Amenazas de seguridad

Las amenazas de seguridad causadas por intrusos en la red pueden originarse tanto en forma interna como externa.

- **Amenazas externas**: Provienen de personas que no tienen autorización para acceder al sistema o a la red de computadoras. Logran introducirse principalmente desde Internet, enlaces inalámbricos o servidores de acceso por marcación o dial
- **Amenazas internas**: Por lo general, conocen información valiosa y vulnerable o saben cómo acceder a esta. Sin embargo, no todos los ataques internos son intencionados.

Con la evolución de los tipos de amenazas, ataques y explotaciones se han acuñado varios términos para describir a las personas involucradas

- **Hacker**: un experto en programación.
- **Hacker de sombrero blanco:** una persona que busca vulnerabilidades en los sistemas o en las redes y a continuación informa a los propietarios del sistema para que lo arreglen.
- **Hacker de sombrero negro**: utilizan su conocimiento de las redes o los sistemas informáticos para beneficio personal o económico.
- **Cracker**: es un término más preciso para describir a una persona que intenta obtener acceso no autorizado a los recursos de la red con intención maliciosa.
- **Phrieaker:** persona que manipula la red telefónica para que realice una función que no está permitida. Por lo general, a través de un teléfono público para realizar llamadas de larga distancia gratuitas.
- **Spammer**: persona que envía grandes cantidades de mensajes de correo electrónico no deseado, por lo general, los spammers utilizan virus para tomar control de las computadoras domésticas y utilizarlas para enviar mensajes masivos.
- **Estafador**: utiliza el correo electrónico u otro medio para engañar a otras personas para que brinden información confidencial como número de cuenta o contraseñas.

Delitos informáticos más frecuentes en la red:

Abuso del acceso a la red por parte de personas que pertenecen a la organización.

Virus.

Suplantación de identidad.

Uso indebido de la mensajería instantánea.

Denegación de servicio, caída de servidores.

Acceso no autorizado a la información.

Robo de información de los clientes o de los empleados.

Abuso de la red inalámbrica

Penetración en el sistema.

Fraude financiero.

Detección de contraseñas.

Registro de claves.

Alteración de sitios web.

Uso indebido de una aplicación web pública.

Hay diversos tipos de ataques informáticos en redes, algunos son:

- **Ataques de denegación de servicios (DOS):** es un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a usuarios legítimos, normalmente provocando la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

- **Man in the middle (MITM):** es una situación donde un atacante supervisa (generalmente mediante un rastreador de puertos) una comunicación entre las 2 partes y falsifica los intercambios para hacerse pasar por una de ellas.
- **Ataques de replay:** una forma de ataque de red en el cual una trasmisión de datos válida es maliciosa o fraudulentamente repetida o recalcada, es llevada a cabo por el autor o por un adversario que intercepta la información y la retransmite posiblemente como parte de un ataque enmascarado.