SEMINARIO 2
SEGURIDAD FÍSICA

Protegiendo el hardware

José Manuel Redondo López Proyecto *"S-81 Isaac Peral"* v4.0

Fuente: Bing Chat AI

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

Logo: @creative_vanesa (*Instagram*)

Objetivos de aprendizaje

- **Conocer los peligros asociados a conceder acceso físico a un sistema informático**
- **Ser capaz de anticipar los peligros que una instalación informática puede tener**
  - Pero desde el punto de vista de su integridad física
- **Conocer las pautas básicas a seguir para crear una instalación física de un sistema informático**
  - Que cumpla un nivel mínimo de requisitos de seguridad

ÍNDICE

< Ir al Índice

Fuente: Bing Chat AI

INTRODUCCIÓN

Conceptos básicos de seguridad física

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

INTRODUCCIÓN

- La seguridad física se refiere a
  - **La seguridad del entorno** donde se encuentran los activos de la organización
    - Edificio, instalación eléctrica, gas, agua, aire acondicionado, puntos de acceso (puertas, ventanas...)
    - Estos elementos pueden comprometer la seguridad de todo el sistema
  - **La seguridad del equipo físico** de un sistema informático
    - Ordenadores, cableado eléctrico y de red, dispositivos de red...
  - **La seguridad del personal** responsable de los sistemas o de su seguridad
    - Administradores, técnicos, personal de seguridad, ..
- El objetivo general es
  - Evitar daños e interferencias contra las instalaciones de la organización y su información
  - Impedir el acceso no autorizado

INTRODUCCIÓN

- **Estas posibles vulnerabilidades de seguridad pueden ocurrir**
  - Durante las operaciones normales realizadas por la organización
  - En situaciones extraordinarias: inundaciones, cortes de energía, ...
  - Por la acción de intrusos
  - Descubiertas por auditores de seguridad
  - Por ataques dirigidos a nosotros
- **La seguridad física es una parte importante de una auditoría de seguridad: no se puede hacer mal**
  - Debido a esto, las políticas y metodologías de seguridad (como ISO 27002, OSSTMM, tema de **teoría 4**) tienen una sección dedicada a ella
  - También hay otras guías de seguridad física
    - "Normas de la autoridad nacional para la protección de la información clasificada"
      - Del CNI (Centro Nacional de Inteligencia)
      - https://www.cni.es/comun/recursos/descargas/DOCUMENTO_5_-_Normas_de_la_Autoridad.pdf
    - Real decreto 704/20122 (20 de Mayo) aprobando el reglamento para la protección de infraestructuras críticas
      - https://boe.es/diario_boe/txt.php?id=BOE-A-2011-8849

< Ir al Índice

Fuente: Bing Chat AI

PROTEGIENDO EL ENTORNO

Asegurando el sitio donde tienes tus ordenadores

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

Seguridad física del entorno

- Acceso físico
- Acceso al centro de datos
- Amenazas externas y ambientales
- Fuente de alimentación
- Comunicaciones
- Seguridad en las oficinas
- Trabajar en áreas seguras
- Warchalking

¡Esta no es una buena forma de luchar contra inundaciones! ☺. Fuente: https://www.pinterest.com/pin/557390891385500743/

Entorno: Edificio

- En seguridad física el primer elemento a considerar es el "contenedor" del equipamiento: el edificio
- Es necesario tener planos **actualizados** (¡y **realistas**!)

5.2 Seguridad Física

Contempla el nivel de seguridad física alcanzado en las instalaciones que albergan la Sala de Máquinas objeto de estudio.

5.2.1 Ubicación

Las instalaciones del Centro se encuentran en el Edificio de Ciencias del Campus de Llamaquique, situado en la Calle Calvo Sotelo s/n, repartidas por las plantas del sótano, bajo, primera, segunda y tercera (incluyendo bajocubierta). Todas ellas comparten instalaciones con aulas de formación y despachos del profesorado.

En la planta sótano se encuentra la acometida de suministro y las calderas del sistema de calefacción, así como el cuadro central de activación de dispositivos de seguridad (aspersores, circuitos hidráulicos, eléctricos, etc.). Esta planta dispone de dos accesos a la calle, uno de ellos es la salida de emergencia y el otro el patio de acceso a la vivienda del bedel. La entrada principal al edificio se encuentra en la planta baja, interceptada por un doble cierre de verja de hierro y puertas de cristal, tras las que se encuentra situada la cabina de Conserjería.

Fuente: *Diagnóstico de la Seguridad de los Sistemas de Información*. PFC Cód. DMKPC-0737. EUITIO (antecesora de la EII)

Entorno: Acceso físico

- Debe realizarse un inventario **de todos los accesos posibles**
- Todos los accesos al edificio deben revisarse
  - **¡Para que los usuarios no autorizados no puedan entrar en él fácilmente!**
  - A través de los **medios "típicos"**
    - Puertas de acceso, de servicio, de garaje...
  - **O medios "alternativos"**
    - Ventanas, tragaluces, conductos de ventilación o de servicio, ...
- El objetivo es proponer las contramedidas que se consideren necesarias
  - Estas incluyen barreras, cerraduras, detectores, cámaras...

Nuestro edificio falla este test...¡todo el mundo puede entrar!

Fuente: *GIS de la Universidad de Oviedo*

Entorno: Acceso físico

- Este ejemplo muestra la auditoría de seguridad física realizada a nuestra escuela hace años
- Muestra edificios, controles de acceso, mediciones de seguridad y su estado operativo actual
- Hay varias deficiencias detectadas
  - No hay cerraduras / llaves de seguridad
  - ¡Alarmas desactivadas!
  - ... (tranquil@s, era en otro edificio ☺)

☑ *Enumerar las áreas con control de acceso.*

Todos los edificios de **EUITIO** (incluyendo el **Aulario de Geológicas** y la **Facultad de Magisterio**) disponen de control de acceso al edificio mediante cabinas.

Dentro del **Edificio de Ciencias**, el acceso a los laboratorios, aulas, despachos y secretaría se controla mediante cerradura. Las llaves son almacenadas por el responsable del despacho, guardando siempre el bedel en la garita de la entrada una copia de todas las llaves del edificio. La garita está cerrada, a su vez, por una llave que sólo tiene el bedel.

☑ *Examinar los tipos de dispositivos de control e acceso.*

Los accesos a las áreas restringidas se controlan mediante cerradura ordinaria. Los accesos desde el exterior se controlan mediante rejas y portalones de hierro en las puertas y ventanas de la planta baja.

☑ *Examinar los tipos de alarmas.*

Todas las alarmas han sido desactivadas debido al elevado número de incidentes diarios que provocaban los alumnos.

☑ *Determinar el nivel de complejidad de los dispositivos de control de acceso.*

Las cerraduras y las llaves no son de seguridad. Las puertas que cierran el acceso a las áreas restringidas dentro de los edificios no son blindadas, ni los marcos tampoco.

Las rejas que protegen las ventanas de la planta baja son fijas. No obstante, algunas ventanas de la primera planta son relativamente sencillas de alcanzar y no disponen de ningún medio de disuasión ante ataques intrusivos.

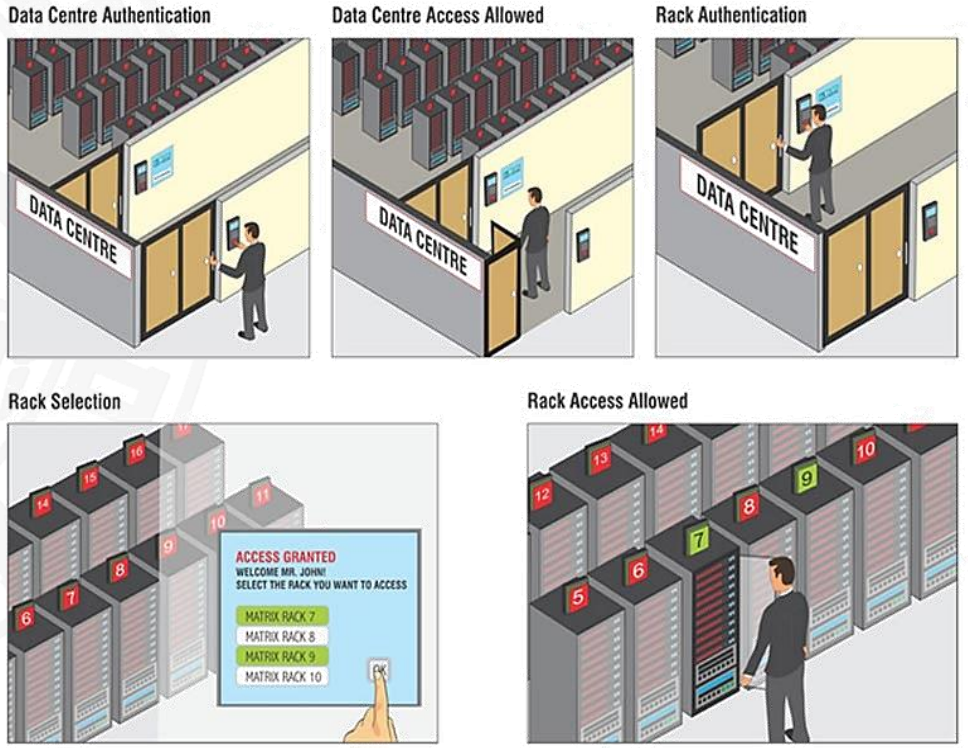
Fuente: *Diagnóstico de la Seguridad de los Sistemas de Información*. PFC Cód. DMKPC-0737. EUITIO

Entorno: Acceso al centro de datos

- **Cada acceso a las salas del centro de datos debe ser estudiado y protegido individualmente**
  - Independientemente de las políticas y medidas del edificio
- **Los accesos deben ser controlados para permitir solo usuarios autorizados**
  - Usando controles adicionales como cerraduras electrónicas con código, guardias de seguridad...
- **Todo acceso debe ser autorizado y anotado, siguiendo un procedimiento establecido**
  - Incluyendo personal no técnico (limpieza, mantenimiento...)
- **Las salas del centro de datos deben estar aisladas por paredes y puertas sólidas**
- **No debe ser posible acceder de otra forma**
  - Ventanas, conductos…

El centro de datos de nuestra escuela…

- Está correctamente aislado
- Accesible a través de puertas de seguridad
- Los racks tienen puertas individuales
- ¡Pero no se documenta el control de acceso!



Fuente: https://www.isrmag.com/matrix-access-control-data-centre-solution

Entorno: Amenazas externas y del entorno

- El diseño y construcción del edificio debe minimizar los efectos de posibles desastres que puedan ocurrir en el entorno donde se encuentra
- Debe prestarse especial atención a esto en zonas problemáticas
  - Zonas sísmicas, de inundaciones, de deslizamientos de tierra, etc.
- El edificio debe tener instalaciones de detección y extinción de incendios
  - En el centro de datos no deben ser agresivos con el hardware
  - Basados en CO_2 o espuma, no en agua directamente
  - Los sistemas más modernos usan agua micropulverizada
- El centro de datos debe soportar inundaciones
  - Debido a averías en el edificio (tuberías)
  - O por causas atmosféricas
  - Normalmente se logra con detectores, bombas de drenaje, falsos suelos-suelo técnico...

Nuestra escuela…

- **No tiene medidas contra problemas con el entorno (pero no está en una zona problemática)**
- **No tiene equipos contra incendios adaptados a ordenadores**
- **No hay medidas contra inundaciones**

ENTORNO: ¡ESTAS AMENAZAS SON MUY REALES!

Las inundaciones obligan al desalojo de 40 pacientes del Hospital de Arriondas

• El desbordamiento de los ríos ha forzado a trasladar a los afectados a otros centros hospitalarios del Principado de Asturias

Evacuación de pacientes del Hospital de Arriondas (Asturias) (EP)

AGENCIAS

24/11/2021 16:32 | Actualizado a 24/11/2021 16:39

Cuarenta pacientes del Hospital del Oriente de Asturias, en Arriondas, están siendo trasladados a otros centros

Al Minuto

West Ham – Brighton & Hove Albion: El partido de fútbol de Jornada 14 , en directo

Fuente: https://www.lavanguardia.com/local/asturias/20211124/7885837/inundaciones-obligan-desalojo-40-pacientes-hospital-arriondas.html

INTERNET NEWS MARCH 10, 2021 / 8:41 AM / UPDATED 9 MONTHS AGO

Millions of websites offline after fire at French cloud services firm

By Mathieu Rosemain, Raphael Satter 3 MIN READ

PARIS (Reuters) - A fire at a French cloud services firm has disrupted millions of websites, knocking out government agencies' portals, banks, shops, news websites and taking out a chunk of the .FR web space, according to internet monitors.

Fuente: https://www.reuters.com/article/us-france-ovh-fire-idUSKBN2B20NU

Entorno: Amenazas externas y del entorno

- **Todas las medidas mencionadas tienen sentido si la zona de construcción tiene un riesgo potencial para cualquiera de estos problemas**
  - Si la ubicación del edificio está libre de actividad sísmica, se pueden "relajar"
- **El instituto geológico y minero publica los riesgos de cada zona en España**
- **La auditoría de la escuela arroja un resultado satisfactorio en este asunto**
  - Como decía, ¡no estamos en una zona peligrosa!

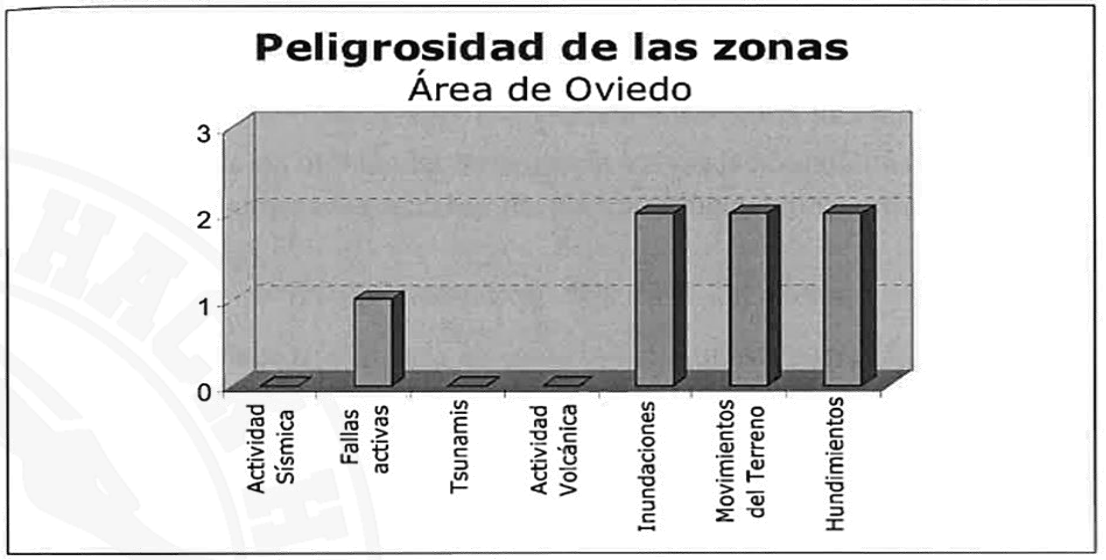


Figura 7 Fuente: Instituto Geológico y Minero de España

En cuanto al impacto de riesgo geológico para el área de Oviedo, zona donde se ubican las instalaciones, y según se muestra en el gráfico adjunto de la página anterior, presenta un riesgo nulo de sufrir desastres por actividad sísmica, Tsunamis y erupciones volcánicas; un riesgo bajo de sufrir desastres por fallas activas; y un riesgo moderado ante desastres por inundaciones, movimientos del terreno o hundimientos.

5.2.2 Desastres Naturales

Garantía de que las instalaciones están protegidas contra desastres naturales: existencia de sistemas de evacuación ante inundaciones; protección contra vendavales, sismos, rayos, etc.; resistencia de techo y estructura; etc.

Aspectos positivos:

Fuente: *Diagnóstico de la Seguridad de los Sistemas de Información*. PFC Cód. DMKPC-0737. EUITIO

Entorno: Sistema eléctrico

- **Es necesaria una fuente de alimentación estable e ininterrumpida para garantizar un trabajo adecuado de los ordenadores**
  - Esta fuente de alimentación debe estar adecuadamente protegida contra sobretensiones
- **La instalación eléctrica debe estar protegida contra posibles ataques**
  - **Dentro del edificio**: diseño adecuado de la instalación por separación de fases...
  - **Exterior**: conexiones eléctricas protegidas
- **Una fuente de alimentación es más segura cuanta más redundancia tenga**
  - En las líneas eléctricas de la empresa suministradora
  - La contratación del suministro de energía a varias empresas con sistemas de distribución independientes
    - ¡Si la red de distribución permite hacerlo!
  - Instalación de generadores eléctricos
  - Dentro del edificio, la instalación de múltiples circuitos de alimentación del centro de datos

ENTORNO: SISTEMA ELÉCTRICO

- **En nuestra escuela la instalación del sistema eléctrico dentro del edificio es adecuada**
- **No hay información sobre la periodicidad de las operaciones de mantenimiento**
- **No hay redundancia**
  - Sólo una empresa suministra energía, no hay circuitos redundantes...
  - La redundancia suele tener un alto coste
  - Para justificar su implementación, la información almacenada en los sistemas informáticos debe ser crítica

5.2.3 Sistema Eléctrico

Verifica que el suministro de fluido eléctrico mantiene sus características principales: garantía del suministro y conocimiento del tendido; estabilidad de suministro y controles del tendido; existencia de SAI, SAI, grupos electrógenos; diversificación de suministro e iluminación de emergencia; etc.

Aspectos positivos:

+ (I) El suministro eléctrico del edificio de la Facultad de Ciencias se considera fiable a la vista de las estadísticas de pérdidas de suministro proporcionadas por **Hidrocantábrico** al **Vicerrectorado de Infraestructuras**.

+ (I) Se controla la estabilidad y el voltaje de la línea en la Sala de Máquinas y los laboratorios.

+ (I) Todas las zonas de los edificios de la Facultad de Ciencias, Facultad de Geología y Facultad de Magisterio disponen de alumbrado de emergencia, cuyo mantenimiento es responsabilidad del **Vicerrectorado de Infraestructuras** quien lo ha subcontratado a la empresa **Eulen**. El alumbrado es comprobado regularmente, así como la verificación del estado del cableado (incluyendo puntos de iluminación, tomas de energía).

+ (N) Los cables de suministro eléctrico están protegidos por tubos rígidos en las bajantes dentro del edificio, y por canaletas metálicas en el exterior.

Aspectos negativos:

- (I) *RF100*

No se dispone de esquemas eléctricos actualizados.

- (I) ***RF101***

Se desconoce si se pasan inspecciones técnicas de los sistemas eléctricos, así como su alcance y periodicidad.

Fuente: *Diagnóstico de la Seguridad de los Sistemas de Información*. PFC Cód. DMKPC-0737. EUITIO

Entorno: Comunicaciones

- El diseño de la red del edificio y centro de datos debe ser resistente contra interrupciones generales
- De nuevo esto se puede lograr mediante redundancia de equipos (routers, hubs, ...) y del cableado
- Deben considerarse también medidas de prevención de posibles ataques desde el interior del edificio
  - El cableado y el equipo de red no deben estar accesibles, sino ocultos y protegidos dentro de falsos techos, suelos técnicos, etc.
  - No deben dejarse accesibles bocas de red ni otro tipo de equipamiento sin vigilancia
    - Un intruso podría conectar un ordenador portátil u otro tipo de equipo de vigilancia

Entorno: Seguridad en la oficina

Visibilidad de dispositivos

- Las comunicaciones por radio, como las de los dispositivos de control de acceso o el hardware que emite señales RFID, deben estar aisladas si fuera posible
- Dispositivos como Flipper Zero (https://flipperzero.one/) pueden usarse para hackearlos

Visibilidad física

- El trabajo del usuario/empleado no debe ser observable desde el exterior del edificio
- El monitor y el teclado deben estar orientados de tal manera que un "espía" no pueda ver su contenido o lo que se escribe
  - Es una forma común de averiguar contraseñas / información sensible

Cámaras de seguridad

- Instaladas donde se almacenen datos valiosos
- Deben utilizarse de acuerdo con una política establecida por la empresa
- Y de acuerdo con la legislación vigente (derechos de imagen de los usuarios, ASLEPI)

ENTORNO: TRABAJAR EN ÁREAS SEGURAS

- **Además de los sistemas informáticos, el personal también debe estar protegido**
  - Se deben crear planes de evacuación para situaciones peligrosas
  - El personal debe estar capacitado para utilizar estas medidas de seguridad

5.2.6 Fuego (Prevención)

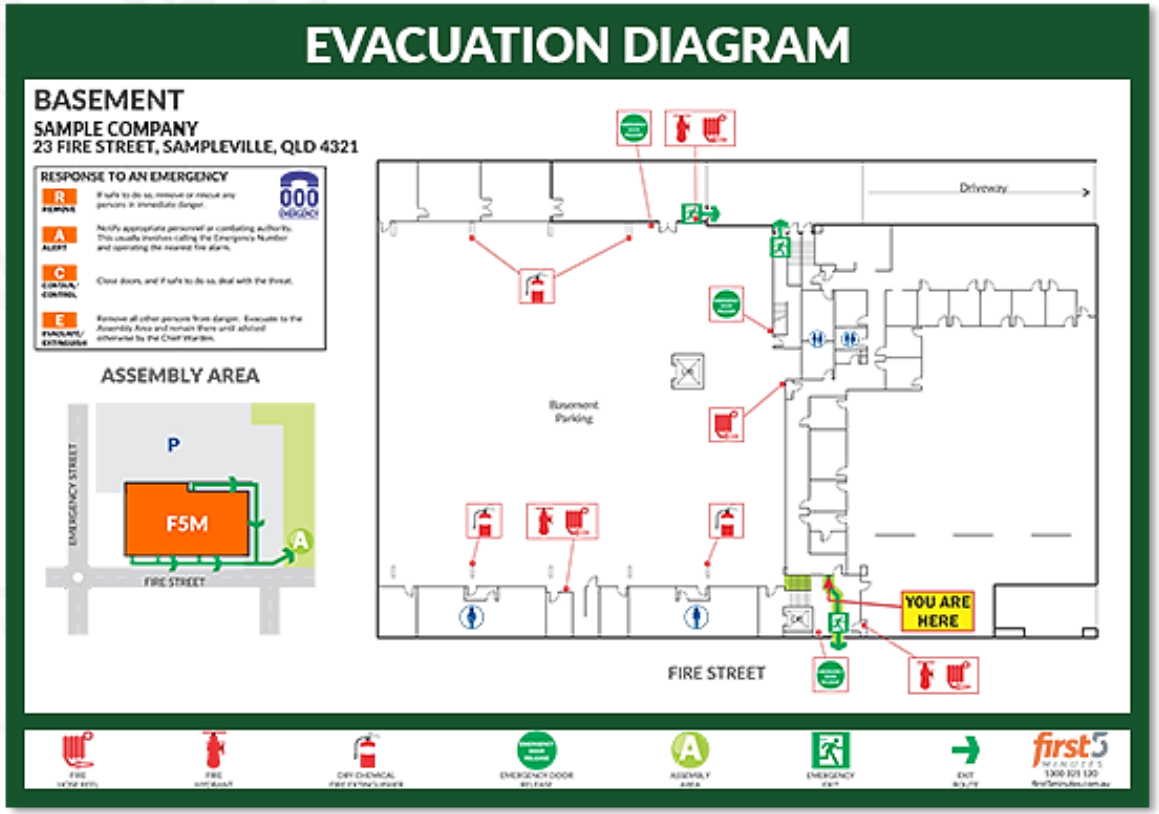
Análisis de las medidas aplicadas para la prevención de fuegos: existencia de vías libres en caso de siniestro; presencia limitada de materiales combustibles; puertas, paredes y falso techo resistente al fuego; impartición de cursillos de formación y simulacros de incendios; prevención eléctrica contra el fuego, diseños resistentes al fuego; etc.

Aspectos positivos:

+ (I) El material de primeros auxilios está guardado en conserjería, en un armario adecuadamente cerrado y señalizado pintado de blanco con una cruz roja. Puede utilizarse en cualquier momento en caso de ser necesario.

+ (I) Cuentan con extintores colocados estratégicamente y con indicadores visibles que facilitan su localización. Los extintores son revisados dentro de los plazos establecidos por la ley, para garantizar su funcionamiento en el momento que sean necesarios.

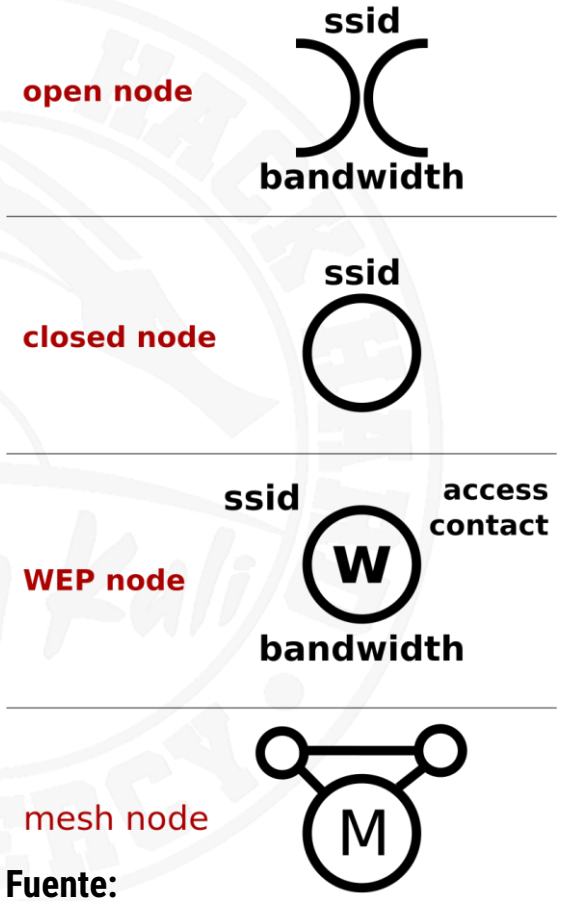
Fuente: *Diagnóstico de la Seguridad de los Sistemas de Información*. PFC Cód. DMKPC-0737. EUITIO



Fuente: https://www.first5minutes.com.au/services/fire/evacuation-diagrams

Entorno: Warchalking

- Técnica que consiste en pintar símbolos informativos en las paredes de un edificio
- Estos símbolos forman un lenguaje
  - Proporcionan información sobre las redes Wifi disponibles fuera del edificio
- Encontrar estos símbolos en un muro de un edificio requiere poner en marcha contramedidas inmediatamente para evitar más problemas



Fuente:
https://hackingblogs.com/warchalking/

Fuente:
http://etutorials.org/Networking/beginners+guide+to+wi-fi+wireless+networking/Part+III+Going+Mobile+with+Wi-Fi/Chapter+11.+Where+Can+You+Wi-Fi/War+Driving+and+War+Chalking/

< Ir al Índice

Fuente: Bing Chat AI

Protegiendo el equipamiento

Seguridad del hardware

Departamento de Informática
Universidad de Oviedo

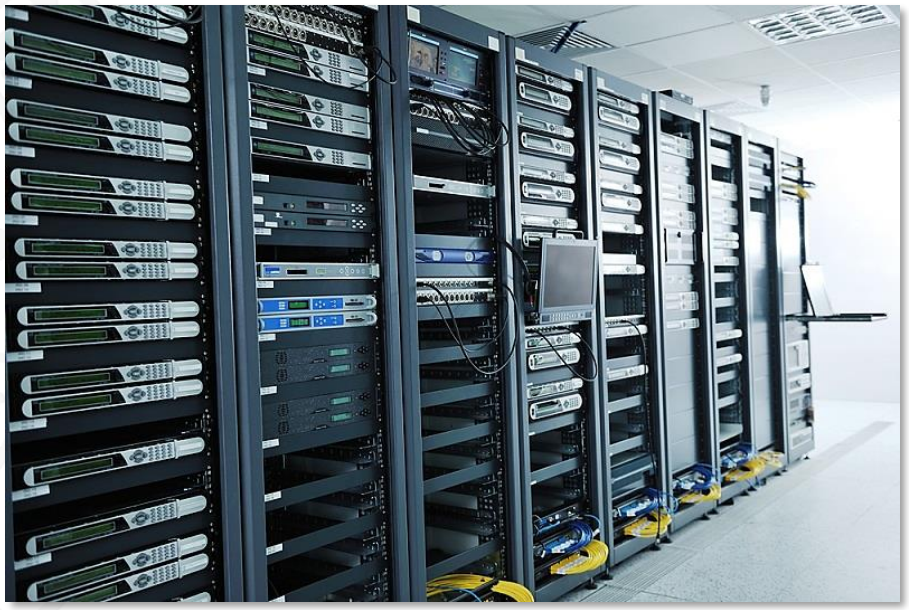
Universidad de Oviedo

SEGURIDAD FÍSICA DEL HARDWARE

- **Las medidas de seguridad del entorno deben complementarse con medidas relacionadas con el propio hardware**
  - Instalación
  - Acceso físico al hardware
  - Plan de evacuación del hardware
  - Fuente de alimentación
  - Tratamiento del calor
  - Disposición del cableado
  - Backups
  - Redundancia
  - Eliminación/retirada del hardware
  - Seguridad fuera de las instalaciones

Equipamiento físico: Instalación de equipos

- **Hay una serie de medidas que podemos tomar para garantizar que todos los equipos funcionen según lo previsto**
  - **Planificación cuidadosa** del espacio disponible
  - **Calidad del equipamiento**: la relación coste-calidad deberá evaluarse al comprar equipos, de acuerdo con los parámetros establecidos por la empresa
  - Se recomienda la instalación en **cabinas o bastidores/racks** para mejorar la protección del equipo
  - Los racks deben tener espacio reservado para **sistemas SAI** (UPS)
    - Son fundamentales para el correcto funcionamiento en caso de cortes de energía



Fuente: https://tecnotraffic.net/rack-de-servidor-vs-rack-de-red-diferencia-entre-rack-de-servidor-y-de-red/

Equipamiento físico: Acceso físico al hardware

- Además de proteger el centro de datos, cada usuario debe tener **solamente acceso físico a las máquinas autorizadas**
  - Equipos de red, servidores...
- Deben ser "imposibles" de abrir, para evitar robos o manipulaciones
  - El resto de las medidas no son válidas si alguien puede abrir un ordenador o forzar la cerradura de un rack para robar componentes

Fuente: https://www.startech.com/es-eu/gestion-de-servidores/rk3236bkf

- **Deben deshabilitarse los dispositivos externos capaces de grabar información si lo determina la política de la empresa**
  - DVD-RW, dispositivos USB...
  - Esto deshabilita la extracción no autorizada de información

¿Por qué prevenir el acceso físico? Hardware hacking

- **Dejar a personas no autorizadas acceder a nuestro hardware puede facilitar una serie de ataques**
- **Uno de los más famosos es usar un dispositivo BadUSB**
  - USBs que emulan un teclado con pulsaciones/comandos preprogramados
  - Así cualquiera podrá ejecutar comandos en nombre del usuario actual, pero normalmente sin que él lo sepa
  - El dispositivo parece otro distinto (cable USB, pendrive...)
    - https://www.redeszone.net/tutoriales/seguridad/rubber-ducky-ataque-dispositivo/
  - Ejemplos:
    - **Rubber Ducky USB pendrive** (https://thehackerway.com/2017/09/05/vuelve-el-patito-low-cost-ahora-grazna-como-un-usb-rubber-ducky-original/)
    - **Evil Crow mobile cable** (https://thehackerway.com/2019/12/23/evil-crow-cable-por-que-troyanizar-hardware/)
  - ¡Pueden ser muy baratos!: https://thehackerway.com/2017/07/10/badusb-ultra-low-cost/
  - El jailbreak de PlayStation® 3 fue un ataque de este tipo:
    - https://es.wikipedia.org/wiki/PlayStation_Jailbreak

Equipamiento físico: Plan de evacuación del hardware

Seguridad de Sistemas Informáticos

- **No sólo el personal debe ser evacuado en caso de emergencia**
  - ¡El hardware podría serlo también!
- **Debe establecerse también un plan de evacuación de hardware**
  - Detallando cómo y dónde se puede trasladar el hardware crítico para el funcionamiento de la empresa en el menor tiempo posible
  - Especificando en qué orden se evacuarán los diferentes dispositivos
  - Dependiendo de
    - La importancia de los datos que contienen
    - Y de los procesos que soportan

Fuente: https://www.firesafe.org.uk/fire-emergency-evacuation-plan-or-fire-procedure/

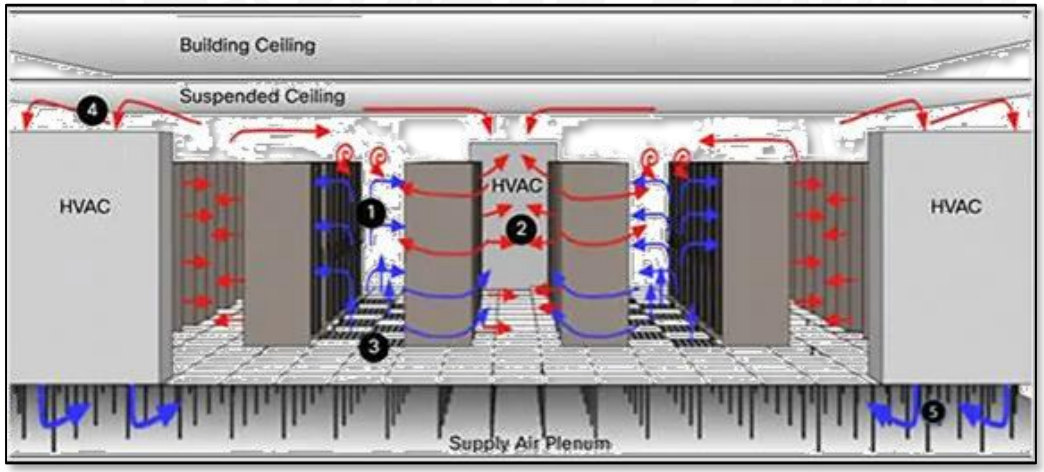
Equipamiento físico: Fuentes de energía

- **Todos los elementos de hardware deben estar protegidos contra sobretensiones o cortes de energía ocasionales**
  - Mediante SAI/UPS (Sistemas de Alimentación Ininterrumpida)
- **La planificación de los SAI debe ser apropiada**
  - Un solo SAI grande
  - SAIs más pequeños, individuales por equipo / departamento
- **La instalación eléctrica debe ser estudiada y preparada adecuadamente**
  - Con cuadros de protección eléctrica, limitadores de tensión, etc.

Fuente:
https://new.abb.com/ups/es/sistemas-sai/sai-trif%C3%A1sicas-industrial/pcs100-ups-i/destacable

Equipamiento físico: Tratamiento del calor

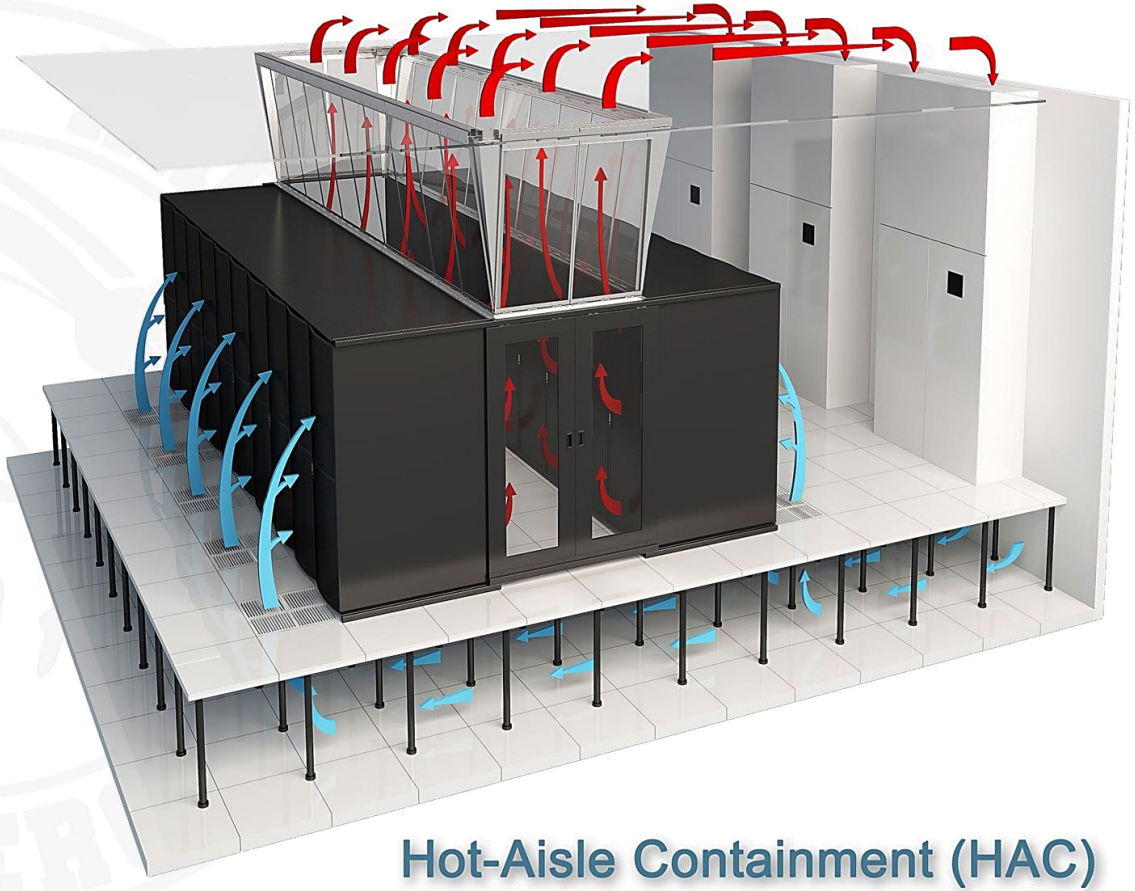
- **Todos los dispositivos informáticos generan una cantidad considerable de calor**
  - El calor debe ser extraído de su entorno
  - Para evitar daños por **sobrecalentamiento** o degradación del rendimiento (**throttling**)
- **La gestión de la refrigeración debe comenzar con un diseño de equipo adecuado**
  - Pasillos fríos / pasillos calientes
  - Si hay muchos equipos y otras soluciones no son suficientes deben instalarse **sistemas de aire acondicionado**
  - Una ventilación adecuada de las instalaciones es necesaria en cualquier caso
- **La redundancia de dispositivos de ventilación previene fallos**



Fuente:
https://medium.com/@rajatghosh/mystery-of-data-center-hot-spots-994073b48fdb

Equipamiento físico: Tratamiento del calor

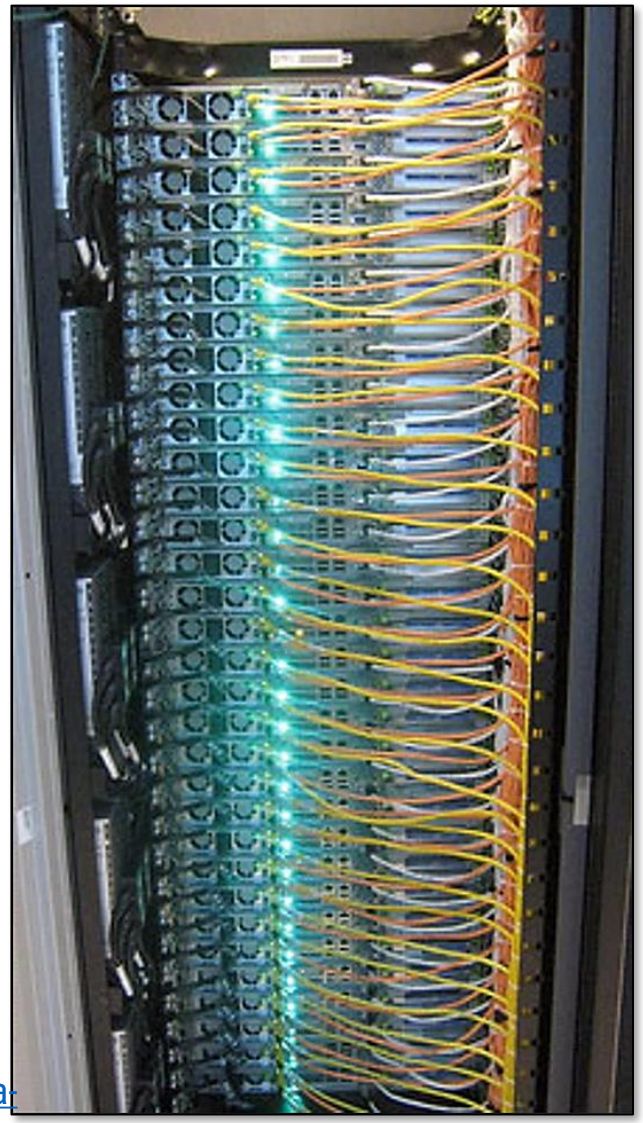
- **La instalación en racks puede provocar la acumulación de calor**
  - Podrían necesitarse modelos con sistemas integrados de ventilación y refrigeración
- **Son necesarios sistemas de monitorización de temperatura, tanto en cada dispositivo como en los armarios**
  - Además, deben instalarse en diferentes puntos de la sala estratégicamente
- **Es necesario usar software de monitorización adecuado y alarmas**
  - Ej.: Nagios (usado por nuestra escuela)
- **El hardware moderno se puede configurar para reducir su frecuencia de CPU o aumentar la velocidad de los ventiladores en caso de sobrecalentamiento**
  - Usando diferentes umbrales de temperatura



Fuente: http://www.bluewavenetwork.net/data-centers.html

Equipamiento físico: Disposición del cableado

- **En una determinada instalación pueden coexistir diferentes tipos de cableado**
  - Eléctrico, red de "par trenzado", red óptica, red coaxial, telefónico...
- **En general, todo el cableado que transmite datos basados en impulsos eléctricos podría ser perturbado**
  - Normalmente por campos electromagnéticos generados por las conducciones eléctricas (Ondas y Electromagnetismo)
- **La instalación debe hacerse de tal manera que dicha interferencia sea mínima**
  - "Blindando" los cables eléctricos y/o de datos, instalándolos en lugares diferentes, etc.

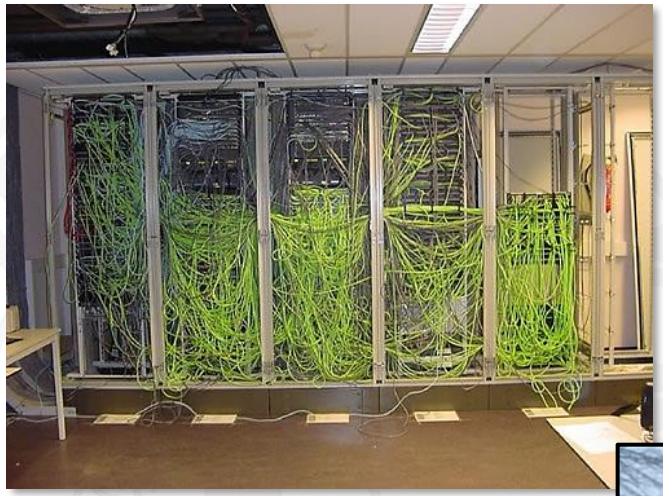


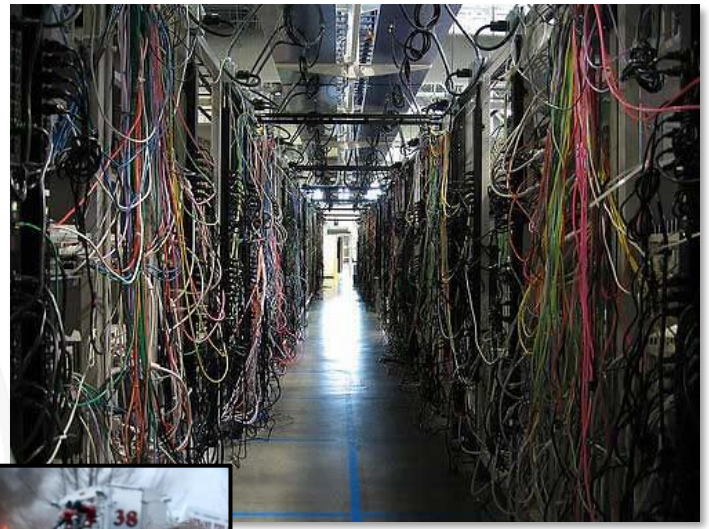
Fuente: https://www.cablinginstall.com/home/article/16481472/spectacular-data-center-cabling

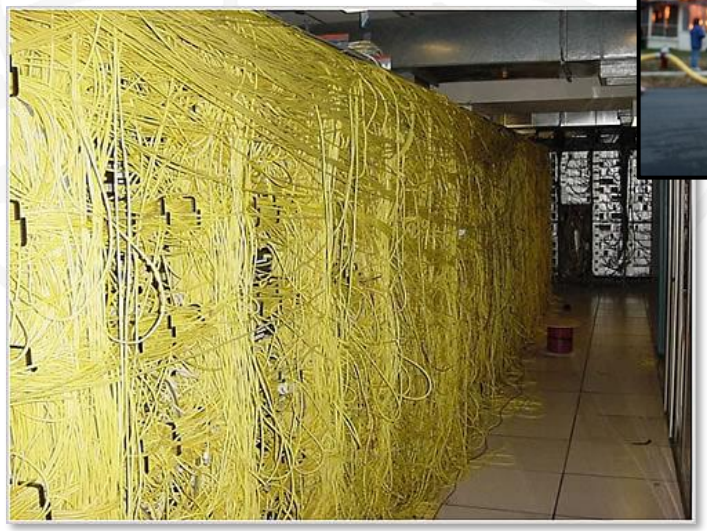
Equipamiento físico: Disposición del cableado

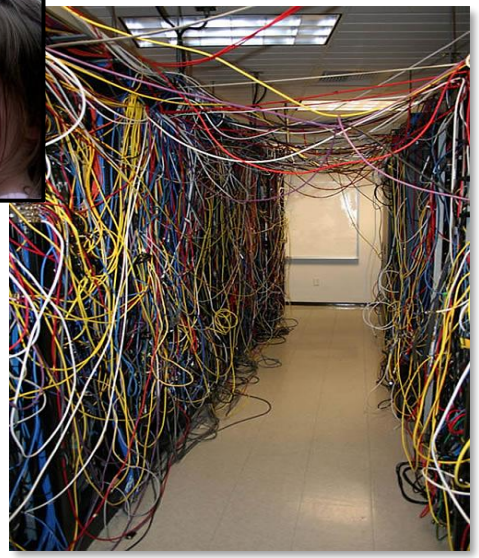
- **Desafortunadamente es común encontrar cableado con diseños "subóptimos"**
  - ¡Incluso muy propensos a fallos!
- **Esto lleva a que**
  - Desenchufar un cable suponga un tiempo de inactividad del sistema (parcial o total)
  - La documentación insuficiente sobre el diseño del cableado aumente el tiempo de reparación

Fuente: https://www.dotcom-monitor.com/blog/es/2020/05/25/servidor-cable-hell-worst-wiring-jobs-ever/









EQUIPAMIENTO FÍSICO: BACKUPS

- **Debe establecerse una política de backups clara**
  - Esta determina **qué** se copia, **cuándo** se copia, y **sobre qué dispositivos**
  - Deben también considerarse la **seguridad** y **las pruebas planificadas de restauración de estas copias**
- **Los datos críticos deben tener varias copias almacenadas**
  - En recintos ignífugos
  - En diferentes salas del edificio
  - En diferentes edificios
  - Externalizando su almacenamiento / realización
- **En ASR se ven aspectos relativos a backups**

5.3.2 Copias de Respaldo y Procedimientos de Recuperación

Aspectos positivos:

+ (I) Los becarios hacen Copia de Respaldo del servidor web de **EUITIO**.

+ (N) Cada equipo del laboratorio tiene una imagen, almacenada en CD-ROM, que permite recuperar la configuración del sistema en poco tiempo.

Aspectos negativos:

- (I) ***RL100***

No existe una política para la realización de Copias de Respaldo y los procedimientos de Recuperación.

- (I) ***RL101***

No existe un lugar centralizado para custodiar las Copias de Respaldo realizadas.

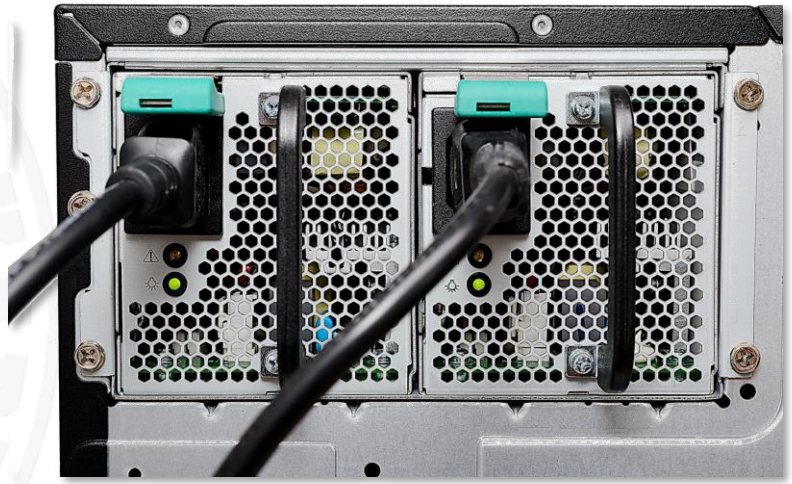
- (I) ***RL102***

No existen ordenadores de respaldo para el caso de caída de los equipos principales.

Fuente: *Diagnóstico de la Seguridad de los Sistemas de Información*. PFC Cód. DMKPC-0737. EUITIO

Equipamiento físico: Redundancia

- La seguridad para prevenir fallos en los equipos (fortuitos o no) generalmente se logra a través de su redundancia
- Esta redundancia puede ocurrir en diferentes niveles
  - Al **nivel de la máquina** (clústeres, nubes, ...)
  - **Redundancia de componentes** (procesador, memoria, fuentes de alimentación, ...)
    - Es interesante, en cualquier caso, que además de la redundancia tengan características de intercambio en caliente (hot-swap)
  - A **nivel de datos**, replicando el contenido de los sistemas de almacenamiento a otros (preferiblemente en otra ubicación)
  - Como se mencionó anteriormente, también el sistema eléctrico, el de refrigeración, ... deben ser redundantes



Fuente:
https://www.racksolutions.com/news/blog/redundant-power-supply/

Equipamiento físico: Deshacerse del hardware

- **Increíblemente, una gran cantidad de información útil sobre una empresa puede encontrares inspeccionando sus residuos (dumpster diving)**
  - No es una costumbre de los milenials (según ciertos periódicos ☺), sino un potencial delito
  - https://searchsecurity.techtarget.com/definition/dumpster-diving
- **Esta información podría ser clave para realizar ataques**
- **Por lo tanto, debe establecerse una política apropiada de tratamiento de residuos**
  - Destrucción por medios adecuados, gestión por una empresa externa especializada, ...

Fuente: https://www.pcmag.com/news/morgan-stanley-discarded-old-hard-drives-without-deleting-customer-data

Equipamiento físico: Seguridad fuera de la oficina

- El personal **debe prestar especial atención a sus dispositivos portátiles** porque son susceptibles de ser robados / perdidos
  - Por ejemplo, en los aeropuertos de EE. UU. se pierden más de 12.000 ordenadores portátiles por semana
- Su salida fuera de la empresa debe estar justificada, autorizada y seguir una serie de reglas de seguridad
  - Su ubicación **siempre** debe ser controlada
  - No deben contener información valiosa, sólo ser terminales de los servidores de la empresa
    - Si deben almacenar información localmente, **debe cifrarse**
  - Cualquier usuario que utilice dispositivos portátiles de la empresa debe conocer las políticas de seguridad de la empresa y las condiciones de uso de los dispositivos (instalación de software...)
  - Todos los ordenadores, al regresar a la empresa, deben ser revisados para localizar virus, troyanos software nuevo instalado... (o devueltos a una situación “de fábrica”)
- Si se permite traer dispositivos USB de fuera, deben considerarse dispositivos como **AuthUSB Safedoor** para prevenir ataques vía USB
  - https://www.authusb.net/safe-door/

< Ir al Índice

Fuente: Bing Chat AI

PROTEGIENDO AL PERSONAL

Seguridad y recursos humanos

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

Seguridad del personal

- **Las políticas de seguridad del personal tienen como objetivo**
  - Evitar pérdidas, daños o comprometer activos, así como la interrupción de las actividades de la organización
  - Prevenir exposiciones a riesgos, robos de la información o de recursos de tratamiento de información: se deben guardar los recursos en cajones y/o en archivadores bajo llave
- **Como parte de esta política de seguridad, debería contemplarse**
  - **No dejar funciones y equipos de soporte desatendidos**
    - Ej.: si se está imprimiendo información confidencial de la empresa
  - Uso **protectores de pantalla protegidos por contraseña** y **bloquear** el ordenador si está desatendido
- **Los controles de seguridad deben abarcar el ciclo de vida completo de los trabajadores**
  - Desde su selección hasta el momento en que abandonan la organización

< Ir al Índice

Fuente: Bing Chat AI

Protección antes del arranque

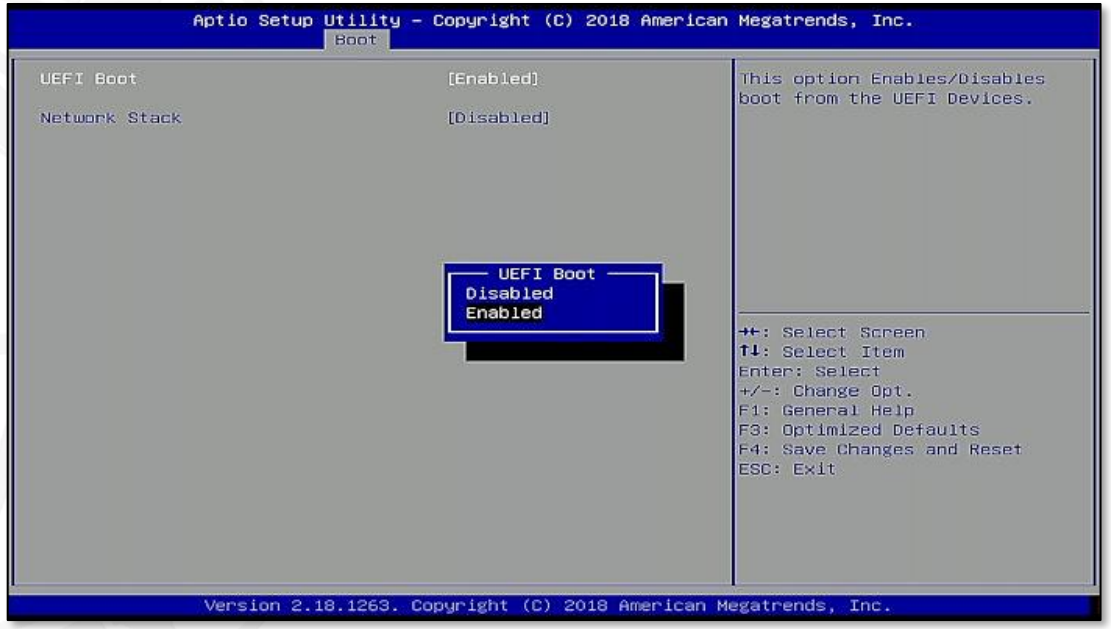
Protección adicional antes del arranque del SO

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

Operaciones de seguridad antes del arranque

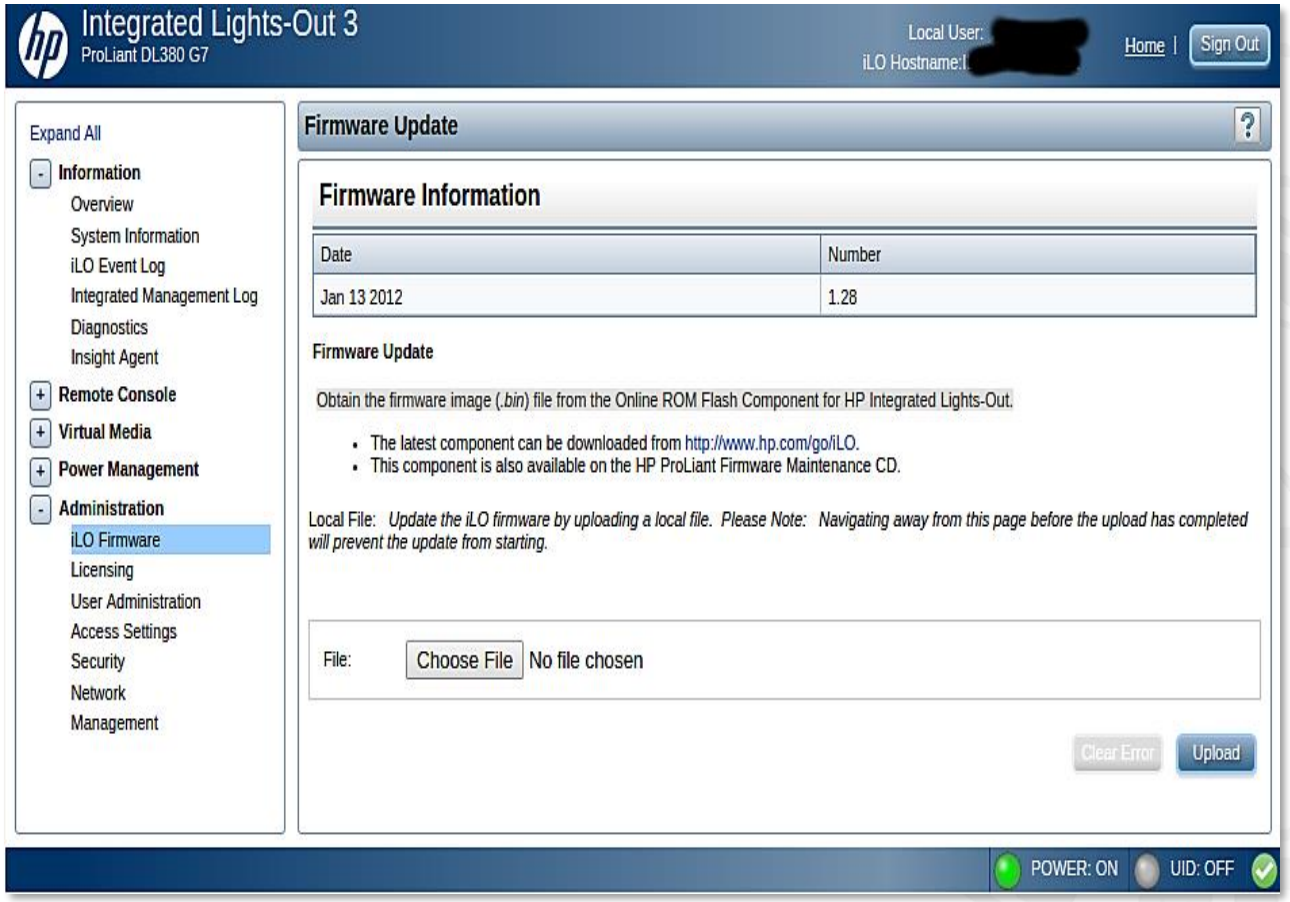
- **Antes de arrancar un equipo, hay una serie de operaciones que se deben realizar para garantizar la máxima seguridad**
  - Habilitar SecureBoot (**Esencial**)
  - Utilizar una clave UEFI para arrancar el sistema (**Adecuado**)
  - Uso del modo UEFI (**Esencial**)
  - Establecer una clave para acceder a la configuración UEFI (**Esencial**)
  - Limite el acceso al software de acceso fuera de banda, como LOMs (Lights-Out Management)
    - Vistos más tarde
  - De igual modo, limitar o deshabilitar el protocolo **Wake On Lan** (WOL)
    - Para impedir que se pongan en marcha máquinas por culpa de agentes externos



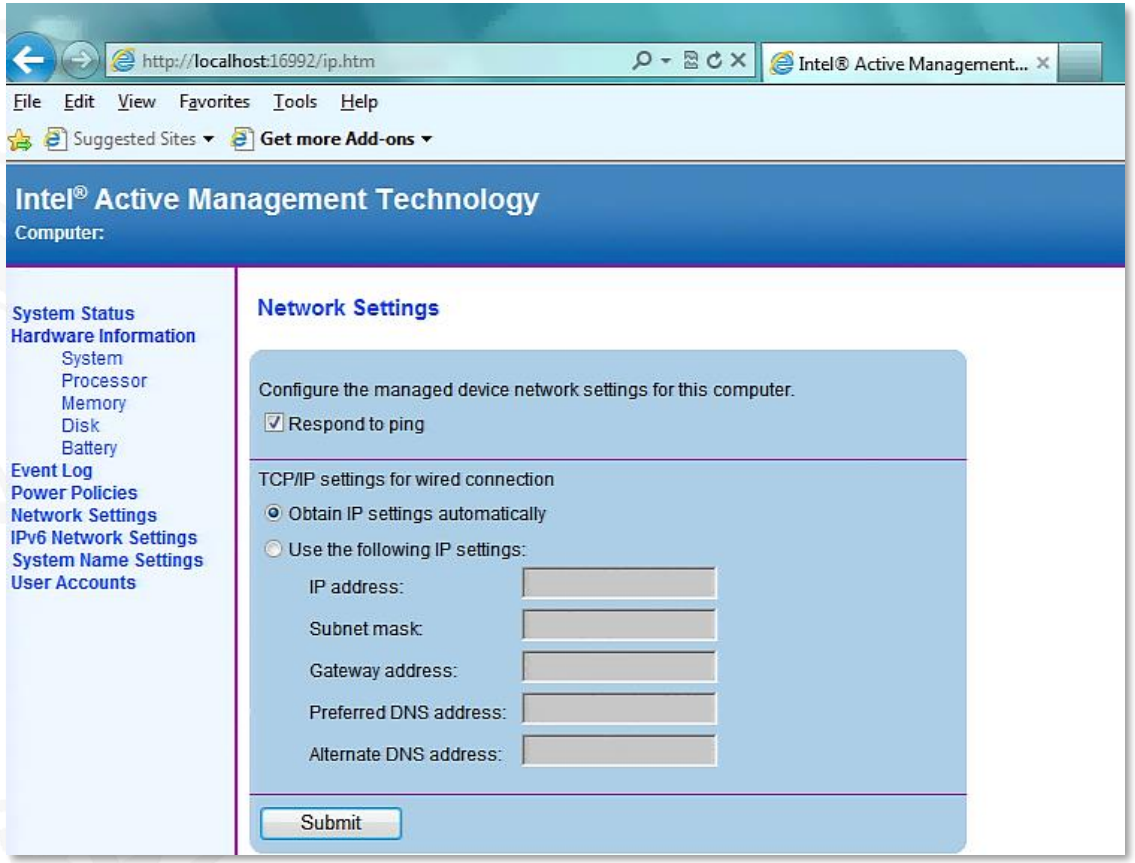
Sistemas LOM

- **Permiten la gestión remota de un ordenador...¡incluso si está apagado!**
  - Debido a eso, proteger el acceso a los mismos es crítico
- **Algunos LOM requieren conectarse a una interfaz de red determinada**
  - Solo se pueden acceder a ellos a través de una interfaz de red específica, que solo se usa para administración
- **Es importante saber si nuestros servidores tienen sistemas LOM activos**
  - Ya que se pueden usar para acceder de manera fraudulenta al servidor y llevar a cabo ataques **sin restricciones**
- **Además, a veces tienen errores que pueden comprometer nuestro servidor**
  - Por lo tanto, deben estar debidamente actualizados, securizados o desactivados si no se usan
- **Los LOM más conocidos son:**
  - **Intel AMT** (integrado en muchos modelos de gama alta Intel Core iX y Xeon):
    - https://en.wikipedia.org/wiki/Intel_Active_Management_Technology
  - **HP ILO**
    - https://en.wikipedia.org/wiki/HP_Integrated_Lights-Out
  - **Dell iDRAC**
    - https://en.wikipedia.org/wiki/Dell_DRAC

SISTEMAS LOM: HP ILO E INTEL AMT

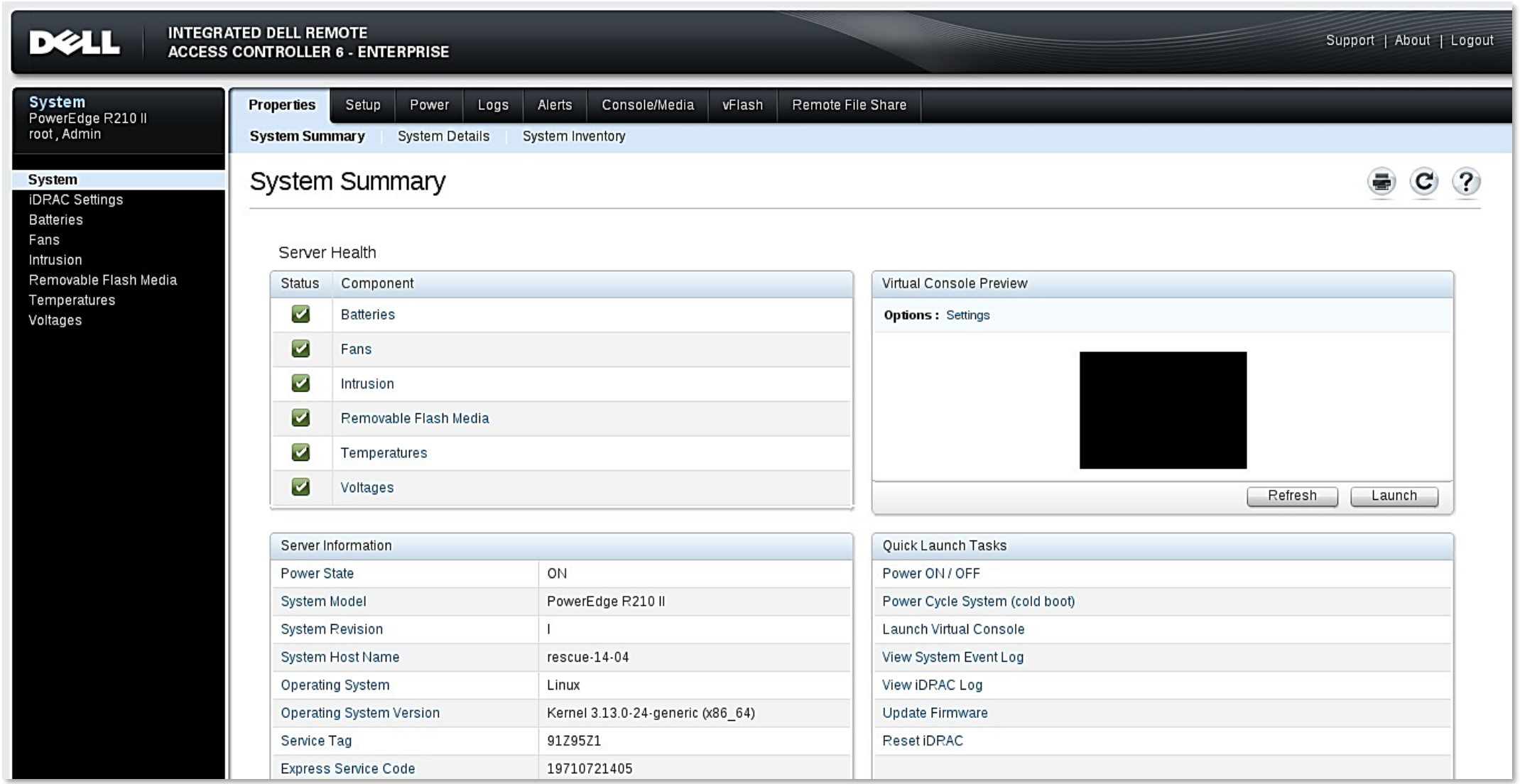


Fuente: https://serverfault.com/questions/658529/ilo-3-firmware-update-hp-proliant-dl380-g7



Fuente: https://arstechnica.netblogpro.com/information-technology/2017/05/the-hijacking-flaw-that-lurked-in-intel-chips-is-worse-than-anyone-thought/

SISTEMAS LOM: DELL IDRAC



Fuente: https://www.dell.com/support/kbdoc/es-es/000123577/configuracion-y-administracion-de-idrac-6-y-lifecycle-controller-para-los-servidores-dell-poweredge-11g

Lista de logros para autoevaluación: Seminario 2

?

- Entender el concepto de LOM y sus posibles problemas
- Entender todas las potenciales fuentes de problemas de seguridad física
- Conocer términos habituales de seguridad física: **dumpster diving**, **war chalking**...
- Ser consciente de los problemas derivados de la retirada de **hardware** inadecuada
- Entender cómo las políticas de seguridad deben incluir también al personal
- Entender las potenciales implicaciones de seguridad de sacar equipos fuera de la oficina
- Conocer las fuentes de problemas de seguridad física del entorno
- Conocer las fuentes de problemas de seguridad física del equipamiento

SEMINARIO 2
SEGURIDAD FÍSICA

Fuente: Bing Chat AI

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo