ACTIVIDADES SOBRE SEGURIDAD INFORMÁTICA

1. Abre el navegador **Google Chrome** e investiga cómo se eliminan los datos de navegación (el Historial, las Cookies y los Archivos Temporales). Escribe detalladamente la secuencia de pasos a seguir para conseguirlo.

2. Instala **Mozilla Firefox** y realiza las mismas operaciones del ejercicio anterior con el navegador Mozilla Firefox. Escribe, de nuevo, la secuencia de pasos a seguir.

3. ¿Cuál es término correcto para referirse genéricamente a todos los programas que pueden infectar ordenador?

4. Define los términos:
   a. Seguridad física
   b. Seguridad lógica
   c. Seguridad activa
   d. Seguridad pasiva

5. Enumera algunas medidas de seguridad física
6. Enumera algunas medidas de seguridad lógica.
7. Investiga **cómo funciona un antivirus** leyendo el siguiente artículo:
   http://www.escudoantivirus.com/como-funciona-un-antivirus/

8. Enumera diez anivirus gratuitos. Consulta en el siguiente artículo:
   https://www.xataka.com/basics/once-programas-para-eliminar-malware-gratis-como-utilizarlos

9. Explica las diferencias entre **Virus, Gusano y Troyano.**

10. Investiga en Internet qué caracteriza el comportamiento de los siguientes tipos de malware (son algunos de los más conocidos):
    a. Adware:
    b. Bloqueador:
    c. Bulo (Hoax):
    d. Capturador de pulsaciones (Keylogger):
    e. Espía (Spyware):
    f. Ladrón de contraseñas (PWStealer):
    g. Puerta trasera (Backdoor):
    h. Rootkit:
    i. Secuestrador del navegador (browser hijacker):
    j. Cibersquatting: (www.incibe.es/protege-tu-empresa/blog/aprende-detectar-el-cybersquatting-tu-marca)
    k. Eavesdropping
    l. Ataque man-in-the- middle.
    m. Ataque a la fuerza bruta. ¿Serías capaz de crear un programa para averiguar una contraseña de 4 caracteres?

11. Lee el artículo de la Oficina de Seguridad del Internauta (OSI) sobre redes zombi y responde:

https://www.osi.es/es/actualidad/blog/2014/03/14/que-es-una-botnet-o-una-red-zombi-de-ordenadores

a) ¿Cómo funciona una red zombi?
b) ¿Qué utilidad tiene que un ordenador pertenezca a una red zombi o botnet?
c) ¿Cómo puedes evitar que tu ordenador acabe en una botnet?

12. ¿Cuáles son las vías de entrada típicas del malware a los ordenadores?

13. Lee estos artículos sobre el **Phishing** y responde:
https://www.infospyware.com/articulos/que-es-el-phishing/
https://www.avast.com/es-es/c-phishing
    a) ¿Qué es el Phishing?
    b) ¿Qué tipo de información roba? y ¿Cómo se distribuye?
    c) ¿Cómo puedo reconocer un mensaje de phishing?
    d) Enumera algunos consejos para evitar y protegerse del phishing
14. ¿Qué es la criptografía?
15. Entra en la web siguiente y cifra el mismo mensaje "HOLA" con diferentes algoritmos de cifrado: AES, DES, Rijndael 192, Rijndael 256, Serpent, TripleDES, **https://cifraronline.com/**

16. Lee el siguiente artículo sobre el **certificado digital** y responde a las preguntas:

https://www.xataka.com/aplicaciones/certificado-digital-todo-lo-que-necesitas-saber-para-solicitar-e-instalarlo-en-tu-navegador

a) ¿Qué es un certificado digital?
b) ¿Qué nos permite hacer un certificado digital?
c) Pasos a seguir para solicitar el certificado digital
d) ¿Dónde se instala el certificado digital?