Definición de Seguridad Informática

La seguridad informática se define como la protección otorgada a un sistema de información automatizado para lograr los objetivos de preservar la integridad, disponibilidad y confidencialidad de los recursos del sistema de información, que incluyen hardware, software, firmware, información/datos y telecomunicaciones.

La Triada CIA

Confidencialidad: Preservación de restricciones autorizadas sobre el acceso y la divulgación de información, incluida la protección de la privacidad personal y la información propietaria.

Integridad: Protección contra la modificación o destrucción no autorizada de información, garantizando la no repudiación y la autenticidad.

Disponibilidad: Garantía de acceso y uso oportunos y confiables de la información.

Niveles de Impacto

Bajo: Efecto adverso limitado en las operaciones organizacionales, activos o individuos.

Moderado: Efecto adverso serio en las operaciones organizacionales, activos o individuos.

Alto: Efecto adverso severo o catastrófico en las operaciones organizacionales, activos o individuos.

Retos de la Seguridad Informática

Complejidad de la seguridad.

Necesidad de considerar posibles ataques.

Colocación física y lógica de elementos.

Incorporación de algoritmos o protocolos adicionales.

Vigilancia constante y monitoreo regular.

Percepción de la seguridad como un impedimento a la eficiencia.

Activos de un Sistema Informático

Hardware, software, datos, instalaciones de comunicación y redes.

Vulnerabilidades, Amenazas y Ataques

Vulnerabilidades: Corrupto (pérdida de integridad), Fugas (pérdida de confidencialidad), Inaccesibilidad o lentitud (pérdida de disponibilidad).

Amenazas: Capaces de explotar vulnerabilidades.

Ataques: Pasivos (aprenden o usan información sin afectar los recursos del sistema), Activos (alteran recursos del sistema o afectan su operación).

Contramedidas

Medios para tratar ataques de seguridad: prevención, detección y recuperación.

Principios de Diseño de Seguridad

Economía de mecanismo, fallos seguros, mediación completa, diseño abierto, separación de privilegios, principio de privilegio mínimo, mecanismo común mínimo, aceptabilidad psicológica, aislamiento, encapsulación, modularidad, estratificación, menor asombro.

Superficies de Ataque

Incluyen vulnerabilidades accesibles y explotables en un sistema, como puertos abiertos, servicios internos, interfaces SQL, formas web y ataques de ingeniería social.

Políticas y Estrategias de Seguridad

Política de Seguridad: Declaración formal de reglas y prácticas para proteger recursos críticos.

Implementación de Seguridad: Prevención, detección, respuesta y recuperación.

Evaluación: Proceso de examen de productos o sistemas informáticos respecto a ciertos criterios.

Estrategia de Seguridad Informática

Comprende los principios de diseño de seguridad, superficies de ataque, implementación de seguridad, garantía y evaluación. Incluye conceptos básicos de seguridad informática, retos, modelos, amenazas, ataques y activos, además de requisitos funcionales de seguridad.