Seguridad en el Entorno Físico.

Caso Práctico

Juan e Iván están en una cafetería, es su tiempo de descanso, hablan animadamente. Juan pregunta:

¿Has visto el video sobre el nuevo centro de proceso de datos (CPD) de Google hecho con contenedores?

-¿Contenedores?

-Sí, sí, contenedores, Iván, los contendores dan modularidad al CPD, cada contenedor es un bloque de dos pasillos de armarios de comunicaciones, uno a cada lado.

-¿Y qué ventaja tiene que sean contenedores?

-Bueno, Iván, es más fácil todo, las necesidades de energía eléctrica del contenedor, la refrigeración instalada en cada contendor es la misma, el acceso al mismo. Al ser igual en todos parece que está cómo más organizado y más sencillo de controlar.

-Y, ¿pueden mover los contenedores?

-Sí, Iván, sí, tienen una grúa para moverlos.

-Entonces deben estar en una nave enorme, si cabe incluso una grúa de contendores.

-Sí, Iván, es bastante grande, tanto es así que el empleado o empleada que lo manipula usa un patinete para desplazarse.

-Oye, Juan, podíamos montar nosotros un CPD de esos en la empresa, en lugar de tener un armario de comunicaciones por departamento. Es más, el armario de informática siempre está abierto, dicen que así se refrigeran mejor los switches.

-Pues no es mala idea, Iván, si todo estuviera centralizado, tendríamos mejor control de servidores, accesos y demás, pero ¿dónde lo colocamos?

-No sé. Voy a llamar a Ignacio, a ver qué le parece la idea.

Cuando oigas **entorno físico** piensa que se están refiriendo 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. Te diré que 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 estudiarás desde las medidas más conocidas contra incendios, hasta los sistemas de control de acceso más complejos.

Reflexiona

No sirve de nada la aplicación de medidas de seguridad a través de software y olvidarnos de las medidas de seguridad de las instalaciones físicas.

Mostrar retroalimentación

Si el objetivo es acceder a la información que tiene un equipo, cualquier solución es buena, conectarse al equipo con herramientas de hacking o sustraer el disco duro.

Autoevaluación

Un DATACENTER es el lugar físico donde se encuentran los equipos informáticos de la empresa. ¿Verdadero o falso?

○ Verdadero ○ Falso

Verdadero
Es VERDAD, que al lugar físico donde se centraliza el almacenamiento de los equipos físicos y servidores se llama DATACENTER y se utiliza este término anglosajón ampliamente pues parece más idóneo que su equivalente en castellano: Centro de datos.

Seguridad en el Entorno Físico.

Caso Práctico

Juan recibe una llamada de Ignacio, que está en un curso sobre Seguridad y Auditoría Informática, en la Universidad Europea de Madrid:

-Juan, ¿qué tal van las cosas por la oficina?

-Bien, pocas novedades, Ignacio. ¿Qué tal el curso?

-Bueno de momento hemos tenido las presentaciones y el registro de los participantes. Después del descanso hablarán de los nuevos retos relacionados con la seguridad de acceso mediante el uso del DNI electrónico.

- Ese es el tema que a ti más te interesaba, Ignacio, ¿no? Espero que disfrutes de ella y cumpla las expectativas que esperabas.

- A ver, Juan, para poder disfrutar de la conferencia necesito que me hagas un favor, vete al instituto en el que estuvimos el otro día arreglando un switch y diles que te cuenten qué es ese "**TSCI**" (Tele Sala de Consulta en Internet)" que quieren montar en el hall. Que vaya Iván contigo, que el hable y tú tomas notas.

-¿Tele Sala de Consulta en Internet? Nunca había oído nada parecido.

-Ni yo, Juan, ni yo, se lo han inventado ellos, le han puesto ese nombre porque les gusta.

-Vale, de acuerdo, iremos esta misma mañana. Pero ¿qué es lo que tengo que apuntar?

-Bueno pues me interesa que tengas en cuenta las condiciones de seguridad que rodean al "TSCI" y cómo controlar quién entra y sale de él.

-A ver si me he enterado bien, Iván conoce el tema y mientras el habla yo tengo que tomar notas sobre los aspectos de seguridad existentes en el edificio y en concreto sobre el lugar dónde se va a situar el "TSCI". También tengo que estudiar quién y cuándo entraré en el recinto y cómo vamos a controlar ese acceso.

-Exacto, Juan, ahora tengo que colgar, que va a empezar la conferencia. Gracias por adelantado, te debo una.

-Nada hombre, hoy por ti y mañana por mí.

Juan se queda algo inquieto, mucha responsabilidad estudiar el edificio y lo que más tarde se va a instalar. Empieza a hacer una lista de lo que tiene que revisar y qué sistemas existen de control de acceso a recintos. Se queda tan concentrado en su búsqueda que no oye a Iván avisarle de que se tienen que marchar.

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 olvides 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 o root 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 debes 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.

> "Entendemos 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.

Reflexiona

Se suele decir que la seguridad informática es un camino y no un destino.

Mostrar retroalimentación

Con esta afirmación nos referimos a que, como hemos dicho, 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.

Debes conocer

Algunos ejemplos de hoja de visita, puedes ver un ejemplo de los formularios que rellenan cuando una persona entra al recinto y de la hoja de visita que se entrega al visitante y debe de traer firmada.

Hoja de visita. (0.12 MB)

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.  Central de alarma detectora de robos e incendios.
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.  Detector de intrusos por detección de volumen.
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.  Detector de rotura de cristales por vibración abierto para ver el circuito.
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 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.

Para saber más

En la siguiente página web de Securitas Direct verás con animaciones los elementos de seguridad instalados en las empresas.

Página Securitas Direct.

Autoevaluación

Las áreas significativas son zonas donde está almacenada la información. ¿Verdadero o falso?

Sugerencia

○ Verdadero ○ Falso

Verdadero
Área significativa es el lugar físico donde hay algo de valor, en una empresa son los datos, por ello, el acceso a estos recintos debe ser controlado.

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.

Elementos de la red eléctrica

Elementos de la red eléctrica	Ejemplos de medidas de seguridad
Red eléctrica externa.	Inaccesibilidad al cableado externo. Protección y cubrimiento del cableado.
Red eléctrica interna.	Cumple la UNE –EN. **Potencia suficiente.**
Personas.	Tomas de tierra.

La toma de tierra evita el riesgo de electrocución de las personas y de averías de equipos y es obligatoria su instalación.

Consulta el Real Decreto 842/2002 en el BOE - Modificado a 10 de Abril de 2019, Boletín Oficial del Estado donde se aprueba el Reglamento Electrotécnico de baja tensión, es decir **230 Voltios(V) y 50 Hertzios (Hz).**

Ejercicio resuelto

Iván ha comprobado la instalación eléctrica en las inmediaciones del lugar donde se va a instalar la **"TSCI"** (Tele Sala de Consulta en Internet)". Tienen un contrato de 25 Amperios. Quiere calcular cuántos amperios más van a suponer los cinco equipos añadidos en la "TSCI" (Tele Sala de Consulta en Internet).

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?

Si Potencia = Voltaje*Intensidad y el voltaje de acometida de baja tensión es de 230 Voltios.

Mostrar retroalimentación

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 estabas 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 quieres 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 Cantabria 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.

Seguridad de materiales eléctricos

Recursos frente a fallos en el suministro de energía eléctrica	Solución de seguridad
Grupo electrógeno.	Genera corriente eléctrica independientemente de la corriente eléctrica.
Sistemas de alimentación ininterrumpida (SAI).	Protección frente a variaciones puntuales en el suministro de energía, como picos de intensidad que podrían dañar el sistema y proporciona corriente durante un espacio corto de tiempo a los equipos.
Luces de emergencia.	Iluminan el edificio para poder abandonar el edificio y/o acceder a servidores para apagarlos con normalidad y/o solucionar el problema que causó la avería.

Para saber más

"Los data centers en Japón hacen frente a los apagones intermitentes", artículo publicado el 16 de marzo de 2011 por Yevgeniy Sverdlik y traducido por Virginia Toledo. En él verás los problemas de suministro energético que se crearon tras el terremoto ocurrido en Japón en marzo del 2011 y el posterior tsunami. Y qué medidas preventivas les fueron útiles tras el suceso.

Consecuencias del terremoto y tsunami ocurrido en Japón en marzo del 2011.

Condiciones ambientales: Humedad y Temperatura.

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.

0:00 / 0:17

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 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.** Este sistema 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.

Para saber más

Las refrigeraciones pueden ser por varios medios: aire, por agua, refrigeración de acople cerrado y glicol para armarios, salas de servidores y centros de datos. En este enlace verás los diferentes sistemas de refrigeración que existen clasificados según su tipo.

Sistemas de refrigeración en un CPD.

Autoevaluación

Alternar pasillos fríos y calientes en los CPD, consigue un flujo de aire vertical. ¿Verdadero o Falso?

Sugerencia

○ Verdadero ○ Falso

Falso
Al alternar pasillo fríos y calientes lo que se consigue es un flujo de aire HORIZONTAL, pues el aire caliente sube y al subir genera una depresión que es llenado por el aire frío del pasillo de al lado, luego la corriente GENERADA es el tránsito de ese aire frío hacia el pasillo caliente, por tanto HORIZONTAL.

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

Reflexiona

Las partículas de polvo son un gran enemigo de los ordenadores, pues cubren los circuitos y ventiladores impidiendo su buen funcionamiento. ¿Qué podemos hacer para defender a nuestros equipos del polvo?

Para defender a nuestros equipos del polvo podemos aislarlos, ventilar el lugar o controlar 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.

Autoevaluación

Algunas de las medidas de seguridad activa que debemos tomar para nuestra TSCI del caso práctico, son:

- [ ] Extintores con CO_2 o de agua nebulizada al ser equipamiento electrónico.
- [ ] Los detectores de agua en el suelo.
- [ ] Los sistemas de desviación y absorción del agua en los baños.
- [ ] Dejar los cristales que forman parte de los muros incompletos en su parte más alta para ventilar.

Mostrar retroalimentación

Solución

1. Incorrecto
2. Correcto

3. Correcto
4. Correcto

Centro de Proceso de Datos y su Entorno Físico.

Caso Práctico

-Oye Juan, esa idea tuya de instalar un CPD me ha gustado mucho.

-Vamos, Ignacio, seguro que ya lo habías pensado antes tú.

-Pues no, no lo había pensado.

-Tú conoces bien el local, ¿dónde lo instalarías?

-Bueno hay un cuarto de limpieza en el sótano que no se utiliza, aunque allí hace bastante calor. El baño de esta planta lleva tiempo cerrado desde que se estropeó el grifo del lavabo no se ha vuelto a usar.

-Y ¿qué te parece en el pasillo? Al final hace un hall enorme, que nadie usa, es sólo un sitio de paso.

- Igual el local de al lado nos vendría bien, tiene una pinta estupenda. Lo reformaron el año pasado, tiene aire acondicionado, dobles techos, ya verás, fíjate luego cuando salgas de la oficina. Se ve al pasar.

-¡Ah, sí, es verdad!, donde estaba antes la venta de congelados al peso. Tenían dos pasillos de frigoríficos-congeladores. Y dos o tres aparatos de aire acondicionado, que no se los han llevado y deben estar nuevos, pues con el frío que hacía allí, apenas los usaban.

Después de haber nombrado varias veces un **CPD** en esta unidad, vamos a estudiarlo más en detalle.

Un CPD es un **centro de procesos de datos**, normalmente se trata de una sala cuyas dimensiones dependerán de las de la empresa u organización a la que pertenezca. Por ejemplo, la Universidad de Cantabria sitúo su centro de cálculo en una habitación del rectorado en un principio, pues sólo albergaban la base de datos de profesorado, alumnado y PAS en ella. Ahora bien, a medida que fueron aumentado los servicios ofrecidos por la universidad, como la matrícula vía internet, el reconocimiento del alumnado por su tarjeta de estudiante, el control de las aulas de informática, etc.., El espacio se fue quedando pequeño. Entonces, el CPD se alojó en un edificio colindante en una sala fría que ocupaba todo un sótano.

En un CPD podemos encontrar el cableado de red, servidores, discos duros, cortafuegos, ordenadores, copias de seguridad, y todos aquellos elementos que forman parte del sistema informático de la empresa.

En un CPD debemos mantener la disponibilidad de la información, proteger su integridad y salvaguardar siempre la confidencialidad. Seguro que estos conceptos te resultan familiares, pues los has visto en la unidad anterior.

Verás ahora cuáles son las medidas de seguridad que se han de tomas en el entorno del DATACENTER. Algunas ya las conocemos, pero otras nos resultarán totalmente nuevas.

Cuando un CPD es construido pretende ser el lugar donde la información va a ser almacenada. Como ya sabes, los datos es lo más crítico y sensible y, por lo tanto, tendremos que aplicar todas las medidas de seguridad que ya conoces:

- Integridad.
- Confidencialidad.
- Disponibilidad.

Procurando que puedan cumplirse las tres simultáneamente y tendremos en cuenta lo dispuesta en la **LOPDGDD** que ya conoces de la unidad anterior.

Debes conocer

En estos enlaces podrás ver las noticias sobre las consecuencias de la explosión de un transformador en un data center. El vídeo muestra cómo el transformador se está quemando y las consecuencias que se dan mientras el incendio se apaga. Verás que el datacenter no ha sido dañado físicamente pero las condiciones de seguridad obligan a apagar ciertos sectores hasta que el incendio haya sido sofocado.

Graves problemas en el datacenter H1 de The Planet 2°.

Vídeo de la explosión del transformador.

http://www.youtube.com/embed/rfnZuQP2p4Q

Infraestructura.

Nunca empezaríamos una casa por el tejado, dice un refrán, pues esto es lo mismo que ocurre con un centro de datos, antes de nada hay que saber cuáles son las condiciones del entorno en el cual lo vamos a instalar. Veamos qué debemos tener en cuenta. Para decidir la infraestructura, antes tenemos que estudiar las condiciones geológicas en el entorno de nuestro CPD.

Tipos de infraestructuras.

Infraestructura	Debido a	Explicación
Construcción antisísmica.	Probabilidad de terremoto. 	Por ejemplo si se trata de una zona con alto riesgo de terremotos, la construcción tendrá que ser sobre pilares o antisísmica.
Aislamiento térmico.	Altas y/o bajas temperaturas.	Los muros y las ventanas exteriores estarán aislados térmicamente del exterior, así las condiciones de temperatura exterior no afectarán al interior del edificio, o al menos mitigarán su efecto.
Paredes.	Polvo y fuego.	En el interior las paredes tendrán tratamiento ignífugo y anti polvo.
Suelos.	Peso de los equipos de comunicación. Inundaciones. 	El suelo tendrá una alta capacidad de carga, lo que quiere decir que podrá soportar el peso de los armarios de comunicación que se almacenen en el CPD. Y además si instalamos dobles suelos añadiremos protección frente a inundaciones y electrocuciones.

Debes conocer

Si entendemos bien los componentes de un CPD agrupándolos en secciones, buscamos cómo ahorrar energía en cada uno de los procesos. Podrás entender de qué partes consta un CPD y ver un caso real de CPD.

Partes consta un CPD.

Para saber más

Te recomiendo que leas el siguiente documento con detenimiento para que puedas tener una opinión personal del sistema, sus ventajas y sus inconvenientes.

Supercomputador IBM con enfriamiento líquido.

Autoevaluación

¿Qué sistema de los siguientes forma parte de la infraestructura de un CPD?

- ○ Muros de hormigón reforzados.
- ○ Acceso restringido al DC con tarjetas de seguridad.
- ○ Detección de incendios.
- ○ Armario ignífugo para el almacenaje de cintas.

Correcta. Los muros son parte de la infraestructura de un CPD.

Incorrecta. Las tarjetas de seguridad no son infraestructura física del CPD.

Incorrecta. La detección de incendios no es infraestructura física del CPD.

Incorrecta. Losa armarios ignífugos no son infraestructura sino mobiliario del CPD.

Solución

1. Opción correcta
2. Incorrecto
3. Incorrecto
4. Incorrecto

Acceso.

¿Has viajado alguna vez en metro? Seguro que nos hemos comprado un billete con una banda magnética que al introducirla en el torno de control de paso nos permite acceder ya a cualquier metro y línea enlazando unos metros con otros, siempre que no salgas al exterior, claro.

Un Control de Accesos no es más que un mecanismo que en función de la identificación ya autentificada, permite acceder a recintos, datos o recursos.

Cada vez más, se hace necesario controlar, gestionar y monitorizar los movimientos de las personas que entran y salen de nuestras instalaciones.

Las medidas de seguridad de un DATACENTER dependerán de las dimensiones del mismo, vamos a enumerar todas las medidas de control de acceso conocidas que en un DATACENTER se pueden establecer:

- **Personal de seguridad:** éste es un recurso de un alto coste que sólo las grandes empresas pueden abordar.
- **Control de acceso a zonas interiores:** Por ejemplo, cuando aparcas en un parking subterráneo, recibes la tarjeta de entrada que te permite el acceso y en la que se encuentra grabada la hora de ingreso en el parking.
- **Lectores de matrículas:** Siguiendo con el ejemplo del parking, en la tarjeta, además, se graba también la matrícula del coche.
- **Blindar las puertas en las áreas críticas.** En muchas comunidades autónomas es obligatorio que existan estas puertas para proteger algunas zonas en caso de incendio, por ejemplo, puertas ignífugas.
- **Sistemas biométricos:** Que reconocen a las personas de la misma forma, o parecida a cómo lo hacemos nosotros normalmente, rasgos faciales, color de ojos….
- **Control de acceso personal y/o electrónico** al CPD y nuevo control en las distintas zonas: si el sistema que estamos defendiendo es crítico, deberíamos de defender también el acceso a determinadas zonas del mismo con sistemas de seguridad, por ejemplo, mediante códigos en puertas.

Para saber más

En el incendio de Valdecilla (Hospital Universitarios de Santander), el humo no puede escapar por las ventanas atornilladas por motivos de seguridad de los enfermos psiquiátricos.

Alarma por incendio.

Redundancia.

Siguiendo con el refranero español: dos mejor que una. Si se trata de servidores en los cuales la información es crítica, qué mejor que tener la información duplicada por si uno de los equipos se estropea, poder tener otro que entre en servicio inmediatamente. Los elementos redundantes que tenemos deben de existir de forma ideal son:

- Un **CPD de respaldo**, es un edificio que contenga exactamente lo mismo que el CPD original, es decir, yo tengo dos CPD´s igualitos y, además,s situados en diferentes localización, como dicen los ingleses "just in case", es decir, si se diera el caso de que uno de ellos no pudiera dar servicio, el otro, que es una réplica de éste, entraría en funcionamiento tan solo en unas horas. Como en el caso del DATA CENTER H1 de THE PLANET que vimos en el punto 3 de esta misma unidad.
- **Diferentes proveedores** de internet, ya que si en alguno de ellos se produce una avería, se podría utilizar el otro. Por ejemplo en España, puedes tener contratada una línea con telefónica y otra con ONO, así la probabilidad de que el acceso a internet no falle es mucho más baja que en el caso de tener varias líneas con el mismo operador.
- El **control de la temperatura**, la humedad y el filtrado del aire, también tiene que tener salvaguarda, para que en caso de fallar el sistema principal, entre en funcionamiento el sistema secundario.
- En caso de fuego, habrá que tener en cuenta todos los posibles orígenes del fuego para adoptar las medidas necesarias de detección y extinción.
- En cuanto a la **acometida eléctrica,** también conviene tener más de una compañía proveedora. Si una de ellas falla o se produce un apagón, disponemos de la otra compañía. En algunos lugares, si no existen dos compañías, deben tener un generador independiente que suministre electricidad al CPD.

Debes conocer

Este es el enlace a la página web de CIO, donde explican qué es la eficiencia energética en un centro de datos o data center y cómo se puede medir mediante los ratios: PUE y DCiE.

Página web de CIO

Un centro de datos suele tener las dimensiones de una fábrica en una gran nave. Para poner en marcha un centro de datos se necesitan una gran cantidad de servidores, normalmente en granjas o en racks dentro de armarios de comunicación. Estos armarios de comunicación o estas granjas producen una gran cantidad de calor, por lo que hay que enfriar las salas en las que se encuentran.

Además, consumen gran cantidad de energía eléctrica, por lo que la “**acometida”** a estos centros de datos no suele de ser de baja tensión, como la de nuestras casas, sino de media tensión, como la de las empresas. Por lo tanto, también tendrán que disponer de un transformador de esa media tensión a baja tensión. Esto supone una gran inversión en infraestructura.

Así que la seguridad en estos centro de datos abarca casi todos los aspectos vistos hasta ahora.

Para saber más

Para entender mejor la redundancia puedes ver este video del primer CPD de contenedores de Google. Por ejemplo, todos los ordenadores están conectados a su propio SAI. La redundancia hace que el gasto se multiplique por dos, por ello, en el video insisten en la búsqueda de la eficiencia de todos los sistemas.

(El video está en inglés, si algo no entiendes puedes activar los subtítulos automáticos de Youtube.com que traducen literalmente lo que está diciendo.)

Visita guiada al primer data center de contenedores de Google.

https://www.youtube.com/embed/zRwPSFpLX8I

Autoevaluación

Qué significa las siglas PUE:

- ○ *Power Usage Efficiency*, se calcula dividiendo el consumo del equipamiento IT por el consumo total del centro de datos.
- ○ *Datacenter Infrastructure Efficiency*. Es el resultado de dividir el consumo del equipamiento IT dividido por el consumo total del centro y multiplicado por 100.
- ○ *Power Usage Efficiency*, se calcula dividiendo el consumo total del centro por el del equipamiento IT.
- ○ Power Usage Efficiency, se calcula dividiendo el consumo total del centro por el del equipamiento IT y multiplicado por 100.

No es correcta, pero te has acercado mucho a la respuesta correcta.

Incorrecta, este es el sistema de medición de las eficiencia de un data center en Europa, y es diferente al POE de Estados Unidos.

Correcta. Muy bien, por tanto que el PUE de Google sea de 1.25 de muestra una gran eficiencia en el consumo de energía, pues lo habitual es que sea de 2.

Falso, pues no se trata de un tanto por ciento.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

Sistemas de Control de Acceso.

Caso Práctico

-Juan, me llaman de dirección, han desaparecido tres portátiles de nuestra empresa.

-Madre mía, tres portátiles, pues no parece fácil llevarse así tres portátiles de golpe.

- Ya, parece que alguien entró en la garita de los conserjes y los cogió, se los colgó del brazo y no se han vuelto a ver. ¿Qué podemos hacer?

-Bueno, lo único que se me ocurre es tomar alguna medida de control de entrada y salida del personal para que no vuelva a ocurrir.

-Ya, pero somos 134 en la empresa, y todos entramos a la misma hora. Si pones un sistema de control de entrada se van a formar colas por la mañana.

-Bueno, si sólo fuera por la mañana, imagínate a la hora de salida, allí habría más que palabras.

-Veo que me has entendido perfectamente. ¿Qué podemos hacer?

-Pues tengo una amiga en la universidad, le puedo preguntar cómo controlan allí el acceso, creo que acaban de instalar un sistema de control de alumnos.

-Vale, pues vete allí, habla con ella y que te enseñe cómo como es el sistema y que tal funciona. Haz fotos de todo lo que puedas. Sobre todo de las horas punta, cuando todos entran o salen de clase.

-Bien, voy a llamarle a ver cuándo puede reunirse conmigo.

Vas a empezar por ver los dispositivos que controlan el acceso. Para saber qué cantidad de elementos de seguridad tenemos que utilizar, es imprescindible valorar el impacto que la pérdida de datos y/o hardware supondría para la empresa. Este impacto puede ser económico, de imagen de empresa y/o personales.

Según el impacto que la pérdida de datos vaya a atener tendremos que escoger diferentes sistemas electrónicos, mecánicos y/o biométricos. Estos sistemas se pueden clasificar en autónomos y dependientes:

- Los **sistemas independientes** son aquellos que no necesitan una conexión a internet, se auto gestionan. También se llaman autónomos, la ventaja de estos sistemas es que su coste es muy reducido.
- En contraposición nos encontramos con los **sistemas dependientes** que necesitan una conexión a internet pues es desde el servidor desde donde son gestionados.

Si un sistema autónomo tiene la posibilidad de que mediante un dispositivo adicional conectado a él se puede conectar a internet, entonces el sistema se denomina **autónomo convertible**.

Y vas a terminar estudiando el personal de vigilancia, éstos tienen unas funciones establecidas por ley y diferenciada según sea subcontratada a:

1. Otra empresa.
2. Personal de vigilancia de la propia empresa.

Personal de Vigilancia y Control.

Imagina que acabas de abrir el periódico y te encuentras este anuncio: “Se precisa persona de 40 a 55 años, buen trato y buena presencia para Vigilancia en portón de entrada del complejo para el control de personas y vehículos. Imprescindible trabajar sábados, domingos y festivos de 10:00 a 20:00. Días libres únicamente entre semana. Meses de enero, febrero y parte de Marzo. Importante que viva en zona cercana a Parque Juan Carlos I.”

S busca una persona que vigile la entrada a un recinto, estas personas se encargan de controlar el acceso a un determinado espacio. Deben hacerlo en las horas en las que el establecimiento está abierto, esto incluye fines de semana. Es por tanto una de las soluciones más caras para una empresa. Contratar personas para vigilar el acceso, pero asimismo es una de las más eficaces.

Te interesará saber que la normativa sobre competencias del personal de vigilancia y control se encuentra recogida en **Ley 5/2014, de 4 de abril, de Seguridad Privada.** En ella se describe el reglamento de Seguridad Privada.

Son diferentes las competencias del personal de seguridad de la empresa y del personal de seguridad privada.

La lectura de las leyes, a veces necesita aclaraciones y, por ello, el Ministerio del interior tiene en su página web una zona de respuestas dadas por la secretaría técnica a preguntas de los ciudadanos y en él se pueden encontrar explicaciones sencillas a las dudas más habituales.

Para saber más

En la página web del ministerio del interior encontramos explicaciones sobre la seguridad privada, por ejemplo, diversas cuestiones relacionadas con la prestación de servicios de seguridad privada en establecimientos públicos.

Ejemplo de contenidos de la web del Ministerio del interior

Autoevaluación

La normativa sobre competencias del personal de vigilancia y control se encuentra recogida en la Ley 5/2014, de 4 de abril. ¿Verdadero o Falso?

○ Verdadero ○ Falso

Verdadero

Así es, la ley española sobre competencias del personal de seguridad se encuentra recogida en la Ley 5/2014, de 4 de abril, de Seguridad Privada.

Dispositivos de Control de Acceso en un Datacenter.

- **Tarjetas:**
  Es el sistema más extendido en Data Center. El sistema consiste en proporcionar acceso a las personas que posean una tarjeta de entrada que la empresa les suministra con la que se controla el acceso, incluso en intervalos de tiempo y se identifica a las personas que acceden al mismo tiempo.

  Tipos de tarjetas:

  - **Tarjetas de contacto.** Las tarjetas magnéticas son leídas por contacto. Es un sistema muy económico y sencillo de instalar pero la banda magnética se degrada con cada lectura. Además, son muy sensibles al calor y a campos magnéticos, con lo cual, su deterioro es rápido.
  - **Las tarjetas de proximidad** funcionan por **RFID** (Radio frecuencia) y pueden ser leídas desde 15 centímetros las de corto alcance, hasta 2 metros, las de largo alcance. La Radio frecuencia es ventajosa pues al no producirse contacto no hay desgaste de las tarjetas por rozamiento, y es un sistema muy cómodo pues con llevar la tarjeta en el bolsillo el sistema detecta la misma sin necesidad de moverla de su ubicación.

- **Teclados:**
  Son casi siempre numéricos, en ellos se introduce un código para acceder al recinto. Pueden ser digitales y mecánicos, estos últimos muy difundidos en el Reino Unido. Los electrónicos necesitan una batería o estar conectados a la red, pues la cerradura asociada también es eléctrica.

  En estos teclados-cerradura, la contraseña debería de cambiarse con cierta asiduidad, pues es la misma para todos los usuarios y usuarias.

  Un ejemplo de cerradura mecánica puede ser el portal de casa o el portón del garaje. Tienen la desventaja que no se identifican a las personas que acceden, sólo se controla el acceso a los que conocen la contraseña.

Reflexiona

El control de acceso físico es una medida de seguridad activa que previene peligros que en último extremo podrían afectar al núcleo de cualquier sistema de información: **los datos.**

Autoevaluación

¿Qué ventaja representan los teclados frente a las tarjetas de proximidad?

- ○ Que no pueden ser dañados por vandalismo.
- ○ Que no los tienes que llevar encima.
- ○ Que se te puede olvidar la contraseña.
- ○ Ninguna.

Incorrecta, Son los teclados susceptibles de ser dañados por vandalismo, puesto que se encuentran visibles.

Correcta.

No es correcto, pues esto es una desventaja del teclado, no una ventaja.

Falso, los teclados sí presentan alguna ventaja frente a las tarjetas, inténtalo de nuevo.

Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

Sistemas de Reconocimiento de Personas.

Como ya sabes, los teclados y tarjetas tienen como misión principal permitir el acceso, mediante la apertura de la puerta en la que están situados.

Según las características de estos teclados y/o tarjetas podemos hacer una identificación del acceso asignando diferentes contraseñas a cada usuario y usuaria.

Y podemos avanzar en complejidad con horarios de apertura para determinados usuarios y usuarias y almacenamiento de intentos frustrados de acceso si estos elementos están conectados a un ordenador.

Los teclados siempre se encuentran junto a las puertas y son visibles para poder introducir la contraseña de acceso. Sin embargo, las tarjetas pueden tener lectores mecánicos para su lectura o lectores por radio-frecuencia invisibles para el usuario.

Por supuesto, también cabe la posibilidad de que ambos sistemas se presenten combinados, es decir, un sistema de acceso por tarjeta. Una vez reconocida la tarjeta, solicite el código de la misma, estos sistemas combinados proporcionan una doble seguridad, puesto que si la tarjeta se extravía, alguien desconocido no puede acceder al edificio con ella, porque desconoce el código a teclear.

De esta forma estamos haciendo un reconocimiento de la persona que accede y además autenticando su identidad.

Debes conocer

Vídeo de los servicios que ofrece la. Tarjeta Universitaria Inteligente (TUI). Está desarrollada por la Universidad de Cantabria en colaboración con el Banco Santander para el acceso de personas a las distintas instalaciones del campus universitario.

https://www.youtube.com/embed/GLtIoyrqNa8

Vídeo de los servicios que ofrece la Tarjeta Universitaria Inteligente

Voy a intentar aclarar la palabra autenticar, pues la vamos a utilizar de ahora en adelante y no es un error, sino un nuevo concepto. Autenticar es dar fe de la verdad de un hecho o documento con autoridad legal. Por ejemplo, si tú llevas el DNI de ese amigo o esa amiga, al que casualmente te pareces mucho, podrías pasar por él o ella. Si además del DNI, te piden firmar, entonces, no es tan fácil que te hagas pasar por él o ella, puesto que tendrías que también imitar su firma. Luego cuando hablamos de autenticación nos referimos al procedimiento de comprobación de la identidad del usuario.

Ahora te reto a que reflexiones sobre las formas que conoces para identificar a las personas. La forma más antigua es **porque ya le conoces**. Es decir, identificas sus rasgos personales con esa persona. Otra forma habitual de identificación es por contraseña, por ejemplo, tu usuario y contraseña en el equipo de casa. Y la última forma de identificar a las personas es por algo que llevan, por ejemplo, el DNI. Pues bien, al DNI, a la contraseña y a los rasgos personales se les llama **entidades**. Luego estamos realizando la autenticación (diciendo que la persona que porta la entidad es la que dice ser) a través de una entidad.

Si generalizamos, una entidad es:

- Algo que tienes. Por ejemplo la llave de casa.
- Algo que sabes. El PIN de tu tarjeta de crédito.
- Algo que eres. Alto o alta, delgado o delgada, ojos azules…

Autoevaluación

Relaciona la clasificación de entidades para reconocer a personas con ejemplos de éstas.

Ejercicio de relacionar

Algo que la persona…	Relación	Propiedades
Sabe	☐	1. Tarjeta.
Es	☐	2. Password.
Posee	☐	3. Pelirrojo o pelirroja.

Enviar

Las personas llevan tarjetas que las identifican, saben contraseñas que les permiten el acceso y tienen unas características personales que les definen.

Sistemas Biométricos e Identificación Personal.

Si buscas biometría en el diccionario encontrarás que es el estudio de los métodos que permiten reconocer a seres humanos fundamentándose en factores genéticos o en determinados rasgos físicos o de conducta.

Pero si de personas estamos hablando, tendremos que tener en cuenta que las personas, pierden o extravían lo que poseen, o bien, olvidan o confunden lo que memorizan. Con lo cual, hay que tener en cuenta que ambas autenticaciones tienen problemas:

Ejemplos autenticación

Autenticación por posesión: Lo que alguien posee puede ser sustraído, perdido, olvidado, extraviado (descolocado)... Cuando el medio cae en manos de personas no autorizadas, éstas adquieren los "privilegios" de las autorizadas.	**Autenticación por conocimiento:** Lo que se sabe o memoriza puede ser olvidado, ser confundido, ser unificado o ser asociado a datos externos. Ej.: 25% de las personas que poseen tarjetas de cajero (crédito o débito) escriben su PIN en lugares fácilmente accesibles (la cartera, la pantalla del PC, notas en casa, la propia tarjeta, etc.).

Podemos afirmar pues que el problema es que NO se puede distinguir al usuario impostor con posesión y/o conocimiento del medio de seguridad utilizado (password, PIN, etc.).

Es cuando para resolver el problema podríamos utilizar los rasgos (físicos) de las personas.

Podremos escoger dos tipos de rasgos:

- **Rasgos fisiológicos**: huellas dactilares, geometría de la mano/dedo, iris, ADN, etc.
- **Rasgos del comportamiento**: voz, firma, modo de teclear, modo de andar, etc.
  Este tipo de autenticación se llama autenticación biométrica y casi todo son ventajas:
  - No pueden ser sustraídos, perdidos, olvidados o descolocados.
  - Representan una manifestación tangible de lo que alguien es.

Reflexiona

Desde el punto de vista de la seguridad un sistema biométrico es aquel que es capaz de afirmar que la persona que intenta acceder es quién dice ser. ¿Cómo una máquina puede hacer este reconocimiento?

Mostrar retroalimentación

Una máquina hace un reconocimiento de una persona mediante la lectura de una característica física de la misma. Por ejemplo, la huella digital. Los datos físicos recogidos se transforman en datos lógicos mediante fórmulas complejas matemáticas. El resultado de esta transformación siempre el mismo, o con un margen de error muy pequeño.

Autoevaluación

Una desventaja de la autenticación por posesión es:

Olvido. ¿Verdadero o falso?

Sugerencia

○ Verdadero ○ Falso

Verdadero
Sí, para entrar en la oficina tienes que llevar la tarjeta de identificación de la empres y se te olvida en casa, pues NO puedes entrar en la oficina. Es una de las desventajas de la identificación por posesión, el olvido.

Propiedades (ideales) de los Rasgos Biométricos.

Tú eres capaz de reconocer a un amigo instantáneamente, de frente, de perfil, e incluso sólo viendo la parte de atrás de su cabeza, y esto lo haces, aparentemente, sin esfuerzo, abres tus ojos e interpretas el mundo que ves a través de ellos. Puedes entonces pensar que nuestro sistema sensorial es un pequeño científico que genera hipótesis sobre el mundo. Eso precisamente, es lo que queremos que hagan los sistemas de detección biométricos. Que distingan los rasgos de las personas tal y cómo en ellas están definidas. Pero claro, tendremos que escoger uno de estos rasgos y para que sea científicamente válido tendrá que cumplir unas determinadas condiciones:

- **Universalidad:** Toda persona debe poseer dicho rasgo biométrico.
- **Unicidad:** Personas distintas deben poseer rasgos diferenciados / distintos.
- **Permanencia**: El rasgo debe ser invariante con el tiempo a corto plazo.
- **Perennidad:** El rasgo debe ser perpetuo, es decir, invariante con el tiempo a largo plazo (vida de la persona).
- **Mensurabilidad:** El rasgo debe poder ser caracterizado cuantitativamente.

Por cumplir estas características, algunos de estos rasgos biométricos son utilizados por la policía para identificar a las personas desde hace décadas. Vas a ver cómo algunos de ellos se pueden utilizar para controlar el acceso de personas. Te preguntarás si alguno de estos rasgos podrá ser fiable, es decir, que no pueda ser truncado o utilizado de forma fraudulenta. A esto se le llama un **sistema robusto**, y **cómodo**, además de **rápido** para los usuarios. Por último, no tiene que ser peligroso para la salud y/o la integridad física de las personas.

Es igual de importante que los otros tres aspectos citados que la forma de reconocimiento de las personas sean aceptados por éstas de forma voluntaria. Por tanto, la caracterización de los sistemas biométricos se hace en función de:

- **Rendimiento**: precisión en el proceso de identificación.
- **Aceptabilidad**: grado de aceptación/rechazo personal y social del sistema biométrico.
- **Evitabilidad**: capacidad de eludir el sistema mediante procedimientos fraudulentos.

Ahora tendrás que escoger con qué magnitud biométrica te quedas. Y tendrás que decidir si el sistema es lo suficientemente bueno para usarse como identificador de personas o como respaldo de otro sistema de identificación adicional. Por ejemplo, podemos solicitar una identificación adicional a los estudiantes que portan la tarjeta universitario inteligente. Puede ser la huella dactilar. Con esta nueva medida, no hay posibilidad de intercambio de las tarjetas. La persona queda identificada (por su nombre) y autenticada (por su huella dactilar).

Para saber lo bueno que es un sistema biométrico y poder compararlo con otro, establecemos **tres variables.** En conjunto nos darán la velocidad de reconocimiento de la persona (tiempo de verificación), cuántas veces confunde a una persona autorizada con otra que no lo está (falsa aceptación) o, al revés, no permite el acceso a una persona autorizada aún cuando ésta es quién dice ser (falso rechazo):

- **Tasa de falso rechazo:** Posibilidad de que un dispositivo biométrico no reconozca a una persona autorizada.
- **Tasa de falsa aceptación:** Probabilidad de que un dispositivo biométrico permita entrar a una persona no autorizada.
- **Tiempo de verificación / desempeño:** Tiempo de verificación es el tiempo que tarde el sistema en identificar al individuo una vez que éste ha presentado la variable biométrica al lector. Desempeño es el tiempo total que la persona emplea en el control de acceso, desde que llega al lugar hasta que es admitida y tecleado su código y el sistema de apertura se ha puesto en funcionamiento.

Autoevaluación

Relaciona rasgo de una persona que la caracteriza con la propiedad que posee escribiendo el número asociado a la propiedad que le corresponda en el hueco correspondiente.

Ejercicio de relacionar

Rasgo	Relación	Propiedades
El color de los ojos.	☐	1. Mensurabilidad.
La forma de los dientes.	☐	2. Permanencia.
Las sortijas de la mano derecha.	☐	3. Unicidad.

Enviar

El color de los ojos es permanente, pero no es medible y probablemente no sea único. La forma de los dientes de las personas es única, pero es difícilmente medible y no es permanente a lo largo de la vida. Las sortijas son fácilmente medibles, contando cuántas, pero no tienen la propiedad de unicidad, puesto que pueden repetirse en forma y número y además no se llevan permanentemente.

Sistemas Biométricos más utilizados.

Cuando en el instituto le pidieron a Iván que buscara una solución al chequeo de horarios y control de asistencia del personal al **TSCI** para evitar que un visitante marque la entrada de otro pensó que la mejor opción era implementar un sistema que utilizara un lector de Huellas digitales. Con ella, podrá marcar la hora de entrada y salida de los visitantes ya que se puede utilizar tanto en puertas como en ordenadores, como segundo sistema de verificación. Además, del sistema de usuario y la contraseña.

Huellas

La huella es la misma a lo largo de la vida. Aunque heridas en los dedos pueden impedir una lectura correcta de la misma y sí que cambia de tamaño, creciendo la huella a medida que persona se desarrolla. Suelen tener una tasa de falso rechazo menor del 1% y una tasa de falsa aceptación del 0.0001%. Un promedio de tiempo de verificación de 0.5 segundos. Es el sistema más barato del mercado para control de acceso.

Manos

Los sistemas de reconocimiento que utilizan la mano, la pueden utilizar de diferentes maneras. El sistema más fiable es el que utiliza el entramado de venas de ella, que es el mismo a lo largo de la vida de la persona y es diferente en todo el mundo.

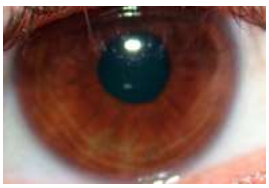
Otros sistemas utilizan la geometría de la mano, su tamaño, forma de la palma y de los dedos.

La mano es leída con maquinaría óptica. Esta maquinaria lleva asociado unos algoritmos que crean patrones a partir de los datos leídos. Esta maquinaria está integrada en un lector de control de acceso en el cual se introduce la mano.

La tasa de falso rechazo es la misma que la tasa de falsa aceptación y la tasa de error: 0,1%. El tiempo de verificación ronda el segundo.

Los últimos sistemas de reconocimiento de la mano introducen un sistema que evalúa una imagen tridimensional de parte de la misma, por ejemplo cuatro dedos y parte de la palma de la mano. Estos sistemas son los más utilizados dentro del control de acceso de personas.

Ojos



El iris es la parte del ojo que tiene color y es inalterable a lo largo de la vida, como también lo son las venas de la retina del ojo. Ambos son usados para la identificación de las personas. El reconocimiento de las venas de la retina del ojo se utiliza desde 1982 y tiene un 0.4% de tasa de falso rechazo. Sin embargo, la tasa de aceptación es de 0,001%. El tiempo de verificación oscila entre 1.5 y 4 segundos, esta variación depende del número de usuarios y usuarias y puede funcionar de forma autónoma o en red e ir asociada al uso de tarjetas. Sin embargo, los datos del reconocimiento del iris, se utilizan desde 1994 con unas estadísticas mucho mejores: menos de 0,001% de tasa de falso rechazo y falsa aceptación. El tiempo de verificación es entorno a 2segundos y puede funcionar de forma autónoma o en red.

Voz

¿Reconoces las voces de tus amigos y familiares al teléfono? Se puede reconocer la voz utilizando los tonos graves y agudos, las distintas vibraciones de la laringe o los tonos nasales para reconocer la identidad de las personas. Muchas compañías han intentado realizar sistemas de reconocimiento de voz, pero son pocas las que actualmente se encuentran en el mercado. Para reconocer la voz se colocan teléfonos en los puntos de acceso que se enlazan con un ordenador central, que es el que realiza la verificación. Es un sistema que no puede funcionar de forma autónoma, debe funcionar siempre en red y del que no hay estadísticas sobre tasas de falso rechazo o falsa aceptación. El tiempo de verificación se estima en 1,5 segundos.

Autoevaluación

Teniendo en cuenta los datos que acabas de leer sobre los sistemas biométricos de reconocimiento de personas. ¿Cuál es el más rápido?

- ○ Manos.
- ○ Iris.
- ○ Voz.
- ○ Huella dactilar.

No es correcta. Un segundo es poco tiempo, pero hay sistemas más rápidos aún.

Falso. Este es el sistema más lento. Hay sistemas más rápidos que tardan menos de los 2 segundos que se tardan en leer el iris.

Incorrecta. Hay sistemas con mejores tiempos que los 1,5 segundos que se tardan en reconocer la voz.

Correcta. El más rápido son las huellas dactilares con 0,5 segundos.

Solución

1. Incorrecto
2. Incorrecto
3. Incorrecto
4. Opción correcta

Autoevaluación

¿Cuáles de los siguientes sistemas son más fiables de reconocimiento de personas?

- ○ Geometría de la mano.
- ○ Voz.
- ○ Retina.
- ○ Huella dactilar.

No es correcta. Los sistemas de reconocimiento de geometría no son los más fiables, pues la mano crece a lo largo de la vida.

Falso. Los sistemas de reconocimiento de la voz no son los más fiables, pues el tono de la voz se puede imitar.

Correcta. Los más fiables son los sistemas de reconocimiento de retina, pues es invariable a lo largo de la vida.

Incorrecta. Los sistemas de reconocimiento de huella dactilar no son los más fiables, pues el dedo crece a lo largo de la vida.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

Políticas, Planes y Procedimientos de Seguridad.

Caso Práctico

-Hola Juan, soy Ignacio, llamo para felicitarte. Mi jefe está muy contento con el sistema de control de acceso, un éxito.

- Me alegro mucho, gracias a Julia que nos habló de la experiencia en la universidad sobre este tema.

-Bueno, agradéceselo de mi parte. Por cierto, me acaba de llegar un fax del instituto donde estuvimos el otro día.

-¿Qué quieren?

-Pues se han enterado del robo de los tres portátiles en nuestra empresa y el jefe de estudios quiere que exista por escrito cuáles son las normas de funcionamiento para los sistemas de seguridad establecidos, es decir, qué es lo que se espera que suceda en un día normal. También saber cómo y cuándo se vigila lo que graban las cámaras de seguridad. Y qué tienen que hacer los vigilantes para demostrar que han estado vigilando.

-No lo entiendo muy bien, ¿quieren dejar por escrito cómo funciona el sistema de seguridad de las cámaras?, ¡pero si llevan más de dos años con él y lo saben de sobra!

-Ya pero el personal cambia y estos dos primeros años las cámaras han sido disuasorias. Ahora quieren establecer quién está al mando de las cámaras para que siempre haya alguien mirando la pantalla. Además, quieren que redactemos una guía de cómo se utilizan los recursos del instituto, es decir, los ordenadores.

-Bueno, bien, entiendo que es poner por escrito lo que les hemos dicho de palabra. Me pregunto ¿para qué?

-Pues creo que quieren saber qué tal está funcionando y comprobar que funciona bien o mal al final de curso e ir mejorando la guía poco a poco.

Hoy es imposible hablar de un sistema cien por cien seguros, sencillamente porque el costo de la seguridad total es muy alto, recuerda que hablaremos de fiabilidad.

Al igual que la universidad de Cantabria, algunas organizaciones gubernamentales y no gubernamentales internacionales han desarrollado documentos, directrices y recomendaciones que orientan en el uso adecuado de las nuevas tecnologías. El fin es obtener el mayor provecho y evitar el uso indebido de las mismas, lo cual puede ocasionar serios problemas en los bienes y servicios de las empresas en el mundo.

En este sentido, las Políticas de Seguridad Informática **(PSI)**, surgen como una herramienta organizacional para concienciar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos.

De acuerdo con lo anterior, el proponer o identificar una política de seguridad requiere:

- Un alto compromiso con la organización.
- Agudeza técnica para establecer posibles fallos y debilidades.
- Constancia para renovar y actualizar dicha política.
- Considerar el dinámico ambiente que rodea las organizaciones modernas.

Llegados a este punto podemos definir una "Política de Seguridad" como un conjunto de requisitos definidos por los responsables de un sistema, que indica en términos generales lo que está y lo que no está permitido en el área de seguridad durante la/las operación/es general/es del sistema.

Para saber más

La Universidad de Cantabria ha creado unas "Políticas generales de uso de las Salas y Aulas de Informática" y un "Reglamento de Uso de Recursos de Tecnologías de la Información y las comunicaciones". En estos documentos verás cómo se tratan los aspectos de seguridad del personal y otros como la privacidad de los usuarios, los manuales de políticas y procedimientos, la sensibilización de los usuarios.

Normativa General de las Aulas y Salas de Informática de la Universidad de Cantabria

Reglamento de Uso de Recursos de Tecnologías de la Información y las Comunicaciones en la Universidad de Cantabria

Elementos de las políticas de seguridad.

Si abrimos la puerta de nuestra casa y nos encontramos dentro una persona que no conocemos, en seguida nos surgen algunas preguntas, ¿quién es esa persona?, ¿cómo ha entrado en la casa y cuándo entró?, o ¿cuánto tiempo lleva dentro de la casa?

Claro que podemos añadir preguntas cuando estas tres hayan sido contestadas, pero **quién, cuándo y cómo** son las tres preguntas fundamentales cuya respuesta será lo que conforme la política de seguridad. Quién entra, cómo ha entrado y cuándo entró y salió de las dependencias de nuestro centro de datos o del lugar que deseamos proteger.

Si hablamos de informática, lo que tenemos que proteger es el lugar donde se encuentran los datos y recursos que compartimos.

El caso más habitual en las empresas es un **NAS (**Network Attached Storage) es el nombre dado a la tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento de un computador con ordenadores personales o servidores clientes a través de una red. Aquí, los empleados y empeladas guardan sus ficheros personales y comparten información. Quién, cuándo y cómo accede a ese NAS es algo que debe ser controlado por el administrador en función de la política de seguridad establecida por la empresa. Por ejemplo, en la tabla puedes ver una de las normas más elementales para el NAS, el horario en el que los empleados y empleadas pueden acceder a él. Este horario normalmente coincide con el horario de la empresa. Fuera de él, el empleado o empleada no debería necesitar dicha información, por tanto, es una norma general de seguridad cerrar el acceso a ese usuario cuando no lo va a usar.

La **RFC 1244** define Política de Seguridad como: "una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requerirán".

La política se refleja en una serie de normas, reglamentos y protocolos a seguir, donde se definen las medidas a tomar para proteger la seguridad del sistema. Pero, ante todo, una política de seguridad es una forma de comunicarse con los usuarios y usuarias. Siempre hay que tener en cuenta que la seguridad comienza y termina con personas y debe:

- **Ser holística** (cubrir todos los aspectos relacionados con la misma). No tiene sentido proteger el acceso con una puerta blindada si a ésta no se la ha cerrado con llave.
- **Adecuarse a las necesidades y recursos.** No tiene sentido adquirir una caja fuerte para proteger un lápiz.
- **Ser atemporal**. El tiempo en el que se aplica no debe influir en su eficacia y eficiencia.
- **Definir estrategias y criterios generales** a adoptar en distintas funciones y actividades, donde se conocen las alternativas ante circunstancias repetidas.

Cualquier política de seguridad ha de contemplar los elementos claves de seguridad ya mencionados: la Integridad, Disponibilidad, Privacidad y, adicionalmente, Control, Autenticidad y Utilidad.

No debe tratarse de una descripción técnica de mecanismos de seguridad, ni de una expresión legal que involucre sanciones a conductas de los empleados y empleadas. Es más bien una descripción de lo que deseamos proteger y el porqué. En este sentido, las Políticas definen **"qué"** se debe proteger en el sistema, mientras que los Procedimientos de Seguridad deben describir **"cómo"** se debe conseguir dicha protección.

En definitiva, si comparamos las Políticas de Seguridad con las Leyes en un Estado de Derecho, los Procedimientos serían el equivalente a los Reglamentos aprobados para desarrollar y poder aplicar las Leyes. Y serán completados ambos documentos con los procedimientos de seguridad donde se detallen los pasos necesarios para implementar cada operación.

Autoevaluación

Podemos definir una Política de Seguridad como:

- ○ Una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran.
- ○ Conjunto de decisiones que definen cursos de acción futuros, así como los medios que se van a utilizar para conseguirlos.
- ○ La definición detallada de los pasos a ejecutar para llevar a cabo unas tareas determinadas.

Correcta. En la RFCs 1244 se habla de lo que es una política de seguridad.

Incorrecta. Esto no es la política de seguridad sino el plan de seguridad que permite e implantar las Políticas de Seguridad.

No es correcta. Esto es el procedimiento de seguridad, que permiten aplicar las Políticas de Seguridad que han sido aprobadas por la organización.

Solución

1. Opción correcta
2. Incorrecto
3. Incorrecto

Características deseables de las Políticas de Seguridad.

Quizás en este momento te sea de gran utilidad ver un ejemplo de política de seguridad, junto con los procedimientos y las tareas que éstas llevan asociadas en el plan de seguridad.

Política de seguridad

Política	Procedimiento	Plan
Protección del servidor web del instituto contra accesos no autorizados.	Actualización del software del servidor Web.	Revisión diaria de los parches publicados por el fabricante del software. Seguimiento de las noticias sobre fallos de seguridad.
	Revisión de los registros de actividad en el servidor.	Revisión semanal de los "logs" del servidor para detectar situaciones anómalas. Configuración de alertas de seguridad que permitan reaccionar de forma urgente ante determinados tipos de ataques e intentos de intrusión.

Y ahora vamos a crear una política de seguridad, la tarea se hace más sencilla si tenemos en mente un ejemplo. Imaginemos el servidor web de un instituto. En este servidor web se encuentran alojadas la página web del instituto, de la biblioteca y un gestor de contenidos o intranet.

- **Primer paso:** Lo más recomendable es crear unas guías de cómo realizar cada una de las tareas para aquellas personas que las llevan a cabo. Al mismo tiempo crear otras guías para usuarios con las directrices de lo que se considera un uso aceptable del sistema. Además, hay que instalar el hardware y software necesario para reforzarlas con otras que indiquen cuál es la forma que se espera que los usuarios. Por otra parte, habrán de instalarse y configurarse el hardware o software de seguridad necesario.
- **Segundo paso**: Definir claramente las responsabilidades exigidas al personal con acceso al sistema: técnicos, analistas y programadores, usuarios finales, directivos, personal externo a la organización.
- **Tercer paso**: Debe cumplir con las exigencias del entorno legal.
- **Cuarto paso:** Revisar de forma periódica las políticas de seguridad para poder adaptarlas a las nuevas exigencias de la organización y del entorno tecnológico y legal.
- **Quinto paso:** Aplicación del principio de "Defensa en profundidad": definición e implantación de varios niveles o capas de seguridad.
- **Sexto paso:** Asignación de los mínimos privilegios. Los servicios, las aplicaciones y usuarios del sistema deberían tener asignados los mínimos privilegios necesarios para que puedan realizar sus tareas. La política por defecto debe ser aquella en la que todo lo que no se encuentre expresamente permitido en el sistema estará prohibido. Las aplicaciones y servicios que no sean estrictamente necesarios deberían ser eliminados de los sistemas informáticos.
- **Séptimo paso:** Configuración robusta ante fallos. Los sistemas deberían ser diseñados e implementados para que, en caso de fallo, se situaran en un estado seguro y cerrado, en lugar de en uno abierto y expuesto a accesos no autorizados.
- **Octavo paso**: Las Políticas de Seguridad no deben limitarse a cumplir con los requisitos impuestos por el entorno legal o las exigencias de terceros, sino que deberían estar adaptadas a las necesidades reales de cada organización. Es importante que se reflejen las características específicas de cada empresa o institución en las políticas, pues los entornos de una a otra pueden ser muy cambiantes.

Autoevaluación

Cuál de las siguientes NO es una características deseables de las políticas de seguridad:

- ○ Analizar con antivirus todo el correo que reciban.
- ○ Control de acceso físico al sitio donde se encuentra los ordenadores.
- ○ Políticas de seguridad a nivel de Sistema Operativo.
- ○ Suspender una semana sin empleo y sueldo a cualquier empleado que revele su contraseña.

No es correcto. Esta sí es una característica deseable de la política de seguridad.

Falso. Esta sí es una característica deseable de la política de seguridad.

Incorrecta. Esta sí es una característica deseable de la política de seguridad.

Correcta. Las penalizaciones no deben formar parte de las políticas de seguridad.

Solución

1. Incorrecto

2. Incorrecto
3. Incorrecto
4. Opción correcta

Definición e Implantación de las Políticas de Seguridad.

Cuando definitivamente Iván se dispuso a implantar la política de seguridad tuvo en cuenta los recursos, instalaciones y procesos a los que afectaba, marcando claramente los objetivos y prioridades.

La Dirección en todo momento le ayudó a identificar todos los elementos que forman parte de la política, tanto elementos físicos como lógicos. Analizó y gestionó los posibles riesgos, asignó responsabilidades, definió qué se puede y qué no se puede hacer si eres un usuario o usuaria del sistema.

Por otra parte, identificó las medidas, normas y procedimientos de seguridad a implantar, y cómo gestionar los incidentes. Para ello, diseñó un plan de contingencia cumpliendo en todo momento la legislación vigente, y por último, definió las posibles violaciones y las consecuencias derivadas del incumplimiento de las políticas de seguridad.

Otro factor importante es determinar qué personas están implicadas en las Políticas de seguridad y no menos importantes son los documentos que hay que crear, en los cuales debe figurar información similar a la reflejada en este formulario:

En los procedimientos será necesario especificar además de lo arriba indicado, estos otros conceptos:

- Descripción detallada de las actividades que se deben ejecutar.
- Personas o departamentos responsables de su ejecución.
- Momento y/o lugar en que deben realizarse.
- Controles para verificar su correcta ejecución.

Autoevaluación

Cuál de las siguientes NO deben tenerse en cuenta al implantar una política de seguridad:

- ○ Analizar y gestionar los posibles riesgos, y asignar responsabilidades.
- ○ Identificar las medidas, normas y procedimientos de seguridad a implantar.
- ○ Gestionar los incidentes.
- ○ Describir detalladamente las actividades que se deben ejecutar.

No es correcta. La gestión y el análisis de los posibles sí debe forma parte del procedimiento no de la política de seguridad. Igualmente que la asignación de responsabilidades.

Falso. La identificación de medidas, normas y procedimientos sí debe forma parte del procedimiento no de la política de seguridad.

Incorrecta. La gestión de los incidentes sí debe forma parte del procedimiento no de la política de seguridad.

Correcta. La descripción detallada de las actividades que se deben ejecutar forma parte del procedimiento no de la política de seguridad.

Solución

1. Incorrecto
2. Incorrecto
3. Incorrecto
4. Opción correcta

Inventario y Auditoría.

Todo ha de estar bien inventariado, desde los recursos hardware, como ordenadores hasta los lugares donde la información está almacenada, bases de datos, archivos, documentos, etc. Por tanto, la implantación de los distintos elementos de las Políticas de Seguridad requiere de un inventario previo y del mantenimiento de un registro actualizado de los recursos del sistema informático. El conjunto de recursos que podrás encontrar en la organización son: equipamiento de hardware y de comunicaciones, software, datos, documentación, manuales, consumibles, etc.

Asimismo, será necesario que identifiques los distintos puntos de acceso a la red y los tipos de conexiones utilizadas, tales como:

- **Centros de tratamiento y locales** donde se encuentren ubicados los servidores/computadoras o se localizan medios de almacenamiento con copias de los datos.
- **Puestos de trabajo**, bien locales o remotos, desde los que se pueda tener acceso a los ficheros con datos de carácter personal.
- Servidores, computadoras personales, laptops, agendas electrónicas, impresoras y otro **equipamiento informático.**
- **Sistemas operativos** y aplicaciones informáticas instaladas.
- Infraestructura de **red de datos y de comunicaciones** de la organización.
- **Documentación y manuales** de las aplicaciones y dispositivos del sistema informático.
- **Bases de datos**, archivos y documentos…

El inventario de los distintos recursos te facilitará el posterior análisis de las vulnerabilidades del sistema informático, identificando los posibles objetivos de los ataques o intentos de intrusión.

Es importante que distingas entre los servicios ofrecidos para las usuarias y usuarios internos y para los externos. Así, los responsables de la organización podrán definir las condiciones de uso aceptable para cada uno de estos servicios. También las áreas o departamentos se van a encargar de ofrecer los distintos servicios y qué personas serán las responsables de administrar y supervisar cada uno de estos servicios.

Realización de pruebas y auditorías periódicas.

La realización de pruebas y auditorías periódicas de seguridad constituyen un elemento de gran importancia para poder comprobar la adecuada implantación de las directrices y medidas definidas en las Políticas de Seguridad.

Debes conocer

Intrusión, vulnerabilidades, ingeniería social, son algunos de los aspectos que se deben tratar en las auditorías de seguridad. Lee la presentación sobre auditorías para aprender más al respecto.

Auditoría de seguridad.

0:00 / 0:34

Elementos de las Políticas de Seguridad.

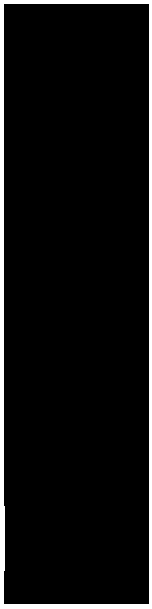
¿Te has planteado ya realizar una política de seguridad? A veces es mejor empezar por un plan de seguridad sencillo, por ejemplo, la política de seguridad de tu portátil (suponiendo que tengas uno). Seguro que hay políticas no escritas sobre el mismo. Como quién es el responsable de autorizar el acceso al mismo, bueno dicho así suena extraño, pero casi seguro que esa persona eres tú. Es decir, tú dices quién puede usar o no el ordenador. ¿Y si un amigo o amiga te lo pidiera prestado? ¿Le harías algunas advertencias o le avisarías para que no hiciera determinadas acciones con él? Evidentemente, quieres que cuando te lo devuelva, esté igual que se lo dejaste…, bueno pues todos estos aspectos son los mismos que hay que considerar en las políticas de seguridad.

Vamos a ponernos manos a la obra, ahora tenemos que **desarrollar la política de seguridad.** Son muchos los aspectos que tenemos que considerar, así que lo haremos analizando cada uno de ellos: personal, adquisición de productos, instalaciones… Y dentro de cada uno de ellos, desglosaremos todos los aspectos posibles, explicando con mayor profundidad los más habituales.

Debes conocer

Son muchos los elementos de las políticas de seguridad que tenemos que tener en cuenta. Desarrollar una política de seguridad supone conocer todos los puntos que en ella se pueden incluir. En la siguiente presentación tienes desarrollados todos los puntos de una política de seguridad.

Elementos de las políticas de seguridad.



0:00 / 3:09

"Cuando no ocurre nada, nos quejamos de lo mucho que gastamos en seguridad. Cuando algo sucede, nos lamentamos de no haber invertido más... Más vale dedicar recursos a la seguridad que convertirse en una estadística".

Autoevaluación

Cuál de las siguientes NO deben tenerse en cuenta al controlar la impresora en red:

- ○ Limitar y controlar accesos mediante contraseña.
- ○ Controlar cuánto dura el tóner escribiendo la fecha en que fue reemplazado en el mismo tóner.
- ○ Establecer el horario de oficina cómo el único plausible para imprimir.
- ○ Los empleados no pueden compartir impresoras.

No es correcta. La limitación es necesaria y establecer una contraseña para acceder a la impresora es una buena política de seguridad.

Correcta. El gasto de tóner NO forma parte de la política de seguridad de la empresa, pues no pone en peligro la integridad de los datos.

Falso. No poder imprimir cuándo la oficina está cerrada es una buena política de seguridad.

Incorrecta. Saber quién puede utilizar la impresora y desde qué equipo lo hace es una buena política de seguridad.

Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

Anexo.- Licencias de recursos.

Licencias de recursos utilizados en la Unida

Recurso (1)	Datos del recurso (1)	Recurso (2)
	Autoría: David Goehring. Licencia: CC BY. Procedencia: http://www.flickr.com/photos/carbonnyc/2294144289/	
	Autoría: Alessandro Quisi. Licencia: CC BY-NC-SA 2.5. Procedencia: http://recursostic.educacion.es/bancoimagenes/ArchivosImagenes/DVD03/CD05/880__21_a_1.jpg	
	Autoría: Plan de Alfabetización Tecnológica Extremadura. Licencia: cc by-nc-nd. Procedencia: http://www.flickr.com/photos/patextremadura/4643852621/	
	Autoría: José Alberto Bermúdez. Licencia: CC BY-NC-SA 2.5. Procedencia: Montaje sobre: http://recursostic.educacion.es/bancoimagenes/ArchivosImagenes/DVD19/CD07/175529_jpg_1.jpg	
	Autoría: Francisco Javier Martínez Adrados. Licencia: CC BY-NC-SA 3.0. Procedencia: http://recursostic.educacion.es/bancoimagenes/ArchivosImagenes/DVD12/CD01/19584__54_m_1.jpg	
	Autoría: Alberto Arribas Merino. Licencia: CC BY-NC-SA 3.0. Procedencia: http://recursostic.educacion.es/bancoimagenes/bancoimagenes/ArchivosImagenes/DVD13/CD05/25270__133_a_1.jpg	
	Autoría: Margarita Irene Marín. Licencia: CC BY-NC-SA 2.5. Procedencia: http://recursostic.educacion.es/bancoimagenes/ArchivosImagenes/DVD27/CD02/196315_jpg_1.jpg	
	Autoría: Javier Eleta Salazar. Licencia: CC BY-NC-SA 2.5. Procedencia: http://recursostic.educacion.es/bancoimagenes/ArchivosImagenes/DVD21/CD05/180293_a_1.jpg	

iButton, Touch Memories o Llaves Electrónicas de Contacto.

Buscando una alternativa a las tarjetas de magnéticas, aparecieron las llaves electrónicas de contacto, resistentes a campos electromagnéticos y al calor. Además, van bien aisladas en carcasas metálicas, cubiertos de material plástico. Este las hace invulnerables al polvo y la suciedad. Al ser del tamaño de una llave, las puedes llevar en el mismo llavero con las otras llaves.

Se llaman las **Smart Locks** de la empresa KwikSet, y es una familia de productos que permitirá que desde cualquier parte del mundo puedas:

- Cerrar o abrir la cerradura.
- Verificar si la cerradura está abierta o cerrada.
- Ver los horarios cuando ésta fue abierta/cerrada.
- Recibir notificaciones por email cuando es abierta/cerrada.

Además, puedes asignar diferentes códigos para diferentes personas, lo que significa que no solo puedes saber los horarios en cuando las diferentes puertas son abiertas y/o cerradas, sino que también por quien.

Para saber más

En este enlaces verás algo que casi seguro que ya habías pensado, existiendo varias empresas que facilitan esta funcionalidad. Te permite monitorear y manipular por Internet las cerraduras de tu casa, y de una manera bastante completa y elegante.

La cerradura inteligente para abrir y cerrar tu casa con el móvil

SmartLocks de Kwikset

Debes conocer

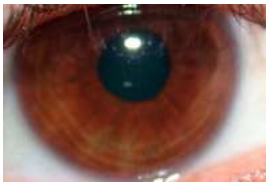
Vídeo donde se puede ver el modus operandi del ibutton.

Funcionamiento de ibutton. Ejemplo de ibutton

Comparación de Métodos Biométricos.

Son tantos los métodos biométricos que hay en el mercado que encontrar cuál es el que más nos conviene resulta difícil. Decidirse por uno en concreto supone haberlos comparado con los otros. Para compararlos tenemos que conocer datos concretos y comparables de cada uno de ellos.

Puedes utilizar las variables conocidas de fiabilidad, facilidad de uso y aceptación. Y complementarlas con los usos habituales de esos sistemas. Otra característica importante para decidir es ver cuáles son las interferencias o inconvenientes que presentan cada una de ellas. Y por último, si el sistema identifica a la persona, o identifica y además "autentica", es decir, comprueba que la persona es quién dice ser.

	Ojo - Iris. 	**Huellas dactilares.** 	**Geometría de la mano.** 	**Voz.** 
Fiabilidad.	Muy Alta.	Alta.	Alta.	Alta.
Facilidad de uso.	Media.	Alta.	Alta.	Alta.
Prevención de ataques.	Muy Alta.	Alta.	Alta.	Media.
Aceptación.	Media.	Media.	Alta.	Alta.
Identificación y autenticación.	Ambas.	Ambas.	Autenticación.	Autenticación.
Interferencias.	Gafas.	Suciedad, heridas, asperezas.	Artritis, reumatismo.	Ruido, resfriados.
Utilización.	Instalaciones nucleares, servicios médicos, centros penitenciarios.	Policía, industrial.	General.	Accesos remotos en bancos o bases de datos.

Para saber más

A continuación se presenta un interesante artículo sobre el uso de las huellas dactilares en los smartphones, y se debate sobre su seguridad.

¿Esta tu smartphone bien protegido con la huella dactilar?

Debes conocer

En este vídeo podrás escuchar cómo Alvy del blog www.microsiervos.com, cuenta de manera amena y muy rápida alguno de los sistemas de identificación biométrica.

Entrevista a Alvy de microsiervos.com.

«Sistemas de Identificació...