JESUÏTES El Clot
Escola del Clot

M011-SEGURIDAD INFORMÁTICA Y ALTA SEGURIDAD

UF1- Seguridad Fisica, lógica y legislación

ACTIVIDAD 4

Curs: 2018-19

CFGS: ASIX2

Alumne : Arnau Subirós Puigarnau

Data : 1-11-2018

Nom i Cognoms	Data
Arnau Subirós Puigarnau	**1-11-2018**

ACTIVIDAD 4 : Buscar los mecanismos que existen a nuestra disposición y clasificarlos en cada uno de los apartados que se indican en la tabla.

Generar un documento de trabajo completo, es decir textos y tablas + imágenes o esquemas complementarios que permitan comprender correctamente cada uno de los mecanismos que se clasifican en cada apartado enunciado en la tabla.

(Número de páginas mínimo 15.)

Mecanismos de Seguridad			
Física activa	Física pasiva	Lógica activa	Lógica pasiva

Nom i Cognoms | **Data**

Arnau Subirós Puigarnau | **1-11-2018**

INDICE

Nom i Cognoms	Data
Arnau Subirós Puigarnau	**1-11-2018**

1. ¿Qué significa seguridad activa y seguridad pasiva?

La Seguridad Integral está formada por tres medios que deben coordinarse a la perfección para conseguir su plena eficacia. Estos tres medios son:

- **Medios Humanos**: personal de seguridad pública o privada.
- **Medios Técnicos**: Pasivos (o físicos) y Activos (o electrónicos).
- **Medios Organizativos**: Protocolos, planes y normativa.

Medios Técnicos Pasivos o Seguridad Física.

La seguridad pasiva o seguridad física tiene que orientarse a la disuasión de cualquier amenaza o en caso de que ésta se produzca, debe retardar ésta para que no alcance su objetivo fácilmente y exista un margen de tiempo para que haya una alarma y la reacción correspondiente.
La seguridad física está integrada por un conjunto de medios pasivos como:

- Vallas o cercado.
- Barreras para vehículos.
- Puertas.
    - De Seguridad: nivel básico de protección.
    - Blindadas: nivel medio-alto de protección.
    - Acorazadas: con el máximo nivel protección, suelen instalarse en cámaras acorazadas y bancarias,
- en zonas donde hay que proteger objetos de gran valor o en áreas de considerable riesgo.
- Rejas y contraventanas.
- Cajas fuertes.
- Cámaras Acorazadas.

Nom i Cognoms	Data
Arnau Subirós Puigarnau	**1-11-2018**

Medios Técnicos Activos o Seguridad Electrónica.

La seguridad activa o seguridad electrónica tiene la función primordial de alertar, ya sea localmente o remotamente, de cualquier intento de violación de la seguridad física (rotura de ventanas o puertas, manipulación de una caja o intrusiones en zonas delimitadas con vallas o barreras).
Un sistema de seguridad electrónica está formado por distintos elementos relacionados a nivel de instalación y que han de coordinarse para ser efectivos.

- Alimentación.
- Detectores de presencia de uso interior o exterior (sensores).
- Controles de acceso.
- Señalizadores o Alarmas.

Los detectores de alarma son los encargados de iniciar la alarma en caso de observarse cualquier alteración en el estado de normalidad de una zona. En general los podemos agrupar en dos tipos:

- ❏ Sensores perimetrales o de penetración.
- ❏ Sensores volumétricos o espaciales.

Los sensores perimetrales son los más simples y suelen dedicarse a controlar aberturas (como las puertas y las ventanas) y siguen siendo muy efectivos para detectar cualquier rotura o intento de forzar una entrada.
Los sensores volumétricos suelen ser más sofisticados y su funcionamiento se basa en detectar movimientos de intrusos que hayan superado los sensores perimetrales instalados.
Podríamos clasificar de forma resumida los tipos de detectores de alarma según el tipos de alarma.

- Infrarrojo pasivo o PIR.
- Detector de ultrasonidos
- Contactos màgneticos ubicados en las puertas (normalmente produce muchas falsas alarmas por el viento y que el magnético tenga holgura y se mueva)
  - Lapa caja fuerte : Es un contacto magnético (más complejo destinado solo al uso de caja fuertes)
- Barreras (con infrarrojos)
- sensores de humo/calor/incendio
- sensores de gas
- detectores de rotura de cristal (ubicado como el nombre indica en ventanas o locales con un cristal para mostrar el interior
- sensores sísmicos (detecta la vibración)

Una vez detectada una intrusión o una amenaza por cualquiera de los sensores integrados en el sistema de seguridad electrónica, ha de producirse la alarma o aviso correspondiente, a fin de que se puedan tomar las medidas oportunas, notificar los hechos a FFCCSSEE

Nom i Cognoms	Data
Arnau Subirós Puigarnau	**1-11-2018**

(GC,PN,Mossos y Ertzaintza) según el Orden INT 316/2011 (ya que no se pasa aviso por un salto, hay unas normas que acatar , además hay que diferenciar los tipos de grados (1,2,3 o 4) según el tipo de establecimientos

- A distancia➢. Llamada telefónica➢. **Comunicación a una C.R.A. o Central Receptora de Alarmas** (por línea telefónica o radio).

- A la CRA según lo solicite el cliente, se pueden recibir las señales de alarma por varios medios (línea telefónica, GPRS TMC, GPRS Teltronic, GPRS Paradox,etc) vía radio...se puede tener 1 o varias líneas redundantes(para que no quede incomunicado)

- Especiales. Circuito cerrado de televisión (CCTV): con grabadora o cámaras digitales.

En la actualidad se suelen usar dos o más avisadores para aumentar el grado de seguridad y de fiabilidad de las alarmas, detectando intrusiones o accesos no autorizados con mayor exactitud.

La calidad de un sistema de seguridad no viene determinada sólo por tener la alarma más sofisticada y los mejores sensores. L**a eficacia de un sistema de seguridad se basa en la correcta coordinación de todos los elementos y al final siempre depende de la profesionalidad de la empresa que gestione su seguridad, y de la formación del personal responsable.**

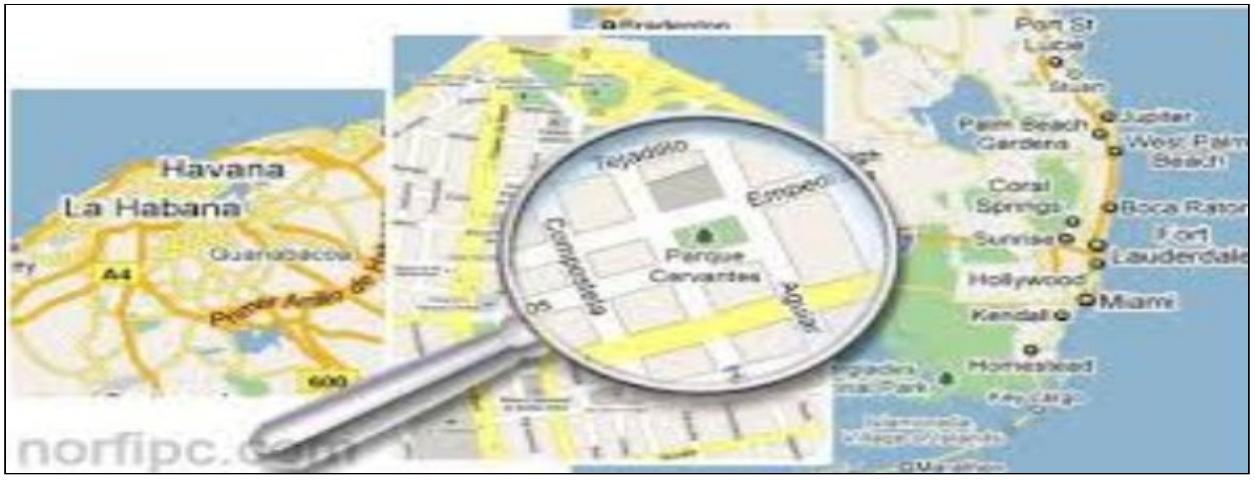
Nom i Cognoms	Data
Arnau Subirós Puigarnau	**1-11-2018**

2. Clasificación de seguridad

Se pueden hacer diversas clasificaciones de la seguridad informática en función de distintos criterios.
Según el activo a proteger, es decir, todos los recursos del sistema de información necesarios para el correcto funcionamiento de la actividad de la empresa, d**istinguiremos entre seguridad física y lógica**; en dependencia del momento preciso de actuación, **entre seguridad pasiva y activa**, según se actúe antes de producirse el percance, de tal manera que se eviten los daños en el sistema, o después del percance, minimizando los efectos ocasionados por el mismo.

2.1. Seguridad física

La seguridad física es aquella que trata de proteger el hardware (los equipos informáticos, el cableado …) de los posibles desastres naturales (terremotos, tifones …), de incendios, inundaciones, sobrecargas eléctricas, de robos .etc.



Nom i Cognoms **Data**

Arnau Subirós Puigarnau **1-11-2018**

A continuación vamos a enumerar las principales amenazas y los mecanismos para salvaguardarse de las mismas:

AMENAZAS	MECANISMOS DE DEFENSA
Incendios	• El mobiliario de los centros de cálculo debe ser ignífugo. • Evitar la localización del centro de procesamiento de datos cerca de zonas donde se manejen o almacenen sustancias inflamables o explosivos. • Deben existir sistemas anti-incendios, detectores de humo, rociadores de gas, extintores … para sofocar el incendio en el menor tiempo posible y así evitar que se propague ocasionando numerosas pérdidas materiales.
Inundaciones	• Evitar la ubicación de los centros de cálculo en las plantas bajas de los edificios para protegerse de la entrada de aguas superficiales. • Impermeabilizar las paredes y techos del CPD. Sellar las puertas para evitar la entrada de agua proveniente de las plantas superiores.
Robos	• Proteger los centros de cálculo mediante puertas con medidas biométricas, cámaras de seguridad, vigilantes jurados … ; con todas estas medidas pretendemos evitar la entrada de personal no autorizado.
Señales electromagnéticas	• Evitar la ubicación de los centros de cálculo próximos a lugares con gran radiación de señales electromagnéticas, pues pueden interferir en el correcto funcionamiento de los equipos informáticos y del cableado de red. • En caso de no poder evitar la ubicación en zonas con grandes emisiones de este tipo de señales deberemos proteger el centro frente de dichas emisiones mediante el uso de filtros o de cableado especial, o si es posible, utilizar fibra óptica, que no es sensible a este tipo de interferencias.
Apagones	• Para evitar los apagones colocaremos Sistemas de Alimentación Ininterrumpida, SAI, que proporcionan corriente eléctrica durante un periodo de tiempo suficiente.
Sobrecargas eléctricas	• Además de proporcionar alimentación, los SAI profesionales incorporan filtros para evitar picos de tensión, es decir, estabilizan la señal eléctrico.
Desastres naturales	• •Estando en continuo contacto con el Instituto Geográfico Nocional y la Agencia Estatal de Meteorología, organismos que informan sobre los movimientos sísmicos y meteorológicos en España.

Nom i Cognoms	Data
Arnau Subirós Puigarnau	1-11-2018

2.2. Seguridad lógica

La seguridad lógica complementa a la seguridad física, protegiendo el software de los equipos informáticos, es decir, las aplicaciones y los datos de usuario, de robos, de pérdida de datos, entrada de virus informáticos, modificaciones no autorizadas de los datos, ataques desde la red, etc.

A continuación vamos a enumerar las principales amenazas y los mecanismos para salvaguardarse de las mismas:

AMENAZAS	MECANISMOS DE DEFENSA
Robos	• **Cifrar la información almacenada en los soportes para que en caso de robo no sea legible.** • **Utilizar contraseñas para evitar el acceso a la información.** • **Sistemas biométricos (uso de huella dactilar, tarjetas identificadoras, caligrafía …).**
Pérdida de información	• **Realizar copias de seguridad para poder restaurar la información perdida.** • **Uso de sistemas tolerantes a fallos, elección del sistema de ficheros del sistema operativo adecuado.** • **Uso de conjunto de discos redundantes, protege contra la pérdida de datos y proporciona la recuperación de los datos en tiempo real.**
Pérdida de la integridad en la información	• **Uso de programas de chequeo del equipo, SiSoft Sandra 2000, TuneUp** • **Mediante la firma digital en el envío de información a través de mensajes enviados por la red.** • **Uso de la instrucción del sistema operativo Windows sfc (system file checker).**
Entrada de virus	• **Uso de antivirus, que evite que se infecten los equipos con programas malintencionados.**
Ataques desde la red	• **Firewall, autorizando y auditando las conexiones permitidas.** • **Programas de monitorización. • Servidores Proxys, autorizando y auditando las conexiones permitidas.**
Modificaciones no autorizadas	• **Uso de contraseñas que no permitan el acceso a la información.** • **Uso de listas de control de acceso.** • **Cifrar documentos.**

Nom i Cognoms	Data
Arnau Subirós Puigarnau	**1-11-2018**

2.3. Seguridad activa

La seguridad activa la podemos definir como el conjunto de medidas que previenen e intentan evitar los daños en los sistemas informáticos.

A continuación vamos a enumerar las principales amenazas y los mecanismos para salvaguardarse de las mismas:

AMENAZAS	MECANISMOS DE DEFENSA
Uso de contraseñas	• Previene el acceso a recursos por parte de personas no autorizadas.
Listas de control de acceso	• Previene el acceso a los ficheros por parte de personal no autorizado.
Encriptación	• Evita que personas sin autorización puedan interpretar la información.
Uso de software de seguridad informática	• Previene de virus informáticos y de entradas indeseadas al sistema informático.
Firmas y certificados digitales	• Permite comprobar la procedencia, autenticidad e integridad de los mensajes.
Sistemas de ficheros con tolerancia a fallos	• Previene fallos de integridad en caso de apagones de sincronización o comunicación.
Cuotas de disco	• Previene que ciertos usuarios hagan un uso indebido de la capacidad de disco.

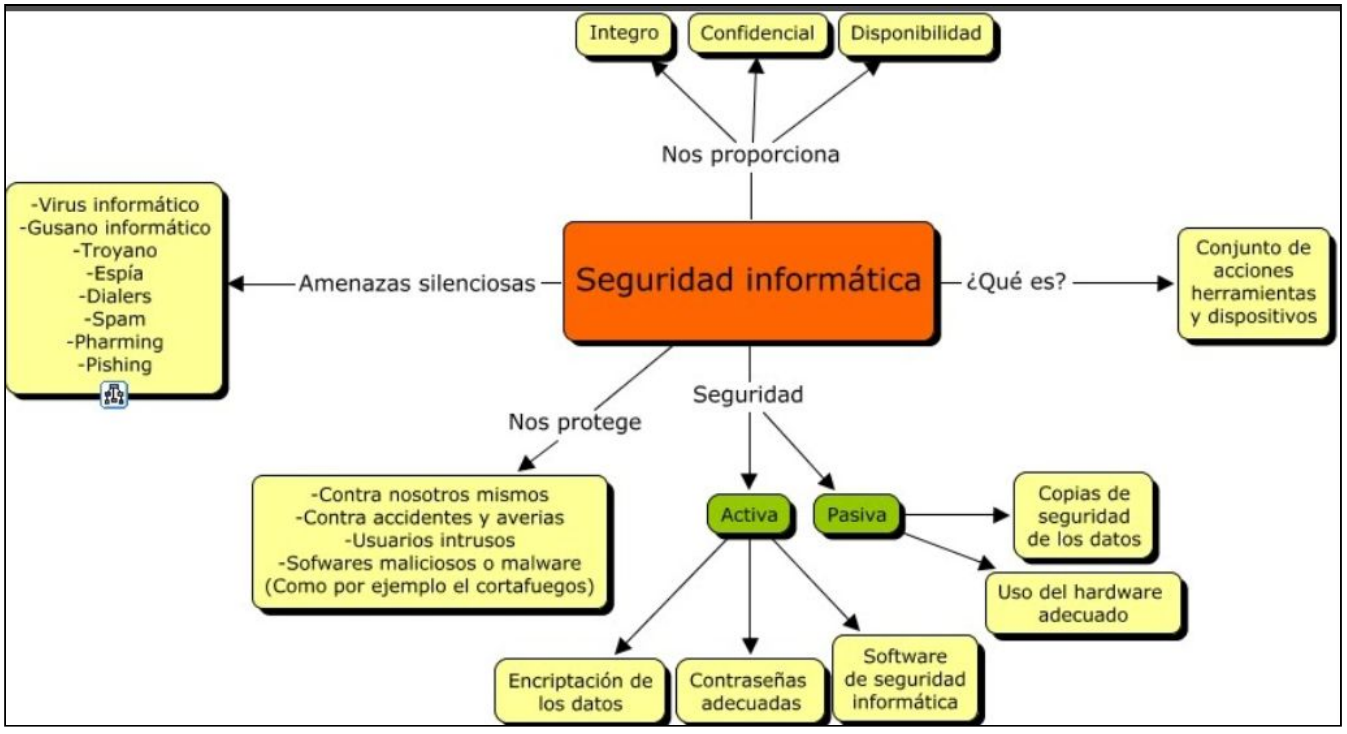
Nom i Cognoms	Data
Arnau Subirós Puigarnau	1-11-2018

2.4. Seguridad pasiva

La seguridad pasiva complementa a la seguridad activa y se encarga de minimizar los efectos que haya ocasionado algún percance.

A continuación vamos a enumerar las principales amenazas y los mecanismos para salvaguardarse de las mismas:

TÉCNICAS DE SEGURIDAD PASIVA	OBJETIVO
Conjunto de discos redundantes	• Podemos restaurar información que no es válida ni consistente.
SAI	• Una vez que la corriente se pierde las baterías del SAI se ponen en funcionamiento proporcionando la corriente necesaria para el correcto funcionamiento.
Realización de copias de seguridad	• A partir de las copias realizadas, podemos recuperar la información en caso de pérdida de datos.



Nom i Cognoms	Data
Arnau Subirós Puigarnau	**1-11-2018**

MECANISMOS DE SEGURIDAD

	SEGURIDAD FÍSICA ACTIVA	SEGURIDAD FÍSICA PASIVA	SEGURIDAD LÓGICA ACTIVA	SEGURIDAD LÓGICA PASIVA
1	Control de Acceso a personas	SAIS para la eliminación de picos de tensión	Sistema de huella dactilar	Cifrado en soportes externos
2	Instalación eléctrica	control de incendios	Contraseñas	Copias de seguridad
3	Programas de Monitorización	seguro (contra robos, inundaciones, fallos eléctricos..)	Tarjetas	Sistemas tolerantes a fallos (RAIDS)
4	Fijación de componentes	mecanismo de tolerancia a fallos (RAIDS)	Caligrafía	Discos redundantes
5	Control de temperatura	Renovación de equipos	Firma digital	Chequeo de discos
6	Humedad del ambiente	Equipos de sustitución	Antivirus	Conjunto de discos redundantes
7	Polvo	Sistemas Biométricos	Firewall autorizado	SAI
8	Agua	-	Auditoría automática	Realización de copias de seguridad
9	Protección contra incendios	-	Servidores Proxy	-
10	Mobiliario Ignífugo	-	Encriptación	-
11	Detectores de Humo	-	-	-
12	Rociadores de gas	-	Cifrado en la documentación	-
13	Extintores	-	Cursos de formación a trabajadores	-
14	Ubicación adecuada	-	-	-
15	Contacto con el Instituto Geográfico Nacional	-	-	-
16	Puertas de seguridad	-	-	-
17	Vigilantes jurados	-	-	-
18	Fibra óptica- evitar señales electromagnéticas	-	-	-

Nom i Cognoms **Data**

Arnau Subirós Puigarnau **1-11-2018**

3. Glossario (conceptos más importantes de la Seguridad Física Activa)

3.1. Control de Acceso

El espacio en el que se encuentre el hardware debe contar con distintas restricciones de acceso a las personas, en función del impacto que tendría sobre un sistema informático el robo o deterioro de dicho elemento hardware.Por tanto, parece obvio, que los servidores de una empresa deben situarse en los recintos más seguros de ésta, nunca en la entrada de la compañía o en áreas de paso o de descanso de la misma .

- Hay que tener en cuenta que no no sólo tenemos que considerar como agentes delictivos a las personas externas a nuestra organización, sino que hemos de considerar la posibilidad de tener saboteadores internos.
- Es realmente fácil copiar los datos de una compañía sin dejar huellas en el sistema y que es extraordinariamente fácil camuflar un pendrive o incluso un DVD.

Nom i Cognoms	Data
Arnau Subirós Puigarnau	**1-11-2018**

3.1.1. Tipos de Control de Acceso

El control de acceso se puede realizar de maneras diversas:

- Apertura y cierre de puertas controlado: permitir o negar el acceso basado en restricciones temporales en determinadas áreas o sectores de nuestra organización
- Servicio de vigilancia: se colocarán guardias o personal de seguridad en los lugares estratégicos para controlar la entrada y salida del personal de la empresa
- Formularios: que deberácumplimentar toda persona ajenaa la compañía previa identificación del personal visitante
- Teclados:Permiten introducir una contraseña que permite el acceso a los usuarios. Esta debe cambiarse con cierta frecuencia.
  - Básicos : una misma contraseña para todos
  - Complejos: contraseñas personalizadas
  - Interiores
  - Exteriores
- Uso de credenciales de identificación: por parte de todo el personal de una empresa,tanto propio como visitante, de manera que sea fácil reconocer:
  - Quien es cada persona
  - Su función en la compañía
  - Su nivel de seguridad
    - **Normal :** Para el personal permanente en la empresa
    - **Temporal** : Para el personal recién ingresado o con un contrato de servicio
    - **Contratista** : Para el personal ajeno a la empresa que tiene acceso a la misma (como mantenimiento, reponedores de màquinas exponedoras, etc..)
    - **Visitas** : Válido durante un periodo corto de tiempo

******En algunos casos se utiliza la credencial de seguridad para la apertura de puertas, quedando registrado en cada momento donde accede el personal de la compañía e incluso negando el paso a zonas no autorizadas.*******

El uso de credenciales implica que la persona se identifica por algo que posee : llave, tarjeta de identificación o tarjeta inteligente.Cada una debe poseer un **PIN único**.*La desventaja de este sistema de acceso es que las tarjetas pueden ser robadas, copiadas, etc, de manera que cualquier persona que las posee puede acceder.*

Nom i Cognoms **Data**

Arnau Subirós Puigarnau **1-11-2018**

3.1.2. Como se realiza dicho Control de Acceso

- **Seguridad Biométrica:** Permiten reconocer a seres humanos basándose en factores genéticos o en determinados rasgos de conducta.Permite la autenticación de personas utilizando tecnologías electrónicas capaces de discriminar y reconocer, con un margen de error nulo o muy próximo a cero, *la identidad dela persona que solicita el acceso a zonas restringidas*.
    - Basados en características físicas:Identifican una persona:iris, manos, facial, huellas dactilares
    - Hábitos o comportamiento:forma de andar, la firma,escritura manual.

Ejemplos basados en características físicas



CARACTERÍSTICAS FACIALES	OJO(iris)	HUELLAS DACTILARES	ESCRITURA Y FIRMA	VOZ
Fiabilidad	Muy alta	Muy alta	Media	Alta
Facilidad de uso	Media	Alta	Alta	Alta
Prevención de ataques	Muy alta	Alta	Media	Media
Aceptación	Media	Alta	Muy alta	Alta
Estabilidad	Alta	Alta	Baja	Media

Nom i Cognoms	Data
Arnau Subirós Puigarnau	1-11-2018

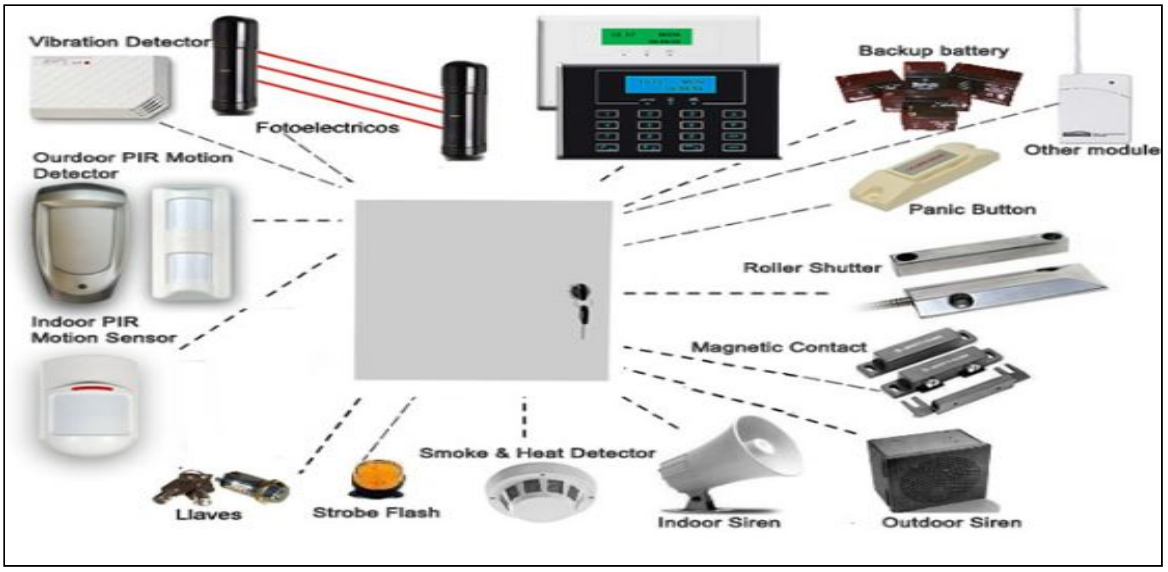
Ejemplos basados en hábitos de comportamiento

- **Alarma contra intrusión:** Básicamente una alarma consta de:
  - Módulo central : consola electrónica que controla el funcionamiento de todo el sistema de alarmas

  - Detectores: Sensores que detectan variaciones en el volumen, temperatura,…del espacio que abarcan

  - Sistema de cableado
  - Contactos magnéticos: conectados a puertas y ventanas para detectar la apertura de cualquiera de estos elemento
  - Avisadores telefónicos: Emiten señales acústicas o visuales
  - Pulsadores de emergencia: situados fuera de la vista de los posibles intrusos
  - Alarma: Suele ser un dispositivo sonoro que emite una fuerte señal cuando se detecta la presencia de un intruso en una zona de acceso restringido. Suele ir acompañada de otro dispositivo que emite señales luminosas.

Nom i Cognoms	Data
Arnau Subirós Puigarnau	1-11-2018



3.2. Sistema, componentes y herramientas que aseguran de forma activa nuestro hardware

3.2.1. Sistemas de alimentación interrumpida (SAI):Un SAI es un dispositivo electrónico que permite *proteger los equipos frente a los picos o caídas de tensión. De esta manera disponemos de una mayor estabilidad frente a los cambios que se producen en la red eléctrica*,elimina armónicos de la red y además nos proporciona una fuente de alimentación auxiliar en caso de cortes de luz. .Un SAI consta de unas baterías que almacenan energía de la red eléctrica y de unos alternadores que suministran energía eléctrica constante a los equipos informáticos. La energía que nos proporciona un SAI es bastante limitada. Puede durar desde media hora hasta un par de horas en función de la potencia del SAI y de la carga soportada.

Los problemas de la energía son:

- Cortes de energía o apagones
- Bajadas instantáneas de energía o microcortes
- Picos de tensión
- Bajadas de tensión sostenida
- Sobrevoltaje o subidas de tensión
- Ruido eléctrico
- Variaciones de frecuencia
- Transientes o micro picos

Nom i Cognoms	Data
Arnau Subirós Puigarnau	**1-11-2018**


3.2.2. Grupo Electrógeno : Un grupo electrógeno es una máquina que mueve un generador de electricidad a través de un motor de combustión interna.
Son comúnmente utilizados cuando hay déficit en la generación de energía eléctrica de algún lugar, o cuando son frecuentes los cortes en el suministro eléctrico

3.2.3. Regletas Protectoras: Son una solución barata al problema de las subidas de tensión. No son comparables a los SAI ya que no protegen de los cortes de suministro, pero pueden ser útiles para proteger nuestro hardware, por un módico precio, de la acción:

- De rayos
- Bajadas y subidas de tensión
- Ruido eléctrico

Nom i Cognoms	Data
Arnau Subirós Puigarnau	1-11-2018

3.2.4. Cableado: Es muy importante que las conexiones se realicen bien y con materiales en perfecto estado y de buena calidad para la seguridad de los equipos y de las personas.

- Se debe evitar el sobre calientamiento de los componentes, así como conectar demasiados dispositivos a una misma toma para evitar accidentes, cortocircuitos, …
- El tipo de enchufe debe tener suficiente potencia para resistir si conectamos varios equipos.
- No se debe utilizar cables diseñados para otro uso, ni realizar empalmes de cables que no cumplan con las normas de seguridad

3.2.5. Monitorización del hardware: Para comprobar el correcto funcionamiento del sistema y detección de errores en componentes físicos (velocidad de ventiladores, calor del microprocesador,…)
Se utilizan:

- Medios hardware : : *El polímetro* permite conocer las corrientes de un componente. A simple vista podemos ver: piezas en mal estado, mal instaladas,…

- Medios software: : Es el más utilizado, permite controlar errores y el rendimiento de los equipos. Podemos analizar el uso de la CPU memoria RAM disponible, consumida y libre, el uso del disco duro y su estado, la gráfica, los buse

Nom i Cognoms	Data
Arnau Subirós Puigarnau	1-11-2018

3.2.6. Fijación de los componentes físicos: Es muy importante fijar de forma correcta los componentes físicos de un ordenador.

- El propio equipo produce vibraciones que pueden afectar al hardware, disco duro, lector cd/DVD, ventilador, son ejemplos de elementos con partes móviles que transmiten esa energía al resto.
- Conexiones mal realizadas pueden deteriorar los componentes.
- Se puede producir ruido molesto.
- En zonas con mayor actividad sísmica es aconsejable utilizar armarios especiales o encajarlos en zócalos atornillados sobre soportes de goma que absorben las vibraciones

3.3. Control de Tempertura

El funcionamiento idóneo de los equipos informáticos se produce cuando estamos trabajando en un rango de temperaturas comprendidas entre los 15ºC y los 25ºC,aunque trabajan sin dificultad entre los 10ºC y los 32ºC

3.3.1. Terminales de trabajo:Están siendo usados la mayor parte del tiempo por el personal encargados de ellos

3.3.2. Servidores: No requieren presencia humana constante. En los centros de cálculo (Data Center) suelen encontrarse muchos de ellos apilados en racks

- Todos esos servidores funcionando al mismo tiempo 24 horas al día, 365 días al año generan una gran cantidad de energía calorífica que tenemos que disipar de alguna manera, por tanto hemos de tener en cuenta que hemos de instalar un sistema para mantener una temperatura constante en estos datacenter.

- Es importante que el aire pueda circular libremente por todas las zonas del data center y deberemos evitar que la corriente fría saliente del equipo de refrigeración entre directamente en un servidor.

Nom i Cognoms	Data
Arnau Subirós Puigarnau	**1-11-2018**

3.4. Protección contra Incendios

El fuego es una de las principales amenazas contra la seguridad:

- Los incendios son causados por el uso inadecuado de combustibles, fallo de instalaciones eléctricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas.
- El problema que causa un incendio no es únicamente el fuego,hay materiales que se queman sin llama pero provocan mucho calor que deteriora gravemente circuitos y soportes. El humo también ensucia y puede dañar el hardware.
- Los sistemas antifuego causan casi el mismo daño que el propio fuego.
- La protección contra incendios se lleva a cabo con medidas de seguridad pasiva y medidas de seguridad activa

3.4.1. Factores para reducir los riesgos de incendio

- El local no debe estar cercano a áreas donde procesen, fabriquen o almacenen materiales inflamables, explosivos, gases tóxicos o sustancias radioactivas.
- Paredes y suelos de material incombustible y no inflamable.
- Debe construirse un falso suelo instalado sobre el suelo real, con materiales incombustibles y resistentes al fuego.
- No se debe permitir fumar.
- Techos y suelos impermeables.
- Deben existir extintores manuales y/o automáticos (rociadores**)**

3.4.2. Detectores de incendio

- Son dispositivos que se instalan en el techo o en la parte más alta de los muros de las habitaciones
- Se evitan las esquinas pues es donde más tarde llega el humo.
- Hay que instalar tantos puntos de detección de humo como posibles focos de riesgo de incendios.
- Hay que tener en cuenta que el detector convencional detecta el humo a una distancia no superior a seis o siete metros
- Todos están enlazados a una central de alarmas que mostrará cual es el que se ha activado

Nom i Cognoms	Data
Arnau Subirós Puigarnau	**1-11-2018**

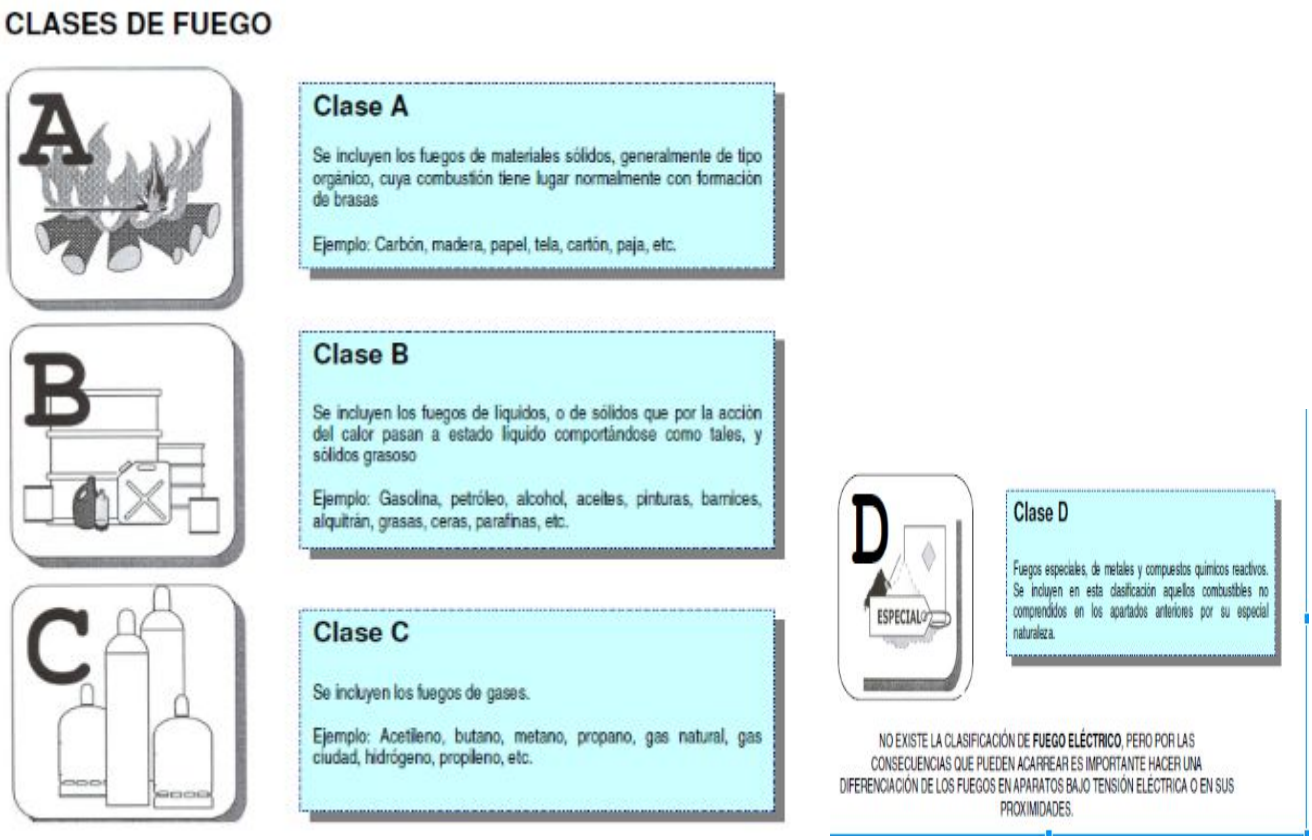
- Tipos de detección

  Cuando el detector percibe aumento considerable de temperatura, presencia de humo o partículas de combustión en el aire, se activa la alarma contra incendios

  - ❏ Sistemas de detección de humo
  - ❏ Sistemas de detección de llamas
  - ❏ Sistemas de detección de calor

- Clases de fuego

  - Clase A :fuegos de material sólido (tipo orgánico)
  - Clase B:fuegos líquidos o sólido grasoso
  - Clase C: fuego de gases
  - Clase D: fuegos especiales de metales y compuestos químicos reactivos



Nom i Cognoms	Data
Arnau Subirós Puigarnau	1-11-2018

- Agentes extintores

CLASE DE FUEGO (UNE 23.010)	AGENTE EXTINTOR							
	AGUA CHORRO (2)	AGUA PULVERIZADA (2)	ESPUMA FÍSICA(2)	POLVO ABC	POLVO BC	POLVO ESPECÍFICO METALES	DIÓXIDO DE CARBONO	SUSTITUTOS DE LOS HALOGENOS
A SOLIDOS	ADECUADO	EXCELENTE	ADECUADO	ADECUADO			ACEPTABLE	ACEPTABLE
B LIQUIDOS		ACEPTABLE	ADECUADO	ADECUADO	EXCELENTE		ACEPTABLE	ADECUADO
C GASES				ADECUADO	ADECUADO			
D METALES ESPECIALES						ADECUADO		

APLICACIONES DE LOS AGENTES EXTINTORES					
		APLICACIONES	VENTAJAS	INCONVENIENTES	PELIGROS
AGUA	CHORRO	-Fuegos con brasa -Refrigeración a larga distancia	-Gran alcance	-Dispersión del incendio -Poca penetración -Daños adicionales	-Fuego de equipos en presencia de tensión eléctrica(con agua pulverizada el peligro es menor) -Fuego en metales
	PULVERIZADA	-Fuego con brasa	Gran penetración en fuegos con brasas	-Poco alcance	
ESPUMA		-Fuegos con brasa -Fuegos de líquidos inflamables	-Efecto acumulable a partir de la densidad critica de aplicación	-Posibilidad de descomposición del espumógeno -Posibilidad de reignición por su bajo poder de refrigeración.	-Fuegos de metales -Fuegos de equipos bajo tensión eléctrica.
POLVO	POLIVALENTE (ABC)	-Fuegos con brasa -Fuegos de líquidos inflamables -Fuegos combustibles gaseosos o líquidos bajo presión -Fuegos de equipos en presencia de tensión eléctrica	-Alta eficacia	-Pueden originar daños en maquinaria o equipos delicados. -Posibilidad de reignición por su bajo poder de refrigeración.	-Fuegos con altas tensiones.

Nom i Cognoms **Data**

Arnau Subirós Puigarnau **1-11-2018**

	QUÍMICO SECO (BC)	-Fuegos de líquidos inflamables. -Fuegos combustibles gaseosos o líquidos bajo presión. -Fuegos de equipos en presencia de tensión eléctrica	-Alta eficacia		-Fuegos con altas tensiones eléctricas
	ESPECIAL(D)	-Fuegos en metales			-Suelen ser específicos para concretos de metales
DIÓXIDO DE CARBONO		-Fuegos de líquidos inflamables y combustibles gaseosos confinados o de pequeño tamaño. -Fuegos en presencia de tensión eléctrica.	-No dejan residuos	-Baja eficacia -Puede originar quemaduras por baja temperatura en la descarga.	-Disminución del % de oxigeno. -Asfixiante
SUSTITUTOS DE LOS HALONES		-Fuegos de líquidos inflamables- -Fuegos de combustibles gaseosos o líquidos bajo presión. -Fuegos en presencia de tensión eléctrica.	-No dejan residuos	-No muy eficaz frente a fuegos con brasa	-Corrosiones -Tóxicos a concentraciones elevadas.

3.4.3. Barreras

Instalación de barreras contra la propagación del fuego como barreras murales

3.4.4. Puertas y compuertas cortafuegos (normas UNE-EN-1634 yUNE-EN-1366)

La utilización de puertas y compuertas cortafuegos está cada vez más extendida, aunque aún no es obligatorio su uso.Hay de varios tipos y se

Nom i Cognoms	Data
Arnau Subirós Puigarnau	**1-11-2018**

clasifican en DF30, DF40 en función de la cantidad de minutos que resisten sin quemarse

3.4.5. Vías de evacuación de personas con su señalización correspondiente

Las vías de evacuación y las salidas de emergencia para casos de incendios deberán estar debidamente señalizadas y constarán en el plan de emergencia de la organización.

- Normas europeas en señalización contra incendios y vías de evacuación:
  - UNE 23033-81
  - UNE 23034-88
  - UNE 23-035-95

Nom i Cognoms	Data
Arnau Subirós Puigarnau	**1-11-2018**

3.4.6. Sistemas de desplazamiento de oxígeno

Reduce la concentración de oxígeno impidiendo la combustión de los equipos

- El agua es uno de los enemigos naturales de nuestro sistema informático y por muy eficaz que sea contra el fuego, no nos sirve de mucho apagar un incendio en un CPD si hemos inundado el sitio y mojado todos los equipos.
- Alguno de estos sistemas utilizan gases inertes como el halón para la extinción de equipos. En cualquier caso, son absolutamente nocivos para el personal humano y por tanto deberemos evacuar a todo el personal una vez se activa el sistema de extinción de incendios hasta que se recupera la normalidad en el CPD.

3.5. Mecanismos de Tolerancia a Fallos

Es la capacidad de los sistemas de seguir funcionando a pesar de la avería de alguno de sus componentes.

Estos mecanismos no se aplican normalmente a equipos de usuario final, sino a aquellos de los que se espera un funcionamiento continuo y sin fallos.

- **Redundancia** :Se consigue duplicando componentes por lo que conlleva una alto coste económico.
  La redundancia puede ser:
  - ❏ Estática : Los componentes duplicados siempre están activos y funcionando
  - ❏ Dinámica : El componente redundante detecta el fallo y comienza a funcionar.

Es normal encontrar sistemas con redundancia en:

3.5.1. Discos duros:

Se usan **RAID** (grupo redundante de discos independientes).Son varios discos físicamente independientes pero que trabajan como un solo disco a nivel lógico. Los datos se copian en los distintos discos

3.5.2. Fuentes de alimentación

Es normal encontrar al menos dos fuentes de alimentación en servidores.

Nom i Cognoms	Data
Arnau Subirós Puigarnau	**1-11-2018**

3.5.3. Tarjetas de red:

También es común encontrar un mínimo de dos. Trabajan a la vez para dar respuesta a picos de peticiones en los servidores. Si alguna falla, el resto sigue con su función.

3.6. Centro de Proceso de Datos(C.P.D).

Se denomina Centro de Proceso de Datos (CPD) a aquellas instalaciones donde se encuentran todos los recursos necesarios para el procesamiento de datos de una compañía (Data Center) .
Las instalaciones consisten en habitaciones debidamente acondicionadas donde se instalan los servidores y los núcleos de las redes de comunicaciones.Casi todas las compañías de tamaño medio o grande dispone de un CPD de mayor o menor tamaño y con diferentes parámetros de seguridad , incluso las grandes compañías internacionales disponen de dos o más CPD situados en localizaciones geográficamente distantes para ser utilizadas en parte o en su totalidad como respaldo o backup del CPD principal.

La misión del CPD es garantizar:

- La continuidad y disponibilidad del servicio a clientes,proveedores, empleados, ciudadanos y empresas colaboradoras.
- La integridad y confidencialidad de la información.

3.6.1. Requisítos generales de un C.P.D.

- ❏ Disponibilidad y monitorización 24x7x365: es decir 24 horas, 7 días a la semana, 365 días al año
- ❏ Fiabilidad infalible (5 nueves): es decir 99,999% de disponibilidad o lo que es lo mismo 1 hora de NO disponibilidad al año
- ❏ Seguridad, redundancia y diversificación: Almacenaje exterior de datos, tomas eléctricas totalmente independientes del servicio de red, servicio de telecomunicaciones duplicados, equilibrio de carga SAI,grupos electrógenos, control de acceso…
- ❏ Control ambiental y prevención de incendios: proporcionar una temperatura y humedad relativa adecuada a las características de los equipos y control de incendios mediante sistemas no nocivos para sistemas eléctricos y equipos de la sala.
- ❏ Acceso a Internet y conectividad a redes WAN para conectividad a Internet: en muchos casos con líneas salientes a más de una ubicación para prevenir cortes de suministro

Nom i Cognoms	Data
Arnau Subirós Puigarnau	**1-11-2018**

3.6.2. Requisítos de infraestructura de un C.P.D.

- ❏ Falsos techos y suelo técnico con placas de fibra de vidrio
- ❏ Cableado estructurado. Todos los cables tendidos bajo el suelo técnico deberían ser LSZH (Low Smoke Zero Halogen)
- ❏ Doble cableado eléctrico
- ❏ Generadores y cuadros de distribuciones eléctricas
- ❏ Alarmas instalados, además de los controles ambientales y de fuego con avisos en remoto

3.6.3. Requisítos de seguridad de un C.P.D.

- ❏ Cerraduras electromagnéticas (controladas por algún mecanismo de control de acceso)
- ❏ Cámaras de seguridad
- ❏ Detectores de movimiento
- ❏ Tarjetas de identificación