GP 9: Unidad 6 - Aspectos de Seguridad

Título de la Actividad: "Reflexión sobre Panorama de Amenazas en nuestra Vida Digital"

Amenazas destacadas de la masterclass

1. Ingeniería social y phishing: Uno de los aspectos más alarmantes fue la exposición sobre técnicas de engaño, como el phishing, que afectan tanto a usuarios comunes como a profesionales. Se mostró cómo los atacantes utilizan correos electrónicos falsos o sitios web clonados para obtener credenciales de acceso o datos sensibles. Esta amenaza es especialmente relevante en el contexto de la seguridad en la gestión de archivos y el acceso a sistemas operativos.

2. Vulnerabilidades en dispositivos conectados (IoT): Otro tema importante fue el crecimiento de amenazas a través de dispositivos IoT. Se advirtió que múltiples artefactos del hogar y entornos laborales están conectados a la red sin la debida configuración de seguridad, lo cual permite accesos no autorizados y el robo de información. Esta problemática se vincula directamente con la arquitectura del sistema y la necesidad de establecer capas de seguridad a nivel de red y sistema operativo.

3. Malware y ransomware: Se analizó el impacto de los programas maliciosos que encriptan archivos (ransomware) y exigen rescates monetarios para su recuperación. Esta amenaza está relacionada con la protección de datos, el uso de backups y la responsabilidad de los sistemas operativos para detectar y contener este tipo de ataques mediante antivirus o mecanismos de aislamiento.

Relación con conceptos de la asignatura

La asignatura ofrece las bases para comprender los elementos que hacen a la arquitectura y seguridad de los sistemas. Por ejemplo, aprendimos que el sistema operativo es clave en la gestión de permisos de archivos, control de usuarios, monitoreo de procesos y configuración de redes seguras.

En la masterclass se destacó la necesidad de actualizar los sistemas operativos y sus componentes como una práctica fundamental de seguridad, lo que enlaza con los temas vistos en clase sobre mantenimiento de sistemas y protocolos de actualización.

El control de acceso a la información, tanto físico como lógico, es otro eje común. Desde la creación de contraseñas seguras hasta la segmentación de redes, todos estos temas fueron tratados tanto en clase como en la charla, mostrando su aplicación real.

Reflexión final: buenas prácticas en redes

Aplicar buenas prácticas en el diseño y la gestión de redes no es solo una tarea técnica, sino una responsabilidad compartida que impacta en la privacidad y seguridad de todos los usuarios. Desde configurar correctamente un router hasta implementar firewalls y sistemas de detección de intrusos, cada decisión influye en la protección de la información.

La masterclass reforzó la idea de que la seguridad debe ser pensada desde el inicio de cualquier sistema, no como un agregado posterior. En este sentido, la formación en temas de arquitectura de sistemas y ciberseguridad resulta esencial para construir entornos digitales más seguros y resilientes.