CLASE 17

SEGURIDAD INFORMATICA

|  |
| --- |
| **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 |

ACTIVIDAD EN CLASE EN VIVO

Escenarios para grupos  - 1, 3, 5, 7, 9

Empresa emergente  dedicada a la venta de productos fertilizantes para campos, con una capacidad financiera acotada, todos sus empleados trabajan on site y están dispuesto  a recibir capacitación, poseen actualmente dos personas encargadas de sistemas, las cuales manejan información sensible, pero que todos los usuarios pueden ver (no es política de la empresa), no realizan copias de información porque no las creen convenientes. Poseen una página web donde hay catálogos y los clientes pueden hacer compras a través de la misma.

1. Hacer un análisis de la situación actual de cada empresa que nos toque.
2. Para cada escenario planteado, crear un plan de seguridad
3. Este plan debe ser de 6 pasos e incluir, seguridad lógica, física, pasiva, activa y controles de medida de seguridad, y de vulnerabilidades que podrían explotar los atacantes.

**Casos de acción**

1. **Seguridad lógica:** generar controles de acceso para limitar el acceso a información sensible, como así también cifrar las comunicaciones relacionadas a las transacciones de venta dentro de la plataforma.
   1. Implementar un esquema de seguridad que permita el acceso a elementos de sistemas únicamente a personal autorizado.

Instalar antivirus y firewalls en todos los equipos de la red local y en los backups remotos.

1. **Física:** Realizar copias de seguridad de los datos.
   1. Faltaría implementar UPS, sistemas redundantes y protección ante amenazas externas como pararrayos, alarmas contra incendio e intrusos, extintores.
2. **Pasiva:** En el disco duro generar backups en una unidad distintas a el S.O. y backups versionados on-cloud.
   1. Programar actualizaciones y escaneos periódicos del antivirus corporativo.
3. **Activa:** Encriptar los datos para que no tengan acceso todos los usuarios a la info sensible.
   1. Establecer políticas de contraseñas seguras para empleados y modificar el login en la página para que solo permita crear cuentas bajo el cumplimiento de dichas políticas.
4. **Controles de seguridad:** dado que los empleados están dispuestos a recibir capacitación, se pueden usar medidas preventivas: informando qué es lo que puede suceder dadas ciertas acciones indebidas, para poder prevenirlas.
5. **Vulnerabilidades:** información sensible no confidencial (cualquier usuario puede verla). Capacitar a los empleados, educando sobre ataques de ingeniería social (realizar simulacros de phishing, rondas informativas, etc.).

Enviar al equipo de sistemas a la DEFCON 21 (https://www.defcon.org/)