Empresa de Servicios Públicos de Sabaneta E.S.P.

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

GESTION DE LA TECNOLOGIA DE LA INFORMACION Y COMUNICACION

Tabla de contenido

METODOLOGIA DE IMPLEMENTACIÓN

Para llevar a cabo la implementación del Sistema de Gestión de Seguridad de la Información, se toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar):

De acuerdo a esto, se definen las siguientes fases de implementación:

1. Diagnosticar
2. Planear
3. Hacer
4. Verificar
5. Actuar

CUMPLIMIENTO DE IMPLEMENTACIÓN

De acuerdo a las fases mencionadas anteriormente, se describe a continuación los dominios que se deben desarrollar:

- Política de Seguridad
- Aspectos organizativos de la seguridad de la información
- Seguridad Ligada a los recursos humanos
- Gestión de Activos
- Cifrado
- Seguridad en las telecomunicaciones
- Gestión de Incidentes de Seguridad de la Información
- Aspectos de seguridad de la información en la gestión de continuidad del negocio

Fase I – Diagnostico

Fase II – Planeación

Fase III – Implementación:

Dentro de esta fase se relacionan los siguientes entregables:

- ✓ Diagnostico
- ✓ Alcance

- ✓ Actualizar manual de políticas de seguridad y privacidad de la información, debidamente aprobadas y socializadas al interior de la Entidad, por la alta Dirección.
- ✓ Inventario de activo de información.
- ✓ Informe de análisis de riesgos, matriz de riesgos, plan de tratamiento de riesgos
- ✓ Declaración de aplicabilidad

Fase III – Implementación:

- ✓ Documento con la estrategia de planificación y control operacional.
- ✓ Documento con el informe del plan de tratamiento de riesgos, que incluya la implementación de controles de acuerdo con lo definido en la declaración de aplicabilidad.
- ✓ Ejecutar y presentación de análisis de vulnerabilidades
- ✓ Resultado de análisis de vulnerabilidades
- ✓ Resultado de entrevistas con los responsables de los procesos y administradores de la plataforma tecnológica y Sistemas de Información.
- ✓ Matriz de Riesgos
- ✓ Plan de tratamiento de los riesgos
- ✓ Indicadores de gestión y de cumplimiento.

Fase IV – Evaluación del Desempeño de la seguridad implementada en SII,

- ✓ Plan de seguridad, evaluación y análisis del SGSI
- ✓ Evaluación del Plan de Tratamiento de Riesgo.

Fase V – Mejora Continua.

- ✓ Plan de seguimiento, evaluación y análisis para el SGSI
- ✓ Auditoría interna
- ✓ Comunicación de resultados y plan de mejoramiento
- ✓ Revisión y aprobación por la alta dirección
- ✓ Documento con el plan de comunicación, sensibilización y capacitación, con los respectivos soportes.

CONSULTAS

Análisis de Riesgo

Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
(ISO/IEC 27000).

Auditoría

Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y determinar el grado en el que se cumplen los criterios de auditoria.
(ISO/IEC 27000).

Autorización

Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

Bases de Datos Personales

Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

Ciberseguridad

Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Ciberespacio

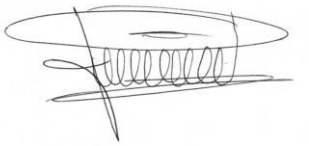
Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

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 (Ley1712 de 2014, art 6).



JUAN PABLO PIMIENTA BOTERO

GERENTE (E)

Elaboró: Diego Armando Zuleta Osorio
Apoyo a la Gestión de la Información y Comunicación como Ingeniero Informático.