Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones
Ley 1712 de 2014	Ley de trasparencia y de acceso a la información pública nacional.
Decreto 2573 de 2014	Por medio del cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea.
Política SGSI Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea	Modelo que emite el Ministerio TIC en temas del Modelo de Gestión de Seguridad de la Información

4. RUPTURAS ESTRATÉGICAS

4.1. Identificación de los activos de Información.

- Ayudar en la transformación del Sector de las Comunicaciones con Tecnologías de la Información
- Ser líder del sector, en el departamento y país con la implementación de las estrategias TI del estado.

4.2. Dominio Gobierno de TI

- Líderes de TI encaminados a la gestión de resultados eficientes
- Servicios de TI soportados en procesos
- Gobernanza efectiva en la toma de decisiones

4.3. Dominio Sistemas de Información

- Sistemas de Información escalables e interoperables y tolerando los procesos al interior de la entidad.
- Disponer de los Sistemas de información en ambientes independientes, autónomos y controlados

4.4. Dominio gestión de información

- Disponibilidad de la información para la toma de decisiones
- Estrategia de información fundamentada en el ciclo de vida de la información
- Mecanismo, obtención y generación de valor a partir de la información

4.5. Dominio servicios tecnológicos

- Servicios tecnológicos con alta disponibilidad y operación
- Gestión de los servicios tecnológicos tercerizada, especializada, gerenciada y con tecnología de punta, según la relación costo/beneficio.

4.6. Dominio uso y apropiación

- Garantía de uso, apropiación y acceso a todos los públicos
- Procesos efectivos en la promoción, divulgación, manejo y gobernanza de información.
- Capacitar el equipo humano de la alcaldía municipal y desarrollar sus capacidades de uso y apropiación de la tecnología de información y comunicaciones.

5. ANÁLISIS DE LA SITUACIÓN ACTUAL

Atendiendo los objetivos nacionales encontramos que Colombia se convertirá en un líder mundial en el desarrollo de aplicaciones sociales dirigidas a los más pobres así mismo tendrá el gobierno más eficiente y transparente gracias a las TIC para el 2020-2023.

Por otro lado, en el departamento de Cundinamarca del cual hace parte La Mesa se han organizado para promover el acceso, desarrollo, uso efectivo, masificación y apropiación social de las Tecnologías de la información y Comunicaciones TIC. En Cundinamarca, se liderarán los estudios y las gestiones necesarias para adelantar los proyectos de carácter red social de datos a corto, mediano y largo plazo.

Implementar un Modelo de Gestión de Seguridad de la Información (SGSI) en la Empresa Regional Aguas del Tequendama S.A. E.S.P., no depende únicamente del área de Sistemas, sino de toda una

cultura organizacional que permita la protección y resguardo de la información. Es tan claro este concepto para la Entidad, que se ha dado un gran paso en este sentido con la adopción del decreto de Riegos, firmada por la Alta Dirección y donde se establecen los tipos de riesgos que tiene la entidad y hace énfasis en los riesgos de seguridad para el manejo de la información, y se imparten instrucciones para el uso y administración del recurso tecnológico de la Empresa Regional Aguas del Tequendama S.A. E.S.P.

Si bien estas políticas no están siendo aplicadas en su totalidad, es importante resaltar que durante el primer semestre de 2018 se viene analizando los controles de la norma ISO 27001

Sin embargo, dado que falta la socialización del mismo, la información crítica o no, personal o institucional, puede ser sustraída por los usuarios en cualquier medio magnético u óptico, lo cual implica una clara vulnerabilidad del manejo de la información que podría ser crítica para la alcaldía.

- Empresa Regional Aguas del Tequendama S.A. E.S.P. ya ha elaborado, aprobado, aplicado, publicado y comunicado un documento de política de seguridad de la información a todos los funcionaros, contratista y proveedores externos de servicios tecnológicos.
- El sistema de cableado de telecomunicaciones y eléctrico presenta disposiciones inadecuadas y deficientes
- Además, no existen implementaciones de seguridad y procedimiento de la Empresa Regional Aguas del Tequendama S.A. E.S.P. asociados como, dispositivos de seguridad, segmentación de red y detección de intrusos.
- No existe plan estratégico de tecnología informática de largo plazo que comprenda las necesidades de equipos, programas y otros servicios.
- No ha definido e implementado una política de copias de seguridad de la información ni repositorios de conocimiento para todos sus activos de información,
- Así mismo no existen políticas de procedimientos de licenciamiento de software, política de hojas de vida de equipos tecnológicos y su bitácora de mantenimiento preventivo o correctivo.
- No existe una política escrita en la compra de equipos de cómputo que cumplan con los requisitos de seguridad en la entidad

6. MODELO DE GESTION DE SEGURIDAD DE LA INFORMACIÓN Y SUS RIESGOS

Lo más complicado al momento de integrar los temas de seguridad de la información es que, generalmente, no están enfocados en los objetivos del negocio y sus intereses, lo que se constituye en la realidad para la Empresa Regional Aguas del Tequendama S.A. E.S.P. Para que un modelo esté en los mismos términos de los objetivos del negocio, debe tener presente tres áreas principales: los lineamientos de seguridad, la gestión de la seguridad y los grupos de interés.

La primera área es tener en cuenta los lineamientos que se van seguir en la Empresa Regional Aguas del Tequendama S.A. E.S.P. son: basados en la ISO 27001, las cuales tienen 133 controles agrupados en los siguientes ítems:

- Política de seguridad
- Organización de la información de seguridad
- Administración de recursos
- Seguridad de los recursos humanos
- Seguridad física y del entorno
- Administración de las comunicaciones y operaciones
- Control de accesos
- Adquisición de sistemas de información, desarrollo y mantenimiento
- Administración de los incidentes de seguridad
- Administración de la continuidad de negocio
- Cumplimiento (legales, de estándares, técnicas y auditorías)

Todos estos lineamientos, apuntan a que el sistema de gestión que se implementa se garantice que la información tenga las tres características básicas: la integridad, la disponibilidad y la confidencialidad. Estas tres características son fundamentales, y podrían complementarse con otras tres, para formar lo que se conoce cómo el Parkerian Hexad: el control de la información que se refiere a que a pesar que la información se pueda perder esta no sea revelada, la verificación del origen de los datos y la utilidad de los datos.

La gestión de seguridad, debe desarrollarse a partir de estrategias, procesos y métricas. La estrategia formada por políticas, estándares y guías son los lineamientos de lo que la organización va a cumplir de acuerdo a los lineamientos de seguridad definidos y adoptados; esta estrategia debe llevar a definir controles de seguridad viables para ser implementados por la organización. Los procesos deben reflejar cómo se implementa lo que fue definido en la estrategia, por lo tanto, deben reflejar de qué forma interviene el recurso humano y la tecnología para cumplir con los controles establecidos. Finalmente, las métricas van a permitir la retroalimentación de todo el sistema, y van a permitir realizar ajustes sobre la estrategia y los procesos de tal forma que se cumpla con lo definido en los lineamientos.

Y por último el área que debe tenerse en cuenta, son los grupos de interés (stakeholders) involucrados en la gestión de la seguridad de la información. Todos deben estar al tanto de los resultados, según las métricas definidas en el modelo, de tal forma que quede claro cómo la gestión de la seguridad aporta a los objetivos del negocio. Esta es quizás el área que más necesite atención, pues es la forma de evidenciar el cumplimiento de las expectativas que tiene la organización con el modelo de gestión de la seguridad.

Planear, plantear, desarrollar, mejorar y ejecutar este modelo, tiene un factor importante, el Funcionario, sin la apropiación y la respectiva concientización del ellos el Modelo se puede quedar en papel.

El Modelo de Seguridad y Privacidad de la Información – MSPI, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

A través del decreto único reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones, se define el componente de seguridad y privacidad de la información, como parte integral de la estrategia Gobierno Digital

Debe ser actualizado periódicamente y proyectado a cuatro años; así mismo recoge además de los cambios técnicos de la norma, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información. La periodicidad con que se hace estas revisiones debe ser anual, de tal forma que lo controles y auditorias durante el transcurso del año se hagan evidentes y sea un manual de conocimiento. (MinTic, 2016)

El Modelo de Seguridad y Privacidad de la Información se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión.

El objetivo principal es generar un documento de lineamientos de buenas prácticas en Seguridad y Privacidad para las entidades del Estado. Este modelo-documento consta de cinco fases, incluidas en la siguiente figura:

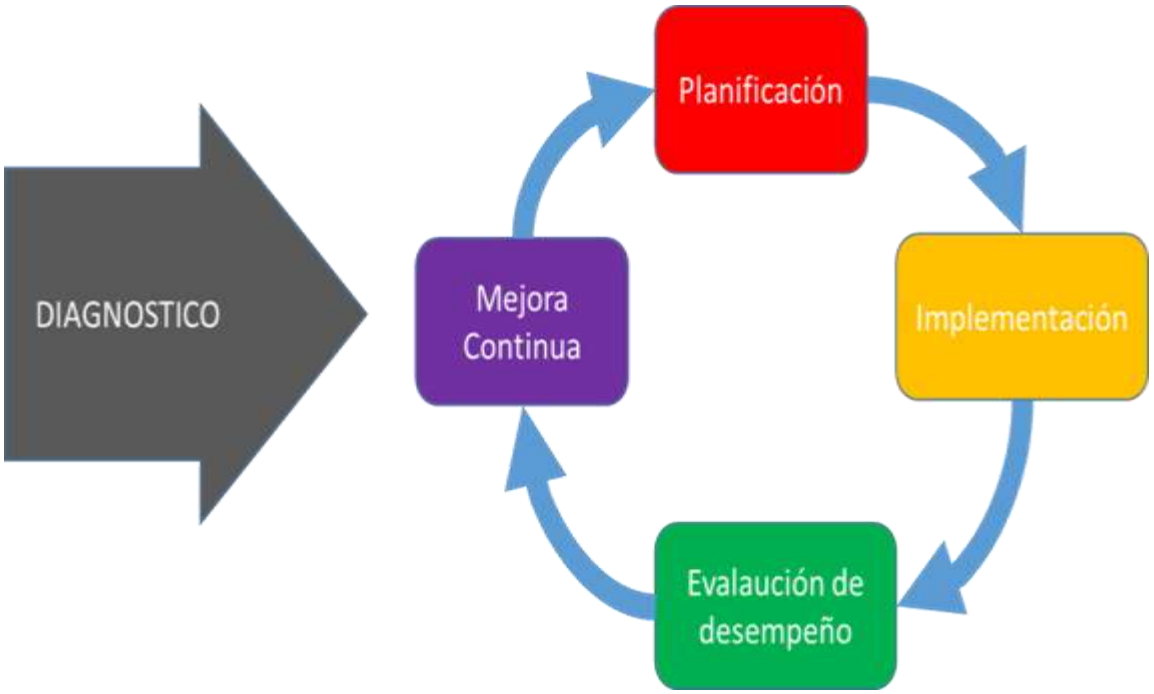

Figura Ciclo de Operación del MGSI
Fuente: Extraído del MinTIC Modelo de Gestión de Seguridad de Información

Con el Diagnostico se pretende identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información, Determinar el nivel de madurez de los controles de seguridad de la información el avance en la implementación del ciclo de operación al interior de la entidad, el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales y uso de buenas prácticas en ciber-seguridad. MinTic (2016) .

Para la fase de Planificación se 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. Este enfoque es por procesos y debe extenderse a toda la Entidad.

Aquí es donde se debe elevar a decreto municipal el MSPI como política, que incluye la voluntad de la Alta Dirección de la Entidad para apoyar la implementación del Modelo de Seguridad y Privacidad de la Información. La política debe contener una declaración general por parte de la administración, donde se especifique sus objetivos, alcance, nivel de cumplimiento.

6.1. Política general del Modelo de Seguridad y Privacidad de la Información

Manual de políticas, donde se describe los objetivos, alcances y el nivel de cumplimiento, que garanticen el adecuado uso de los Activos de información al interior de la Entidad; definiendo las responsabilidades generales y específicas para la gestión de la seguridad de la información

En el manual de políticas de la entidad, se debe explicar de manera general, las políticas, los principios de seguridad y la normatividad pertinente.

La entidad debe evaluar los requerimientos necesarios para ser ajustados o desarrollados en la elaboración de las políticas de seguridad y privacidad, así como en la implementación.

6.2. Gestión y Clasificación de activos de Información

La realización de un inventario y clasificación de activos se ha definido en el Modelo de Seguridad y Privacidad de la Información con respecto a la seguridad de los activos de información de los procesos de una entidad, y cuyo objetivo es dar cumplimiento a cuatro puntos principales descritos a continuación.

- Inventario de activos: todos los activos deben estar claramente descritos y la entidad debe elaborar y mantener un inventario de los mismos.
- Propiedad de los activos: los activos de información del inventario deben tener un propietario y/o responsable.
- Clasificación de la información: La información se deberá clasificar en función de los requisitos legales, valor, criticidad y prejuicio a divulgación o a modificación no autorizada.
- Etiquetado y manipulado de la información: Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.

El inventario de activos de información de la entidad debería especificar para cada activo:

- Información básica del activo (nombre, observaciones, proceso, entre otras).
- El nivel de clasificación de la información.
- Información relacionada con su ubicación, tanto física como electrónica.
- Su propietario y su custodio.
- Los usuarios y derechos de acceso.

El sistema de clasificación definido se basa en la confidencialidad como principio rector en la selección e incluye el tratamiento de la información en cuanto a la Confidencialidad, la Integridad y la Disponibilidad de cada activo. Asimismo, contempla el impacto que causaría la pérdida de alguna de estas propiedades.

Es recomendable desarrollar criterios de impacto del riesgo y especificarlos en términos del grado de daño o de los costos para la entidad, causados por un evento de seguridad de la información, considerando los siguientes aspectos:

- Nivel de clasificación de los activos de información de los procesos
- Brechas en la seguridad dela información (ejemplo: perdidas de confidencialidad, integridad y disponibilidad de la información)
- Operaciones deterioradas
- Perdida del negocio y del valor financiero
- Alteración de planes y fechas limites
- Daños para la reputación
- Incumplimiento de los requisitos legales.

De acuerdo a lo planteado en la guía, la identificación del riesgo se hace con base en causas identificadas para los procesos, dichas causas pueden ser internas o externas, según lo que haya identificado la Entidad a través del Contexto estratégico.

En este momento es importante establecer cuáles son los activos críticos para asociarlos a los procesos correspondientes y de allí generar el listado de procesos críticos. Inventariar los activos de información sensible, revisar los procesos según la clasificación del MECI y del modelo de gestión, con éste punto se revisa la pertinencia del alcance planteado para el MSPI.

6.3. Aplicación de los controles de la ISO 27001

En la norma completa, la primera parte hace referencia a la documentación previa que debe tener la institución y corresponde a los siguientes términos

1. OBJETO
1.1 GENERALIDADES
1.2 APLICACIÓN
2. REFERENCIA NORMATIVA
3. TÉRMINOS Y DEFINICIONES
3.1 Aceptación del riesgo
3.2. Activo
3.3 Análisis de riesgo
3.4 Confidencialidad
3.5 Declaración de aplicabilidad
3.6 Disponibilidad
3.7 Evaluación del riesgo
3.8 Evento de seguridad de la información
3.9 Gestión del riesgo
3.10 Incidente de seguridad de la información
3.11 Integridad
3.12 Riesgo residual
3.13 Seguridad de la información
3.14 Sistema de gestión de la seguridad de la información

Los entregables son los siguientes, primero el decreto de adopción de la política de riesgos en donde se determina los riesgos de la entidad o estratégicos, los riesgos de corrupción y los riesgos de sistema de Información y se da la forma de realizar los mapas respectivos.

El segundo decreto es el cual se adopta la política de Aplicación de objetivos de control y controles riesgos en base a la NTC 150/ IEC 27001 y se determina cual aplicamos y cual no.

El tercer decreto que aplica a los empleados y contratistas es el referente a a la confidencialidad de la información y a la no divulgación que firmarán todos y se registrará en la hoja de vida de los funcionarios y hará parte del contrato de prestación de servicios.

Por último, se determina la cantidad de políticas de acuerdo a la columna de cómo se aplicará el objetivo de control y controles

A continuación, enumeraremos los objetivos y la forma como se aplicaría en dicho decreto:

No.	ITEM	Descripción	Aplica Si/No	Cómo
A.5	**POLITICA DE SEGURIDAD - Nombre**			
A.5.1	**Política de Seguridad de la información - Sub-Nombre**			
A.5.1.1	Documento de la política de Control segundad de la información	La dirección debe aprobar un documento de política de segundad de la información y lo debe publicar y comunicar a todos los empleados y partes externas pertinentes	SI	Decreto de Adopción de Política de Seguridad de la Información
A.5.1.2	Revisión de la política de Control seguridad de la información	La política de seguridad de la información se debe revisar a intervalos planificados o cuando se producen cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz.	SI	Decreto de Adopción de Política de Seguridad de la Información, intervalos de un año y cuando hay cambio de Administración
A.6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN - Nombre**			
A.6.1	**Organización Interna**			
A.6.1.1	Compromiso de la dirección con la seguridad de la Información	La Dirección debe apoyar activamente la seguridad dentro de la organización con un rumbo claro, un compromiso demostrado, una asignación explicita y el conocimiento de las responsabilidades de la seguridad de la información	SI	Decreto de Adopción de Política de Seguridad de la Información
A.6.1.2	Coordinación de la seguridad de la Información	Control – Las actividades de la seguridad de la información deben ser coordinadas por los representantes de todas las partes de la entidad con roles y funciones laborales pertinentes	SI	Decreto de Adopción de Política de Seguridad de la Información
A.6.1.3	Asignación de responsabilidades para la seguridad de la información	Control – Se deben definir claramente todas las responsabilidades en cuanto a la seguridad de la información	SI	Decreto de Adopción de Política de Seguridad de la Información, designación de responsables.
A.6.1.4	Proceso de autorización para los servicios de procesamiento de información	Control – Se debe e implementar un proceso de autorización de la dirección para los nuevos servicios de procesamiento de información	NO	Se trabajará sobre los servicios de Información existentes, cuando se implemente un nuevo Sistema de Información se establecerá el control
A.6.1.5	Acuerdo de confidencialidad	Control – Se debe implementar y revisar con regularidad los requisitos de confidencialidad o los acuerdos de no-divulgación que reflejan las necesidades de la organización para la protección de la información	SI	Decreto de confidencialidad y no-divulgación de la información, su alcance y aplicación
A.6.1.6	Contacto con la Autoridades	Control – Se debe mantener contactos apropiados con las autoridades pertinentes	SI	De acuerdo al mapa de riesgos de Información establecido se debe referir a la autoridad pertinente
A.6.1.7	Contacto con grupos de interés especiales	Control – Se debe mantener los contactos apropiados con grupos de interés especiales, otros foros especializados en seguridad de la información y asociación de profesionales	NO	Aunque se determina la autoridad, la idea es como realizan las actividades las demás alcaldías con el manejo del Modelo de Gestión de Seguridad de la Información
A.6.1.8	Revisión independiente de la seguridad de la información	Control – El enfoque de la entidad para la gestión de la seguridad de la información y su implementación, se deben revisar independientemente a intervalos planificados, o cuando ocurra cambios significativos en la implementación de la seguridad	NO	Aunque la Empresa Regional Aguas del Tequendama S.A. E.S.P. no cuenta con presupuesto para que un tercero revise o audite, este tiene que informar al Ministerio TIC la evolución de Modelo de Gestión de la Seguridad de la Información y tenerlos presentes a los

				entes de control.
A.6.2	**PARTES EXTERNAS**			
A.6.2.1	Identificación de riesgos relacionados con las partes externas	Control – Se deben identificar los riesgos para la información y los servicios de procesamiento de información de la entidad de los procesos del negocio que involucran partes externas e implementar los controles apropiados antes de autorizar acceso	SI	Con la clasificación de la información que se realizó en el numeral 4.3.6, Gestión y Clasificación de activos de Información se cumple
A.6.2.2	Consideración de la seguridad cuando se trata con los clientes	Control – Todos los requisitos identificados se deben considerar antes de dar acceso a los clientes a los activos o a la información de la entidad	SI	Con la clasificación de la información que se realizó en el numeral 4.3.6, Gestión y Clasificación de activos de Información se cumple
A.6.2.3	Consideraciones de la seguridad en los acuerdos con terceras partes	Control – Los acuerdos con terceras partes que implica acceso, procesamiento, comunicación o gestión de la información de la entidad	SI	Cuando un tercero aplica una información clasificada se debe emitir un documento de confidencialidad
A.7	**GESTIÓN DE ACTIVOS**			
A.7.1	**Responsabilidad por los Activos**			
A.7.1.1	Inventario de Activos	Control – Todos los activos deben estar claramente identificados y se debe elaborar un inventario	SI	En cada oficina se determinara de acuerdo a las tablas de retención documental los activos de información
A.7.1.2	Propiedad de los Activos	Control – Toda la información y los activos asociados con los servicios de procesamiento de información deben ser “propiedad” de la entidad	SI	Se determina en la clasificación de los Activos de Información los responsables
A.7.1.3	Uso aceptable de los Activos	Control – Se deben identificar, documentar e implementar las reglas sobre el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de la información	SI	De acuerdo con las Tablas de Retención Documental aprobadas para la Entidad.
A.7.2	**Clasificación de la Información**			
A.7.2.1	Directivas de clasificación	Control – La información se debe clasificar en términos de su valor, de los requisitos legales de la sensibilidad y la importancia para la entidad	SI	Con la clasificación de la información que se realizó en el numeral 4.3.6, Gestión y Clasificación de activos de Información se cumple
A.7.2.2	Etiquetado y manejo de la Información	Control – Se debe desarrollar e implementar un conjunto de procedimientos adecuados para el etiquetado y el manejo de la información de acuerdo al esquema de clasificación adoptado por la entidad	SI	De acuerdo con las Tablas de Retención Documental aprobadas para la Entidad
A.8	**SEGURIDAD DE LOS RECURSOS HUMANOS**			
A.8.1	Antes de la contratación laboral			
A.8.1.1	Roles y Responsabilidades	Control – Se debe definir y documentar los roles y responsabilidades de los empleados, contratistas y usuarios de terceras partes por la seguridad, de acuerdo con la política de seguridad de la información de la entidad	SI	Decreto de Confidencialidad que firman los empleados y contratistas, junto con el documento de confidencialidad de tercera partes.

A.8.1.2	Selección	Control – Se deben realizar revisiones para la verificación de antecedentes de los candidatos a ser empleados o contratistas de acuerdo con los reglamentos, la ética y las leyes pertinentes, y deben ser proporcionales a los requisitos del negocio	SI	Manual de contratación de personal con el decreto de confidencialidad tanto para los empleados nuevos como para los contratistas
A.8.1.3	Términos y Condiciones laborales	Control – Como parte de su obligación contractual los empleados y contratistas deben estar de acuerdo y firmar los términos y condiciones de su contrato con relación a la seguridad de la información	SI	Decreto de Confidencialidad que firman los empleados y contratistas
A.8.2	**Durante la vigencia de la contratación laboral**			
A.8.2.1	Responsabilidad de la dirección	Control – La dirección debe exigir que los empleados y contratistas apliquen la seguridad según la política y los procedimientos establecidos	SI	Delegación de la persona responsable de ejecución y el control del modelo de gestión de seguridad de la información
A.8.2.2	Educación, formación y concientización sobre la seguridad de la información	Control – Todos los empleados de la entidad y los contratistas deben recibir formación adecuada en concientización y actualización regulares sobre las políticas y procedimientos de la entidad	SI	Establecer en la inducción y reinducción del personal sobre las políticas y actualizaciones de la seguridad de la información a empleados y contratistas
A.8.2.3	Proceso disciplinario	Control – Debe existir un proceso disciplinario formal para los empleados que hayan cometido alguna violación a la seguridad	SI	Establecer claramente las sanciones al que haya violación a la seguridad
A.8.3.3	Retiro de los derechos de acceso	Control – Los derechos de acceso de todos los empleados y contratistas a la información se deben retirar al finalizar su contratación o se debe ajustar después del cambio	SI	Política de acceso y retiro de personal empleado o contratista
A.9	**SEGURIDAD FISICA Y DEL ENTORNO**			
A.9.1	**Áreas Seguras**			
A.9.1.1	Perímetro de seguridad física	Control – Se debe utilizar perímetros de seguridad (barreras tales como paredes, puertas de acceso controladas con tarjeta o mostradores de recepción atendidos) para proteger las áreas que contienen información	SI	Se debe establecer la política de áreas de seguridad
A.9.1.2	Controles de acceso físico	Control – Las áreas deben estar protegidas con controles de acceso apropiado para asegurar que solo permite el acceso a personal autorizado	SI	Se solicita la política y la forma de acceso a las zonas protegidas
A.9.1.3	Seguridad de oficinas, recintos e instalaciones	Control – Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones	SI	Dentro de la política de áreas de seguridad, establecer este control
A.9.1.4	Protección contra amenazas externas y ambientales	Control – Se debe diseñar y aplicar protecciones físicas contra daño por incendio, inundación, terremoto, explosión, manifestaciones sociales y otra	NO	Aunque hay una directiva para el desarrollo de este control, se aplicaría después de la implementación del Modelo de Gestión de la Seguridad,

		forma de desastre natural o artificial		como mejora e incluirlas en el comité paritario de seguridad y salud en trabajo
A.9.1.5	Trabajo áreas seguras	Control - Se debe diseñar y aplicar la protección física y las directrices para trabajar en áreas seguras	SI	Se solicita la política y la forma de acceso a las zonas protegidas
A.9.1.6	Áreas de carga, despacho y acceso público	Los puntos de acceso tales como las áreas de carga y despacho, y otros puntos por donde pueda ingresar personal no autorizado a las instalaciones	NO	No aplica por la Alcaldía no tiene área de carga y despacho, tiene de atención al público y están definidas
A.9.2	**Seguridad de los equipos**			
A.9.2.1	Ubicación y protección de los equipos	Control – Los equipos deben estar ubicados o protegidos para reducir el riesgo debido a amenazas o peligros del entorno	SI	Se establecerá a través de una política y se incluirá en comité paritario de seguridad y salud en trabajo
A.9.2.2	Servicios de suministro	Control – Los equipos deben estar protegidos contra fallas de suministro de energía y otras anomalías causadas por fallas en los servicios de suministro	SI	Aunque hay una política que en la adquisición de equipos, se debe comprar con UPS, lo idea es tener una red estructurada con una UPS General
A.9.2.3	Seguridad del cableado	Control – El cableado de energía eléctrica y de telecomunicaciones que transporta datos o presta servicios de información deben estar protegidos	SI	La entidad debe realizar una inversión en el cableado estructurado de la red de datos y eléctrica y hace parte del plan de desarrollo
A.9.2.4	Mantenimiento de equipos	Control – los equipos deben recibir mantenimiento adecuado para asegurar cu continua disponibilidad e integridad	SI	Plan de Mantenimiento de equipos de cómputo, impresoras y redes
A.9.2.5	Seguridad de los equipos fuera de las instalaciones	Control – Se debe suministrar seguridad para los equipos fuera de las instalaciones teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la entidad	SI	Política de uso y manejo de equipos de cómputo fuera de las instalaciones de la entidad
A.9.2.6	Seguridad en la reutilización o eliminación de los equipos de computo	Control – Se deben verificar todos los elementos del equipo que contengan medios de almacenamiento para asegurar que haya eliminado cualquier software	SI	Política de reutilización y eliminación de equipos.
A.9.2.7	Retiro de Activos	Control – Ningún equipo, información o software de deben retirar sin autorización previa	SI	Política de baja de equipos de computo
A.10	**GESTION DE COMUNICACIONES Y OPERACIONES**			
A.10.1	**Procedimientos operacionales y responsabilidades**			
A.10.1.1	Documentación de los procedimientos de operación	Control – Los procedimientos de operación se deben documentar, mantener y estar disponibles para los usuarios que los necesitan	SI	Manuales de operación, mantenimiento y procedimientos establecidos
A.10.1.2	Gestión del cambio	Control – Se debe controlar los cambios en los servicios y los sistemas procesamiento de información	SI	Con la designación de funciones y responsabilidades en el manejo de los sistemas de información, se debe mantener el proceso de cambio

A.10.1.3	Distribución de funciones	Control – Las funciones y las áreas de responsabilidad se deben distribuir para reducir las oportunidades de modificación no autorizada o no intencional, o el uso inadecuado de los activos de la Entidad	SI	Políticas de manejo de claves y uso de ellas para todos los sistemas de información que maneja la alcaldía
A.10.1.4	Separación de las instalaciones de desarrollo, ensayo y operación	Control – Las instalaciones de desarrollo, ensayo y operación deben estar separadas para reducir los riesgos de acceso o cambios no autorizados en sistema operativo	NO	La alcaldía no posee áreas de desarrollo, ensayo y operación
A10.2	Gestión de la prestación del servicio por terceras partes			
A.10.2.1	Prestación de servicio	Control – se deben garantizar que los controles de seguridad, las definiciones de servicio y los niveles de prestación de servicio incluidos en el acuerdo, sean implementado, mantenidos y operados por las terceras partes	NO	La Empresa Regional Aguas del Tequendama S.A. E.S.P. no cuenta con servicios por terceras partes.
A.10.2.2	Monitoreo y revisión de los servicios por terceras partes	Control – Los servicios, reportes y registros suministrados por tercera partes se deben controlar y revisar con regularidad y las auditorias se deben llevar cabo a intervalos regulares	NO	La Empresa Regional Aguas del Tequendama S.A. E.S.P. no cuenta con servicios por terceras partes.
A.10.2.3	Gestión de cambio en los servicios por terceras partes	Control – Los cambios de la prestación de servicios, incluyendo el mantenimiento y mejora de las políticas existentes de seguridad de la información , en los procedimientos y en los controles se deben gestionar teniendo en cuenta la importancia de los sistemas y procesos del negocio involucrados	NO	La Empresa Regional Aguas del Tequendama S.A. E.S.P. no cuenta con servicios por terceras partes.
A.10.3	Planificación y aceptación del sistema			
A.10.3.1	Gestión de la capacidad	Control – Se debe hacer seguimiento y adaptación del uso de los recursos, así como proyecciones de los requisitos de la capacidad futura para asegurar el desempeño requerido del sistema	SI	A través del PETI, se formulara las proyecciones
A.10.3.2	Aceptación del sistema	Control – Se debe establecer criterios de aceptación para sistemas de información nuevos, actualizaciones y nuevas versiones y llevar acabo los ensayos adecuados del sistema durante el desarrollo y antes de la aceptación	NO	Los sistemas de información existentes son en su mayorías aplicaciones que vienen con este proceso, los locales se realiza una actualización cada seis meses que se informa mediante un acta de aceptación
A.10.4	**Protección contra códigos maliciosos y móviles**			
A.10.4.1	Controles contra códigos maliciosos.	Control - Se deben implementar controles de detección, prevención y recuperación para proteger contra códigos maliciosos, así como procedimientos apropiados de concientización de los usuarios	SI	Uso y apropiación de antivirus junto con la capacitación constante en los usuarios, más el proceso de inducción y reinducción
A.10.4.2	Controles contra	Control - Cuando se autoriza la utilización	NO	La Empresa Regional Aguas del

	códigos móviles	de códigos móviles, la configuración debe asegurar que dichos códigos operan de acuerdo con !a política de segundad claramente definida, y se debe evitar la ejecución de los códigos móviles no autorizados.		Tequendama S.A. E.S.P. no maneja códigos móviles
A.10.5	Respaldo			
A.10.5.1	Respaldo de información	Control – Se deben hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldo acordada	SI	Elaboración de política de copias de seguridad
A.10.6	**Gestión de la seguridad de las redes**			
A.10.6.1	Controles de las redes	Control – Las redes se deben mantener y controlar adecuadamente para protegerlas de las amenazas y mantener la seguridad de los sistemas y aplicaciones que usan la red, incluyendo la información en tránsito	SI	Elaboración en el diseño de acuerdo a la norma ISO/IEC 11801:2002 [1]
A.10.6.2	Seguridad de los servicios de la red	Control – En cualquier acuerdo sobre los servicios de la red se debe identificar e incluir las características de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de la red, sin importar si los servicios se prestan en la organización o se contrata externamente	SI	Política en el diseño, implementación y acceso a la red de la Empresa Regional Aguas del Tequendama S.A. E.S.P.
A.10.7	**Manejo de los medios**			
A.10.7.1	Gestión de los medios removibles	Control – Se deben establecer procedimientos para la gestión de los medios removibles	SI	Política de los medios removibles (memorias USB, Discos externos, etc)
A.10.7.2	Eliminación de los medios	Control – Cuando ya no se requieran estos medios, su eliminación se debe hacer de forma segura y sin riesgo, utilizando los procedimientos normales	NO	En la alcaldía no se utiliza medios extraíbles como cintas o casetes de grabación de copia de seguridad
A.10.7.3	Procedimiento para el manejo de la información	Control – Se debe establecer procedimientos para el manejo y almacenamiento de la información con el fin de proteger dicha información contra divulgación no autorizada o uso inadecuado	SI	La clasificación de la información elaborada en el punto 4.3.6.Gestión y Clasificación de activos de Información
A.10.7.4	Seguridad de la documentación del sistema	Control – la documentación del sistema debe estar protegida contra el acceso no autorizado	SI	Política del manejo de la documentación de los sistemas de información
A.10.8	**Intercambio de Información**			
A.10.8.1	Políticas y procedimientos	Control – Se deben establecer políticas, procedimientos y controles formales de	NO	La alcaldía de La Mesa no realiza intercambio de información con otras

[1] ISO/IEC 11801:2002 Information technology – Generic cabling for customer premises especifica sistemas de cableado para telecomunicación de multipropósito

	para el intercambio de información	intercambio para proteger la información mediante el uso de todo tipo de servicios de comunicación		entidades
A.10.8.2	Acuerdos para el intercambio	Control – Se deben establecer acuerdos para el intercambio de la información y del software entre la organización y partes externas	NO	La Empresa Regional Aguas del Tequendama S.A. E.S.P. no realiza intercambio de información con otras entidades
A.10.8.3	Medios físicos de transito	Control – Los medios que contienen información se deben proteger contra el acceso no autorizado, el uso inadecuado o la corrupción durante el transporte más allá de los limites físicos de la organización	NO	La Empresa Regional Aguas del Tequendama S.A. E.S.P.no realiza intercambio de información con otras entidades
A.10.8.4	Mensajería electrónica.	Control - La información contenida en la mensajería electrónica debe tener La protección adecuada	NO	La Empresa Regional Aguas del Tequendama S.A. E.S.P. no posee mensajería electrónica propia, accede a través de una mensajería implementada por el MinTic
A.10.8.5	Sistemas de Información del negocio	Control - Se deben establecer, desarrollar e implementar políticas y procedimientos para proteger la Información asociada con la interconexión de los sistemas de información del negocio	NO	La Empresa Regional Aguas del Tequendama S.A. E.S.P. no posee sistemas de Información del negocio
A.10.9	**Servicios de Comercio Electrónico**			
A.10.9.1	Comercio electrónico	Control - La información involucrada en el comercio electrónico que se transmite por las redes públicas debe estar protegida contra actividades fraudulentas, disputas por contratos y divulgación o modificación no autorizada.	NO	La Empresa Regional Aguas del Tequendama S.A. E.S.P.no maneja el proceso de comercio electrónico
A.10.9.2	Transacciones en línea	Control - la información involucrada en las transacciones en línea debe estar protegida para evitar transmisión incompleta, enrutamiento inadecuado, alteración , divulgación, duplicación o repetición no autorizada del mensaje	NO	La Empresa Regional Aguas del Tequendama S.A. E.S.P.no maneja el proceso de transacciones en linea
A.10.9.3	Información disponible al publico	Control – La integridad de la información que se pone a disposición en un sistema de acceso público debe estar protegida para evitar la modificación no autorizada	SI	En la clasificación de la información 4.3.6 Gestión y Clasificación de activos de Información
A.10.10	**Monitoreo**			
A.10.10.1	Registro de auditorias	Control – Se deben elaborar y mantener durante un periodo acordado las grabaciones de los registros para auditoría de las actividades de los usuarios, las excepciones y los eventos de seguridad de la información con el fin de facilitar las investigaciones futuras y el monitoreo del control de acceso.	NO	La Empresa Regional Aguas del Tequendama S.A. E.S.P. no deja grabaciones de las auditorias, desarrolla a través de informes
A.10.10.2	Monitoreo del uso	Control – Se deben establecer	SI	Los Sistemas de información locales

	del sistema	procedimientos para el monitoreo del uso de los servicios de procesamiento		poseen un monitoreo incorporado
A.10.10.3	Protección de la información del registro	Control - Se deben establecer procedimientos para monitoreo del uso de los servicios de procesamiento de información, y los resultados de las actividades de monitoreo se deben revisar con regularidad	SI	Los registros de uso se deben realizar mediante un monitoreo y una auditoria
A.10.10.4	Registros del administrador y del operador	Control - Se deben registrar las actividades tanto del operador como del administrador del sistema..	SI	Los registros de uso se deben realizar mediante un monitoreo y una auditoria
A.10.10.5	Registro de fallas	Control - Las fallas se deben registrar y analizar, y se deben tomar) las acciones adecuadas	SI	Se debe tener el registro de fallas
A.10.10.6	Sincronización de relojes	Control - Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de la organización o del dominio de seguridad deben estar sincronizados con una fuente de tiempo exacta y acordada.	SI	Se debe tener la hora exacta con el Instituto nacional de metrología
A.11	**CONTROL DE ACCESO**			
A.11..1	**Requisitos del negocio para el control de acceso**			
A.11.1.1	Política de control de acceso	Control - Se debe establecer, documentar y revisar la política de control de acceso con base en los requisitos del negocio y de la seguridad para el acceso	SI	Se debe establecer los roles de cada uno de los usuarios a los sistemas de información
A.11.2	Gestión de acceso de usuarios			
A.11.2.1	Registro De usuarios	Control Debe existir un procedimiento formal para el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de información	SI	Política de acceso, privilegios y revocación de usuarios de los sistemas de información
A.11.2.2	Gestión de Privilegios	Control - Se debe restringir y controlar la asignación y uso de privilegios	SI	Política de acceso, privilegios y revocación de usuarios de los sistemas de información
A.11.2.3	Gestión de contraseñas para usuarios	Control - La asignación de contraseñas se debe controlar a través de un proceso formal de gestión	NO	Ninguno de los Sistemas de Información local tiene un proceso formal de gestión de contraseñas
A.11.2.4.	Revisión de los derechos de acceso de los usuarios	Control - La dirección debe establecer un procedimiento formal de revisión periódica de los derechos de acceso de los usuarios.	NO	Ninguno de los Sistemas de Información local tiene un proceso formal de gestión de contraseñas y revisión
A.11.3	Responsabilidad de los usuarios			
A.11.3.1	Uso de contraseñas	Control – Se debe exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de contraseñas	SI	En el proceso de inducción y reinducción realzar la importancia del cambio y forma de adopción de las contraseñas
A.11.3.2	Equipo de usuario desatendido	Control - Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	NO	En la alcaldía no hay ningún equipo desatendido

A.11.3.3	Política de escritorio despejado y de pantalla despejada	Control-Se debe adoptar una política de escritorio despejado y una política de pantalla despejada para los servicios de procesarniento de información	SI	Política de uso de equipos, escritorio y pantalla despejada junto con la forma de guardar la información en los equipos
A.11.4	Control de acceso a las redes			
A.11.4.1	Política de uso de los servicios de red	Los usuarios sólo deben tener acceso a los servicios para cuyo uso están específicamente autorizados	SI	En el establecimiento de roles, funciones y procedimientos para el uso de los sistemas de información
A.11.4.2	Autenticación de usuarios para conexiones externas	Control - Se deben emplear métodos apropiados de autenticación para controlar el acceso de usuarios remotos.	SI	En la alcaldía o hay autorización para los usuarios remotos para resolver los problemas de los Sistemas de Información Local
A.11.4.3	Identificación de los equipos en las redes	La identificación automática de los equipos se debe considerar un medio para autenticar conexiones de equipos v ubicaciones especificas	SI	Política de mapas e identificación de equipos en la red
A.11.4.4	Protección de los puertos de configuración y diagnóstico remoto	El acceso lógico y físico a los puertos de configuración y de diagnóstico deben estar controlados	NO	La alcaldía no posee puertos de diagnóstico y configuración
A.11.4.5	Separación en las redes	Control - En las redes se deben separar los grupos de servicios de información, usuarios y sistemas de información	SI	Elaborar una política de administración de redes
A.11.4.6	Control de conexión a las redes	Control - Para redes compartidas, especialmente aquellas que se extienden más allá de las fronteras de la entidad, se debe restringir la capacidad de los usuarios para conectarse a la red, de acuerdo con la política de control del acceso y los requisitos de aplicación	SI	Elaborar una política de administración de redes
A.11.4.7	Control de enrutamiento en la red	Control Se deben implementar controles de enrutamiento en las redes con el fin de asegurar que las conexiones entre computadores y los flujos de información no incumplan la política de control del acceso de las aplicaciones	SI	Elaborar una política de administración de redes
A.11.5	**Control de acceso al sistema operativo**			
A.11.5.1	Procedimiento de ingresos seguros	Control El acceso a los sistemas operativos se debe controlar mediante un procedimiento de registro de inicio seguro	SI	Política de uso y manejo de los equipos de cómputo de la Empresa Regional Aguas del Tequendama S.A. E.S.P.
A.11.5.2	Identificación y autenticación de usuarios	Control Todos los usuarios deben tener un identificador único (ID del usuario) únicamente para su uso personal, y se debe elegir una técnica apropiada de autenticación para comprobar la identidad declarada de un usuario	SI	Política de uso y manejo de los equipos de cómputo de la Empresa Regional Aguas del Tequendama S.A. E.S.P.
A.11.5.3	Sistema de gestión de contraseñas	Control - Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las	NO	Ninguno de los Sistemas de Información local tiene un proceso formal de gestión de contraseñas y

		contraseñas		revisión
A.11.5.4	Uso de utilidades del sistema	Se debe restringir y controlar estrictamente el uso de programas utilitarios que pueden anular los controles del sistema y de la aplicaciones	SI	Política de uso y manejo de los equipos de cómputo de la Empresa Regional Aguas del Tequendama S.A. E.S.P.
A.11.5.5	Tiempo de inactividad de la sesión	Control - Las sesiones inactivas se deben suspender después de un periodo definido de inactividad	SI	Política de uso y manejo de los equipos de cómputo de la Empresa Regional Aguas del Tequendama S.A. E.S.P.
A.11.5.6	Limitación del tiempo de conexión	Control - Se deben utilizar restricciones en los tiempos de conexión para brindar seguridad adicional para las aplicaciones de alto riesgo	NO	Dentro del mapa de riesgos no hay aplicaciones de riesgo
A.11.6	**Control de acceso a las aplicaciones y a la información**			
A.11.6.1	Restricción de acceso a la información	Se debe restringir el acceso a la información y a las funciones del sistema de aplicación por parte de los usuarios y del personal de soporte, de acuerdo con la política definida de control de acceso		Política de uso de los sistemas de Información
a.11.6.2	Trabajo remoto	Control - Los sistemas sensibles deben tener un entorno informático dedicado (aislados)	NO	No aplica, no hay equipos ni accesos remotos en la alcaldía de La Mesa
A.11.7.1	Computación y comunicación móviles	Control - Se debe establecer una política formal y se deben adoptar las medidas de seguridad apropiadas para la protección contra los riesgos debidos al uso de dispositivos de computación y comunicaciones móviles.	NO	No aplica, no hay equipos y/o dispositivos móviles asociados en la Empresa Regional Aguas del Tequendama S.A. E.S.P.
A.11.7.2	Trabajo Remoto	Control – Se deben desarrollar e implementar políticas, planes operativos y procedimientos para las actividades de trabajo remoto.	NO	En la Empresa Regional Aguas del Tequendama S.A. E.S.P.no hay trabajo remoto
A.12	**ADQUISISCION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACION**			
A.12.1	**Requisitos de seguridad de los sistemas de información**			
A.12.1.1	Análisis y especificación de los requisitos de seguridad	Control - Las declaraciones sobre los requisitos del negocio para nuevos sistemas de información o mejoras a los sistemas existentes deben especificar los requisitos para los controles de seguridad	SI	Elaborar un manual de compras para el área de TIC
A.12.2	**Procesamiento correcto en las aplicaciones**			
A.12.2.1	Validación de los datos de entrada	Se deben validar los datos de entrada a las aplicaciones para asegurar que dichos datos son correctos y apropiados	NO	Los sistemas locales y otros sistemas que maneja la alcaldía tiene su proceso de validación de datos ingresados
A.12.2.2	Control de procesamiento interno	Control - Se deben incorporar verificaciones de validación en las aplicaciones para detectar cualquier corrupción de la información por errores de procesamiento o actos deliberados	NO	Los sistemas locales y otros sistemas que maneja la Empresa Regional Aguas del Tequendama S.A. E.S.P. tiene su proceso interno
A.12.2.3	Integridad del mensaje	Control - Se deben identificar los requisitos para asegurar la autenticidad y proteger la integridad del mensaje en las	SI	El personal técnico y profesional elaborar política de manejo de integridad de transmisión de datos

		aplicaciones, así como identificar e implementar los controles adecuados		como parte del mantenimiento preventivo de redes La Empresa Regional Aguas del Tequendama S.A. E.S.P.
A.12.2.4	Validación de los datos de salida	Control - Se deben evaluar los dalos de salida de una aplicación para asegurar que el procesamiento de la información almacenada es correcto y adecuado a las circunstancias		
A.2.3	**Controle criptográficos**			
A.12.3.1	Política sobre el uso de controles criptográficos	Control - Se debe desarrollar e implementar una política sobre el uso de controles criptográfico para la protección de la información	NO	La Empresa Regional Aguas del Tequendama S.A. E.S.P. no tiene controles criptográficos
A.12.3.2	Gestión de Llaves	Control - Se debe implementar un sistema de gestión de llaves para apoyar el uso de las técnicas criptográficas por parte de la entidad	NO	La Empresa Regional Aguas del Tequendama S.A. E.S.P. no tiene controles criptográficos
A.12.4	**Seguridad de los archivos del sistema**			
A.12.4.1	Control del software operativo	Control - deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	SI	Manual de uso y operación de los equipos de cómputo de la Empresa Regional Aguas del Tequendama S.A. E.S.P.
A.12.4.2	Protección de los datos de prueba del sistema	Control- Los datos de prueba deben seleccionarse cuidadosamente así como retenerse v controlarse	NO	Dentro de los sistemas que maneja la Empresa Regional Aguas del Tequendama S.A. E.S.P.no hay datos de prueba
A.12.4.3	Control de acceso al código fuente de los programas	Se debe restringir al acceso al código fuente de los programas	SI	En los servidores es restringido el uso, ubicación de los códigos fuentes de los programas locales
A.12.5.	**Seguridad en los procesos de desarrollo y soporte**			
A.12.5.1	Procedimientos de control de cambio	Control - Se deben controlar la implementación de cambios utilizando procedimientos formales de control de cambios.	SI	Política de actualización en los sistemas de información locales, con las nuevas actualizaciones y su debido control
A.12.5.2	Revisión técnica de las aplicaciones después de los cambios en el sistema operativo	Control Cuando se cambian los sistemas operativos, las aplicaciones críticas para el negocio se deben revisar y someter a prueba para asegurar que no hay impacto adverso en las operaciones ni en la seguridad de la organización	SI	Manual y uso de los equipos de cómputo de la Empresa Regional Aguas del Tequendama S.A. E.S.P.
A.12.5.3	Restricciones en los cambios a los paquetes de software	Control - Se debe desalentar la realización de modificaciones a los paquetes de software, limitarlas a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	SI	Manual y uso de los equipos de cómputo de la Empresa Regional Aguas del Tequendama S.A. E.S.P.
A.12.5.4	Fuga de información	Control - Se deben evitar las oportunidades para que se produzca fuga de información	SI	Con el decreto de confidencialidad y los controles de los sistemas de información
A.12.5.5	Desarrollo de	La organización debe supervisar y	NO	La Empresa Regional Aguas del

	software contratado externamente	monitorear el desarrollo de software contratado externamente		Tequendama S.A. E.S.P.no hace este tipo de contratos
A.12.6	Gestión de la vulnerabilidad técnica			
A.12.6.1	Control de vulnerabilidades técnicas	Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso, evaluar la exposición de la organización a dichas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos asociados.	SI	Documentos de las vulnerabilidades técnicas de los Sistemas de información, principalmente locales
A.13.	**GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN**			
A.13.1	**Reporte sobre los eventos y las debilidades de la seguridad de la información**			
A13.1.1	Reporte sobre los eventos de seguridad de la información	Control - Los eventos de segundad de la Información se deben informar a través de los canales de gestión apropiados tan pronto como sea posible	SI	Documento que lleva los incidentes de seguridad y el análisis respectivo para el mapa de riesgos y compras en el área de TIC
A.13.1.2	Reporte sobre las debilidades de la seguridad	Control - Se debe exigir a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información que observen y reporten todas las debilidades observadas o sospechadas en los sistemas o servicios.	SI	Periódicamente se debe realizar con entrevistas y encuestas de satisfacción de uso de los sistemas de Información
A.13..2	**Gestión de los incidentes y las mejoras en la seguridad de la información**			
A.13.2.1	Responsabilidades y procedimientos	Control Se deben establecer las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información	SI	Citamos en el numeral 4.3.9.Roles y Responsabilidades
A.13.2.2	Aprendizaje debido a los incidentes de seguridad de la información	Control – Deben existir mecanismos que permitan cuantificar y monitorear todos los tipos, volúmenes y costos de los incidentes de seguridad de la información	SI	Evaluación y mitigación de lo0s riesgos de seguridad vs el análisis de vulnerabilidades más el análisis en el incidentes de seguridad
A.13.2.3	Recolección de Evidencia	Control - Cuando una acción de seguimiento contra una persona u organización después de un incidente de seguridad de la información Implica acciones legales (civiles o penales), la evidencia se debe recolectar, retener y presentar para cumplir con las reglas para la evidencia establecidas en la jurisdicción pertinente	SI	De acuerdo a las directrices del COLCERT[2] y del Cai Virtual en lo referentes a los incidentes de seguridad que implique acciones legales
A.14	**GESTION DE CONTINUIDAD DEL NEGOCIO**			
A.14.1	**Aspectos de seguridad de la información, de la continuidad del negocio**			
A.14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad	Control - Se debe desarrollar y mantener un proceso de gestión para la continuidad del negocio en toda la organización el cual trate los requisitos de seguridad de la información necesarios para la	SI	Política donde se determina la forma de realizar la continuidad de los sistemas de Información existentes en Caso de un incidente de seguridad

[2] Grupo de respuesta a emergencias Cibernéticas de Colombia (http://www.colcert.gov.co/)

	del negocio	continuidad del negocio de la entidad		
A.14.1.2	Continuidad del negocio y evaluación de riesgos	Se deben identificar los eventos que pueden ocasionar Interrupciones en los procesos del negocio junto con la probabilidad y el impacto de dichas interrupciones, así como sus consecuencias para la seguridad de la información	SI	Mapa de riesgos del sistema de Información – continuidad del negocio
A.14.1.3	Desarrollo e implementación de planes de continuidad que incluyen la seguridad de la información	Control Se deben desarrollar e implementar planes para mantener o recuperar las operaciones y asegurar la disponibilidad de la información en el grado y la escala de tiempo requeridos, después de la interrupción o la falla de los procesos críticos para el negocio	SI	Política donde se determina la forma de realizar la continuidad de los sistemas de Información existentes en caso de un incidente de seguridad
A.14.1.4	Estructura para la planificación de la continuidad del negocio	Control - Se debe mantener una sola estructura de los planes de continuidad del negocio, para asegurar que todos los planes son consistentes, y considerar tos requisitos de la seguridad de la información de forma consistente, así como identificar las prioridades para pruebas y mantenimiento	SI	Política donde se determina la forma de realizar la continuidad de los sistemas de Información existentes en caso de un incidente de seguridad
A.14.1.5	Pruebas, mantenimiento y reevaluación de los planes de continuidad de negocio	Control - Los planes de continuidad del se deben negocio someter a pruebas y revisiones periódicas para asegurar su actualización y su eficacia	SI	Realizar pruebas de continuidad de negocio junto la verificación de las copias de seguridad
A.15	**CUMPLIMIENTO**			
A.15.1	**Cumplimiento de los requisitos legales**			
A.15.1.1	Identificación de la legislación aplicable	Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, así como el enfoque de la organización para cumplir estos requisitos se deben definir explícitamente, documentar y mantener actualizados para cada sistema de información " para la entidad	SI	De acuerdo a los parámetros legales de Colombia más los establecidos por la procuraduría general de la nación y el Ministerio TIC
A.15.1.2		control - Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material con respecto al cual pueden existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.	SI	En el uso del software y el cumplimiento de Sayco y Acinpro sobre software legal
A.15.1.3	Protección de los registros de la organización	Control - Los registros importantes se deben proteger contra pérdida, destrucción y falsificación, de acuerdo con	SI	Se aplica la política de copias de seguridad de la información relevante

		los requisitos estatutarios, reglamentarios contractuales y del negocio		
A.15.1.4	Protección de los datos y privacidad de la información personal	Control - Se debe garantizar la protección de los datos y la privacidad, de acuerdo con la legislación y los reglamentos pertinentes y, si se aplica, con las cláusulas del contrato	SI	Política de privacidad de la información tanto para los empleados como para los contratistas
A.15.1.5	Prevención del uso inadecuado de los servicios de procesamiento de información	Control - Se debe disuadir a los usuarios de utilizar los servicios de procesamiento de información para los propósitos no autorizados	SI	Política de privacidad de la información tanto para los empleados como para los contratistas
A.15.1.6	Reglamentación de los controles criptográficos	Se deben utilizar controles criptográficos que cumplan todos los acuerdos, las leyes y los reglamentos pertinentes	NO	La Empresa Regional Aguas del Tequendama S.A. E.S.P.no tiene controles criptográficos
A.15.2.	Cumplimiento de las políticas y las normas de seguridad y cumplimiento técnico			
A.15.2.1	Cumplimiento con las políticas y normas de seguridad	Los directores deben garantizar que todos los procedimientos de segundad dentro de sus áreas de responsabilidad se llevan a cabo correctamente para lograr el cumplimiento con las políticas y las normas de seguridad	SI	Compromiso del concejo de gobierno con el modelo de gestión de seguridad de la información
A.15.2.2	Verificación del cumplimiento técnico	Control - Los sistemas de información se deben verificar periódicamente para determinar el cumplimiento con las normas de implementación de la seguridad	SI	En las auditorias se debe verificar todo con respecto al manejo uso y copias de seguridad de la información
A.15.3.1	Controles de auditoria de los Sistemas de Información	Control Los requisitos y las actividades de auditoria que implican verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar el riesgo de interrupciones de los procesos del negocio.	SI	Control de software y requisitos de uso y manejo de los equipos de cómputo de la Empresa Regional Aguas del Tequendama S.A. E.S.P.
A.15.3.2	Protección de las herramientas de auditoria de los sistemas de información	Se debe proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar su uso inadecuado o ponerlas en peligro	NO	Los sistemas de información locales no tienen un sistema de auditoria

Programación especial

- Programa anual de mantenimiento de equipos e impresoras
- Programación de copias de seguridad de las bases de datos
- Manejo de la gestión documental
- Compra de antivirus