**Endurecimiento de seguridad:** proceso de reforzar un sistema para reducir su vulnerabilidad y superficie de ataque (vulnerabilidades potenciales que se pueden explotar). Por ejemplo, en una casa la superficie de ataque serian puertas y ventanas que un ladrón puede usar para acceder, y el endurecimiento sería poner cerraduras. Como parte del endurecimiento de seguridad, los analistas realizan procedimientos regulares de mantenimiento para mantener los dispositivos y sistemas de red funcionando de forma segura y óptima. Puede llevarse a cabo en cualquier dispositivo o sistema que pueda verse comprometido, tanto hardware como software, por lo tanto, puede incluir la protección de un espacio físico con cámaras y guardias. Algunos de los tipos mas comunes de procedimientos de endurecimiento de seguridad son:

* Actualizaciones de software (parches): son realizadas para aumentar la seguridad y corregir vulnerabilidades de una red
* Cambios en la configuración de aplicaciones de dispositivos: un ejemplo de esto puede ser exigir contraseñas más largas o un cambio más frecuente de las mismas
* Eliminación o desactivación de aplicaciones y servicios no utilizados
* Desactivación de puertos no utilizados
* Reducción de los permisos de acceso en los dispositivos
* Minimizar el número de aplicaciones, dispositivos, puertos y permisos de acceso, lo que hace que la supervisión de la red y los dispositivos sea más eficiente y reduce la superficie de ataque global
* Realizar pruebas de penetración periódicas
* Eliminación de hardware y software
* Implementación de políticas de contraseña seguras: requiere que las contraseñas sigan unas reglas específicas, como por ejemplo un carácter especial, una mayúscula, 3 números y 3 dígitos como mínimo, etc. Además, establecen otras normas como bloquear la cuenta en caso de introducir de forma incorrecta “x” veces la contraseña
* Autenticación de múltiples factores: medida que requiere que un usuario verifique su identidad de dos o más formas para acceder a un sistema

**Sistema operativo:** interfaz entre el hardware de la computadora y el usuario, es el primer programa que se carga cuando se enciende la computadora. Actúa como intermediario entre las aplicaciones de software y el hardware del ordenador. Es importante que sea seguro ya que sino puede llevar a que toda una red se vea comprometida. Algunas tareas de endurecimiento de los SO se realizan a intervalos regulares, tales como actualizaciones, copias de seguridad y mantener una lista actualizada de dispositivos y usuarios autorizados. Otras, se realizan solo una vez como parte de las medidas de seguridad preliminares, como configurar un dispositivo para que se ajuste a un estándar de encriptación segura. Un caso específico puede ser la instalación de parches, que es una actualización de software y sistema operativo que aborda vulnerabilidades de seguridad dentro de un programa o producto. En el caso de los proveedores de SO, con los parches, el sistema debe actualizarse a su última versión, ya que a veces los mismos se publican para solucionar problemas con vulnerabilidades, lo que podría generar que un actor malicioso busque la vulnerabilidad especifica en el SO viejo y así atacar a los usuarios desactualizados

Una *configuración de línea base* es un conjunto documentado de especificaciones dentro de un sistema que se utiliza como base para futuras construcciones, lanzamientos y actualizaciones, como una regla de firewall con una lista de puertos permitidos o no

**Ataque de fuerza bruta:** proceso de ensayo y error para descubrir información privada, entre ellos se encuentran:

* **Ataque de fuerza bruta simples:** cuando los atacantes intentan adivinar las credenciales de inicio de sesión de un usuario, se puede hacer introduciendo cualquier combinación de nombres y contraseñas hasta que funcione
* **Ataques de diccionario:** los atacantes usan una lista de contraseñas de uso común y credenciales robadas en violaciones anteriores para acceder a un sistema