**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

**Maquinas virtuales (VM):** son versiones de software de las computadoras físicas. Proporcionan una capa adicional de seguridad para una organización porque pueden utilizarse para ejecutar código en un entorno aislado, evitando que el mismo afecte al resto de la computadora, además, pueden eliminarse y sustituirse por una imagen prístina después de probar software malicioso. Son útiles cuando se investigan maquinas potencialmente infectadas o se ejecuta software malicioso en un entorno restringido, aunque también existe el pequeño riesgo de que el programa se escape y acceda a la maquina anfitriona

**Entorno aislado (Sandbox):** tipo de entorno de pruebas que le permite ejecutar software o programas separados a su red y se suele usar para probar parches, identificar y solucionar errores o detectar vulnerabilidades. También se pueden usar para evaluar software sospechoso archivos que contienen código malicioso y simular escenarios de ataque. Pueden ser ordenadores físicos autónomos que no están conectados en una red, aunque es más rentable y económico usar software o maquinas virtuales basadas en la nube

Existen medidas que se usan para evitar ataques de fuerza bruta y similares:

* ***Salting y hash:*** convierte la información en un valor único que puede usarse para determinar su integridad. Es una función unidireccional por lo que es imposible de desencriptar y obtener el texto original. Añade caracteres aleatorios a las contraseñas hash, aumentando la longitud y complejidad
* ***Autenticacion de multiples factores y de 2 factores:*** medida de seguridad que requiere que un usuario verifique de dos o mas formas su identidad
* ***CAPTCHA y reCAPTCHA:*** CAPTCHA son las siglas de Completely Automated Public Turing Test to Tell Computers and Humans Apart (Prueba de Turing pública completamente automatizada para distinguir entre ordenadores y humanos). Pide a los usuarios que completen una prueba que muestra que son humanos
* ***Politicas de contraseñas:*** directrices sobre lo compleja que debe ser una contraseña

**Endurecimiento de red:** se centra en el endurecimiento de la seguridad relacionada con la red, como el filtrado de puertos, los privilegios de acceso a la red y encriptación a través de red. Ciertas tareas de endurecimiento de la red se realizan regularmente , mientras que otras se realizan una vez y luego se actualizan según sea necesario. Algunas de las realizadas periódicamente son:

* Mantenimiento de las reglas de firewall
* Análisis de registros de red
* Actualizaciones de parches
* Copias de seguridad de servidores

Los equipos de seguridad usan las herramientas SEM para llevar a cabo el análisis de registros de red

Entre las tareas que se realizan una vez se encuentran:

* Filtrado de puertos en cortafuegos: función del cortafuegos que bloquea o permite ciertos puertos para limitar la comunicación no deseada
* Privilegios de acceso a la red
* Encriptación para la comunicación

**Sistema de detección de intrusiones (IDS):** aplicación que monitoriza la actividad del sistema y alerta sobre posibles intrusiones. Alerta a los administradores basándose en la firma del tráfico malicioso

Esta configurado para detectar ataques conocidos y suelen olfatear los paquetes de datos mientras se desplazan por la red y los analizan en busca de características de ataques desconocidos. Algunos sistemas IDS revisan no sólo en busca de firmas de ataques conocidos, sino también de anomalías que podrían ser el signo de una actividad maliciosa. Cuando el IDS descubre una anomalía, envía una alerta al administrador de la red, que puede investigar más a fondo.

Las limitaciones de los sistemas IDS son que sólo pueden buscar ataques conocidos o anomalías evidentes. Los ataques nuevos y sofisticados podrían no ser detectados. La otra limitación es que el IDS no detiene realmente el tráfico entrante si detecta algo raro. Depende del administrador de la red detectar la actividad maliciosa antes de que cause algún daño a la red.

Si se lo combina con un firewall, añade otra capa de defensa

**Sistema de prevención de intrusiones (IPS):** monitoriza la actividad del sistema en busca de actividades intrusivas y toma medidas para detenerlas. Es mas seguro que un IDS porque no solo alerta, sino que protege

Las organizaciones usan cada vez más redes en la nube, por lo que los analistas deben proteger tanto redes locales como en la nube. Una red en la nube es un conjunto de servidores remotos que ofrecen almacenamiento, procesamiento y análisis bajo demanda. Estos servidores requieren endurecimiento de seguridad y mantenimiento, ya que los proveedores no pueden prevenir todas las intrusiones. A diferencia de las redes tradicionales, se usa una imagen de línea base para comparar y detectar cambios no autorizados. Además, los datos y aplicaciones se separan por tipo y función. La seguridad es una responsabilidad compartida entre el proveedor y la organización, que debe aplicar sus propias medidas de protección.

**Gestión de identidad y acceso:** conjunto de procesos y tecnologías que ayuda a las organizaciones a gestionar las identidades digitales en su entorno, también autoriza como los usuarios pueden utilizar los diferentes recursos de la nube. Un problema común al que se enfrentan las organizaciones cuando utilizan la nube es la configuración poco precisa de los roles de usuario en la nube. Un rol de usuario mal configurado aumenta el riesgo al permitir que usuarios no autorizados tengan acceso a operaciones críticas en la nube.

**Configuración:** cada servicio en la nube requiere una configuración precisa para mantener los estándares de seguridad y cumplimiento. Esto se intensifica durante las migraciones a la nube donde es fundamental garantizar una configuración precisa para cada proceso migrado. Un descuido en este aspecto puede exponer la red a las vulnerabilidades

**Ataques de día cero:** importante consideración de seguridad para las organizaciones que utilizan soluciones de red en nube o tradicionales instalaciones. Es un exploit desconocido hasta ahora. Es más probable que los CSP sepan de un ataque de día cero antes que una organización de TI tradicional. Los CSP disponen de métodos para parchear hipervisores y migrar cargas de trabajo a otras máquinas virtuales. Estos métodos garantizan que los clientes no se vean afectados por el ataque. También hay varias herramientas disponibles para parchear a nivel de sistema operativo que las organizaciones pueden utilizar.

**Visibilidad y seguimiento:** los administradores de red tienen acceso a todos los paquetes de datos que cruzan la red, tanto con las locales como en la nube, por lo que pueden husmear e inspeccionar los paquetes para conocer el rendimiento de la red o comprobar posibles amenazas y ataques. Esta visibilidad también es ofrecida en la nube a través de registros de flujo y herramientas como la duplicación de paquetes. Los CSP asumen la responsabilidad de la seguridad en la nube, pero no permiten que las organizaciones que utilizan su infraestructura supervisen el tráfico en los servidores del CSP. Muchos CSP ofrecen fuertes medidas de seguridad para proteger su infraestructura. Aun así, esta situación puede preocupar a las organizaciones acostumbradas a tener pleno acceso a su red y sus operaciones. Los CSP pagan auditorías de terceros para verificar el grado de seguridad de una red en la nube e identificar posibles vulnerabilidades. Las auditorías pueden ayudar a las organizaciones a identificar si alguna vulnerabilidad se origina en la infraestructura local y si hay algún incumplimiento por parte de su CSP.

**Modelo de responsabilidad compartida:** es un principio de seguridad en la nube que establece que el CSP debe asumir la responsabilidad de la seguridad que afecta a la infraestructura en la nube, incluidos los centros de datos físicos, los hipervisores y los sistemas operativos del host. La empresa que utiliza el servicio en nube es responsable de los activos y procesos que almacena u opera en la nube. Este modelo garantiza que tanto el CSP como los usuarios acordaron sobre donde empieza y termina su responsabilidad acerca de la ciberseguridad. El problema se produce cuando la organización asume que el CSP se ocupa de una seguridad de la que no se responsabiliza

**Hipervisores:** abstraen el hardware del host del entorno del software operativo y existen dos tipos:

1. *Hipervisores de tipo uno:* se ejecutan en el hardware de la computadora anfitriona, por ejemplo, ESXi de VMware
2. *Hipervisores de tipo dos:* funcionan en el software de la computadora del host, como VirtualBox

Los proveedores de servicios en la nube suelen usar los hipervisores de tipo uno y son responsables de gestionarlo junto con otros componentes de virtualización. El CSP se asegura de que los recursos y los entornos de la nube estén disponibles y proporciona parches y actualizaciones con regularidad. Vulnerabilidades en los hipervisores o errores de configuración pueden provocar escapes de maquinas virtuales, lo que es un exploit en el que un actor malicioso obtiene acceso al hipervisor principal

**Línea de base:** cubre, para las redes y operaciones en la nube, como se configura y establece el entorno, es un punto de referencia físico que se puede usar para comparar los cambios realizados. Una configuración y puesta a punto adecuada puede mejorar en gran medida la seguridad y el rendimiento en la nube, como por ejemplo, restringir el acceso al portal de administración del entorno de la nube

**Criptografía en la nube:** se puede usar para asegurar los datos que se procesan y almacenan en un entorno de nube. La misma utiliza sistemas de encriptación y gestión segura de claves para proporcionar integridad y confidencialidad a los datos

**Borrado criptográfico:** método para borrar la clave de encriptación de los datos. Cuando se destruyen los datos en la nube, los métodos mas tradicionales no son tan eficaces, por lo que se usa el borrado criptográfico para destruir las claves criptográficas que desencriptan datos, lo que hace que nadie pueda acceder a los datos en el futuro

**Gestión de claves:** la encriptación moderna se basa en mantener seguras las claves de encriptación, algunas medidas son:

* Modulo de plataformas de confianza (TMP): es un chip de computadora que puede almacenar de forma segura contraseñas, certificados y claves de encriptación
* Modulo de seguridad de hardware de la nube (CloudHSM): dispositivo informático que proporciona almacenamiento seguro para claves criptográficas y procesa operaciones como la encriptación y desencriptación