




El bastionado o *hardening* es un proceso por el que se implementan medidas técnicas y organizativas para reducir las vulnerabilidades de los sistemas, es decir, se trata de protegerlos para que los ciberdelincuentes o *crackers* no puedan acceder a ellos. Por lo tanto, el objetivo del bastionado es eliminar todos los riesgos posibles y minimizar la exposición a las amenazas.

Veamos algunas de las mejores prácticas para minimizar estos riesgos:

- **La auditoría de sistemas:** detectar los fallos y brechas de los sistemas, con el objetivo de establecer qué puntos deben priorizarse. 
- **Fortalecer la red:** asegurar las configuraciones de los cortafuegos o *firewalls*, bloquear o cerrar los puertos que no sean necesarios o no se utilicen; e implementar IDS e IPS para mejorar la protección del tráfico de red.
- **Configurar el *software* de forma segura:** y eliminar el que ya no se utilice o que haya quedado obsoleto. También es importante instalar sistemas operativos y aplicaciones de manera segura, descargados de páginas oficiales y mantenerlos actualizados. 
- **Implementar herramientas antivirus o *antimalware*** que prevengan o actúen eficazmente ante un posible ataque externo. Utilizar, incluso, sistemas EPP (Plataformas de Protección Endpoint) y EDR.
- **Crear políticas de seguridad de usuario:**
  - Contraseñas seguras.
  - Políticas de privilegios mínimos.
  - Políticas de necesidad de saber: acceder solo a la información necesaria para desempeñar sus funciones.
- **Clasificar la información:** según el carácter confidencial de la información, por ejemplo:
  - Confidencial.
  - Restringido.
  - Uso interno.
  - Público.