DAGUAS
S.A. E.S.P. OFICIAL
Desempeño, competitividad y calidad de vida
Vigilado por la SSPD

2024

PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

EMPRESA DAGUAS S.A. E.S.P.

PRESENTADO POR
RECURSOS HUMANOS

3202330493
contacto@daguassa.gov.co
www.daguassa.gov.co

CONTENIDO

1. INTRODUCCION

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

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

El presente documento tiene como fin generar una cultura de prevención contra los riesgos a los que día a día se pudieran ver sometidos los activos de información de la EMPRESA DE SERVICIOS PÚBLICOS DAGUAS S.A ESP. Basados en un enfoque de planeación de gestión del riesgo se pretende realizar una estrategia que permita diagnosticar, evaluar, implementar y desarrollar la gestión de incidentes que afectan al activo de información e implantar unas contramedidas en el sistema de gestión informático para disminuir la probabilidad de su materialización.

El Manual de la política de Gobierno Digital expedido por el MinTIC establece que la política tiene como propósito promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un estado y ciudadanos competitivos, proactivos e innovadores, que generen valor público en un entorno de confianza digital.

la implementación de la política de gobierno digital se ha definido en dos componentes: TIC para el estado y TIC para la sociedad, que son habilitados por cuatro elementos transversales: Arquitectura, Cultura y Apropiación, Seguridad y Privacidad de la Información y Servicios Ciudadanos Digitales. Estos seis elementos, se desarrollan a través de lineamientos y estándares, que son requerimientos mínimos que todos los sujetos obligados deben cumplir para alcanzar los logros de la política.

Considerando que, la Resolución Ministerial 0500 de 2021, establece en su artículo 5,

denominado “Estrategia de Seguridad Digital”, en especial en el numeral 2, indicando que se debe “Contar con un análisis y tratamiento de riesgos de seguridad digital e implementar controles que permitan gestionarlos”, además, en la el anexo 1 de la misma Resolución, en su acápite “Planificación”, señala “Determinar las necesidades y objetivos de seguridad y privacidad de la información teniendo en cuenta su mapa de procesos, el tamaño y en general su contexto interno y externo. Esta fase define el plan de valoración y tratamiento de riesgos, siendo ésta la parte más importante del ciclo, teniendo el Plan de Tratamiento de Riesgos como el documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000), y en el mencionado anexo, en su numeral 7.3.3 Plan de tratamiento de los riesgos de seguridad de la información, tiene como lineamiento que la Entidad debe definir y aplicar un proceso de tratamiento de riesgos de la seguridad de la información.

2. INFORMACIÓN CONSTITUCIONAL

2.1. Misión

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.

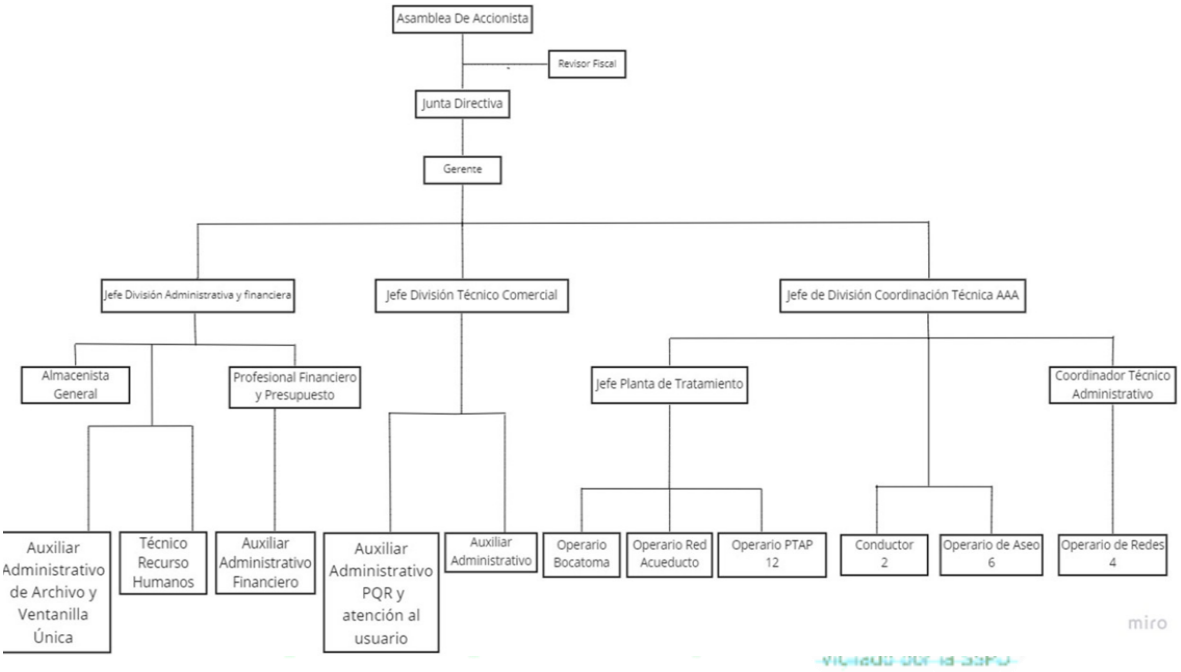
2.2. Visión

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. Objetivo

La actividad principal es la prestación de los servicios de Acueducto, Alcantarillado y Aseo, cumpliendo el objeto social con calidad y eficiencia, posicionarse como la mejor empresa del sector

3. ESTRUCTURA DE LA ORGANIZACIÓN



4. 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 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 LA EMPRESA DE SERVICIOS PUBLICOS DAGUAS SA E.S.P 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, integralidad, 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

5. OBJETIVO GENERAL

Establecer una guía metodológica para el adecuado tratamiento de los riesgos a los que están expuestos los activos de información de la EMPRESA DE SERVICIOS PUBLICOS DAGUAS S.A ESP, que permitan una adecuada toma de decisiones para disminuir la probabilidad que se materialice una amenaza o bien reducir la vulnerabilidad del sistema o el posible impacto en la Entidad, así como permitir la recuperación del sistema o la trasferencia del problema a un tercero.

6. OBJETIVOS ESPECÍFICOS

- Consolidar una administración de riesgos acorde con las necesidades de DAGUAS S.A ESP.
- Proteger los activos de información de DAGUAS S.A ESP acuerdo a su clasificación y criterios de Confidencialidad, Integridad y Disponibilidad
- Crear compromiso en los usuarios del proceso en la Formulación y desarrollo del presente plan en aras de la prevención y administración del riesgo de seguridad de la información.
- Crear conciencia a nivel institucional de la importancia y la necesidad de una correcta gestión del riesgo de seguridad de la información.

7. ALCANCE

- La guía metodológica contempla la implementación y la administración de la gestión del tratamiento riesgo de seguridad de la información en la EMPRESA DE SERVICIOS PUBLICOS DAGUAS S.A ESP, la cual será la pauta para desarrollar las actividades a través de la metodología PHVA (Planear – Hacer – Verificar - actuar) y las directrices de MINTIC.
- Lograr el compromiso de la EMPRESA DE SERVICIOS PUBLICOS DAGUAS S.A ESP para emprender la implementación del plan de gestión del riesgo en la seguridad de la información.
- Designar funciones de liderazgo para apoyar y asesorar el proceso de diseño e implementación del plan de gestión.

8. 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.

- **Anonimización de datos**: eliminar o sustituir algunos nombres de personas (físicas o jurídicas); direcciones y demás información de contacto, como númerosidentificativos, 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 naturalezacibernética.
- **Ciberespacio**: 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 hayadefinido, 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 crearservicios 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 vidasexual 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 públicay cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a ciertosector 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 sergrabados, 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 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 laseguridad 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 tratamientode 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 amenazarla 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 surecepción (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 imprevistoque 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 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 definirlos 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. Sueleconsiderarse como una combinación de la probabilidad de un evento y susconsideraciones. (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 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 objetivosde seguridad de la información y alcanzar dichos objetivos, basando en un enfoquede 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 datay 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

Guía de Gestión de riesgos. Guía No.7 (Seguridad y Privacidad de la Información) de MINTIC. “Todas las referencias a las políticas, definiciones o contenido relacionado, publicadas en la norma técnica colombiana NTC ISO/IEC 27001 vigente e ISO 27005 vigente, así como a los anexos con derechos reservados por parte de ISO/ICONTEC.”

Ley 1581 de 2012: “Por la cual se dictan disposiciones generales para la protección de datos personales”.

Ley 1712 de 2014: "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".

Decreto Presidencial 1083 de 2015: "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública", el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de "11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital".

Decreto Presidencial 612 de 2018: "Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado"

10. CONTEXTO

La implementación del Sistema de Gestión de Seguridad de la Información surge en el contexto de lo expuesto en el Decreto Presidencial 1008 de 2018 referido a las obligaciones de los sujetos obligados en el artículo 2.2.9.1.1.2. para la implementación del habilitador de seguridad de la información, en atención a las orientaciones definidas en el Manual de Gobierno Digital, relacionadas con la adopción e implementación del Modelo de Seguridad y Privacidad de la Información, refrendadas y actualizadas a través del Decreto Presidencial 767 de 2022 en lo referente al habilitador de seguridad y privacidad de la información, el cual derogo el Decreto 1008 de 2018.

De igual manera es importante resaltar que es a través del Decreto Presidencial 612 de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado", en su artículo 1, adiciona al Capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto Presidencial 1083 de 2015, Único Reglamentario del Sector de Función Pública, agregando al anterior Decreto el artículo 2.2.22.3.14, por medio del cual se integran los planes institucionales y estratégicos al Plan de Acción, considerando en su numeral 11 y 12 como obligación la elaboración anual del "Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información" y del "Plan de Seguridad y Privacidad de la Información" respectivamente de cada Entidad, y lo señalado en la Ley 1474 de 2011 por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública, señala en su artículo 74 denominado "Plan de acción de las entidades públicas", indicando que a partir de la vigencia de la presente Ley, todas las entidades del Estado a más tardar el 31 de

enero de cada año, deberán publicar en su respectiva página web el Plan de Acción para el año siguiente"

El desarrollo de las actividades para lograr su consecución estará sujeto a la disponibilidad de recursos (humanos, técnicos, tecnológicos, financieros) que faciliten el cumplimiento de las actividades; de acuerdo con la disponibilidad presupuestal oportuna, al apetito de riesgo institucional y a las orientaciones de la alta dirección, en cuanto al apetito de riesgo institucionales que han adoptado para afrontar el desarrollo y cumplimiento de las actividades planificadas.

Para el desarrollo de las actividades, la Empresa de Servicios DAGUAS S.A. E.S.P. contará con un equipo humano dispuesto para adelantar actividades de sensibilización, capacitación y atención de inquietudes a las dependencias adscritas a la entidad.

11. LAS RESPONSABILIDADES, LOS ROLES, LOS RECURSOS Y LA METODOLOGIA DE CARA A LA GESTION DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN.

LOS RESPONSABLES Y LOS ROLES

- **Los responsables de los procesos:** Identifican, analizan, evalúan y valoran los riesgos por lo menos una vez al año.

Los funcionarios en el desarrollo de sus actividades conocen e identifican cuales son los riesgos existentes por ende deben proponer estrategias para tratarlos y minimizar su impacto en la empresa.

- **La Dirección:** Aprueba las directrices para la administración del riesgo de la seguridad de la información de la entidad.
- **El proceso de Calidad.** En cuanto a la administración del riesgo en la entidad, orienta, coordina, y ajusta los requisitos normativos en El Sistema Integrado de gestión de la calidad.
- **Los Líderes del proceso de Planeación y Sistemas de Información:** Apoyan la gestión en cuanto a Liderazgo.
- **El Líder de Soporte Tecnológico**: Apoya la gestión en el desarrollo de las actividades.
- **Los Líderes SIG**. Apoyan la ejecución de las etapas de gestión del riesgo a nivel de los procesos.

- **Los funcionarios internos y Contratistas**: Son llamados a ejecutar los controles y acciones definidas para la administración de los riesgos con el fin de aportar en la identificación de posibles riesgos que puedan afectar la gestión de los procesos de la entidad.
- **El área de Control Interno**: Se encarga de realizar evaluación y seguimiento a los sistemas y su posible impacto en la entidad.

12. IMPORTANCIA DE LA GESTIÓN DE RIESGOS

En el ámbito empresarial se está dando mayor prioridad a salvar, proteger y custodiar el activo de la información, debido a que los sistemas de información y los avances tecnológicos están siendo implementados en todas las empresas del mundo.
La EMPRESA DE SERVICIOS PUBLICOS DAGUAS SA E.S.P sigue los lineamientos trazados por el Gobierno Nacional en cumplimiento de la Ley de Transparencia 1712 de 2014 y Gobierno en Línea que viene impulsando actividades dentro de las entidades públicas para que se ajusten a modelos y estándares que permitan brindar seguridad a la información dando cumplimiento al Decreto 1078 de 2015.

Los riesgos por desastres naturales, riesgos inherentes relacionados con procesos no adecuados en el tratamiento de la misma información, desconocimiento de normas y políticas de seguridad y el no cumplimiento de estas, suelen ser los temas más frecuentes y de mayor impacto presentes en las empresas. Una entidad sin un plan de gestión de riesgos está expuesta a perder su información.
Todas las organizaciones deberían implementar planes para gestionar los riesgos que afectan a los sistemas de información, tecnologías de información y activos informáticos, considerando que en la actualidad los riesgos más comunes son generados por ataques dirigidos al software empresarial, afectando la disponibilidad e integridad de la información almacenada o transportada a través de los equipos de comunicación.

Por esta razón hay que estar preparados para prevenir todo tipo de ataques o desastres, ya que cuando el costo de recuperación supera al costo de prevención es preferible tener implementados planes de gestión de riesgos que permitan la continuidad del negocio tras sufrir alguna pérdida o daño en la información de la entidad.

CONSIDERANDO LA SITUACIÓN ACTUAL DE LA IMPORTANCIA DE LA GESTIÓN DE RIESGOS

En el ámbito empresarial se está dando mayor prioridad a salvar, proteger y custodiar elactivo de la información, debido a que los sistemas de información y los avances tecnológicos están siendo implementados en todas las empresas del mundo.

La EMPRESA DE SERVICIOS PUBLICOS DAGUAS S. A E. S.P sigue los lineamientos trazados por el Gobierno Nacional en cumplimiento de la Leyde Transparencia 1712 de 2014 y Gobierno en Línea que viene impulsando actividades

dentro de las entidades públicas para que se ajusten a modelos y estándares que permitan brindar seguridad a la información dando cumplimiento al Decreto 1078 de 2015.

Los riesgos por desastres naturales, riesgos inherentes relacionados con procesos no adecuados en el tratamiento de la misma información, desconocimiento de normas y políticas de seguridad y el no cumplimiento de estas, suelen ser los temas más frecuentesy de mayor impacto presentes en las empresas. Una entidad sin un plan de gestión de riesgos está expuesta a perder su información.

Todas las organizaciones deberían implementar planes para gestionar los riesgos que afectan a los sistemas de información, tecnologías de información y activos informáticos, considerando que en la actualidad los riesgos más comunes son generados por ataques dirigidos al software empresarial, afectando la disponibilidad e integridad de la información almacenada o transportada a través de los equipos de comunicación.

Por esta razón hay que estar preparados para prevenir todo tipo de ataques o desastres,ya que cuando el costo de recuperación supera al costo de prevención es preferible tener implementados planes de gestión de riesgos que permitan la continuidad del negocio trassufrir alguna pérdida o daño en la información de la entidad.

Considerando la situación actual de la EMPRESA DE SERVICIOS PUBLICOS DAGUAS SA E.S.P, para reducir los niveles de riesgo, esindispensable diseñar un plan para iniciar las prácticas de las normas y políticas de seguridad e implementar procesos que aseguren la continuidad de los servicios.

13. ETAPAS PARA LA ADMINISTRACIÓN DEL RIESGO

El proceso de gestión del riesgo en la seguridad de la información puede ser iterativo para las actividades de valoración del riesgo y/o el tratamiento del mismo. Este enfoque puede incrementar la profundidad y el detalle de la valoración en cada iteración como semuestra en la figura tomada de la NTC ISO IEC 27005. Para reducir los niveles de riesgo, es indispensable diseñar un plan para iniciar las prácticas de las normas y políticas de seguridad e implementar procesos que aseguren la continuidad de los servicios.

Las etapas a considerar durante la administración del riesgo para DAGUAS S.A ESP son las siguientes:

- **Contexto estratégico:** Se determinarán los factores externos e internos del riesgo.
- **Identificación:** Se identificarán las causas, riesgo, consecuencias y clasificación del riesgo.
- **Análisis:** Se calificará y evaluará el riesgo inherente.
- **Valoración:** se identificará y evaluaran los controles; se deberá incluir la determinación del riesgo residual.
- **Manejo:** Se determinará, si es necesario, acciones para el fortalecimiento de los controles.
- **Seguimiento:** Se evaluará los riesgos de manera integral.

14. METODOLOGÍA DE IMPLEMENTACIÓN

Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información en DAGUAS SA E.S.P, se toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – Min TIC, a través de los decretos emitidos.

De acuerdo con esto, se definen las siguientes fases de implementación del MSPI (Modelo de Seguridad y Privacidad de la Información):

15. SEGUIMIENTO Y EVALUACIÓN

Cada doce (12) meses Control Interno realizará seguimiento a todo el componente deadministración de riesgos y verificará aspectos como:

- **Cumplimiento de las políticas y directrices para la administración del riesgo:**

- metodología de Administración del Riesgo (diseño y funcionamiento).

- **Administración de los riesgos por proceso e institucionales:** calificación y evaluación, efectividad de los controles y cumplimiento de las acciones.

  Los resultados de la evaluación y las observaciones de la persona que haga las veces de Control Interno deben ser presentados a la Alta Dirección, para que se tomen las decisiones pertinentes que garanticen la sostenibilidad de la Administración del Riesgo en la organización.

16. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE ACTIVOS DE INFORMACIÓN POR CATEGORÍAS

Según lo expuesto en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas emitida por el Departamento Administrativo de la Función Pública, el tratamiento de riesgos es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, por lo tanto dicha planeación en este caso en particular, hace alusión al tratamiento de riesgos de Seguridad y Privacidad de la Información enfocado en la seguridad de la información sobre los activos, para lo cual se realizan un conjunto de actividades durante la vigencia orientadas a implementar los

controles requeridos y priorizados. En atención a lo anterior, a continuación, se describen las actividades más relevantes orientadas al tratamiento de riesgos de Seguridad y Privacidad de la Información.

ACTIVIDAD	RESPONSABLES	SEGUIMIENTO Y EVALUACIÓN
Realizar la Adquisición e implementación de controles de seguridad de la información para abordar los riesgos de seguridad y privacidad de la información identificados, analizados, valorados y priorizados sobre los activos de información bajo la responsabilidad de cada dependencia a nivel central.	Todas las dependencias de la Empresa de Servicios Públicos DAGUAS S.A. E.S.P.	ENERO A DICIEMBRE
Realizar los procesos requeridos para el seguimiento a la operación de los controles de seguridad de la información para abordar los riesgos de seguridad y privacidad de la información identificados, analizados, valorados y priorizados sobre los activos de información bajo la responsabilidad de cada dependencia a nivel central	Todas las dependencias de la Empresa de Servicios Públicos DAGUAS S.A. E.S.P.	ENERO A DICIEMBRE
Realizar el seguimiento a las actividades de identificación y operación de controles de seguridad de la información para abordar los riesgos de seguridad y privacidad de la información identificados, analizados, valorados y priorizados sobre los activos de información bajo la responsabilidad de cada dependencia a nivel central.	Todas las dependencias de la Empresa de Servicios Públicos DAGUAS S.A. E.S.P.	ENERO A DICIEMBRE