UNIVERSIDAD DE LAS FUERZAS ARMADAS

ESPE

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

GESTIÓN DE LA SEGURIDAD INFORMÁTICA

Ing. Cesar Ivan Chiliquinga Mendoza

TAREA 2.2 Política

Integrantes:

- Enríquez Granda Ronaldo Daniel
- Tinoco Ochoa Jeimmy Anahí

Fecha: 19 de enero de 2025

NRC: 3894

Política del Sistema de Gestión de Seguridad de la Información (SGSI)

1. Resumen de la política

La Empresa XYZ reconoce que la información es uno de sus activos más valiosos y críticos para el cumplimiento de sus objetivos estratégicos. Esta política establece los lineamientos esenciales para proteger la información en todas sus formas frente a riesgos internos y externos. La protección de la confidencialidad, integridad y disponibilidad de los datos no solo es un requisito operativo, sino también un compromiso con nuestros clientes, empleados y socios.

El principal objetivo de esta política es implementar un enfoque sistemático y documentado para gestionar los riesgos relacionados con la información, cumpliendo con las mejores prácticas internacionales, como la norma ISO 27001, y garantizando la continuidad del negocio.

2. Introducción

En un mundo cada vez más digital, la información representa el eje central de las operaciones de la Empresa XYZ. Puede estar en formato digital, impreso o incluso en la forma de conocimiento tácito compartido entre los empleados. La pérdida o exposición indebida de esta información podría tener consecuencias graves, incluyendo daños financieros, legales y reputacionales.

La seguridad de la información se entiende como la aplicación de controles adecuados para prevenir accesos no autorizados, alteraciones o pérdidas, mientras se asegura la disponibilidad de la información cuando sea necesaria. Este documento establece un marco integral para la gestión de la seguridad de la información, fomentando una cultura organizacional orientada hacia la prevención y mitigación de riesgos.

3. Alcance del SGSI

El Sistema de Gestión de Seguridad de la Información abarca los procesos, personas y tecnologías utilizados en las operaciones de la Empresa XYZ. Incluye:

- **Desarrollo y mantenimiento de software**: Esto comprende desde la fase de diseño hasta el despliegue y mantenimiento de soluciones en la nube, garantizando que estas cumplan con los estándares de seguridad establecidos.
- **Gestión de datos sensibles**: Protección de información corporativa y de clientes almacenada en plataformas como Microsoft Azure.

- **Entornos de trabajo**: Aplica a las oficinas en Cuenca y a los empleados remotos, limitándose a dispositivos corporativos provistos y gestionados por la empresa.

Exclusiones: La seguridad física de las viviendas de empleados remotos y los dispositivos personales que no sean administrados por la empresa quedan fuera del alcance debido a la falta de control directo. Sin embargo, se establecen recomendaciones y medidas preventivas para mitigar riesgos asociados.

4. Objetivos del SGSI

El SGSI tiene como objetivos clave:

1. **Proteger la información crítica**: Evitar la pérdida, robo o modificación no autorizada de datos que podrían impactar la operatividad de la empresa o la confianza de sus clientes.
2. **Cumplimiento normativo**: Garantizar que las operaciones cumplan con la Ley Orgánica de Protección de Datos Personales en Ecuador y con cualquier regulación internacional aplicable.
3. **Mejorar la resiliencia organizacional**: Desarrollar una capacidad robusta para prevenir, detectar, responder y recuperarse ante incidentes de seguridad.
4. **Fomentar una cultura de seguridad**: Educar a todos los empleados en las mejores prácticas de seguridad y en la importancia de la protección de la información.

5. Responsabilidades

- **Dirección General**: Proveer liderazgo y compromiso para garantizar que los recursos necesarios sean asignados y que los objetivos del SGSI se alineen con las metas estratégicas de la organización. Revisar periódicamente la efectividad del sistema.
- **CTO (Daniel Enríquez)**: Responsable de supervisar la implementación del SGSI, coordinar auditorías internas y garantizar la actualización continua de los controles.
- **Encargada de Seguridad de la Información (Jeimmy Tinoco)**: Gestionar las evaluaciones de riesgos, diseñar controles y capacitar al personal en temas de seguridad.
- **Empleados**: Cumplir con las políticas y reportar cualquier incidente sospechoso de inmediato. Participar en capacitaciones para aumentar su conocimiento en ciberseguridad.

- **Proveedores (Microsoft Azure)**: Garantizar que sus servicios cumplan con los estándares de seguridad exigidos, proporcionando evidencia de auditorías regulares.

6. Principales resultados esperados

1. **Minimizar incidentes de seguridad**: Lograr que las violaciones de seguridad sean prevenibles y que, en caso de ocurrir, su impacto sea mínimo.
2. **Protección de activos clave**: Garantizar la seguridad de los datos, dispositivos y procesos críticos para la continuidad operativa.
3. **Transparencia y confianza**: Fortalecer la confianza de los clientes y socios al demostrar un compromiso constante con la seguridad de la información.

7. Políticas relacionadas

- **Política de uso de dispositivos corporativos**: Garantiza que los dispositivos sean utilizados únicamente para fines autorizados y con configuraciones de seguridad aprobadas.
    - **Objetivo**: Proteger la información corporativa y mitigar riesgos de pérdida de dispositivos.
    - **Por qué es importante**: La falta de control sobre dispositivos corporativos podría generar fugas de información y exponer datos sensibles.
- **Política de acceso remoto**: Define los requisitos para conexiones seguras, como el uso obligatorio de VPN y autenticación multifactor.
    - **Objetivo**: Reducir los riesgos asociados con accesos remotos no autorizados.
    - **Por qué es importante**: Los accesos remotos son un vector común de ataque; asegurar estos puntos minimiza la exposición.
- **Política de respuesta a incidentes**: Proporciona un marco para identificar, responder y recuperar de incidentes de seguridad.
    - **Objetivo**: Asegurar que cualquier incidente sea manejado de manera eficaz y oportuna.
    - **Por qué es importante**: Una respuesta rápida y bien estructurada reduce el impacto en las operaciones y protege la reputación.

- **Política de gestión de riesgos**: Establece un enfoque para identificar, analizar y mitigar los riesgos que puedan afectar la información y los sistemas.
    - **Objetivo:** Reducir al mínimo el impacto de los riesgos mediante medidas proactivas y correctivas.
    - **Por qué es importante:** Una gestión efectiva de riesgos garantiza la continuidad operativa y la seguridad de los datos.

- **Política de control de acceso**: Regula el acceso a la información según roles y responsabilidades, asegurando que solo las personas autorizadas puedan acceder a datos sensibles.
    - **Objetivo**: Prevenir accesos no autorizados y proteger la información crítica.
    - **Por qué es importante**: El acceso no controlado puede llevar a violaciones de seguridad y pérdida de datos.

8. Revisión y actualización de la política

Esta política será revisada al menos una vez al año para asegurar su relevancia y eficacia. Adicionalmente, se realizarán revisiones extraordinarias en caso de cambios significativos en el entorno legal, tecnológico o interno.