TALLER CONTROL DE LA SEGURIDAD DIGITAL
INSTRUCTOR
JORGE ENRIQUE SANCHEZ PINO

1. ¿Qué es la seguridad informática y por qué es importante?

2. ¿Cuáles son las principales amenazas a la seguridad informática?

3. ¿Cuáles son las diferencias entre un virus, un gusano y un troyano?

4. ¿Qué es un ataque de fuerza bruta y cómo se puede prevenir?

5. ¿Qué es un ataque de phishing y cómo se puede detectar?

6. ¿Qué es el malware y cuáles son sus tipos más comunes?

7. ¿Cuáles son las mejores prácticas para crear contraseñas seguras?

8. ¿Qué es la autenticación de dos factores y cómo puede ayudar a mejorar la seguridad?

9. ¿Qué es una vulnerabilidad de día cero y cómo se puede abordar?

10. ¿Cuál es la importancia de mantener el software y los sistemas operativos actualizados?

11. ¿Qué es el cifrado y cómo se utiliza para proteger los datos?

12. ¿Cuál es la diferencia entre seguridad física y seguridad lógica?

13. ¿Qué es una política de seguridad de la información y por qué es necesaria?

14. ¿Cuáles son las medidas de seguridad que se pueden implementar en una red empresarial?

15. ¿Cómo se puede detectar si un dispositivo ha sido comprometido?

16. ¿Cuáles son los pasos que se deben seguir para responder a un incidente de seguridad informática?

17. ¿Qué es un cortafuegos (firewall) y cuál es su función principal?

18. ¿Cuál es la importancia de realizar copias de seguridad de los datos y cómo se pueden hacer de manera efectiva?

19. ¿Qué es un análisis de vulnerabilidades y cómo se puede llevar a cabo?

20. ¿Cuáles son las mejores prácticas para educar a los empleados sobre seguridad informática en una organización?