EMPRESA DE ACUEDUCTO, ALCANTARILLADO Y ASEO DE SAN GIL

Nit 800.120.175-7

Elaboro:
DIEGO ANDRES SUPELANO AMAYA
Ingeniero de Sistemas
Esp. En Seguridad Informática
Jefe de Sistemas y Estadística
2018

Km 1 via al Aeropuerto
San Gil – Santander
(7) 7242590 – 7242564 – 7244433
Contactenos@acuasan.gov.co
www.acuasan.gov.co

#acuasaneice
#acuasaneice
Acuasan San Gil

INTRODUCCIÓN

Con el fin de garantizar el manejo eficaz de la información con la cual trabaja la empresa ACUASAN EICE-ESP por medio de los equipos, aplicaciones informáticas y demás medios con los cuales interactúan diariamente los funcionarios y las OPS 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 revaluación de la seguridad, lo cual arroja como resultado el mejoramiento continuo gracias a la adopción del modelo PHVA.

Para la empresa ACUASAN EICE-ESP como empresa de servicios públicos, es importante y requerido para su operación el contar con un estándar de Seguridad de la Información acorde, a los estándares que ayudará a mantener un sistema coherente con los procesos de la empresa en beneficio a los usuarios.

Continuando con el trabajo ya iniciado con la elaboración del Plan de Implementación del SGSI, se hizo necesario apoyar las actividades desarrolladas internamente a través de la política de seguridad de la información, la cual impulsó las actividades de ajuste de la documentación interna y procesos, los cuales han continuado su evolución y se han adaptado, de acuerdo a las nuevas necesidades de la empresa.

Para esta nueva vigencia, se elabora este Plan Estratégico de Seguridad de la Información, el cual sirva de base, para plantear la estrategia que, acorde al Plan Operativo de la empresa ACUSAN EICE-ESP, los recursos con los que se cuenta y el equipo asignado, permita el cumplimiento de objetivos de seguridad de la información.

OBJETIVOS

Objetivo General

- Desarrollar e Implementar un Plan de Seguridad y Privacidad de la Información, acorde a los requisitos de Gobierno en Línea y la aplicación de la norma ISO 27001:2013, que contribuya a salvaguardar la disponibilidad, integridad y confidencialidad de los activos de información de la empresa ACUASAN EICE-ESP, con el fin de garantizar la continuidad en los procesos misionales.
-

Objetivos Específicos

- Definir las fases para actualizar la Estrategia de Seguridad de la Información.
- Contribuir a la disminución de incidentes y requerimientos relacionados con la seguridad de la información.
- Facilitar la implementación de los lineamientos del Marco de Referencia de Seguridad de la Información de Gobierno en Línea, relacionados con la seguridad de la información.

ETAPAS PARA IMPLEMENTACIÓN DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

ETAPA 1. DEFINIR EL ALCANCE

El alcance integrado de los módulos es el siguiente:

La Empresa ACUASAN EICE-ESP en su Proceso “Gestión de Servicios de Infraestructura Tecnológica” quien determina la implementación, operación, mantenimiento y mejora continua de los Sistemas de Gestión de Seguridad de la Información y de la Gestión de Servicios de Infraestructura Tecnológica, que se desarrollan para el cumplimiento de sus funciones, detalladas en los procedimientos asociados y ejecutados por los funcionarios, así como el control y mitigación de los riesgos de seguridad de la información institucional gestionada por la oficina de sistemas.

Desde la empresa ACUASAN EICE-ESP se atienden los requerimientos de Servicios de Infraestructura Tecnológica para las oficinas de y planta en general, mediante el uso de herramientas tecnológicas de vanguardia, y recursos provistos por terceras partes, los cuales sean viables de implementación con los recursos propios.

ETAPA 2. ACTUALIZAR LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Se plantea la revisión y actualización de la Política de Seguridad de la Información, Resolución 007 del 6 de enero de 2017, con el fin de optimizar el Componente de Gestión de la Seguridad de la Información de la empresa ACUASAN EICE-ESP. Esta política aplica a todos los procesos y procedimientos que conforma el Sistema Integrado de Gestión.

ETAPA 3. METODOLOGÍA PARA LA IMPLEMENTACIÓN.

Teniendo en cuenta el modelo a utilizar con el estándar ISO, se continúa la implementación del ciclo PHVA, como metodología para la mejora continua.

Además, se debe verificar la existencia de los siguientes lineamientos:

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

Lineamientos y Etapas para lograr una buena planificación del SGSI y el ciclo **PHVA**	**LINEAMIENTO 1. IDENTIFICAR EL NIVEL DE MADUREZ EN S.I**
	ETAPA 1. Preparación
	- Plan de capacitación - Conformación Equipo de Gestión del Proyecto.
	ETAPA 2. Análisis situación actual y definición de
	- **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
	ETAPA 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.**
	ETAPA 1. Actividades Lineamientos Nivel Inicial
	- **Obtener soporte de la Dirección de la entidad.** - **Identificar legislación y normatividad aplicable.** - **Definir el alcance del SGSI** - **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.**

HACER	**LINEAMIENTO 3. LLEVAR A LA ENTIDAD A UN NIVEL DE MADUREZ BÁSICO EN SEGURIDAD.**
	ETAPA 1. Actividades Lineamientos Nivel Básico
	- **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 etapa de planeación.** - **Implementar los planes de concientización y entrenamiento.** - **Establecer y gestionar la operación del SGSI y sus recursos.** - **Implementar la infraestructura de respuesta a incidentes.**

VERIFICAR	**LINEAMIENTO 4. LLEVAR A LA ENTIDAD A UN NIVEL DE MADUREZ AVANZADO EN SEGURIDAD.**
	ETAPA 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.** - **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.**
	ETAPA 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, 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, para definir políticas, procesos y procedimientos que den respuesta proactiva a las amenazas sobre seguridad de la información que se presentan en la Empresa ACUASAN EICE-ESP.
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 del modelo integrado de gestión.
Definido	- 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

Administrado	- Se revisa y monitorea periódicamente los activos de información de la Entidad. -Se utilizan indicadores para establecer el cumplimiento de las políticas de seguridad y privacidad de la información. - Se evalúa la efectividad de los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro.
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

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 de los activos fijos de la empresa ACUASAN EICE-ESP.

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 empresa, con el propósito de proteger la misma contra las amenazas presentes en el entorno.

- Organización de la seguridad de la información:

Diseñar una estructura para la gestión de la seguridad de la información dentro la empresa 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 co- responsables de la seguridad de la información.

- Gestión de Activos:

Detalla los activos fijos de la empresa como (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 empresa 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 empresa, 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 empresa, 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 empresa, lo que podría provocar un deterioro de la imagen de la empresa, 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 empresa.