

|  |
| --- |
| UNIDAD 8: RESUMEN  CUADERNO |
|  |
|  |

FUNDAMENTOS DEL HARDWARE

JUAN CARLOS NAVIDAD GARCÍA

**Índice:**

[1. Sistemas informáticos: 4](#_Toc135481340)

[2. Instalación de un Sistema Informático. Elementos: 4](#_Toc135481341)

[2.1. Certificaciones: 4](#_Toc135481342)

[3. Elementos de un sistema informático: 4](#_Toc135481343)

[3.1. Hardware: 4](#_Toc135481344)

[3.2. Recursos humanos: 4](#_Toc135481345)

[3.2.1. Servicio técnico: 4](#_Toc135481346)

[3.2.2. HelpDesk/CAU: 4](#_Toc135481347)

[4. Entorno del sistema: 4](#_Toc135481348)

[4.1. Ubicación del sistema: 4](#_Toc135481349)

[4.2. Tomas de tierra: 4](#_Toc135481350)

[4.3. Conexión de periféricos: 4](#_Toc135481351)

[4.4. Infraestructura de red: 4](#_Toc135481352)

[4.5. Configuración de la BIOS: 4](#_Toc135481353)

[5. Mantenimiento del sistema: 5](#_Toc135481354)

[5.1. Mantenimiento Predictivo: 5](#_Toc135481355)

[5.2. Mantenimiento Preventivo: 5](#_Toc135481356)

[5.3. Mantenimiento Correctivo: 5](#_Toc135481357)

[5.4. Frecuencia del mantenimiento: 5](#_Toc135481358)

[6. Solución de fallos y averías: 5](#_Toc135481359)

[6.1. Averías hardware: 5](#_Toc135481360)

[6.2. Averías software: 5](#_Toc135481361)

[6.3. Procedimiento ante una avería: 5](#_Toc135481362)

[6.4. Detección de averías: 5](#_Toc135481363)

[6.5. Informe de avería: 5](#_Toc135481364)

[6.6. Mensajes de aviso y señales luminosas y acústicas: 5](#_Toc135481365)

[6.7. Averías: síntomas, causas y soluciones: 5](#_Toc135481366)

[6.7.1. Fallos habituales por componentes: 5](#_Toc135481367)

[7. Garantía: 5](#_Toc135481368)

[8. Securización del sistema informático: 5](#_Toc135481369)

[8.1. Bootstrap: 5](#_Toc135481370)

[8.2. Creación de Imágenes del sistema: 5](#_Toc135481371)

[8.3. Malware: 5](#_Toc135481372)

[9. Aseguramiento de la información: 6](#_Toc135481373)

[9.1. Copias de seguridad: 6](#_Toc135481374)

[9.1.1. Tipos de copias de seguridad: 6](#_Toc135481375)

[9.1.2. RAID: 6](#_Toc135481376)

[9.2. Fallos en los soportes: recuperación: 6](#_Toc135481377)

[9.2.1. Recuperación Software: 6](#_Toc135481378)

[9.2.2. Recuperación Software del soporte: 6](#_Toc135481379)

[9.2.3. Recuperación Hardware: 6](#_Toc135481380)

# Sistemas informáticos:

La ISO (Organización Internacional de Estandarización), define un Sistema Informático como:

"Una o más computadoras, el software asociado, los periféricos, los terminales, los operadores humanos, los procesos físicos, los medios de transmisión de la información, etc., que constituyen un todo autónomo capaz de realizar un tratamiento de la información."

La Teoría General de los Sistemas ha influido significativamente en esta definición. Un sistema informático desde un punto de su estructura física y funcional, constituye la base de cualquier sistema de información automatizada (SIA) en la empresa.

Los elementos que componen un sistema informático, son:

* Hardware.
* Software
* Personal
* Documentación
* Procedimientos

# Instalación de un Sistema Informático. Elementos:

## **Certificaciones:**

Existen varias certificaciones relacionadas con la instalación de sistemas informáticos en Europa y España. Algunas de las más importantes son:

* **Certificación CompTIA A+**: Valida conocimientos técnicos para instalar, mantener, reparar y configurar equipos y sistemas operativos informáticos.
* **Certificación Microsoft Certified Systems Engineer (MCSE)**: Acredita conocimiento avanzado en planificación, implementación, mantenimiento y resolución de problemas de sistemas informáticos basados en tecnología Microsoft.
* **Certificación Cisco Certified Network Associate (CCNA)**: Valida habilidades básicas para instalar, configurar y operar redes de computadoras.
* **Certificación Linux Professional lnstitute Certification (LPIC)**: Acredita habilidades para administrar sistemas basados en Linux, incluyendo instalación, configuración, mantenimiento y resolución de problemas.
* **Certificación ITIL (lnformation Technology lnfrastructure Library)**: Acredita conocimiento de las mejores prácticas para la gestión de servicios de tecnología de la información, incluyendo la instalación y configuración de sistemas informáticos

Además de estas, hay otras certificaciones específicas para áreas como seguridad informática, programación y análisis de datos.

# Elementos de un sistema informático:

## **Hardware:**

## **Recursos humanos:**

### Servicio técnico:

### HelpDesk/CAU:

# Entorno del sistema:

## **Ubicación del sistema:**

## **Tomas de tierra:**

## **Conexión de periféricos:**

## **Infraestructura de red:**

## **Configuración de la BIOS:**

# Mantenimiento del sistema:

## **Mantenimiento Predictivo:**

## **Mantenimiento Preventivo:**

## **Mantenimiento Correctivo:**

## **Frecuencia del mantenimiento:**

# Solución de fallos y averías:

## **Averías hardware:**

## **Averías software:**

## **Procedimiento ante una avería:**

## **Detección de averías:**

## **Informe de avería:**

## **Mensajes de aviso y señales luminosas y acústicas:**

## **Averías: síntomas, causas y soluciones:**

### Fallos habituales por componentes:

# Garantía:

# Securización del sistema informático:

## **Bootstrap:**

La rutina Bootstrap es una de las rutinas principales del BIOS y recordamos que es la encargada de lanzar a Memoria y CPU el programa que se encuentra en el sector de arranque de la unidad de arranque (disco duro, usb, etc), también llamado sector cero.

Básicamente consiste en recorrer las unidades de nuestro equipo en el orden que se ha configurado en BIOS, y lanzar el primer software de arranque que encuentre.

SecureBoot:

Con UEFI y el particionado GPT se introduce un método para securizar el sector de arranque y evitar que un software no firmado pueda desplazar al cargador del sistema y ponerse él.

Para evitar esto se realiza un intercambio de firmas (claves) que van a garantizar al BIOS UEFI que lo que se está cargando es el sistema operativo y no cualquier otra aplicación.

Reparar el sector de arranque:

Hay muchas veces que, un técnico se encuentra con un equipo que no arranca y sospecha que el motivo es porque el cargador de arranque, ya sea GRUB o el NTLDR de Windows, ha dejado de funcionar. La solución es utilizar Rescatux, o Boot-Rapair-Disk que son distribuciones que permiten a un técnico recuperar el cargador de arranque.

## **Creación de Imágenes del sistema:**

Una imagen del sistema es como una "foto" estática que se le hace al mismo para después volcarla directamente al disco y dejarlo como estaba en el momento en el que se creó la imagen. Actualmente existen varias técnicas para lograr esto, pero vamos a ver dos:

Congelación del sistema (Freeze):

La congelación del sistema consiste en cargar una rutina en el bootstrap del sistema que restaura el sistema operativo a un estado anterior en cada inicio. Esto se hace mediante la copia de archivos clave del sistema, como el registro y la tabla de particiones, en lugar de crear una imagen completa del sistema, lo cual sería más lento. Sin embargo, esta técnica a menudo no es compatible con secure boot. Por ejemplo se puede utilizar el software RebootRestoreRX.

Creación de Imágenes completas:

Esta opción consiste en crear imágenes completas del disco duro o de alguna partición del mismo. Para ello existe numeroso software propietario, pero Clonezilla es actualmente el programa más utilizado.

## **Malware:**

El malware se refiere a software malicioso como virus, troyanos, adware, entre otros. Un antivirus, como el que viene incluido en Windows, no es suficiente para protegernos completamente del malware. Esto se debe a que el malware evoluciona constantemente y puede encontrar nuevas formas de vulnerar la seguridad del sistema a través de exploits. El antivirus puede tardar en detectar y no siempre puede eliminar el malware una vez que se ha propagado.

Si tenemos un dispositivo infectado los pasos para proceder son los siguientes:

* No volver a arrancar con el disco duro contaminado ni con ninguna USB del usuario, ya que también puede estar infectada
* Respaldar los datos del disco duro contaminado
* Instalar un antivirus en USB desde una máquina limpia y arrancar el sistema con él. Hacer una limpieza profunda del mismo.
* Si no conseguimos reparar el sistema de esta forma, habrá que hacer una copia de seguridad de los datos y borrar completamente las particiones del disco infectado, ya que pueden existir particiones ocultas en las que el virus se esconda.
* Reinstalar el sistema operativo y volcar de nuevo los datos (después de desinfectarlos)

# Aseguramiento de la información:

## **Copias de seguridad:**

### Tipos de copias de seguridad:

### RAID:

## **Fallos en los soportes: recuperación:**

### Recuperación Software:

### Recuperación Software del soporte:

### Recuperación Hardware: