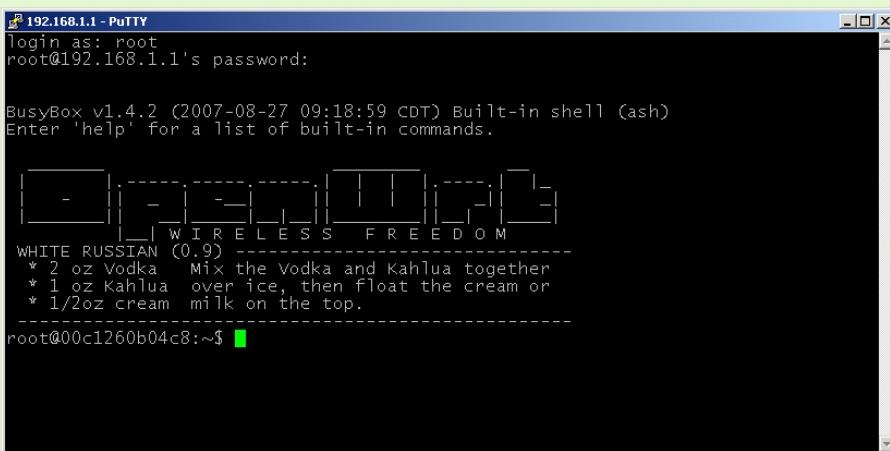


# **Configuración de los sistemas informáticos.**

## Caso práctico



El responsable de seguridad de los sistemas informáticos de la empresa ACME SL ha estado analizando algunos de los servicios detectando que el servicio SSH es muy utilizado por

los administradores de la empresa. Al ser un servicio crítico, considera que debe ser bastionado de cara a aumentar el nivel de seguridad de las tareas asociadas a la utilización del SSH.

Para ello deberán implementarse una serie de medidas de seguridad que afectan a los sistemas informáticos en los que se use SSH.

## **Objetivos:**

En esta unidad se conocerán los protocolos para el intercambio de comandos y transferencia de ficheros más comunes. Explicando las características de cada uno de ellos y cuáles de estos pueden ser vulnerados y atacados desde el punto de vista de la seguridad. Nos centraremos en la características de cifrado, autenticación y protocolos de operación para definir las reglas de firewall a nivel local y de dispositivos de red.

Este análisis inicial nos permitirá explicar posteriormente el paradigma de reducción de la superficie de exposición, para sólo aquellos protocolos necesarios en nuestro sistema.

Estudiaremos cómo se relación los procesos del sistema con la seguridad, y cómo podemos aplicar medidas de protección de los procesos: ASLR y DEP o contar con el apoyo de herramientas que nos permitan controlar los procesos y vigilarlos.

También trataremos los sistemas de protección de frente a virus e intrusiones como son los HIDS.

Cerraremos el capítulo explicando la importancia de tener un plan de copias de seguridad para no perder la información en caso de desastre o incidente, sobretodo ante el creciente número de incidentes de ransomware. Y con otra medida de respaldo con la contratación de servicios a proveedores externos y las políticas de seguridad que debemos tener en cuenta ante su externalización

# 1.- Reducción del número de servicios, Telnet, RSSH, TFTP, entre otros.



## Caso práctico

En los sistemas antiguos de la fábrica se tiene que utilizar protocolo FTP debido a que los sistemas son antiguos (sistemas legacy) y no pueden cambiar. Unos auditores externos han recopilado información del sistema para comentarnos las debilidades. Nos han entregado un fichero con todas las contraseñas de los robots.



[plusplushosting](#). Extrayendo contraseñas de las comunicaciones (Dominio público)

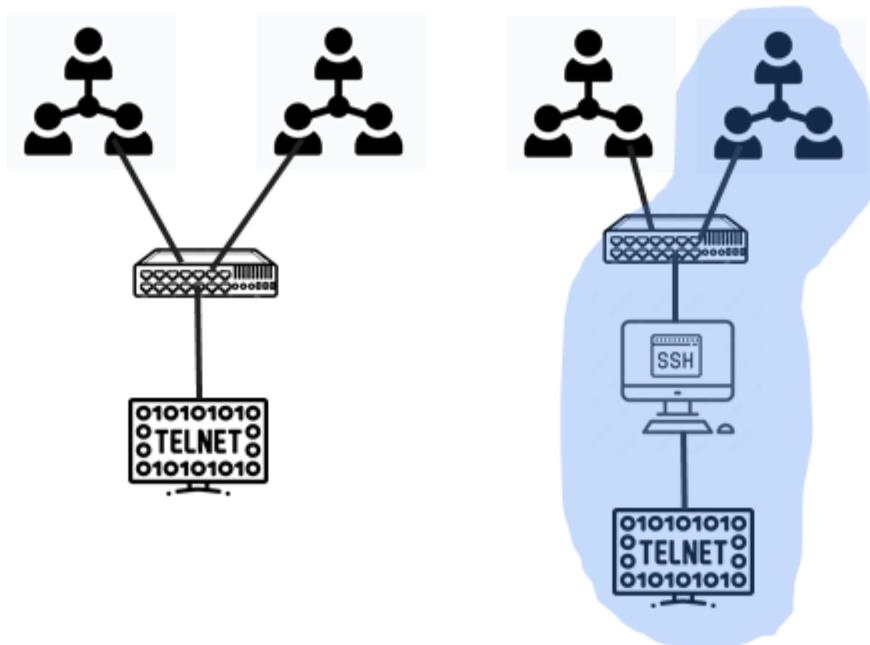
¿Por qué crees que ha pasado esto?

FTP

Aquellos protocolos que no sean necesarios y sean vulnerables, deben ser eliminados de los sistemas. Ya que es necesario la protección de los sistemas a través de la eliminación de aquellos protocolos que no sean seguros o que presenten vulnerabilidades.

Si los protocolos vulnerables son imprescindibles para la operativa del sistema. Se deben realizar un túnel, tunelización, de las comunicaciones para poder realizar la comunicación de una manera más segura. Otro de los mecanismos de seguridad es establecer reglas de comunicación en base a la configuración de los firewalls de red y los firewalls locales del equipo que alberga el servicio.

Otro de los mecanismos es aislar el servicio vulnerable y acceder únicamente desde una máquina de salto que tenga un protocolo y una medidas de seguridad adecuadas, mitigando el riesgo a través del acceso controlado desde una sola máquina.



Héctor Fernández Bardal (Dominio público)

La utilización de comunicaciones cifradas a través de protocolos de comunicación seguro es un requisito de seguridad del bastionado de los sistemas. Para saber las vulnerabilidades de los protocolos se pueden buscar a través de páginas web públicas donde se indican qué vulnerabilidades tienen los protocolos que se están utilizando.

- <https://www.cvedetails.com/>
- <https://cve.mitre.org/>
- <https://www.incibe-cert.es/alerta-temprana/vulnerabilidades>
- <https://www.exploit-db.com/search>

La utilización de protocolos vulnerables puede proporcionar a los atacantes un método de acceso inicial para posteriormente continuar en la toma de control del sistema, bien a través de exploits, shell de control remoto, revelación de información, ...

# 1.1.- Telnet.

Telnet es un protocolo que permite conectarse a un equipo y ejecutar de comandos de manera remota. Se establece inicialmente una comunicación cliente-servidor que permite interactuar con el servidor. El puerto reservado para el servicio de telnet es TCP 23.

Los mensajes se envían en claro (sin cifrar), por lo que un atacante que esté escuchando la conversación podría leer los comandos ejecutados, así como otro tipo de información como son los nombres de usuarios y contraseñas que se intercambian en la comunicación.

Telnet es un comando que está tanto en los sistemas operativos Windows como Linux. Aunque existen programas que permiten ejecutar el cliente para conectarse contra un servidor remoto:

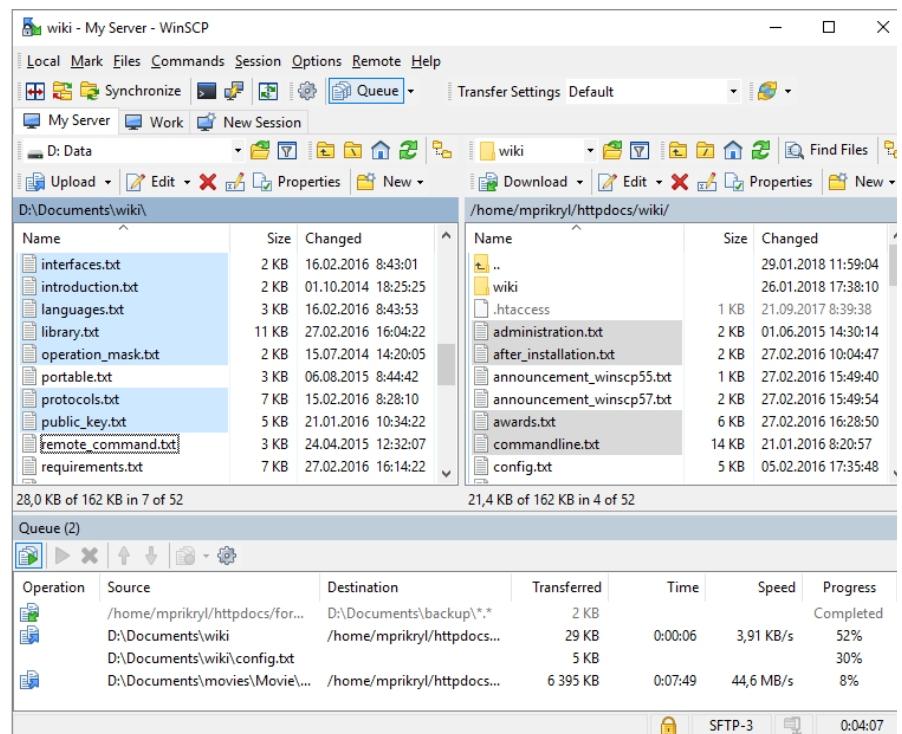
- [WinSCP](#)
- [Putty](#)

Mediante la herramienta nmap, podemos hacer un fingerprint del protocolo que esté corriendo en remoto, para saber la versión del servidor de telnet, si tiene vulnerabilidades conocidas, ...

Además, existen herramientas de fuerza bruta que nos permiten adivinar el usuario y la contraseña como son: [hydra](#), [medusa](#), ...

La mejor forma de bastionar el protocolo Telnet es sustituirlo por SSH. Si por cualquier caso el servicio debe estar disponible porque está implementado en un “sistema legacy” el objetivo es configurarlo de manera segura e implementar medidas de refuerzo complementario (**medidas compensatorias**) como pueden ser:

- Aumentar la vigilancia mediante la monitorización.
- Diseño de arquitectura basado en el aislamiento del servicio, o control de acceso a través de una máquina de salto.
- Aumentar el control de acceso al servicio.
- Reforzar las medidas de seguridad del sistema operativo base que alberga el servicio.
- ....



Y en cuanto sea posible, sustituir el protocolo por otro que cumpla con los requisitos funcionales y pueda tener un mayor nivel de seguridad.

Recuerda que dentro de las medidas generales de seguridad también se deben implementar en estos servicios:

- Actualizaciones del producto.
- Copias de seguridad de la configuración y de los datos.
- Establecer una máquina de salto a un servidor ssh para posteriormente acceder al servicio vulnerable.

Telnet a veces es utilizado por los atacantes como método rápido para la obtención de información del sistema a través del “Banner” del servicio. (Fingerprint). También se podría utilizar telnet para interactuar con el protocolo SNMP (TCP/25), POP3 (TCP/110), IMAP (TCP/143), HTTP (TCP/80),...

## Para saber más

Para más información sobre como sustituir el [servicio telnet por ssh de SANS](#).



## Autoevaluación

¿Para qué otra cosa se puede utilizar telnet?

- Ataque de fuerza bruta
- Saber las vulnerabilidades
- Analizar puertos abiertos y enviar comandos al servidor

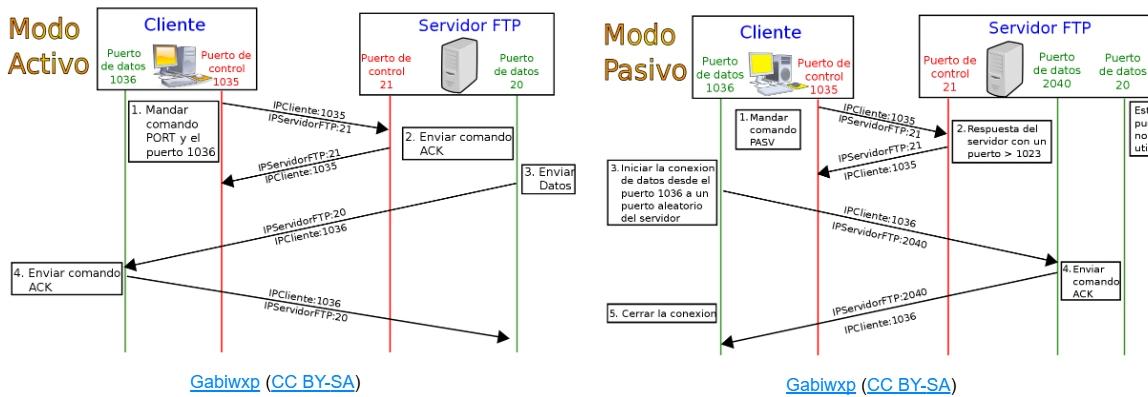
## 1.2.- TFTP/FTP.

### 1.2.- TFTP/FTP

Es un protocolo que fue creado para la transmisión remota de ficheros. En el que se crean 2 canales uno para transmitir datos y otro para ejecutar comandos remotos.

Existen 2 modos de funcionamiento del protocolo que es necesario conocer, para poder configurar las reglas del firewall asociado al servicio.:.

- **Activo:** el servidor siempre crea el canal de datos en el puerto 20 TCP y el cliente crea el canal de datos en un puerto aleatorio mayor que el TCP/1024. El cliente envía el número de puerto aleatorio al servidor para establecer la conexión, al ser un puerto cambiante. Por lo tanto, el servidor no conoce el puerto de funcionamiento del cliente y esto complica la definición de reglas de firewall.
- **Pasivo:** el servidor FTP abre un puerto de datos aleatorio TCP entre 1024-5000 lo comunica al cliente FTP de tal manera que sea el cliente quien conecte con ese puerto del servidor y así no sea necesario aceptar conexiones aleatorias inseguras para realizar la transferencia de datos.



El canal por donde se transmiten los datos de control es hacia el puerto TCP 21.

La diferencia entre [TFTP y FTP](#) es que FTP es un protocolo orientado a la conexión (TCP), mientras que TFTP es un protocolo no orientado a la conexión(UDP). Otra de las diferencias es que FTP requiere autenticación y TFTP no requiere autenticación.

Por lo que el servicio de TFTP debe ser protegido mediante reglas de firewall.

Ambos son protocolos que pueden ser utilizados para la transferencia de archivos. Esto puede ser aprovechado por los atacante para permitirles transferir ficheros al servidor, y en una segunda etapa el atacante hará un llamamiento a los ficheros transferidos al sistema para ejecutar las acciones maliciosas.

Aquí podemos ver un ejemplo práctico de la [explotación de un servicio TFTP](#).

Como medida de protección, es necesario habilitar el servicio FTP con contraseña, ya que existe la posibilidad de configurar el servicio sin la autenticación a través de usuario y contraseña, sino que están configurado de tal manera que se pueden transferir ficheros con un usuario anónimo. Esta es alguna de las características que se deberían configurar, ya que por defecto está permitido el uso de usuario anónimo..

Windows ya indica en su página oficial cómo [configurar el servicio de FTP a través de IIS](#).

En el siguiente enlace se puede ver una serie de [comandos FTP](#) que se utilizan una vez realizada la conexión.

A continuación, se indican algunos programas para configurar el servicio de FTP:

- <https://security.appspot.com/vsftpd.html>
- <http://www.proftpd.org/>
- <https://www.uftpserver.com/>
- <https://filezilla-project.org/>

Se debe implementar la versión segura del protocolo [SFTP o FTPS](#).



## Autoevaluación

¿Cuál es la versión segura del protocolo FTP?

- TFTP
- FTPS/SFTP
- FTTH

## **1.3.- RSSH / SSH.**

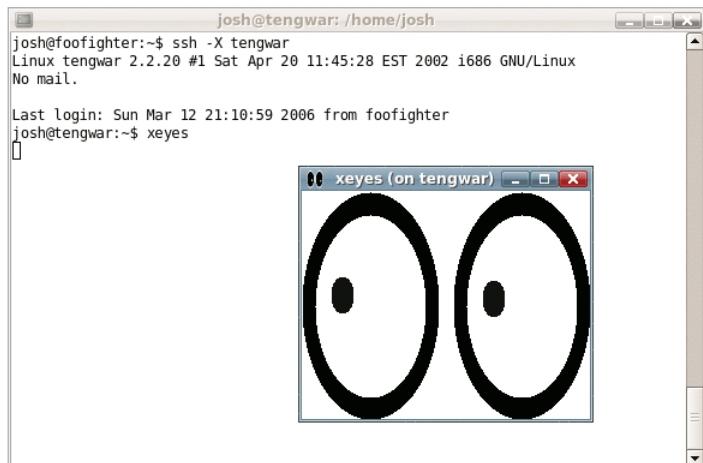
---

### **1.3.- RSSH / SSH**

RSSH es una versión reducida de SSH que sólo permite scp (security copy) y sftp (secure ftp).

El software permite realizar la transmisión de ficheros mediante una comunicación cifrada entre el cliente y el servidor remoto al que se conectan. Mediante esta conexión segura se establece la comunicación para la gestión de los equipos.

Estas son algunas de las medidas de protección para el servicio ssh:



[Tene~commonswiki \(CC BY-SA\)](#)

- El acceso a la máquina debe ser con los permisos mínimos de acceso y en una segunda etapa se debe realizar la elevación de privilegios para determinadas acciones privilegiadas. Pero el acceso inicial no debe de ser con privilegios de administración.
- Es recomendable incluir un mecanismo de autenticación robusto, por ejemplo acceso con certificados y/o integrar la autenticación con el servicio de autenticación del sistema.
- Limitar el número de intentos, para que no se puedan realizar el ataque de fuerza bruta.
- Los tiempos de sesión e inactividad se deben limitar para que el usuario no se deje abierta la sesión en una máquina y pueda sufrir el robo de sesión o la manipulación de la misma.
- Establecer los permisos de los archivos asociados al servicio, protegiendo los archivos que guardan las claves privadas y públicas de la autenticación basada en clave asimétrica.
- Se de utilizar una versión del software y protocolo sin vulnerabilidades del protocolo. Como es la versión 1.
- Se eliminará el acceso al entorno gráfico del equipo que alberga el servicio
- Eliminar de acceso del usuario superadmin root.
- Establecer las reglas de los usuarios que pueden acceder al servicio, y desde qué dispositivo lo pueden realizar.
- No se permite el acceso de usuarios sin contraseña.
- Los usuarios tendrán un mensaje indicado las características del contexto al entorno que acceden y las normas regulatorias que los cubre, este aspecto cubre la concienciación de las malas prácticas.
- Eliminar el comando rsh a través de archivos rhost. del servicio. La autenticación criptográfica basada en host de SSH es más segura que la autenticación .rhosts. Sin embargo, no se recomienda que los hosts confíen unilateralmente entre sí, incluso dentro de una organización. Por lo que se procederá a eliminar esta característica.
- Se garantizará que los usuarios no puedan usar variables de entorno al demonio SSH.
- Utilizar algoritmo de cifrado robustos.

De cara a configurar el acceso con claves criptográficas.

- Las claves públicas están establecidas en el directorio home de cada uno de los usuarios ~/.ssh/id\_rsa. Este fichero debe establecer los permisos de lectura y escritura para su propietario pero no para el resto de usuarios y grupos (600).
- El acceso por ssh con clave privada se realiza por ssh -i /ruta/clave/privada usuario@ip\_dominio.com

## Referencias

- <http://www.openssh.com/security.html>
- <https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/3674-ccn-stic-619-implementacion-de-seguridad-sobre-centos7/file.html>
- Security of Interactive and Automated Access Management Using Secure Shell (SSH) (nist.gov)



## Pregunta Verdadero-Falso

¿Es vulnerable ataque de fuerza bruta SSH?

- Verdadero
- Falso

## **2.- Hardening de procesos (eliminación de información de depuración en caso de errores, aleatorización de la memoria virtual para evitar exploits, etc.).**

---



## Caso práctico

Uno de las técnicas más utilizadas por los atacantes es a través de la infección de procesos. Por lo que el control y los mecanismos de protección de los procesos del sistema es un mecanismo de defensa eficiente contra el código malicioso. Aplicar estos mecanismos nos evitan tener menos incidentes.

Administrador de tareas de Windows				
Archivo Opciones Ver Ayuda				
Aplicaciones Procesos Servicios Rendimiento Funciones de red Usuarios				
Nombre de imagen	Nombre de usuario	CPU	Memoria ...	Descripción
nvvsvc.exe	[REDACTED]	00	1.396 KB	
nvxdsync.exe	[REDACTED]	00	1.864 KB	
openvpn-gui.exe	[REDACTED]	00	824 KB	OpenVPN GUI for Windows
stray64.exe	[REDACTED]	00	2.076 KB	IDT PC Audio
SynTPEnh.exe	[REDACTED]	00	2.000 KB	Synaptics TouchPad Enh...
SynTPHelper.exe	[REDACTED]	00	596 KB	Synaptics Pointing Device ...
taskhost.exe	[REDACTED]	00	2.740 KB	Proceso de host para tare...
taskmgr.exe	[REDACTED]	00	4.144 KB	Administrador de tareas d...
VBoxSVC.exe	[REDACTED]	00	3.240 KB	VirtualBox Interface
VirtualBox.exe	[REDACTED]	00	19.992 KB	VirtualBox Manager
VirtualBoxVM.exe	[REDACTED]	00	540 KB	VirtualBox Virtual Machine
VirtualBoxVM.exe	[REDACTED]	01	58.600 KB	VirtualBox Virtual Machine
VirtualBoxVM.exe	[REDACTED]	00	592 KB	VirtualBox Virtual Machine
WebexHost.exe *32	[REDACTED]	00	3.208 KB	Cisco Webex Meetings
winlogon.exe	[REDACTED]	00	1.316 KB	

Identifica los procesos de Windows y sus características

Procesos

Se establecerán principios de configuración segura básicos para cada uno de componentes software instalados en los equipos, tanto del sistema operativo base como de cada uno de los programas específicos para cada una de las tareas asignadas del sistema.

Dentro de los elementos comunes de configuración serán:

- Eliminación de usuarios por defecto
- Modificación de las contraseñas por defecto del Sistema.
- Activar el registro de eventos del sistema
- Se permite la gestión de usuarios a través de roles y grupos, que permitan asignar a cada usuario los privilegios mínimos indispensables para el desarrollo de sus tareas.
- Se establecerán mensajes informativos respecto a las responsabilidades del usuario a la utilización de los sistemas.
- Los equipos se bloquean después de un tiempo de inactividad.
- Únicamente estarán abiertos aquellos puertos que son necesarios para el desarrollo de la actividad. Bloqueándose a nivel de firewall local y de los firewalls de red del sistema.
- Se debe contar con herramientas de protección antimalware como antivirus. Y estos deberán estar actualizados.
- Todo el software debe estar actualizado a la última versión.

Para el control de la ejecución de software se pueden utilizar una herramienta que permite únicamente la ejecución de ciertos programas en los equipos. Para entornos [Microsoft existe la herramienta AppLocker](#). Además, se debería monitorizar la ejecución de nuevos programas en los equipos a través de herramientas como HIDS.

- Además, se deben aplicar medidas de seguridad relativas a:
- Protección en reposo mediante el cifrado de los datos
- Protección en tránsito mediante el cifrado de las comunicaciones
- Protección en uso que es la seguridad de los datos asociado a los procesos.

Microsoft ha implementado la característica Anti-Malware Scan Interface (AMSI) que permite detectar el script cuando se ejecuta en memoria, proporcionando a los AV una copia de lo que se está ejecutando.

Los procesos maliciosos, cada vez más elaborados, realizan acciones anormales en el sistema que impiden su detección. Por eso es necesario controlar los cambios de claves de registro, la jerarquía de los procesos que ejecutan, el tiempo de ejecución de los procesos, ... muchas de estas tareas son las que se realizan en las tareas de Threat hunting y que posteriormente son implementados como reglas de detección.

La información de registros logs es información sensible para el sistema por dos motivos, porque permite conocer información relativa al sistema y son las evidencias de los sucesos de un sistema ante un incidente de seguridad. Por lo que el acceso a dichos componentes debe estar regulado y protegido.

Existen herramientas en sistemas operativos como ProcMon de sysinternals que nos permite tener información de los procesos que se están ejecutando en nuestro sistema operativo. También puede ser utilizado otra herramienta de sysinternal para enviar información sobre los procesos como puede ser sysmon.

- [Sysinternals Procmon](#)
- [Sysinternals Sysmon](#).

A continuación, se detallan algunas de las medidas para proteger la memoria de los sistemas:

## **ASLR**

Técnica que evita la explotación de vulnerabilidades sobre la corrupción de memoria. Y que un atacante pueda saltar a una dirección de memoria que conozca que se está ejecutando una función, disponiendo de forma aleatoria las posiciones del espacio de direcciones de los datos de un proceso (ejecutable más los datos alojados en la pila).

## Aislamiento del núcleo

Características de seguridad disponibles en el dispositivo que usa la seguridad basada en virtualización.

### Integridad de memoria

Impide que los ataques inserten código malintencionado en procesos de alto nivel de seguridad.



Desactivado

Héctor Fernández Bardal (Dominio público)

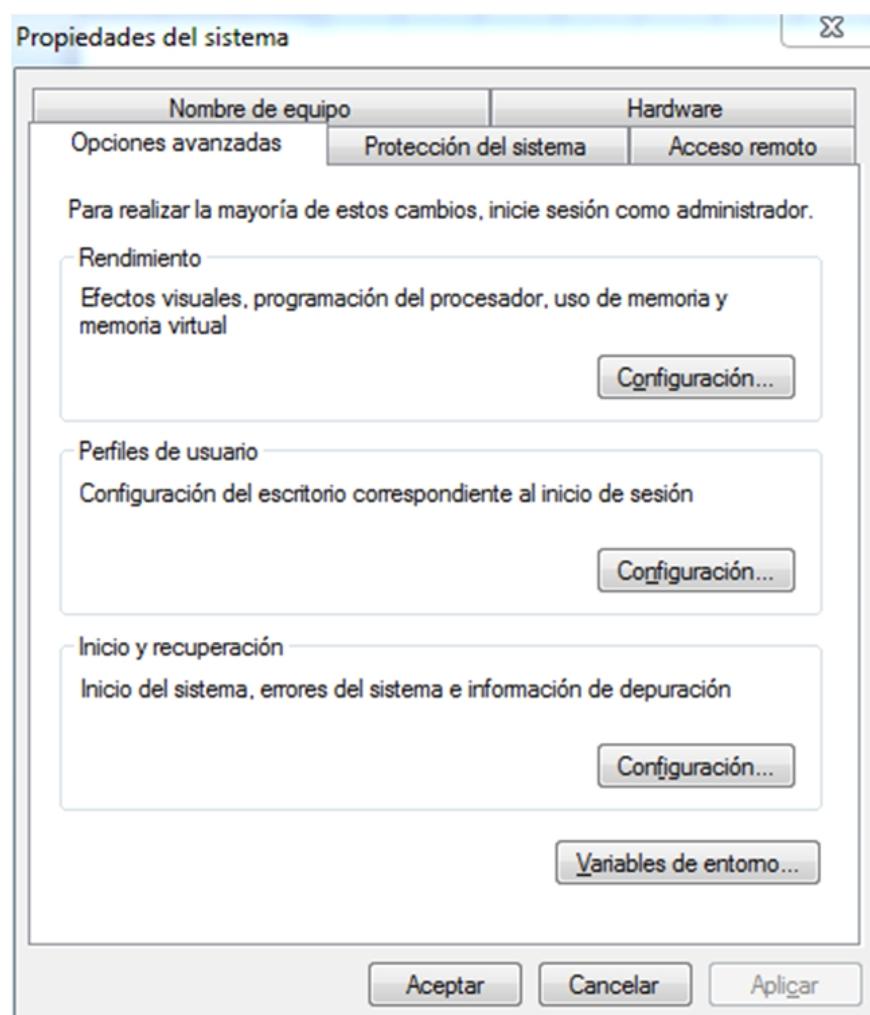
### DEP - "Función de prevención de ejecución de datos de Windows".

El código malicio realiza la ejecución de código fuera de las ubicaciones reservadas a la ejecución sistema operativo Windows y programas autorizados.

Mediante el mecanismo de protección DEP nos aseguramos que se utiliza la memoria de manera segura y en caso de utilización incorrecta el programa se cerrará y notificará.

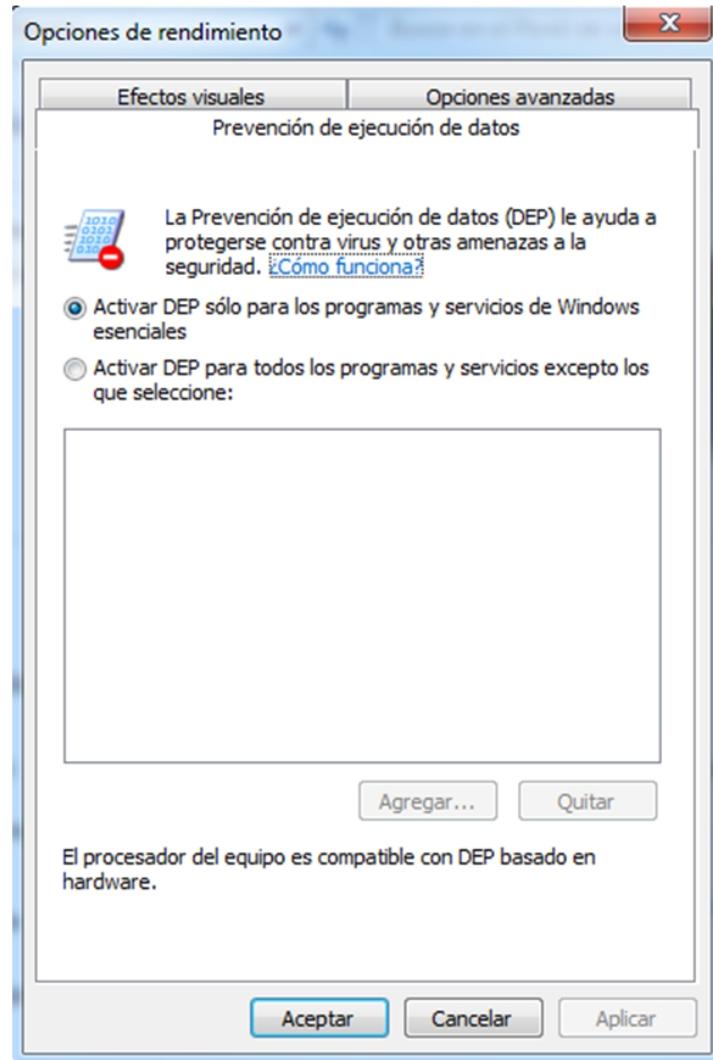
Por lo que utilizaremos siempre el software compatible con DEP.

1. Inicio --> Equipo --> Propiedades --> Configuración avanzada



Héctor Fernández Bardal (Dominio público)

2. Sistema --> Cambiar configuración avanzada del sistema --> Opciones avanzadas --> Configuración --> Prevención de ejecución de datos



Héctor Fernández Bardal (Dominio público)

Ambas protecciones están dirigidas por un lado a impedir la ejecución de instrucciones en ciertas regiones de memoria como el stack y por otro lado, proporcionar cierta aleatoriedad al espacio de direcciones del proceso (heap, stack, librerías, etc) para hacer más complejo el uso de direcciones hardcodeadas o de técnicas como ret-to-libc. Mediante el uso de direcciones predecibles (p.ej. librerías estáticas) y ROP el atacante, podrá en determinadas ocasiones eludir dichas restricciones de seguridad.

## Referencias

- <https://www.mandiant.com/resources/six-facts-about-address-space-layout-randomization-on-windows>
- <https://www.dell.com/support/kbdoc/es-es/000147101/what-is-data-execution-prevention-dep>
- [https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/deteccion\\_apt.pdf](https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/deteccion_apt.pdf)



## Autoevaluación

¿Qué herramienta de Windows permite controlar las aplicaciones que se pueden ejecutar?

- AppLocker
- CloseLocker
- Bitlocker

### **3.- Eliminación de protocolos de red innecesarios (ICMP, entre otros).**



#### **Caso práctico**

Uno de los trabajadores de la empresa de "Chocolates el niño" se ha descargado una herramienta de detección de puertos abiertos. Es un apasionado de la seguridad, y ha decidido informar a los administradores que hay puertos abiertos y detrás hay servicios corriendo configurados por defecto, por lo que acceder a ellos en muchos casos es muy fácil.



EOI (Dominio público)

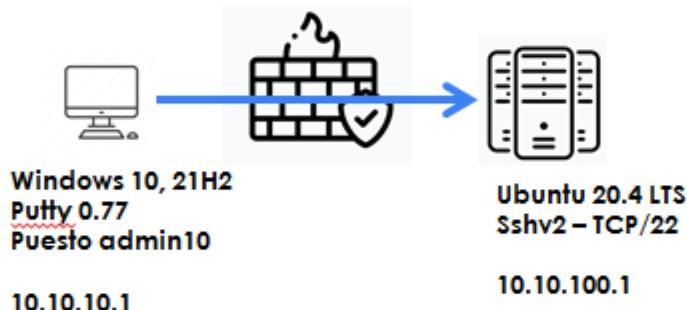
Debemos establecer medidas de protección de los servicios, eliminando en primer lugar el acceso a ellas desde el exterior. Para ello sólo tenemos que aplicar un mecanismo básico pero importante.

**Puertos cerrados**

### **3.- Eliminación de protocolos de red innecesarios (ICMP, entre otros)**

El control de las comunicaciones es una actividad que requiere de una gestión a lo largo del ciclo de vida de los sistemas implantados. Esto se empieza a concebir desde las fases de diseño, con el diagrama de arquitectura del sistema indicando los flujos de información entre los diferentes componentes del sistema y los protocolos utilizados.

La realización del diagrama facilitará a los gestores de redes y sistemas el control de las comunicaciones y los puertos que deben estar abiertos en la red para permitir únicamente aquellas comunicaciones establecidas y por los equipos.



Héctor Fernández Bardal (Dominio público)

La gestión de estas comunicaciones deberá estar actualizada ante cambios de la arquitectura o de los componentes del sistema.

La gestión estará complementada por mecanismos de monitorización de los elementos que protegen las comunicaciones como son los firewalls, para que en caso de producirse una comunicación no controlada o el intento de la realización de dichas comunicaciones permita determinar el motivo de porqué se han realizado. Una vez analizada la información relativa a la conexión se reportará un incidente o un falso positivo por el mal funcionamiento de equipo del sistema que ha originado la alerta.

Los protocolos innecesarios deben ser eliminados a nivel de red y a nivel de sistema operativo configurando los firewalls de red y firewall de los sistemas operativos.

Un ejemplo es el protocolo [IPv6](#), que no están siendo implementados en España al ritmo que creímos y está activo en muchas redes y sistemas por defecto. Este protocolo está siendo utilizado por los atacantes porque el nivel de conocimiento del protocolo es bajo y porque por defecto muchos servicios se levantan en dicho protocolo sin que los administradores lo haya desactivado a pesar de no estar siendo utilizado.

Este es el resultado de que estamos utilizando masivamente el protocolo NAT para poder extender la utilización IPv4 en lugar de IPv6. Poniendo como salvaguarda de los servicios y punto clave de seguridad nuestro servicio de NAT. El cual está siendo un punto de configuración crítica de los sistemas. Pero ante determinados servicios, sobretodo los asociados a las comunicaciones seguras donde el protocolo debe ser interrumpido (rotura del protocolo) a través de dispositivos NAT específicos. Pero el NAT no debería ser una medida de protección, ya que el NAT no constituye más que un mecanismo de ocultación de la infraestructura, y que los atacantes saben que está siendo utilizada, por lo que utilizan otras técnicas para poder acceder al descubrimiento de la arquitectura.



## Autoevaluación

Bajo qué circunstancias habilitaríamos el ICMP desde el punto de vista de la ciberseguridad.

- Desde IPs controladas y sólo para cierto tipos de ICMP
- Para los usuarios internos
- Los usuarios del departamento del sistema

## 4.- Securización de los sistemas de administración remota.



### Caso práctico

Los administradores del sistema han estado trabajado desde casa y tuvieron que acceder a la administración desde IPs externas a la organización. Relajando las reglas de acceso desde IPs internas. Esto ha puesto en peligro la parte más crítica de los sistemas, ya que si una de las cuentas de estos usuarios se viera comprometida, el sistema ser vería afectado con más impacto.

Habría que pensar cómo les damos a los administradores acceso a la administración, ya que sus ordenadores personales pueden suponer un riesgo, porque además no controlamos la comunicaciones que viajan por la red de Internet.



[Ssl2Buy](#) (Dominio público)

Administración segura.

Todos los sistemas de administración remotos debe ser actualizados para no disponer de vulnerabilidades conocidas.

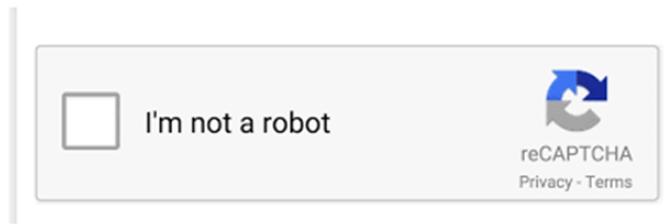
Además, dichos servicios deben estar protegidos como elementos críticos del sistema, ya que permiten tomar el control de los sistemas y poder extraer información, elevar privilegios, ...

Las comunicaciones deben realizarse a través de protocolos de cifrado seguro que impidan que se pueda visualizar la información que se transmite en la comunicación.

La autenticación deberá estar basada en usuario y contraseña, y un segundo factor de autenticación que refuerce el acceso.

Además, debe de contar con mecanismo de protección:

- Bloqueo de usuario frente ataques de fuerza bruta.
- No mostrar información relevante que indique la existencia de los usuarios.
- Control del origen desde la que se hace la conexión remota.
- Análisis del equipo origen aplicaciones cliente que permitan analizar el estado del equipo en origen: que el equipo esté actualizado, que disponga de un antivirus, que tenga el firewall habilitado, ...
- Deberá haber procedimientos operativos de recuperación de contraseñas y realizar la baja de los usuarios.
- Utilización de mecanismos CAPTCHA para evitar la utilización de herramientas automáticas.



Héctor Fernández Bardal. CAPCHA (Dominio público)



Héctor Fernández Bardal (Dominio público)

Los accesos deben haber sido aprobados por el responsable del sistema.

Es necesario además definir el nivel de acceso de cada uno de los usuarios que acceda al sistema y el tiempo necesario de acceso al sistema. Además, se deberá realizar una recertificación de los accesos periódicamente con el fin de mantener el control de los usuarios que tienen acceso a la plataforma.

Se deberá contar con un mecanismo de monitorización, que permita auditar los registros (logs) de la aplicación control remoto y detectar los intentos no deseados de acceso al sistema.

Los accesos remotos a los sistemas deben estar controlados, y debe haber los mínimos indispensables. Priorizando el acceso al sistema a través de un punto central que permita realizar el salto a los diferentes sistemas, y no tener múltiples sistemas de control remoto y hacia múltiples equipos que dificulta la administración y el control de los accesos.

El acceso remoto deberá estar alineado con los procesos de alta, modificación y baja de permisos de los usuarios en el sistema, bien a través de un sistema de [gestión de identidades\(PIM\)](#) y un sistema de accesos privilegiados (PAM). Todos estos procesos deben estar alineados con los procesos operativos de seguridad, también llamados POS.

El nivel de acceso remoto para los usuarios privilegiados debería estar reforzado, ya que el acceso de estos usuarios al sistema tiene un mayor impacto en la organización. Por lo que se deberían aumentar y reforzar los requisitos de seguridad.

También se debería de tener en cuenta si la aplicación de acceso remoto tendría que estar expuesta al dominio público de Internet. Esta situación tendría aparejada la inclusión del refuerzo de medidas de seguridad. Se debe establecer desde qué localizaciones o desde qué dispositivos deberemos hacer esos accesos remotos. Siempre basados en una defensa en profundidad, en el que el acceso a determinados servicios se haga desde dispositivos controlados y que cumplan unos requisitos mínimos de seguridad.



## Autoevaluación

¿Qué sistemas nos ayudarán a gestionar el control de accesos de usuarios privilegiados?

- PIM/PAM
- Kerberos
- LDAP

## 5.- Sistemas de prevención y protección frente a virus e intrusiones (antivirus, HIDS, etc.).



### Caso práctico

Después de varias malas prácticas por parte de los usuarios la empresa "CJ" como son : descarga de archivos de fuentes no confiables, acceder a todos los enlaces que reciben en sus correos electrónicos, apuntarse a todos los sorteos para recibir premios, registrarse con su correo corporativo para acceder a las zonas privadas,... La empresa decidido buscar una solución que le permita gestionar sus equipos y protegiéndolos, sabiendo lo que sucede al momento. La solución consiste en un pequeño software se instala en los equipos y monitoriza los parámetros que considera que se ajustan a las necesidades de la empresa.



EOI (Dominio público)

Este agente tiene que ser capaz de:

1. Buscar vulnerabilidades
2. Detectar actividades sospechosas: acceso sospechoso, ataques de fuerza bruta, escalado de privilegios...
3. Recopilar y analizar toda la información que se recibe.
4. Detectar anomalías de comportamiento

¿Qué es?

# Sistemas de prevención y protección frente a virus e intrusiones (antivirus, HIDS, etc.)

Existen varios sistemas que previene de la protección contra software maliciosos y virus. Los sistemas que se implementen deben ser complementarios entre ellos y además de proporcionar protección deben proporcionar información sobre el equipo ante un incidente. También se considera eficiente que el sistema disponga de un mecanismo de reacción automática (defensa activa) en caso de que el sistema esté en peligro.

Las herramientas pueden ser de 2 tipos:

- Activas: en las que se realizan contramedidas de protección para que el código malicioso no consiga su objetivo. Estas herramientas deben ser actualizadas ya que los métodos de ataque también evolucionan en el tiempo.
- Pasivas. Sólo avisan de que se está produciendo una situación anómala en el sistema, pero no realizan una reacción.

Active response: este es el concepto que tienen los HIDs de cómo reaccionar ante determinados eventos sospechosos. Hay que particularizar las reglas al entorno en las que se han implementado.



[OSSEC](#). OSSEC (Dominio público)

Algunos ejemplos de programas de active response de libre distribución es [OSSEC](#) o la versión más reciente [Wazuh](#).

Los mecanismos de protección deben contar un sistema de actualizaciones ante nuevas vulnerabilidades, y de poder ser parametrizables para el entorno en el que son configurados, pudiendo añadir excepciones que deberán ser documentadas y analizadas previa a su aplicación.

Se debe contar en la red con diferentes mecanismos de detección de código malicioso ya que existen técnicas de evasión de antivirus. Ya que el hecho de disponer de diferentes antivirus en la red puede complicar al atacante la técnica de evasión al tener que evadir varios antivirus. Esto es posible verlo en la práctica a través de plataformas de sistemas de detección on-line de antivirus, donde se puede visualizar que es detectable para algunos motores antivirus y sin embargo para otros no, como es el servicio de [VirusTotal](#).

Intentemos muchas veces ponernos en la mente de los atacantes y buscar una contramedida que impida llevar a cabo ciertas actividades. Así por ejemplo podríamos hacer un ejercicio de simulación de un ataque accediendo a nuestro sistema sistema y utilizando las herramientas de protección como un endpoint (EDR) o antivirus, para saber si es posible detectar el ataque a través de nuestro sistema de protección. En el ejercicio la simulación se deben aplicar las técnicas de [evasión de los sistemas de protección](#) y de recopilación del [información de seguridad del sistema](#). Con el objetivo de saber si nuestro sistema permite tener una eficiencia ante ataques de ciertas familias de malware.

Los sistemas de detección de intrusos (IDS) a través del análisis de trazas de red que son enviadas al dispositivo, alertan en base a reglas. Acompañado a la alerta tiene que haber implementado un procedimiento de gestión de la alerta, ya que el sistema sólo genera alarmas, pero no mecanismos de protección que sí lo hace el [IPS](#), que en base a las alertas para los ataques.

Existe muchas formas de determinar reglas para un IDS, las reglas de Snort están basadas en firmas, que están clasificadas por [categorías](#).

La monitorización del tráfico de red para ser enviado a los IDS, se hace a través de métodos de port-mirroring o con un dispositivo que se denomina tap (antiguos hub) que reenvían todos los paquete a todos los puertos por métodos de broadcast.

Las reglas de los IDS pueden estar basadas en:

- Comportamiento. Necesitamos conocer el funcionamiento normal del sistema para detectar las anomalías.
- Firmas: Detectan el tráfico malicioso en base a reglas.

La aplicación de parches de seguridad debe estar alineado el control de activos y software del sistema, ya que debemos estar informados de los parches de seguridad y vulnerabilidades que van publicando los fabricantes en base a nuestro catálogo de activos y software continuamente actualizado.

Las actualizaciones se deben forzar en los equipos y no deben quedar como una tarea dependiente del usuarios, por lo que deben estar basados días programados. Una tarea complementaria a la actualización es el reinicio de equipos, ya que muchos equipos no cogen las actualizaciones hasta que el equipo es reiniciado.

Las actualizaciones también deben estar orientadas a las herramientas de detección de artefactos de seguridad como pueden ser:

- Antivirus
- HIDS, NIDS... (dominios, hash, ips,...)

Para dispositivos móviles también es necesario la utilización de un MDM que permita la actualización de estos dispositivos y el control de las herramientas que se pueden ejecutar en la parte de los equipos. Siempre orientado a una red BYOD,

Aquello que pierda soporte y no tenga actualización es el momento de utilizar otro equipo y comenzar a utilizar las nuevas versiones del productos.

#### Básicos en las actualizaciones

- Descarga de sitios oficiales
- Comprobación de la integridad de la descarga
- Pruebas en entornos de preproducción. Si se puede.
- Mejor hacerlo que esperar a tener la seguridad al 100%

#### Referencias:

- <https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/keeping-devices-and-software-up-to-date>
- <https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/actualizacionsoftware.pdf>
- <https://www.incibe.es/protege-tu-empresa/blog/si-tu-pyme-protegida-quiere-estar-siempre-tienes-actualizar>
- <https://www.osi.es/es/actualizaciones-de-seguridad>
- <https://docs.microsoft.com/en-us/mem/configmgr/sum/understand/software-updates-introduction>
- <https://docs.microsoft.com/en-us/windows/deployment/update/how-windows-update-works>



## Pregunta Verdadero-Falso

El HIDS y el antivirus son incompatibles

Verdadero     Falso

## 6.- Configuración de actualizaciones y parches automáticos.



### Caso práctico

Eternal Blue (MS17-010) fue una vulnerabilidad con mucho impacto en las organizaciones. La vulnerabilidad afecta al servicio de compartir archivos para los sistemas operativos Windows, proporcionando al atacante control remoto total sobre la máquina.

Microsoft rápidamente proporcionó una solución (parche) para subsanar este error, pero muchas organizaciones siguen teniendo esta actualización sin aplicar y estamos en 2023. Desconocemos el motivo, aun sabiendo que ha sido el elemento principal de éxito del ransomware WannaCry. Muchas organizaciones aplicaron el parche después de sufrir el ataque a pesar de que estaba disponible.



[Blas Palinckx](#) (Dominio público)

Esta vulnerabilidad tiene muchos exploits que cualquier usuario con conocimientos medios de ciberseguridad podría utilizar para entrar en sistemas que no estén actualizados o parcheados. Vamos hacer una aproximación a la cantidad de software e información que hay en la red sobre esta vulnerabilidad y que muchos no han parcheado o no parchearon en su día a tiempo.

No ransomware.

# Configuración de actualizaciones y parches automáticos.

Las actualizaciones y parches de seguridad constituyen uno de los pilares fundamentales de los sistemas, ya que es una de las recomendaciones de seguridad que está en todas las listas de acciones recomendadas para mantener el nivel de seguridad de los sistemas.

El software tiene un ciclo de desarrollo en el que se implementan nuevas funcionalidades y también se corrigen errores detectados en sus versiones actuales. Además, este ciclo de actualizaciones se realiza conforme a los fallos de seguridad publicados que puedan tener un impacto en el funcionamiento del software o del sistema que los aloja. Teniendo en cuenta que el software está instalado en sistemas con complejas relaciones entre ellos, un fallo de seguridad en uno de los componentes software puede dañar el sistema entero. Recordamos el paradigma la seguridad: **La seguridad de un sistema es la seguridad de su punto más débil.**

Esto es debido a que el software está en constante cambio por su utilización, investigación de los analistas de software, investigación de los analistas de seguridad y expertos que se dedican a tareas como [bug bounty](#) permiten detectar fallos de seguridad de los sistemas. Ante estos fallos de seguridad que debilitarían de manera global el sistema, los desarrolladores trabajan para solventar este error permitiendo así que el sistema se mantenga en un nivel de seguridad aceptable.

Es por ello por lo que una vez que el producto ha sido actualizado, es necesario que se produzca la actualización por parte de los administradores del sistema.

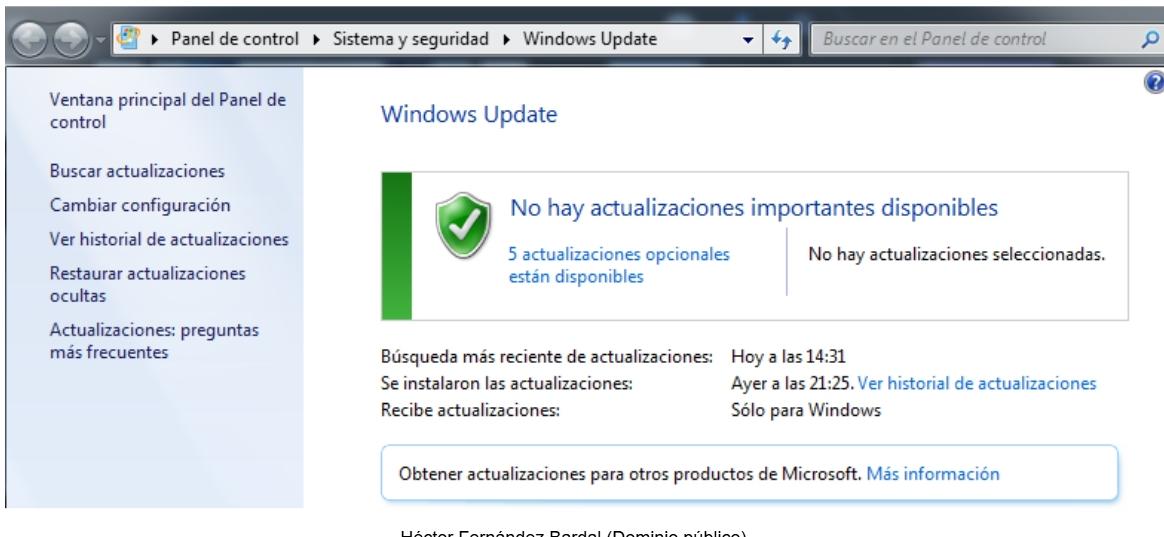
Algunas compañías como Microsoft aglutan las actualizaciones de software una vez al mes (primer martes de cada mes), para no estar sacando parches continuamente y los agrupan en actualizaciones de seguridad, salvo aquellas que consideran especialmente crítica que la denominan parches de [seguridad de vulnerabilidades de día cero](#).

Debido a que en los equipos corre varios programas de software, es necesario disponer de mecanismos de protección frente ataques porque los desarrolladores del software necesitan un tiempo para solucionar el fallo, y porque muchos fallos no se han descubierto y están en desconocimiento tanto de los atacantes como de los desarrolladores.

En este punto vamos a que diferenciar el software libre del software de licencia, ya que el método de la búsqueda de la solución a diferentes fallos de seguridad puede ser tratado de diferente manera.

Mientras que el software licenciado está apoyado por un equipo de soporte que realizará la búsqueda y desarrollo de una solución, y la solución será enviada a los sistemas que dispongan de la licencia,. El software libre depende más de la agilidad de la comunidad para buscar una solución, es cierto que entre más amplia sea la comunidad más probabilidad hay de que dicho software sea actualizado y mantenido rápidamente.

Para el desarrollo de software libre, o módulos de código que se han desarrollado bajo software libre y han sido utilizados en software licenciado, se está viendo incrementado el impacto de seguridad de estos módulos cuando son ampliamente utilizados, como recientemente el [fallo de seguridad de log4j](#).



Normalmente las arquitecturas de para el servicio de actualización pueden ser dos:

- Arquitectura distribuida del sistema, donde cada uno de los equipos realiza la actualización del software descargándose independientemente los parches y posteriormente son instalados en los equipos. Esto es recomendable para organizaciones pequeñas, o entornos domésticos, donde no existe una infraestructura mediana/grande, y en la que no existe un equipo de TIC especializado para la gestión de la infraestructura
- Arquitectura centralizada de actualización, donde existe un servidor interno de actualizaciones, donde inicialmente se descargan todas las actualizaciones, para posteriormente ser distribuidas al resto de los equipos del sistema. No teniendo cada uno de los equipos una conexión directa con el proveedor. Esta arquitectura centralizada está más aplicada a entornos empresariales, y con administradores del sistema que permiten gestionar los servicios de actualizaciones, liberando aquellas actualizaciones que, aun teniendo un impacto positivo para la organización desde el punto de vista de la seguridad, tienen un impacto negativo para la operatividad del sistema. Además, en este sistema, se reduce el volumen de datos desde el proveedor del software, y se pueden priorizar el nivel de actualización del sistema y que menos impacto tenga para la organización la realización de la actualización. Sobretodo en lo relativo a los parches que se han de instalar en servidores críticos de la organización como por ejemplo: AD, servidor de archivos, servidores de bases de datos, ...que requieren de una parada más controlada del sistema.

Existen varias herramientas para la realización de búsqueda de vulnerabilidades que complementa las tareas de actualización. Esta software realiza la búsqueda de vulnerabilidades que no ha podido ser parcheadas y permite tener un control y estado de actualización del sistema, dos de las herramientas más conocidas son:

- [Nessus](#)
- [OpenVas](#) (incluida en Kali Linux)

En la ejecución de los escaneos se deben realizar con credenciales, ya que muchas de las vulnerabilidades no son descubiertas si no se realiza el análisis con los permisos adecuados. La realización de escaneos automáticos tienen las siguientes características:

- Son fáciles de programar y repetir. Es fácil saber el nivel de parcheo. Además las herramientas suelen tener características de informes.
- Se puede cruzar con el inventario de activos.
- Producen “mucho ruido” en la red y consumo de recursos.
- Las herramientas tienen que cubrir el mayor conjunto de elementos. Las licencias de los productos completos son caras.
- Existen soluciones open-source pero que no tienen una inteligencia tan amplia.



## Autoevaluación

¿Cómo se debe aplicar el escaneo de vulnerabilidades y proporcione el mayor número de información?

- Con credenciales
- Siempre desde la misma IP
- Sólo buscando las de nivel medio y bajo

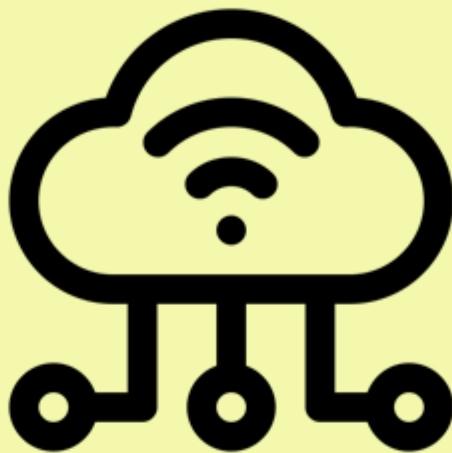
## 7.- Sistemas de copias de seguridad.



### Caso práctico

Con el crecimiento de los ataques por ransomware para muchas empresas las copias de seguridad han sido la salvaguardia de poder restaurar sus sistemas y no perder el trabajo de años, pérdidas económicas o en muchos casos tener que cerrar la compañía. Muchas de las empresas aún teniendo un programa de copias de seguridad no pudieron afrontar un ataque por ransomware porque los sistemas de copia también se vieron afectados.

En las políticas de copias de seguridad, ¿cuál es uno de los requisitos de la política que ayudan a proteger la información?



EOI. Cloud backup (Dominio público)

La solución está ahí afuera

## 7.- Sistemas de copias de seguridad

Los sistemas de copia de seguridad permiten recuperar el sistema ante un incidente grave de seguridad que ha dejado el sistema inoperativo y ha producido la pérdida de datos. Entre ellos, este año están todos los incidentes relacionados con ransomware. Una de las medidas de protección contra este tipo de ataques es tener una [gestión eficiente de las copias de seguridad](#).

Así mismo el sistema de copias de seguridad y las copias de seguridad deberán estar protegidas, ya que son un punto crítico para resolver estos incidentes. Por lo que los atacantes están incluyendo en su fase de ataque la destrucción del sistema de copia y las copias de seguridad realizadas para que no puedan ser restauradas. Especialmente en los ataques de ransomware.

En este capítulo trataremos el concepto de tener una copia de respaldo fuera del sistema, bien en servicios contratado por un proveedor en la nube, o bien a través del almacenamiento de las copias en sistemas externos protegidos a través de elementos de seguridad física como cajas fuertes, armarios o salas con control de acceso.

Por otro lado, el sistema en sí de copias de seguridad debe ser tratado como un **sistema crítico**, y el acceso y control de la información se debe realizar si es posible a través de una red de propósito específico que permita realizar las copias de una manera eficiente, y tener el sistema una defensa más en profundidad de cara a que sólo los usuarios con tareas relacionadas con la realización de copias puedan tener acceso al sistema.

Si las copias de seguridad han sido realizadas conforme a las necesidades del sistema, el impacto de pérdida de información tiene un bajo impacto, en otro caso el impacto aumentará conforme el tiempo que no se tenga información de respaldo. Si que es cierto que existe un cierto periodo de pérdida del servicio debido a que será necesaria la recuperación del sistema dañado e inoperativo.

También hay que tener en consideración las copias de seguridad de las configuraciones del sistema para que este tiempo de vuelta a la normalidad sea más eficiente y realista. Ya que muchas veces no disponer de las complejas configuraciones que tienen algunos sistemas, impiden que, aun teniendo la copia de la información, esta no puede ser puesta en producción porque no va alineada con la configuración necesaria. Normalmente la copia de configuración viene acompañada del manual de recuperación en caso de desastre y en la simulación de restauración de copias de seguridad periódicamente, para comprobar que la copia que se realiza de la información y de la configuración sea suficiente.



[Datos 101](#) (Dominio público)

Se deben establecer prioridades en la realización de las copias de seguridad atendiendo a la criticidad del sistema y de la información almacenada en él, así como dimensionar la infraestructura acorde el volumen de información que es necesario almacenar en el sistema y el tiempo de retención de la información del sistema.

Como resumen pasamos a indicar una estrategia de copias de seguridad basado en la regla 3.2.1:

- Deberías al menos almacenar 3 copias actualizadas de tus datos
- Las copias deben ser almacenadas en 2 medios diferentes
- Una de las copias deberá ser almacenada de manera off-line.

Complementario al plan de copias de seguridad, deberá existir un plan de recuperación ante desastres



## Pregunta Verdadero-Falso

Una vez realizadas las copias de seguridad no es necesario comprobarlas.

Verdadero  Falso

## 8.- Shadow IT y políticas de seguridad en entornos SaaS.



### Caso práctico

El grupo APT está analizando a su próxima víctima, saben que muchos de los usuarios del sistema utilizan software portable de edición de fotografía. Saben que lo utilizan porque no necesita instalación y tiene mejores funcionalidades que el que le proporciona la compañía.

Los atacantes han inyectado malware en este software portable y lo han subido a una web, indicando que es gratuito y no necesita instalación. Muchos de los usuarios ya se lo han descargado.



EOI (Dominio público)

Los usuarios a veces buscan alternativas a las proporcionadas por las empresas pero no evalúan el riesgo de los "productos gratuitos" que los atacantes utilizan como método de ingenierías social.

No con portables

## Shadow IT y políticas de seguridad en entornos SaaS

Las políticas de seguridad en entornos cloud (SaaS, PaaS, ...) deben estar respaldados por una matriz de responsabilidades (matriz RACI) entre el proveedor y el cliente que delimita las tareas asociadas al proveedor y al cliente, pero que se estén realizando conforme a las políticas de seguridad del sistema.

En el caso de un servicio SaaS las copias de seguridad son responsabilidad proveedor, el cliente deberá ser informado de la realización de copias de seguridad y las evidencias que indican que se han realizado.



[Shadow IT](#) (Dominio público)

Además las copias de seguridad deben cumplir con las mismas medidas de que las que se realizan de manera interna:

- Tiempo de retención
- Cifrado de las copias
- Procedimiento en caso de recuperación
- Realización de simulacros de recuperación
- Fiabilidad de las copias a través de test de las copias realizadas.
- Las copias están etiquetadas y son fácilmente identificables.

Los sistemas que sean proporcionados en las organizaciones a través de proveedores externos deben cumplir con las mismas medidas de seguridad que estén implementadas en la organización. Para no dejar sin cubrir ninguna de las tareas, lo que llevaremos a cabo es delimitar todas las responsabilidades del servicios relativos a la seguridad, para que ningún ámbito se quede sin cubrir y por lo tanto no sea una dejación de funciones dicha tarea. Una vez que se ha definido las funciones también se deberá implementar dentro del los procedimientos operativos de seguridad, aquellos procesos que formen parte de la seguridad como la comunicación de un incidente, la brecha de seguridad de los datos, la caída del servicio, la actualización de los componentes, medidas regulatorias adicionales que hay que implementar, la gestión de excepciones, la formación de los técnicos que administran la plataforma desde el punto de vista de la seguridad,...

## 8.1.- Shadow IT.

---

### Shadow IT

Las aplicaciones y sistemas olvidados y que no tienen un mantenimiento constituyen un elemento vulnerable para la organización desde el punto de vista de la seguridad. Dentro de este contexto encontramos dispositivos, software, servicios en la nube, servicios on-premise.

La iniciativas de muchos departamentos por sacar sus proyectos con la utilización de las TIC y dejar de lado la aplicación de la seguridad constituye un riesgo para todo el sistema. De ahí que el control de activos constituye un elemento fundamental para tener una gestión de todos los elementos del sistema.

Los administradores se puede apoyar en la utilización de múltiples herramientas para la detección de:

- Elementos de red a través de [NAC](#)
- Control de software instalados con agentes de control de inventario, HIDS,...
- Servicios centralizados de control de la configuración como: [SCCM](#) de Microsoft, [Ansible](#) o [Jenkins](#) para entornos Linux,... Muchas de estas herramientas puede ser utilizadas también con propósito de seguridad en el mundo de las operaciones [DevSecOps](#).



# Jenkins

[The Jenkins project \(CC BY-SA\)](#)

Desde la organización se debe contar con políticas que incluyan a los equipos de seguridad desde el diseño de los programas que utilizan la tecnología, que actualmente son casi todos los proyectos empresariales, ya que se ha demostrado el beneficio de uso

de la TIC.

También existen malas prácticas por parte de los usuarios de utilizar software personal o que más conocen en lugar de utilizar el que les proporciona la compañía, a parte de concienciar al usuario sobre estas malas prácticas. Se debe aplicar medidas técnicas que impidan la descarga e instalación de software que no está aprobado y configurado por la compañía:

- No permitir la descarga de ficheros ejecutables, no permitiendo la navegación a páginas web de software.
- Controlar la entrada de ficheros ejecutable a través del correo electrónico o de los mecanismos de intercambio de información que la empresa proporcione.
- Desinstalar los ficheros ejecutables no controlados.
- La búsqueda de ficheros ejecutables y maliciosos.
- Actualización de patrones de búsqueda en base a IOCs: hash, nombres de ficheros,...

Esto además debe estar alineado con las políticas de concienciación, ya que muchos usuarios utilizan plataformas de descarga gratuita de software, que además de incurrir en un delito de propiedad intelectual. Muchos estudios revelan que este software tiene malware asociado.

El ciclo de vida del software debe también finalizar con una etapa de desinstalación, borrado y actualización de los mecanismos de seguridad que estaban asociados al software:

- Eliminación de protocolos, puertos, reglas,...en los dispositivos de la red.
- Desinstalación de software
- Eliminación de usuarios
- Baja de los procedimientos de copia y recuperación de desastres.
- Destrucción de los dispositivos que albergaban la información
- Desconexión de los elementos con los que se integraba y operaba.



## Autoevaluación

¿Qué es un software portable?. Sus riesgos en la seguridad.

- Un software que se autocopia sólo
- Software que sólo se puede instalar en portátiles
- Un software que no necesita instalación sólo son necesarios permisos de ejecución.

# Condiciones y términos de uso de los materiales

Materiales desarrollados inicialmente por el Ministerio de Educación, Cultura y Deporte y actualizados por el profesorado de la Junta de Andalucía bajo licencia Creative Commons BY-NC-SA.



MINISTERIO  
DE EDUCACIÓN  
Y FORMACIÓN PROFESIONAL



Antes de cualquier uso leer detenidamente el siguiente [Aviso legal](#)

## Historial de actualizaciones

Versión: 01.00.00

Fecha de actualización: 04/07/23

Versión inicial de los materiales.