PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

EMPRESA PIEDECUESTANA ESP

Piedecuestana
DE SERVICIOS PUBLICOS E.S.P.

ELABORÓ	FECHA	REVISÓ	FECHA	APROBÓ	FECHA
Profesional en Calidad	06/07/2018	Director Administrativo y Financiero	06/07/2018	Comité de Calidad	06/07/2018

TABLA DE CONTENIDO

PÁG.

LISTA DE TABLAS

LISTA DE GRÁFICAS

PÁG

1. INTRODUCCIÓN

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la Empresa Municipal de Servicios Públicos y Domiciliarios de Piedecuesta – Piedecuestana ESP tiene como fin identificar y dar a conocer la implementación de un plan el cual concientice a los trabajadores, contratistas y usuarios en general del correcto tratamiento de la información teniendo siempre muy presente la privacidad de la información como objetivo principal.

El Plan Estratégico de Tecnologías de Información y de Comunicaciones de la Empresa Municipal de Servicios Públicos y Domiciliarios de Piedecuesta – Piedecuestana ESP, construye una guía que orienta, define lineamientos para el mejoramiento del nivel de madurez institucional en la implementación de soluciones tecnológicas que generen valor y promuevan el cumplimiento de la misión con sostenibilidad tecnológica, para proporcionar los servicios tecnológicos requeridos, de manera que transformen y mejoren sus procesos y procedimientos misionales y de gestión administrativa. De cara a mantener este plan ajustado a las necesidades de la entidad, el PETI será un instrumento sujeto de mejora y por lo tanto, será sometido a revisiones y mejoras conforme se requiera.

2. OBJETIVO

Controlar y minimizar los riesgos asociados a los procesos tecnológicos existentes, en la empresa Piedecuestana ESP con el fin de salvaguardar los activos de información, el manejo de medios, control de acceso y gestión de usuarios.

3. TÉRMINO Y DEFINICIONES

- **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos

obligados. (Ley 1712 de 2014, art 4)

- **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...) que tenga valor para la organización. (ISO/IEC 27000).

- **Activo de Información:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

- **Confidencialidad:** Propiedad que determina que la información está disponible ni sea revelada a quien no esté autorizado (2.13 ISO 27000)

- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- **Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que

terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

- **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. (Decreto 1377 de 2013, art 3).

- **Derecho a la Intimidad:** Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

- **Disponibilidad:** Propiedad que la información sea accesible y utilizable por solicitud de los autorizados (2.10 ISO 27000)

- **Encargado del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3).

- **Estimación del riesgo:** Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

- **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. (ISO/IEC 27000).

- **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

- **Información Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

- **Integridad:** Propiedad de salvaguardar la exactitud y el estado completo de los activos (2.36 ISO 27000)

- **Partes interesadas (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 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. (ISO/IEC 27000).

- **Privacidad:** En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades

destinatarias del Manual de GEL la correlativa obligación

- **Procedimiento:** Sucesión cronológica de acciones concatenadas entre sí, para la realización de una actividad o tarea específica dentro del ámbito de los controles de Seguridad de la Información.

- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

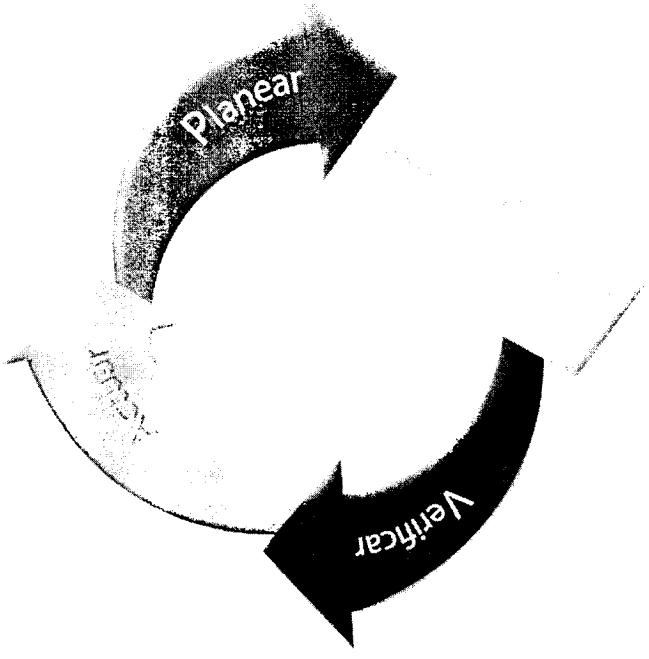
- **Titulares de la información:** Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).

- **Transferencia del riesgo:** Compartir con otra de las partes la pérdida o la ganancia de un riesgo. NOTA: En el contexto de los riesgos en la seguridad de la información, únicamente se consideran las consecuencias negativas (pérdidas) para la transferencia del riesgo.

- **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. (ISO/IEC 27000).

La entidad y los trabajadores oficiales son los principales encargados de conocer, implementar, garantizar el cumplimiento y monitorear los resultados de la estrategia

permitiendo en la entidad una mejora integral de la competitividad y del servicio con el objetivo de mejorar continuamente la calidad ofrecida a los usuarios, optimizar la productividad y aumentar a través de las nuevas tecnologías la rentabilidad de la empresa.



Gráfica 1. Ciclo PHVA.

7. ACTIVIDADES PARA LA IMPLEMENTACIÓN

- Realizar Diagnóstico
- Implementar políticas enfocadas a la seguridad de la Información.
- Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información

IDENTIFICACION DEL RIESGOS			SEGUIMIENTO PLAN DE TRATAMIENTO		
RIESGO	**DESCRIPCION**	**CAUSAS**	**PLAN DE TRATAMIENTO (ACCIONES)**	**RESPONSABLES**	**INDICADOR**
Adulteración de la información	Es el uso indebido o manipulación de la información actas, bases, registro fotográfico, fílmico, medidores cadena de custodia, acuerdos de pago, expedientes, respuestas oficios, tutelas.	1. Fácil acceso a las carpetas de archivo 2. Que el servidor público reciba para él o para otro dinero directa o indirectamente para anular o modificar un proceso, trámite o inicio de procedimiento. 3. Ausencias de controles y seguimientos a los procesos.	1 y 3. Implementación y desarrollo de un aplicativo basado en una propuesta llevada a Informática. 2.Monitoreo de las actividades de los analistas y operarios frente a las actividades realizadas 4.Verificación de la información	Director Financiero y administrativo Director de Planeación e Infraestructura Director Comercial	Número de casos detectados / Número de actividades realizadas < 0,001% Número de casos detectados / Número de actividades realizadas <
Sistemas de información susceptibles de manipulación o adulteración.	La tecnología utilizada en los procesos de Contratación puede ser vulnerable ante posibles saboteos con el propósito de re direccionar los procesos de Contratación.	1. Tecnología de baja seguridad y Obsoleta 2. Modificación de datos ó registro de información sin la debida autorización, en la página web de contratación o en los archivos de la carpeta procesos de la Dirección de Contratación y Compras. 3. Perdida de llaves y/o código fuente de la página web de contratación.	1. Incorporación de la empresa a los programas de lucha anticorrupción, publicación de los procesos contractuales.	Director Financiero y administrativo Director de Planeación e Infraestructura Director Comercial	Cantidad de minutas publicadas / cantidad de minutas por publicar

Tabla 1. Mapa de riesgos Sistemas e Informática empresa Piedecuestana ESP

- Realizar Inventario de Activos de Información con los líderes de cada Proceso.
- Realizar la Valoración de los Activos de Información con los líderes de cada Proceso

- Realizar el Plan de tratamiento de los riesgos (Riesgo Inherente y Riesgo Residual)
- Socializar el Plan de Tratamiento de Riesgo
- Realizar seguimiento del Plan de Tratamiento de Riesgo

8. CUMPLIMIENTO DE IMPLEMENTACIÓN

Para dar el total de cumplimiento de la implementación de la metodología mencionada anteriormente, se exponen las siguientes actividades y tareas a desarrollar de acuerdo a lo establecido por la empresa Piedecuestana ESP:

- Implementar la Política de Seguridad de la información.
- Implementar la Política de Administración de datos.
- Implementar las Políticas de Comunicaciones.
- Aspectos organizativos de la seguridad de la información
- Seguridad de la Información enfocada a los recursos humanos
- Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.
- Revisión de los Controles de acceso
- Gestión de Incidentes de Seguridad de la Información

9. CRONOGRAMA

No.	ACTIVIDAD	RESPONSABLE	FECHA TENTATIVA IMPLEMENTACION
1	Realizar diagnóstico	Profesional Universitario y/o apoyo	Junio 2019
2	Implementar políticas enfocadas a la seguridad de la información	Profesional Universitario	Octubre 2019
3	Elaborar el alcance del plan de tratamiento de riesgos de seguridad y privacidad de la información.	Apoyos TIC	Noviembre 2019
4	Realizar el Plan de tratamiento de los riesgos (Riesgo Inherente y Riesgo Residual)	Profesional Universitario / apoyo TIC	Noviembre 2019
5	Realizar seguimiento del Plan de Tratamiento de Riesgo	Profesional Universitario	Diciembre 2019
6	Socializar el Plan de Tratamiento de Riesgo	Profesional Universitario	Diciembre 2019

Tabla 2. Cronograma implementación.

10. SEGUIMIENTO

La empresa Municipal de Servicios Públicos y Domiciliarios de Piedecuesta – Piedecuestana ESP evaluará el desempeño del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información a través de la revisión de las acciones que se están llevando a cabo y evaluará la eficiencia en su implementación, adelantando verificaciones y seguimientos al menos una vez al año o cuando sea

necesario, evidenciando todas aquellas situaciones o factores que pueden estar influyendo en la aplicación de las acciones de tratamiento.

11. MONITOREO

El monitoreo al Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información debe estar a cargo del Control Interno y la Dirección de Planeación, aplicando y sugiriendo los correctivos y ajustes necesarios para propender por un efectivo manejo del riesgo.

12. CONCLUSIONES

El seguimiento constante a los procesos y la implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información deben ser ejecutados, monitoreados y actualizados constantemente. Así mismo, se hace indispensable implementar dicho plan porque nos permite prevenir posibles amenazas encontradas en la infraestructura tecnológica de la empresa Piedecuestana ESP.