1**-** ¿Que es un metadato?

Son un conjunto de datos que describen el contenido informativo de un recurso, de archivos o de información de los mismos. Quiere decir, que es información que describe otros datos.

2- ¿Qué es un método de autenticación? ¿Por qué es recomendable utilizar 2FA?

Los métodos de autenticación son uno o varios **procedimientos informáticos** que permiten **confirmar que un usuario de un sitio o servicio es quien dice ser**.

Proporciona un **control de acceso a los sistemas**, comprobando si las credenciales de un sujeto se ajustan a aquellas registradas en una base de datos de usuarios autorizados o en un servidor de autenticación de datos.

Es recomendable utilizar una autentificación 2Fa ya que además de ingresar un usuario y contraseña, pide una segunda autenticación, de esa forma podemos evitar un ingreso a la cuenta no deseado. Al activarlo podemos verificar correctamente quien esta ingresando a la cuenta somos nosotros.

3- ¿Cuándo usamos redes WiFi públicas que recaudos debemos tomar?

* Verificar la autenticidad de la red WiFi
* Utilizar una red privada virtual (VPN)
* Evitar acceder a sitios web sensibles
* Asegurarse de que las páginas web sean seguras
* Desactivar la opción de compartir archivos
* Mantener actualizados tus dispositivos y aplicaciones
* Desconectarse de la red WiFi cuando no la necesites

4- ¿A qué nos estamos refiriendo con el término "Malware"?

El malware es un software o código informático diseñado para infectar, dañar o acceder a sistemas informáticos. Hay diferentes tipos de malware, y cada uno infecta o corrompe dispositivos de forma distinta, pero todas las variantes de malware están diseñadas para poner en peligro la seguridad y privacidad de los sistemas informáticos.

5- ¿A qué nos estamos refiriendo con el término "Ransomware"?

Un *r*ansomware es un malware que entra a un ordenador o a un sistema para **cifrar los datos que este contiene,** y de esta manera, pedir un “rescate” a cambio de liberar el bloqueo.

6- ¿A qué nos estamos refiriendo con el término "Phishing"?

Los ataques de phishing son correos electrónicos fraudulentos, mensajes de texto, llamadas telefónicas o sitios web diseñados para engañar a los usuarios para descargar [malware](https://www.ibm.com/es-es/topics/malware), compartir información confidencial o datos personales u otras acciones que expongan a sus organizaciones.

El phishing es el tipo más común de [ingeniería social](https://www.ibm.com/es-es/topics/social-engineering), la práctica de engañar, presionar o manipular a las personas para enviar información o activos a las personas equivocadas.

7- ¿Qué es una red VPN, Tor, darknet?

**Que es un proxy?**