



## Guía Virtual de Networking Essential

Fecha de entrega 30 de septiembre

**Primera parte:** Complete el siguiente cuestionario en su cuaderno. Debe entregar como tarea las fotografías de su cuaderno en donde resolvió este cuestionario. Recuerde identificar cada página de su cuaderno en donde trabajó y que la fotografía sea clara.

1. ¿Qué son intrusos?
2. ¿Qué son amenaza?
3. ¿De qué forma pueden acceder los intrusos a nuestra red?
4. ¿Qué daños pueden causar los intrusos a la red a la que acceden?
5. ¿A quiénes se les llama piratas informáticos?
6. ¿Cuáles son las 4 amenazas que pueden causar los piratas informáticos?
7. ¿Por qué roban información los piratas informáticos?
8. ¿Qué efectos tiene para nosotros la pérdida o manipulación de datos por parte de los piratas informáticos?
9. ¿Cómo nos afecta la interrupción de servicios?
10. ¿Qué puede hacer un pirata informático si roba nuestra identidad?
11. ¿De dónde puede ser las amenazas a una red?
12. ¿Cómo se dan las amenazas externas?
13. ¿Cómo se dan las amenazas internas?
14. ¿Por qué las amenazas internas no siempre son intencionales?
15. ¿Cuándo son intencionales las amenazas internas?
16. Investiga y escribe brevemente "Cómo proteger la información en los dispositivos con computadoras, laptop, tablet o smartphones por robos"
17. ¿Por qué las conductas humanas son el método más común para obtener acceso a una red?
18. ¿Qué es la ingeniería social como amenaza para la seguridad de una red?
19. ¿Por qué un usuario es el enlace más débil en la seguridad de una red?
20. ¿Cuáles son los métodos más comunes utilizados por un hacker para obtener información?
21. ¿Cómo se realiza el pretexting?
22. ¿Cuáles serían ejemplos de pretexting?
23. ¿Cómo se realiza el phishing?
24. ¿Cómo se realiza el vishing o phishing telefónico?
25. ¿Cuáles son algunas de las técnicas de ataques por software a las redes?
26. ¿Qué es un virus informático?
27. ¿Cómo se puede transmitir un virus?
28. ¿Qué es un virus tipo gusano?
29. ¿Cómo funciona un virus tipo gusano?
30. ¿Qué es un virus tipo troyano?
31. ¿Cómo funciona un virus tipo troyano?
32. ¿Qué es el Saturación SYN (Sincrónica)?
33. ¿Cómo funciona el ping de la muerte?
34. ¿Qué significa DDoS?
35. ¿Cómo funciona del DDoS?
36. ¿Cómo funciona el ataque de fuerza bruta?
37. ¿Qué es un spyware?
38. ¿Qué son las cookies de seguimiento?
39. ¿Qué es el adware?
40. ¿Qué son los pop under y ventanas emergentes?
41. ¿Cuál es la diferencia entre un pop under y ventanas emergentes?
42. En una infección tipo botnet ¿Quién es el zombie y quién es el bot?
43. ¿Cuáles son algunos de los procedimientos simples de seguridad?
44. ¿Cuáles son algunos de los procedimientos avanzados de seguridad?
45. ¿Cuáles son dos de los procedimientos de seguridad más fáciles de implementar y no requieren de conocimientos técnicos avanzados?
46. Si mi equipo de fútbol favorito es comunicaciones y mi contraseña es Cremas ¿Cuál sería el procedimiento para que mi contraseña sea fácil de recordar, pero difícil de decifrar?
47. ¿Cuáles son algunas de las herramientas y aplicaciones de seguridad para la protección de redes?