



Empresa Regional Aguas del Tequendama S.A. E.S.P.
Anapoima – La Mesa



Empresa Regional Aguas del Tequendama S.A. E.S.P.
Anapoima – La Mesa.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023

La Mesa, enero de 2023

Sede Administrativa y PQR:
Diagonal 8 No. 1 – 37 Barrio Quintas de San Pablo
La Mesa, Cundinamarca. Teléfono 8471213
usuario@aguasdeltequendama.com
info@aguasdeltequendama.com

Oficina PQR Anapoima - Cundinamarca. Carrera 3 # 1- 41 Sur San José
Celular PQR 3142807615
pqranoima@aguasdeltequendama.com
www.aguasdeltequendama.com



Empresa Regional Aguas del Tequendama S.A. E.S.P.
Anapoima – La Mesa

INTRODUCCION

con el fin de garantizar el manejo eficaz de la información con la cual trabaja la EMPRESA REGIONAL AGUAS DEL TEQUENDAMA S.A. E.S.P por medio de los equipos, aplicaciones informáticas y demás medios con los cuales interactúan diariamente los funcionarios y usuarios en general, se hace necesario identificar y gestionar las actividades que se relacionan con la Seguridad de la Información.

Esto se logra por medio de un Sistema de Gestión de Seguridad de la Información acorde con referentes nacionales e internacionales como la norma ISO 27001:2013, que permite la evaluación de riesgos, el establecimiento de controles, la evaluación de la conformidad de las partes interesadas, tanto internas como externas y contribuye en la ejecución de un plan de continuidad de negocio, de tratamiento de incidentes y de contingencia que son vitales para la institución, como medida preventiva ante cualquier eventualidad a la cual se pueda ver expuesta. Este Sistema de Gestión de Seguridad de la Información además permite el fortalecimiento de los procesos por medio del diseño, implementación y reevaluación de la seguridad, lo cual arroja como resultado el mejoramiento continuo gracias a la adopción del modelo PHVA (Planear-Hacer- Verificar- Actuar).

Para LA ERAT S.A E.S.P como entidad de carácter público, del orden territorial, cuyo objetivo principal es la prestación y/o operación y/o administración y/o distribución y/o comercialización de los servicios públicos domiciliarios de acueducto, alcantarillado y aseo de los municipios de la Mesa y Anapoima, es importante y requerido para su operación el contar con un estándar de Seguridad de la Información acordes, este estándar ayudará a mantener un sistema coherente con los procesos de la entidad en beneficio de la comunidad.

Para lograr este objetivo, las políticas aquí definidas brindan las herramientas necesarias para que los funcionarios, contratistas y terceros que hacen parte del Sistema de Gestión de Seguridad de la Información (SGSI en adelante) de LA ERAT S.A E.S.P, puedan adoptar los controles requeridos para asegurar la información, gestionar con eficiencia los riesgos de seguridad y mejorar continuamente el SGSI, ello solo es posible a través de la integración de políticas, procedimientos, sistemas de información y controles con un fin común: gestionar de manera pertinente y eficaz los riesgos, de tal forma que las partes interesadas obtengan un alto nivel de seguridad y confianza; Se entiende, por lo tanto, que las políticas deben ser plenamente conocidas y cumplidas por los funcionarios, contratistas y terceras partes que tienen acceso a los activos de información y a los sistemas de procesamiento de información de LA ERAT S.A E.S.P., en este sentido, es indispensable que sus esfuerzos y capacidades se concentren en lograr los fines primordiales de las políticas, como son: generar controles para proteger los activos de información; crear conciencia en los usuarios acerca del uso responsable de las tecnologías de la información y comunicaciones y realizar una gestión de riesgos adecuada que permita minimizar el impacto frente a un eventual caso de materialización.

Señe Administrativa y PQR:

Diagonal 8 No. 1 – 37 Barrio Quintas de San Pablo
La Mesa, Cundinamarca. Teléfono 8471213
usuario@aguasdeltequendama.com
info@aguasdeltequendama.com

Oficina PQR Anapoima - Cundinamarca. Carrera 3 # 1- 41 Sur San José
Celular PQR 3142807615

pqranoima@aguasdeltequendama.com
www.aguasdeltequendama.com



PLATAFORMA ESTRATÉGICA

Misión

Prestar los Servicios Públicos de Acueducto, Alcantarillado y Aseo en los Municipios de La Mesa y Anapoima, aplicando como principios el compromiso y la eficiencia, contribuyendo al mejoramiento de la calidad de vida de nuestros usuarios.

Visión

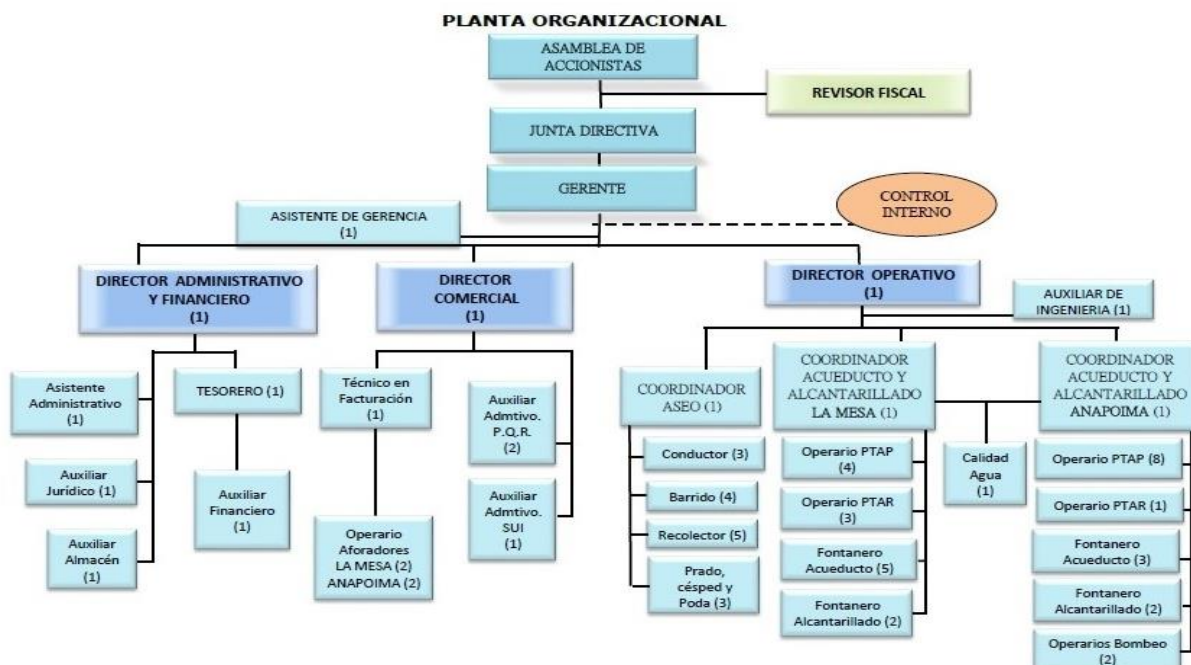
En el año 2035, La Empresa Regional Aguas del Tequendama S.A. E.S.P, será una Empresa líder y reconocida en la prestación de los Servicios Públicos de Acueducto, Alcantarillado y Aseo, cumpliendo estándares de calidad, continuidad y eficiencia, siendo referente en la región aplicando políticas de protección ambiental y desarrollo sostenible.

PRINCIPIOS Y VALORES INSTITUCIONALES

- ❖ **RESPONSABILIDAD:** Es un valor ético que implica el compromiso de los directivos y funcionarios de LA ERAT S.A E.S.P., en el cumplimiento de sus funciones y actividades establecidas en la normatividad vigente, en los estatutos de la empresa, en el reglamento interno de trabajo y en el código de ética encaminados a fortalecer la Misión de la empresa y satisfacer las expectativas de los grupos de interés: Clientes, accionistas, proveedores y sociedad en general y la conservación del medio ambiente.
- ❖ **TRABAJO EN EQUIPO:** Es un comportamiento pilar en LA ERAT S.A E.S.P, que busca siempre el crecimiento personal, permitiendo así que sus funcionarios adopten conductas de armonía y trabajo en equipo para una vida laboral saludable.
- ❖ **EFICACIA Y EFICIENCIA:** Estamos dispuestos a cumplir oportunamente nuestro compromiso de prestar los servicios públicos de acueducto, alcantarillado, aseo y alumbrado públicos a la comunidad bajo los principios de austeridad, integridad racionalidad, honestidad y transparencia.
- ❖ **SENTIDO DE PERTENENCIA:** Es un comportamiento pilar en LA ERAT S.A E.S.P, que busca siempre el crecimiento personal, permitiendo así que sus funcionarios adopten conductas de armonía y trabajo en equipo para una vida laboral saludable
- ❖ **LIDERAZGO:** Estamos comprometidos en dar ejemplo, influyendo positivamente en el trabajo de los demás, generando resultados exitosos.

- ❖ **CREATIVIDAD:** Nuestra capacidad de generar nuevas ideas, acciones y estrategias novedosas, nos permite transformar nuestro entorno por medios de soluciones originales a los problemas.
- ❖ **EXCELENCIA:** Perseguimos incasablemente el éxito en lo que hacemos, por lo que nos exigimos a diario para ofrecer un servicio con calidad.

ESTRUCTURA ORGANIZACIONAL



DESCRIPCIÓN DE LA ESTRUCTURA ORGÁNICA

Empresa Regional Aguas del Tequendama S.A E.S.P

Asamblea de Accionistas: Órgano de administración y fiscalización dentro de la sociedad anónima, donde se toman las decisiones clave funcionamiento de la sociedad.

Revisor Fiscal: Delegatario de los socios para ejercer inspección permanente a la administración y validar los informes que está presente, debiendo rendir informes a los mismos en las reuniones estatutarias.



Empresa Regional Aguas del Tequendama S.A. E.S.P.
Anapoima – La Mesa

Gerente: Planear, organizar, integrar dirigir y controlar las actividades generales de la Empresa, velando por el cumplimiento de su plan estratégico, implementando herramientas administrativas, financieras y operativas que redunden en el desarrollo y optimización de la Empresa, en concordancia con sus planes administrativos y operativos, representando legalmente a la entidad ante los diferentes organismos de vigilancia, control y regulación.

Control Interno: Asesorar, dirigir, organizar, formular políticas y adoptar planes, programas y proyectos para la implementación y manejo adecuado del Sistema de Control Interno de la entidad.

Director Administrativo y Financiero: Planear, organizar, integrar dirigir y controlar las actividades administrativas y financieras de la Empresa, coordinando sus funciones con la Gerencia General y las demás Áreas, procurando la oportuna consecución y adecuado manejo custodia de los valores y medios de pago de la Empresa.

Director Comercial: Planear, organizar, integrar dirigir y controlar las actividades comerciales relacionadas con los procesos de facturación de la Empresa, coordinando sus funciones con la Gerencia General y demás Áreas.

Director Operativo: Planear, organizar, integrar dirigir y controlar las actividades técnicas y operativas de la Empresa, coordinando sus funciones con la Gerencia y las demás Áreas, ejecutando adecuadamente los procesos que garanticen la correcta prestación de los servicios de acueducto, alcantarillado y aseo a cargo de la Empresa.

JUSTIFICACIÓN

En la actualidad, la seguridad en la información es una de las preocupaciones más grandes que puede llegar a tener una compañía, ya que se refiere a garantizar la calidad, disponibilidad, veracidad y confidencialidad de su activo más preciado: la información.

La información es un activo que, como otros activos comerciales importantes, es esencial para el negocio de una organización y en consecuencia necesita ser protegido adecuadamente. Esto es especialmente importante en el ambiente comercial cada vez más interconectado. Como resultado de esta creciente interconectividad, la información ahora está expuesta a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades.

Hoy en día las empresas que manejen sistemas de información han generado la necesidad del aseguramiento de la información, generando políticas y controles, buscando garantizar la estabilidad y confiabilidad de la información, proyectándose ser



reconocidas a nivel nacional como internacional, teniendo buena credibilidad y ubicándose siempre en los primeros lugares.

Teniendo en cuenta la obligatoriedad de cumplimiento de lo definido en la estrategia de Gobierno en Línea, y el conjunto de normativas que rigen al respecto, además de la situación actual del sistema de información y los servicios tecnológicos de Empresa Regional Aguas del Tequendama S.A E.S.P, se hace necesario levantar una línea de base sobre la cual se articulen diferentes esfuerzos encaminados a ofrecer la seguridad en la información, teniendo en cuenta las distintas amenazas y vulnerabilidades que pueden comprometer la integridad de los datos, en las redes, en los servicios y demás herramientas tecnológicas dispuestas para tal fin.

Es importante aclarar que este proyecto se encamina a formar las bases para una declaratoria de lineamientos progresivamente aplicables que vayan dando forma al Plan de Seguridad Informática partiendo desde las copias de seguridad, su protección, integridad, restricción de acceso y demás elementos a tener en cuenta.

Los principales beneficiarios son en primera medida la Alta Dirección, ya que se ofrecerá disponibilidad y veracidad en la información que se usa para la toma de decisiones. Por otra parte, los usuarios finales del sistema de información que alimentan y requieren de agilidad y seguridad al momento de ingresar información que puede o no ser pública, a través de los servicios tecnológicos de la entidad.

OBJETIVO GENERAL

Planificar, orientar y desarrollar los mecanismos necesarios para dotar de disponibilidad, confidencialidad e integridad al conjunto de datos y activos de información de la Entidad.

OBJETIVOS ESPECÍFICOS

- ❖ Formular el esquema de seguridad de la información de acuerdo a las necesidades del Sistema de Información de LA ERAT S.A E.S.P.
- ❖ Instaurar medidas de control de acceso a los activos de información de LA ERAT S.A E.S.P
- ❖ Alinear a la normatividad vigente las políticas de gestión y administración de activos de información de LA ERAT S.A E.S.P
- ❖ Establecer las acciones, documentos, procedimientos y responsabilidades frente a la garantía de la seguridad de la información en LA ERAT S.A E.S.P.
- ❖ Proyectar la implementación del presente plan junto con sus actividades y documentos relacionados.
- ❖ Fortalecer la seguridad de la información, además de promover y mantener la confianza de los funcionarios, contratistas y terceros, mediante el desarrollo,

- implementación y cumplimiento de las políticas y procedimientos establecidos dentro del SGSI.
- ❖ Cumplir con los principios de confidencialidad, disponibilidad e integridad de la información, garantizando la protección de los activos de información de LA ERAT S.A E.S.P
 - ❖ Apoyar el cumplimiento de los principios de la función administrativa correspondientes a la legalidad, economía, eficacia, contradicción y publicidad, a través de los lineamientos establecidos por el SGSI.
 - ❖ Incentivar la cultura de la Seguridad y Privacidad de la Información fortaleciendo las buenas prácticas y la conciencia de los funcionarios, contratistas y terceros.
 - ❖ Gestionar los riesgos de seguridad de la información con el fin de evitar el impacto en los objetivos estratégicos de LA ERAT S.A E.S.P, en especial, en aquellos que afecten los procesos misionales.
 - ❖ Garantizar la continuidad del negocio mediante la implementación de planes y controles que sea necesario desarrollar frente a la existencia de incidentes de seguridad de la información.
 - ❖ Apoyar las innovaciones y proyectos tecnológicos que garanticen los niveles de seguridad de la información previstos por la Entidad.

TÉRMINOS Y DEFINICIONES

- ❖ **Activo:** en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.
- ❖ **Amenaza:** causa potencial de un incidente no deseado, que pueda provocar daños a un sistema o a la organización.
- ❖ **Amenaza informática:** la aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado (Ministerio de Defensa de Colombia).
- ❖ **Análisis de riesgos:** proceso que permite comprender la naturaleza del riesgo y determinar su nivel de riesgo.
- ❖ **Anonimización del dato:** eliminar o sustituir algunos nombres de personas (físicas o jurídicas); direcciones y demás información de contacto, como números identificativos, apodos o cargo.
- ❖ **Autenticación:** provisión de una garantía de que una característica afirmada por una entidad es correcta.
- ❖ **Autenticidad:** propiedad de que una entidad es lo que afirma ser. (ISO 27000.es, 2012).
- ❖ **Ciberseguridad:** capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

- ❖ **Ciberspacio:** ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701).
- ❖ **Confidencialidad:** propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- ❖ **Control:** comprenden las políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control también es utilizado como sinónimo de salvaguarda o contramedida, es una medida que modifica el riesgo.
- ❖ **Custodio de activo de información:** identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de administrar y hacer efectivo los controles que el propietario del activo haya definido, con base en los controles de seguridad disponibles en la entidad.
- ❖ **Datos abiertos:** son datos primarios o sin procesar puestos a disposición de cualquier ciudadano, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.
- ❖ **Datos biométricos:** parámetros físicos únicos de cada persona que comprueban su identidad y se evidencian cuando la persona o una parte de ella interacciona con el sistema (huella digital o voz).
- ❖ **Datos personales sensibles:** se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos.
- ❖ **Dato privado:** es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.
- ❖ **Dato público:** es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas.
- ❖ **Dato semiprivado:** es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.
- ❖ **Disco duro:** disco de metal cubierto con una superficie de grabación ferro magnético. Haciendo una analogía con los discos musicales, los lados planos de la placa son la superficie de grabación, el brazo acústico es el brazo de acceso y la púa (aguja) es la cabeza lectora/grabadora. Los discos magnéticos pueden ser grabados, borrados y re-grabados como una cinta de audio.
- ❖ **Disponibilidad:** propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

- ❖ **DVD:** Disco Versátil (video) Digital. En la actualidad constituye el natural sucesor del CD para la reproducción de sonido e imagen de calidad.
- ❖ **Evento de seguridad de la información:** ocurrencia identificada de estado en un sistema de información, servicio o red que indica una posible brecha de seguridad, falla de un control o una condición no identificada que puede ser relevante para la seguridad de la información.
- ❖ **Gestión de claves:** son controles que realizan mediante la gestión de claves criptográficas.
- ❖ **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.
- ❖ **Gestión de riesgos:** actividades coordinadas para dirigir controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.
- ❖ **Habeas data:** derecho a acceder a la información personal que se encuentre en archivos o bases de datos; implica la posibilidad de ser informado acerca de los datos registrados sobre sí mismo y la facultad de corregirlos.
- ❖ **Impacto:** el coste para la empresa de un incidente “de la escala que sea”, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.
- ❖ **Incidente de seguridad de la información:** evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- ❖ **Información:** La información está constituida por un grupo de datos ya supervisados y ordenados, que sirven para construir un mensaje basado en un cierto fenómeno o ente. La información permite resolver problemas y tomar decisiones, ya que su aprovechamiento racional es la base del conocimiento.
- ❖ **Integridad:** la propiedad de salvaguardar la exactitud y complejidad de la información.
- ❖ **Inventario de activos:** lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos. (ISO 27000.es,2012).
- ❖ **No repudio:** servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido). (ISO-7498-2).
- ❖ **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 continuidad 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.

- ❖ **Proceso:** conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas. (ISO 27000.es, 2012).
- ❖ **Propietario de activo de información:** identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información asignados.
- ❖ **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 consideraciones. (ISO Guía 73:2002).
- ❖ **Responsable del tratamiento:** persona natural o jurídica. Pública o privada. Que por sí misma o en asocio con otros. Decida sobre la base de datos y/o el Tratamiento de los datos.
- ❖ **Segregación de tareas:** reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.
- ❖ **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, basando en un enfoque de gestión y de mejora a un individuo o entidad.
- ❖ **Titular de la información:** es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de hábeas data y demás derechos y garantías a que se refiere la presente ley.
- ❖ **Trazabilidad:** cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.
- ❖ **Vulnerabilidad:** debilidad de un activo o control que pueda ser explotado por una o más amenazas. (ISO 27000.es, 2012).

MARCO NORMATIVO

El Sistema de Gestión de Seguridad de la Información de la Empresa Regional Aguas del Tequendama S.A E.S.P. se ciñe a la normatividad legal vigente colombiana, tal como se describe enseguida:

- ❖ Ley 527/99: Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos
 - ❖ Ley 594/00: Por medio de la cual se dicta la Ley General de Archivo y se dictan otras disposiciones.
 - ❖ La Ley 850/03 establece en su artículo 9º: Principio de Transparencia
 - ❖ Ley 1266/08: Por la cual se dictan 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
 - ❖ Ley 1221 de 2008: Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones
 - ❖ Ley 1273/09: Por medio de la cual 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.
 - ❖ CONPES 3701 de 2011: Lineamientos de política para ciberseguridad y Ciberdefensa
 - ❖ Resolución 2886 de 2012: Por la cual se definen las entidades que harán parte de la Red Nacional de Fomento al Teletrabajo y se dictan otras disposiciones.
 - ❖ Ley 1581/12: Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales
 - ❖ Decreto 884 de 2012: Por medio del cual se reglamenta la Ley 1221 de 2008 y se dictan otras disposiciones.
 - ❖ Decreto 886 de 2014: Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, en lo relativo al
- Registro Nacional de bases de datos.
- ❖ En el Decreto Nacional 2573 de 2014: Estrategia de Gobierno en Línea de la República de Colombia
 - ❖ LEY 1712 DE 2014: Ley de Transparencia y del Derecho de Acceso a la Información Pública
 - ❖ Decreto 103 de 2015: Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones

PLAN GENERAL DE SEGURIDAD DE LA INFORMACIÓN

El Plan de seguridad es un documento de alto nivel que denota el compromiso de la Empresa Regional Aguas del Tequendama S.A E.S.P con la seguridad de la información; Este Plan contribuye a minimizar los riesgos asociados a daños, proyecta la eficiencia administrativa y asegura el cumplimiento de las funciones misionales de la entidad apoyada en el uso adecuado de TICs.

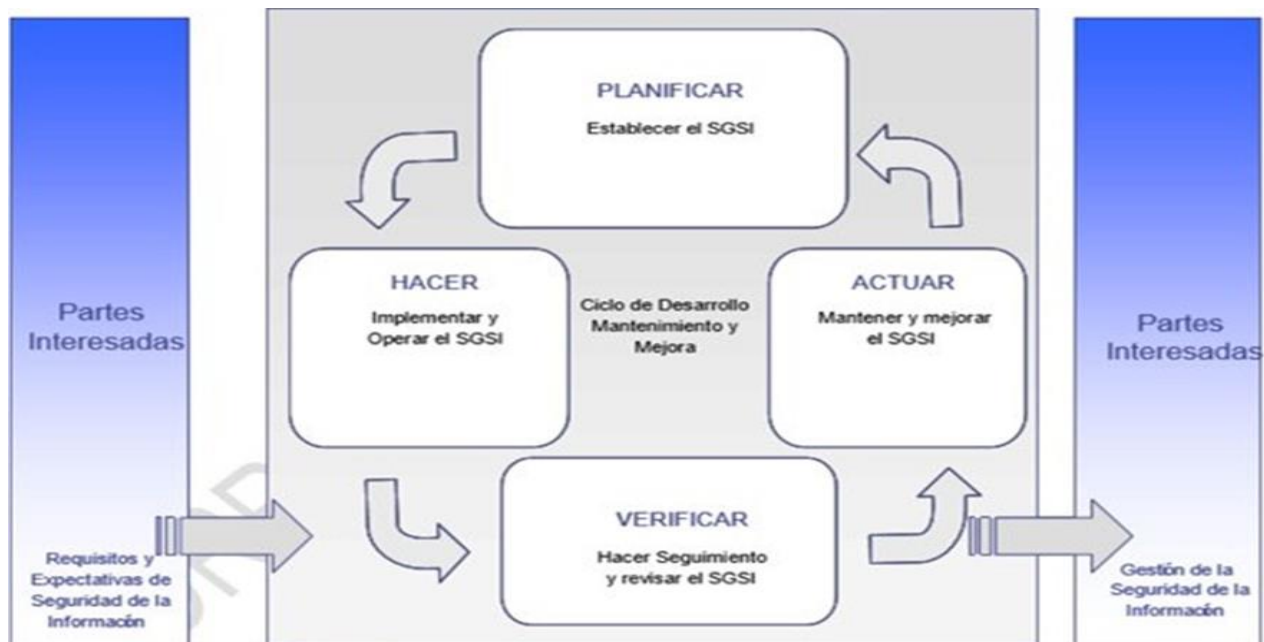
DETALLE:

La Empresa Regional Aguas del Tequendama S.A E.S.P debe salvaguardar las características de integridad, disponibilidad y confidencialidad de la seguridad de la información, mediante la adopción de políticas y procedimientos institucionales orientadas al logro de sus objetivos estratégicos, en estricto cumplimiento de las normas vigentes; De este modo, la empresa velará por la adecuada gestión de los riesgos, la adopción de buenas prácticas en el uso de los activos de información y la mejora continua de las competencias del talento humano.

La eficiencia de la política de seguridad de la información se construye a través del liderazgo y compromiso de la Alta Dirección y la participación activa de los funcionarios, contratistas y terceros, quienes mancomunadamente deberán alcanzar el nivel de cumplimiento según los lineamientos y requisitos de seguridad de la información determinados aquí, así como el desarrollo de estrategias de mejora continua y gestión oportuna frente a incidentes o eventos de seguridad de la información.

METODOLOGÍA PARA LA IMPLEMENTACIÓN DEL PROYECTO

El modelo a implementar es el ciclo Deming o ciclo PHVA, como metodología para la mejora continua.



ACTIVIDADES SEGÚN LINEAMIENTOS PARA LA IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD DE LA INFORMACIÓN

Una vez la entidad ha logrado alinearse con el SGSI entra en el ciclo PHVA	LINEAMIENTO 1. IDENTIFICAR EL NIVEL DE MADUREZ EN S.I
	FASE 1. Preparación <ul style="list-style-type: none"> - Plan de capacitación - Conformación Equipo de Gestión del Proyecto
	FASE 2. Análisis situación actual y definición de brechas. <ul style="list-style-type: none"> - Diseñar y aplicar encuesta de seguridad. - Definir nivel de madurez: Realizar autoevaluación con respecto a los niveles de seguridad. - Definición de brechas:
	Revisión de estructura organizacional. Revisión por niveles de madurez de acuerdo a los requisitos del manual de GEL.Revisión de controles de SI (Existentes y ausentes). Definir el estado actual de SI de la entidad. Definición del plan o cronograma a seguir para disminuir la brecha y alinearse con el nivel de madurez adecuado.
	FASE 3. Alineación con el Sistema de Gestión de Seguridad de la Información SGSI. <ul style="list-style-type: none"> - Ejecución del Programa para la reducción de la brecha.
PLANEAR	LINEAMIENTO 2. LLEVAR A LA ENTIDAD A UN NIVEL DE MADUREZ INICIAL EN SEGURIDAD.
	FASE 1. Actividades Lineamientos Nivel Inicial <ul style="list-style-type: none"> - Obtener soporte de la Dirección de la entidad. - Identificar legislación y normatividad aplicable. - Definir el alcance del SGSI “SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN” - Definir la Política de la Seguridad de la información. - Realizar el análisis de riesgo: Definir la aproximación para la Gestión del Riesgo.Realizar la identificación de Activos. Identificar los riesgos Analizar el riesgo en contexto de los objetivos de la entidad y partes interesadas. - Selección de Controles. - Plan de Tratamiento del riesgo. - Generar el DDA - Declaración de aplicabilidad.



HACER	LINEAMIENTO 3. LLEVAR A LA ENTIDAD A UN NIVEL DE MADUREZ BÁSICO EN SEGURIDAD.
	FASE 1. Actividades Lineamientos Nivel Avanzado. - Implementar el plan de tratamiento del riesgo. - Documentar los controles del SGSI: Definir métricas y medidas para medir el desempeño del SGSI. - Implementar políticas y controles de seguridad de la fase de planeación. - Implementar los planes de concientización y entrenamiento. - Establecer y gestionar la operación del SGSI y sus recursos.
VERIFICAR	LINEAMIENTO 4. LLEVAR A LA ENTIDAD A UN NIVEL DE MADUREZ AVANZADO EN SEGURIDAD.
	FASE 1. Actividades Lineamientos Nivel Avanzado. - Ejecutar plan operacional. - Revisiones regulares de eficacia: Monitorear y revisar políticas, estándares, procedimientos y prácticas. Revisar la eficacia de las operaciones de seguridad usando métricas y mediciones.
	- Revisar el nivel del riesgo residual. - Realizar Auditorías internas. - Realizar Auditorías externas. - Revisión de la dirección del SGSI. - Registro del impacto en el SGSI.

ACTUAR	LINEAMIENTO 5. LLEVAR A LA ENTIDAD A UN NIVEL DE MADUREZ DE MEJORAMIENTO PERMANENTE EN SEGURIDAD.
	<p>FASE 1. Actividades Lineamientos Nivel Mejoramiento Permanente.</p> <ul style="list-style-type: none"> - Implementar las mejoras identificadas y aprobadas al SGSI en un nuevo ciclo. - Tomar medidas preventivas y correctivas. - Aplicar las lecciones aprendidas. - Comunicar los resultados. - Proceso continuo y Gestión auto sostenible del modelo de las entidades: <p>Revisión de Política de Seguridad. Verificación del alcance del conjunto de políticas en la entidad. Revisión de los activos de información de la entidad. Revisión del riesgo residual. Recopilación y análisis de los indicadores del modelo. Análisis de estadísticas de incidentes de seguridad de la información en entidades del Estado. Implementación de los ajustes.</p>

Posterior a la revisión de cumplimiento de los lineamientos, se debe verificar el nivel de madurez del CGSI.






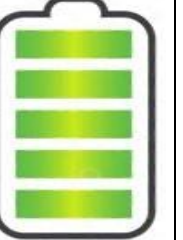
“Componente de Gestión de Seguridad de la Información”, de acuerdo a como se describe a continuación:

MODELO DE MADUREZ

NIVEL	DESCRIPCION
INEXISTENTE	<ul style="list-style-type: none"> - Se han implementado controles en su infraestructura de TI, seguridad física, seguridad de recursos humanos entre otros, sin embargo, no están alineados a un Modelo de Seguridad. - No se reconoce la información como un activo importante para su misión y objetivos estratégicos. - No se tiene conciencia de la importancia de la seguridad de la información en las entidades.



INICIAL	<ul style="list-style-type: none">- Se han identificado las debilidades en la seguridad de la información.- Los incidentes de seguridad de la información se tratan de forma reactiva.- Se tiene la necesidad de implementar el MSPI “MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN”, para definir políticas, procesos y procedimientos que den respuesta proactiva a las amenazas sobre seguridad de la información que se Presentan en la Entidad.
REPETIBLE	<ul style="list-style-type: none">- Se identifican en forma general los activos de información.- Se clasifican los activos de información.- Los servidores públicos de la entidad tienen conciencia sobre la seguridad de la información.- Los temas de seguridad y privacidad de la información se tratan en los comités del modelo integrado de gestión.
ADMINISTRADO	<ul style="list-style-type: none">- La Entidad ha realizado un diagnóstico que le permite establecer el estado actual de la Seguridad de la información.- La Entidad ha determinado los objetivos, alcance y límites de la seguridad de la información.- La Entidad ha establecido formalmente políticas de Seguridad de la información y estas han sido divulgadas.- La Entidad tiene procedimientos formales de seguridad de la Información.- La Entidad tiene roles y responsabilidades asignados en seguridad y privacidad de la información.- La Entidad ha realizado un inventario de activos de información aplicando una metodología.- La Entidad trata riesgos de seguridad de la información a través de una metodología.- Se implementa el plan de tratamiento de riesgos.
OPTIMIZADO	<ul style="list-style-type: none">- En este nivel se encuentran las entidades en las cuales la seguridad es un valor Agregado para la organización.- Se utilizan indicadores de efectividad para establecer si la entidad encuentra retorno a la inversión bajo la premisa de mejora en el cumplimiento de los objetivos misionales.

NIVEL 0 INEXISTENTE	NIVEL 1 INICIAL	NIVEL 2 REPETIBLE	NIVEL 3 DEFINIDO	NIVEL 4 ADMINISTRADO	NIVEL 5 OPTIMIZADO
					
Desconoce o no tiene en cuenta el tema de seguridad de la información	Reconoce que tiene problemas de seguridad y que estos necesitan ser resueltos	Tiene procedimientos no formales de seguridad	En este nivel se Realizan las fases de: etapas previas a la Planificación e Implementación.	Ha realizado las fases de evaluación de desempeño y mejora continua	Encuentra, en la seguridad de la información un valor agregado para la entidad
MODELO NIVEL DE MADUREZ					

HERRAMIENTAS PARA LA EJECUCIÓN DEL PROYECTO

Finalmente, a continuación, se lleva a cabo una reseña de las principales características de la norma ISO/IEC 27001:2013, la cual se ha seleccionado como estándar para la implementación y mantenimiento del CGSI dentro La Empresa Regional Aguas del Tequendama S.A E.S.P

Objetivos de control:

Políticas de seguridad de la Información:

Establece la necesidad de definir un conjunto de políticas aplicadas a todas las actividades relacionadas con la gestión de la seguridad de la información dentro de la Organización, con el propósito de proteger la misma contra las amenazas presentes en el entorno.

Organización de la seguridad de la información:

Sugiere diseñar una estructura para la gestión de la seguridad de la información dentro la Organización que establezca los roles y responsabilidades con la seguridad de la información a lo largo de la misma.



Seguridad del Recurso Humano:

Establece la necesidad de educar e informar a los empleados actuales y potenciales sobre lo que se espera de ellos en materia de seguridad y confidencialidad de la información que manejan.

También determina cómo incide el papel que desempeñan los empleados como responsables de la seguridad de la información.

Gestión de Activos:

Detalla los elementos de la Organización (servidores, PCs, medios magnéticos, información impresa, documentos, etc.), que deben ser considerados para establecer un mecanismo de seguridad que permita garantizar un nivel adecuado de protección.

Control de acceso:

Establece la importancia de monitorear y controlar el acceso a la red y los recursos de aplicación para protegerlos contra los abusos internos e intrusos externos; Asimismo, establece los diferentes tipos de accesos o privilegios a los recursos informáticos (sistema operativo, aplicaciones, correo electrónico, Internet, comunicaciones, conexiones remotas, etc.) que requiere cada empleado de la Organización y el personal externo que brinda servicios, en concordancia con sus responsabilidades.

Esto permitirá identificar y evitar acciones o actividades no autorizadas, garantizando los servicios informáticos.

Cifrado:

Garantiza el uso adecuado y eficaz del cifrado para proteger la confidencialidad, autenticidad y/o integridad de la información.

Seguridad física y ambiental:

Responde a la necesidad de proteger las áreas, los equipos y los controles generales. El objetivo principal es la prevención de accesos no autorizados a las instalaciones de la Organización, con especial atención a todos los sitios en los cuales se procesa información (centros de cómputo, PC de usuarios críticos, equipos de los proveedores de servicios, etc.), y áreas en las cuales se recibe o se almacena información (magnética o impresa) sensible (fax, áreas de envío y recepción de documentos, archivadores, etc.), minimizando riesgos por pérdidas de información, hurto, daño de equipos y evitando la interrupción de las actividades productivas.



Empresa Regional Aguas del Tequendama S.A. E.S.P.
Anapoima – La Mesa

Seguridad de las operaciones:

Define las políticas, procedimientos y responsabilidades para asegurar la correcta operación de las instalaciones de procesamiento de información.

Seguridad de las comunicaciones:

Define las políticas y procedimientos para asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información.

Adquisición, desarrollo y mantenimiento de los sistemas de información:

Establece la necesidad de implantar medidas de seguridad y aplicación de controles de seguridad en todas las etapas del proceso de desarrollo y mantenimiento de los sistemas de información. Además, considera los mecanismos de seguridad que deben implantarse en el proceso de adquisición de todos los sistemas o aplicaciones de la Organización, para prevenir pérdidas, modificaciones, o eliminación de los datos, asegurando así la confidencialidad e integridad de la información.

Relación con proveedores:

Permite asegurar la protección de los activos de información que son accedidos por proveedores.

Gestión de Incidentes de Seguridad:

Establece la necesidad de desarrollar una metodología eficiente para la generación, monitoreo y seguimiento de eventos e incidentes de seguridad aspectos de seguridad de la información en la gestión de la continuidad del negocio: Considera el análisis de todos los procesos y recursos críticos del negocio, y define las acciones y procedimientos a seguir en casos de fallas o interrupción de los mismos, evitando la pérdida de información y la no disponibilidad de los procesos productivos de la Organización, lo que podría provocar un deterioro de la imagen de la Organización, una posible pérdida de clientes o incluso una dificultad severa que impida continuar operando.



CUMPLIMIENTO

Imparte instrucciones a las organizaciones para que verifiquen si el cumplimiento con la norma técnica ISO/IEC 27002:2013, concuerda con otras leyes, reglamentos, normatividad y obligaciones contractuales o cualquier requerimiento de seguridad, tales como propiedad intelectual, auditorías, contrato de servicios, entre otros. Esta sección también requiere una revisión a las políticas de seguridad, al cumplimiento y las consideraciones técnicas; asimismo, busca garantizar que las políticas de seguridad y privacidad de la información sean acordes a la infraestructura tecnológica de la Organización.

APROBACIÓN

	ELABORADÓ POR	REVISADÓ POR	APROBADÓ POR
NOMBRE	DANIEL FELIPE SUÁREZ MONTILLA	DORA ALICIA DÍAZ TORRES	JOSÉ WILLIAM TEJEDOR BAYONA
CARGO	ASESOR MIPG	DIRECTORA ADMINISTRATIVA Y FINANCIERA	GERENTE
FIRMA	FIRMADO EN ORIGINAL	FIRMADO EN ORIGINAL	FIRMADO EN ORIGINAL
FECHA	31 DE ENERO DEL 2023	31 DE ENERO DEL 2023	31 DE ENERO DEL 2023