Presentación

Nombre: Moisés Ricardo

Apellido: Zabala Bueno

Matricula: 20200927

Materia: Seguridad Informática

Trabajo: Resumen ejecutivo #5

Docente: Ernesto Wachsmann

En la clase pasada estuvimos viendo el tema de política de seguridad, sus objetivos, otros temas relacionados a la seguridad y también vimos un ejemplo de una política de seguridad.

La política de seguridad es un conjunto de principios y directrices establecidos por una organización para proteger sus activos de información y garantizar la confidencialidad, integridad y disponibilidad de estos.

Estos son los objetivos principales de la política de seguridad:

Protección de recursos: Proteger los recursos de información de una organización, como datos, sistemas, redes y activos físicos.

Autenticación: Verificar la identidad de los usuarios a través de métodos como contraseñas, autenticación de dos factores o biometría, para asegurarse de que solo las personas autorizadas puedan acceder a la información.

Autorización: Asegura que cada usuario tenga los privilegios adecuados para acceder a la información y realizar las acciones necesarias en función de sus roles y responsabilidades.

Integridad: Garantizar la integridad de la información, lo que implica protegerla de modificaciones no autorizadas o manipulaciones indebidas. Esto se logra a través de técnicas como firmas digitales, controles de versiones y registros de auditoría.

No repudio: Busca evitar que una parte niegue haber realizado una acción o transacción. Esto se logra mediante la implementación de mecanismos de registro y seguimiento que permiten demostrar la validez y la autoría de las acciones realizadas.

Confidencialidad: Implica protegerla contra el acceso no autorizado o la divulgación indebida, mediante técnicas como el cifrado de datos, el control de acceso y la gestión de permisos.

Actividades de seguridad de auditoría: Establece la realización de actividades de auditoría y seguimiento para evaluar y verificar la efectividad de las medidas de seguridad implementadas.

Otro tema que vimos fueron los estándares y normas de seguridad, la política de seguridad establece los estándares y normas que deben seguirse para proteger los activos de información. Agregan el uso de contraseñas seguras, la implementación de firewalls y sistemas de detección de intrusos, la realización regular de copias de seguridad de los datos, entre otros.

Después vimos la familia de Normas ISO/IEC 27000 que proporciona un marco de mejores prácticas para la gestión de la seguridad de la información. Estas normas abarcan aspectos como la gestión de riesgos, la seguridad física, la seguridad de los sistemas de información y la continuidad del negocio.

Por último, vimos la legislación la cual ayuda a que la política de seguridad se deba cumplir con las leyes y regulaciones aplicables en materia de seguridad de la información. Esto puede incluir leyes de protección de datos, regulaciones sectoriales específicas y requisitos legales relacionados con la privacidad y la seguridad de la información.