

Configuración de dispositivos para la instalación de sistemas informáticos.

Caso práctico

El CISO de la compañía ACME S.L. quiere que se investigue si los sistemas donde se guarda información sensible y crítica son seguros. Por lo que ha pedido que se revisen las medidas de seguridad relativas a estos sistemas poniendo el foco en aspectos tales como:

- ✓ Configuración segura de la BIOS/UEFI.
- ✓ Riesgos asociados a los puertos de conexión y los puertos en los que se pueden conectar dispositivos para el intercambio de información u otros periféricos.
- ✓ Seguridad de los sistemas de ficheros: SUID de los ficheros, permisos de directorios, compartición de directorios,...



[Mouaqip](#) (Dominio público)

Objetivos:

En este módulo estudiaremos la importancia de preparar los equipos con los elementos que provee el fabricante. Configurando de manera segura la BIOS/UEFI, y todos los riesgos asociados a los puertos de conexión y los puertos en los que se pueden conectar dispositivos para el intercambio de información u otros periféricos.

Mostraremos los aspectos de seguridad en el proceso de arranque del sistema, configurando el arranque seguro del mismo y aquellos medios que permiten vigilar el arranque y los cambios de configuración del mismo.

Finalizaremos el módulo con la configuración segura de los sistemas de ficheros, particiones y la manera de establecer el cifrado en reposo para la información, sobretodo si el dispositivo está destinado a albergar información sensible.

1.- Precauciones previas a la instalación de un sistema informático: aislamiento, configuración del control de acceso a la BIOS, bloqueo del orden de arranque de los dispositivos, otros.



Caso práctico

En la oficina de Mario algunos trabajadores se tienen que quedar más tiempo en la oficina para acabar el proyecto en el que están inmersos. La pasada semana aparecieron en Internet documentos confidenciales que estaban en su ordenador personal. Nadie sabe qué ha podido pasar ya que la política de la empresa tiene contraseñas robustas de acceso al dominio y los USB están deshabilitados para que no pueda haber fugas de información ni infecciones por malware por la utilización de USBs personales que los trabajadores pueden conectar a los ordenadores.

The screenshot shows the PhoenixBIOS Setup Utility interface. The menu bar at the top includes Main, Advanced, Security, Boot, and Exit. The Main tab is selected. The main window displays various system configuration options:

PhoenixBIOS Setup Utility	
Main	Advanced
System Time:	[19:17:19]
System Date:	[10/28/2014]
Legacy Diskette A:	[1.44/1.25 MB 3½"]
Legacy Diskette B:	[Disabled]
▶ Primary Master	[None]
▶ Primary Slave	[None]
▶ Secondary Master	[CD-ROM]
▶ Secondary Slave	[None]
▶ Keyboard Features	
System Memory:	640 KB
Extended Memory:	2096128 KB
Boot-time Diagnostic Screen:	[Enabled]

On the right side of the screen, there is a vertical column labeled "Item Specific Help" which contains the instruction: "<Tab>, <Shift-Tab>, or <Enter> selects field."

At the bottom of the screen, a keyboard legend provides key mappings for navigation and function keys:

F1	Help	↑↓	Select Item	-/+	Change Values	F9	Setup Defaults
Esc	Exit	↔	Select Menu	Enter	Select ▶ Sub-Menu	F10	Save and Exit

[Neoguias. Configuración BIOS \(Dominio público\)](#)

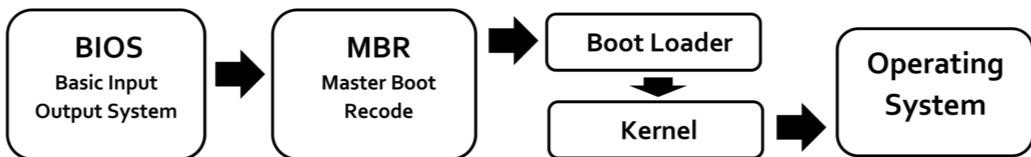
La empresa decide contratar a un consultor para que analice el ordenador de Mario y ver si tiene algún virus, pero no han encontrado software malicioso. Por lo que deciden analizar cada uno de los parámetros de configuración del PC y se dan cuenta que el acceso a la BIOS no dispone de contraseña. ¿Pudo ser el vector de entrada?

Protege la BIOS

La protección de los dispositivos que van a formar parte de los sistemas también constituye un elemento de protección de cara al bastionado de los sistemas. La normativa relativa a los requisitos de seguridad de los sistemas (CCN-STIC, ENS, NIST) indica que es necesario llevar a cabo una configuración segura de la BIOS bajo los siguientes criterios:

- Mínima funcionalidad
- Acceso por contraseña
- Se activará el arranque seguro
- Actualización del firmare
- Comprobación de la integridad de firmware
- Revisión del proceso de arranque
- Revisión de los dispositivos conectados (puertos)

Legacy Boot



[Amila Ruwan \(CC BY-SA\)](#)

Analizando los elementos propios de los sistemas, habrá que tener en cuenta la configuración segura de los siguientes elementos de los equipos:

- Control de configuración de BIOS y UEFI
- Orden de arranque.
- Puertos de conexión: Bluetooth, wifi, NFC, ...
- Dispositivos de almacenamiento: USB, CD-ROM, tarjetas,...

Esta configuración está asociada al fabricante de los equipos. La mayoría de las recomendaciones y posibilidades de configuración desde el punto de vista de la seguridad vienen determinadas por sus manuales de usuario. Cada vez más fabricantes crean apartados específicos de configuración relativas a la seguridad.

Ya se han detectado ataques a las infraestructuras ligados a la cadena de suministro de equipos que venía infectados desde el fabricante. Este es el motivo por el que los riesgos en la cadena de suministros se han elevado, ya que es necesario aumentar esa confianza entre el cliente y el proveedor de los dispositivos que van a formar parte de las redes.

En algunos casos como el de redes clasificadas oficiales, los productos que forma parte de la red tienen que estar dentro del catálogo de productos acreditados que pasan una serie de controles y auditorías.

El CCN tiene publicado su catálogo de productos a través de su guía [CCN-STIC 105](#).

Lo que se busca es tener productos en origen seguros desde el diseño y asegurar todo el ciclo de vida de los productos desde su inicio. En el siguiente enlace se puede ver una guía de referencia de certificación de productos basado en la [metodología de certificación española de productos LINCE](#).

Otra referencia que hace mención a la utilización de productos seguros en las redes es el [Esquema Nacional de Seguridad](#) en su versión de Mayo de 2022.

1.1.- Control de configuración BIOS/UEFI.

Control de configuración BIOS/UEFI

La UEFI o BIOS(Basic Input/Output System) es el primer software que se ejecuta al arrancar el equipo, por lo que ya ha sido objetivo de atacantes, ya que la infección de este software aumenta el nivel de la persistencia en el sistema y la dificultad de detección. Por lo que es uno de los softwares críticos que debemos tener en cuenta en el plan de actualizaciones.

La BIOS suele estar desarrollada por el fabricante del equipo (original equipment manufacturer - OEM). Por lo que son ellos los que deben proporcionar el software original y sus actualizaciones.

El software UEFI (Unified Extensible Firmware Interface) surgió posteriormente, añadiendo nueva funcionalidades a BIOS como proporcionar acceso remoto, lo que abre un nuevo vector de ataque en el arranque del sistema. UEFI se define como una versión más moderna y segura, pero si la configuración se deja por defecto no será tan segura.

Suele estar guardado en memorias específicas: CMOS, EEPROM, ROM, Flash... por lo que su configuración permanece almacenada mientras exista una fuente de alimentación conectada, por ejemplo a través de un pila. Por lo que puede ser borrado quitando la pila o activado algún mecanismo que deje el sistema sin alimentación. Esto permite eliminar las modificaciones realizadas en la configuración de la BIOS, si se diera el caso que tuviéramos que resetear la configuración a valores de fábrica por algún error en la configuración u olvido de contraseña.

Este tipo de software también puede estar presente en tarjeta gráficas, controladores de tarjetas de red,....

La actualización de la BIOS vendrá marcada por el método que establezca el fabricante. Algunas de las actualizaciones de este firmware se realizará desde sistema ópticos, USB,..

La BIOS/UEFI realiza el proceso de inicio y carga de software:

- Comprobación del Hardware del equipo
- Iniciación del Hardware
- Inicio del sistema operativo.

Debido al impacto que tiene la BIOS en el arranque de los sistemas, se debe establecer el control de la configuración de la BIOS /UEFI a través de contraseña, para tener controlado el acceso a los cambios de configuración. Además, se debe establecer un procedimiento operativo que permita el cambio de configuración de cualquier elemento de la BIOS. Al no existir un control de usuarios, la contraseña debe ser custodiada y actualizada según los procedimientos de seguridad de la organización.

Para más información acerca de los [ataques más comunes a las EUFI](#).

Además, es necesario considerar que las empresas proveedoras de software de UEFI tenga un plan de actualización y mitigación de vulnerabilidades y una metodología de desarrollo basado en la seguridad desde el desarrollo (security by-design).

Los organismos internacionales han publicado guías de configuración segura de este software:

- [Guía NIST de protección de BIOS](#)
- [Guía NIST de protección de BIOS de servidores](#).

Entre los procedimientos de autenticación segura del EUFI y BIOS está el mecanismo de actualización protegido por contraseña, no permitiendo la realización de actualización remota o sólo desde dispositivos controlados. En caso de permitirlo, sería necesario monitorizar y controlar con los dispositivos de seguridad (firewalls) las conexiones que permiten la actualización de estos dispositivos, y sólo desde las redes internas.

El no disponer de control de acceso a la BIOS/UEFI permitirá a un usuario no deseado cambiar:

1. Secuencia de arranque
2. Habilitar puertos y dispositivos de comunicación: bluetooth, wifi, nfc
3. Solicitud de contraseña con cada arranque del sistema

Recordar que es posible resetear la configuración por defecto de BIOS dejando sin energía a la memoria que almacena la configuración (CMOS) a través de una batería o pila que está dentro de placa. Este mecanismo requiere de acceso físico al equipo, por lo que se deberían establecer si se considera medidas de protección física de los dispositivos, con pegatinas anti tamper para comprobar que los dispositivos no han sido manipulados. En caso de detectar la manipulación, es necesario activar el procedimiento de cambio de contraseña de la BIOS.



[Amazon](#) (Dominio público)

Hay dos métodos que pueden mitigar la infección de la BIOS, instalar la BIOS sin permisos de escritura y verificar su integridad en cada proceso de arranque.

La descarga del software de actualización de la BIOS sólo se debe realizar desde las páginas oficiales del fabricante. Es necesario controlar la integridad del software descargado y mantenerlo actualizado. Existen proyectos de software sobre la UEFI que incluyen la [seguridad](#) como uno de los aspectos a tener en cuenta. Es una manera de tener el control del código de la BIOS pero que necesita de mantenimiento, actualización y configuración con personal propio o con apoyo de la comunidad. Los dos proyectos más destacados son:

- <https://libreboot.org/>
- <https://www.coreboot.org/>

Referencias:

https://csrc.nist.gov/csrc/media/publications/sp/800-147b/final/documents/draft-sp800-147b_july2012.pdf

<https://support.lenovo.com/sg/es/solutions/ht502745>

<https://download.lenovo.com/bsco/index.html>



Autoevaluación

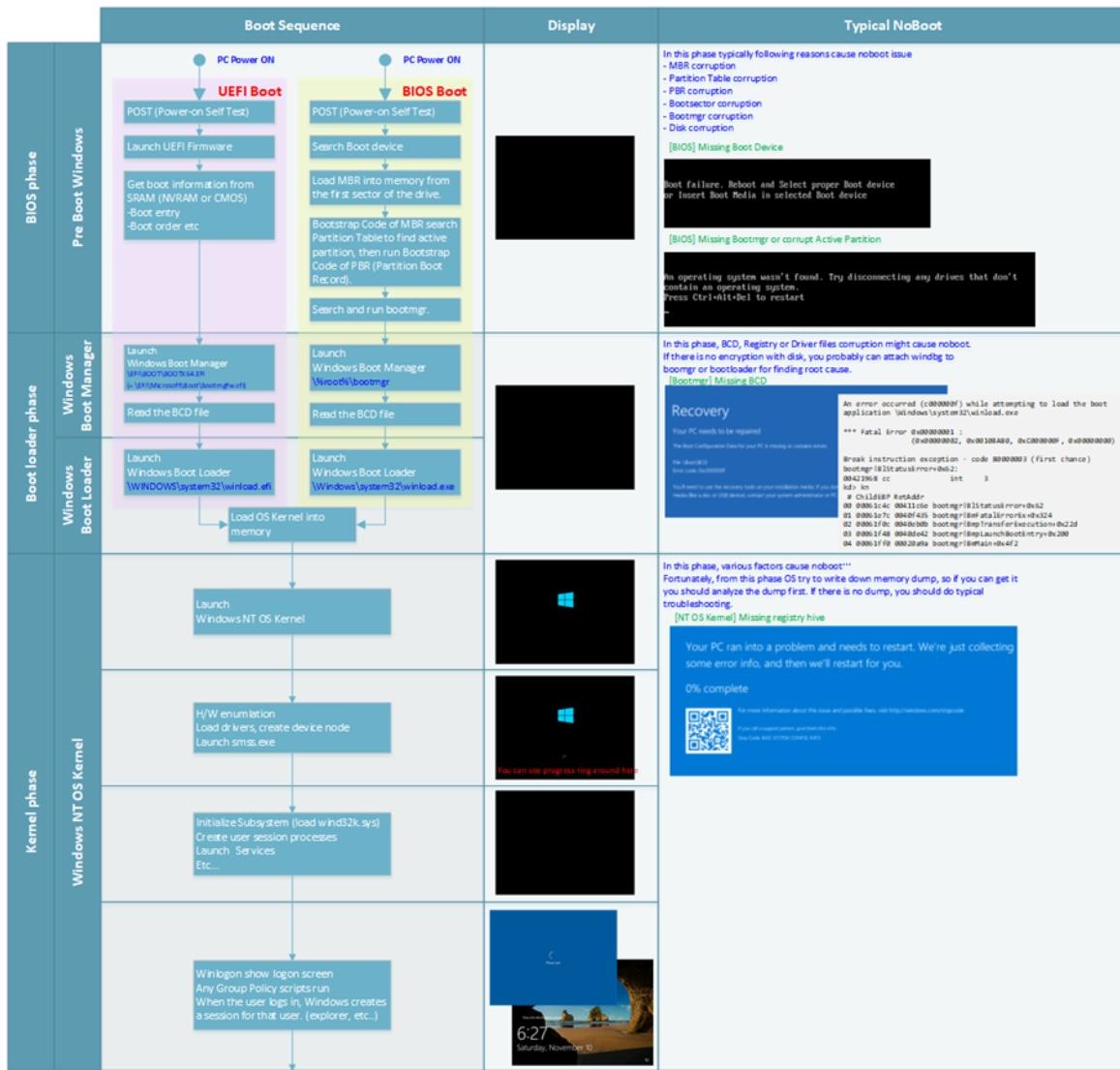
¿Es necesario actualizar el software de la BIOS?

- Verdadero
- Falso

1.2.- Secuencia de arranque.

Secuencia de arranque

La modificación de la secuencia de arranque permitirá iniciar el equipo con otro sistema operativo, que podrá tener acceso a los ficheros del sistema. Los métodos más comunes del cambio de secuencia de arranque es cambiando la configuración en la BIOS y utilizar un dispositivo externo con un arranque desde un sistema operativo que no tenga medidas de seguridad ni sea controlado por los administradores del sistema.



1.3. Puertos de conexión: Ethernet, Wifi, Bluetooth,....

Minimizar los riesgos de conexiones incontroladas en los equipos, pasa por evitar las conexiones a redes wifi que no estén controladas por la organización (públicas, acceso libre, dispositivos bluetooth, o conexiones a redes cableadas de otros sistemas).

Únicamente serán permitidas conexiones hacia puntos Wifi o de Ethernet de confianza, estableciendo una conexión VPN contra la organización, cuando esta se produzca desde fuera de las instalaciones (teletrabajo, viajes,...).

La organización permitirá únicamente estas 2 vías de conexión:

- Dispositivos controlados
- Conexiones a redes públicas protegidas por mecanismos de protección de la información a través de túneles VPN como extensión de su red.

Los dispositivos controlados son aquellos dispositivos que han sido configurados acorde a las políticas y normas de seguridad de la organización. Esto abarca todo tipo de conexiones: wifi, ethernet y bluetooth... y en caso de que los usuarios puedan establecer configuraciones hacia cualquier punto de acceso lo utilicen como vía de comunicación protegida por un túnel (VPN, HTTPS,...). De tal manera que no puedan realizar conexiones sin restricciones para por ejemplo poder navegar libremente, ... Estas medidas de seguridad deben ser implementadas de cara a tener un control de las conexiones, o minimizadas con la vigilancia y la respuesta rápida ante incidentes de seguridad.

Security

I/O Port Access

Ethernet LAN	[Enabled]
Wireless LAN	[Enabled]
Wireless WAN	[Enabled]
Bluetooth	[Enabled]
USB Port	[Enabled]
Memory Card Slot	[Enabled]
Smart Card Slot	[Enabled]
RFID	[Enabled]
Integrated Camera	[Enabled]
Integrated Audio	[Enabled]
Microphone	[Enabled]
Fingerprint Reader	[Enabled]
Thunderbolt(TM) 4	[Enabled]
NFC Device	[Enabled]

Héctor Fernández (Dominio público)

Algunos fabricantes disponen de [simuladores de BIOS](#) en sus páginas web, como por ejemplo el fabricante de Lenovo. Lo que permite a los usuarios familiarizarse con las BIOS.



Autoevaluación

Tener el Bluetooth activado en los equipos para que los usuarios conecten sus dispositivos inalámbricos de audio no supone un riesgo.

Verdadero Falso

1.4.- Puertos de conexión: USB.

La conexión de dispositivos externos al equipo como norma general deben ser deshabilitados, ya que constituyen un elemento incontrolado de entrada y salida de información y por lo tanto de riesgos de infección y exfiltración de la información.

Algunas estaciones deben tener habilitada estos dispositivos por motivos de funcionalidad como la conexión de dispositivos periféricos. En este caso la instalación de los drivers del dispositivo tiene que estar controlado a través de restricción de permisos de administrador. Serán los administradores los que realizarán la instalación de los drivers y el control de las listas de dispositivos permitidos.

No permitiéndose la conexión de dispositivos de manera incontrolada. Dichos dispositivos de intercambio (USB) deberán estar registrados como activos del sistema con un identificador único.

Entre los dispositivos que pueden constituir una amenaza para los sistemas, existen dispositivos específicos que permitirían una puerta de entrada al sistema, o de recopilación crítica.

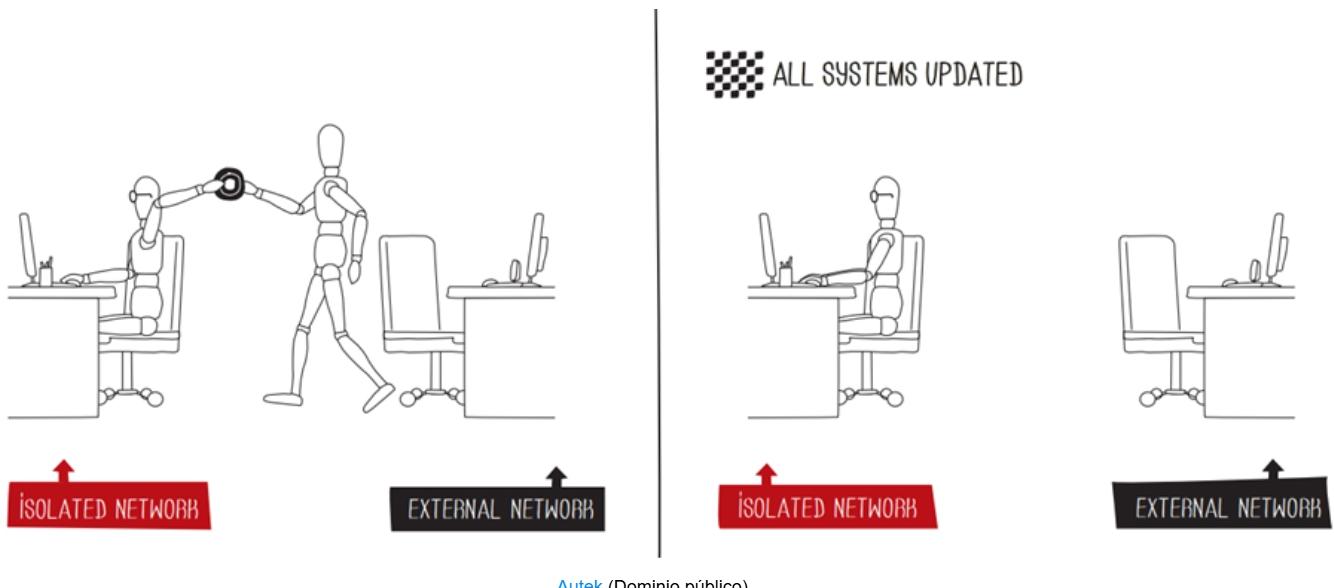
- [Rubber Ducky](#)
- [LAN Turtle](#)
- Yard Stick One
- Key Logger
- [USB Killer](#)

Existe herramientas que permite la [gestión y control de los dispositivos conectados](#) a los equipos mediante listas blancas, así como el ataques físicos a los equipos a los que se conecta el dispositivo.

Todos estos riesgos relativos a la utilización de dispositivos USB son elementos a considerar desde el punto de vista de la seguridad. Y se debe establecer en que equipos específicos se pueden utilizar. Una opción es utilizarlos sólo en equipo aislados de la red que cumplen las funciones de equipo de análisis de dispositivos USB, eliminando los riesgos a tener los USB activos en todos los equipos de la organización aumentando la probabilidad de:

- Infección
- Fuga de información
- Accesos remotos no controlados,...

Los equipos aislados que tenga como finalizada el intercambio de información a través de USB con los equipos de la red, utilizan el procedimiento de intercambio de información a través del medio que comúnmente se denomina air-gap. Aunque existen otros medios de información de intercambio de información entre dominios con diferentes grados de seguridad en el tratamiento de la información, como pueden ser pasarelas o diodos. Estos mecanismos son los se denominan dispositivos de protección de perímetro (DPP).



[Autek](#) (Dominio público)

Estos procedimientos de seguridad minimizan los riesgos, pero no los eliminan al 100%, como sucedió con el famoso [incidente de Stuxnet](#).

En estos dispositivos es necesario establecer procedimientos operativos de seguridad para la utilización de los dispositivos externos como USB en ciertas tareas como: actualizaciones del sistema operativo, actualizaciones de software de seguridad como las firmas del antivirus, ...



Autoevaluación

¿Qué es el air-gap?

- Mecanismo para templetizar los equipos
- Un nuevo malware
- Mecanismo para intercambiar información entre dos equipos aislados a través de un dispositivo externo: USB key, disco duro portátil, CD, ...

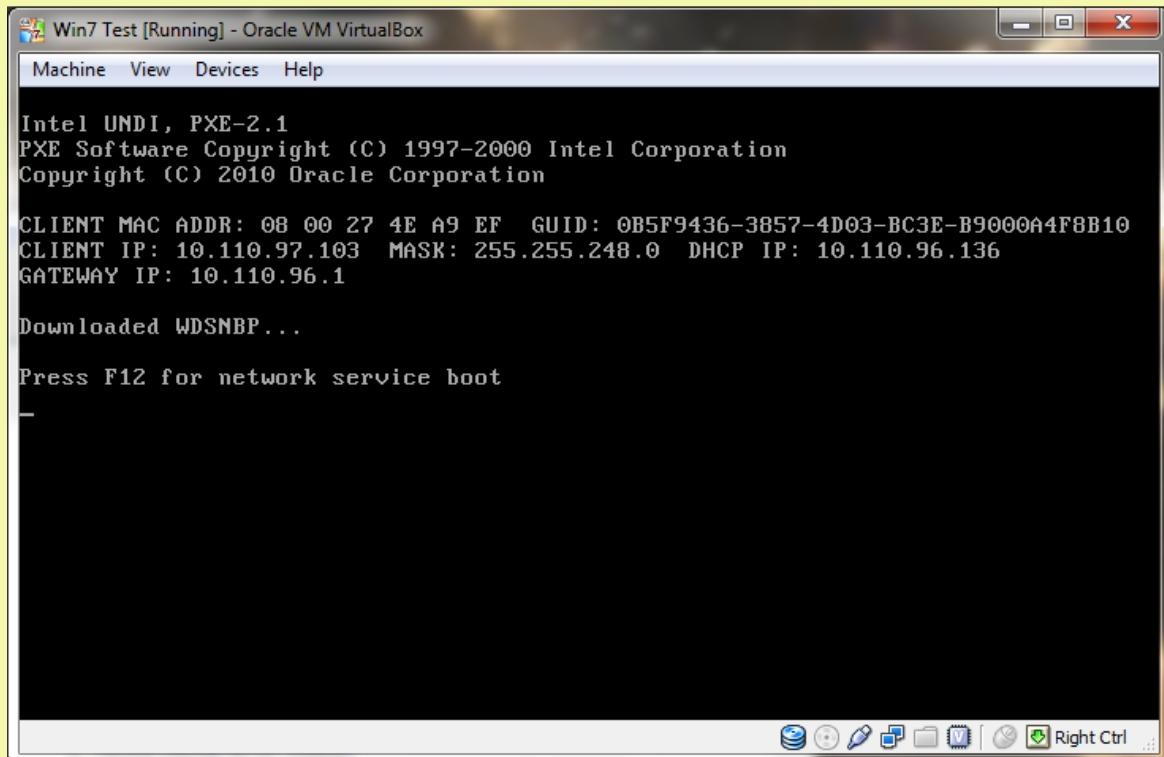
2.- Seguridad en el arranque del sistema informático, configuración del arranque seguro.



Caso práctico

Los administradores del sistema de la Universidad de Castilla-La Mancha utilizan PXE para facilitar la instalación de las imágenes de Windows a través de la red. Esto lleva asociado un servidor (WDS) que procesa las solicitudes y envía la imagen al equipo para instalarla.

Existen procesos asociados a la instalación de la imagen por PXE como son: DHCP, TFTP. Cuando los ficheros son transferidos al equipo comienza la instalación.

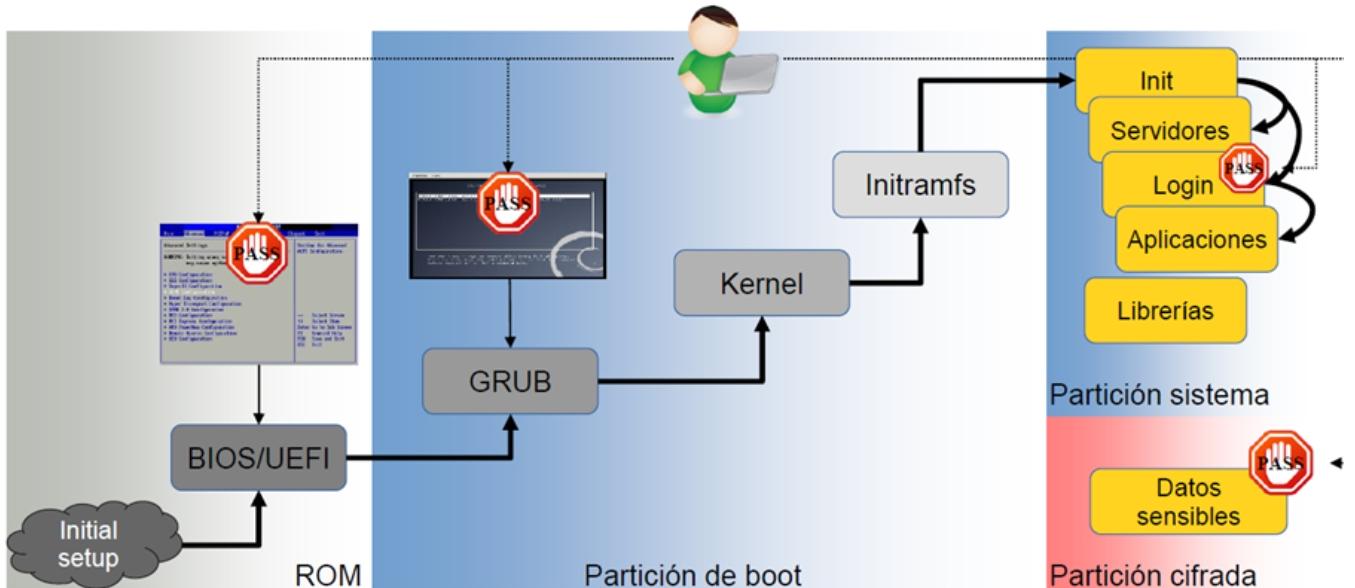


[James Preston \(Dominio público\)](#)

Lo importante es conocer los detalles de funcionamiento de PXE para saber cómo se puede explotar y qué valores necesitamos configurar para que este proceso no suponga un riesgo.

PXE seguro

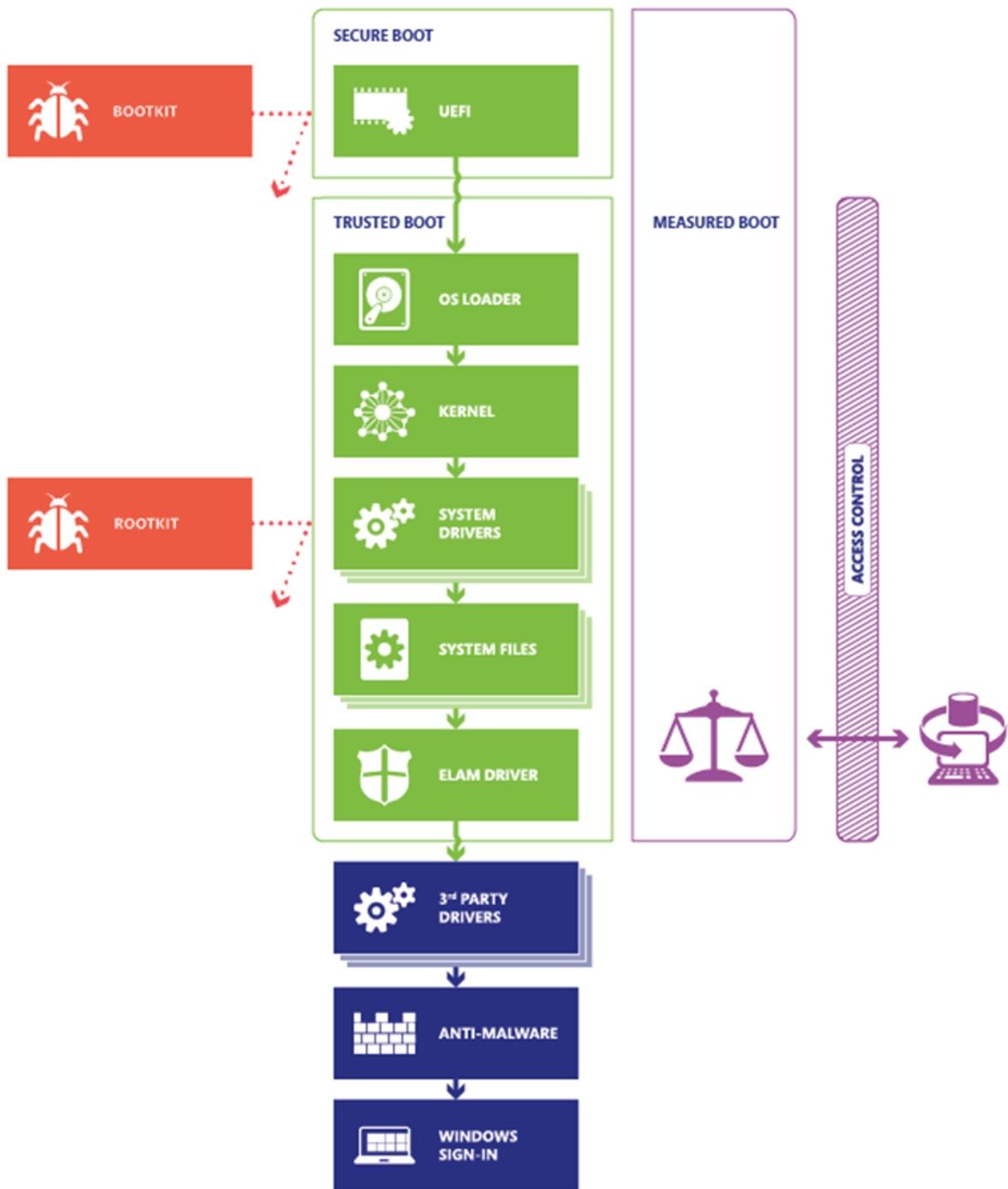
Para realizar un control sobre el arranque seguro del sistema operativo debemos conocer cómo se realiza un inicio normal de nuestro sistema operativo, para poder detectar cualquier anomalía que se produzca durante el arranque.



[Hector Marco / Ismael Ripoll](#) (Dominio público)

Debemos además tener en cuenta las amenazas de malware de rootkit que se instalan en el arranque del sistema que son difíciles de detectar y que provocan que muchas de las herramientas de seguridad no funcionen ante este tipo de amenazas.

Una de las labores de seguridad relativas al inicio del sistema, es realizar un análisis de la jerarquía de procesos que se ejecutan en Windows con el objetivo de poder determinar y analizar los posibles ataques en el inicio de un sistema operativo. En este caso de Windows este análisis nos ayudará a determinar si los atacantes se encuentran en la fase de persistencia en su Kill-Chain.



[Micosoft](#) (Dominio público)

Estas son las medidas de seguridad que debemos establecer en el arranque:

- Comprobación de la integridad del sistema.
- Envío de logs de arranque al SOC para su análisis.

Existen herramientas que permiten controlar el arranque de los equipos. Para los sistemas operativos de Linux se pueden utilizar las siguientes herramientas:

- [AppArmor](#)
- [SELinux](#)

Para un análisis seguro de un equipo se puede utilizar un arranque con un dispositivo externo (liveCD o liveDVD) que permita la ejecución de un sistema operativo certificado y configurado de manera segura. De tal manera que podemos partir de un modo seguro para analizar el equipo. Aunque esta medida tiene que estar controlada solo para casos de análisis de equipos o equipos que tengan una funcionalidad específica y queremos que el equipo permanezca inmutable.

También es importante proteger el [arranque por PXe](#). En el siguiente enlace se puede ver una forma de atacar un equipo [redirigiendo el arranque PXe](#) hacia un servidor malicioso. Este procedimiento de instalación y arranque de sistemas suele tener contraseñas guardadas en ficheros de scripts que están en claro. Es necesario proteger estas contraseñas en claro.

En el siguiente enlace se muestran algunos [modos de arranque seguro](#) para diagnosticar el sistema.

Los gestores de arranque también presentan vulnerabilidades, por lo que es necesario realizar la actualización de este software. Los gestores de arranque deben tener configurado la contraseña para el acceder a la configuración y poder cambiarla. Como es el caso del gestor de [arranque del grub](#).

3.- Seguridad de los sistemas de ficheros, cifrado, particionado, entre otros.



Caso práctico

Los comerciales de la empresa de Ricardo, viajan por toda Europa y muchas veces tienen que llevar el portátil a todos lados. El riesgo de robo del portátil es alto porque un pequeño descuido, dejarlo en el hotel encima de la cama, olvidarlo en una cafetería,...puede suponer que desaparezca. Pero a veces es inevitable.



Héctor Fernández. *Gusanos en ficheros* (Dominio público)

El portátil es algo material que supone un coste para la empresa, pero tiene más valor la información. Así que tenemos que ponerle una capa de protección a esa información y aunque el portátil se vea expuesto a sustracción. Hay que intentar que se lleven una caja fuerte, pero sin la llave.

Protege la información

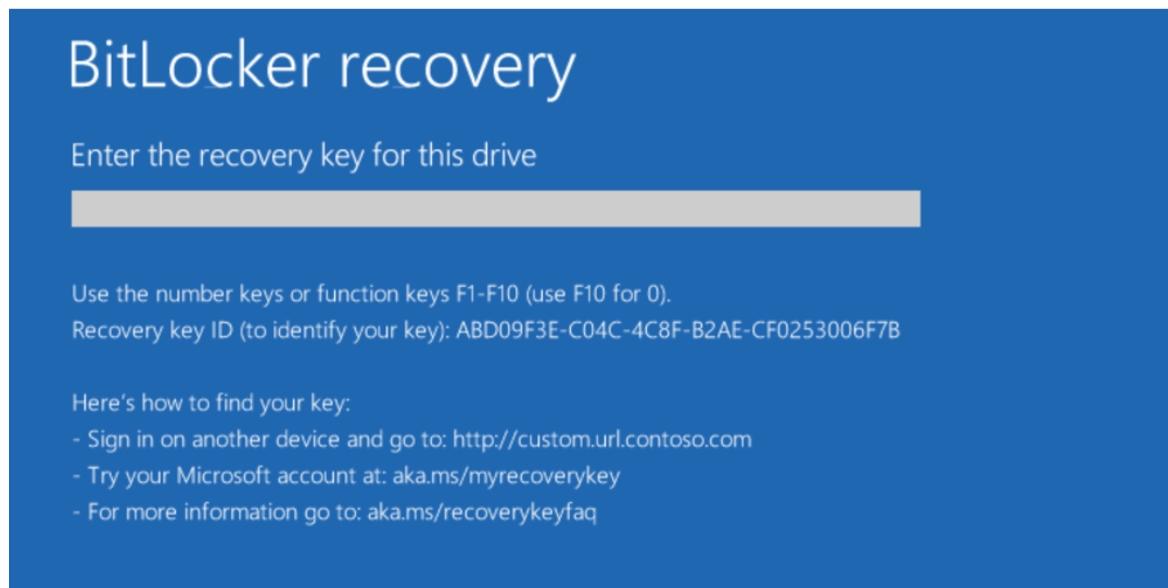
Seguridad de los sistemas de ficheros, cifrado, particionado, entre otros.

Los sistemas son importantes por la información que almacenan. Ya que el sistema en sí sólo soporta los mecanismos necesarios para el tratamiento de la información. Por lo que debemos proteger o proporcionar al sistema de los mecanismos de protección del dato.

Entre los mecanismos de protección está el cifrado de la información, que es la medida de seguridad que en caso de robo de la información permite proteger la información y que esta no sea utilizada por personas que no deberían tener acceso a ella y que puedan perjudicar a la organización o ser utilizadas con otros fines para las que fueron creadas.

Esta información debería ser cifrada en todos los niveles del sistema, tanto a nivel de sistema de ficheros, como de los dispositivos extraíbles: USB, memorystick, CD, DVD, También deben aplicarse estos mecanismos de protección para la información almacenada en la nube.

Uno de los mecanismos más utilizados por Windows es el cifrado de información a través de [BitLocker](#). Para los sistemas Linux existe el cifrado a través de la herramienta [gpg](#), teniendo los modos de clave simétrica y asimétrica.



También dentro del ciclo de vida de la información está el borrado seguro de la misma, de tal manera que no pueda ser recuperada por métodos forenses y que permita recuperar la información. Estas son algunas de las referencias a herramientas de borrado seguro:

- [Herramientas de borrado seguro de INCIBE](#).
- [Herramienta de Borrado Seguro de CCN](#).

Los mecanismos de borrado seguro de la información deberá esta aplicado a todos los dispositivos: ordenadores, portátiles, servidores, discos duros, USB, móviles,..

Los usuarios deben estar concienciados de no almacenar la información en sus dispositivos locales, sino que se deben almacenar en servidores de ficheros, bases de datos, ...que tengan un bastionado de la información y del sistema. Ya que dichos servicios se pueden proteger con otro nivel adicional de seguridad y se centrarían los esfuerzos en generar una protección adicional sobre el servicio. Además de que estos servicios estarán protegidos por el plan de recuperación ante desastres o por incidentes de seguridad como el Ransomware como son las copias de seguridad.

Existe una tendencia a la utilización de sistemas virtualizados con el despliegue de las máquinas virtuales (VDI/VGI) en el momento que el usuario solicita el despliegue de su máquina mediante sistemas de virtualización. Y una vez que el usuario deja de utilizar el sistema la información se borrará del equipo, esto permite proteger la información ante el robo de dispositivos. Además, las tecnologías de comunicaciones actuales con anchos de banda altos nos permiten obtener esa información de una manera rápida sin necesidad de disponer de un equipo potente.

El particionado del sistema de archivos se realizará según la funcionalidad el sistema. Esto permitirá asignar permisos a cada una de las particiones para proporcionar el mínimo privilegio a cada una de ellas. Estableciendo permisos por particiones así como la gestión de permisos de los ficheros que se alojan en las particiones.

La elección de cada uno de los sistemas de archivos estará relacionada con las características que proporciona cada uno de los sistemas de archivos.

Para sistemas operativos Linux se indican algunos de los modificadores del fichero de configuración de las particiones (/etc/fstab) y sus características de montaje inicial asociadas al sistema de ficheros:

- Noauto: montaje automático.
- Noexec: no admitirá la ejecución de ficheros.
- Nodev: no admitirá la instalación de dispositivos.
- Permisos: permisos de solo lectura(ro) y lectura y escritura (rw).
- Default: opciones para esta configuración (rw, uid, dev, exec, auto, nouser, async)

Además, se deberá proteger aquellas particiones que alberguen información de los usuarios y configuraciones del sistema, para que en caso de recuperación del sistema se haga de una manera rápida y eficaz. A continuación, se indica la guía de referencia del CCN relativo al [bastionado de sistemas Linux con la configuración de las particiones](#).

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.



GOBIERNO
DE ESPAÑA

MINISTERIO
DE EDUCACIÓN
Y FORMACIÓN PROFESIONAL



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

Historial de actualizaciones