LABORATORIO #23
Roberto Blanco

Introducción

Las políticas de seguridad constituyen un pilar fundamental en la protección de los datos dentro de un sistema de información. A través de ellas se establece un proceso claro y detallado sobre cómo se deben abordar las medidas de seguridad en la empresa, especificando su correcta aplicación y el camino que se debe seguir para su implementación. En este documento se describirán las políticas a adoptar, junto con las estrategias de prevención y mitigación ante posibles incidentes de seguridad. Además, se definirá la asignación de roles a los empleados, de modo que cada uno pueda cumplir adecuadamente con sus responsabilidades.

Propósito

El objetivo de estas políticas es garantizar un entorno seguro y ordenado en la empresa, asegurando el correcto funcionamiento de sus sistemas. Las políticas permiten identificar y controlar actividades inseguras que podrían comprometer los datos críticos de la organización. Es importante destacar que estas políticas son obligatorias; sin ellas, la empresa no podría considerarse como tal en términos de seguridad informática, ya que son esenciales en cualquier acción que se lleve a cabo.

Alcance

SecureSoft no se limita a aplicar políticas de seguridad de manera interna, sino que su alcance está enfocado en la oferta de un amplio portafolio de servicios y soluciones en ciberseguridad para sus clientes. Entre los servicios que brinda se incluyen:

- **Consultoría**: Asistencia en el diseño e implementación de políticas de seguridad, incluyendo estándares como ISO 27001, y en la gestión de riesgos.
- **Seguridad ofensiva**: Ejecución de pruebas de penetración (ethical hacking) para detectar vulnerabilidades.
- **Seguridad defensiva**: Vigilancia constante de amenazas (24/7) y respuesta ante incidentes.
- **Implementación de soluciones**: Instalación y configuración de herramientas de seguridad, como cortafuegos.
- **Capacitación**: Formación del personal en prácticas de ciberseguridad.
- **Protección de datos**: Asesoría sobre el cumplimiento de normativas de privacidad y protección de información

Principios Fundamentales

Para una correcta integración de las políticas de seguridad, es vital identificar claramente qué se necesita proteger: los datos. Estos deben cumplir con tres principios básicos de la ciberseguridad: confidencialidad, integridad y disponibilidad. Es decir, los datos deben estar protegidos contra accesos no autorizados, mantenerse íntegros sin alteraciones indebidas, y estar disponibles cuando se requieran. Solo el personal autorizado debe tener acceso a ellos, asegurando que la información esté siempre completa y segura.

Roles	Responsabilidades
Consultor estrategico	Diseñar e implementar las politicas de seguridad de la empresa.
Auditor y evaluador	Realizar pruebas para identificar vulnerabilidades en la seguridad empresarial.
Operador de seguridad	Supervisar los eventos relacionados con la seguridad dentro de la organización.
Formador	Capacitar al personal sobre las politicas de seguridad establecidas.
Implementador tecnico	Actuar de forma inmediata ante incidentes de seguridad, minimizando su impacto.
Soporte continuo	Mejorar y actulizar los sistemas para asegurar su funcionamiento a futuro.