Podemos definir qué es la seguridad informática como el proceso de prevenir y detectar el uso no autorizado de un sistema informático. Implica el proceso de proteger contra intrusos el uso de nuestros recursos informáticos con intenciones maliciosas o con intención de obtener ganancias, o incluso la posibilidad de acceder a ellos por accidente.

La seguridad informática es en realidad una rama de un término más genérico que es la seguridad de la información, aunque en la práctica se suelen utilizar de forma indistinta ambos términos. La seguridad informática abarca una serie de medidas de seguridad, tales como programas de software de antivirus, firewalls, y otras medidas que dependen del usuario, tales como la activación de la desactivación de ciertas funciones de software, como scripts de Java, ActiveX, cuidar del uso adecuado de la computadora, los recursos de red o de Internet.

áreas principales que cubre la seguridad informática

Confidencialidad: Sólo los usuarios autorizados pueden acceder a nuestros recursos, datos e información.
Integridad: Sólo los usuarios autorizados deben ser capaces de modificar los datos cuando sea necesario.
Disponibilidad: Los datos deben estar disponibles para los usuarios cuando sea necesario.
Autenticación: Estás realmente comunicándote con los que piensas que te estás comunicando.

Hay también ciberdelincuentes que intentarán acceder a los ordenadores con intenciones maliciosas como pueden ser atacar a otros equipos o sitios web o redes simplemente para crear el caos.

Los hackers: de por sí la palabra es un neologismo utilizado Para referirse a un Experto en las informática. El entendimiento que poseen estos atacantes Es más profundo que el resto de las personas/técnicos, ya que tienen la habilidad De razonar igual o mejor que muchos de los programas o aplicaciones, Y esto en realidad no es tan ilógico, ya que las computadoras y las utilidades que Se encuentran instaladas en ellas fueron creadas por personas.

•Los crackers: cracker viene del inglés "crack" (romper) y Justamente es lo que ellos Hacen. Saben más o menos lo mismo que los hackers pero no comparten la ética. Por consiguiente, no les importa romper una arquitectura o sistema una vez dentro, Ni tampoco borrar, modificar o falsificar algo; es por eso que la teoría habla De que: "los hackers son buenos y los crackers son malos".

• Los lamers: se usa la palabra lamer o lammer para hablar en forma despectiva de De una persona que no posee los mismos conocimientos que tienen los expertos, Pero que conserva la misma intención. Más puntualmente, se denomina de esta manera a la persona que quiere aprender A ser un experto sin siquiera poner Esfuerzo en aprender. Más que nada, es una palabra que usan los hackers o crackers para discriminarse Del "resto" y de los novatos que se quieren iniciar y no saben cómo, ni tampoco Poseen la pasión que los expertos tenían cuando empezaron. Hoy en día, también se emplea la palabra "luser" que es una mezcla del término "loser" (perdedor, fracaso) y el término "user" (usuario).

Phreakers: Los Phreakers son crackers cuya debilidad son los ataques relacionados con empresas telefónicas, sobre todo para obtener llamadas gratis. Circula una leyenda acerca de uno de los primeros individuos de está especie, el Capitán Crunch, capaz de marcar números de teléfono silbando en el auricular los tonos de cada número.

Todos los factores anteriores vuelven a hacer hincapié en la necesidad de que nuestros datos deben permanecer seguros y protegidos confidencialmente. Por lo tanto, es necesario proteger tu equipo y eso hace que sea necesaria y muy importante todo lo que es la seguridad informática.

Medidas para el mantenimiento de la seguridad informática y la prevención de intrusiones

Los ataques más utilizados en contra de un sistema informático son los troyanos, los gusanos y la suplantación y espionaje a través de redes sociales. También son populares los ataques DoS/DDoS, que pueden ser usados para interrumpir los servicios. A menudo algunos usuarios autorizados pueden también estar directamente involucrados en el robo de datos o en su mal uso. Pero si se toman las medidas adecuadas, la gran mayoría de este tipo de ataques pueden prevenirse, por ejemplo a través de la creación de diferentes niveles de acceso, o incluso limitando el acceso físico.

Las medidas de seguridad informática que puedes tomar incluyen:

Asegurar la instalación de software legalmente adquirido: por lo general el software legal está libre de troyanos o virus.
Suites antivirus: con las reglas de configuración y del sistema adecuadamente definidos.
Hardware y software cortafuegos: los firewalls ayudan con el bloqueo de usuarios no autorizados que intentan acceder a tu computadora o tu red.
Uso de contraseñas complejas y grandes: las contraseñas deben constar de varios caracteres especiales, números y letras. Esto ayuda en gran medida a que un hacker pueda romperla fácilmente.

*Cuidado con la **ingeniería social**: a través de las redes sociales los ciberdelincuentes pueden intentar obtener datos e información que pueden utilizar para realizar ataques. Criptografía, especialmente la encriptación: juega un papel importante en mantener nuestra información sensible, segura y secreta.*

Elementos vulnerables en un S.I.

Seguridad es un concepto asociado a la certeza, falta de riesgo o contingencia conviene aclarar que no siendo posible la certeza absoluta el elemento de riesgo está siempre presente independientemente de las medidas que tomemos por lo que debemos hablar de niveles de seguridad, la seguridad absoluta no es posible y en adelante entenderemos que la seguridad informática es un conjunto de técnicas encaminadas a obtener niveles altos de seguridad, la seguridad es un problema integral, los problemas de seguridad informática no pueden ser tratados aisladamente ya que la seguridad de todo el sistema es igual a su punto más débil. El uso de sofisticados algoritmos y métodos es inútil si no garantizamos la confidencialidad de las estaciones de trabajo, por otra parte, existe algo que los hackers llaman ingeniería asociada que consiste simplemente en conseguir mediante un engaño que los usuarios autorizados revelen sus passwords, por lo tanto la educación de los usuarios es fundamental para que la tecnología de seguridad pueda funcionar.

Los 3 elementos principales a proteger en cualquier sistema informático son el software, el hardware y los datos. Por hardware entendemos el conjunto de todos los elementos físicos de un sistema informático como CPU, terminales, cableados, medios de almacenamiento secundarios, tarjeta de red, etc... Por software entendemos el conjunto de programas lógicos que hacen funcionar el hardware tanto sistemas operativos como aplicaciones y por datos el conjunto de información lógica que3 Amenazas Física maneja el software y el hardware como por ejemplo paquetes que circulan por un cable de red o entradas de una base de datos.

Habitualmente los datos constituyen los 3 principales elementos a escoger ya que es el más amenazado y seguramente el más difícil de recuperar. También tenemos que ser conscientes de que las medidas de seguridad que deberán establecerse comprenden el hardware el sistema operativo, las comunicaciones, medidas de seguridad física, controles organizativos y legales.

1.4 Las amenazas.

Las amenazas de un sistema informático pueden provenir desde un hacker remoto que entra en nuestro sistema desde un troyano, pasando por un programa descargando de forma gratuita que nos ayuda a gestionar nuestras fotos pero que supone una puerta trasera a nuestro sistema permitiendo la entrada a espías hasta la entrada no deseada al

sistema mediante una contraseña de bajo nivel de seguridad; se pueden clasificar por tanto en amenazas provocadas por personas, lógicas y físicas. A continuación se presenta a una relación de los elementos que potencialmente pueden amenazar a nuestro sistema. La primera son las personas, la mayoría de los ataques a nuestro sistema van a provenir de forma intencionada o inintencionada de personas y pueden causarnos enormes pérdidas. Aquí se describen brevemente los diferentes tipos de personas que pueden constituir un riesgo para nuestros sistemas:

1 Personas:

Personal (se pasa por alto el hecho de la persona de la organización incluso a la persona ajeno a la estructura informática, puede comprometer la seguridad de los equipos)
Ex-empleados (generalmente se trata de personas descontentas con la organización que pueden aprovechar debilidades de un sistema del que conocen perfectamente, pueden insertar troyanos, bombas lógicas, virus o simplemente conectarse al sistema como si aun trabajaran en la organización)
Curiosos (son los atacantes juntos con los crackers los que más se dan en un sistema)
Hackers (una persona que intenta tener acceso no autorizado a los recursos de la red con intención maliciosa aunque no siempre tiende a ser esa su finalidad)
Crackers(es un término más preciso para describir una persona que intenta obtener acceso no autorizado a los recursos de la red con intención maliciosa)
Intrusos remunerados (se trata de personas con gran experiencia en problemas de seguridad y un amplio conocimiento del sistema que son pagados por una tercera parte generalmente para robar secretos o simplemente para dañar la imagen de la organización)
2 Amenazas lógicas:

Software incorrupto(a los errores de programación se les llama Bugs y a los programas para aprovechar uno de estos fallos se les llama Exploits.)
Herramientas de seguridad (cualquier herramienta de seguridad representa un arma de doble filo de la misma forma que un administrador las utiliza para detectar y solucionar fallos en sus sistemas o la subred completa un intruso las puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar los equipos, herramientas como NESUS, SAINT o SATAN pasa de ser útiles a peligrosas cuando la utilizan Crackers.)
Puertas traseras (durante el desarrollo de aplicaciones grandes o sistemas operativos es habitual que entre los programadores insertar atajos en los sistemas habituales de autenticación del programa o núcleo de sistema que se está diseñando.) Son parte de código de ciertos programas que permanecen sin hacer ninguna función hasta que son activadas en ese punto la función que realizan no es la original del programa si no una acción perjudicial.)
Canales cubiertos (son canales de comunicación que permiten a un proceso trasferir información de forma que viole la política de seguridad del sistema.)

Virus (un virus es una secuencia de código que se inserta en un fichero ejecutable denominado huésped de forma que cuando el archivo se ejecuta el virus también lo hace insertándose a sí mismo en otros programas.)
Gusanos(es un programa capaz de ejecutarse y propagarse por sí mismo a través de redes en ocasiones portando virus o aprovechando bugs de los sistemas a los que se conecta para dañarlos a ser difíciles de programar su numero no es muy elevado pero el daño que causa es muy grave.)
Caballos de troya(son instrucciones escondidas en un programa de forma que este parezca realizar las tareas que un usuario espera de el pero que realmente ejecuta funciones ocultas.), Programas conejo o bacterias(bajo este nombre se conoce a este programa que no hace nada útil si no que simplemente se delimitan a reproducirse hasta que el número de copias acaba con los recursos del sistema produciendo una negación del servicio.

3 Amenazas Físicas: Robos, sabotajes, destrucción de sistemas. Suministro eléctrico. Condiciones atmosféricas. Catástrofes naturales.

1.5 Formas de protección de nuestro sistema:
Para proteger nuestros sistemas hemos de realizar una análisis de las amenazas potenciales, las perdidas que podrían generar y la probabilidad de si ocurrencia a partir de este análisis hemos de diseñar una política de seguridad que defina responsabilidades y reglas a seguir para evitar tales amenazas o minimizar sus efectos en caso de que se produzcan, a esto se le llama mecanismo de seguridad, son la herramienta básica para garantizar la protección de los sistemas o la red. Estos mecanismo se pueden clasificar en activas o pasivas.

Activas> evitan daños en los sistemas informáticos mediante empleo de contraseñas adecuadas en el acceso a sistemas y aplicaciones, encriptación de los datos en las comunicaciones, filtrado de conexiones en redes y el uso de software especifico en seguridad informática.
Pasiva> minimizan el impacto y los efectos causados por accidentes mediante uso de hardware adecuado, protección física, eléctrica y ambiental, realización de copias de seguridad.
Tema 2 Seguridad Física

2.1. Principios de la seguridad física
La seguridad física consiste en la aplicación de barreras físicas, y procedimientos de control como medidas de prevención y contra medidas ante amenazas a los recursos y la información confidencial, se refiere a los controles y mecanismos de seguridad dentro y alrededor de la obligación física de los sistemas informáticos así como los medios de acceso remoto al y desde el mismo, implementados para proteger el hardware y medios de almacenamiento de datos. Cada sistema es único, por lo tanto la política de seguridad a implementar no sera única es por ello siempre se recomendara pautas de aplicación general y no procedimientos específicos.

La seguridad física esta enfocada a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico donde se encuentra ubicado el centro.

Las principales amenazas que se ven en la seguridad física son amenazas ocasionadas por el hombre como robos destrucción de la información , disturbios, sabotajes internos y externos, incendios accidentales, tormentas e inundaciones.

2.1.1 Control de acceso
El control de acceso no solo requiere la capacidad de identificación, sino también asociar la apertura o cierre de puertas, permitir o negar acceso,basado en restricciones de tiempo, área o sector dentro de una organización. Es decir se verificará el nivel de acceso de cada persona mediante aplicación de barreras (llave, tarjeta, password)

El servicio de vigilancia es el encargado del control de acceso, de todas las personas al edificio, este servicio es el encargado de colocar a los guardias en lugares estratégicos para cumplir con sus objetivos y controlar el acceso del personal. A cualquier personal ajeno a la planta se le solicitara completar un formulario de datos personales, los motivos de la visita, hora de ingreso y salida, etc.

El uso de credenciales de identificación es uno de los puntos mas importantes del sistema de seguridad, a fin de poder efectuar un control eficaz de ingreso y salida del personal a los distintos sectores de la empresa, en este caso la persona se identifica por algo que posee por ejemplo una llave, una tarjeta de identificación o una tarjeta inteligente... Cada una de estas debe tener un pin único siendo este el que se almacena en una base de datos que controla el servicio de vigilancia para su posterior seguimiento si fuera necesario. Su mayor desventaja es que estas tarjetas pueden ser robadas, copiadas, etc...

Estas credenciales se pueden clasificar de la siguiente manera:
Normal o definitiva: para el personal permanente de la empresa,
Temporal : para el personal recién ingresado,
Contratistas:personas ajenas a la empresa que por razones de servicio debe ingresar en la misma, visitas: para un uso de horas.
Las personas también pueden acceder mediante algo que saben (un numero de identificación o un password) que se solicitara a su entrada.

Los datos introducidos se contrastaran contra una base de datos donde se almacenan los datos de las personas autorizadas. Este sistema tiene la desventaja que generalmente se elijen identificadores sencillos o bien se olvida o incluso la base de datos pueden ser alteradas o robadas por personas no autorizadas, la principal desventaja de la aplicación del personal de guardia es que este puede llegar a ser sobornado para dar acceso o incluso poder salir con materiales no autorizados, esta situación de soborno puede ocurrir

frecuentemente por lo que es recomendable la utilización de sistemas biométricos para el control de acceso.

2.1.2 Sistemas biométricos
Definimos la biometría como la parte de la biología que estudia de forma cuantitativa la variabilidad individual de los seres vivos utilizando métodos estadísticos. La biometría es una tecnología que realiza mediciones de forma electrónica, guardad compara características únicas, para la identificación de personas.

La forma de identificación consiste en la comparación de características físicas de cada persona, por un patrón conocido y almacenado en una base de datos. Los lectores biométricos que identifican a la persona por lo que es manos, ojos, huellas digitales y voz.

Beneficios de una tecnología biométrica:
Pueden eliminar la necesidad de poseer una tarjeta para acceder y de una contraseña difícil de recordar o que finalmente acabe escrita en una papel y visible para cualquier persona.
Los coste de administración son mas pequeños se realizan un mantenimiento del lector y una persona se encarga de mantener una base de datos. Además las características biometrícas son intransferibles a otra persona.

La emisión de calor: Se mide la emisión de calor del cuerpo (termo-grama) realizando un mapa de valores sobre la forma de cada persona.
Huella digital: Pasado en el principio no existe dos huellas digitales idénticas, este sistema viene siendo usado desde el siglo pasado con excelentes resultados. Cada huella digital posee pequeños arcos, ángulos, bucles, remolinos llamados minucias. Características y la posición de cada una de ellas es lo analizado para establecer la identificación de una persona. Esta testado que cada persona posee 30 minucias y que dos personas no tiene mas de 8 minucias iguales de lo que hace el método sumamente fiable.

Verificación de la voz: La emisión de una o mas frases es grabada y en el acceso se compara la voz, entonación, diptongos, agudeza, etc.... Este sistema es muy sensible a factores externos como el ruido, el estado de animo, enfermedades, envejecimiento, etc

Verificación de patrones oculares: Estos modelos esta basados en los patrones del iris o la retina y en estos momentos son los considerados en lo mas eficaces. Su principal resistencia por parte de las personas a que les analice los ojos por rebelarse en los mismo enfermedades que en ocasiones se quieran mantener en secreto.

Verificación automática de firmas: Mientras es posible para que falsificador producir una buena copia visual o facesinin es extremadamente difícil reproducir la dinámicas de una persona, por ejemplo, las firmas que genuinan con exactitud. Esta técnica usada visiones acústicas toma los datos del proceso dinámico de firmas o de escribir.

La secuencia sonora de emisión acústica generada en el proceso de escribir constituyen un patrón que es único en cada individuo. EL patrón contiene información expresa sobre la manera en que la escritura es ejecutada, el equipamiento de colección de firmas es inherentemente de bajo coste y robusto, excepcionalmente consta de un bloque de metal por un otro material con propiedades acústicas similares y una computadora con bases de datos con patrones de firmas asociadas a cada usuario.

Existe unas otras soluciones a la biometría mas complejas y menos usadas en acceso a organizaciones o a un sistemas informático concreto como son la geometría de las manos y el reconocimiento facial.

Ocular
Huellas
Escritura
Voz
Fiabilidad
Muy alta
Muy alta
Media
Alta
Facilidad de uso
Media
Alta
Alta
Alta
Prevención de ataque
Muy Alta
Alta
Muy Alta
Alta
Aceptación
Media
Alta
Muy Alta
Alta
Estabilidad
Alta
Alta
Baja
Media

<!---

Ojo Huellas Escritura Voz
Fiabilidad Muy alta Muy alta Media Alta
Facilidad de uso Media Alta Alta Alta

Prevención de ataque
Muy alta Alta Media Media
Aceptación Media Alta Muy alta Alta
Estabilidad Alta Alta Baja Media
-->

2.1.3 Protección electrónica
Se llama así a la detección de robo, intrusión, asalto e incendios mediante la utilización de sensores conectados a centrales de alarmas. Estas centrales tienen conectado los elementos de señalización que son los encargados de hacer saber al personal de una situación de emergencia.

Cuando uno de los elementos sensores detectan una situación de riesgo estos transmiten inmediatamente el aviso a la central, esta procesa la información recibida, y ordena en repuesta la emisión de señales sonoras o luminosas alertando de la situación, todos estos elementos poseen un control contra sabotaje de manera que si en algún elemento se corta la alimentación o se produce la rotura de algunos de sus componentes se enviaran una señal a la central de alarma para que esta acciones los elementos de señalización correspondiente.
Las barreras infrarrojas y de microondas: Transmiten y reciben haces de luces infrarrojas y de microondas respectivamente. Se codifican por medio de pulsos con el fin de evadir los intentos de sabotaje. Estas barreras están compuesta por un emisor y un receptor de igual tamaño y apariencia externa. Cuando el haz es interrumpido se activa el sistema de alarma y luego vuelve al estado de alerta, estas barreras son inmunes a fenómenos aleatorios como calefacción, luz ambiental, vibraciones, movimientos de masas de aire, etc
Detector ultrasónico: Este equipo utiliza ultrasonidos para crear un campo de ondas. De esta manera cualquier movimiento, que realice un cuerpo dentro del espacio protegido generara una pertuvacion en dicho campo que accionara la alarma, este sistema posee un circuito refinado que elimina las falsas alarmas, la cobertura puede llegar a un máximo de 40 metros cuadrados.
Circuitos cerrados de televisión (CCTV): Permite el control de todo lo que sucede en la planta según lo captado por la cámaras extrategicamente colocadas. Los monitores de estos circuitos deben estar ubicados en un sector de alta seguridad. Las cámaras pueden estar a la vista para ser utilizadas como medidas disuasivas u ocultas para evitar que el intruso sepa que esta siendo captado.

2.1.4 Condiciones ambientales
Normalmente se recibe por anticipado los avisos de tormentas, tempestades, tifones y catástrofes sísmicas. Las condiciones atmosféricas severas se asocian a ciertas partes del mundo y la probabilidad de que ocurran esta documentada.

La frecuencia y severidad de su ocurrencia debe ser tenidas en cuenta al decidir la construcción de un edificio. La comprobación de los informes meteorológicos o la existencia de un servicio de una tormenta severa permiten que se tomen precauciones adicionales tales como la retirada de objetos móviles, la provisión de calor, iluminación o combustible para la emergencia.

Los incendios: Son causados por el uso inadecuado de combustible, fallo de la instalación eléctricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas. El fuego es una de las principales amenazas contra la seguridad es considerado el enemigo numero uno de las computadoras. Desgraciadamente los sistemas contra fuego dejan mucho que desear causando casi igual daño que el propio fuego. El dióxido de carbono actual alternativa al agua
resulta peligroso para los empleados si quedan atrapados.

Los diversos factores a contemplar para reducir los riesgos de incendios son:
El área en la que se encuentra las computadoras deben estar en un local que no sea combustible o inflamable.
EL local no debe situarse encima o debajo o adyacente a áreas donde se procesen, fabriquen o almacenen materiales inflamables, explosivos o gases tóxicos, o sustancias radioactivas.
Las paredes deben hacerse de materiales incombustibles y extenderse desde el suelo al techo, debe construirse un falso suelo sobre el suelo real con materiales incombustibles y resistentes al fuego, no debe estar permitido fumar en el área de proceso.
El suelo y el techo del CPD y del centro de almacenamiento de medios magnéticos deben ser impermeables, deben instalarse extintores manuales y/o automáticos.
El sistema de aire acondicionado: Se debe proveer de un sistema de calefacción, ventilación y aire acondicionado separado, para que se dedique al cuarto de computadoras y equipos de proceso de datos en forma exclusiva. Es recomendable redes de protección de incendios e inundaciones en todo el sistema de cañerías al interior y exterior, detectores y extintores de incendios, monitores y alarmas efectivas.

Inundaciones: La invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos ocasionada por la falta de drenaje ya sea natural o artificial es una de las causas de mayores desastres en centros de computo. Ademas de las causas naturales de inundaciones pueden existir la posibilidad de una inundación provocada por la necesidad de apagar un incendio en un piso superior. Para evitar este inconveniente se puede tomar las siguiente medidas. Construir techos - habitaciones impermeables y acondicionar las puertas para contener el agua.

Terremotos: Estos fenómenos sin-micos pueden ser tampoco intensos que solo los instrumentos muy sensibles lo detectan o tan intensos que causen destrucción de edificios y asta la perdida de vidas humanas. El problema en la actualidad es que estos fenómenos están ocurrido en lugares donde no se le asociaban.

2.2 Sistemas de alimentación interrumpida
Trabajar con computadoras indica trabajar con electricidad por lo tanto estas es una de las principales asear a considerar en la seguridad física, ademas es una problemática que abarca desde un usuario hogareño hasta la gran empresa.

Un SAI es un dispositivo que gracias a sus baterías puede proporcionarte energía eléctrica tras un apagón a todos los dispositivos que tengas conectados durante un tiempo ilimitado permitiendo poder apagar los equipos sin que sufran fuertes sus fuentes de alimentación. Los dispositivos hardware no irán enchufados a las tomas de corriente directamente se enchufaran al SAI que estará conectado al enchufe, asiendo de este modo el intermediario entre la red eléctrica y los dispositivos hardware.

Otra de las funciones de los SAI es mejorar la calidad de la energía eléctrica que llega a los aparatos filtrando subidas y bajadas de tensión y eliminando armónicos en caso de usar corriente alterna. Los SAI dan energía eléctrica a equipos llamados cargar criticas como pueden ser aparatos médicos, industriales o informáticos que requieren tener siempre alimentación y que esta sea de calidad

2.2.1 Causas y efectos de los problemas de la red eléctrica
El papel de un SAI es suministrar potencia eléctrica en ocasiones de fallo de suministro en un intervalo corto sin embargo muchos sistemas de alimentación interrumpida son capaces de corregir otros fallos de suministro.
Los nueves problemas de la energía son :
Corte de energía o apagones: Es la perdida total de suministro eléctrico causado por relámpagos fallos de la linea de energía, excesos de demandas accidentes y desastres naturales. Pueden causar daños en el equipo electrónico, perdida de datos, o parada del sistema.
Bajada de voltaje momentánea o micro-cortes: Es la caída momentánea del voltaje generada por el arranque de grandes cargas encendidos de maquinarias pesadas o fallos de equipos, se presenta de manera similar a los apagones pero en oleadas repentinas, causa principalmente daños al hardware y perdida de datos.
Ciclo de tensión o altos voltajes momentáneos: Producidos por una rápida reducción de cargas cuando el equipo pesado es apagado, o por voltajes que están por encima del ciento diez por ciento de la nominal, los resultados pueden ser daños irreversibles.
Bajadas de tensión sostenidas: Bajo voltaje sostenido en la linea por periodos largos de unos cuantos minutos, horas y hasta días pueden ser causados por una reducción intencionada de la tensión para conservar energías durante los periodos de mayor demanda. Puede causar daños al hardware principalmente.
Sobrevoltaje o lineas de tensión: sobrevoltaje en la linea por periodos largos. Puede ser causado por un relámpago y puede incrementar el voltaje de la linea hasta 6000 volteos en exceso casi siempre ocasiona perdidas de la información y daños del hardaware.
Ruido eléctrico: Interferencias de alta frecuencia causada por radiofrecuencia o interferencias electromagnéticas, pueden ser causadas por transmisores, maquinas de

soldar, impresoras, relámpagos,.... Introduce errores en los programas y archivos así como daños a los componentes electrónicos.
Variación de frecuencia: Se refiere a un cambio de estabilidad de la frecuencia, resultado de un generador o pequeños sitios de cogeneracion siendo cargados o descargados, puede causar funcionamiento errático de los equipos, perdidas de información, caídas del sistema y daños de equipos.
Transientes o micropicos: Es la caída instantánea del voltaje en el rango de los nanosegundos, la duración normal es mas corta que un pico , puede originar comportamientos extraños y proporcionado estrés en los componentes electrónicos quedando propensos a fallos.
Distorsión armónica: Es la distorsión de la onda normal, causadas por cargas no lineales conectadas a la misma red de los equipos informáticos y/o aplicaciones criticas: maquinas fax, copiadoras, son ejemplos de cargas no lineales puede provocar sobrecalentamiento en los ordenadores errores de comunicación y daño del hardware.

Consecuencias:
Un mal suministro de energía eléctrica afecta a la productividad de las empresas, ya que destruye información, dañan las infraestructuras, generan estrés y generan perdidas.

2.2.2 Tipos de SAIs
Según el tipo de energía eléctrica que producen a su salida hay dos tipos:
SAI de continua: Los equipos o cargas conectados a los SAI requieren una alimentación de corriente continua por lo tanto estos transformaran corriente alterna a la red a corriente continua y la usaran para alimentar a la carga y almacenarla en su batería, por lo tanto no requieren convertidores en la batería y las cargas.
SAI de alterna: Estos SAIs obtienen en su salida una señal alterna por lo que necesitan un inversor para transformar la señal continua que tienen las baterías en una señal alterna. Habitualmente es el tipo de SAI que se comercializa ya que los equipos informáticos requieren corriente alterna para su funcionamiento, la mayoría de los SAI comerciales permiten conexión de red o red local entre PC y el sai para motorizar su estado en el PC mediante el software según los fallos eléctricos que corrigen disponibilidad, habilidad, etc se pueden clasificar en:
SAI offline o interactivo no senoidal (protección nivel 3 equipos básicos): Por su precio es el más extendido, sobre todo para la protección de pequeñas cargas. Estos tipos de sai alimentan las cargas criticas con una seguridad protección relativa dependiendo de tipo offline(estabilizados o/y con o sin filtros). Dentro de una escala de 1 al 100 estarían entre 40-60 en relación a protección. Básicamente los equipos ofline actúan en el momento en que la red desaparece o baja por debajo de los 220 voltios, y produciendo en el cambio de red a baterías un pequeño micro-corte en el cual para una mayoría de equipos eléctricos e informáticos es inapreciable no así para equipos muy sostificados.
SAI on-line y line interactive(protección nivel 5): El SAI on-line cumple verdaderamente para todos los problemas ocasionados por fallos en la compañía eléctrica tanto como por otros problemas ocasionados por las lineas eléctricas dentro de polígonos industriales, y oficinas como puede ser el ruido eléctrico, suele dar una protección de 70-90 sobre 100.

Existen diferentes tipos pero todos cumplen su función dejando pocas ventanas abiertas a posibles problemas.
SAI on-line doble conversión (protección de nivel nueve): La verdadera diferencia de los SAI se encuentra en los equipos ya que off line linea interactiva y on-line de una conversión depende de una u otra manera de la entrada eléctrica al equipo cumpla una mínimas condiciones para el correcto funcionamiento de los equipos. Los equipos de doble conversión no depende de la linea de entrada para trabajar con una doble conversión de eliminando por completo todos los problemas ocasionados por la compañías eléctricas ademas de los problemas meteorológicos.

2.2.3 Potencia necesaria
Para ajustarlas dimensiones y capacidad eléctrica del SAI es necesario realizar un cálculo de la potencia que consumimos y por tanto que necesitamos suministrar.
La potencia eléctrica se define como la cantidad eléctrica o trabajo o que se consume en una determinada unidad de tiempo. Si la tensión eléctrica (voltaje) se mantiene constante la potencia es directamente proporcional a la corriente eléctrica (intensidad en amperios), esta aumenta si la corriente aumenta.

Cuando se trata de corriente continua la potencia eléctrica desarrollada en un cierto instante en un dispositivo de dos terminales es el producto de la diferencia del potencial entre dichos terminales y la intensidad de corriente que pasa a través del dispositivo, este es:

*P=V*I. P expresada en vatios, y expresada en voltios, i expresada en amperios.*

El circuito eléctrico de corriente alterna se emplea medidas de potencia eficaz o aparente y potencia real, la unidad de potencia para configurar un SAI es el voltioamperio(va) que es potencia aparente también denominada potencia efectiva o eficaz. Para calcular cuanta energía requiere tu equipo busca el consumo en la parte trasera o en el manual de usuario, si tenemos la potencia en vatios(potencia real), multiplica la potencia en vatios por 1,4 para tener en cuenta el tipo máximo de potencia que pueda alcanzar su equipo, en ocasiones el factor 1,4 puede ser 1,33 o 1,6 o facto divisor 0,7 o 0,75. Si lo que se encuentra es la tensión y la corriente nominales para calcular la potencia aparente hay que multiplicar la corriente (amperios) por la tensión(voltios) obtenidos la potencia en volteos para luego multiplicar por el factor 1,4.
2.3 Centro de procesos de datos.
Se denomina centro de procesamiento de datos CPD aquella ubicación donde se procesa todos los recursos necesarios para el procesamiento de una organización. También se conoce como centro de computo o centro de calculo, o centro de datos por su equivalente en ingles data center. Dicho recursos consisten esencionalmente en una dependencias debidamente acondicionadas y rede de comunicaciones.

2.3.1 Equipamiento de un CPD

Un CPD por tanto es un edificio o sala de gran tamaño usada para mantener en el una gran cantidad de equipamiento electrónico.

Suelen ser creados y mantenidos por grandes organizaciones con objeto de tener acceso a la información necesaria para sus operaciones. Por ejemplo un banco puede tener un data center con el propósito de almacenar todos los datos de sus clientes y las operaciones que estos realizan sobre sus cuentas. Prácticamente todas las compañías que son medianas o grandes tienen algún tipo de CPD mientras que las mas grandes llegan a tener varios interconectados en distintas ubicaciones
geográficas.

Entre los factores mas importantes que motivan en la creación de CPD se puede destacar garantizar la continuidad y disponibilidad del servicio de clientes, empleados, ciudadanos, proveedores, y empresas colaboradoras pues en estos ámbitos es muy importante o de comuniones implicados como los servidores de bases de datos que puedan contener información critica

Requisitos generales:
Disponibilidad y monitorización 24x7x365:
Fiabilidad infalible los cinco nueves es un 99,99 % de la disponibilidad, lo que se traduce en una hora de no disponibilidad al año. Los CPD deben tener redes y equipos altamente robustos y comprobados.
Seguridad, redundancia y diversificación. Almacenaje exterior de datos, tomas de alimentación eléctrica totalmente independientes y de servicio de telecomunicaciones para la misma configuración equilibrio de cargas, SAI, control de acceso,....
Control ambiental-prevención de incendios: El control del ambiente trata de la calidad de aire, temperatura, humedad, electricidad, control de fuego, y por supuesto acceso físico.
Acceso a Internet y conectividad a redes de área extensa (WAN) para conectividad a internet: Los CPD deben ser capaces de hacer frente a la mejora y avance de equipos de los estándares y ancha de banda exigidos pero sin dejar de ser manejables y fiable.

El diseño de un CPD comienza por la elección de su situación geográfica y requiere un balance entre diversos factores:
Coste económico: Coste de terreno impuesto, municipal, seguro, etc,
Infraestructuras en las cercanías: Energía eléctrica, carreteras, acometidas de electricidad, centralita de comunicaciones.
Riesgo: Posibilidad de inundaciones, incendios, robos, terremotos.

Una vez seleccionada la ubicación geográfica es necesario encontrar unas dependencias adecuadas para su finalidad ya se trate de una local de nueva construcción u otra ya existente a comprar o alquilar.

Algunos requisitos de las dependencias son:

Una buena ubicación son las plantas intermedias o ubicaciones centrales en entornos de campus.
Una planta con altura de suelo a techo de 3 metros, preferiblemente mas. Esto será suficiente para un piso con un falso suelo de 300 a 600 milímetros y proporcionara el suficiente espacio libre para los equipos y racks.
Una ruta de acceso amplia para canalizaciones. Las rutas deben ser grandes y bastantes fuerte para servir como toma de aire, material informático, módulos de fuente de alimentación continua.
Espacio para sala posibles de extensión.
Aun cuando se disponga del local adecuado siempre es necesario algún despliegue de infraestructuras en su interior:
Falsos suelos y techos con placas de techo de vidrio
Todos los cables tendidos bajo el suelo deberían de ser LSZH, doble cableado eléctrico, generadores de distribución eléctrica,
Acondicionamiento de salas: Las paredes del CPD deben tener un grado de resistencia mínimo al fuego de una hora (RF-60) aunque se recomienda un grado RF-120 y deben proporcionar barrera contra al humo.
Todas la puertas de acceso deben tener una ventana con cierre propio.
Todos los materiales utilizados en la construcción en la sala de ordenadores deben ser incombustibles.
Para controlar el daño por agua todas las entradas del piso, de la pared y el techo deben estar selladas.
Los extintores manuales contra el fuego deben ser de dióxido de carbono u otros gases con agente de extinción.No deben haber componentes químicos de extinción, polvo seco en el área de ordenador.
Instalación de alarma, control de temperatura y humedad con avisos SNMP, SNTP o SMS/MMS vía teléfono móvil.

Generalmente en un CPD todos los grandes servidores se suelen concentrar en una sala denominada sala fría, nevera o pecera. Esta sala requiere un sistema especifico de refrigerador para contener una temperatura baja (entre 21º o 23º) necesaria para evitar averías de la computadoras a causas del sobre calentamiento, según las normas internacionales la temperatura exacta debe ser 22,3 grados centígrados. La pecera debe contar con medidas estrictas de seguridad en el acceso físico así como medidas de extinción de incendios adecuadas al material eléctrico tales como extinción por agua nebulizadas o bien por gas inergen, dióxido de carbono o nitrógeno, una parte importante de estas infraestructuras son aquellas a la seguridad física de la instalación lo que incluye:
Cerradura electromagnéticas contratadas por algún mecanismo de control de acceso, tarjeta pin o biometria.
Tornos.
Cámaras de seguridad.
Detectores de movimiento.
Tarjetas de identificación.

Una vez acondicionado el habitáculo se procede a la instalación de las computadoras. Esta tarea requiere un diseño lógico de redes y entornos, algunas actuaciones son:
Instalación y configuración de los servidores.
Despliegue del cableado y configuración de la electrónica de red, pasarelas, encaminadores.
Segmentación de redes locales y creación de redes virtuales.
Creación de zonas desmilitarizados.
Creación de la red de almacenamiento de la información.
Creación de los entornos de explotación, preexplotacion, desarrollo de aplicaciones, y gestión de red.
TEMA 3: SEGURIDAD LÓGICA

3.1 PRINCIPIOS DE LA SEGURIDAD LÓGICA

La mayoría de los daños que puede sufrir un sistema informático no será solo los medios físicos sino contra información almacenada y procesada. El activo mas importante que se posee es la información y por tanto deben existir técnicas mas allá de la seguridad física que la aseguren, estas técnicas las brinda la seguridad lógica.

Es decir que la seguridad lógica consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y solo se permita acceder a ellos a las personas autorizadas para ello.

Los objetivos que se plantean serán:

Restringir el acceso al arranque (desde la BIOS) al S.O, los programas y archivos.
Asegurar que los usuarios puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
Asegurar que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto analizando periódicamente los mismos.

3.2 TÉCNICAS DE CONTROL DE ACCESO
Estos controles pueden implementarse en la BIOS, el S.O, sobre los sistemas de aplicación, en las DB, en un paquete especifico de de seguridad o en cualquier otra aplicación. Constituyen una importante ayuda para proteger al S.O de la red, al sistema de aplicación y demás software de la utilización o modificaciones no autorizadas. Para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con acceso permitido) y para resguardad la información confidencial de accesos no autorizados. Así mismo es conveniente tener en cuenta otras consideraciones referidas a la seguridad lógica como por ejemplo las relacionadas al procedimiento que se lleva a cabo para determinar si corresponde un permiso de acceso

3.2.1 IDENTIFICACIÓN Y AUTENTICACIÓN

Se denomina identificación al momento en que el usuario se da a conocer en el sistema y autenticación a la verificación que se realiza en el sistema sobre esta identificación. Existen 4 tipos de técnicas que permiten realizar la autenticación de la identidad del usuario, las cuales pueden ser utilizadas individualmente o combinadas:

Algo que solamente el individuo conoce: Una clave, un pin etc..
Algo que la persona posee: Una tarjeta.
Algo que el individuo es: Huella digital o voz
Algo que el individuo es capaz de hacer: Patrones de escritura.

Para conocer más acerca de estas técnicas vaya al tema de Seguridad Física.

Desde el punto de vista de la eficiencia es conveniente que los usuarios sean identificados y autenticados una sola vez, pudiendo a partir de ahí acceder a todas las aplicaciones y datos que su perfil permita, ya sea en local o remoto. Esto se denomina SINGLE LOGIN o SINCRONIZACIÓN DE PASSWORDS. Una de las posibles técnicas para implementar esta única identificación sería la utilización de servidores de autenticación sobre el que se identifican los usuarios y que se encarga luego de autenticar al usuario sobre los restantes equipos. Este servidor no tiene que ser necesariamente un solo equipo y puede tener sus funciones distribuidas geográficamente de acuerdo a los requerimientos de carga de tarea (LDAP o ACTIVE DIRECTORY).

La seguridad informática se basa en gran medida en la efectiva administración de los permisos de acceso a los recursos informáticos basados en la identificación, autenticacion y autorización de accesos

3.2.1.1 PASSWORD SEGURAS

Para un atacante una contraseña segura debe parecerse a una cadena aleatoria de caracteres, puede conseguir que su contraseña sea segura por los siguientes criterios:
Que no sea corta, cada carácter que agrega a su contraseña aumenta exponencialmente el grado de protección que esta ofrece, las contraseñas deben contener un mínimo de 8 caracteres lo ideal es que contengan 14 o mas, muchos sistemas también admiten el uso de la barra espaciadora de modo que se pueden crear contraseñas de varias palabras (una frase codificada) por lo general una frase codificada resulta mas fácil de recordar y mas difícil de adivinar que una contraseña simple.
Combina letras, números y símbolos, cuantos mas diversos sean los tipos de caracteres mas difícil será adivinarla.
Cuantos menos tipos de caracteres haya en la contraseña mas larga deberá ser esta. Una contraseña de 15 caracteres formada únicamente por letras y números es una 33000 veces mas segura que una de 8 caracteres compuestas por caracteres de todo tipo. Si la contraseña no puede tener símbolos deberá ser considerablemente mas larga para

conseguir el mismo grado de protección. Una contraseña ideal combinaría una mayor longitud y distintos tipos de símbolos.
Utiliza todo tipo de teclas, no te limites a los caracteres mas comunes los símbolos que necesitan que se presione la tecla mayúscula junto con un número son muy habituales, tu contraseña será mucho mas segura si eliges entre todos los símbolos del teclado incluidos los símbolos de puntuación así como los exclusivos de tu idioma.
Utiliza palabras y frases que te resulten fáciles de recordar pero que a otras personas les sea difícil de adivinar. La manera mas sencilla de recordar tus contraseñas y frases codificadas consiste en anotarlas, no hay nada malo en anotar las contraseñas si bien estas anotaciones deben estar debidamente protegidas para que resulten seguras y eficaces.
Por lo general las contraseñas escritas en un trozo de papel suponen un riesgo menor en Internet que un administrador de contraseñas, un sitio web u otra herramienta basada en Software.
Algunas estrategias que deben evitarse son:
No incluya secuencias ni caracteres repetidos, cadenas como 12345678, 22222222, abcdefg o el uso de letras adyacentes en el teclado no ayudan a crear contraseñas seguras.
Evita utilizar sustituciones de letras por símbolos o números similares por ejemplo la i por el 1, la a por la @, o la o por el 0. Estas sustituciones pueden ser eficaces cuando se combinan con otras medidas, con una mayor longitud, errores ortográficos voluntarios, variaciones entre mayúsculas y minúsculas.
No utilice el nombre de inicio de sesión, cualquier parte del nombre, fecha de nacimiento, numero de la SS o datos similares propios o de tus familiares constituye una mala elección.
No utilices palabras del diccionario de ningún idioma los delincuentes emplean herramientas capaces de descifrar rápidamente contraseñas basadas en palabras de distintos diccionarios que también abarcan palabras inversas, errores ortográficos comunes y sustituciones esto incluye todo tipo de blasfemias y palabrotas.
Utiliza varias contraseñas para distintos entornos, si alguno de los equipos o sistemas en línea que utilizan esta contraseña queda expuesto toda la información protegida también estará en peligro.
Evita utilizar sistemas de almacenamiento en linea, si algún usuario malintencionado encuentra estas contraseñas tendrá acceso a toda tu información.
Opción de contraseña en blanco: Una contraseña en blanco en su cuenta es mas segura que una contraseña poco segura como 1234, puedes optar por usar contraseñas en blanco en la cuenta del equipo si se cumplen estos criterios:
Tiene solo un equipo o bien tiene varios pero no necesita obtener acceso a la información de un equipo desde los otros
El equipo es físicamente seguro (confías en todas las personas que tienen acceso físico al equipo).
No siempre es buena idea usar una contraseña en blanco, por ejemplo es probable que un equipo portátil no sea físicamente seguro.
Cuida tus contraseñas y frases codificadas tanto como la información que protegen, no la reveles a nadie, protege las contraseñas registradas, no las facilites nunca por correo

electrónico, cambia tus contraseñas con regularidad y no las escribas en equipos que no controlas.

3.2.2 ROLES
El acceso a la información también puede controlarse a través de la función perfil o rol del usuario que requiere dicho acceso. Algunos ejemplos de roles serían programador, líder del proyecto, administrador del sistema etc..

En este caso los derechos de acceso y política de seguridad asociada pueden agruparse de acuerdo con el rol de los usuarios

3.2.3 LIMITACIONES A LOS SERVICIOS
Estos controles se refieren a las restricciones que dependen de parámetros propios de de la utilización de la aplicación o preestablecidos por el administrador del sistema. Un ejemplo podría ser licencias para la utilización simultanea de un determinado producto software para 5 personas de manera que desde el sistema no se permita la utilización del producto simultáneamente a un sexto usuario

3.2.4 MODALIDAD DE ACCESO
Se refiere al modo de acceso que se permite al usuario sobre los recursos y la información esta modalidad puede ser:

Lectura: el usuario puede únicamente leer o visualizar la información pero no puede alterarla, debe considerarse que la información puede ser copiada o impresa
Escritura: este tipo de acceso permite agregar datos, modificar o borrar información
Ejecución: otorga al usuario el privilegio de ejecutar programas.
Borrado: permite al usuario eliminar recursos del sistema como programas, campos de datos o archivos.
Todas las anteriores
Ademas existen otras modalidades de acceso especiales:

Creación: permite al usuario crear archivos nuevos, registros o campos.
Búsqueda: permite listar los archivos de un directorio determinado

3.2.5 UBICACIÓN Y HORARIOS
El acceso a determinados recursos del sistema puede estar basado en la ubicación física o lógica de los datos o personas. En cuanto a los horarios este tipo de controles permite limitar el acceso de los usuarios a determinadas horas del día o a determinados días de la semana. Se debe mencionar que en estos dos tipos de controles siempre deben ir acompañados de algunos de los controles anteriormente mencionados.

3.3 ADMINISTRACIÓN

Una vez establecidos los controles de acceso sobre los sistemas y a las aplicaciones es necesario realizar una eficiente administración de estas medidas lo que involucra la implementación, seguimientos, pruebas y modificaciones sobre los accesos de los usuarios en los sistemas. La política de seguridad que se desarrolle respecto a la seguridad lógica debe guiar a las decisiones referidas a la determinación de los controles de accesos, especificando las concesiones necesarias para el establecimiento de perfiles de usuario. La definición de permisos de acceso requiere determinar cual será el nivel de seguridad necesario sobre los datos por lo que es imprescindible clasificar la información determinando el riesgo que produciría una eventual exposición de la misma a usuarios no autorizados así los diversos niveles de la información requerirán diferentes medidas y niveles de seguridad. Para empezar la implementación es conveniente empezar definiendo las medidas sobre la información mas sensible o las aplicaciones mas críticas y avanzar de acuerdo a un orden de prioridad decreciente establecido alrededor de las aplicaciones.

Tiene que existir una conciencia de la seguridad organizacional por parte de todos los empleados, esta consciencia puede alcanzarse mediante el ejemplo del personal directivo en el cumplimiento de las políticas y estableciendo compromisos firmados por el personal donde se especifique la responsabilidad de cada uno. Además debe existir una concienciación por parte de la administración hacia el personal en donde se remarque la importancia de la información y las consecuencias posibles de su perdida o apropiación por agentes extraños a la organización.

3.3.1 ADMINISTRACIÓN DEL PERSONAL Y USUARIOS
Este proceso lleva generalmente 4 pasos:

Definición de Puestos: Debe contemplarse la máxima separación de funciones y el otorgamiento mínimo de permisos de acceso por cada puesto para la ejecución de las tareas asignadas.
Determinación de la sensibilidad del puesto: Es necesario determinar si la función requiere permisos arriesgados que le permitan alterar procesos, perpetuar fraudes o visualizar información confidencial.
Elección de la persona para cada puesto: Requiere considerar los requerimientos de experiencia y conocimientos técnicos necesarios para cada puesto, así mismo para los puestos definidos como críticos puede requerirse una verificación de antecedentes personales.
Entrenamiento inicial y continuo del empleado: Cuando la persona ingresa a la organización debe comunicársele las políticas de seguridad de la organización y su responsabilidad. El personal debe sentir que la seguridad es un elemento prioritario.

3.4 ACTUALIZACIONES DEL SISTEMA Y APLICACIONES
Los ciber-delincuentes suelen aprovechar las vulnerabilidades mas recientes que requieren actualización inmediata de los sistemas, los fabricantes de software actualizan sus programas cada vez que se descubre un agujero de seguridad.

Es de vital importancia actualizar los sistemas, tanto en sistema operativo como el resto de aplicaciones tan pronto como sea posible. La mayoría de aplicaciones y sistemas disponen de la opción de actualización automática se recomienda activar dicha opción.

Tema 4- Software de seguridad.

4.1. Software malicioso.

Con el nombre de software malicioso o malware agrupamos los virus o gusanos,troyanos y en general todos los tipos de programas que han sido desarrollados para entrar en ordenadores sin permiso de su propietario para producir efectos no deseados, estos efectos se producen algunas veces sin que nos demos cuenta del acto.

4.1.1. ¿Qué son los virus?

Son programas maliciosos creados para manipular en normal funcionamiento de los sistemas sin el conocimiento ni consentimiento de los usuarios, actualmente por sencillez, el termino virus es ampliamente utilizado para referirse genéricamente a todos los programas que infectan a un ordenador aunque en realidad, los virus son un tipo especifico de este tipo de programas. Para referirse a todos ellos también se suelen emplear las palabras código malicioso, software malicioso, software malintencionado o la más usual malware .

Los programas maliciosos pueden alterar tanto el funcionamiento del equipo como la información que contiene o se maneja en ella, las acciones realizadas en la maquina pueden variar desde el robo de información sensible o el borrado de datos hasta el uso de equipos como plataforma para cometer otro tipo de actividades ilegales como es el caso de las redes zombies o botnet pudiendo llegar incluso a tener sus respectivas consecuencias legales.

En sus comienzos la motivación principal de los creadores de virus era la del reconocimiento publico, cuanta mas relevancia tuviera el virus, mas reconocimiento obtenía su creador, por este motivo las acciones a realizar por el virus debían ser visibles para el usuario, suficientemente dañinas como para tener relevancia Por ejemplo: eliminar ficheros importantes,cambiar el tipo de letra, formatear el disco duro, etc. Sin embargo la evolución de las tecnologías de la comunicación y su penetración en casi todos los aspectos de la vida diaria ha sido vista por todos los ciber delincuentes como un negocio muy lucrativo.

Los creadores de virus han pasado a tener una motivación económica por lo que actualmente son grupos muchos mas organizados que desarrollan los códigos maliciosos con la intención de que pasen lo mas desapercibido posible y dispongan de mas tiempo para desarrollar su actividad maliciosa.

Hay varias formas en las que el creador del programa malicioso puede obtener un beneficio económico, las más comunes son:

Robar información sensible del ordenador infectado, como datos personales, contraseñas, credenciales de acceso a diversas entidades...
Crear una red de ordenadores infectados generalmente llamada red zombie o botnet para que el atacante pueda manipularlos todos simultáneamente y vender estos servicios a entidades sin escrúpulo que puedan realizar operaciones poco legitimas como el envío de spam, envío de mensajes de pishing, acceder a cuentas bancarias, realizar ataques de denegación de servicios, etc.
Vender falsas soluciones de seguridad que no realizan las funciones que afirman, por ejemplo, falsos antivirus que muestran mensajes con publicidad informando que el ordenadores tiene virus y que en realidad no es así.
Cifrar el contenido de ficheros dentro de el ordenador y solicitar un rescate al usuario para recuperar la información como hacen los criptovirus.

Los programas maliciosos afectan a cualquier dispositivo que tenga un sistema operativo como: Ordenadores personales, servidores, teléfonos móviles, PDA's, videoconsolas.

4.2.Clasificación de tipos de virus.

Los distintos códigos maliciosos pueden clasificarse en función de diferentes criterios, los mas comunes son por su capacidad de propagación y por las acciones que realizan en el equipo infectado. Algunos de los programas maliciosos pueden ser asociados a un tipo concreto mientras que a otros se les suele incluir dentro de varios grupos a la vez.

También cabe mencionar que muchas de las acciones que realizan los códigos maliciosos en algunas circunstancias se pueden considerar legítimas por lo tanto como dijimos anteriormente solo se considera que un programa es malicioso cuando actúa sin el consentimiento ni conocimiento del usuario.

4.2.1._Según su capacidad de propagación.

Virus:
El nombre es una analogía a los virus reales ya que infectan a otros archivos, es decir, solo pueden existir en un equipo dentro de otro fichero. Los ficheros infectados generalmente son ejecutables .exe .src o en versiones antiguas .com o .bat pero también pueden infectar otro tipo de archivos, por ejemplo, un virus de macro infectará programa que utilicen macros como los productos OFFICE.

Los virus se ejecutan con se ejecuta el fichero infectado aunque algunos de ellos además están preparados para activarse sólo cuando se cumple una determinada condición, por ejemplo un fecha completa. Cuando están en ejecución, suelen infectar a otros ficheros con las mismas características que los del fichero anfitrión, si el fichero que infectan se

encuentra dentro de un dispositivo extraíble o una unidad de red, cada vez que un nuevo usuario accede al fichero infectado, su equipo también se verá comprometido.

Los virus fueron el primer tipo de código malicioso que surgió aunque actualmente casi no se encuentran nuevos virus pasando a hallarse en los equipos otros tipos de códigos maliciosos como los gusanos y troyanos que se explican a continuación.

Gusanos:
Son programa cuya característica principal es realizar el numero máximo de copias de si mismo para facilitar su propagación, a diferencia de los virus no infectan otros ficheros. Se suelen propagar por los siguientes medios:

Correo electrónico
Correo p2p, explotando alguna vulnerabilidad.
Mensajería instantánea.
Canales de chat.

Generalmente los gusanos utilizan la ingeniería social para incitar al usuario receptor a que abra o utilice determinado fichero que tiene la copia del gusano, de este modo, si el gusano se propaga en redes P2P las copias del gusano suelen tener nombres sugerentes como por ejemplo de alguna película de actualidad, para los gusanos que se propagan por correo el asunto y el adjunto suelen ser llamativos para incitar al usuario a que se ejecute la copia del gusano.

Eliminar un gusano suele ser mas fácil que eliminar un virus al no infectar ficheros no es necesario quitar solo algunas partes del mismo, basta con eliminar el archivo en cuestión.

Por otro lado, para garantizar la auto-ejecución suelen modificar ciertos parámetros del sistema por ejemplo pueden cambiar la carpeta inicio con el listado de todos los programas que se tienen que ejecutar al arrancar el ordenador para incluir la copia del gusano o modificar alguna clave del registro que sirva para ejecutar programas en determinado momento al arrancar el ordenador cuando se llama a otro programa, etc.

Troyanos:
Crecen de rutina propia de propagación, pueden llegar al sistema de diferentes formas, las mas comunes son: descargado por otro programa malicioso, descargado por el consentimiento del usuario al visitar una pagina web maliciosa, dentro de otro programa que simula ser inofensivo.

4.2.2._Según las acciones que realiza.

Es posible que un programa malicioso pertenezca a un tipo en concreto aunque también puede suceder que pertenezca a varias de estas categorías a la vez.
Los diferentes tipos de códigos maliciosos son:

Adware: Muestra publicidad generalmente relacionado con los espías por lo que se suelen conectar a un servidor remoto para enviar la información recopilada y definir publicidad. Algunos programas en sus versiones gratuitas o de evaluación, muestran este tipo de publicidad, en este caso deberán avisar al usuario que la instalación del programa conlleva la visualización de publicidad.

Bloqueador: Impide la ejecución de determinados programas o aplicaciones también puede bloquear el acceso a determinadas direcciones de Internet, generalmente impiden la ejecución de programas de seguridad para que resulte más difícil la detección y eliminación de programas maliciosos en el ordenador. Cuando bloquean el acceso de direcciones de Internet estas suelen ser páginas de seguridad informática. Por un lado logran que los programas de seguridad no se puedan descargar actualizaciones y por otro en caso de que un usuario se quiera documentar de alguna amenaza informática no podrá acceder a las direcciones en las que se informa de dicha amenaza.

Bomba lógica: Programa o parte de un programa que no se ejecuta hasta que se cumple una determinada condición, por ejemplo una fecha o la ejecución de algún archivo.

Broma: No realiza ninguna acción maliciosa, pero hacen pensar a los usuarios que su ordenador está infectado. Por ejemplo, mostrando un falso mensaje de que se van a borrar todos los datos o mover el ratón de forma aleatoria.

Bulo: Mensaje electrónico enviado por un conocido que intenta hacer creer al destinatario algo que es falso. Como alertar de virus inexistentes, noticias engañosas y solicitan ser enviados a todos los contactos. Algunos de estos mensajes pueden ser peligrosos. Por que en ocasiones solicitan realizar al usuario la eliminación de ficheros del ordenador necesarios para su funcionamiento.

Keylogger: Monotoriza las pulsaciones del teclado capturando claves de acceso a determinadas cuentas bancarias, conversaciones y mensajes escritos en la máquina.

Clicker: Redirecciona las páginas de internet logrando aumentar el número de visitas de dicha página, pudiendo realizar ataques DDoS o engañar al usuario sobre la página que está visitando, por ejemplo, creyendo que está accediendo a la página de un banco, cuando en realidad accede a una dirección falsa.

Criptovirus: Hace inaccesibles determinados ficheros y coacciona al usuario a pagar un rescate para poder acceder a la información. Generalmente cifra ficheros con los que suele trabajar el usuario como documentos de texto, hojas de calculo, imágenes, etc.

Descargador: Descarga otros programas generalmente también maliciosos, y suelen acceder a Internet para descargar estos programas.

Espía: Roba información del equipo para enviarla a un servidor remoto. Esta información varia según el espía, algunos recopilan información relativa a los hábitos de uso del ordenador como el tiempo de uso, y páginas visitadas en Internet. Otro roban información confidencial, como nombres de usuarios y contraseñas.

Exploit: Tipo de software que se aprovecha de un bug del sistema para tener acceso no autorizado al mismo.

Herramienta de fraude: Simula el comportamiento anormal del sistema y propone la compra de algún programa para solucionarlo, los más comunes son los falsos antivirus.

Instalador: Instala y ejecuta otros programas generalmente maliciosos.

Ladron de contraseñas: Roba nombres de usuarios y contraseñas generalmente accediendo a los ficheros que almacenan esta información.

Marcador: Actúa cuando el usuario accede a internet realizando llamadas a números de tarificación adicional. Lo que provoca un aumento de la factura telefónica. Este tipo, está actualmente en desuso por que solo funciona si la conexión se hace mediante módem. No se pueden realizar llamadas mediante conexiones ADSL o WIFI.

Puerta trasera: Permite el acceso de forma remota a un sistema operativo, página web o aplicación evitando las restricciones de control y autenticación. Puede ser utilizado por responsables de sistemas o webmaster con diversos fines dentro de una organización, pero también puede ser utilizado por otros atacantes para realizar acciones como leer ficheros, moverlos, subirlos al ordenador, descargarlos o eliminarlos, reiniciar el ordenador, obtener información como el nombre del equipo, MAC, SO instalado.

Rootkit: Toma el control de administración en el sistema, generalmente para ocultar su presencia y la de otros programas maliciosos o para esconder ficheros, los procesos generados, conexiones creadas, etc...
También pueden permitir a un atacante remoto tener permisos de administrador para realizar las acciones que desee, cabe destacar que a veces se usan sin fines maliciosos.

Secuestrador del Navegador: Modifica la página de inicio del navegador, la página de búsqueda, o la página de error, también puede añadir barras de herramientas o incluir

enlaces a favoritos. Generalmente para aumentar las visitas de la página destino. Es importante saber que aplicaciones son las que se usan para este propósito.

4.2.3._Otros tipos de virus.

Ladrones de información(infostealer): es el nombre genérico de programas informáticos maliciosos del tipo troyano, que se introducen a través de internet en un ordenador con el propósito de obtener de forma fraudulenta información confidencial del propietario, tal como su nombre de acceso a sitios web, contraseña o número de tarjeta de crédito.

Código delictivo(crimeware):es un tipo de software que ha sido específicamente diseñado para la ejecución de delitos financieros en entornos en línea. Con el fin de conseguir el robo de identidades para acceder a los datos de usuario de las cuentas en línea de compañías de servicios financieros o compañías de venta por correo, con el objetivo de obtener los fondos de dichas cuentas, o de completar transacciones no autorizadas por su propietario legítimo, que enriquecerán al ladrón que controla el crimeware.

Greyware (grayware):es un término aplicado a un amplio rango de programas que son instalados en la computadora de un usuario para dar seguimiento o reportar cierta información a un tercero. Estas aplicaciones son usualmente instaladas y "corren" sin el permiso del usuario.

4.2.4._Programas no recomendables.
Existen algunos programas que sin realizar directamente ninguna acción dañina se consideran maliciosos:
-Programas que realizan acciones ilegales:

Generador de claves: Generan las claves necesarias para que funcione determinado programa de pago de forma gratuita. Es independiente del programa de pago.

Crack: Parche informático que se desarrolla para que determinado programa de pago funcione de manera gratuita.

Herramientas de creación de malware(constructor): No realiza ninguna acción maliciosa en el ordenador, es empleado por programadores maliciosos para crear programas dañinos personalizados.

El uso y pertenencia de estos programas no solo están tipificados como delito por la legislación española si no que además suelen ser utilizados para propagar otros programas maliciosos que están ocultos.

Cookies maliciosas: Existen tipos de ficheros que según el uso que tengan pueden o no ser peligrosos, son las cookies, Son pequeños ficheros de texto que se crean en el navegador al

visitar paginas web. Almacenan diversa información que por lo general, facilita la navegación del usuario por la pagina web que se esta utilizando y lo mas importante es que no tienen capacidad para consultar información del ordenador en el que están almacenadas. Sin embargo, también existen cookies maliciosas que monitorizan las actividades del usuario en internet con fines maliciosos, por ejemplo capturar datos del usuario y contraseñas de acceso a determinadas paginas web o vender los hábitos de navegación a empresas de publicidad.

4.3._Protección y desinfección.
Existen gran variedad de formas por las que los virus, gusanos y troyanos pueden llegar a un ordenador. En la mayoría de los casos, prevenir la infección resulta relativamente fácil siguiendo unas sencillas pautas. Las formas en las que un programa puede llegar al ordenador son las siguientes:

Explotando una vulnerabilidad: Cualquier programa del ordenador puede tener una vulnerabilidad que puede ser aprovechada para introducir programas maliciosos en el ordenador, es decir, todos los programas que se hayan instalado en el equipo, ya sean sistemas operativos como WINDOWS-LINUX-MACOOS, navegadores web como Internet Explorer-Firefox-Opera-Chrome, etc...clientes de correo, o cualquier otra operación como reproducciones multimedia, programas de ofimática,compresores, etc... Es posible que tengan alguna vulnerabilidad que sea aprovechada por algún atacante para introducir programas maliciosos, para prevenir quedarse infectado de esta forma, se recomienda tener siempre actualizado el software del equipo.

Ingeniería social: Apoyado en técnica de ingeniería social para premiar al usuario que realice determinada opción, la ingeniería social se utiliza sobre todo en correos de phishing pero puede ser usada de mas formas como por ejemplo informando de una falsa noticia como alertar como el comienzo de una falsa guerra, incluyendo un enlace donde pueden verse los detalles del a noticia dirigiéndonos realmente a una pagina web con contenido malicioso.Contra esta técnica lo mas importante es no hacer caso a correos recibidos de remitentes desconocidos y tener en cuenta que su banco nunca les va a pedir sus datos bancarios por correo.

Por un archivo malicioso: Esta es la forma que tienen gran cantidad de troyanos de llegar al equipo. El archivo puede llegar como adjunto de un mensaje por redes p2p como un enlace a un fichero que se encuentra en internet a través de carpetas compartidas en las que el gusano haya dejado una copia del mismo, etc. la mejor forma de prevenir la infección es analizar con un antivirus actualizado todos los archivos antes de ejecutarlos aparte de no descargar archivos de fuentes que no sean fiables.

Dispositivos extraíbles: Muchos gusanos suelen dejar copias de si mismos en dispositivos extraíbles para que automáticamente cuando es dispositivo se conecta al ordenador ejecutar he infectar el nuevo equipo. La mejor forma de evitar quedarse infectados es deshabilitar el autoarranque de los dispositivos que se conectan al ordenador.

Aunque como se ha visto, existe gran cantidad de códigos malicosos es muy fácil prevenir de quedarse infectado.

Basta con seguir las recomendaciones de seguridad:
Mantenerte informado sobre las novedades y alertas de seguridad.
Manteen actualizado tu equipo, tanto el sistema operativo como cualquier aplicación que tengas activada.
Haz copias de seguridad con cierta frecuencia.
Utiliza software legal que suele ofrecer garantía y soporte.
Utiliza contraseñas fuertes en todos los servicios para dificultar la suplantación del usuario.
Utiliza herramientas de seguridad que te ayudan a reparar tu equipo frente a las amenazas de internet.
Crea diferentes usuarios, cada uno de ellos pon les permisos mínimos para poder realizar las operaciones permitidas.

4.3.1._ Seguridad en Internet.

En la navegación web:
No lo descargues ni ejecutes ficheros desde sitios sospechosos.
Analiza con un antivirus todo lo que descargues.
Mantén actualizado tu navegador.
Configura el nivel de seguridad de tu navegador.
Instala un cortafuegos.
Descarga los programas desde los sitios oficiales.
Puedes utilizar mata-emergentes para eliminar las molestas ventanas emergentes(pop-up) o configura tu navegador para evitarlas.
Utiliza una cuenta sin permisos de administrador.
Borra los cookies, ficheros temporales y el historial cuando utilices equipos ajenos.

Precauciones con el correo electrónico:
No abras ficheros adjuntos sospechosos o que no haya solicitado.
Utiliza un filtro anti-spam.
Analiza los anexos con un antivirus.
Desactiva la lista previa de tu cliente de correo.
No facilites tu cuenta de correo a desconocidos ni la publiques alegremente.
No respondas a mensajes falsos ni a cadenas de correos.
Borra el historial del destinatario cuando reenvíes mensajes a múltiples direcciones.

Cuando utilices e-comercio o comercio electrónico.
Nos sirve que la web empiece por HTTPS.

Observa que aparece un candado en la parte inferior derecha de tu navegador.
Asegurarte de la validez de los certificados(pulsando en el candado) que coinciden con la entidad solicitada que sean vigentes o validos.
Ten en cuenta que tu banco nunca te pedirá información confidencial por correo electrónico ni por teléfono.
Evita el uso de equipos públicos (cibercafes, estaciones, aeropuertos) para realizar transiciones comerciales.
Desactiva la opción auto-completar si accedes desde un equipo distinto al habitual o compartes tu equipo con otras personas.
Cierra tu sesión cuando acabes.
Instala alguna herramienta de antifraude para evitar acceder a páginas fraudulentas.

En los chats y programas de mensajería instantánea.
Evita invitaciones a visitar sitios web que resulten sospechosas o que procedan de desconocidos.
Rechazo de ficheros adjuntos que no haya solicitado por lo que carezcan sospechosos.
Ten precaución al conversar o agregar contactos desconocidos.
No facilites datos confidenciales.

En redes p2p con software de descarga o webs de descarga.
Analiza todos los archivos que te descargues.
No compartas software legal.
Ejecuta el cliente p2p en una sesión de usuario con permisos limitados.
Modifica el nombre de las carpetas de descarga ya que muchos códigos maliciosos busca rutas fijas para replicarse.
Presta atención a la extensión de los archivos que descargues por ejemplo una imagen nunca tendrá extensión .exe

Cuando juegos online a través de Internet.
Evitar compartir usuarios y contraseñas tanto dentro del juego como fuera.
Actualiza el software de juego.
No adquieras créditos en páginas de subastas en linea sin que estén certificados por los creadores del juego.
Vigila los movimientos de tu cuenta o tarjeta bancaria si la tienes asociada al juego.
Controla tu tiempo de juego ya que esta actividad puede ser muy adictiva.

4.4._Herramientas software antimalware.

4.4.1._ Antivirus.

Un antivirus es un programa informático específicamente diseñado para detectar, bloquear y eliminar códigos maliciosos, aunque se sigue utilizando la palabra antivirus estos programas han evolucionado y son capaces de detectar y eliminar no solo virus si no también otros tipos de códigos maliciosos como gusanos, troyanos, espías, etc.

Las plataformas mas atacadas por virus son la linea de sistemas Windows de Microsoft respecto a los sistemas derivados de UNIX como GNU Linux, Bsd solarix o MACCOOS, han corrido mejor suerte debido al sistema de permisos.

Existen 2 formas diferentes de utilizar un antivirus según donde esté instalado: Local o En Línea y en función a las ventajas e inconvenientes utilizaremos una u otra.

4.4.1.1._ Antivirus de escritorio.

Se suelen utilizar en modo residente para proteger al ordenador en todo momento de cualquier posible infección ya se navegar por Internet, recibir algún correo infectado, o introducir en el equipo algún dispositivo extraíble que esté infectado. No necesitan que el ordenador esté conectado a Internet pero si es necesario actualizarlos frecuentemente.

Recomendamos tener solo un antivirus en el escritorio, ya que varios podrían ocasionar problemas de incompatibilidad. Actualmente la mayoría de los antivirus tienen la opción de actualizarse automáticamente lo que es muy recomendable.

TABLA COMPARATIVA ANTIVIRUS DE PAGO

McAFee
Norton Symantec
E S E T NOD32
PANDA SECURITY
Antivirus
S
S
S
S
Antispyware
S
S
S
S
Link Scanner
N
N
N
S
Antirootkit

S
S
S
S
Web Shield
N
S
S
S
ID Protection
S
S
N
S
Firewalls
S
S
S
S
Antispam
N
N
N
S
64 bits
N
LIMITADO
S
S
Español
S
S
S
S
Soporte
30 DÍAS
S
S
S
MAC / Linux
N
MAC
LINUX
LINUX

Consumo de Recursos
MEDIO
MUCHOS
POCOS
POCOS

4.4.1.2._Antivirus en línea.

Los antivirus en linea son muy útiles para analizar el ordenador con un segundo antivirus cuando sospechamos que el equipo puede estar infectado, para ejecutarlos es necesario acceder en el navegador a una página web de Internet. Estos antivirus no sirven para prevenir infecciones ni se instalan en el pc como un programa convencional. El tiempo de escaneo varia en función de tu conexión, la carga de los servidores, o el volumen de datos que quiera rastrear.

La mayoría de estos servicios, descargan un subprograma (ACTIVX o JAVA) por lo que la primera vez que se accede tardan unos minutos en arrancar. Entre otros encontramos:
Español:

-ESET ONLINE SCANER. Ofrece una versión gratuita de us escaner en línea, busca malware y lo elimina, funciona bajo internet explorer,firefox,nexcape y opera.

-TREND MICRO HOUSECALL. Utiliza un aplet de java lo que permite que sea soportado por todos los navegadores, tiene incorporada una herramienta de chequeo de puertos, funciona bajo plataformas windows y linux.

-ACTIVE SCAN2.0(Panda). Para eliminar parte de las amenazas hay que registrarse de forma gratuita y para eliminar todas, hemos de comprar el producto. Al terminar el escaneo permite guardar un informe completo, funciona baso sistemas windows.
Inglés:

-ONLINE SCANER. Descarga un subprograma llamado ACTIVEX, se pueden seleccionar las opción de configuración del análisis, permite escanear la memoria de tu sistema(archivos, carpetas, disco y sector de arranque) ofreciendo opción de desinfectar o eliminar archivos infectados.

-SYMANTEC SECURITY CHECK. Descarga un subprograma (ACTIVEX) y realiza un escaneo de todas las unidades del sistema sin dar opción a un subconjunto. La búsqueda no se remonta a ficheros compartidos.

4.4.1.3._Laboratorios de pruebas.

Muchos de las propias empresas muestran estudios en sus paginas web demostrando que son mejores que la competencia pero estos estudios pierden validez al ser conducidos por la propia empresa. También pierden validez los estudios conducidos por los propios usuarios debido a que generalmente, la muestra de virus es muy pequeña y puede malinterpretar los resultados, por ejemplo contando la detección de un falso positivo como verdadera.

También tenemos que tener en cuenta que la tasa de detección puede variar de mes a mes debido al gran numero de malware que se crea y es mejor de comparar un estudio con otro meses mas antiguo, además ha de recordar que ningún antivirus es 100% perfecto.

Los estudios con validez son los hechos por empresas o laboratorios independientes los cuales no deberían tener presión de ninguna manera para la clasificación de productos

Webs Interesantes:
-Av comparativas: http://www.av-comparatives.org

-Av test.org: http://www.av-test.org

-ISCA Labs: http://icsalabs.com

-Virus Bulleting: http://www.virusbtn.com/

-Web Coast Labs: http://www.westcoastlabs.org/

4.4.2._ Antispyware.
Los spyware o programas espía son aplicaciones que se dedican a compilar información del sistema para luego enviarlas a través de internet generalmente alguna empresa de seguridad, todas estas acciones se hacen de forma oculta al usuario o bien se enmascaran tras confusas actualizaciones al instalar terceros programas por lo que rara vez el usuario es consciente de ello. No debes fiarte de todas las herramientas antiespias ya que algunas pueden tener códigos maliciosos, publicidad engañosa, no ofrecer la perfección prometida, he incluso dar como resultado falsos positivos.

4.4.2.1._Antiespias de escritorio.
Son aquellos que requieren de instalación en el pc, se suelen utilizar en modo residente, analizan cualquier fichero que se accede en tiempo real como complemento los antivirus para proteger al ordenador en todo momento de cualquier posible infección de código espia.

4.4.2.2._Antiespias en linea.
Son accesibles a través del navegador y no necesitan una instalación completa, necesitan por tanto una conexión a internet.

4.4.3._Otras herramientas antimalware.

4.4.3.1._ Herramientas de bloqueo:

-Antifraude: Estas herramientas nos informan de la peligrosidad de los sitios que visitamos, en algunos casos, nos informan de forma detallada de que enlaces de esas paginas se consideran peligrosas y porqué motivo, algunos ejemplos son:
Spoofstick: es un software que se instala con una extensión del navegador que sirve para comprobar que las paginas que visitamos son autenticas y no potencialmente peligrosas.
Netcraft: protege de los ataques de phising vigila donde se hospeda y proporciona un índice de riesgo a los sitios que visita.

-Útiles anti-spam: el spam podemos definirlo como envío masivo de correo electrónico no deseado, un alto porcentaje de correo electrónico es spam. Principalmente se utiliza como complemento a otras técnicas que tiene como fin ultimo, engañarnos con el fin de recoger un beneficio económico, además el simple hecho del envío y la recepción de este correo provoca un tráfico de datos que ayudan a saturar internet. Las herramientas antispam tratan de mitigar el efecto del spam y son programas que filtran los correo electrónicos tratando de eliminar los que consideran spam, algunos ejemplos son:
Trendmicro: pone a nuestra disposición una herramienta para controlar el origen de los correos electrónicos.(Comodo time machine) esta herramienta de instala en forma de plugin del navegador y funciona con el correo web de gmail, windows live hotmail, yahoo, además de con el programa outlook express, el programa comprueba si el correo recibido corresponde a la empresa que debería y que no es un interno de phising, actualmente no puede confirmar el correo de todas las compañías, pero si tiene muchas, entre ellas unas cuantas de servicios de internet utilizada muy frecuentemente como ganchos para intentos de robo de identidad mediante técnicas de phising. Trabaja en plataformas windows con internet explorer o firefox.
Spanilator: tiene la disposición de todos los usuarios, un programa antispam que se encarga de filtrar los correos electrónicos no deseados que nos envían. No funciona correo web, esta en ingles pero podemos descargar un paquete de idiomas aunque funciona bastante bien no es perfecto y hay que mirar de vez en cuando la carpeta de spam por si elimina algún correo que no debiera. Trabaja con plataformas windows con outlook, opera,eudora,pegasus,fenix,nescape,thunderbird e increbiname.

-Antidialer.
Este tipo de herramientas nos permite controlar a que numero se conecta nuestro módem para que no se conecte a ningún numero de nuestra lista de numero permitidos. Este tipo de fraude ha quedado reducido a las antiguas conexiones de módem de marcación sobre linea telefónica.

-Análisis de gestiones en linea.

Herramientas que ofrece un servicio gratuito para análisis de ficheros sospechosos mediante el uso de múltiples motores antivirus como complemento de una herramienta antivirus, claro que ningún antivirus es fiables, el análisis de un fichero con mas de un motor, traduce un resultado mucho mas fiable que con uno solo. Hay 3 tipos:

Doctor web: Ofrece la herramienta doctor web online para el análisis en linea de direcciones de internet en busca de código malicioso que pudiera estar infectado en alguna pagina html.
Livespam.org: Ofrece una herramienta viruscam que proporciona un servicio gratuito para analizar en linea ficheros sospechosos de hasta 10 megas, con o sin comprimir utilizando varios motores antivirus. La información obtenida en el fichero a optar es orientativa. Como información adicional muestra los ultimo ficheros que ha subido al servidor y el resultado de su análisis, tiene selector de idiomas en la parte superior derecha de nuestra pagina.
Virus total: Es un servicio proporcionado por hispasec que permite escanear archivos menores de 10 megas con unos cuantos motores antivirus y si el fichero subido ya lo ha escaneado, nos lo dice y nos muestra el resultado de los análisis, los resultados son orientativos ya que no todos los motores hacen las mismas detecciones. Puede analizar un archivo con el antivirus de karpersky seleccionando le fichero a escanear y enviándolo al servidor, una vez finalizado el análisis, devuelve un informe con información del resultado del estudio. Si se quiere analizar mas de un fichero tienen que enviarse comprimidos pero el tamaño resultante no puede ser mayor a un 1mega.
Análisis de url: Herramientas para el análisis de paginas web sirven para determinar si el acceso a dicha url puede afectar o no a la seguridad de nuestro sistema, existen varios tipos de analizadores. En función de como se accede al servicio, los que realizan un análisis en linea, los que se descargan como una extensión del navegador y los que se instalan como una herramienta de escritorio. Esos útiles son capaces de categorizar paginas que se desea visitar de modo que estando atentos a la valoración,se puede evitar que el sistema sea infectado por acceder a paginas peligrosas. Estas páginas pueden detectar y ha veces bloquear al acceso de paginas con código maliciosos. Fraude electrónico,contenido inapropiado, he incluso si el código intenta explotar alguna vulnerabilidad, sobre nuestro navegador o sistema, no se asegura que la información que puede ofrecer sea del todo fiable al 100% bien porque la pagina web solicitada no haya sido todavía analizada o porque puedan existir opiniones diferentes de diferentes internautas sobre un mismo sitio web.
TEMA 5 - GESTION DE ALMACENAMIENTO DE LA INFORMACION Editar 0 15…
5.1. INTRODUCCIÓN
Todo equipo informático dispone de un sistema de almacenamiento para guardar los datos. En un altísimo porcentaje, el sistema de almacenamiento está constituido por uno o varios discos duros. Estos serán de mayor o menor sofisticación, pero todos constituyen en sí mismos un elemento dedicado que necesitan unas condiciones mínimas de trabajo.

Hacer trabajar a los discos duros en condiciones extremas puede producir una avería física que como consecuencia podría hacer imposible acceder a la información que contiene. Por

tanto, aunque los 3 elementos principales a proteger son el software ,el hardware y los datos, este último, es el principal elemento de los 3 ya que es el más amenazado y seguramente, el más difícil de recuperar.

Contra cualquiera de los 3 elementos se pueden realizar multitud de ataques o dicho de otra forma, están expuestos a diferentes amenazas. Generalmente, la taxonomía más elemental de estas amenazas las divide en 4 grandes grupos: Interrupción, Interceptación, Modificación y Fabricación.
Una ataque se identifica como interrupción, si se hace con un objeto de sistema, se pierda, quede inutilizable, o no disponible.
Se tratara de una interceptación si un elemento no autorizado consigue un acceso a un determinado objeto del sistema.
Una modificación si además de conseguir el acceso, consigue modificar el objeto, algunos autores consideran un caso especial de la modificación la destrucción, entendiéndola como una modificación que inutilizable el objeto.
Por último se dice que un ataque es una fabricación si se trata de una modificación destinada a conseguir un objeto similar al atacado de forma que sea difícil distinguir entre el original y el fabricado.

El almacenamiento de la información requiere una serie de principios y características que mejorar:
Rendimiento.
Disponibilidad.
Accesibilidad.

5.1.1. Rendimiento

Se refiere a la capacidad de disponer un volumen de datos en un tiempo determinado. Se mide en tasas de transferencia (MBits/s).

Existen muchas tecnologías para fabricar dispositivos de almacenamiento, caracterizadas por: coste por bit, tiempo de acceso y capacidad de almacenamiento. El procesador es el elemento principal del ordenador, interesa que los datos con los que va a operar en un momento dado estén los mas próximas a ellas. Cuando la CPU encuentra un dato que necesita sus registros internos se intenta recuperar del nivel inmediatamente inferior (la caché), si no lo encuentra accede a la RAM y si tampoco está allí al disco duro, discos ópticos, etc. Se debe satisfacer por lo tanto la propiedad de inclusión según la cual la información en un determinado nivel se encuentra replicada en los niveles inferiores. Este principio determina la jerarquía de memorias, ubicación temporal de los datos, que está fuertemente ligada a la necesidad que tiene el micro de emplearlos en un momento determinado. Los datos recientemente accedidos se ubican en las memorias mas rápidas y estas deben estar próximas al microprocesador o a la CPU. Las memorias sucesivamente mayores y mas lentas de mayor tiempo de acceso por bit dispondrán todos los datos potencialmente accesibles por la CPU. La memoria interna de carácter volátil o no permanente en ausencia de alimentación eléctrica de mayor velocidad y coste compone

los 3 escalones superiores de la pirámide (Registros internos, memoria caché y memoria RAM). Los niveles inferiores (discos magnéticos, ópticos y cintas magnéticas) se suelen agrupar con nombre de memoria externa de carácter no volátil, almacena la información de forma permanente en ausencia de electricidad, menor velocidad de acceso y menor coste por bit.
external image jerarquia-de-almacenamiento.jpg

5.1.2. Disponibilidad
La disponibilidad se refiere a la seguridad que la información puede ser recuperada en el momento en que se necesite. Esto es evitar su perdida o bloqueo bien sea por ataque, mala operación accidental o situaciones fortuitas o de fuerza mayor. Las distintas técnicas que hoy favorecen la alta disponibilidad de los sistemas de almacenamiento son:

La redundancia o duplicados de información:
Sistemas RAID de almacenamiento.
Centro de procesamiento de centros de respaldo.

La distribución de la información:
Disponer de copias de seguridad en distintas ubicaciones geográficas.
Medios de almacenamiento extraíbles y portátiles.
Servidores de almacenamiento redundantes y distribuidos geográficamente con sincronización en la información que contienen.
Copias de seguridad en la nube
Servicios de copias de seguridad online.

5.1.3. Accesibilidad
Se refiere a tener disponible la información por parte de los usuarios autorizados. Habitualmente se controla mediante técnicas de control de acceso.

5.2. Medios de almacenamiento
En primer lugar realizaremos una clasificación de los dispositivos de almacenamiento en función de varias características:
La naturaleza del soporte de almacenamiento: magnético,óptico,magnetoóptico, memorias flash.
Si es posible leer o escribir.
Acceso a la información secuencial o directo.
Dispositivos interno o externo al sistema informático.
Conexión entre el soporte de la información y la unidad lectora-escritora.

5.2.1. Soporte de almacenamiento de la información
Se determina soporte a todo material o dispositivo en general destinado a registrar información sera un medio en el que se almacene información con una determinada

escritura y de manera indefinida para que pueda ser utilizada por el sistema o por terceras personas. No se debe confundir soporte de información con periférico. Se considera periférico a cualquier periférico de entrada-salida conectado al ordenador que sirve para leer o escribir información sobre los soportes. Es pues, el soporte, el almacén de la información y el periférico el encargado de leer y escribir información sobre dicho soporte. Los mas extendidos son los siguiente:

Magnéticos: Los discos y cintas magnéticas contienen soportes de información constituidos por un sustrato de plástico o aluminio recubierto con un material magnetizable tradicionalmente oxido férrico o oxido de cromo. La información se graba dentro de unidades elementales o celdas que forman lineas o pistas. Cada celda puede estar sin magnetizar o estar magnetizada en uno de dos estados o campos magnéticos(Norte o Sur) que podrán corresponder a un 0 o a un 1. Para escribir o leer una celda se emplea la electricidad para crear campos magnéticos orientados en una dirección u otra para representar 1 o 0. Ejemplos: Cintas magnéticas, discos magnéticos son los mas empleados para el almacenamiento masivo de gran volumen de información.
Ópticos: Usan la energía lumínica mediante un rayo láser u un elemento lumínico para almacenar o leer la información. Los 0 o 1 se representan por la presencia o ausencia de una señal luminosa, ejemplos: dvd's, cd's. Los mas extendidos de uso portátil multimedia, comercial, con usos de solo lectura.
Magnetoópticos: Son soportes que permiten la lectura y la escritura. La información no se graba de manera mecánica, se graba magnéticamente. Los discos vírgenes tienen una magnetización previa mediante láser es posible cambiar la magnetización de las celdas. Los discos magnetoópticos como el cd-mo son regrabables aunque son mas duraderos que los cd-w ya que estos se van degradando en cada operación de escritura. Los mini disck y unidades zip han tenido un gran éxito comercial en los 80's y 90.
Flash USB: Emplean memoria semiconductora en uno o varios chips de tipo flash NAND su cualidad mas destacada es que a pesar de ser memoria semiconductora mantiene su contenido sin necesidad de suministrar energía eléctrica mediante tecnología de puerta flotante, los electrones quedan confinados en el transistor que forma la celda de memoria, ejemplo: memorias de cámaras, memorias usb.

5.2.2. Lectura-escritura

De todos los soportes se puede extraer la información almacenada, pero en algunos casos solo se puede realizar una escritura por lo que no se podrá volver a escribir en ellos. Podemos clasificarlos en:
Reutilizables o regrabables: Podemos emplear el mismo soporte todas las veces que deseemos, ejemplos, cinta magnética,memoria usb, cd-rw.
No reutilizable o de solo lectura: Una vez que se graba la información no se puede modificar, tan solo leerla, ejemplos cd, dvd.

5.2.3. Acceso a la información

Secuencial: Para acceder a un dato tenemos que leer u escribir todos los anteriores, ejemplo, la grabación de un cd y en una cinta magnética la lectura y escritura.

Directo: Podemos acceder a cualquier dato de forma casi inmediata, ejemplo, la lectura de un cd, disco duro, memoria USB es directa. Podemos leer cualquier archivo sin necesidad de acceder a los demás.

5.2.4. Ubicación de la unidad
Interna: La unidad lectora-grabadora ser localiza dentro de la carcasa del ordenador, ejemplos, discos duros,unidades de cd.
Externa: la unidad lectora-grabadora se sitúa fuera del ordenador, ejemplos, memoria USB,disco duro externo,unidad lectora de dvd y cd externa.

5.2.5._Conexión entre soporte y unidad
Removibles: El soporte que almacena la información se puede cambiar permaneciendo la unidad lectora-grabadora, ejemplos, cd,dvd.
No removibles: El soporte que almacena la información y la unidad lectora-grabadora se encuentran unidos,ejemplo, los discos duros y la memoria USB.

5.3. Almacenamiento redundante y distribuido
Uno de los principios que tiene el almacenamiento seguro de la información debe ser la disponibilidad. La redundancia o creación de duplicados exactos de la información posibilita que ante perdidas de información sea posible recuperar los datos. La redundancia la analizaremos desde 2 puntos de vista, los sistemas RAID de almacenamiento redundante y los sistemas distribuidos o centros de respaldo con sincronización de datos.
5.3.1. RAID
En informática el acrónimo RAID hace referencia a un sistema de almacenamiento que usa múltiples discos duros entre los que distribuye o replica datos dependiendo de su configuración a la que suele llamarse nivel. Los beneficios de un RAID respecto a un único disco son uno o varios de los siguientes: mayor integridad, mayor tolerancia a fallos, mayor rendimiento y mayor capacidad.

En el nivel mas simple, un RAID combina varios discos duros en una sola unidad lógica, así en lugar de ver varios discos duros diferentes, el sistema operativo ve uno solo. Los RAID suelen usarse en servidores y normalmente aunque no es necesario se implementan como unidades de disco de la misma capacidad debido a decremento del precio de los discos duros y la mayor disponibilidad de las opciones RAID incluidas en los chipset de las placas base. Los RAIDs se encuentran también como opción en los ordenadores personales mas avanzados, frecuentemente en las computadoras dedicadas a tareas intensivas de almacenamiento como edición de audio y vídeo.

Implementaciones
La distribución de datos en varios discos puede ser gestionada por hardware dedicado o por software, además existen sistemas RAID híbridos basados en software y hardware especifico.

En la implementación con software, el sistema operativo gestiona los discos a través de una controladora de disco normal, considerada tradicionalmente como una operación. Podría considerarse más lenta pero con el rendimiento de las CPU modernas puede llegar a ser mas rápida que algunas implementaciones hardware a expensas a dejar mas tiempo de proceso al resto de tareas del sistema.

Una implementación de RAID basada en hardware requiere al menos una controladora RAID especifica ya sea como una tarjeta de expansión independiente o integrada en la placa base que gestione las operación de los discos y efectué los cálculos de paridad. Esta opción suele ofrecer un mejor rendimiento y hace que el soporte por parte del sistema operativo sea mas sencillo. Las implementaciones basadas en hardware suelen soportar sustitución en caliente, permitiendo que los discos que fallen puedan reemplazarse sin necesidad de parar el sistema. En los RAIDs mayores la controladora y los discos suelen montarse en una caja externa especifica conectada al sistema mediante una o varias conexiones SCSI y fibrreCHANNEL. A veces el sistema RAID es totalmente autónomo conectándose al sistema como NAS.

Los RAIDs híbridos se han hecho muy populares con la introducción de controladoras RAID(hardware) mas baratas. En realidad, el hardware es una controladora de disco normal pero el sistema incorpora una aplicación de bajo nivel que permita a los usuarios construir RAID controlados por la BIOS. Será necesario utilizar un controlador de dispositivo especifico para que el sistema operativo reconozca la controladora como un único dispositivo RAID.

Los RAIDs por software suelen presentar el problema de tener que reconstruir el conjunto de discos cuando el sistema es reiniciado tras un fallo para asegurar la integridad de los datos. Por el contrario los sistemas gestionados por software son mucho mas flexibles, permitiendo por ejemplo construir RAID de particiones en lugar de discos completos y agrupar en un mismo RAID discos conectados en barias computadoras. Los basados en hardware añaden un punto de fallo mas al sistema: la controladora RAID.

Todas las implementaciones pueden soportar el uso de uno o mas discos de reserva, unidades instaladas que pueden desmontarse inmediatamente tras el fallo de un disco RAID. Esto reduce le tiempo de reparación al acortar el tiempo de reconstrucción del RAID.

Las configuraciones RAID mas usados comúnmente son:
RAID 0 (conjunto dividido).
RAID 1 (conjunto en espejo)
RAID 5 (conjunto dividido con paridad distribuida)

5.3.3.1.1 RAID 0 (DATA STRIPING)

Un RAID 0 también llamado con junto dividido o volumen dividido, distribuye los datos equitativamente entre dos o mas discos sin información de paridad que proporcione redundancia.

Se usa normalmente para incrementar el rendimiento aunque también puede utilizarse como forma de crear un pequeño número de grandes discos virtuales a partir de un gran número de pequeños discos físicos.
Mejora el rendimiento pero no aporta seguridad.

Un RAID 0 puede ser creado con discos de diferentes tamaños, pero el espacio de almacenamiento añadido al conjunto estará limitado por el tamaño de discos más pequeño, por ejemplo si un disco de 300 Gigas se divide con uno de 100 Gigas el tamaño del conjunto será solo de 200 Gigas ya que cada disco aporta solo 100 gigas.

Este es el esquema del RAID 0, se escribe paralelamente.

external image Recuperacion-de-datos-de-arreglo-RAID-0.jpg

5.3.1.2 RAID 1 (DATA MIRRURING)
Un RAID 1 crea una copia exacta o espejo de un conjunto de datos en dos o más discos, esto resulta útil cuando el rendimiento en lectura es mas importante que la capacidad.

Un conjunto RAID 1 solo puede ser tan grande como el mas pequeño de sus discos.

Un RAID 1 clásico consiste en dos discos en espejo lo que incrementa exponencialmente la fiabilidad respecto a un solo disco.

Adicionalmente dado que todos los datos están en dos o más discos con hardware habitualmente independiente, el rendimiento de lectura se incrementa aproximadamente como múltiplo lineal del número de copias, es decir que puede estar leyendo simultáneamente los datos diferentes en discos diferentes por lo que su rendimiento se duplica.

Para maximizar los beneficios sobre el rendimiento del RAID1 se recomienda el uso de controladores de disco independientes, una para cada disco, practica que algunos denominan splitting o duplexing.

Como en el RAID 0 el tiempo medio de lectura se reduce ya que los sectores a buscar pueden dividirse entre los discos bajando el tiempo de búsqueda y subiendo la tasa de transferencia con el único límite de la velocidad soportada por la controladora RAID. Sin embargo muchas tarjetas RAID 1 IDE antiguas leen solo de un disco por lo que su rendimiento es igual al de un único disco. Algunas implementaciones RAID 1 antiguas también leen ambos discos simultáneamente, y compara los datos para detectar

errores.La detección y corrección de errores en los discos duros modernos hacen esta práctica poco útil, dado que los datos deben ser escritos en todos los discos el rendimiento no mejora.

El RAID 1 tiene muchas ventajas de administración por ejemplo, es posible dividir el espejo, marcar disco duro como inactivo, hacer una copia de seguridad de dicho disco y luego reconstruir el espejo.

external image RAID1.gif

5.3.1.3 RAID 2,3,4 (Disco de paridad dedicado)
Un RAID 2 divide los datos a nivel de bits en lugar de a nivel de bloques y usa un código de Hammig para la corrección de errores. Los discos son sincronizados por la controladora para funcionar al unísono. Eeste es el único nivel RAID original que actualmente no se usa, permite tasas de transferencias extremadamente altas.

Un RAID 3 usa división a nivel de bytes con un disco de paridad dedicado. El RAID 3 se usa rara vez en la práctica, uno de sus efectos secundarios es que normalmente no puede atender varias peticiones simultáneas debido a que por definición cualquier simple bloque de datos se dividirá por todos los miembros del conjunto, residiendo la misma dirección dentro de cada uno de ellos. Así cualquier operación de lectura o escritura exige activar todos los discos del conjunto.

Un RAID 4 usa división a nivel de bloques con un disco de paridad dedicado, necesita un mínimo de 3 discos físicos.
El RAID 4 es parecido al RAID 3 excepto porque divide a nivel de bloque en lugar de a nivel de bytes. Esto permite que cada miembro del conjunto funcione independientemente cuando se solicita un único bloque. Si la controladora de disco lo permite un conjunto RAID 4 puede servir varias peticiones de lectura simultáneamente. En principio sería posible servir varias peticiones de escritura simultáneamente pero al estar toda la información de paridad en un solo disco este se convertía en el cuello de botella del conjunto.
======
external image raid_4_image.gif?version=1&modificationDate=1307811217000

==

5.3.1.4 RAID 5
Un raid 5 usa división de datos a nivel de bloques distribuyendo la información de paridad entre todos los discos miembros del conjunto. El RAID 5 ha tenido popularidad gracias a su bajo coste de redundancia,generalmente el RAID 5 se implementa con soporte hardware para el calculo de la paridad. Cada vez que un bloque de datos se escribe se genera un bloque de paridad dentro de la misma división,un bloque se compone a medio de muchos sectores consecutivos de disco,una serie de bloques (un bloque de cada uno de los discos

del conjunto)recibe el nombre colectivo de división,si otro bloque a alguna porción de un bloque es escrita en esa misma división,el bloque de paridad o una parte del mismo,es recalculada y vuelta a escribir,las escrituras en un RAID 5 son costosas en términos de operaciones de disco y trafico entre los discos y la controladora.Un RAID 6 amplia el nivel del RAID 5 añadiendo otro bloque de paridad,por lo que divide los datos a nivel de bloques y distribuye los dos bloques de paridad,entre todos los miembros del conjunto

5.3.1.5 Niveles RAID anidados

-Muchas controladoras permiten anidar niveles RAID,es decir que un RAID pueda usarse como elemento básico de otro en lugar de discos,resulta instructivo pensar en estos conjuntos como capas dispuestas unas sobre otras,con los discos físicos en la inferior ,los RAID anidados se indican normalmente,uniendo en un solo número,los correspondientes a los niveles RAID usados,añadiendo aveces un símbolo +,entre ellos,por ejemplo el RAID 10 O RAID 1+0,consiste conceptualmente en múltiples conjuntos de nivel uno,almacenados en discos físicos con un nivel 0 encima,agrupando los anteriores niveles 1,al anidar niveles RAID,se suele combinar un nivel que proporcione redundancia,con un RAID 0,que aumente el rendimiento,con estas configuraciones,es preferible tener el RAID 0 como nivel mas alto y los conjuntos redundantes debajo,porque asi sera necesario reconstruir menos discos,cuando 1 falle,así el RAID 10,es preferible al RAID 0+1,aunque las ventajas administrativas,de dividir el espejo del RAID 1 se perderán,los niveles RAID anidados mas comúnmente usados son:

RAID 0+1(un espejo de divisiones)
RAID 1+0(una división de espejos)
RAID 30(una división de niveles raid con paridad dedicada)
RAID 100(una división,de una división de espejos.

5.3.2._Centros de Respaldo:

-Se trata de otra opción para posibilitar la redundancia y distribución de la información,es un centro de procesamiento de datos,específicamente diseñado para tomar el control de otro CPD principal en caso de contingencia o fallo,un centro de respaldo,se diseña bajo los mismos principios que cualquier CPD,pero bajo algunas consideraciones más. En primer lugar debe elegirse una localización,totalmente distinta a la del CPD principal ,con objeto de que no se vean afectados ambos simultáneamente por la misma contingencia,es habitual situarlos entre 20 y 40 kms del CPD principal esta distancia estará limitada,por las necesidades de comunicaciones entre ambos. En segundo lugar el equipamiento electrónico e informático del centro de respaldo debe ser absolutamente compatible con el existente en el CPD principal,esto no implica que deba ser exactamente igual,normalmente todos los procesos del CPD no son críticos,por este motivo no hay que duplicar todo el equipamiento,por otra parte no se necesita el mismo nivel de servicio en caso de emergencia,en consecuencia es posible utilizar hardware menos potente,la pecera de un centro de respaldo recibe estas denominaciones en función de su equipamiento:

Sala blanca:Cuando el equipamiento es exactamente igual al existente en el CPD principal

Sala de backups:Cuando el equipamiento es similar,pero no exactamente igual
-En tercer lugar el equipamiento software debe ser idéntico al existente en el CPD principal,esto implica exactamente las mismas versiones y parches del software principal o de software base y de las aplicaciones corporativas que estén en explotación en el CPD principal,de otra manera no se podría garantizar totalmente la continuidad de operación,por ultimo es necesario contar con una replica de los mismos datos con los que trabaja el CPD principal este es el problema principal de los centros de respaldo de datos. Existen 2 políticas o aproximaciones a este problema:

Copia síncrona de los datos:Se asegura que todo datos escrito en el CPD principal,también se escribe en el centro de respaldo antes de continuar con otra operación.
Copia asíncrona de los datos:No se asegura que todos los datos descritos en el CPD principal se escriba en el CPD de respaldo por lo que puede existir un desfase temporal entre ambos
-Un centro de respaldo por si solo no basta para hacer frente a una contingencia grave,es necesario disponer de un plan de contingencia corporativo con las actuaciones en caso de incidente.
-El centro de respaldo no es la única manera de articular un plan de contingencias,también es posible el outsourcing(externalización de servicios similares)
5.4._Almacenamiento Remoto:

-Las posibilidades en las redes han crecido exponencialmente en los últimos años estudiando incluso la posibilidad,de eliminar el almacenamiento en el equipo local,hoy en dia existen principalmente 3 tipos de almacenamiento remoto:

SAN(red de almacenamiento)
NAS(almacenamiento conectado en red)
Almacenamiento en la nube.

-El sistema DAS es el método tradicional de almacenamiento y el mas sencillo consiste en conectar el dispositivo de almacenamiento directamente al servidor o estación de trabajo,es decir físicamente conectado al dispositivo que hace uso de él. Es el caso convencional de un disco duro conectado directamente al sistema informático. Una SAN se puede considerar una extensión DE UN DAS,donde en un DAS hay un enlace punto a punto entre el servidor y su almacenamiento una SAN permite a varios servidores acceder a varios dispositivos de almacenamiento, en una red compartida,tanto en SAN como en DAS las aplicaciones hacen sus peticiones de datos,al sistema de ficheros directamente,la diferencia reside en la manera que dicho sistema de ficheros obtiene los datos requeridos del almacenamiento,en DAS el almacenamiento es local mientras que el SAN es remoto. SAN utiliza diferentes protocolos de acceso como FIBBRE CHANEL y GIGABIT ETERNET,en el

lado opuesto de encuentra la tecnología NAS donde las aplicaciones hacen las peticiones de datos a los sistemas de ficheros de manera remota,mediante protocolos CIFS y NFS .

-El rendimiento de la SAN esta directamente relacionado con el tipo de red que se utiliza en el caso de una red de canal de fibra el ancho de banda es de 100MB/s y de puede extender aumentando la cantidad de conexiones de acceso,la capacidad de una SAN se puede extender de una manera casi ilimitada y puede alcanzar cientos y hasta miles de TB,una SAN permite compartir datos entre varios equipos de la red sin afectar al rendimiento porque el trafico SAN,esta totalmente separado del trafico de usuarios,son servidores de aplicaciones que funcionan como una interfaz entre la red de datos(generalmente de fibra) y la red de usuarios(por lo general eternet).Una SAN es mucho mas costosa que una NAS,ya que la primera es una arquitectura completa que utiliza una tecnología que todavía es muy cara

5.5._Copias de Seguridad y Restauración.

Las copias de seguridad(backup) son réplicas de datos que nos permiten recuperar la información original en caso de ser necesario es un archivo digital, un conjunto de archivos o la totalidad de los datos considerados lo suficientemente importantes para ser conservados, estas copias se pueden almacenar en soportes extraíbles en otros directorios o particiones de datos de nuestra máquina en unidades compartidas de otros discos, discos de red o servidores remotos.

La copia de seguridad es útil por varias razones:

-Para restaurar un ordenador a un estado operacional después de un desastre(copia de seguridad del sistema).

-Para restaurar un pequeño número de ficheros despumes de que hayan sido borrados o dañados accidentalmente(copias de seguridad de datos).

En el mundo de la empresa además es útil y obligatorio para evitar ser sancionado por los órganos de control y materias de protección de datos(en España, la Agencia Española de Protección de Datos).

Normalmente las copias de seguridad se suelen hacer en cintas magnéticas si bien dependiendo de lo que se trate podrían usarse CD's, DVD's, discos ZIP, magnetoópticos, pen drive o pueden realizarse en un centro de respaldo remoto propio o vía internet.

La copia de seguridad puede realizarse sobre los datos en los cuales incluyen también archivos que formen parte del sistema operativo, así las copias de seguridad suelen ser utilizadas como la ultima linea de defensa contra perdidas de datos, se convierten por lo tanto en el ultimo recurso a utilizarse.

Las copias de seguridad en un sistema informático tienen por objetivo, mantener cierta capacidad de recuperación de la información ante posibles perdidas, esta capacidad puede llegar a ser muy importante, incluso critico para las empresas.

5.5.1._Modelos de almacén de datos.

Cualquier estrategia de copia de seguridad empieza con el concepto de almacen de datos, los datos de la copia deben ser almacenados de alguna manera y probablemente deban

ser organizados por algún criterio. Para ello se puede utilizar desde una hoja papel con una lista de cintas de la copia de seguridad y las fechas en las que fueron hechas, hasta un sofisticado programa con una base de datos relacional. Cada uno de los distintos almacenes de datos tiene sus ventajas, esto esta muy relacionado con los esquemas de rotación de la copia de seguridad elegido:

-Desectructurado: un almacén desectructurado podría ser simplemente una pila de CD's con una mínima información sobre que ha sido copiado y cuando. Esta es la forma mas fácil de implementar pero ofrece pocas garantías de recuperación de datos.

-Completa+Incremental: Un almacén completo-incremental propone ser mas factible que el almacenamiento de varios copias de la misma fuente del dato. En primer lugar, se realiza la copia de seguridad completa del sistema, mas tarde, se realiza una copia de seguridad incremental, es decir, solo con los ficheros que se haya modificado desde la ultima copia de seguridad. Recuperar y restaurar un sistema completamente a un cierto punto en el tiempo requiere localizar una copia de seguridad completa y todas las incrementales posteriores realizada hasta el instante que se desea restaurar. Los inconvenientes son tener que tratar con grandes series de copias incrementales y contar con un gran espacio de almacenaje.

-Espejo+Diferencial: es similar al almacén completo incremental pero en lugar de hacer un copia completa seguida de incrementales, este modelo ofrece un espejo que refleja el estado del sistema a partir de la ultima copia y un historial de copias diferenciales. Una ventaja de este modelo es que solo requiere una copia de seguridad completa inicial. Cada copia diferencial es inmediatamente añadida al espejo y los ficheros son reemplazados, son movidos a una copia incremental inversa. Una copia diferencial puede sustituir a otra copia diferencial mas antigua sobre la misma copia total.

-Protección continua de datos: este modelo va un paso mas haya y en lugar de realizar copias de seguridad periódicas, el sistema automáticamente registra cada cambio en el sistema anfitrión. Este sistema reduce al mínimo la cantidad de información perdida en caso de desastre.

-Sintética: Esta tecnología permite crear una nueva imagen de copia de respaldo a partir de copias de respaldo anteriormente completas y posteriores incrementales. Es de gran utilidad sobre todo en redes de almacenamiento SAN ya que no es necesaria la participación del host/nodofinal quitándole mucha carga de proceso.

5.5.2._Diseño de estrategias de Backup.

Un esquema de copias de seguridad efectiva debe tener en consideración la limitaciones de la situación, todo esquema tiene cierto impacto en el sistema que ha sido copiado, si este impacto es significativo, la copia debe ser acotada en tiempo. Todos los soportes de almacenamiento tienen una capacidad limitada, finita y un coste real. Buscar la cantidad correcta de capacidad acorde con las necesidades de la copia de seguridad es una parte importante del diseño de la copia. Alcanzar los objetivos definidos en vista de la limitaciones puede ser una tarea muy difícil. Habrá que tener en cuenta:

Horarios: programar un horario de ejecución de las copias aumenta considerablemente su efectividad y nivel de optimización. Muchos paquetes software ofrecen esta posibilidad.

Autenticación: para poder copiar todos los datos, dentro o fuera del sistema, se requiere acceso sin restricción. Utilizar un mecanismo de autenticación es una buena manera de evitar que el esquema sea usado por actividades sin autorizar.
Cadena de confianza: los soportes de almacenamiento portátiles son elementos físicos que deben ser gestionados por personas de confianza. Establecer una cadena de confianza es critico para la seguridad de los datos.
Reportando: en configuraciones mas largas los reportes o informes son útiles para monitorizar los medios usados, el estado de los dispositivos, errores, coordinación de saltos y cualquier otra información sobre el proceso de Backup.
Verificación: muchos programas de copia de seguridad hacen uso de Check-sum y Hashes, esto ofrece muchas ventajas:
Permiten la integridad de los datos ser verificados sin hacer referencia al archivo original. Algunos programas de copia de seguridad pueden utilizar los Check-sum para evitar redundancias en las copias de archivos y así mejorar las redundancias de las copias.

5.5.3. Manipulación de los datos.

Es una practica habitual manipular los datos guardados en las copias de seguridad para optimizar tanto los procesos de copia como el almacenamiento.
Compresión: la compresión es el mejor método para disminuir el espacio de almacenaje y reducir el coste.
Redundancia: cuando varios sistemas guardan sus copias en el mismo sistema de almacenamiento existe la posibilidad de redundancia de los datos copiados. Si tenemos estaciones de trabajo con el mismo sistema operativo, compartiendo el mismo almacén de datos, es posible que la gran mayoría de archivos sean comunes. El almacén de datos realmente solo necesita almacenar una copia de estos ficheros para luego ser usada para cualquier estación. Esta técnica se puede realizar a través de fichero o incluso a nivel de bloque.
Desduplicación: a veces las copias de seguridad están duplicadas en un segundo soporte para optimizar velocidades de restauración(en paralelo) o incluso disponer de una sola copia,a salvo, en un lugar diferente.
Cifrado: usar soportes de almacenamiento desmontable o portátiles implica el riesgo de perderse o ser robados. Cifrar la información puede mitigar este problema aunque presenta nuevos inconvenientes. Cifrar es un proceso que consume mucho tiempo de CPU y puede bajar la velocidad de copiado y en segundo lugar, la compresión es menos eficaz.

5.5.4. Software de backup y restauración.

Es importante definir previamente los requerimientos específicos para determinar el software adecuado. Entre los mas populares se encuentran Cobian,SECOFI y copiadata aunque existen infinidad de programas adaptados a cada necesidad. Para adecuación a la LOPD de ficheros con datos de carácter personal de nivel alto(salud, religión, etc) la regulación exige copias de datos cifrados y en ubicación diferente al lugar de origen, para estos casos, lo mejor es contar con un software que realice copias de manera automática almacenando los datos cifrados en un centro de datos externo. Es muy importante que nos cercioremos de que hacemos copias correctamente y comprobemos que somos capaces de

restaurarlas en su ubicación original. En el hipotético caso de que no pudiéramos restaurar nuestra información existe una ultima alternativa en el mercado que son las aplicaciones de recuperación de datos como Free doctor, estelar... También existen métodos de recuperación vía web como E-ROL. Por ultimo, hay casos extremos como unidades dañadas, podríamos recurrir a laboratorios especializados en recuperación de datos como Discovery Labs para el usuario hogareño, existe la posibilidad de usar cuentas de correo para mantener las copias de seguridad.

TEMA 6 - SEGURIDAD EN REDES Editar 0 20…

6.1. Aspectos Generales

Sin importar que estén conectadas por cable o de manera inalámbrica, las redes de computadoras cada vez se tornan mas esenciales para las actividades diarias. Tanto las personas como las organizaciones dependen de sus computadoras y de las redes para funciones como correo electrónico, contabilidad, organización y administración de archivos.

Las intrusiones de personas no autorizadas pueden causar interrupciones costosas en la red y pérdidas de trabajo, los ataques a una red pueden ser devastadores y pueden causar pérdida de tiempo y de dinero debido a los daños o robos de información o de archivos importantes.

A los intrusos que obtienen acceso mediante la modificación del software o la explotación de las vulnerabilidades del software se les denominan "Piratas Informáticos". Una vez que un pirata tiene el acceso a una red pueden surgir 4 tipos de amenazas:

Robo de información
Robo de identidad
Perdida y manipulación de datos
Interrupción del servicio.

Las amenazas de seguridad causadas por intrusos en la red pueden originarse tanto en forma interna como externa.

-Amenazas externas: Provienen de personas que no tienen autorización para acceder al sistema o a la red de computadoras. Logran introducirse principalmente desde Internet, enlaces inalámbricos o servidores de acceso por marcación o dial-

-Amenazas internas: Por lo general, conocen información valiosa y vulnerable o saben cómo acceder a esta. Sin embargo, no todos los ataques internos son intencionados.

Con la evolución de los tipos de amenazas, ataques y explotaciones se han acuñado varios términos para describir a las personas involucradas

Hacker: un experto en programación. Recientemente este término se ha utilizado con frecuencia con un sentido negativo para describir a una persona que intenta obtener acceso no autorizado a los recursos de la red con intención maliciosa.

Hacker de sombrero blanco: una persona que busca vulnerabilidades en los sistemas o en las redes y a continuación informa a los propietarios del sistema para que lo arreglen.
Hacker de sombrero negro: utilizan su conocimiento de las redes o los sistemas informáticos para beneficio personal o económico, un cracker es un ejemplo de hacker de sombrero negro.
Cracker: es un término más preciso para describir a una persona que intenta obtener acceso no autorizado a los recursos de la red con intención maliciosa.
Phrieaker: persona que manipula la red telefónica para que realice una función que no está permitida. Por lo general, a través de un teléfono público para realizar llamadas de larga distancia gratuitas.
Spammer: persona que envía grandes cantidades de mensajes de correo electrónico no deseado, por lo general, los spammers utilizan virus para tomar control de las computadoras domesticas y utilizarlas para enviar mensajes masivos.
Estafador: utiliza el correo electrónico u otro medio para engañar a otras personas para que brinden información confidencial como número de cuenta o contraseñas.

Estos son los delitos informáticos más frecuentes en la red:

Abuso del acceso a la red por parte de personas que pertenecen a la organización.
Virus.
Suplantación de identidad.
Uso indebido de la mensajería instantánea.
Denegación de servicio, caída de servidores.
Acceso no autorizado a la información.
Robo de información de los clientes o de los empleados.
Abuso de la red inalámbrica
Penetración en el sistema.
Fraude financiero.
Detección de contraseñas.
Registro de claves.
Alteración de sitios web.
Uso indebido de una aplicación web publica.

Hay diversos tipos de ataques informáticos en redes, algunos son:
Ataques de denegación de servicios (DOS): es un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a usuarios legítimos, normalmente provocando la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.
Man in the middle (MITM): es una situación donde un atacante supervisa (generalmente mediante un rastreador de puertos) una comunicación entre las 2 partes y falsifica los intercambios para hacerse pasar por una de ellas.
Ataques de replay: una forma de ataque de red en el cual una trasmisión de datos válida es maliciosa o fraudulentamente repetida o recalcada, es llevada a cabo por el autor o por

un adversario que intercepta la información y la retransmite posiblemente como parte de un ataque enmascarado.

6.2.CORTAFUEGOS

En el Protocolo TCP/IP el puerto es una numeración lógica que se asigna a las conexiones tanto en origen como en destino sin significación física. El permitir o denegar acceso a los puertos es importante por que las aplicaciones servidoras deben escuchar en un puerto conocido de antemano para que un cliente pueda conectarse. Esto quiere decir que cuando el sistema operativo recibe una petición a ese puerto la pasa a la aplicación que escucha en él (si hay alguna) y a ninguna otra. Los servicios mas habituales tienen asignados los llamados puertos bien conocidos por EJe: 80 para Servidor web, 21: Puerto FTP, 23: TELNET etc.
Así pues cuando pides acceso a una pagina web su navegador pide acceso al puerto 80 del servidor web y si este numero no se supiera de antemano o estuviera bloqueado no podría recibir la pagina.

Un puerto puede estar:
ABIERTO: Acepta conexiones hay una aplicación escuchando en este puerto. Esto no quiere decir que se tenga acceso a la aplicación solo que hay posibilidades de conectarse.
CERRADO: se rechaza la conexión. Probablemente no hay aplicación escuchando en este puerto o no se permite acceso por alguna razón. Este es el comportamiento normal del sistema operativo.
BLOQUEADO O SIGILOSO: no hay respuesta, este es el estado real para un cliente en Internet. De esta forma ni siquiera se sabe si el ordenador esta conectado. Normalmente este comportamiento se debe a un cortafuegos o a que el ordenador esta apagado. Para controlar el estado de los puertos de conexión a redes TCP-IP y por tanto las aplicaciones que lo usan emplearemos un cortafuegos (firewall).

El cortafuegos o Firewall es una parte de un sistema o una red que esta diseñada para bloquear el acceso no autorizado permitiendo al mismo tiempo comunicaciones autorizadas. Los cortafuegos pueden ser hardware o software o una combinación de ambos y se utilizan con frecuencia para que una serie de usuarios autorizados se conecten a una red privada o Intranet.

Firewall: Todos los paquetes de la red pasan por el cortafuegos que examina y bloquea loa que no cumplen los criterios de seguridad especificados. Algunos cortafuegos muestran un mensaje al usuario mostrando el programa o proceso que solicita la comunicación preguntándole si la permite o la deniega. El problema surge cuando el nombre del proceso que muestran no lo reconocemos o que tiene el mismo que un proceso confiable conocido, en este caso hay que tener en cuenta varias cosas : si deniego el acceso a un programa este puede no funcionar, la siguiente vez que me pregunte le permitiré el acceso y en caso de funcionar la próxima vez que me pregunte le permitiré acceso permanentemente es importante leer siempre los mensajes para permitir o denegar acceso.

VENTAJAS de un cortafuegos:
Protege de intrusiones, el acceso a ciertos segmentos de la red sólo se permite a maquinas autorizadas de otros segmentos o de Internet.
Protección de la información privada: permite definir distintos niveles de acceso a la información de manera que cada grupo de usuarios definido tenga solo acceso a los servicios e información que les son estrictamente necesarios.
Optimización de acceso: Identifica los elementos de la red internos y optimiza que la comunicación entre ellos sea mas directa.
LIMITACIONES de un cortafuegos: Cualquier tipo de ataque informático que use trafico aceptado por el cortafuegos o que sencillamente no use la red seguirá constituyendo una amenaza.

POLÍTICAS del cortafuegos: Hay 2 políticas básicas que cambian radicalmente la filosofía de la seguridad de la información:
Políticas restrictiva: se deniega todo el trafico excepto el que esta explicita mente permitido hay que habilitar expresamente los servicios que se necesiten.
Política permisiva: se permite todo el trafico excepto el que esta denegado. Cada servicio potencialmente peligroso necesitara ser aislado mientras que el resto de trafico no sera filtrado.
La política restrictiva es la mas segura ya que tiene control para no permitir trafico peligroso. Sin embargo la política permisiva es posible que no haya contemplado trafico peligroso y sea aceptado por omisión. No es recomendable tener mas de un cortafuegos ejecutándose simultáneamente en la misma maquina.
cortafuegos.svg.png

Una zona desmilitarizada o red perimetral es un área local que se ubica entre la red interna de una organización y una red externa, generalmente Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa. Los equipos en la DMZ no pueden conectar con la red interna. Esto permite que los equipos de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la

zona desmilitarizada se convierte en un callejón sin salida. La DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores de correo electrónico, servidores Web y DNS.
images.jpg

im

6.3.-Listas de control de acceso(ACL) y filtrado de paquetes.

Una lista de control de acceso o ACL es un concepto de seguridad informática usado para fomentar la separación de privilegios, es una forma de determinar los permisos de acceso apropiados a un determinado objeto dependiendo de diferentes aspectos del proceso que hace el pedido. Las ACL permiten controlar el flujo del tráfico en equipos de redes como routers y witches, su principal objetivo es filtrar tráfico permitiendo o denegando el trafico de red de acuerdo a alguna condición, sin embargo, también tienen usos adicionales como por ejemplo distinguir tráfico prioritario.

Las listas de control de acceso pueden configurarse para controlar el tráfico entrante y saliente y en este contexto son similares a un cortafuegos. Se pueden considerar como cada una de las reglas individuales que controlan y configuran un cortafuegos.

6.3.1.-ACL en routers.

En el caso concreto de los routers de la compañía CISCO las ACL son listas de condiciones que se aplican al tráfico que viaja a través de una interfaz del router y se crean según el protocolo la dirección o el puerto a filtrar. Estas listas indican al router qué tipos de paquetes se deben aceptar o desplazar en las interfaces del router, ya sea a la entrada o a la salida.

Las razones principales para crear las ACL son:

Limitar el tráfico de la red.
Mejorar el rendimiento de la red.
Controlar el flujo del tráfico decidiendo qué flujo de tráfico se bloquea y cúal se permite ya sea por direccionamiento o por servicios de la red.
Proporcionar un nivel básico de seguridad para el uso de la red

Existen 2 tipos de ACL:

1. ACL estándar: Especificamos una sola dirección de origen.

2. ACL extendida: Especificamos una dirección de origen y de destino, se utilizan más que las estándar porque ofrecen un mayor control, verifica las direcciones de paquetes de origen y destino y también protocolos y números de puertos.

6.3.2.-IPTABLES.
El cortafuegos utilizado para gestionar las conexiones de red de los sistemas GNU Linux desde la versión 2.4 del núcleo es IPTABLES, las posibilidades de IPTABLES son prácticamente infinitas y un administrador que quiera sacarle el máximo provecho puede realizar configuraciones extremadamente complejas, para simplificar, diremos que básicamente IPTABLES permite crear reglas que analizarán los paquetes de datos que entran, salen o pasan por nuestra máquina y en función de las condiciones que mantengamos, tomaremos una decisión que normalmente sera permitir o denegar que dicho paquete siga su curso. El cortafuegos controla las comunicaciones entre la red y el exterior para crear las reglas podemos analizar muchos aspectos de los paquetes de datos, podemos filtrar paquetes en función de:

Tipo de paquete de datos:
IMPUT(paquetes que llegan a nuestra maquina).
OUTPUT(paquetes que salen de nuestra maquina).
FORWARD(paquetes que pasan por nuestra maquina).

Interfaz por la que entran (-i) o salen (-o) los paquetes: ETH0, wlan1.

IP origen de los paquetes(-s): IP concreta(10.0.1.3),rango de red(10.0.1.0/8)

IP destinada a los paquetes(-d): IP concreta, 2 rango de red.
Protocolo de los paquetes (-t): TCP, UDP, CMP...

Hacer NAT es modificar IP origen y destino para conectar nuestra red a otra red o a Internet
y hacer pre-routing es filtrar antes de enrutar
y hacer post-routing es filtrar después de enrutar.

Una forma sencilla de trabajar con IPTABLES es permitir las comunicaciones que interesen y luego denegar el resto de la comunicaciones, lo que se suele hacer es definir la política por defecto, aceptar, después crear reglas concretas para permitir las comunicaciones que nos interesen y finalmente denegar el resto de comunicaciones, lo mejor sera crear un script en el que dispondremos de la secuencia de reglas que queremos aplicar a nuestro sistema.

6.4.Redes inalámbricas.

Los cables que se suelen usar para construir redes locales van desde el cable telefónico hasta la fibra óptica. Algunos edificios se construyen con los cables instalados para evitar gasto de tiempo y dinero posterior y de forma que se minimice el riesgo de un corte, rozadura u otro daño accidental. Los riesgos mas comunes para el cableado se pueden resumir en los siguientes.

Interferencias: estas modificaciones pueden estar generadas por cables de alimentación de maquinaria pesada o por equipos de radio o microondas. Los cables de fibra óptica no sufren el problema de alteración por acción de campos eléctricos, por tanto son mas seguros.

Corte del cable: la conexión establecida se rompe lo que impide que el flujo de datos circule por el cable.

Daños en el cable: los daños normales con el uso pueden dañar el apantallamiento que preserva la integridad de los datos transmitidos o dañar al propio cable lo que hace que las comunicaciones dejen de ser fiables.

La mayoría de las organizaciones clasifican estos problemas como daños naturales sin embargo también se puede ver como un medio para atacar la red si el objetivo es únicamente interferir en su funcionamiento

El cable de red ofrece también un nuevo frente de ataque para un determinado intruso que intentase acceder a los datos esto se puede hacer:

Desviando o estableciendo una conexión no autorizada en la red

Un sistema de administración y procedimiento de identificación de acceso adecuado, hace difícil que se puedan obtener privilegios de usuarios en la red pero los datos que fluyen a través del cable pueden estar en peligro

Haciendo una escucha sin establecer conexión, los datos se pueden seguir y pueden verse comprometidos.

Luego no hace falta penetrar en los cables físicamente para obtener los datos que transportan. En ocasiones para mejorar la seguridad de las comunicaciones cableadas se adoptan medidas como:

Cableado de alto nivel de seguridad: son cableados de redes que se recomiendan para instalaciones con grado de seguridad militar, el objetivo es impedir la posibilidad de infiltraciones y monitoreo de la información que circula por el cable. Consta de un sistema de tubos herméticamente cerrados por cuyo interior circula aire a presión y el cable, a lo largo de la tubería, hay sensores conectados a una computadora, si se detecta algún tipo de variación de presión se dispara un sistema de alarma.

Protección electromagnética: cableado coaxial y de pares, ftp y stp.

6.4.1.¿Qué es una red inalámbrica?

Es una red que permite a sus usuarios conectarse a una red local o a Internet sin estar conectados físicamente mediante cables ya que los datos se transmiten por el aire, los dispositivos que nos permiten interconectar dispositivos inalámbricos son los puntos de acceso que controlan el acceso y las comunicaciones de usuarios conectados a la red y las tarjetas receptoras, para conectar una computadora, ya sean internas (DCI) o USB. Los puntos de acceso funcionan a modo de emisor remoto, es decir, se instalan en lugares donde la señal inalámbrica se quiera difundir y reciben la señal bien por un cable o bien capturan la señal débil inalámbrica y la amplifica.

Los puntos de acceso pueden estar integrados con módems o routers inalámbricos convencionalmente denominado router wifi, los paquetes de información en las WLAN viajan en forma de ondas de radio que pueden viajar mas haya de las paredes y filtrarse en habitaciones, casas o habitaciones contiguas o llegar hasta la calle. Si nuestra instalación esta abierta sin seguridad, una persona con conocimientos básicos podría no sólo utilizar nuestra conexión a Internet,si no también acceder a nuestra red interna o a nuestro equipo donde podríamos tener carpetas compartidas o analizar toda la información que viaja por nuestra red mediante sniffers y obtener así contraseñas de nuestra cuenta de correo, contenido de nuestras conversaciones, etc.

Si la infiltración no autorizada de por si ya es grave en una instalación residencial(casa) mucho mas peligroso es en una instalación corporativa o empresarial y desgraciadamente, las redes cerradas son mas bien escasas.

6.4.2.Consejos de seguridad.

Asegurar el punto de acceso por ser un punto de control de las comunicaciones de todos los usuarios y por tanto críticos en las redes inalámbricas:

Cambia la contraseña por defecto: todos los fabricantes ofrecen un password por defecto de acceso a la administración del punto de acceso, al usar un fabricante la misma contraseña para todos sus equipos es fácil o posible que el observador la conozca.

Aumentar la seguridad de los datos transmitidos: usar encriptación WEP o WPA, las redes inalámbricas basan su seguridad en la encriptacion de los datos que viajan a través de aire. El método habitual es la encriptación WEP pero no podemos mantener WEP como única estrategia de seguridad ya que no es del todo seguro, existen aplicaciones para Linux o Windows que escaneando suficientes paquetes de información son capaces de obtener las claves WEP y permitir acceso de intrusos en nuestra red. Activa la encriptación de 128bits WEP mejor que la de 64bits. Algunos puntos de acceso más recientes soportan también encriptación WPA y WPA2, encriptación dinámica y más segura que WEP, si activas WPA en el punto de acceso tanto los accesorios como los dispositivos WLAN de tu red como tu sistema operativo debe de soportar.

Ocultar tu red WIFI: cambia el SSID por defecto en lugar de mi AP o Apmanolo o el nombre de la empresa es preferible coger algo menos atractivo como wroken, down o desconectado, si no llamamos la atención del observador hay menos posibilidades de que este intente entrar en nuestra red.

Desactiva también el broadcasting SSID o identificador de la red inalámbrica. El broadcasting SSID permite que los nuevos equipos que quieran conectarse a la red wifi

identifiquen automáticamente el nombre y los datos de la red inalámbrica evitando así la tarea de configuración manual. Al desactivarlo tendrás que introducir manualmente el SSID en la configuración de cada nuevo equipo que quieras conectar.
Evitar que se conecten:
Activa el filtrado de direcciones mac: para activar el filtrado mac dejaras que solo los dispositivos con las direcciones mac especificadas se conecten a tu red wifi. Por un lado es posible conocer las direcciones mac de los equipos que se conectan a la red con tan solo escuchar con el programa adecuado ya que las direcciones mac se transmiten en abierto sin encriptar entre el punto de acceso y el equipo, además aunque en teoría las direcciones mac son únicas a cada dispositivo de red y no pueden modificarse hay comando o programas que permiten simular temporalmente por software una nueva dirección mac para una tarjeta de red.
Establece el número máximo de dispositivos.
Desactiva DHCP en el router o en el punto de acceso en la configuración de los dispositivos o accesorios WIFI, tendrás que introducir a mano la dirección IP, la puerta de enlace, la máscara de subred y los DNS. Si el observador conoce el rango de IP que usamos en nuestra red no habremos conseguido nada con este punto.
Desconecta el AP cuando no lo uses: el AP almacena la configuración y no necesitaras introducirla de nuevo cuando lo conectes.
Cambia las claves regularmente: puede ser necesario entre 1 y 4 GB de datos para romper una clave WEP dependiendo de la complejidad de las claves de manera que cuando llegue a este caudal de infor4macion transmitida es recomendable cambiar las claves.
Tema 7. Criptografía.

A lo largo de la historia el ser humano ha desarrollado unos sistemas de seguridad que le permiten comprobar en una comunicación la identidad del interlocutor(tarjetas de identificación, firmas) , asegurarse que solo obtendrá la información el destinatario solicitado(correo certificado) que además ésta no podrá ser modificada(notariado) e incluso que ninguna de las 2 partes podrá negar el hecho(notariado firma) ni cuando se produjo(fechado de documentos).
En la mayor parte de los casos el sistema de seguridad se basa en la identificación física de la persona, información que contrasta con el documento de identidad.
Actualmente, cada vez mayor número de actividades se están trasladando al mundo electrónico a través de internet, se hace por lo tanto necesario trasladar también los sistemas de seguridad a este contexto en el que el principal problema reside en que no existe contacto directo entre las partes implicadas.
Necesitamos un documento digital que ofrezca las mismas funcionalidades que los documentos físicos con el añadido de ofrecer garantías aun sin presencia física.
¿Cómo se resuelve este problema? Gracias a mecanismos criptográficos cuyos elementos fundamentales son el certificado digital y la firma electrónica.

7.1. Principios de la criptografía.
La criptografía es el arte o la ciencia de cifrar o descifrar información mediante técnicas especiales y se emplea frecuentemente para permitir un intercambio de mensajes que solo

puedan ser leídos por personas a las que van dirigidos y que poseen los medios para descifrarlos.
Con mas precisión cuando se habla de esta área de conocimiento como ciencia se debería hablar de criptología que engloba tanto a las técnicas de cifrado, es decir la criptografía como sus técnicas complementarias entre las cuales se incluye el criptoanálisis que estudia métodos empleados para romper textos cifrados con objeto de recuperar la información original en ausencia de claves.
La criptografía se considera una rama de las matemáticas y en la actualidad de la informática y la telemática que hace uso de métodos y técnicas matemáticas con el objeto principal de cifrar un mensaje o archivo por medio de un algoritmo usando una o mas claves.
En la jerga de la criptografía, la información original que debe protegerse se denomina texto en claro o texto plano, el cifrado es el proceso de convertir el texto plano en un galimatías ilegible denominado texto cifrado o criptograma. Por lo general, la aplicación concreta del algoritmo de cifrado(cifra) se basa en la existencia de una clave, información secreta que adapta el algoritmo de cifrado para cada uso distinto.
Las 2 técnicas mas sencillas de cifrado en la criptografía clásica son la sustitución(que supone el cambio de significado de los elementos básicos del mensaje, las letras, los símbolos o los dígitos) y la transposición(supone una reordenación de los mismos).
La gran mayoría de las cifras básicas son combinaciones de estas 2 operaciones bascas.
El descifrado es el proceso inverso que recupera el texto plano a partir del criptograma y la clave. El protocolo criptográfico especifica los detalles de como se utiliza los algoritmos y las claves(y otras operaciones primitivas) para conseguir el efecto deseado. El conjunto de protocolos, algoritmos de cifrado, procesos de gestión de claves y actuaciones de los usuarios es lo que constituye en conjunto un criptosistema que es con lo que el usuario final trabaja e interactúa.
Existen 2 grandes grupos de cifras, los algoritmos que solo utilizan una clave tanto en el proceso de cifrado como en el de descifrado y los que emplean una clave para cifrar mensajes y una clave distinta para descifrarlos. Los primeros se denominan cifrar simétricas de clave simétrica o de clave privada y son la base de los algoritmos de cifrado clásico. Los segundos se denomina cifras asimétricas de clave asimétrica o de clave publica y forman el núcleo de las técnicas de cifrado modernas.
En el lenguaje cotidiano la palabra código se usa de forma indistinta con cifra, en la jerga de la criptografía sin embargo el termino tiene un uso técnico especializado: los códigos son un método de criptografía básica que consiste en sustituir unidades textuales mas o menos larga o complejas al igualmente palabras o frases para ocultar el mensaje; por ejemplo cielo azul podría significar apagar al amanecer. Por el contrario las cifrar clásicas normalmente sustituyen o reordenan los elementos básicos del mensaje, letras, dígitos o símbolos en el ejemplo anterior "RCNM ARCTEEAAL AAA" seria un criptograma obtenido por transposición. Cuando se usa una técnica de códigos la información secreta suele recompilarse en un libro de códigos.

7.1.1. Criptografía simétrica.

La criptografía simétrica es un método criptográfico en el cual se usa la misma clave para cifrar y descifrar mensajes, las 2 partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar.
Un buen sistema de cifrado pone toda la seguridad en la clave y ninguna en el algoritmo, en otras palabras, no debería ser de ninguna ayuda para un atacante conocer el algoritmo que se está usando, solo si el atacante obtuviera la clave le serviría conocer el algoritmo, los algoritmos ampliamente utilizados tienen estas propiedades(por ejemplo GNU PJ).
Dado que toda la seguridad esta en la clave, es importante que sea muy difícil adivinar el tipo de clave, esto quiere decir, que el abanico de claves posibles debe ser amplio.
Actualmente, los ordenadores pueden descifrar claves con extrema rapidez y esta es la razón por la cual el tamaño de clave es importante en los criptosistemas modernos.
El algoritmo DES usa una clave de 56bits lo que significa que hay 2elevado56 claves posibles, esto representa un numero muy alto de claves pero un ordenador genérico puede comprobar el conjunto posible de claves en cuestión de días, una máquina especializada puede hacerlo en horas.
Algoritmos de cifrado de diseño mas reciente como 3DES, LOUFISH e IDEA usan claves de 128bits lo que significa que existen 2elevado128 claves posibles. La mayoría de las tarjetas de crédito y otros medios de pago electrónico tienen como estándar el algoritmos 3DES.
El principal problema de los sistemas de cifrado simétrico no esta ligado a su seguridad si no al intercambio de claves. Una vez que el remitente y el destinatario hayan intercambiado las claves pueden usarlas para comunicarse con seguridad, sería mucho mas fácil para un atacante intentar interceptar una clave que probar las posibles combinaciones del espacio de claves.
Otro problema es el numero de claves que se necesitan, si tenemos un numero n de personas que necesitan comunicarse entre si se necesitan n/2 claves para cada pareja de personas que tengan que comunicarse de modo privado. Esto puede funcionar con un grupo reducido de personas pero seria imposible llevarlo a cabo con grupos más grandes.

7.1.2. Ataques criptográficos.

En criptografía se denomina ataque de fuerza bruta a la forma de recuperar una clave probando todas las combinaciones posibles hasta encontrarla. Dicho de otro modo, define al procedimiento por el cual a partir del conocimiento del algoritmo de cifrado empleado y de un par texto claro-texto cifrado se realiza el cifrado y respectivamente de descifrado de uno de los miembros del par con cada una de las posibles combinaciones de clave hasta obtener el otro miembro del par. El esfuerzo requerido para que la búsqueda sea exitosa con probabilidad mejor que la par será 2elevado-n operaciones donde n es la longitud de la clave.
Otro factor determinante en el coste de realizar un ataque de fuerza bruta es el juego de caracteres que se pueden utilizar en la clave. Contraseñas que solo utilicen dígitos numéricos serán mas fáciles de descifrar de aquellas que incluyen otros caracteres como letras, la complejidad compuesta por la cantidad de caracteres en una contraseña es logarítmica.
Los ataques por fuerza bruta son muy costosos en en tiempo computacional por lo que suelen combinarse con un ataque de diccionario.

Un ataque de diccionario es un método de cracking que consiste en intentar de averiguar una contraseña probando todas las palabras del diccionario. Este tipo de ataque suele ser mas eficiente que un ataque de fuerza bruta ya que muchos usuarios suelen utilizar un palabra existente en un lengua como contraseña para que sea fácil de recordar, lo cual no es una practica recomendable.
Los ataques de diccionario tienen pocas probabilidades de éxito con sistemas que emplean contraseñas fuertes con letras en mayúscula y minúscula mezcladas por números y con cualquier tipo de símbolos. Sin embargo, para la mayoría de los usuarios recordar contraseñas tan complejas resulta complicado. Existen variantes que comprueban también alguna de las típicas sustituciones (determinadas letras con números, intercambio de 2 letras, abreviaciones) así como distintas combinaciones de mayúsculas y minúsculas.
Otra solución habitual para no tener que memorizar un numero elevado de contraseñas es utilizar un gestor de contraseñas. Estos programas también nos pueden ayudar a generar contraseñas seguras(asegurándonos que no se trate de un spyware).
Una forma sencilla de proteger un sistema contra los ataques de fuerza bruta o los ataques de diccionario es establecer un numero máximo de tentativas, de esta forma se bloquea el sistema automáticamente después de un numero de intentos infructuosos predeterminados. Un ejemplo de este tipo de sistema es el mecanismo empleado en las tarjetas SIM que bloquea automáticamente tras 3 intentos fallidos al introducir el código PIN.
Para solucionar estos problemas, se mejora la seguridad de los sistemas mediante la criptografía asimétrica y la criptografía híbrida.

7.1.3. Criptografía de clave asimétrica.

En este caso, cada usuario del sistema criptográfico ha de poseer una pareja de claves:
Clave privada: Será custodiada por su propietario y nos se dará a conocer a ningún otro.
Clave pública: Será conocida por todos los usuarios.

Esta pareja de claves es complementaria, lo que cifra una, solo lo puede descifrar la otra y viceversa. Estas claves se obtienen por métodos matemáticos complicados de forma que por razones de tiempo de computo es imposible conocer una clave a partir de la otra.
Los sistemas de cifrado de clave pública se basan (en funciones HASH de un solo sentido) que aprovechan particularidades por ejemplo de los números primos. Una función de un solo sentido es aquella cuya computación es fácil mientras que su inversión resulta extremadamente difícil pero tiene una trampa, esto quiere decir que si se conociera alguna pieza de la información sería fácil computar el inverso. Dado un cifrado de clave publica basado en factorización de números primos, la clave publica contiene un numero compuesto de dos factores de números primos grandes y el algoritmo de cifrado usa este compuesto para cifrar el mensaje. El algoritmo para descifrar el mensaje requiere el conocimiento de los factores primos par que el descifrado sea fácil si poseemos la clave privada que contiene uno de los 2 factores pero extremadamente difícil en caso de no tener ninguno.
Como los sistemas de cifrado simétricos buenos, con un buen sistema de cifrado de clave pública, toda la seguridad descansa en la clave y no en el algoritmo. Por lo tanto el tamaño

de la clave es una medida de la seguridad del sistema pero no se puede comparar con el tamaño de la clave del cifrado simétrico para medir la seguridad.
En un ataque de fuerza bruta sobre un cifrado de clave publica con un tamaño de 512bits, el atacante debe factorizar un numero compuesto codificado en 512bits(hasta 155 dígitos decimales). La cantidad de trabajo para el atacante será diferente dependiendo del cifrado que esté atacando. Mientras 128bits son suficientes para cifrados simétricos, se recomienda el uso de claves publicas de 1024bits para la mayoría de los casos.

La mayor ventaja de la criptografía asimétrica es que se puede cifrar con una clave y descifrar con otra pero el sistema tiene bastantes desventajas:
Para una misma longitud de clave y mensaje se necesita mayor tiempo de proceso.
Las claves deben ser de mayor tamaño que las simétricas.
El mensaje cifrado ocupa mas espacio que el original.
El sistema de criptografía de curva elíptica representa una alternativa menos costosa para este tipo de problemas.

Herramientas como PGP, SSH o la capa de seguridad SSL utilizan un híbrido formado por la criptografía asimétrica para intercambiar claves de criptografía simétrica y la criptografía simétrica para la transmisión de la información.
Algunos algoritmos de técnicas de clave asimétrica son:
Diffie-Hellman
RSA
DSA
ELGAMAL
Criptografía de curva elíptica.
-Otros algoritmo de clave asimétrica pero inseguros:
MEKLE-HELLMAN.
KNAPSACK
Algunos protocolos que usan los algoritmos antes citados son:
DSS con el algoritmo DSA.
PGP.
GPG, una implementación de OPENPGP.
SSH.
SSL.
TLS.
El beneficio obtenido consiste en la supresión de la necesidad del envío de la clave siendo por lo tanto un sistema mas seguro.
El inconveniente es la lentitud de la operación. Para solventar dicho inconveniente el procedimiento que suele seguirse para realizar el cifrado de un mensaje es utilizar un algoritmo de clave pública junto a uno de clave simétrica.

7.1.4. Cifrado de clave pública.
El uso de claves asimétricas ralentiza el proceso de cifrado para solventar dicho inconveniente se utiliza un algoritmo de clave pública junto a uno de clave

simétrica,veamos cual es el procedimiento:Ana y Bernardo tienen sus pares de claves respectivas,Ana escribe un mensaje a Bernardo lo cifra con clave simétrica(clave de sesión que se genera aleatoriamente),para enviar la clave de sesión de forma segura esta se cifra con la clave publica de Bernardo. Bernardo recibe el mensaje cifrado y en primer lugar utiliza su clave privada para descifrar la clave de sesión,una vez obtenida esta ya puede descifrar el mensaje original.
Con este sistema conseguimos:
Confidencialidad:solo podrá leer el mensaje el destinatario del mismo.
Integridad:el mensaje no podrá ser modificado.
Pero todavía quedan sin resolver los problemas de autenticación y no repudio
7.1.5. Firma digital.
La firma digital permite al receptor verificar la autenticidad del origen de la información así como verificar que dicha información no ha sido modificada desde su generación, de este modo ofrece soporte para la autenticación e integridad así como para el no repudio en origen ya que la persona origina un mensaje firmado digitalmente no puede argumentar que no lo es. La firma digital es un cifrado del mensaje que se está afirmando pero con la clave privada del emisor, sin embargo, ya se ha comentado el principal inconveniente de los algoritmos de clave publica, su lentitud que crece con el tamaño del mensaje a cifrar. Para evitar este problema, la firma digital hace uso de funciones de HASH, una función HASH es una operación que se realiza sobre un conjunto de datos de cualquier tamaño de tal forma que se obtiene como resultado otro conjunto de datos denominado resumen de tamaño fijo e independiente del tamaño original que además tiene la propiedad de estar asociado unívocamente a los datos iniciales, es decir, que es prácticamente imposible encontrar 2 mensajes distintos que tengan un resumen HASH idéntico.
Veamos cual es el procedimiento: Ana escribe un mensaje a Bernardo, es necesario que Bernardo pueda verificar realmente que es Ana quien ha enviado el mensaje, por lo tanto Ana tiene que firmarlo:
Resume el mensaje o datos mediante una función HASH.
Cifra el resultado de la función HASH con su clave privada, de esta forma obtiene su firma digital.
Envia el mensaje original a Bernardo junto con su firma.
Descifra el resumen del mensaje mediante la clave pública de Ana.
Aplica al mensaje la función HASH para obtener el resumen.
Compara el resultado recibido con el obtenido a partir de la función HASH, si son iguales, Bernardo puede estar seguro de quien ha enviado el mensaje y que éste no ha sido modificado.

SHA y MD5 son 2 ejemplos de este tipo de algoritmos que implementan funciones HASH, el DSA es un algoritmo de firmado de clave publica que funciona como hemos descrito(usado en GNUPG), algunas aplicaciones son: mensajes con autenticidad asegurada, mensaje sin posibilidad de repudio, contratos comerciales electrónicos, factura electrónica, transiciones comerciales electrónicas, notificaciones judiciales electrónicas, voto

electrónico, tramites de seguridad social, contratación publica. Con este sistema conseguimos:autenticación, integridad, no repudio en origen.

7.1.5. Certificados digitales.

Según puede interpretarse de los apartados anteriores, la eficacia de las operaciones de cifrado y firma digital basa en criptografía de clave publica solo esta garantizada si se tiene la certeza de que la clave privada de los usuarios solo es conocida por dichos usuarios y que la clave publica pueda ser dada a conocer a todos los demás usuarios con la seguridad de que no exista confusión entre las claves publicas de los distintos usuarios.

Para garantizar la unicidad de las claves privadas se suele recurrir a soportes físicos tales como tarjetas inteligentes o tarjetas pcmecias que garantizar la duplicidad de claves, además las tarjetas criptográficas suelen estar protegidas por un numero personal o PIN solo conocido por su propietario que garantiza que si se extravía la tarjeta, nadie que no conozca dicho numero podrá hacer uso de ella.

Por otra parte, para asegurar que una determinada clave publica pertenece a un usuario en concreto se utilizan los certificados digitales que son documentos electrónicos que asocian una clave publica con la identidad de su propietario.

En general un certificado digital es un archivo que puede emplear un software para firmar digitalmente archivos en los cuales puede verificarse la identidad del firmante.

La extensión del certificado con clave privada suele ser un .TFX o .P12 mientras que el certificado que no tiene clave privada solo la publica, suele ser de extensión .CER o .CRT.

Adicionalmente además de la clave publica y la identidad de su propietario, un certificado digital puede contener otro atributos para, por ejemplo, concretar el ámbito de utilización de la clave publica, las fechas de inicio y fin de la validez del certificado, etc.

7.1.6. Terceras partes de confianza.

Una vez definido el concepto de certificado digital se plantea una duda, ¿Como puedo confiar si un determinado certificado es valido o si está falsificado? La validez de un certificado es la confianza en que la clave publica contenida pertenece al usuario indicado en el certificado. La validez del certificado en un entorno de clave publica es esencial ya que se debe conocer si se puede confiar o no en que el destinatario del mensaje será o no realmente el que esperamos.

La manera en la que se puede confiar en el certificado de un usuario con el que nunca hemos tenido ninguna relación previa es mediante la confianza en terceras partes, la idea consiste en que 2 usuarios, puedan confiar directamente entre sí, si ambos tiene relación con una tercera parte ya que esta puede dar fe de la fiabilidad de los 2.

La necesidad de una tercera parte confiable(TPC o TTP) es fundamental en cualquier entorno de clave publica de tamaño considerable debido a que es impensable que los usuarios hayan tenido relaciones previas antes de intercambiar información cifrada o firmada. Además la mejor forma de permitir la distribución de claves publicas (o certificados digitales) de los distintos usuarios, es que algún agente en quien todos los usuarios confine se encargue de su obligación en algún repositorio al que todos los usuarios tengan acceso.

En conclusión se podrá tener confianza en el certificado digital de un usuario al que previamente no conocemos si dicho certificado está avalado por una tercera parte en la

que sí confiamos. La forma en la que esta tercera parte avalará que el certificado es de fiar, es mediante su firma digital sobre el certificado. Por tanto, podremos confiar en cualquier certificado digital firmado por una tercera parte en la que confiamos. La tercera parte de confianza que se encarga de la firma digital de los certificados de los usuarios de un entorno de clave publica se conoce con el nombre de autoridad de certificación(AC).
El modelo de confianza basado en terceras partes confiables es la base de la definición de las infraestructuras de la clave publica(ICP o PKI).

7.2. Firma electronica.

7.2.1. DNIE.
El documento nacional de identidad (DNI) emitido por la dirección general de policía, es un documento que acreedita desde hace más de 50 años la identidad, datos personales y la nacionalidad española de su titular.
Con la llegada de la sociedad de la información y la generalización del uso de Internet, se hace necesario adecuar los mecanismos de acreeditación de personalidad a la nueva realidad y disponer de un instrumento eficaz que traslade al mundo digital las mismas certezas con las que operamos cada día en el mundo físico y que esencialmente son:
Acreeditar electrónicamente y de forma indubitada la identidad de la persona.
Firmar digitalmente documentos electrónicos otorgandoles una validez jurídica equivalente a las que le proporciona la firma manuscrita.
Para responder a estas nuevas responsabilidades nace el documento nacional de identidad electronico similar al tradicional y cuya principal novedad es que incorpora un pequeño circuito integrado capaz de guardar de forma segura información y de procesarla internamente.
En la medida en la que el DNI electronico vaya sustituyendo al DNI tradicional y se implante las nuevas aplicaciones, podremos utilizarlo para:
Realizar compras firmadas a través de Internet.
Hacer trámites completos en las administraciones públicas a cualquier hora y sin tener que desplazarse ni hacer colas.
Realizar transaciones seguras con entidades bancarias.
Acceder al edificio donde trabajamos.
Utilizar de forma segura nuestro ordenador personal.
Participar en una conversación por Internet con la certeza de que nuestro interlocutor es quien dice ser.

El DNI electrónico tiene grandes ventajas para el ciudadano:
Desde el punto de vista de la seguridad, el DNI electrónico es un documentos más seguro que el tradicional pues incorpora mayores y más sofisticadas medidas de seguridad que harán virtualmente imposible su falsificación.
Desde el punto de vista de la comodidad, con el DNI electrónico se podrán realizar trámites a distancia y en cualquier momento.
El DNI electrónico se expedirá de forma inmediata.

Hacer trámite sin tener que aportar documentación que ya exista en la Administración, una de las ventajas del uso de DNIE y los servicios de administración electronica basados en él, será la práctica eliminación del papel en la tramitación.
Desde el punto de la economía: el DNI electrónico es un documento más robusto, tiene una duración prevista de unos 10 años, el DNIE mantiene las medidas del DNI tradicional.

En cuanto al chip criptográfico contiene la siguiente información en formato digital:
Un certificado electrónico para autenticar la personalidad del ciudadano.
Un ceritificado electrónico para firmar electrónicamente con la misma validez jurídica que la firma manuscrita.
Certificado de la autoridad de certificación emisora.
Claves para su utilización.
La plantilla biométrica de la impresión dactilar.
La fotografía digital del ciudadano.
La imagen digitalizada de la firma electrónica.
Datos de la afiliación del ciudadano correspondientes con el contenido personalizado en la tarjeta.

Los elementos de seguridad del documento para impedir su falsificación :
Medidas de seguridad físicas:
Visibles a simple vista(tintas ópticamente variables, relieves, fondos de seguridad).
Verificando mediante medios ópticos y electrónicos(tintas visibles con luz ultravioleta, microescrituras).
Medidas de seguridad digitales:
Encriptación de los datos del chip.
Ping de acceso a la funcionalidad del DNI.
Las claves nunca abandonan el chip.
La autoridad de certificación es la dirección general de la policía.

Para la utilización del DNI electrónico es necesario utilizar con determinados elementos hardware y software:
Elementos hardware:
Un ordenador personal(a partir de pentium 3).
Un lector de tarjetas inteligente que cumpla con el estándar ISO-7816.
Elementos software:
Sistemas operativos(windows 2000,xp y vista, linux y MAC).
Navegadores(explorer 6.0 o superior,firefox 1.5 o superior, netcape 4.78 o superior)
Controladores/documentos criptograficos: para poder interaccionar adecuadamente con las tarjetas criptográficas, en un entorno windows, el equipo debe tener instalado el servicio criptografic services probider (CSP) y en entornos unix/linux o MAC a través de un módulo denominado PKCS#11, estos módulos pueden obtenerse en www.dnielectronico.es/descargas.