|  |  |
| --- | --- |
| **DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA** | |
| **Nombre de la Actividad** | Seguridad digital |
| **Objetivo de la actividad** | Reconocer las normas y estándares de seguridad de la información y la ciberseguridad. |
| **Tipo de actividad sugerida** | Falso-Verdadero |
| **Archivo de la actividad**  **(Anexo donde se describe la actividad propuesta)** | Anexos / CF01\_ActividadDidáctica |

**INSTRUCCIONES PARA EL APRENDIZ**

Apreciado aprendiz, a continuación encontrará una actividad didáctica, para afianzar los conceptos y aprendizajes del componente de formación. Lea, las situaciones y marque como falso o verdadero, la formulación a la cual corresponde.

1. Un estándar tiene como función la elaboración de una serie de especificaciones técnicas que son adoptadas de manera voluntaria.

R/ Verdadero.

1. Un intento de estandarizar seguridad en IoT lo realiza la ISO por medio de la norma ISO / IEC 3041.

R/ Falso.

1. Un *botnet* es un dispositivo IoT.

R/ Falso.

1. Una comunicación internet con dispositivos IoT no necesita encriptación.

R/ Falso.

1. El DDoS es sistema operativo *Disk Operating System*.

R/ Falso.

1. Autenticación es lo mismo que autorización.

R/ Falso.

1. SSL / TSL provee comunicación segura encriptando la información enviada entre un cliente y un servidor.

R/ Verdadero.

**Retroalimentación:**

**1.** La normalización o estandarización tiene como función la elaboración de una serie de especificaciones técnicas – NORMAS – que son adoptadas de manera voluntaria.

**2.** El estándar ISO / IEC 30141 es la primera arquitectura de referencia que tiene como objetivo hacer que el IoT sea eficiente, interrumpible, seguro y resistente a ataques.

**3.** Un *botnet* es un conjunto de dispositivos conectados a Internet, cada uno de los cuales está ejecutando uno o varios *bots*. Este lo que hace es atacar usando DDoS, enviar *spam* a los dispositivos, detectar contraseñas y distribuir *ransomware*.

**4.** Una debilidad grande es la transmisión de datos entre dos dispositivos IoT, estos dispositivos continuamente están transmitiendo información de todo tipo entre ellos y hacia los aplicativos en la nube, de aquí que es importante que la comunicación sea encriptada antes de enviarla.

**5.** Significa Denegación de Servicio Distribuido, en inglés *Distributed Denial of Service*, el objetivo de este ataque es inhabilitar por completo el uso de cualquier sistema, una aplicación *software* o una máquina.

**6.** La definición de autenticación y autorización son distintas en el contexto de la seguridad, la autenticación verifica la identidad del usuario que quiere acceder a un sistema, mientras que la autorización válida si efectivamente el usuario tiene el permiso para acceder al mismo.

**7.** El protocolo usa algoritmos de encriptación para cifrar la comunicación entre un cliente y un servidor.

**Correcto:**

Has relacionado correctamente cada uno de los conceptos con su respectiva respuesta, ¡Felicitaciones!, esto da cuenta de la comprensión de algunos conceptos clave del componente formativo. ¡Sigue adelante con el mismo empeño!

**Incorrecto:**

Has relacionado incorrectamente alguno de los conceptos con su respectiva respuesta, no te desanimes, revisa nuevamente el contenido del componente formativo y vuelve a intentarlo. ¡Mucho ánimo!