**Preguntas de seguridad**

¿Qué son los tokens de seguridad?

* Un token de seguridad es un dispositivo físico y portátil que genera una clave de manera aleatoria, la cual se actualiza automáticamente tras un periodo de tiempo determinado. Estos tokens están conectados a un recurso electrónico al cual un usuario sólo podrá acceder son la clave de su token, gracias a este dispositivo se reducen en gran medida las posibilidades de fraude.

¿Qué es la criptomoneda? Explica cómo funcionan.

* La criptomoneda es un tipo de divisa digital, la cual utiliza técnicas criptográficas para controlar las transacciones y que no tengan que depender de las entidades financieras. Estas tienen muchas características similares al dinero convencional ya que pueden ser transferidas a cualquier parte del mundo y ser cambiadas por bienes o servicios.

¿Qué es el ciber espionaje? Indica un hecho histórico en este aspecto.

* El ciber espionaje es el conjunto de técnicas que se utilizan para obtener información confidencial de personas u organizaciones sin su permiso. Estos ataques se pueden realizar desde cualquier punto del mundo a través de la utilización de malware (Troyanos y Spyware).
* Un caso histórico de ciber espionaje fuer el “Octubre Rojo”. Un malware que descubrió vulnerabilidades de Microsoft Word y Excel con el fin de infiltrarse en sistemas ajenos y recopilar datos.

Busca dos ataques criptográficos en nuestra historia reciente, indica que ocurrió y como se solucionó.

* La aseguradora Adeslas sufrió un ataque criptográfico en su sistema el día 9 de septiembre de 2020. La empresa ha sido víctima de un ataque con *ransomware* el cual ha encriptado gran parte de la información que tenían en sus bases de datos. Esto supone un secuestro de la información que manejaba esta compañía y debido a que no han aceptado pagar para recuperar la información han terminado perdiendo gran parte de la información que tenían. Aún a día de hoy siguen trabajando para restaurar la información a través de sus copias de seguridad.
* En octubre de 2020 se descubrió una vulnerabilidad que permitía hacerse con las claves de cifrado de conexiones VPN o sesiones WEB. Esta vulnerabilidad afectó a un gran número de dispositivos de la marca Cisco que utilizaban un algoritmo de generación de números pseudoaleatorios. El ataque DUHK (Don’t use Hard Keys) consiguió descifrar estas claves a partir de la obtención de la semilla que utiliza este algoritmo para generar números

Busca cual es el futuro de la criptografía.

* El futuro de la criptografía pasa por la computación cuántica. Los algoritmos de clave pública / clave privada actual como el RSA utilizan la factorización de números primos enormes como base para su seguridad, un ordenador actual tardaría décadas en descomponer uno de estos números. Sin embargo, los ordenadores cuánticos pueden realizar esta tarea en cuestión de minutos. Debido al arma de doble filo que pueden suponer los ordenadores cuánticos, ya se están desarrollando algoritmos que puedan ser resistentes ante tal capacidad de computación. En la actualidad hay un total de 48 algoritmos en desarrollo para hacer frente a este problema pero los propios algoritmos suponen un problema de por sí para los ordenadores actuales ya que requieren una alta capacidad de recursos y memoria.