LABORATORIO 23 CYBERSEGURIDAD

SECURESOFT

Introducción

Las políticas de seguridad son un gran pilar en lo que es la protección de los datos en un sistema de información ya que con estas tenemos un proceso claro y detallado de todo lo que se abordará en la empresa, ah si como también como debemos aplicarlas de la manera más óptima y como no era de otra que se debe seguir para implementar estás políticas en nuestra empresa, hablaremos de cada una de esta políticas que se van a implementar y a su vez de como debemos prevenir y mitigar incidentes en caso tal ocurran, y como se deben asignar cada rol a los empleados de esa empresa para que puedan hacer correctamente su trabajo.

Propósito

El propósito de estás políticas es de mantener un orden y correcto funcionamiento de la seguridad en esta empresa ya que las políticas nos ayudarán a controlar cualquier actividad insegura que pueda afectar seriamente los datos críticos de la empresa, cabe aclarar que las políticas de seguridad son obligatorias y sin ellas la empresa no podría considerarse con este nombró ya que son muy importantes al momento de realizar cualquier acción en esta.

Alcance

SecureSoft no tiene un alcance interno como una empresa que define sus propias políticas, sino que su alcance refiere a la amplia gama de servicios y soluciones de ciberseguridad que ofrecen a sus clientes.

Estos servicios incluyen:

- Consultoría: Ayudan a otras empresas a diseñar e implementar sus propias políticas de seguridad (incluyendo ISO 27001) y a gestionar riesgos.
- Seguridad Ofensiva: Realizan pruebas de penetración (ethical hacking) para encontrar vulnerabilidades.
- Seguridad Defensiva: Monitorean amenazas 24/7 y ayudan en la respuesta a incidentes de seguridad.
- Implementación de Soluciones: Instalan y configuran herramientas de seguridad como firewalls.

- Capacitación: Concientizan a los empleados sobre ciberseguridad.
- Protección de Datos: Asesoran sobre el cumplimiento de normativas de privacidad.

Principios fundamentales

Para poder integrar las políticas de seguridad debemos tener en claro que es lo que debemos proteger y son los datos y con todo esto, sabemos que estos datos deben ser confidenciales, íntegros y disponibles a cada momento que se necesiten, siempre debemos analizar todos estos datos y ver qué ninguno le falte algo además que solo las personas autorizadas puedan ver su contenido ya que todos estos principios son muy básicos en la ciberseguridad .

Roles	Responsabilidades
Consultor estratégico	Encargado diseñar e implementar las políticas de seguridad de la empresa
Auditor y evaluador	Encargado de hacer pruebas para identificar vulnerabilidades de seguridad en la empresa
Operador de seguridad	Encargado de supervisar eventos de seguridad dentro de la empresa
Formador	Encargado de capacitar a los empleados sobre las políticas de seguridad establecidas
Implementador técnico	Encargado de actuar inmediato ante incidentes de seguridad y ah si prevenir impactos fuertes para la empresa
Soporte Continuo	Encargado de mejorar y actualizar los sistemas para un correcto funcionamiento en el futuro