CLASE 15

AMENAZAS

|  |
| --- |
| **Amenazas Informáticas**   * ciberseguridad   + disciplina dentro del campo de la informática encargada de la protección de sistemas, redes, programas e individuos de ataques cuyo fin es el de conseguir, destruir o capturar información privilegiada o confidencial a cambio de algún beneficio ya sea económico, social, reputacional, etc. * malware   + término amplio que describe cualquier programa o código malicioso que es dañino para los sistemas   + tipos     - virus       * tipo de programa o código malicioso escrito para modificar el funcionamiento de un equipo       * diseñado para propagarse de un equipo a otro       * insertan o se adjuntan a un programa o documento legítimo que admite macros a fin de ejecutar su código     - troyano       * se camufla como software legítimo       * una vez activados, los troyanos pueden permitir a los cibercriminales espiar, robar datos confidenciales y obtener acceso por una puerta trasera al sistema infectado       * no pueden multiplicarse     - gusanos       * programas que realizan copias de sí mismos, alejándose en diferentes ubicaciones del ordenador sin necesidad de interacción por parte del usuario       * el objetivo de este malware suele ser colapsar los ordenadores y las redes informáticas, impidiendo así el trabajo a los usuarios       * no infectan archivos     - adware       * programas diseñados para mostrar publicidad en la computadora, redirigir las solicitudes de búsqueda a sitios web de publicidad y recopilar datos comerciales acerca del usuario (como los tipos de sitios web que visitas) para mostrarte avisos personalizados       * pueden ser maliciosos (sin autorización del usuario), o invasivos (autorización del usuario)     - spyware       * recopilan información de un ordenador o dispositivo informático y transmitir la información a una entidad externa sin el permiso del dueño del ordenador     - rootkit       * diseñado para infectar un PC, el cual permite  instalar diferentes herramientas que le dan acceso remoto al ordenador       * se oculta en la máquina, dentro del sistema operativo     - botnet       * utiliza virus troyanos especiales para crear una brecha en la seguridad de los ordenadores de varios usuarios, tomar el control de cada ordenador y organizar todos los equipos infectados  que el cibercriminal puede gestionar de forma remota     - crimeware       * utiliza la ingeniería social principalmente para lograr su objetivo       * buscan principalmente credenciales de acceso a bancos, métodos de pago y todo lo relacionado con las finanzas     - ransomware       * diseñado para infiltrarse y encriptar información sin el consentimiento de su propietario * seguridad de la información   + pilares:      * protección de la información:      * fallas y vulnerabilidades   + fallas     - una falla o bug (insecto) es un error en un programa o S.O. que desencadena un resultado no deseado     - tipos:      * vulnerabilidades   + debilidad o fallo de un sistema informático que puede poner en riesgo la integridad, confidencialidad o disponibilidad de la información   + pasos para detectar una vulnerabilidad: |