PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CONTENIDO

1. INTRODUCCIÓN

Con el fin de garantizar el manejo eficaz de la información con la cual trabaja la EMPRESA DE SERVICIOS PÚBLICOS PUBLICOS DE DAGUAS S.A E.P. S 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.

Este Sistema de Gestión de Seguridad de la Información además permite el fortalecimiento de los procesos por medio del diseño, implementación y revaluación de la seguridad, lo cual arroja como resultado el mejoramiento continuo gracias a la adopción del modelo PHVA (Planear-Hacer- Verificar- Actuar).

Para DAGUAS S.A E.S.P como entidad de carácter público, del orden municipal , 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 del municipio de Carmen de Apicalá Tolima, 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 DAGUAS 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.

2. PLATAFORMA ESTRATEGICA

2.1. MISION

La prestación de los Servicios Públicos Domiciliarios de Acueducto, Alcantarillado y Aseo, teniendo como principales objetivos la calidad y la continuidad en la prestación del servicio, con especial protección del medio ambiente, aplicando los principios de eficiencia, eficacia y ética, con un sistema tarifario justo, mejorando la cobertura para contribuir en el desarrollo de la comunidad, la empresa y nuestro talento humano.

2.2. VISION

La empresa se ha proyectado para consolidarse buscando ser líder en la prestación de Servicios Públicos de Acueducto, Alcantarillado y Aseo; en desarrollo de la imagen corporativa y como ejemplo regional dentro de los principios de Eficiencia, Eficacia y Transparencia, con calidad y responsabilidad destacándose por su rentabilidad, economía y control de recursos, creando sentido de pertenencia a nivel interno y externo.

2.3. PRINCIPIOS DE LA EMPRESA

Los principios éticos y rectores de la Empresa de Servicios Públicos de DAGUAS S.A. E.S.P." están adoptados mediante el documento "PRINCIPIOS Y VALORES INSTITUCIONALES – A.01.02.OD.09"

- **RESPONSABILIDAD:** Es un valor ético que implica el compromiso de los directivos y funcionarios de DAGUAS ES 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 la condición de trabajo utilizada por DAGUAS S.A. E.S.P. que más influye en los trabajadores de forma positiva porque

permite que haya un compañerismo, generando buenos resultados en las tareas asignadas

- **EFICIENCIA Y EFICACIA:** Estamos dispuestos a cumplir oportunamente nuestro compromiso de prestar los servicios públicos de acueducto, alcantarillado, aseos a la comunidad bajo los principios de austeridad, integridad racionalidad, honestidad y transparencia.

- **SENTIDO DE PERTENENCIA:** Es un comportamiento pilar en DAGUAS SA 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.

2.4. PRINCIPIOS GENERALES DE ATENCIÓN AL USUARIO

La Empresa observara los siguientes principios en la atención al usuario:

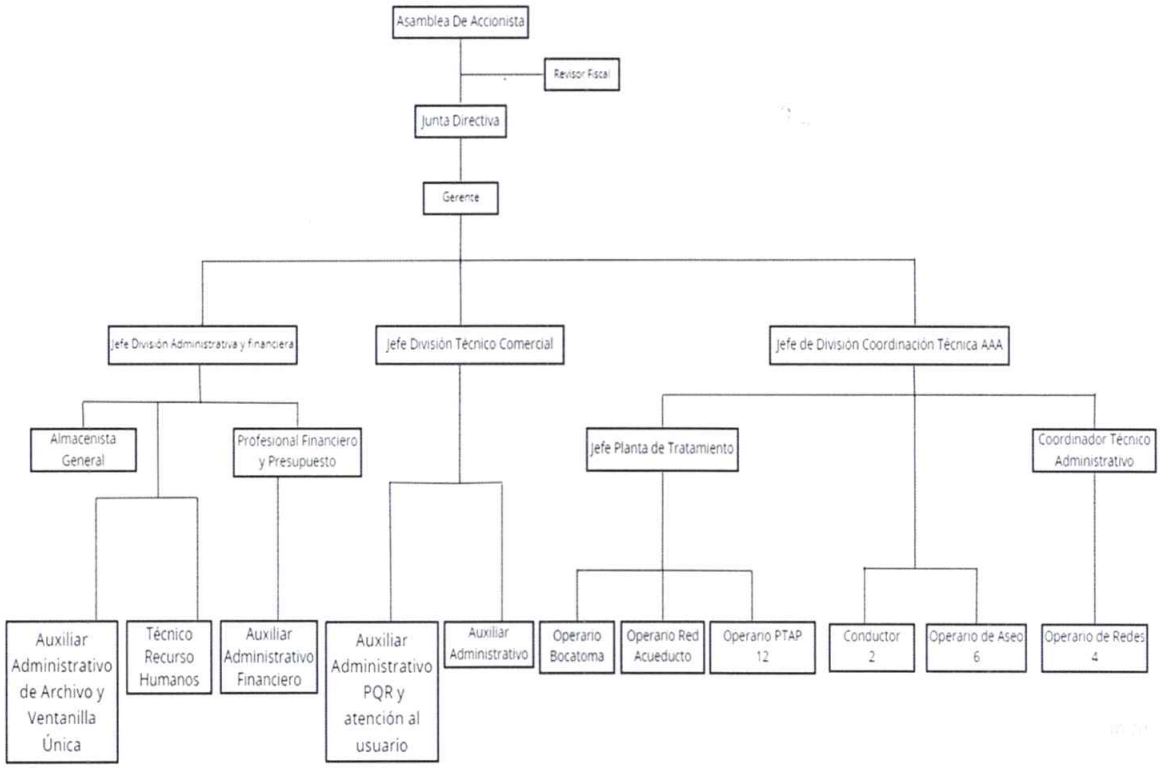
- **SERVICIO DE CALIDAD:** la Empresa y su personal deberá prestar un servicio con calidad y efectividad, basado en una administración abierta y accesible. Entendiéndose como un servicio con cortesía, objetividad e imparcialidad.

- **LEGALIDAD:** la Empresa actuara conforme a las normas y procedimientos fijados por la legislación de servicios públicos y la Normatividad vigente aplicable a la empresa.

- **IGUALDAD:** La empresa respetara el principio constitucional de la igualdad, garantizando el trato no discriminatorio a sus usuarios según los términos establecidos en la ley.

- **COHERENCIA:** la empresa será coherente en su conducta administrativa y operativa y cualquier excepción a este principio deberá justificarse debidamente.

2.5. ESTRUCTURA ORGANIZACIONAL



3. JUSTIFICACION

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 lanecesidad 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 LA EMPRESA DE SERVICIOS PUBLICOS DAGUAS 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 Plande Seguridad Informática partiendo desde las copias de seguridad, su protección,integralidad, restricción de acceso y demás elementos a tener en cuenta.

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.

4. 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.

5. OBJETIVOS ESPECÍFICOS

- Formular el esquema de seguridad de la información de acuerdo a las necesidadesdel Sistema de Información de DAGUAS S.A ESP.
- Instaurar medidas de control de acceso a los activos de información de DAGUAS S.A ESP
- Alinear a la normatividad vigente las políticas de gestión y administración de activosde información de DAGUAS S.A ESP
- Establecer las acciones, documentos, procedimientos y responsabilidades frente a la garantía de la seguridad de la información de DAGUAS S.A ESP.
- Proyectar la implementación del presente plan junto con sus actividades y documentos relacionados.
- Cumplir con los principios de confidencialidad, disponibilidad e integridad de la información, garantizando la protección de los activos de información de DAGUAS S.A ESP.

6. ALCANCE Y DELIMITACION DEL PLAN

El objetivo que se busca con la implementación de su SGSI es mejorar los niveles de seguridad de la información y la protección de los activos de información, para lograrlo sabe que es indispensable implementar los controles según lo señalado por el estándar ISO 27001:2013 y la normatividad vigente aplicable.

Por tal razón, los funcionarios, contratistas y terceros que interactúen con los activos de información de DAGUAS SA E.S.P, como ya se ha mencionado, deberán conocer y cumplir las políticas, procesos y procedimientos que hacen parte del SGSI, salvaguardando ante todo los principios de confidencialidad, integridad y disponibilidad que los protegen frente a cualquier tipo de tratamiento.

7. MARCO DE REFERNCIA Y ANTECEDENTES

En los últimos años, las entidades públicas tienden a mejorar la eficiencia, efectividad y eficacia de su gestión a partir de la reducción de costos por diferentes medios y buscando siempre la mejora del aprovechamiento de sus recursos, para lo cual buscan: optimizar sus procesos misionales, revisar y actualizar políticas de adquisición en la entidad, automatizar los procesos manuales, dinamizar la integración de los procedimientos de su sistema integrado de gestión, entre otros.

Esto se realiza a partir de los lineamientos de la Política Gobierno en Línea, en la cual se describen las características sobre las cuales debe enmarcarse la ejecución de todos estos objetivos.

Para la optimización de estos procesos se hace necesario utilizar las tecnologías de información de acuerdo a las necesidades de la entidad, teniendo en cuenta la visión, misión y estrategias que la alta dirección quiere implementar en la Entidad.

El Plan Estratégico de Tecnología de Información y comunicación (PETI) es un conjunto de políticas tecnológicas e iniciativas del área de sistemas que deben soportar la visión, misión y estrategias que DAGUAS SA E.S.P tiene, teniendo en cuenta que la razón de ser de las tecnologías de información son las áreas misionales de la entidad y por ende ambas perspectivas (misión y tecnología) deben estar alineadas y contar con mecanismos para facilitar este alineamiento.

De su mano, el Plan de Seguridad Informática debe constituirse como una línea de mando sobre la cual se establezcan los parámetros a seguir para garantizar su principal objetivo. A este se relacionan a su vez varios procedimientos, enfocándonos en el procedimiento de Copias de Seguridad.

8. TERMINOS 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 dañosa 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.
- **Anonimizarían del dato:** eliminar o sustituir algunos nombres de personas (físicaso 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.
- **Ciberespacio**: ámbito o espacio hipotético o imaginario de quienes se encuentraninmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701).
- **Confidencialidad:** propiedad de la información de no ponerse a disposición o serrevelada 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 administrary hacer efectivo los controles que el propietario del activo haya definido, con base en loscontroles 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

compruebansu 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 afectanla 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 relevantepara el titular.
- **Dato público:** es el dato calificado como tal según los mandatos de la ley o de laConstitución 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 sectoro 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 placason 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 yre-grabados como una cinta de audio.
- **Disponibilidad:** propiedad de la información de estar accesible y utilizable cuandolo 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 unsistema 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 lainformación.
- **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 quesu 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, serafectada 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 lasprincipales funciones misionales o del negocio en el caso de un evento imprevisto **Plan de tratamiento de riesgos:** documento que define las acciones para gestionar losriesgos de seguridad de la información inaceptables e implantar los controles necesariospara proteger la misma.
- **Proceso:** conjunto de actividades interrelacionadas o interactuantes quetransforman unas entradas en salidas. (ISO 27000.es, 2012).
- **Propietario de activo de información:** identifica a un individuo, un cargo, procesoo 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. Quepor sí misma o en asocio con otros. Decida sobre la base de datos y/o el Tratamiento delos 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 unao más amenazas. (ISO 27000.es, 2012).

9. MARCO NORMATIVO

- 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 regulael 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 sedictan otras disposiciones.
- Decreto 886 de 2014: Por el cual se reglamenta el artículo 25 de la Ley 1581 de2012, 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 InformaciónPública
- Decreto 103 de 2015: Por el cual se reglamenta parcialmente la Ley 1712 de 2014y se dictan otras disposiciones.

10. PLAN GENERAL DE SEGURIDAD DE LA INFORMACIÓN

El Plan de seguridad es un documento de alto nivel que denota el compromiso de la EMPRESA DE SERVICIOS PUBLICOS DAGUAS 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 apoyadas en el uso adecuado de TICS.

DETALLE:

La EMPRESA DE SERVICIOS PUBLICOS DAGUAS 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.

11. METODOLOGIA PARA LA IMPLEMENTACION DEL PROYECTO

12. 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 - Plan de capacitación - Conformación Equipo de Gestión del Proyecto
	FASE 2. Análisis situación actual y definición de brechas. - 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. - 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 - 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.
	LINEAMIENTO 3. LLEVAR A LA ENTIDAD A UN NIVEL DE MADUREZ BÁSICO EN SEGURIDAD.

HACER	**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 MADUREZAVANZADO 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.

	LINEAMIENTO 5. LLEVAR A LA ENTIDAD A UN NIVEL DE MADUREZ DE MEJORAMIENTO PERMANENTE EN SEGURIDAD.
ACTUAR	**FASE 1. Actividades Lineamientos Nivel Mejoramiento Permanente.** - 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: 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.

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	DESCRIPCIÓN
INEXISTENTE	- 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	- 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	- 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 delmodelo integrado de gestión.
ADMINISTRADO	- 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	- 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

13. HERRAMIENTAS PARA LA EJECUCION DEL PROYECTO

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 unmecanismo 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) sensitiva (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.

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.

OSCAR IVAN CARABALI COLLANTES
Gerente

MELIDA LEAL
Jefe de División
Administrativa y Financiera