POLÍTICA DE SEGURIDAD DIGITAL

EMPRESA DE SERVUCIOS PÚBLICOS DE ACUEDUCTO Y ALCANTARILLADO DEL CARMEN DE BOLÍVAR ACUECAR SA ESP

2024

TEL. (5) 6862822
ACUECARS.COM
CARRERA 52 N° 25-43
CONTACTENOS.ACUECAR@GMAIL.COM

INTRODUCCION

La Política de Seguridad Digital es desarrollada por ACUECAR SA ESP, con el fin de proteger los activos de información que manejan (trabajadores, contratistas, terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos y apoyan la implementación del Sistema de Gestión de Seguridad de la Información. Para su implementación se generarán y publicarán las políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales para la gestión de la seguridad de la información.

En cumplimiento a lo estipulado en el Modelo Integrado de Planeación y Gestión MIPG, como marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos , con integridad y calidad en el servicio, incorpora la política de seguridad digital en el marco de la tercera dimensión: Gestión con valores para resultados.

1. OBJETIVO

La Política de Seguridad Digital de ACUECAR SA ESP establece lineamientos robustos para proteger la información y los sistemas digitales de la empresa contra accesos no autorizados, ataques cibernéticos y otras amenazas digitales, asegurando la confidencialidad, integridad y disponibilidad de los datos para una Operación continua y segura.

2. MARCO NORMATIVO

Esta política se fundamenta en las normativas nacionales y estándares de seguridad de información aplicables, incluyendo:

- Decreto 1499 de 2017: Como parte del Modelo Integrado de Planeación y Gestión (MIPG), - incorpora la Seguridad Digital para fortalecer las capacidades de protección de datos en el sector público.

- Decreto 1078 de 2015 (Art. 2.2.9.1.2): Regula la seguridad digital para asegurar que las entidades públicas protejan sus activos digitales, minimizando riesgos.

- Ley 1581 de 2012: Dispone el marco para la protección de datos personales, especificando los protocolos necesarios para la gestión segura de información sensible.

3. ALCANCE

Esta política se aplica a todas las áreas de ACUECAR SA ESP y cubre la protección de todos los activos de información, sistemas, bases de datos, redes y dispositivos utilizados para la prestación de servicios y la gestión administrativa.

4. LINEAMIENTOS ESTRATÉGICOS

- **Confidencialidad de la Información:** Asegurar que la información sensible de la empresa y de los usuarios esté protegida mediante controles que prevengan el acceso no autorizado.

- **Integridad de los Datos**: Garantizar que los datos permanezcan inalterados a menos que el cambio sea autorizado y registrado, evitando cualquier manipulación indebida.

- **Disponibilidad de Servicios y Datos**: Establecer sistemas redundantes y prácticas de recuperación que garantizan la continuidad de los servicios y datos críticos ante incidentes.

- **Protección frente a amenazas**: Implementar un entorno de seguridad cibernética sólida, incluyendo la utilización de firewalls, antivirus y filtros de acceso, para resguardar los activos de la empresa de ataques externos e internos.

- Restricción de Dispositivos Externos: Limitar el uso exclusivo de equipos propiedad de ACUECAR SA ESP, prohibiendo el uso de dispositivos de almacenamiento externos como unidades USB, discos duros portátiles, y otros dispositivos no autorizados para prevenir el ingreso de malware y la fuga de información.

5. RESPONSABILIDADES

- **Área de Sistemas y Comunicaciones**: Liderará la definición e implementación de medidas de seguridad digital, el monitoreo continuo de los sistemas, la configuración de protocolos de acceso seguro y la respuesta ante cualquier incidente de seguridad.

- **Líderes de Proceso**: Colaborarán con el área de Sistemas en la identificación de riesgos específicos de sus áreas, participarán en la implementación de controles y reportarán posibles vulnerabilidades incidentes.

- **Todo el Personal**: Deberá cumplir estrictamente con los protocolos de seguridad digital, siguiendo las prácticas de protección de datos y reportando cualquier actividad sospechosa o riesgo detectado.

6. IMPLEMENTACIÓN

- **Controles de Acceso**: Implementar controles de acceso basados en el rol de cada usuario, con el fin de asegurar que sólo el personal autorizado tenga acceso a la información sensible de la empresa.

- **Monitoreo Permanente y Detección de Amenazas**: Implementar sistemas de monitoreo en tiempo real que alerten sobre actividades sospechosas o inusuales en los sistemas. Esto incluye el uso de software de detección de intrusiones (IDS) y gestión de eventos de seguridad (SIEM) para una supervisión continua.

- **Respuesta a Incidentes**: Desarrollar y mantener un Plan de Respuesta a Incidentes que incluya procedimientos detallados para la identificación, contención, erradicación y recuperación ante un ataque o fuga de información. El área de Sistemas gestionará este plan y realizará simulacros de respuesta para asegurar su eficacia.

- **Auditorías y Evaluaciones de Seguridad**: Programar auditorías de seguridad periódicas y evaluaciones de vulnerabilidad para identificar y corregir fallos en los sistemas de protección digital. Los resultados serán analizados y, de ser necesario, se actualizarán los controles y medidas de seguridad.

- **Restricciones en el Uso de Dispositivos de Almacenamiento Externo**: Establecer controles para prevenir el uso de dispositivos externos, como USB, discos duros externos o cualquier otro medio de almacenamiento externo en las estaciones de trabajo, evitando riesgos de seguridad y manteniendo un control riguroso sobre la información.

7. JUSTIFICACIÓN

La implementación de esta Política de Seguridad Digital tiene como propósito:

Resguardar la integridad, confidencialidad y disponibilidad de los datos de ACUECAR SA ESP y de sus usuarios, cumpliendo con la normativa nacional y evitando la exposición a riesgos digitales.

Garantizar la continuidad de los servicios mediante el establecimiento de un sistema robusto de prevención, detección y respuesta ante incidentes, minimizando cualquier impacto negativo en la operación.

Prevenir la pérdida o fuga de datos a través del control y restricción de dispositivos de almacenamiento externos, promoviendo un entorno controlado y seguro en el uso de la información.

Promover una cultura de ciberseguridad dentro de la empresa, en la que todos los colaboradores desempeñen un rol activo en la protección de la información.