SEMINAR 2
PHYSICAL SECURITY

Protecting the hardware

JOSÉ MANUEL REDONDO LÓPEZ *"S-81 ISAAC PERAL"* PROJECT V3.0

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

Logo: @creative_vanesa (*Instagram*)

Learning goals

José Manuel
Redondo López

- **Know the dangers associated to grant physical access to a computer system**
- **Be able to anticipate the dangers that a computer installation may have**
  - But from the point of view of its physical integrity
- **Know the basic guidelines to follow in order to create a computer system installation**
  - That meet a minimum level of physical security requirements

INDEX

- Introduction
- Protecting the environment
- Protecting the equipment
- Protecting personnel
- Pre-boot protection (LOM systems)

< Go to Index

Source: zona-militar.com

INTRODUCTION

Basic physical security concepts

Introduction

José Manuel
Redondo López

- **Physical security refers to**
  - **The security of the environment** where the assets of the organization are located
    - Building, electrical, gas, water, air conditioning, access points (doors, windows, ...)
    - These elements may compromise the security of the whole system
  - **The security of the physical equipment** of computer systems
    - Computers, electrical and network wiring, network devices...
  - **The security of the personnel** in charge of the systems or its security
    - Administrators, technicians, security personnel...
- **The general goal is**
  - To prevent damage and interference against the organization premises and information
  - Prevent unauthorized access

INTRODUCTION

José Manuel
Redondo López

- **These possible security vulnerabilities can be located**
  - During the normal operations performed by the organization
  - In extraordinary situations: floods, power outages…
  - By intruders
  - By security auditors
  - By targeted attacks
- **Physical security is an important part of any security audit: it cannot be neglected**
  - Because of this, security policies and methodologies (like ISO 27002, and OSSTMM, see security policies theory topic) have a special section for it
  - There are also other physical security guidelines
    - "Normas de la autoridad nacional para la protección de la información clasificada"
      - From the Spanish CNI (Center of National Intelligence)
      - https://www.cni.es/comun/recursos/descargas/DOCUMENTO_5_-_Normas_de_la_Autoridad.pdf
    - Royal Decree 704/2011 (May 20th), approving the regulations for the protection of critical infrastructures
      - https://boe.es/diario_boe/txt.php?id=BOE-A-2011-8849

< Go to Index

Source: zona-militar.com

PROTECTING THE ENVIRONMENT

Secure where your computers are placed

PHYSICAL SECURITY OF THE ENVIRONMENT

José Manuel
Redondo López

- Physical access
- Access to the datacenter
- External and environmental threats
- Power supply
- Communications
- Security in offices
- Working in safe areas
- Warchalking

Environment: Building

José Manuel
Redondo López

- In physical security first we need to consider is the "container" of the equipment: the buildings
- It is necessary to have **updated (and realistic!) blueprints**

5.2 Physical Security

It contemplates the physical security level of the facilities under study that house the Machine Room.

5.2.1 Location

The Center's facilities are in the **Science Building** of the **Llamaquique Campus**, located on Calle Calvo Sotelo s/n, spread over the basement, ground, first, second and third floors (including undercover). All of them share facilities with teaching classrooms and faculty offices.

In the basement there is the power connection and the boilers of the heating system, as well as the central panel for activating safety devices (sprinklers, hydraulic and electrical circuits, etc.). This floor has two street accesses, one of them is the emergency exit and the other the access patio to the janitor's house.

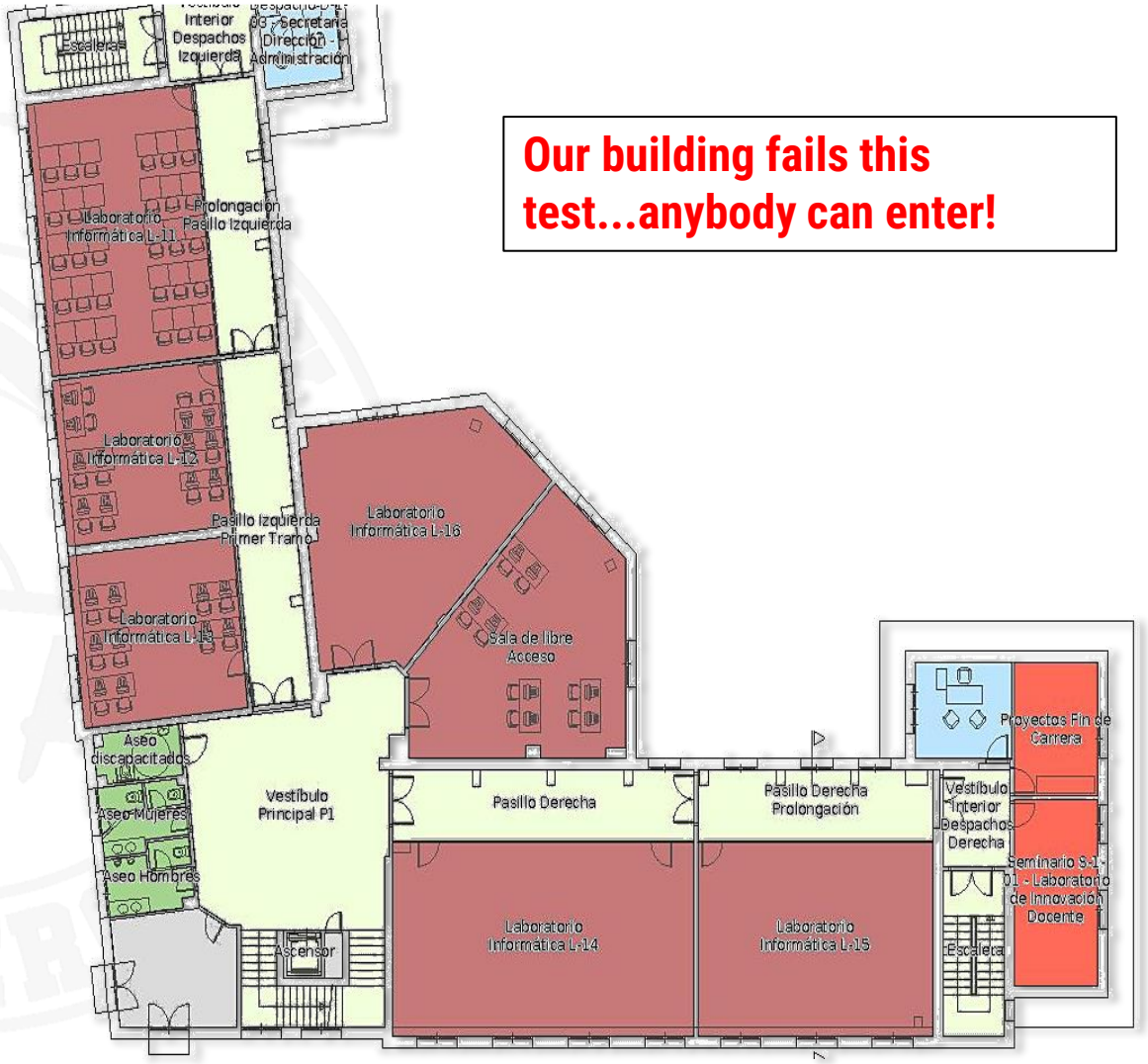
The main entrance of the building is on the ground floor, intersected by a double closure of iron gate and glass doors, behind which the janitor cabin is located.

Source: *Security diagnosis of information systems*. PFC Cód. DMKPC-0737. EUITIO (now EII) (***translated***)

Environment: Physical access

José Manuel
Redondo López

- **An inventory of all possible accesses must be performed**
- **All accesses to the building must be checked**
  - **So unauthorized users cannot easily enter in the building!**
  - Through **"typical" means**
    - Main access doors, service doors, garage gates...
  - **Or "alternative" means ☺**
    - Windows, skylights, ventilation or service ducts ...
- **The goal is proposing all necessary countermeasures necessary**
  - These include bars, locks, detectors, cameras...



Our building fails this test...anybody can enter!

Source: *GIS of the University of Oviedo*

Environment: Physical access

José Manuel
Redondo López

- **This example shows a physical security audit done to our school previous buildings many years ago**
- **Shows buildings, access controls, security measurements and their current operational state**
- **There are several deficiencies detected**
  - No secure locks / keys
  - Deactivated alarms!
  - …

✔ List the areas with access control

All **EUITIO** buildings (including the **Geological Lecture Hall** and the **Teaching Faculty**) have access control to the building through booths.

Inside the **Science Building**, access to laboratories, classrooms, offices and the secretariat is controlled using locks. The keys are stored by the person in charge of the office. The janitor keeps in the entrance booth a copy of all the keys of the building. This booth is closed by a key that only the janitor has.

✔ Examine the type of access control devices

Access to restricted areas is controlled by an ordinary lock. Access from the outside is controlled by bars and iron gates on the doors and in ground floor windows

✔ Examine the types of alarms.

All the alarms have been deactivated due to the high number of daily incidents caused by the students

✔ Determine the level of complexity of the access control devices

Locks and keys are not security ones. The doors that close the access to the restricted areas inside the buildings are not reinforced, nor are the frames.

The bars that protect the ground floor windows are fixed. However, some windows on the first floor are relatively easy to reach and have no means of deterring intrusions.

Source: *Security diagnosis of information systems*. PFC Cód. DMKPC-0737. EUITIO (***translated***)

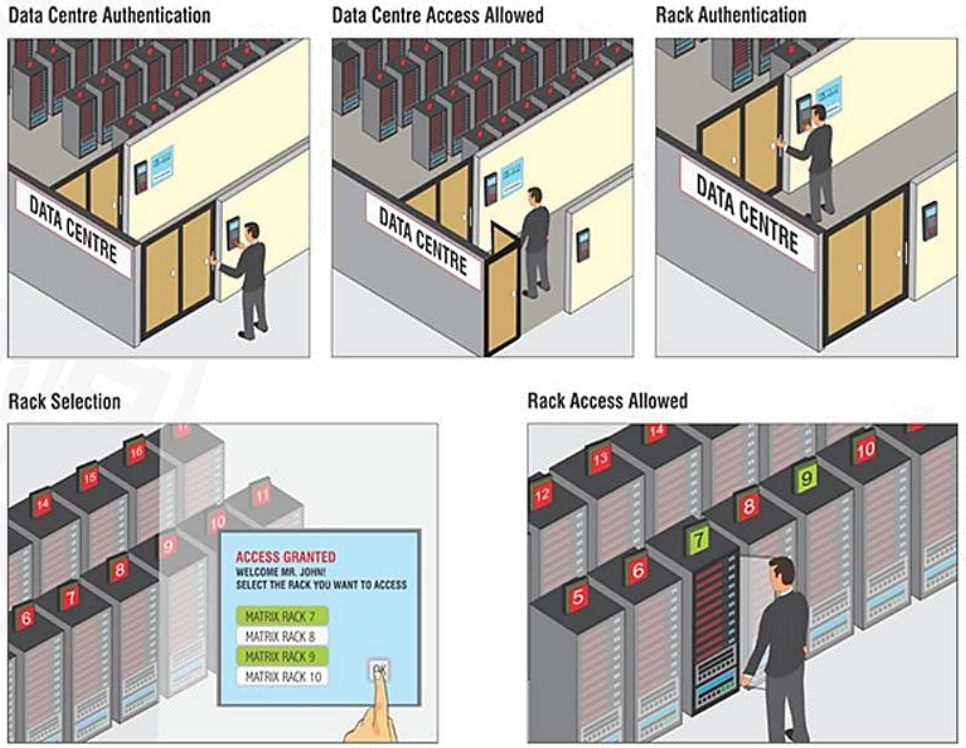
Environment: Access to the data center

José Manuel
Redondo López

- **Access to the data center rooms must be studied and protected**
  - Independently to the building access measures and policies
- **Accesses must be controlled to allow only authorized users**
  - Using additional controls, like electronic locks with access codes, security guards...
- **All access must be authorized and documented, following the established procedure**
  - Including non-technical personal (cleaning, maintenance…)
- **Data center rooms should be conveniently insulated by sufficiently solid walls and doors**
- **No other accesses must be possible**
  - Windows, ducts…

Our school data center…

- Is correctly insulated
- Only accessible through doors
- Computer racks have individual locked doors
- **But no access control is documented!**



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

Environment: External and environmental Threats

José Manuel
Redondo López

- **The design and construction of the building must minimize the effects of possible disasters that may occur in the environment**
- **Particular attention should be paid to this in problematic areas**
  - Seismic areas, flood zones, landslides, etc.
- **The building must have the corresponding fire detection and suffocation facilities**
  - In the data center, these should not be aggressive with the hardware
  - Must be based on CO2 or foam, not water streams or similar
  - Newer systems use micro-pulverized water
- **The data center must be prepared to face flooding**
  - Because of breakdowns in the building (pipes)
  - Or for atmospheric causes
  - Usually achieved with detectors, drainage pumps, false/raised floors ("suelo técnico" in Spanish)...

Our school…

- **No environmental measures were taken (but we are not in a problematic zone)**
- **No fire extinguishing equipment adapted to computers**
- **No measured to prevent flooding**

ENVIRONMENT: THESE THREATS ARE VERY REAL

José Manuel
Redondo López

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

Source: 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.

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

Environment: External and environmental Threats

José Manuel
Redondo López

- **All the mentioned measures make sense if the building zone has a potential risk for any of these problems**
  - If the location of the building is free of seismic activities, these can be relaxed
- **Spanish geological and mining institute publishes the risks associated with any zone**
- **Our school audit throws a satisfactory result in this matter**
  - We are not in a dangerous zone!

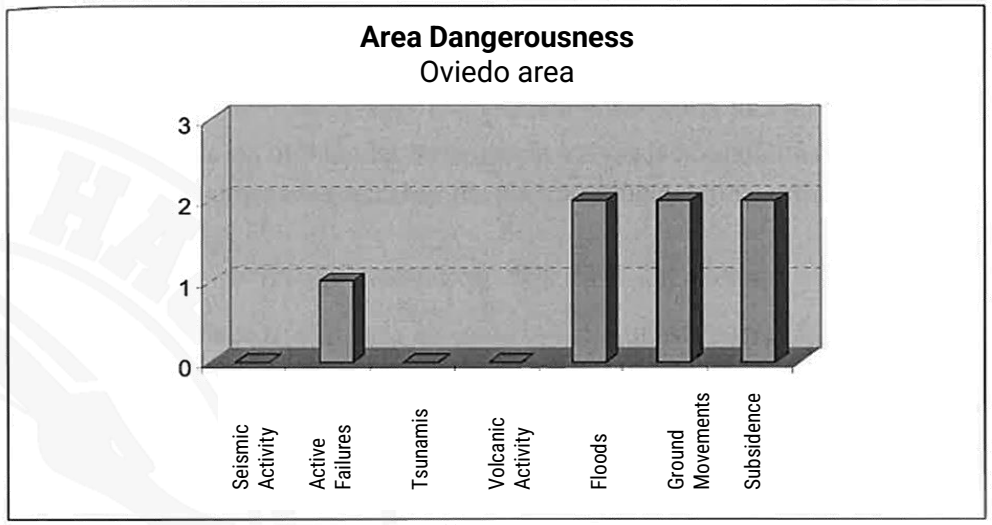


Figure 7 Source: Geological and Mining Institute of Spain

Regarding the impact of geological risk for the Oviedo area, the area where the facilities are located, and as shown in the attached graph on the above page, it presents a null risk of suffering disasters due to seismic activity, tsunamis and volcanic eruptions; a low risk of disasters due to active faults; and a moderate risk of disasters due to floods, ground movements or subsidence.

5.2.2 Natural Disasters

Guarantee that the facilities are protected against natural disasters: existence of evacuation systems in case of floods; protection against gales, earthquakes, lightning, etc.; roof and structure resistance; etc.

Source: *Security diagnosis of information systems*. PFC Cód. DMKPC-0737. EUITIO

Environment: Power supply

José Manuel
Redondo López

- **A stable and uninterrupted power supply is needed to ensure proper computer equipment operation on every situation**
  - This power supply must be adequately protected from surges
- **The electrical installation must be protected against attacks**
  - **Inside the building**: appropriate design of the installation by phase separation, ...
  - **Outside**: protected electrical connections
- **A power supply is safer the more redundancy it has**
  - On the power lines of the supplying company
  - Having power supply contracts with different companies with independent distribution systems
    - If the distribution network allows!
  - Installing an electric generators
  - Inside the building, installing multiple power circuits in the data center

ENVIRONMENT: POWER SUPPLY

José Manuel
Redondo López

- **Our school power line installation inside the building is adequate**
- **There is no information about periodicity of the maintenance operations**
- **There is no redundancy**
  - Only one company supply power, no redundant circuits…
  - Redundancy typically has a high cost
  - Information in computer systems must be critical to justify implementing it

5.2.3 Electrical System

Verifies that the supply of electrical power maintains its main characteristics: guarantee of supply and knowledge of the cable laying; supply stability and line controls; existence of UPS, generator sets; diversification of supply and emergency lighting; etc.

Positive aspects:

+ (I) The electrical supply of the Faculty of Sciences building is considered reliable in view of the supply loss statistics provided by **Hidrocantábrico** to the **Vice-Rectorate of Infrastructures**.

+ (I) The stability and voltage of the line are controlled in the Engine Room and the laboratories.

+ (I) All the areas of the buildings of the Faculty of Sciences, the Faculty of Geology and the Faculty of Teaching have emergency lighting, whose maintenance is the responsibility of the **Vice-rectorate of Infrastructures**, which has subcontracted it to the company **Eulen**. The lighting is checked regularly, as well as the verification of the status of the wiring (including lighting points, power outlets).

+ (N) The electrical supply cables are protected by rigid tubes in the downspouts inside the building, and by metal gutters outside.

Negative aspects:

- (I) RF100

Up-to-date electrical diagrams are not available.

- (I) RF101

It is unknown whether technical inspections of electrical systems are carried out, as well as their scope and frequency.

Source: *Security diagnosis of information systems*. PFC Cód. DMKPC-0737. EUITIO

Environment: Communications

José Manuel
Redondo López

- **The building and data center network design must be resilient against general outages**
- **Again, this can be achieved by equipment (routers, hubs, ...) and wiring redundancy**
- **Prevention measures of possible attacks from inside the building must also be considered**
  - Wiring and network equipment should not be accessible, but hidden and protected within false ceilings, technical floors, etc.
  - Network connectors and other equipment should not be left accessible unattended
    - An intruder could hook up a laptop or other type of surveillance equipment

Environment: Office security

José Manuel
Redondo López

- **Device visibility**
  - Radio communications, such as access control systems or hardware emitting RFID signals must be insulated if possible
  - Devices like Flipper Zero (https://flipperzero.one/) may hack them
- **Physical visibility**
  - User / employee work should not be observable from the outside of the building
  - The monitor and keyboard must be oriented in such a way that a "spy" cannot see its contents or what it is typed
  - It is a common way of guessing passwords / sensitive information

- **Security cameras**
  - Installed where valuable data is stored
  - They must be used in accordance with a policy established by the company
  - And in accordance with the current legislation (user data image rights protection, **ASLEPI**)

ENVIRONMENT: WORKING IN SAFE AREAS

José Manuel
Redondo López

- **In addition to computer systems, staff must be also protected**
  - Evacuation plans should be created for dangerous situations
  - Staff should be trained to use these security measures

5.2.6 Fire (Prevention)

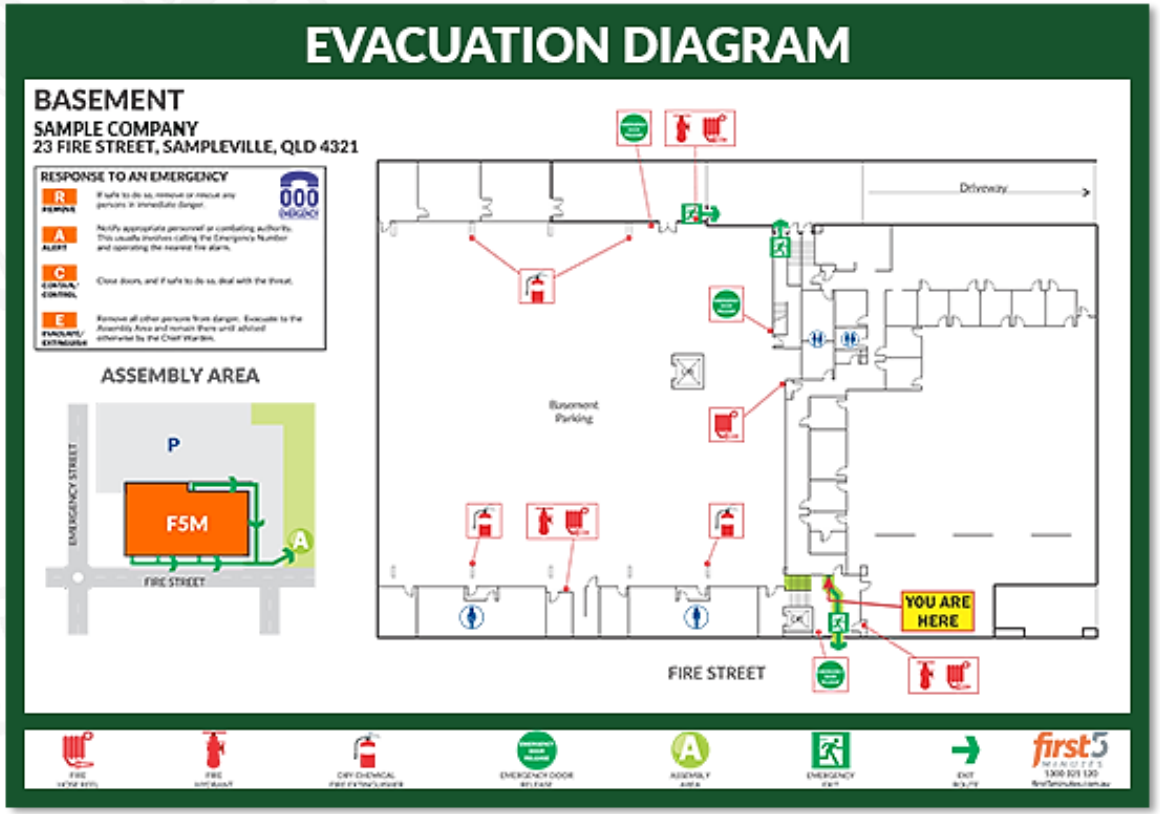
Analysis of the measures applied to prevent fires: existence of escape routes in the event of an accident; limited presence of combustible materials; fire resistant doors, walls and false ceiling; delivery of training courses and fire drills; electrical fire prevention, fire resistant designs; etc.

Positive aspects:

+ (I) The first aid material is stored in the janitor booth, in a suitably closed cabinet marked with a red cross painted white. It can be used at any time if necessary.

+ (I) They have strategically placed fire extinguishers and visible indicators that facilitate their location. The fire extinguishers are checked within the periods established by law, to guarantee their operation when they are necessary.

Source: *Security diagnosis of information systems*. PFC Cód. DMKPC-0737. EUITIO

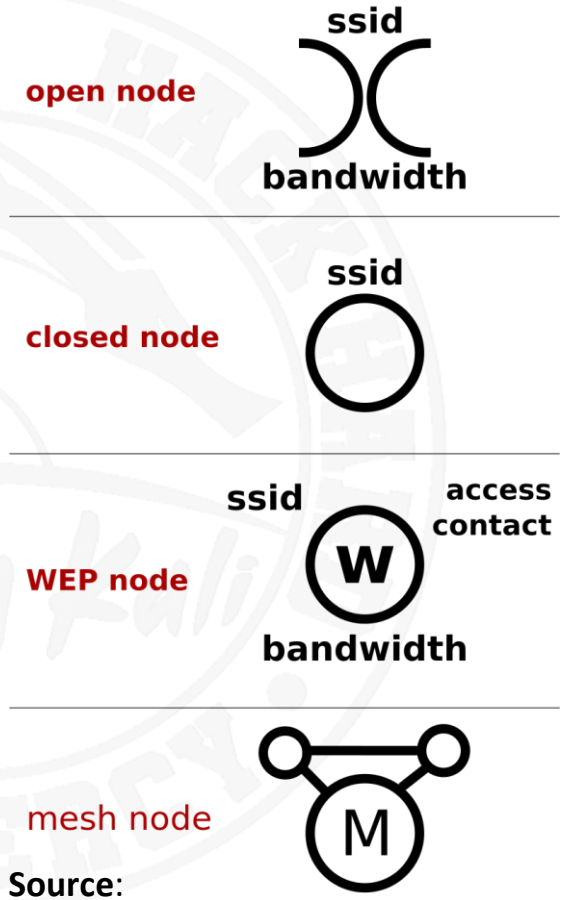


Source: https://www.first5minutes.com.au/services/fire/evacuation-diagrams

Environment: Warchalking

José Manuel
Redondo López

- **Consists on painting informative symbols on building walls**
- **These symbols form a language**
  - Provide information about Wi-Fi networks available outside the building
- **Finding these symbols in a building wall requires providing immediate countermeasures to avoid further problems**



Source:
https://hackingblogs.com/warchalking/

Source:
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/

< Go to Index

Source: zona-militar.com

PROTECTING THE EQUIPMENT

Security of the hardware

PHYSICAL SECURITY OF THE HARDWARE

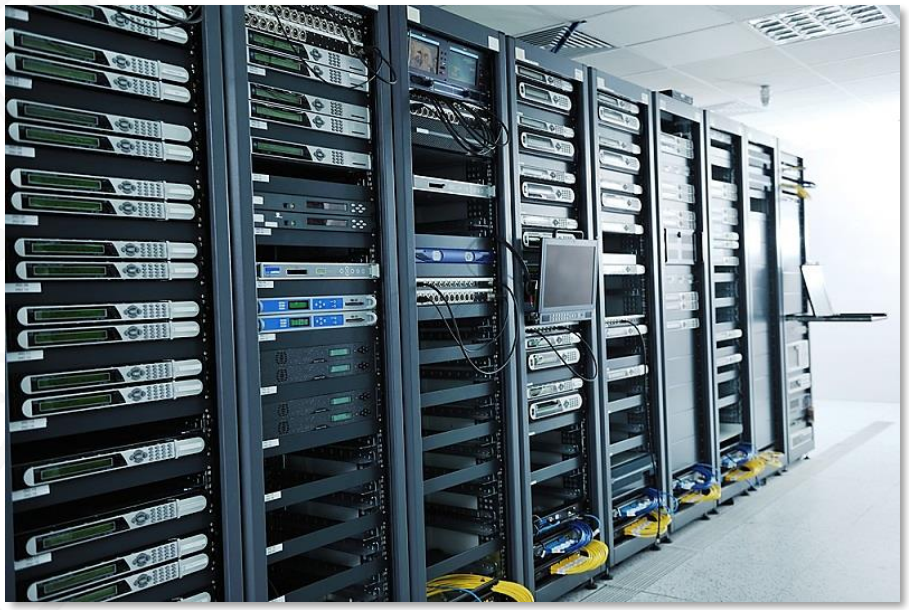
José Manuel
Redondo López

- **Environmental security measures must be complemented with measures related to the hardware itself**
  - Installation
  - Physical access to hardware
  - Hardware evacuation plan
  - Power supply
  - Heat treatment
  - Wiring arrangement
  - Backups
  - Redundancy
  - Disposal of hardware
  - Off-site security

PHYSICAL EQUIPMENT: EQUIPMENT INSTALLATION

José Manuel
Redondo López

- **To ensure that all equipment work as intended, there are a series of measures we can take**
  - **Careful planning** of the available space
  - **Quality of the equipment**: the cost-quality ratio will need to be evaluated when purchasing equipment according to company parameters
  - Installation in **cabinets or racks** is recommended to improve equipment protection
  - Racks must have space reserved for **UPSs systems**, as they are critical to the proper functioning in case of power outages



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

Physical equipment: Physical access to hardware

José Manuel
Redondo López

- **In addition to protect the datacenter, each user must only have physical access to authorized machines**
  - Network equipment, servers, PCs...
- **They must be "impossible" to open, to prevent theft or manipulation**
  - The rest of measures are invalid if anybody can open a computer or lockpick a rack to steal components

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

- **External devices able to record information must be disabled if determined by the company policy**
  - DVD-RW, USB devices…
  - This disables unauthorized extraction of information

Why preventing physical access? Hardware hacking

José Manuel
Redondo López

- **Letting unauthorized persons access our hardware can lead to a number of attacks**
- **One of the most famous is using a BadUSB device**
  - USB devices that emulate a keyboard with preprogramed keystrokes/commands
  - This way, anyone can run commands in name of the current user, but normally the user will not know it
  - The device itself disguises as other hardware device (USB cable, pendrive...) (https://www.redeszone.net/tutoriales/seguridad/rubber-ducky-ataque-dispositivo/)
  - Examples:
    - **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/)
  - They can be extremely cheap!: https://thehackerway.com/2017/07/10/badusb-ultra-low-cost/
  - The PlayStation® 3 Jailbreak was also an attack of this type:
    - https://es.wikipedia.org/wiki/PlayStation_Jailbreak

Physical equipment: Hardware evacuation plan

José Manuel Redondo López

- **Not only staff must be evacuated in case of emergency**
  - Hardware could also require evacuation too!
- **A hardware evacuation plan must also be established**
  - Detailing how and where critical hardware for the company operations can be moved in the shortest time
  - It must specify in what order the different devices will be evacuated
  - Depending on
    - The importance of their contained data
    - The processes they support

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

Physical equipment: Power supply

José Manuel
Redondo López

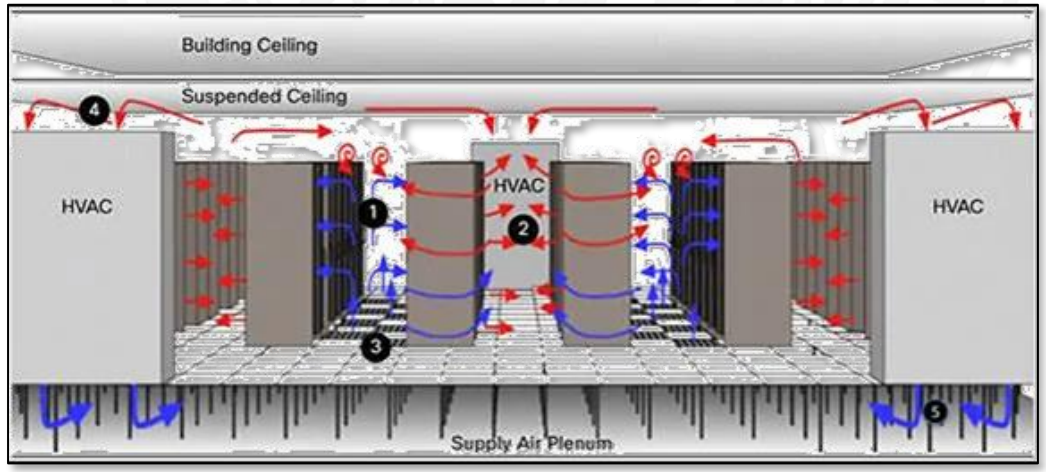
- **All hardware elements must be protected from surges or occasional power outages**
  - Via **UPS** (Uninterruptible Power Systems)
- **UPS planning should be appropriate**
  - A single large UPS
  - Smaller UPS, separated by team / department
- **The electrical installation must be properly studied and prepared**
  - With electrical protection devices, voltage limiters, etc.

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

Physical equipment: Heat treatment

José Manuel
Redondo López

- **All computer devices generate a considerable amount of heat**
  - Heat must be extracted from device surroundings
  - To avoid **overheating** damage or performance degradation (**throttling**)
- **Cooling management should start with an appropriate equipment layout**
  - **Cold corridors / hot corridors**
  - **Air conditioning** systems must be installed if we maintain many devices and other cooling solutions are not enough
  - In any case **proper ventilation of the premises is needed**
- **Providing redundancy to ventilation devices prevents failures**

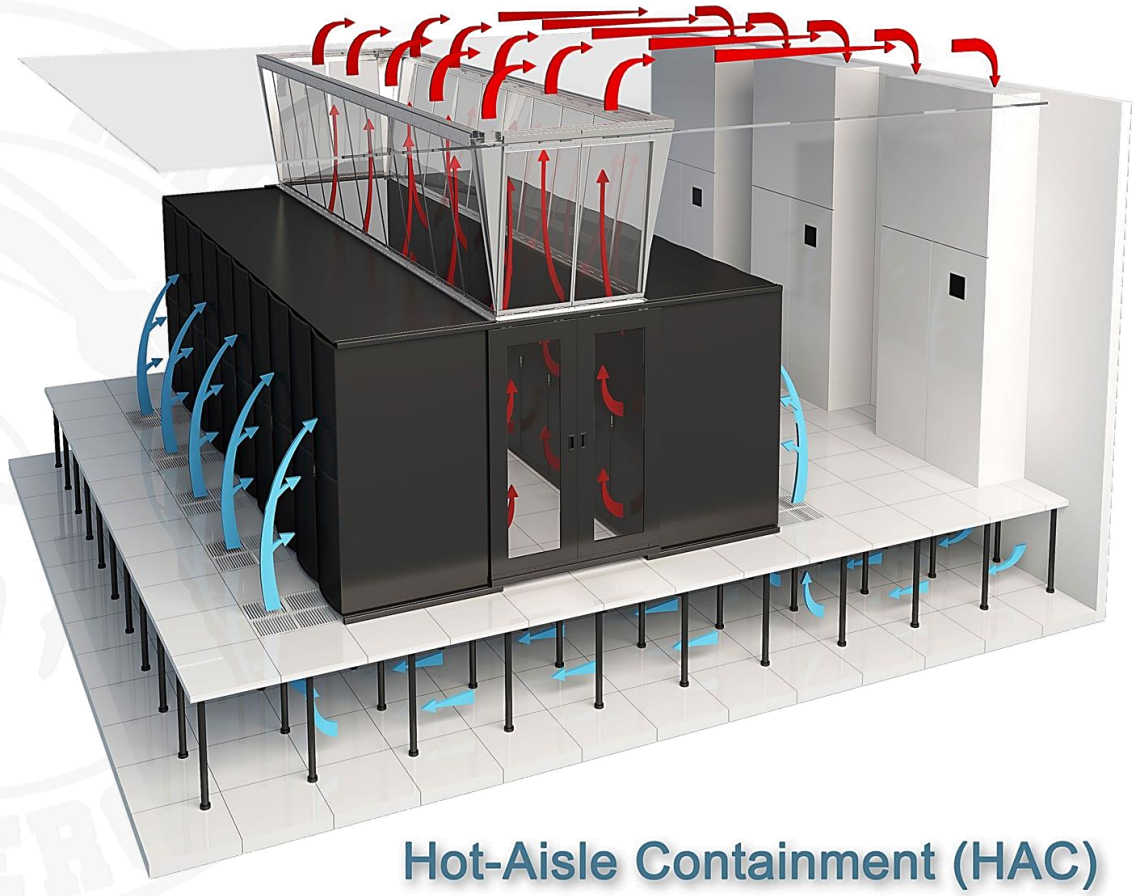


Source:
https://medium.com/@rajatghosh/mystery-of-data-center-hot-spots-994073b48fdb

Physical equipment: Heat treatment

José Manuel
Redondo López

- **Racks installation can accumulate heat**
  - Models with integrated ventilation and cooling systems could be necessary
- **Temperature monitoring systems are required, both in devices and cabinets**
  - They should be strategically installed in different points of the room
- **Usage of adequate monitoring software and alarms is also necessary**
  - E. g., Nagios software used by our school
- **Hardware can be configured to reduce its CPU frequency or increase fan speed in case of overheating**
  - Using different temperature thresholds



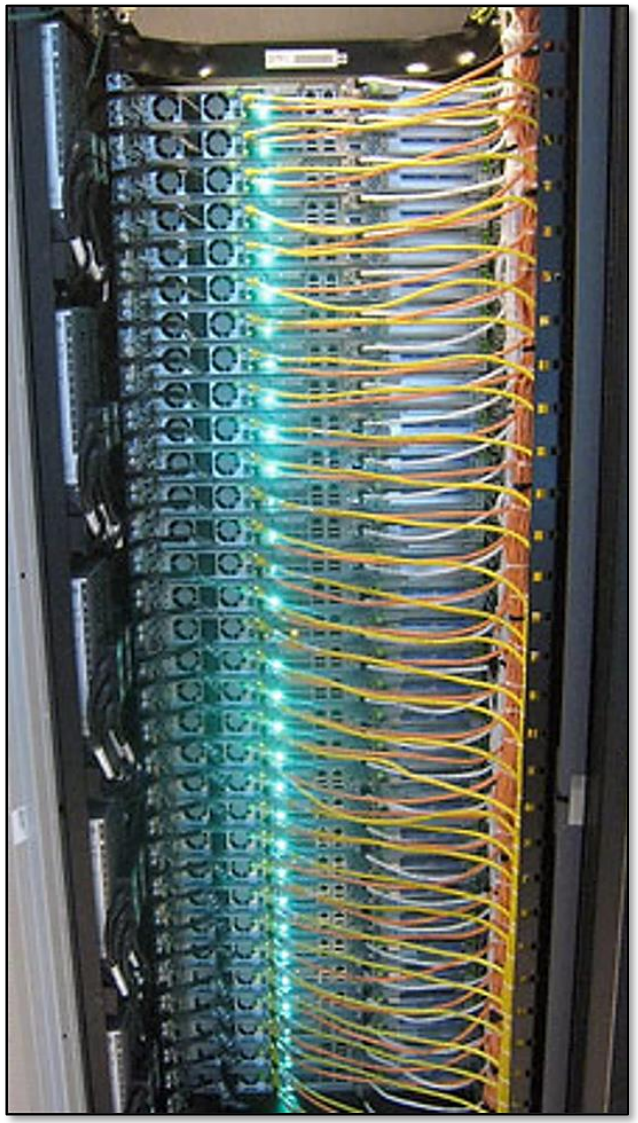
Hot-Aisle Containment (HAC)

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

Physical equipment: Wiring arrangement

José Manuel
Redondo López

- **Different types of wiring may coexist in an installation**
  - Electrical, "twisted pair" network, optical network, coaxial network, telephone wiring…
- **In general, all wiring that transmits data based on electrical impulses could be disrupted**
  - Normally, by electromagnetic fields generated by electrical conductions
- **Installation must be done in such a way that such interference is minimal**
  - "Shielding" electrical and / or data cables, installing them in different places…



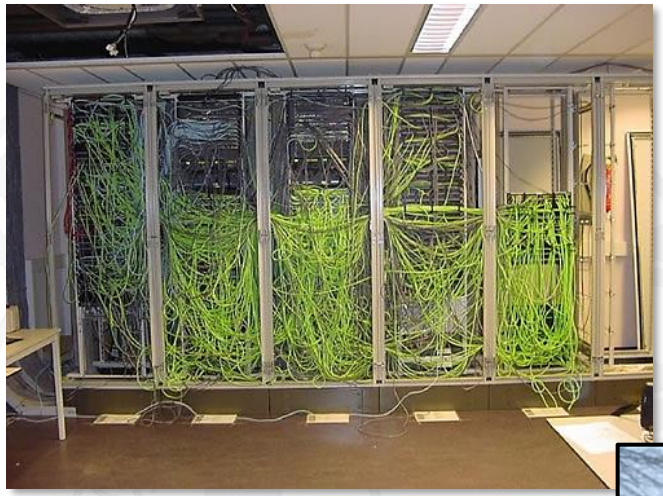
Source: https://www.cablinginstall.com/home/article/16481472/spectacular-data-center-cabling

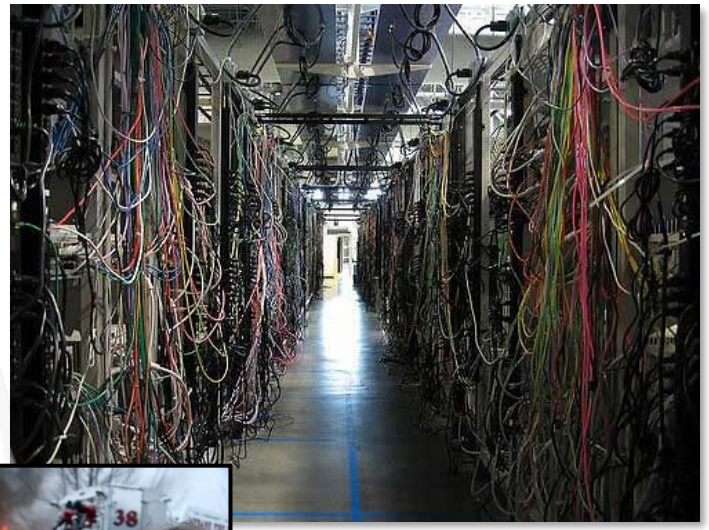
Physical equipment: Wiring arrangement

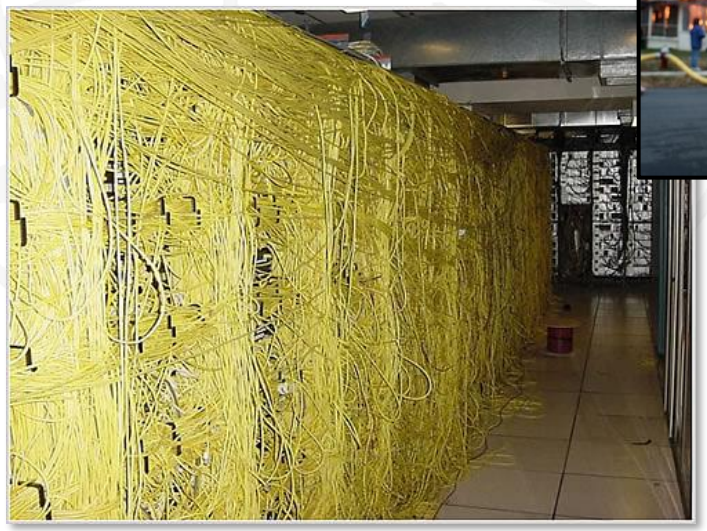
José Manuel
Redondo López

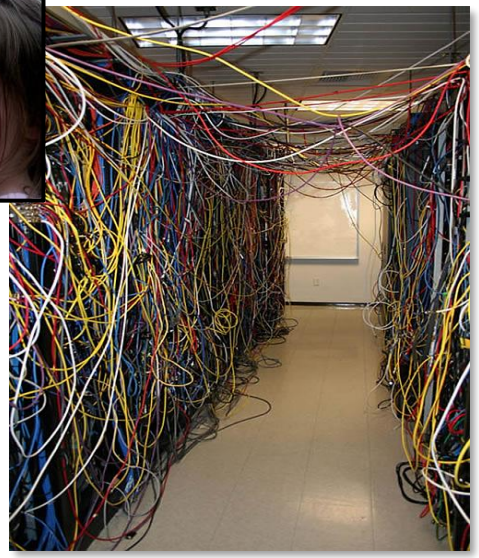
- **Unfortunately, it is common to find wiring following suboptimal layouts**
  - Even failure-prone ones!
- **This leads to**
  - Unplugging / breaking a cable causes partial system downtime
  - Insufficient documentation about cable layout, increasing repair / upgrade time

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









Physical equipment: Backups

José Manuel
Redondo López

- **A backup policy should be clearly established**
  - It determines **what** is copied, **when** it is copied, and **on which device**
  - The security of these copies should be also considered
- **Critical data should have multiple copies, stored properly**
  - In fire-proof enclosures
  - In different rooms of the building
  - In different buildings
  - Outsourcing the storage / realization
- **ASR covers backups in detail**

5.3.2 Backup Copies and Recovery Procedures

Positive aspects:

+ (I) School grant holders a Backup Copy of the EUITIO web server.

+ (N) Each computer in the laboratory has an image, stored on CD-ROM, which allows the system configuration to be recovered in a short time.

Negative aspects:

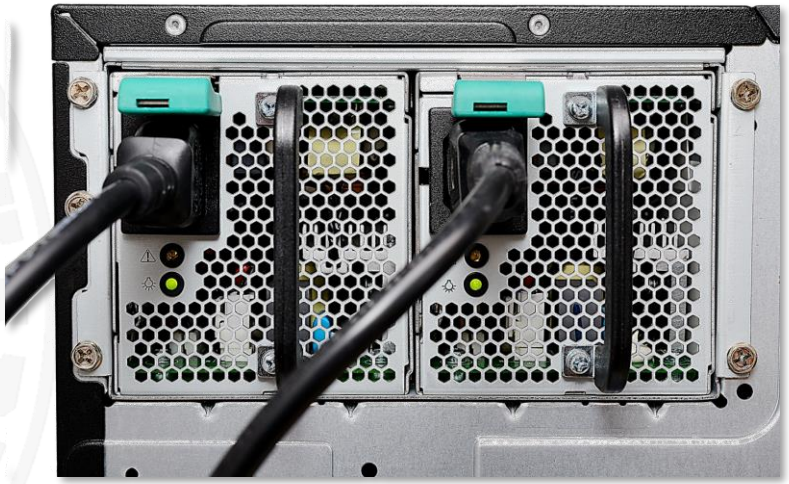
- (I) **RL100**
There is no policy for Backup and Recovery procedures.
- (I) **RL101**
There is no centralized place to store Backup Copies made.
- (I) **RL102**
There are no backup computers in case of equipment crash main.

Source: *Security diagnosis of information systems*. PFC Cód. DMKPC-0737. EUITIO

Physical equipment: Redundancy

José Manuel
Redondo López

- **Security to prevent equipment failure (fortuitous or not) usually requires equipment redundancy**
- **This redundancy can occur at different levels**
  - At the **machine level** (clusters, clouds, ...)
  - **Component redundancy** (CPU, memory, power supplies, ...)
    - It is interesting, in any case, that in addition to redundancy they have hot-swap features
  - At the **data level**, replicating the contents of the storage systems to others (preferably in another location)
  - As previously mentioned, also electrical, cooling, ... systems should be redundant



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

Physical equipment: Hardware disposal

José Manuel
Redondo López

- **Incredibly, a lot of useful information about a company can be found by inspecting around an organization's waste (dumpster diving)**
  - https://searchsecurity.techtarget.com/definition/dumpster-diving
- **This information could be key to perform attacks**
- **Therefore, an appropriate waste treatment policy should be established**
  - Destruction by appropriate means, management by a specialized external company, ...

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

Physical equipment: Off-site security

José Manuel
Redondo López

- **Staff must pay special attention to their portable devices because they are susceptible to being stolen / lost**
  - For example, in US airports more that 12,000 portable computers are lost per week
- **Moving one outside the company must be justified and authorized**
  - Its location must always be tracked
  - They should not contain valuable information, just work as terminals of the company's servers
    - If they must store information locally, it must be encrypted
  - Any user of the company portable devices must be aware of the company's security policies and the usage conditions
  - When returning to the company, all PCs should be checked for malware, additional installed software...
- **If bringing USB devices from the outside is possible, a device like AuthUSB Safedoor must be considered to prevent attacks based on USB devices**
  - https://www.authusb.net/safe-door/

< Go to Index

Source: zona-militar.com

PROTECTING PERSONNEL

Security and Human Resources

Personnel security

José Manuel
Redondo López

- **Personnel security policies aim to**
  - Avoid loss, damage or compromise assets as well as disruption of the activities of the organization
  - Prevent exposures to risks and steal of information or information processing resources: store resources in locked drawers and/or filing cabinets
- **As part of this security policy, the following topics should be considered**
  - **Do not leave functions and support equipment unattended,**
    - E. g.: if sensitive company information is being printed
  - Use **password protected screen savers** and **lock** the computer if unattended
- **Security controls must cover the entire workers life cycle**
  - From their selection interview to when they leave the organization

< Go to Index

Source: zona-militar.com

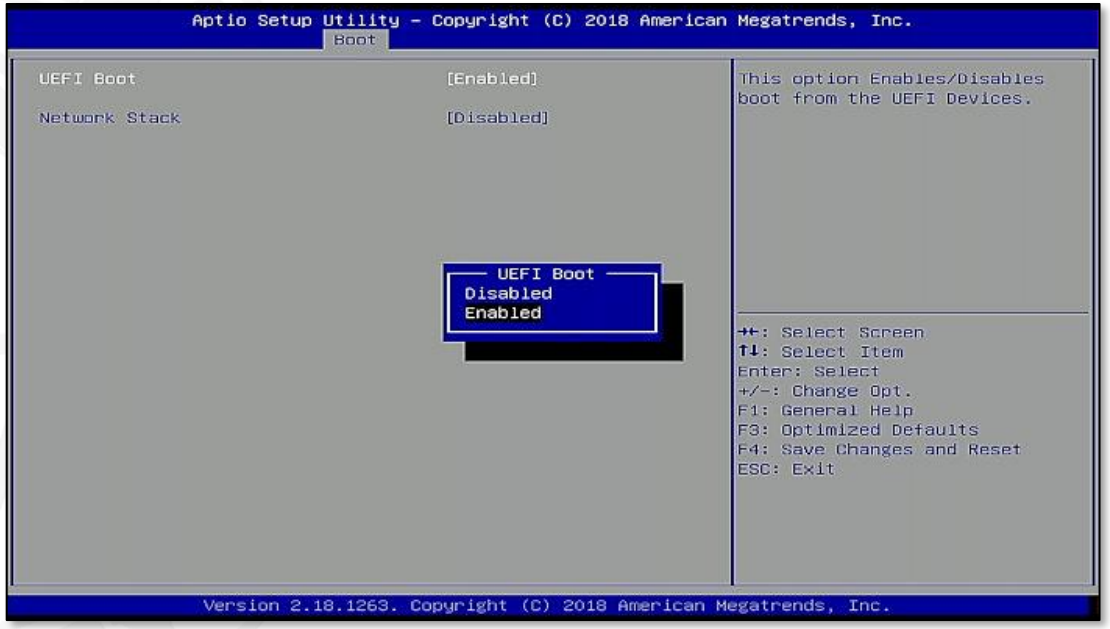
Pre-boot protection

Additional protection before booting the OS

PRE-BOOT SECURITY OPERATIONS

José Manuel
Redondo López

- **Before booting a computer, there are some operations that should be performed to ensure maximum security**
  - Enable SecureBoot (**Essential**)
  - Use a UEFI password to boot the system (**Suitable**)
  - Using UEFI mode (**Essential**)
  - Set a password to access the UEFI configuration (**Essential**)
  - Limit access to out-of-band access software, like **LOMs** (Lights-Out Management)
    - Seen later
  - Also limit access or disable **Wake-On-LAN** enabled network cards
    - To avoid machines to be put online by external agents



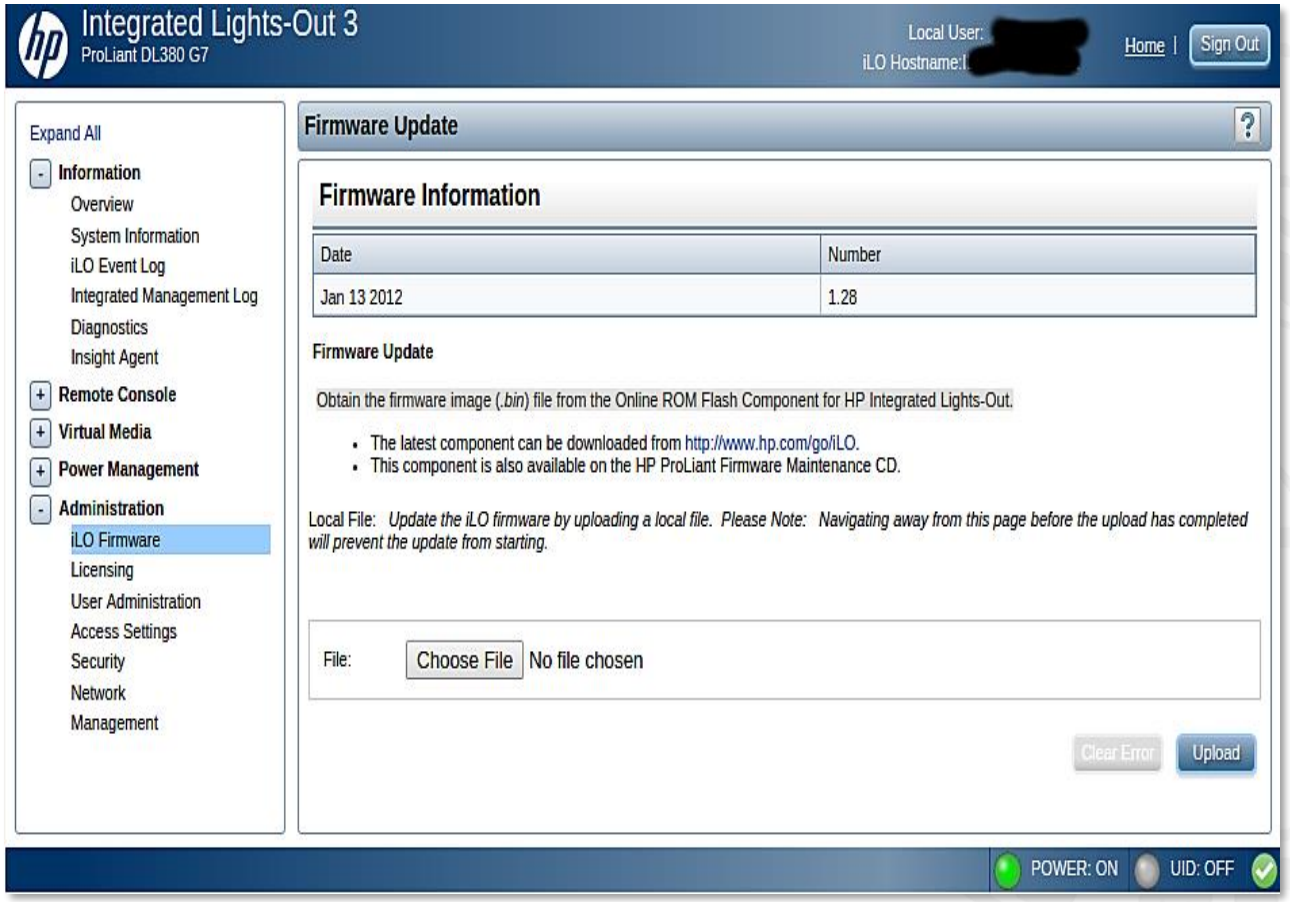
LOM SYSTEMS

José Manuel
Redondo López

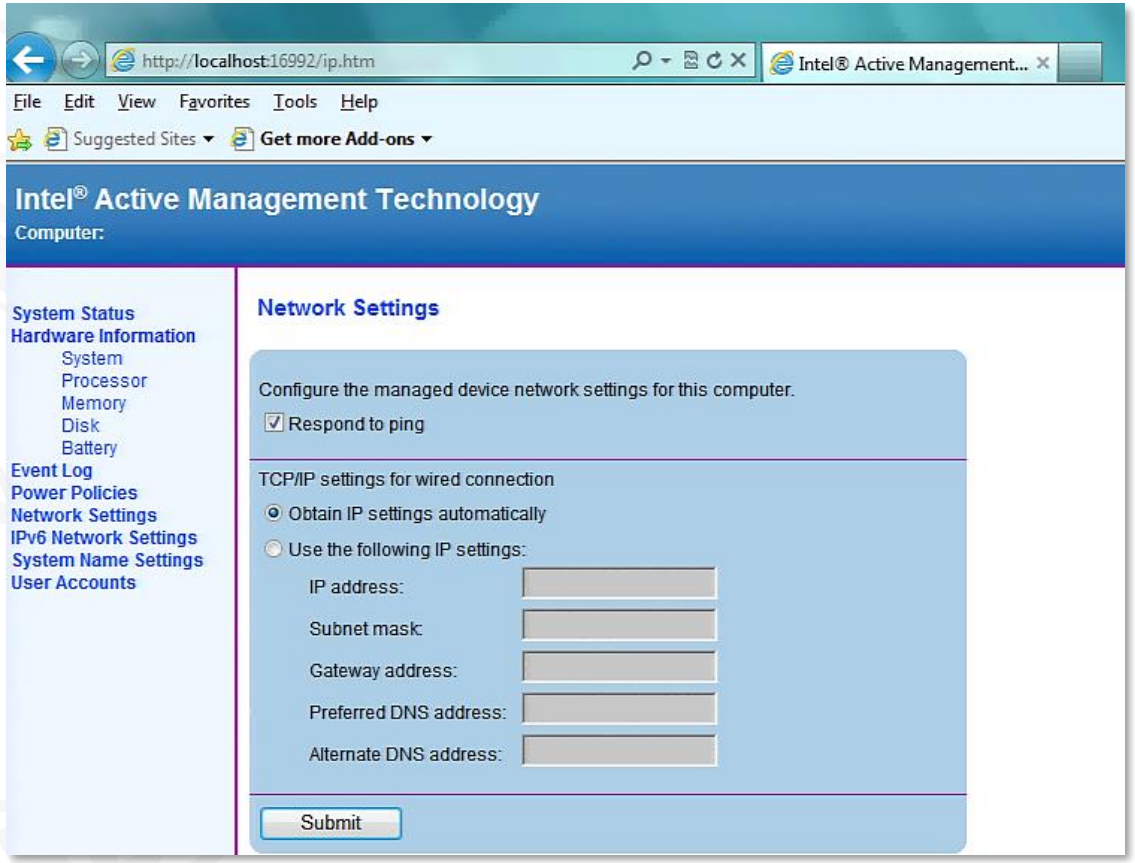
- **Allow remote computer management, even if powered off!**
  - Because of it, protecting its access is critical
- **Some LOMs require connecting to a particular network interface**
  - They can only be accessed through a specific one, that will be ideally used only for administration
- **It is important to consider if they exist**
  - Because they can be used to fraudulently access a server and unfold attacks **with no restrictions**
- **They sometimes present bugs that can compromise our server**
  - Therefore, they must be properly secured or deactivated if they are not to be used
- **Some popular LOMs are**
  - **Intel AMT** (integrated into numerous Intel Core iX and Xeon models)
    - 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

LOM SYSTEMS: HP ILO AND INTEL AMT

José Manuel
Redondo López



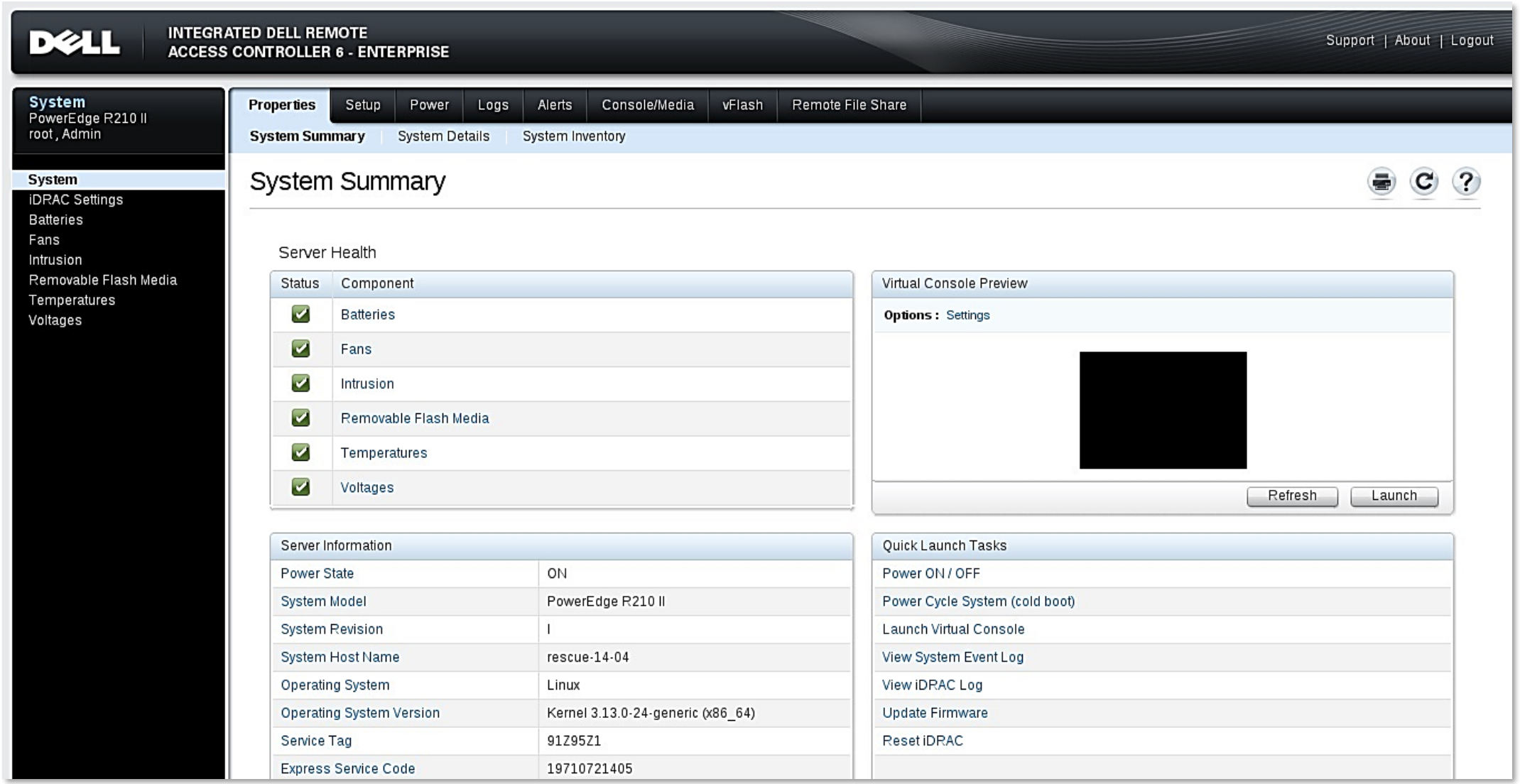
Source: https://serverfault.com/questions/658529/ilo-3-firmware-update-hp-proliant-dl380-g7



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

LOM SYSTEMS: DELL IDRAC

José Manuel
Redondo López



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

SELF-EVALUATION ACHIEVEMENT LIST: SEMINAR 2

José Manuel
Redondo López

Rank	Concept
	Understand the LOM concept and its potential problems
	Understand all the potential sources of physical security problems
	Know about common physical security terms: dumpster diving, war chalking...
	Be aware of the potential problems derived from not correctly disposing your hardware
	Understand how security policies must also cover company personnel
	Understand the potential security implications of taking equipment off-site
	Know all the possible sources of physical security problems related to the environment
	Know all the possible sources of physical security problems related to the equipment
	**Let's get physical**: Acquire a basic understanding of what physical security means and requires

SEMINAR 2
PHYSICAL SECURITY

Source: zona-militar.com