“UNIVERSIDAD PRIVADA DOMINGO SAVIO”

ACTIVIDAD 03

ETICA AMENAZAS VULNERABILIDADES

Integrante:

Jarlen Carrillo Herbas

Materia:

Seguridad Informática

Docente:

Ing. Hugo Arnaldo Guzmán Centellas

Fecha:

11/07/2024

Santa Cruz – Bolivia

ACTIVIDAD 3

1. Qué es la Ética y Legalidad de la Seguridad Informática

La ética y la legalidad en seguridad informática se refieren al conjunto de normas y principios que regulan el uso ético y legal de los sistemas de información y tecnologías relacionadas. Esto implica el respeto por la privacidad, la integridad de los datos, el cumplimiento de las leyes y regulaciones vigentes, así como la adopción de prácticas que promuevan la transparencia y la responsabilidad en el manejo de la información digital.

2.- Vulnerabilidades físicas y Vulnerabilidades lógicas

Las vulnerabilidades físicas se refieren a debilidades en la infraestructura física de los sistemas informáticos, como la falta de controles de acceso físico o la protección inadecuada contra desastres naturales. En contraste, las vulnerabilidades lógicas son fallos en el software o configuraciones que pueden ser explotadas por intrusos para comprometer la seguridad, como errores de programación, configuraciones incorrectas o falta de actualizaciones de seguridad.

3.- Amenazas a la seguridad informática

Las amenazas a la seguridad informática incluyen diversos riesgos que pueden comprometer la confidencialidad, integridad y disponibilidad de los datos. Esto abarca desde hackers que intentan penetrar sistemas para obtener información confidencial, hasta sniffers que interceptan datos en redes no protegidas, spammers que inundan correos electrónicos con mensajes no deseados, y amenazas internas provocadas por empleados con acceso privilegiado que abusan de sus derechos.

4.- Fases y tipos de ataques informáticos

Los ataques informáticos pasan por varias fases, que incluyen la recolección de información sobre el objetivo (reconocimiento), la penetración en el sistema (intrusión), el mantenimiento del acceso (persistencia), la manipulación o robo de datos (explotación) y la cobertura de huellas (eliminación de evidencias). Los tipos de ataques varían desde el phishing y la ingeniería social hasta el malware y el ransomware, cada uno con métodos específicos para comprometer sistemas informáticos.

5.- Virus y otros códigos dañinos

Los virus y otros códigos dañinos son programas diseñados para replicarse y causar daño en los sistemas informáticos. Los virus se adjuntan a archivos o programas legítimos y se propagan cuando estos son ejecutados. Otros códigos dañinos incluyen gusanos que se replican sin necesidad de un archivo huésped y troyanos que aparentan ser programas legítimos, pero realizan acciones maliciosas sin el conocimiento del usuario.

6.- Medios y herramientas de protección

Para proteger los sistemas informáticos, se utilizan diversas medidas y herramientas de seguridad, como firewalls para proteger redes contra accesos no autorizados, antivirus para detectar y eliminar virus y otros malware, cifrado de datos para proteger la confidencialidad de la información, y políticas de seguridad que promueven el uso seguro de sistemas y datos. Además, el uso de autenticación multifactor y la capacitación continua del personal son fundamentales para mitigar riesgos y fortalecer la seguridad informática.