Seguridad en el entorno físico

Cuando se habla de **entorno físico** piensa nos referimos a los espacios donde se encuentran los equipos informáticos y los espacios circundantes a ellos, puertas, cerraduras, ventanas,…. La presencia de mecanismos de seguridad en el entorno físico de un sistema de información constituye una garantía para los datos, pero al mismo tiempo pueden constituir un problema si no están bien instalados, configurados o mantenidos.

Un sitio oficial, un instituto o una empresa, son buenos ejemplos de edificios que albergan equipos informáticos. Cualquier edificio cuenta con unas determinadas instalaciones iniciales, por ejemplo, el cableado eléctrico. Conocer cuáles son esas instalaciones con las que el edificio cuenta y verificar que cumplen las **normas de seguridad**, es el primer paso para minimizar los **riesgos** que acechan al hardware de la empresa, el instituto, etc.

Si todos los servidores están en un único lugar, entonces, ése será el lugar que hay que defender y proteger. En el entorno físico donde se encuentran los equipos informáticos como servidores y armarios de comunicación se suele llamar centro de proceso de datos (CPD) o **datacenter**.

Puede ser tan pequeño como un armario de comunicaciones o tan grande como la empresa decida. ¿Te imaginas cómo es de grande el CPD de Google? Las medidas de seguridad tendrán que ser acordes con el tamaño del CPD. Si sólo tienes un armario de comunicaciones, pues con saber quién tiene la llave solucionado. Ahora bien, si es todo un edificio, entonces, tendremos que vigilar, quién entra y sale, cuándo lo hace, qué zonas puede visitar…

En esta unidad se estudiaran desde las medidas más conocidas contra incendios, hasta los sistemas de control de acceso más complejos.

SPOF

Chema Alonso, es un experto en seguridad y uno de los fundadores de Informática64, una empresa afincada en Móstoles en el año 2000 cuya especialidad es la seguridad informática, ya sean auditorías, formación o consultoría. Suele decir, Chema Alonso, que "*La seguridad de una empresa es tan fuerte como el punto donde menos está segura*.

SPOF, Single Point of Failure, en español se podría traducir como único punto de fallo.", Con esto, quiere decir que hay que tener asegurados en la empresa todos los elementos de la misma.

Si se trata de asegurar físicamente los ordenadores, servidores o armarios de comunicaciones, tendremos que tener en cuenta dónde están y quién tiene acceso a ellos. Además de analizar cuán importante es alguno, (o todos), de nuestros equipos o servidores, y tener previsto cualquier fallo que pudiera afectarle. Desde que se va la luz, hasta un terremoto, pasando por un incendio,

inundación, robo… Todos estos **SPOF** es lo que llamamos **entorno físico.**

No conviene que olvidar que hoy en día, los ladrones utilizan viejas técnicas para robar servidores. Así que esa contraseña que tanto estuviste pensando y que tan segura era para tu administrador pasan a un segundo plano. Alguien se ha llevado físicamente el servidor, y en algunos casos, simplemente usando una sierra eléctrica para acceder al servidor y llevárselo a su casa

Acceso de personas al recinto

No debemos que olvidar que la protección física de los equipos, es tan importante o más que la lógica. Una vez que tenemos los equipos protegidos nos interesa saber quién y cuándo entra y sale de los recintos donde los ordenadores están guardados, pues eso forma parte de su seguridad.

“Se entiende por protegido: Libre y exento de todo peligro, daño o riesgo”.

El control de acceso de personas es algo que probablemente te resulte familiar, pues son cada vez más frecuentes los guardias de seguridad en los edificios oficiales que solicitan el DNI para entrar y te proporcionan una **tarjeta de visitante**. Ahora bien, hay otros métodos más eficientes si los que acceden al edificio lo hacen habitualmente. Los más utilizados son las **tarjetas magnéticas**, que permiten el acceso a determinadas zonas. Pero hay otros en el mercado como los **lectores de huella digital** o de **iris**, o cualquier otro elemento **biométrico**. Otro elemento preventivo son las **cámaras de vigilancia** para video vigilancia o tele vigilancia.

"Vigilantes jurados, video cámaras, biometría, tarjetas magnéticas, tarjetas de proximidad son elementos de seguridad activa."

También podría darse el caso de una combinación de dos o más de estos sistemas. Esta seguridad es **activa**, puesto que las medidas son principalmente preventivas, es decir, evitar que pueda suceder algo. Ahora bien, algunas de estas medidas son a la vez correctivas. Por ejemplo, las grabaciones de las cámaras pueden servir para identificar posteriormente a los **intrusos** que se saltaron el puesto de control del edificio.

Recuerda, lo que afirmábamos en la unidad anterior: La seguridad absoluta es imposible, por eso hablaremos siempre de **fiabilidad**.

Se suele decir que la seguridad informática es un **camino**y no un destino: la seguridad informática consiste en una serie de medidas que debemos tomar a lo largo del tiempo buscando alcanzar la máxima fiabilidad. Pero este conjunto de medidas tendrán que mantenerse y actualizarse de forma adecuada a lo largo del tiempo.

Quizá el acceso de personas al recinto se entienda mejor con un ejemplo práctico:

El acceso de personas al recinto industrial de las afueras de Madrid: Toda persona que accede al recinto deberá hacerlo por la puerta principal y la persona de recepción deberá cumplir las siguientes etapas:

1. **Identificación** de la(s) persona(s) visitante(s) y de la persona/sección a la que se desea acceder.
2. **Comunicación telefónica** con la persona/sección destinataria para que dé su conformidad al acceso. Ésta deberá enviar a alguien para que reciba y acompañe al visitante o hacerlo personalmente.
3. **Cumplimentación del registro de Control** de accesos de personas (código...) que deberá firmarlo la visita comprometiéndose al cumplimiento de las normas generales de seguridad.
4. **Entrega** de:
    - Hoja de visita que deberá firmar la persona visitada. En el reverso de esta hoja se indica la información básica sobre cuestiones y normas generales de seguridad del centro.
    - Tarjeta identificativa de persona que deberá adherirse en un sitio visible y cuya numeración coincidirá con la de la hoja de visita.
    - Los medios de protección necesarios, en los casos que se requieran.
    - A la salida la persona visitante deberá entregar al personal de recepción la hoja de visita firmada por la persona visitada y la tarjeta identificativa. Se registrará la hora de salida en el registro de Control de accesos de personas.

Alarma contra intrusos

Bueno, ahora vamos a proteger nuestros datos de una posible sustracción de los mismos, es decir, evitar que las personas que pasen cerca o al lado de nuestros equipos, tengan acceso a ellos. En nuestros ordenadores, tenemos almacenados nuestra preciada información, esencial para el buen funcionamiento de la empresa.

El objetivo es proteger los datos de intrusos e intrusas y el modo de realizarlo es instalar alarmas para detectar la presencia de personas no autorizadas en las áreas significativas, es decir, en las zonas donde está almacenada la información. Normalmente, equipos y/o discos duros.

Los sistemas de alarmas están compuestos por:

Elementos de los sistemas de alarmas

Elemento del sistema de alarma.	Descripción.
Módulo central.	 Es el sistema electrónico controlador de todos los elementos del sistema. A él están todos conectados y desde él podremos configurar la activación y desactivación del sistema, así como el modo de aviso cuando una alarma se produce.
Detectores.	 Son detectores de volumen, humo, temperatura, anhídrido carbónico, etc. Generalmente detecta los cambios que en estas variables se producen. Los sistemas son detección que utilizan pueden ser infrarrojos, microondas, ultrasonidos o frecuencias de sonido cuando se trata de detectar rotura de cristales.
Sistemas inalámbricos o de cableado.	Es el sistema de comunicación de los distintos componentes con el módulo central.
Baterías autónomas o de emergencia.	 Baterías autónomas son aquellas que proporcionan alimentación eléctrica a los elementos no conectados a la corriente eléctrica. Baterías de emergencia son aquellas que se ponen en funcionamiento cuando no hay corriente eléctrica.
Contactos magnéticos.	En puertas o ventanas detectan la apertura de las mismas, tienen un cierto retraso por si el que ha abierto la puerta no es un intruso y desactiva la alarma en esos pocos segundos. De no ser así, la alarma salta.
Avisador telefónico.	Un modo de avisar de una intrusión es la recepción de un mensaje en el móvil o de una llamada de voz de un número concreto, ambos alertan de intrusión pues

Elemento del sistema de alarma.	Descripción.
	son efectuadas por el avisador telefónico cuando se produce una anomalía.
Pulsadores de emergencia.	Son activadores de la alarma por personas, por ejemplo, un dependiente o dependienta puede tener un pulsador de emergencia debajo del mostrador si detecta la entrada de un sospechoso o sospechosa a su comercio.
La alarma.	Es normalmente acústica y visual, situada en un lugar poco accesible por las personas y protegida de los elementos meteorológicos si está en el exterior.

Instalación eléctrica

Aunque no es muy recomendable manipular los magnetotérmicos para realizar “demostraciones”, este ejemplo nos deja claro que existe una dependencia funcional de los equipos informáticos de la corriente eléctrica como única fuente de energía. Por tanto, tendremos que considerar a ésta como un elemento más de la seguridad en el entorno físico.

Teniendo esto en cuenta, distinguimos entre:

- **Red eléctrica externa**: Cuya función es el suministro de energía desde la subestación de distribución hasta los usuarios finales (medidor del cliente). De la seguridad de ésta se ocupa la compañía suministradora y en esta instalación tendremos que fijarnos en la protección del cableado visible y la no existencia de algún punto vulnerable, es decir, alguna parte del cableado accesible fácilmente por las personas. Cualquier modificación en este sentido debe ser solicitada a la compañía suministradora.
- **Red eléctrica interna**: Esta red pertenece a la empresa o persona propietaria del inmueble y debe de tener la potencia suficiente para hacer funcionar todo el sistema sin riesgo de cortes de suministro por exceso de consumo. Debe estar montada con elementos homologados y cumplir las normas españolas (UNE, Norma Europea aprobada por la Agencia Española de Normalización y Acreditación, más conocida como AENOR) y europeas. (EN, acrónimo de European Norms, es decir normas europeas aprobadas por el comité Europeo de Normalización o CEN). La potencia eléctrica, P, es el producto de V *I (Voltaje*Intensidad), es decir, la suma de todas las intensidades necesarias en todos los equipamientos nos daría como resultado al multiplicarlo por V (230 voltios en baja tensión) la potencia necesaria para suministro de todos nuestros equipamientos.
- **Personas**: Podemos considerarlas parte del sistema eléctrico. Como usuarios o usuarias que son del mismo, tienen que estar protegidos de las descargas que pudieran producirse mediante la instalación de tomas de tierra

Cálculo de la intensidad

Una empresa tiene un contrato con la empresa suministradora eléctrica de 25 Amperios. Se van a añadir cinco equipos nuevos y se quiere calcular cuántos amperios más van a suponer.

Si son cinco equipos y cada uno de ellos, estando a máximo rendimiento, necesita 87 Vatios para la CPU y 20 Vatios para la pantalla. (Pleno rendimiento quiere decir, encendidos, grabando un disco en la grabadora y con la pantalla encendida.)

¿Cuál es la intensidad que consumen los cinco equipos funcionando a la vez?

Tener en cuenta que **Potencia = Voltaje*Intensidad** y el voltaje de acometida de baja tensión es de **230 Voltios**

Solución:

> Si P=V*I, entonces I=P/V, luego para calcular la intensidad, divido la potencia de cada uno de los equipos entre el voltaje, 230 Voltios, y multiplico por cinco equipos.
>
> Con lo que obtengo el resultado de los amperios que consumirían los equipos a pleno rendimiento.
>
> Intensidad = Potencia / Voltaje = (87 + 20) Vatios * 5 equipos / 230 Voltios = 2,326 Amperios.

Seguridad de materiales eléctricos y protección de personas frente a la electricidad

Seguro que alguna vez has estado trabajando en casa, escribiendo algo con el procesador de textos cuando de repente, se fue la luz. En cuanto la luz volvió comprobaste qué parte no se había almacenado y tuviste que volver a teclearlo. Si tuvieras una empresa y todos los datos de clientes y productos estuvieran almacenados en un ordenador, esos datos serán sensibles, no podrías permitir que por un apagón se perdieran datos, es necesario tomar más medidas, pues la información almacenada en los equipos es **crítica**. Un apagón puede destruir la **mecánica** o la **electrónica** de un **disco duro**. Perder la información del disco duro de nuestra empresa con clientes y pedidos no es algo que queremos que pase. Además, si alguien en el momento que se fue la luz estaba tramitando un pedido, ¿cómo quedó la transacción?, ¿qué parte de los datos están almacenada?

Hay que tener en cuenta que el apagón no está llevando a situaciones no deseadas por el simple hecho de que “se fue la luz”. No es algo que pase todos los días, pero ocurre de tarde en tarde y **no podemos prevenir** cuándo y cómo será el próximo apagón.

Debes tener en cuenta esa posibilidad para defender a tu equipo de daños materiales y estar seguro que las transacciones no han terminado de forma traumática, sino que todo está controlado. Para ello, el o los equipos con datos sensibles deben contar con **suministro eléctrico adicional**. Estas son las soluciones que existen en el mercado para este problema:

- **Grupo electrógeno**: Es un generador de corriente eléctrica, independiente del suministro de la red eléctrica. Generan corriente a partir de gasóleo y pueden mantener en funcionamiento los sistemas informáticos críticos en situaciones de falta de suministro eléctrico. Por ejemplo, El centro de procesos de datos del gobierno de Canarias dispone de un grupo

electrógeno para mantener en funcionamiento el centro de proceso de datos a pleno rendimiento en caso de un fallo en el suministro eléctrico, siempre que el grupo electrógeno disponga de gasóleo, claro.

- **SAI o Sistemas de alimentación ininterrumpida**: Dada la importancia de estos elementos como protectores frente a disfunciones del suministro de energía eléctrica lo trataremos en la siguiente unidad con mayor profundidad.
- **Luces de emergencia**: Son luces en las puertas y zonas de evacuación del edificio que se encienden sólo en el caso de fallar el suministro eléctrico y proporcionan al personal la iluminación necesaria para abandonar el edificio y/o resolver los problemas que han causado el apagón

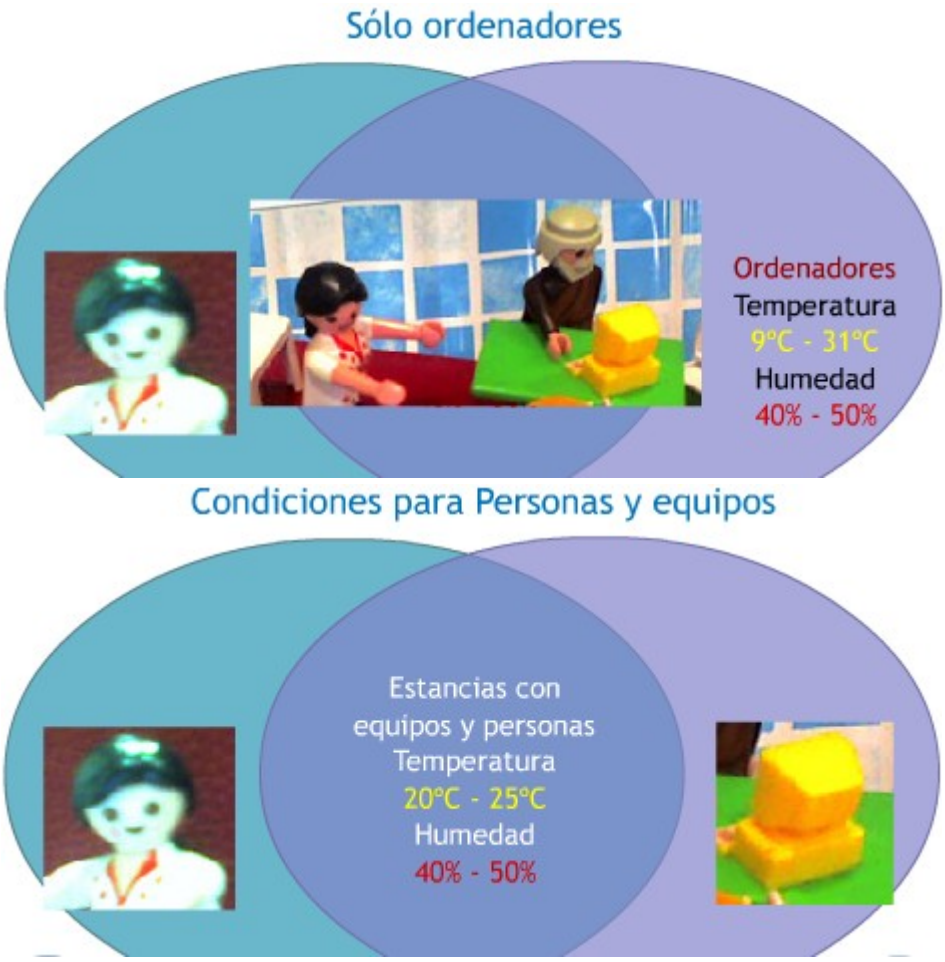
Condiciones ambientales y de humedad

Sabes que nosotros y las personas en general nos encontramos a gusto entre 20 y 25 ºC. Sin embargo, los ordenadores tienen un rango mayor de temperatura de trabajo, pues pueden hacerlo entro los 9º y los 33º. Buscaremos una temperatura ideal para ambos, personas y ordenadores, si es necesario que las personas estén también en el recinto.

Tienes que tener en cuenta que la climatización de las zonas de ordenadores sea agradable para las personas y, al mismo tiempo, no poner el riesgo el buen funcionamiento de los equipos.

Si por el contrario estamos hablamos de data centers, las salas se suelen llamar **salas frías,** puesto que la temperatura y humedad en estas salas dedicadas únicamente a equipamiento sólo tienen que tener en cuenta las condiciones en la que los equipos trabajan mejor. Los rasgos de temperatura de los componentes electrónicos son de 20º a 30º centígrados, y la humedad relativa entre 15% y 80%, siempre que la temperatura no pase de los 30º. Más allá de los 70º centígrados los sistemas no funcionan y si la temperatura supera el 90% a 30º, tampoco funcionan. Para recordar un poco mejor estos datos te propongo que veas la siguiente escena:

Datos de temperatura y humedad



Luego en la mayor parte de los casos habrá que **refrigerar**. Se refrigera para mantener las condiciones operativas de los equipos reducir los fallos del hardware y obtener una máxima duración.

- Temperatura mínima-máxima.
- Humedad relativa.

Existen diferentes soluciones de climatización, que pueden ir desde un simple aparato de aire acondicionado a una refrigeración directa de los elementos electrónicos. Aquí puedes ver las más utilizadas en los CPDs:

1. **Climatización por falso suelo**. Es el sistema más frecuente de climatización en CPD. Los CPD´s normalmente disponen de suelo técnico, por lo tanto, el sistema de refrigeración más habitual es el de impulsión de aire frio. El aire frio que sale por las rejillas, colocadas en los pasillos fríos, pasa a través de los servidores y retorna caliente a los acondicionadores a través de la parte superior de los mismos.
2. **Climatización InRow (entre Rack)**. Para minimizar la mezcla de aire entre pasillos fríos y calientes, los equipos de refrigeración se instalan entre Racks, consiguiendo mayor eficiencia energética en un CPD de múltiple pasillos. Estos aspiran el aire del pasillo caliente, lo filtran, enfrían y lo impulsan al pasillo frío. Es decir, se alternan pasillos fríos y calientes consiguiendo un flujo de aire horizontal. El sistema de refrigeración se adapta a cualquier distribución de sala. Por sus características, es muy buena solución para el acondicionamiento en climatización de CPD medianos, que no superan los 100 m2 y que

cuentan con un máximo de 30 racks.

3. **Climatización de precisión complementaria para servidores de alta densidad**. El sistema anterior de refrigeración no es suficiente si en los racks se acumulan gran cantidad de servidores. Son los llamados servidores de alta densidad. Para estos casos sería necesario climatización de precisión directa del rack o una climatización directa del chip, pero claro, esto es el futuro. Esta climatización está diseñada, sólo hay que empezar a construirla. Tendremos que estar preparados para localizar la refrigeración en el punto verdaderamente sensible de los equipos, sus chips o tarjetas

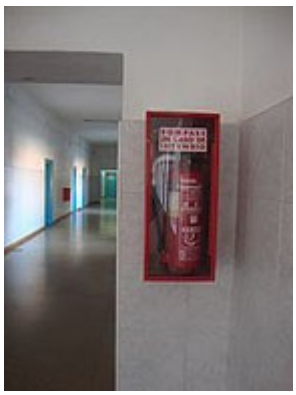
Enemigos de los ordenadores: Partículas de polvo, agua y fuego

Para defender a nuestros equipos del polvo podemos **aislarlos**, **ventilar** el lugar o **controla**r el **contenido de la atmósfera** en la que se encuentran:

- **Ventilación**: Un sistema de ventilación natural o bien instalar purificadores de aire que retienen en sus filtros el polvo suspendido.
- **Aislamiento integral**: Si se trata de un CPD se convierte en una zona muy sensible por lo que se hace necesario aislarlo del polvo y otras partículas como veremos más adelante.
- **Pureza del aire**: Para saber lo puro es el aire en una estancia, podemos instalar **detectores de gases** que sean capaces de detectar desde el oxígeno, al metano entre otros muchos más.

Cuando se trate de ordenadores, debemos defendernos de **fugas de agua**, **filtraciones de lluvia** o cualquier otro tipo de **inundaciones**, pues el agua les causa daños, a veces, irreparables. ¿Qué tenemos que hacer? :

- **Sistemas de desviación**: Los grifos y salidas de agua deben estar lejos de las salas con equipos informáticos, y además, contar con sistemas de desviación y absorción del agua en caso de escapes de agua.
- **Sistemas de salvaguarda**: Los equipos físicamente deben alejarse de las ventanas y si están sobre el suelo, elevarlos.
- **Sistemas de detección**: Si queremos asegurarnos de que el agua no va a dañar nuestros sistemas podemos incluir detectores de agua en aquellos lugares a los que ésta llegaría en primer término en caso de fuga, que suele ser, en el suelo, en las paredes o en el techo.



El fuego puede producir daños en los equipos informáticos irreparables, así que tendremos que tomar medidas **pasivas** y **activas**. La causa más probable de incendio en un equipo o CPD es el sistema eléctrico.

Podemos defendernos del fuego con medidas de seguridad pasiva:

- **Barreras**: Evitan la propagación del fuego. Vías de evacuación: ofrecen a las personas la posibilidad de abandonar el edificio en caso de incendio.
- **Extintores**: Y/o otros elementos para detener el fuego cuando éste se halla declarado