Bastionado de redes y sistemas

1. **Firewalls y segmentación de redes**:
    - *Firewalls*: Estos dispositivos o programas se utilizan para filtrar y controlar el tráfico de red, protegiendo así la red contra posibles amenazas externas. Pueden ser hardware o software y establecen reglas para permitir o bloquear el tráfico basado en diversos criterios como dirección IP, puerto, protocolo, etc.
    - *Segmentación de redes*: Consiste en dividir una red en segmentos más pequeños o subredes para mejorar la seguridad. Esto reduce la superficie de ataque y limita la propagación de posibles amenazas.

2. **Políticas de acceso y control de permisos**:
    - Las políticas de acceso definen quién tiene acceso a qué recursos y en qué condiciones. Estas políticas deben ser coherentes, restrictivas y se aplican a través de mecanismos como la autenticación multifactorial, los niveles de privilegio, etc.
    - El control de permisos determina los niveles de acceso que tienen los usuarios o sistemas a recursos específicos, asegurando que solo tengan acceso a lo que necesitan y están autorizados a usar.

3. **Actualizaciones y parches de seguridad**:
    - Las actualizaciones y parches son fundamentales para cerrar posibles vulnerabilidades en sistemas y software. Mantener actualizados los sistemas y

aplicar parches de seguridad ayuda a proteger contra amenazas conocidas y ataques basados en vulnerabilidades conocidas.

4. **Monitoreo y registro de actividades**:
   - El monitoreo constante de la red y los sistemas permite identificar actividades inusuales o posibles intrusiones. Los registros de actividad son vitales para la detección de amenazas y para realizar un seguimiento de los eventos que ocurren en la red.

5. **Cifrado y protocolos seguros**:
   - El cifrado se utiliza para proteger los datos en tránsito y en reposo, convirtiendo la información en un formato ilegible para cualquier persona no autorizada. Los protocolos seguros, como HTTPS, SSH, etc., utilizan cifrado para garantizar la seguridad de las comunicaciones.

6. **Auditorías y pruebas de penetración**:
   - Las auditorías periódicas permiten evaluar la efectividad de las medidas de seguridad implementadas. Las pruebas de penetración, realizadas por profesionales de seguridad, intentan identificar debilidades y vulnerabilidades para corregirlas antes de que puedan ser explotadas por atacantes.

7. **Formación y concienciación en seguridad**:
   - La formación continua y la sensibilización sobre seguridad son cruciales. Los usuarios deben estar al tanto de las buenas prácticas de seguridad, cómo identificar posibles amenazas como el phishing o el malware, y cómo actuar frente a

ellas.