|  |
| --- |
| Amenazas Informáticas -Clase 15 |
| **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: |
| Seguridad Informática -Clase 17 |
| **Seguridad Informática**   * seguridad activa   + protege y evita daños en los sistemas informáticos   + elementos activos     - servidores, dispositivos móviles, bases de datos, entre otros     - contienen información que alguien quiere vulnerar, obtener, destruir, etcétera   + buenas prácticas:     - uso y empleo adecuado de contraseñas. Una de las técnicas para que una contraseña sea segura consiste en la combinación entre letras, números, mayúsculas y otros caracteres. No se debe usar nombre de mascotas o fechas de nacimiento, entre otros datos que pueden ser de conocimiento público.     - uso de software de seguridad informática, como antivirus, antiespías y cortafuegos.     - encriptar los datos importantes: La encriptación consiste en cifrar los datos o la información mediante un algoritmo de cifrado con una clave para que el dato/información sólo pueda ser leído si se conoce la clave de cifrado. * seguridad pasiva   + conjunto de acciones o técnicas de seguridad que entran en acción para minimizar los daños a los sistemas informáticos   + se activan cuando se ha introducido un malware o cualquier otra amenaza en los sistemas   + buenas prácticas:     - la realización de copias de seguridad de los datos en más de un dispositivo y/o en distintas ubicaciones físicas.     - escanear y limpiar continuamente los equipos para controlar y evitar ataques de malware.     - crear particiones en el disco duro para almacenar archivos y backups/copia de seguridad en una unidad distinta a donde tenemos nuestro sistema operativo.     - frente a un ataque, desconectar el equipo de la red hasta que se pueda solucionar.     - es importante que cuando haya una infección por un virus, comprobar que el antivirus funcione correctamente. * medios de protección   + para que la seguridad informática sea integral sobre los equipos y software informáticos se deben implementar también algunos controles de tipo administrativo y físicos   + clases:      * + auditorías     - auditar es la acción de analizar de manera exhaustiva y profunda las distintas características y áreas de una organización     - en informática, el auditor es el encargado de analizar y determinar que toda la informática de la organización trabaje de manera eficiente     - objetivos:      * + - conocimientos del auditor informático      * + - auditor       * trabajan en pequeños grupos de hasta 4 personas y son el nexo directo con los distintos departamentos y dirección       * plasmará en un informe final todas las debilidades, oportunidades de mejora y recomendaciones para que la organización sin carácter obligatorio decida si aceptarlas o no     - herramientas para auditar      * seguridad física   + establecimiento de técnicas que permiten resguardar de cualquier tipo de daños a los equipos en los cuales se almacena los activos de una organización, sus datos   + tipos:      * seguridad física   + tipo de software que impide que malware o hackers puedan ingresar a nuestra computadora a través de Internet o de una red * seguridad lógica   + conformada por un conjunto de procesos que se encargan de garantizar la seguridad de los datos y sistemas, además controlan el acceso a los mismos   + incluye aspectos como:      * Hacking y Cracking   + hacker     - persona que hackea cualquier tipo de sistema para descubrir sus vulnerabilidades con el objetivo de poder encontrar alguna herramienta que la minimice o suprima —en el caso de un white hat— o utilizar esta vulnerabilidad a su favor —en el caso de un black hat— y esto lo logra en base a su conocimiento     - tipos       * white hats: utilizan los conocimientos en informática y seguridad informática con el fin de defender los sistemas de información       * gray hats: tienen conocimientos tanto de la parte defensiva como ofensiva y pueden trabajar en cualquiera de los ámbitos       * black hats: tienen conocimientos informáticos y recurren a hacer actividades maliciosas o ilegales. También conocidos como crackers     - diferencias entre hacker y cracker       * hacker es un experto en varias ramas técnicas relacionadas con las tecnología de información de las comunicaciones, como son: programación, redes, sistemas operativos e ingeniería de software       * cracker es también un experto, pero además es quien viola la seguridad de un sistema informático con fines ilícitos o con un objetivo deshonesto y no ético |