AGRADECIMIENTOS

Este libro nunca se hubiera hecho realidad sin el apoyo, consejos y contribuciones realizadas por numerosas personas.

En primer lugar a todas las personas que desde pequeño me inculcaron el valor de aprender y de la constancia en el trabajo, sobre todo mis padres, hermanos y profesores.

En segundo lugar, tenemos que dar las gracias con especial atención a José Luis Raya, por sus consejos y correcciones realizadas sobre el estilo y los contenidos. Como especialista en redes de comunicaciones y sistemas operativos y con una abultada experiencia en la publicación de manuales y documentación didáctica, su apoyo ha resultado vital en la consecución de esta obra.

Gracias a todo el equipo de la editorial Ra-Ma (**http://www.ra-ma.es**) por el trabajo realizado y por la oportunidad que nos ha brindado para hacer realidad este manual.

Por último, nos gustaría agradecer al lector la confianza depositada en nosotros. Esperamos que los conocimientos adquiridos le sirvan para su desarrollo profesional e intelectual y abran puertas hacia nuevos aprendizajes.

Introducción

Este libro surge con el propósito de acercar al lector a los aspectos más importantes que encierra la seguridad informática, ante la creciente inseguridad en los sistemas informáticos, donde cada vez contenemos más valiosa información. Con la reforma curricular de formación profesional, enmarcada en la Ley Orgánica de Educación (LOE) los ciclos formativos de la familia profesional de Informática y Comunicaciones poseen como contenido transversal la materia de Seguridad Informática, debido a la creciente demanda de personal cualificado para su administración. Con tal propósito, puede servir de apoyo también para estudiantes del las Ingenierías Técnicas.

Hoy en día, existen muchos usuarios y profesionales de la Informática que discuten las ventajas e inconvenientes de la utilización de un determinado sistema operativo, antivirus o cortafuegos, como solución única a los problemas de la seguridad informática, no entendiendo que en esta materia ha de trabajarse en todos los frentes posibles. Aquí no hay preferencia por ningún sistema en particular, ni se intenta compararlos para descubrir cuál es el mejor de todos, sino enriquecer los contenidos al exponer sus principales características, manejo y métodos para conseguir la máxima fiabilidad de los sistemas.

A lo largo del libro se analiza la seguridad informática desde distintas perspectivas, para completar una visión global de la materia, y no dejar ningún aspecto vulnerable:

- ✓ Principios básicos y problemática de la Seguridad Informática. Capítulo 1.
- ✓ Seguridad física y ambiental en los sistemas informáticos. Capítulo 2.
- ✓ Seguridad lógica. Gestión de usuarios, privilegios, contraseñas, y actualizaciones de sistemas y software. Capítulo 3.
- ✓ Software de seguridad, principalmente antimalware: antivirus y antiespías. Capítulo 4.

- ✓ Gestión de almacenamiento de la información, copias de seguridad y restauraciones. Capítulo 5.
- ✓ Seguridad en redes y comunicaciones, con especial atención a inalámbricas. Capítulo 6.
- ✓ Encriptación de la información. Capítulo 7.
- ✓ Normativa legal en materia de seguridad informática. LOPD y LSSICE. Capítulo 8.
- ✓ Auditoría de sistemas de información disponiendo una metodología para analizar, documentar y mejorar las políticas de seguridad, desde todas las perspectivas analizadas en el presente libro. Capítulo 9.

Uno de los objetivos de este libro es conocer las innovaciones en ataques y vulnerabilidades más actuales en materia informática, haciéndonos más prevenidos y realizar acciones totalmente seguras.

Para el seguimiento de este libro y principalmente de sus actividades y prácticas, se recomienda realizarlas en un blog, que permita el trabajo colaborativo entre autor, docentes y alumnos.

Para todo aquél que use este libro en el entorno de la enseñanza (Ciclos Formativos o Universidad), se ofrecen varias posibilidades: utilizar los conocimientos aquí expuestos para inculcar aspectos genéricos de la seguridad informática o simplemente centrarse en preparar a fondo alguno de ellos. La extensión de los contenidos aquí incluidos hace imposible su desarrollo completo en la mayoría de los casos.

Ra-Ma pone a disposición de los profesores una guía didáctica para el desarrollo del tema que incluye las soluciones a los ejercicios expuestos en el texto. Puede solicitarla a editorial@ra-ma.com, acreditándose como docente y siempre que el libro sea utilizado como texto base para impartir las clases.

Seguridad informática

Objetivos del capítulo

- ✓ Analizar la problemática general de la seguridad informática.
- ✓ Ver desde qué puntos de vista se puede analizar.
- ✓ Identificar las principales vulnerabilidades y ataques a los sistemas.

Supongamos que un día su unidad de DVD empieza a abrirse y cerrarse por sí sola, sin que haya ninguna explicación de ningún otro tipo; supongamos que en la carpeta donde usted archivó unas fotos de sus amigos aparecen, inexplicablemente, fotos de delfines; o supongamos que usted recibe la visita de un vecino, quien lo acusa de haberlo atacado informáticamente, es decir, el vecino recibió un ataque en su ordenador, y al tratar de averiguar quién lo hizo, encontró los datos del ordenador de usted.

Prevenir, corregir y entender estas situaciones son las que dan sentido al estudio de la seguridad informática.

Con la proliferación de la informática en todos los ámbitos de la vida, el número de usuarios y profesionales de informática ha crecido exponencialmente en los últimos años, del mismo modo que las necesidades de comunicación y compartir recursos en red. El desarrollo de las telecomunicaciones en la década de los noventa posibilitó la interconexión de las distintas redes existentes mediante la red global Internet.

Del mismo modo que surgen nuevas posibilidades y ventajas derivadas de la comunicación entre distintos usuarios remotos, en los últimos años han crecido el número de ataques y vulnerabilidades de los sistemas informáticos.

1.1 PRINCIPIOS DE LA SEGURIDAD INFORMÁTICA

La seguridad informática, en general, está teniendo una importancia cada vez mayor. Los usuarios, particulares y trabajadores de las empresas, deben ser conscientes de que el funcionamiento correcto de sus sistemas depende en gran medida, de protegerlos como el mayor de sus tesoros.

La seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

ACTIVIDADES

La seguridad informática lleva asociada un **conjunto de términos**, en muchos casos nuevos términos en inglés, que hacen difícil la tarea de estar al día en materia de seguridad.

Te proponemos que leas un **artículo de actualidad** en el cual deberás identificar palabras relacionadas con conceptos de seguridad informática que no conozcas y realizar un glosario de términos con sus definiciones.

A lo largo del curso te proponemos realizar tus actividades en un **blog** personal, donde puedas compartir tu trabajo con otros usuarios de la red.

Es impresionante la cantidad de sitios web que visitamos, y de empresas/organizaciones que ofrecen vía web los servicios que demandamos, ya sea como forma de vida, por trabajo, ocio, hobbies, interés particular, etc.

Cada día nos suscribimos a nuevos foros, compramos billetes de avión, tren, reservamos hoteles, accedemos a nuestra banca online, facturas de telefonía, luz, gas,... participamos en redes sociales (como Facebook, Twitter, Tuenti, Linkedin,...), gestionamos diferentes cuentas de correo (hotmail, gmail, yahoo,...), compramos y vendemos (Ebay, Paypal), foros

varios dependiendo de si nos gustan los coches, los libros, el cine, la música,... entre otros.

Para cada sitio web, es necesario introducir unas credenciales: en algunos casos podremos elegir el nombre de usuario (siempre y cuando no exista, o tendremos que derivar uno diferente al que generalmente usamos) y una contraseña (que en algunos casos deberá seguir un formato dado por la organización para satisfacer ciertos requisitos de complejidad). A no ser que seamos felices viviendo en el campo, ajenos a una conexión a Internet, estamos obligados a tener un montón de identidades digitales o una única con un nombre de usuario lo suficientemente raro y una misma contraseña.

¿Problemas? Pues ambas posibilidades tienen sus ventajas e inconvenientes. Tener diferentes identidades (pares usuario/contraseña) permite ser uno diferente en cada sitio, de manera que no se pueda concluir mediante herramientas online o mediante análisis las costumbres (a veces contradictorias) de un mismo individuo. Así, si un sitio de los que somos usuarios se ve comprometido (o picamos ante un ataque de *phishing*) y nuestras credenciales son expuestas, las que usamos para el resto de los servicios seguirán seguras. Mucha gente, incluso importante en el mundo de la seguridad, utiliza mecanismos de generación de credenciales basados en el nombre del sitio web o servicio que visitan. Una vez comprometido el algoritmo pensado, todas las credenciales de ese individuo, quedan expuestas.

Por lo mismo y dada la cantidad de servicios online que consumimos, lo más normal es que olvidemos aquellos que no utilizamos tan a menudo y haya que usar las opciones *Lost Password*.

En el caso de usar el mismo usuario/contraseña (siempre que se pueda) para todos los servicios, si alguien averigua nuestras credenciales (por *sniffing*, *shoulder surfing*, compromiso de uno de los *websites*, *ingeniería social*, *phishing*, etc...) podrá probar en otros sitios que exista el mismo usuario o de otros en los que conozca nuestros hábitos.

Para evitar este tipo de disyuntivas, las empresas se gastan un dineral anualmente en lo que se llaman proyectos de gestión de identidades, *single sign-on* y *provisioning*. Para el usuario de a pie, hay en el mercado variedad de productos, comerciales y libres (como por ejemplo KeepassX), que permiten mantener en un contenedor cifrado las diferentes identidades. Para aplicaciones web, incluso los navegadores proveen de servicios propios de auto-rellenado de usuario y contraseña.

En general, estos programas de protección de contraseñas, así como los de gestión de identidades, requieren una autenticación basada en una contraseña maestra. Lo cual nos lleva a otro problema más, si esa contraseña maestra cae, todas las demás quedan expuestas.

Este problema se solucionaría utilizando algún tipo de autenticación fuerte como contraseña maestra, basada en al menos dos factores de estos tres: algo que se tiene, algo que se sabe, algo que se es.

Si no es posible la autenticación fuerte, al menos:

Aseguraos de que cuando insertéis la contraseña maestra de vuestro gestor de credenciales no haya nadie mirando. Si tapáis el PIN cuando metéis la tarjeta en el cajero automático, ¿por qué no tener ciertas precauciones en el teclado del PC?

Como extensión al punto anterior, que no nos miren ni desde fuera ni desde dentro del PC: mantenedlo libre de *troyanos* y *keyloggers*. Política de parches y antivirus actualizados, *firewalls* personales, instalar sólo aquello que estéis seguros que no contiene *spyware/malware* y cuidado con los *rogue antivirus*.

Cerrad la sesión cuando terminéis la actividad para la que os hayáis tenido que autenticar (sobre todo para entornos de banca online).

Cuidado con los enlaces sobre los que pincháis (los que veáis en foros, los que os lleguen por correo), puede llevaros a no dar vuestra contraseña, pero sí a ceder vuestra sesión por robo de *cookies*.

Cuidado con las preguntas secretas para recuperar contraseñas. Extremad precauciones con respuestas demasiado triviales que puedan comprometer vuestra información de una forma trivial por quien os conoce.

Y sobre todo y más importante, cuidado con los ataques basados en ingeniería social. Cuando hay que dar una contraseña a alguien, no fiarse siempre es la opción correcta.

1.2 FIABILIDAD, CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD

Si bien es cierto que todos los componentes de un sistema informático están expuestos a un ataque (hardware, software y datos) son los datos y la información los sujetos principales de protección de las técnicas de seguridad. La seguridad informática se dedica principalmente a proteger la confidencialidad, la integridad y disponibilidad de la información. Por tanto, actualmente se considera generalmente aceptado que la seguridad de los datos y la información comprende tres aspectos fundamentales:

- ✓ Confidencialidad, es decir, no desvelar datos a usuarios no autorizados; que comprende también la privacidad (la protección de datos personales).
- ✓ Integridad, permite asegurar que los datos no se han falseado.
- ✓ Disponibilidad, esto es, que la información se encuentre accesible en todo momento a los distintos usuarios autorizados.

Hay que tener en cuenta que tanto las amenazas como los mecanismos para contrarrestarlas, suelen afectar a estas tres características de forma conjunta. Así por ejemplo, fallos del sistema que hacen que la información no sea accesible pueden llevar consigo una pérdida de integridad.

Generalmente **tienen que existir los tres aspectos descritos para que haya seguridad.**

Dependiendo del entorno en que un sistema trabaje, a sus responsables les interesará dar prioridad a un cierto aspecto de la seguridad. Por ejemplo, en un sistema militar se antepondrá la confidencialidad de los datos almacenados o transmitidos sobre su disponibilidad: seguramente, es preferible que alguien borre información confidencial (que se podría recuperar después desde una cinta de backup) a que ese mismo atacante pueda leerla, o a que esa información esté disponible en un instante dado para los usuarios autorizados.

En cambio, en un servidor NFS de archivos en red, de un departamento se premiará la disponibilidad frente a la confidencialidad: importa poco que un atacante lea una unidad, pero que esa misma unidad no sea leída por usuarios autorizados va a suponer una pérdida de tiempo y dinero.

En un entorno bancario, la faceta que más ha de preocupar a los responsables del sistema es la integridad de los datos, frente a su disponibilidad o su confidencialidad: es menos grave que un usuario consiga leer el saldo de otro que el hecho de que ese usuario pueda modificarlo.

Los conceptos confidencialidad, integridad o disponibilidad son muy comunes en el ámbito de la seguridad y aparecen como fundamentales en toda arquitectura de seguridad de la información, ya sea en el ámbito de la protección de datos, normativa vigente relacionada con la protección de datos de carácter personal, como de códigos de buenas prácticas o recomendaciones sobre gestión de la seguridad de la información y de prestigiosas certificaciones internacionales, éstas últimas, relacionadas con la auditoría de los sistemas de información.

Junto a estos tres conceptos fundamentales se suelen estudiar conjuntamente la autenticación y el no repudio en los sistemas de información. Por lo que suele referirse al grupo de estas características como CIDAN, nombre sacado de la inicial de cada característica.

- ✓ Confidencialidad.
- ✓ Integridad.
- ✓ Disponibilidad.
- ✓ Autenticación.
- ✓ No repudio.

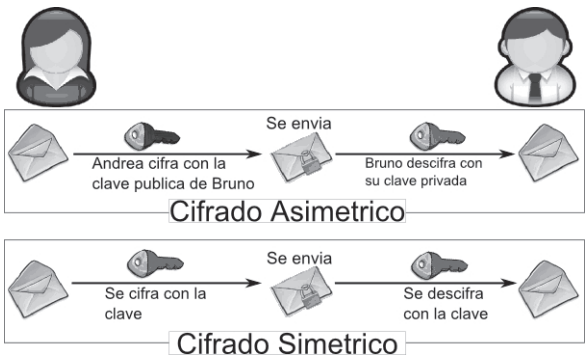
Por estos motivos es importante tener una idea clara de estos conceptos. Veamos con algo más de profundidad los mismos.

1.2.1 CONFIDENCIALIDAD

Se trata de la cualidad que debe poseer un documento o archivo para que este sólo se entienda de manera comprensible o sea leído por la persona o sistema que esté autorizado.

De esta manera se dice que un documento (o archivo o mensaje) es confidencial si y sólo si puede ser comprendido por la persona o entidad a quien va dirigida o esté **autorizada**. En el caso de un mensaje esto evita que exista una intercepción de éste y que pueda ser leído por una persona no autorizada.

Por ejemplo, si Andrea quiere enviar un mensaje a Bruno y que sólo pueda leerlo Bruno, Andrea cifra el mensaje con una clave (simétrica o asimétrica), de tal modo que sólo Bruno sepa la manera de descifrarlo, así ambos usuarios están seguros que sólo ellos van a poder leer el mensaje.



ACTIVIDADES

∅ **Analiza el significado de clave simétrica y asimétrica leyendo el siguiente texto. ¿Podrías poner algunos ejemplos donde se dispongan típicamente claves simétricas y asimétricas? ¿Cómo es que siendo una clave pública en el cifrado asimétrico es más seguro que el cifrado simétrico?**

- Cifrado simétrico: es la técnica más antigua, la más extendida y mejor conocida. Una clave secreta, que puede ser un número, una palabra o simplemente una cadena de letras, aleatorias, se aplica al texto de un mensaje para cambiar el contenido en un modo determinado. Esto podría ser tan sencillo como desplazando cada letra a un número de posiciones en el alfabeto. Siempre que el remitente y destinatario conozcan la clave secreta, puede cifrar y descifrar todos los mensajes que utilizan esta clave.
- Cifrado asimétrico: el problema con las claves secretas intercambiadas a través de Internet o de una gran red es que caigan en manos equivocadas. Cualquiera que conozca la clave secreta puede descifrar el mensaje. Una respuesta a este problema es el cifrado asimétrico, en la que hay dos claves relacionadas, un par de claves. Una clave pública queda disponible libremente para cualquier usuario que desee enviar un mensaje. Una segunda clave privada se mantiene en secreto, de forma que sólo pueda conocerla el destinatario.

Cualquier mensaje (texto, archivos binarios o documentos) que están cifrados mediante clave pública sólo puede descifrarse aplicando el mismo algoritmo, pero mediante la clave privada correspondiente, por lo que aunque algún usuario de la red intercepte y disponga de la clave pública y del mensaje, también deberá disponer de la clave privada que sólo dispone el destinatario. Del mismo modo, cualquier mensaje que se cifra mediante la clave privada sólo puede descifrarse mediante la clave pública correspondiente.

En este caso, cada usuario ha de poseer una pareja de claves:

- Clave privada: será custodiada por su propietario y no se dará a conocer a ningún otro.
- Clave pública: puede ser conocida por todos los usuarios.

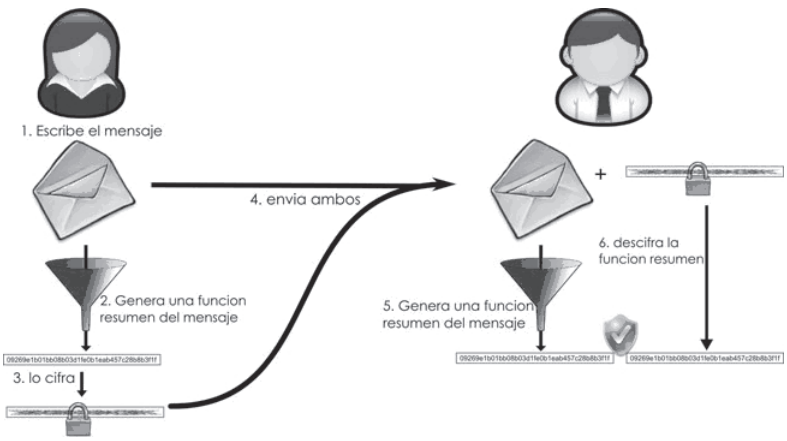
Esta pareja de claves es complementaria: lo que cifra una SÓLO lo puede descifrar la otra y viceversa.

Estas parejas de claves se obtienen mediante métodos matemáticos complejos.

Un problema con el cifrado asimétrico, sin embargo, es que es más lento que el cifrado simétrico. Requiere mucha más capacidad de procesamiento para cifrar y descifrar el contenido del mensaje, pero este coste de tiempo hace del mismo un mecanismo más seguro.

1.2.2 INTEGRIDAD

La integridad es la cualidad que posee un documento o archivo que no ha sido alterado y que además permite comprobar que no se ha producido manipulación alguna en el documento original. Aplicado a las bases de datos sería la correspondencia entre los datos y los hechos que refleja.



En el caso del envío de información y su no modificación durante su viaje a través de una red, teniendo como muestra el ejemplo anterior, Andrea envía tanto el propio mensaje como un resumen cifrado del mismo. Finalmente, Bruno en el lado del receptor, compara el mensaje como resumen (aplicando la misma función que Andrea) y el resumen cifrado enviado. Si en el transcurso de la comunicación el mensaje ha sido alterado por fallos en el canal de comunicaciones o por algún usuario intruso, la comparación será errónea, y si ésta da como resultado "iguales", quiere decir que no ha existido manipulación del mensaje.

1.2.3 DISPONIBILIDAD

Se trata de la capacidad de un servicio, de unos datos o de un sistema, a ser accesible y utilizable por los usuarios (o procesos) autorizados cuando éstos lo requieran.

También se refiere a la seguridad que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor.

ACTIVIDADES

Lee el siguiente artículo sobre alta disponibilidad y explica si el equipo que dispones la posee. Indica algunas medidas para aumentar la disponibilidad ante por ejemplo cortes de suministro de luz, o el error de lectura/escritura en una unidad de disco duro. ¿Qué es un sistema o centro de respaldo? ¿Los sistemas de alta disponibilidad cuántas horas y días a la semana deben funcionar?

Nos referimos a alta disponibilidad (en inglés High Availability) a los sistemas que nos permiten mantener nuestros sistemas funcionando las 24 horas del día, manteniéndolos a salvo de interrupciones.

Debemos diferenciar dos tipos de interrupciones en nuestros sistemas.

- Las interrupciones previstas: las que se realizan cuando paralizamos el sistema para realizar cambios o mejoras en nuestro hardware o software.
- Las interrupciones imprevistas: las que suceden por acontecimientos imprevistos (como un apagón, un error del hardware o del software, problemas de seguridad, un desastre natural, virus, accidentes, caídas involuntarias del sistema).

Y distintos niveles de disponibilidad del sistema:

- Los sistemas de la disponibilidad base: el sistema está listo para el uso inmediato, pero experimentará tanto interrupciones planificadas como no planificadas.
- Los sistemas de disponibilidad alta: incluyen tecnologías para reducir drásticamente el número y la duración de interrupciones imprevistas. Todavía existen interrupciones planificadas, pero los servidores incluyen herramientas que reducen su impacto.
- Entornos de operaciones continuas: utilizan tecnologías especiales para asegurarse de que no hay interrupciones planificadas para backups, actualizaciones, u otras tareas de mantenimiento que obliguen a no tener el sistema disponible.
- Los sistemas de la disponibilidad continua: van un paso más lejos para asegurarse de que no habrán interrupciones previstas o imprevistas que interrumpan los sistemas. Para alcanzar este nivel de la disponibilidad, las compañías deben utilizar servidores duales o los clusters de servidores redundantes donde un servidor asume el control automáticamente si el otro servidor cae.
- Los sistemas de tolerancia al desastre: requieren de sistemas alejados entre sí para asumir el control en cuanto pueda producirse una interrupción provocada por un desastre.

Normalmente, un sistema de alta disponibilidad funciona sobre un sistema de producción y otro sistema de respaldo (o varios, en caso de que queramos un sistema de alta disponibilidad con tolerancia al desastre), donde en caso de alguna incidencia podremos recuperar la información del sistema de producción.

Para que este sistema de respaldo sea realmente efectivo, no tan sólo debe recuperar la información (base de datos) del sistema de producción, sino que debe reflejar cualquier cambio realizado en el mismo (usuarios, autorizaciones, programas, configuraciones, colas de trabajo, etc.) y sobre todo que estos cambios se reflejen en el sistema de respaldo de la forma más automatizada posible.

Las herramientas de alta disponibilidad deben permitirnos por lo tanto disponer de nuestros equipos funcionando **24 horas al día, 7 días a la semana**, ofreciéndonos la seguridad de que bajo cualquier supuesto, nuestro sistema de producción estará disponible casi inmediatamente.

Dada la creciente dependencia en los sistemas, la globalización de los mercados, el comercio electrónico y la alta competencia entre las compañías, los costes asociados a los tiempos de parada (sea cual sea el tipo) son cada vez mayores y las empresas empiezan a tenerlos en consideración.

En el actual entorno de negocios, la alta disponibilidad de nuestros sistemas se ha convertido en una necesidad y no en un lujo.

1.2.4 AUTENTICACIÓN

La autenticación es la situación en la cual se puede verificar que un documento ha sido elaborado (o pertenece) a quien el documento dice.

Aplicado a la verificación de la identidad de un usuario, la autenticación se produce cuando el usuario puede aportar algún modo de que se pueda verificar que dicha persona es quien dice ser, a partir de ese momento se considera un usuario autorizado. La autenticación en los sistemas informáticos habitualmente se realiza mediante un usuario o login y una contraseña o password.

Otra manera de definirlo sería la capacidad de determinar si una determinada lista de personas ha establecido su reconocimiento sobre el contenido de un mensaje.

1.2.5 NO REPUDIO

El no repudio o irrenunciabilidad es un servicio de seguridad estrechamente relacionado con la autenticación y que permite **probar la participación de las partes en una comunicación**. La diferencia esencial con la autenticación es que la primera se produce entre las partes que establecen la comunicación y el servicio de **no repudio se produce frente a un tercero**, de este modo, existirán dos posibilidades:

- **No repudio en origen**: el emisor no puede negar el envío porque el destinatario tiene pruebas del mismo, el receptor recibe una prueba infalsificable del origen del envío, lo cual evita que el emisor, de negar tal envío, tenga éxito ante el juicio de terceros. En este caso la prueba la crea el propio emisor y la recibe el destinatario.
- **No repudio en destino**: el receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción. Este servicio proporciona al emisor la prueba de que el destinatario legítimo de un envío, realmente lo recibió, evitando que el receptor lo niegue posteriormente. En este caso la prueba irrefutable la crea el receptor y la recibe el emisor.

Si la autenticidad prueba quién es el autor de un documento y cuál es su destinatario, el "no repudio" prueba que el autor envió la comunicación (no repudio en origen) y que el destinatario la recibió (no repudio en destino).

Relación de los servicios de seguridad:

En la imagen superior se ilustra cómo se relacionan los diferentes servicios de seguridad, unos dependen de otros jerárquicamente, así si no existe el de más abajo, no puede aplicarse el superior. De esta manera, la **disponibilidad** se convierte en el primer requisito de seguridad, cuando existe ésta, se puede disponer de **confidencialidad**, que es imprescindible para conseguir **integridad**, para poder obtener **autenticación** es imprescindible la integridad y por último el **no repudio** sólo se obtiene si se produce previamente la autenticación.

1.3 ELEMENTOS VULNERABLES EN EL SISTEMA INFORMÁTICO: HARDWARE, SOFTWARE Y DATOS

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 **altos niveles de seguridad** en los sistemas informáticos. Además, la seguridad informática precisa de un nivel organizativo, por lo que diremos que:

Sistema de Seguridad = TECNOLOGÍA + ORGANIZACIÓN

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 la de su punto más débil. Al asegurar nuestra casa no sacamos nada con ponerle una puerta blindada con sofisticada cerradura si dejamos las ventanas sin protección. De manera similar el uso de sofisticados algoritmos y métodos criptográficos es inútil si no garantizamos la confidencialidad de las estaciones de trabajo.

Por otra parte, existe algo que los hackers llaman Ingenieria Social que consiste simplemente en conseguir mediante 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. Es evidente que por mucha tecnología de seguridad que se implante en una organización, si no existe una clara disposición por parte de los directores de la empresa y una cultura a nivel de usuarios, no se conseguirán los objetivos perseguidos con la implantación de un sistema de seguridad.

Los tres elementos principales a proteger en cualquier sistema informático son el *software,* el *hardware* y los datos. Por **hardware** entendemos el conjunto formado por todos los elementos físicos de un sistema informático, como CPU, terminales, cableado, medios de almacenamiento secundario (cintas, CD-ROM, disquetes...) o tarjetas de red. Por **software** entendemos el conjunto de programas lógicos que hacen funcionar al *hardware,* tanto sistemas operativos como aplicaciones, y por **datos** el conjunto de información lógica que manejan el *software* y el *hardware*, como por ejemplo paquetes que circulan por un cable de

red o entradas de una base de datos. Aunque generalmente en las auditorías de seguridad se habla de un cuarto elemento a proteger, los **fungibles** (elementos que se gastan o desgastan con el uso continuo, como papel de impresora, *tóners,* cintas magnéticas,...), aquí no consideraremos la seguridad de estos elementos por ser externos a la red.

Habitualmente **los datos constituyen el principal elemento** de los tres **a proteger**, ya que es el más amenazado y seguramente el más difícil de recuperar: con toda seguridad un servidor estará ubicado en un lugar de acceso físico restringido, o al menos controlado, y además en caso de pérdida de una aplicación (o un programa de sistema, o el propio núcleo del sistema operativo) este *software* se puede restaurar sin problemas desde su medio original (por ejemplo, el CD-ROM con el sistema operativo que se utilizó para su instalación). Sin embargo, en caso de pérdida de una base de datos o de un proyecto de un usuario, no tenemos un medio "original" desde el que restaurar: hemos de pasar obligatoriamente por un sistema de copias de seguridad, y a menos que la política de copias sea muy estricta, es difícil devolver los datos al estado en que se encontraban antes de la pérdida.

También debemos ser conscientes de que las medidas de seguridad que deberán establecerse comprenden el hardware y el sistema operativo, las comunicaciones (por ejemplo, medios de transmisión), medidas de seguridad físicas (ubicación de los equipos, suministro eléctrico, etc.), los controles organizativos (políticas de seguridad, niveles de acceso, contraseñas, normas, procedimientos, etc.) y legales (por ejemplo, la Ley Orgánica de Protección de Datos, LOPD).

1.4 AMENAZAS

Las amenazas a un sistema informático pueden provenir desde un hacker remoto que entra en nuestro sistema con un troyano, pasando por un programa descargado gratuito que nos ayuda a gestionar nuestras fotos, pero que supone una puerta trasera a nuestro sistema permitiendo la entrada a espias, hasta la entrada no deseada al sistema mediante una contraseña de bajo nivel de seguridad. Se pueden clasificar por tanto en amenzas provocadas por:

- ✓ Personas.
- ✓ Amenazas lógicas.
- ✓ Amenazas físicas.

A continuación se presenta una relación de los **elementos que potencialmente pueden amenazar a nuestro sistema.**

- **Personas.** No podernos engañarnos: la mayoría de ataques a nuestro sistema van a provenir en última instancia de personas que, intencionada o inintencionadamente, pueden causarnos enormes pérdidas. Generalmente se tratará de piratas que intentan conseguir el máximo nivel de privilegio posible aprovechando alguno (o algunos) de los riesgos lógicos de los que hablaremos a continuación, especialmente agujeros del *software.* Pero con demasiada frecuencia se suele olvidar que los piratas "clásicos" no son los únicos que amenazan nuestros equipos: es especialmente preocupante que mientras que hoy en día cualquier administrador mínimamente preocupado por la seguridad va a conseguir un sistema relativamente fiable de una forma lógica (permaneciendo atento a vulnerabilidades de su *software*, restringiendo servicios, utilizando cifrado de datos...), pocos administradores tienen en cuenta factores como la ingeniería social o el basurero, a la hora de diseñar una política de seguridad.

  Aquí se describen brevemente los diferentes tipos de personas que de una u otra forma pueden constituir un riesgo para nuestros sistemas; generalmente se dividen en dos grandes grupos: los atacantes **pasivos** aquellos que fisgonean por el sistema pero no lo modifican o destruyen, y los **activos** aquellos que dañan el objetivo atacado, o lo modifican en su favor.

- ***Personal.*** Se pasa por alto el hecho de que casi cualquier persona de la organización, incluso el personal ajeno a la infraestructura informática (secretariado, personal de seguridad, personal de limpieza y mantenimiento...) puede comprometer la seguridad de los equipos. Aunque los ataques pueden ser intencionados (en cuyo caso sus efectos son extremadamente dañinos, recordemos que nadie mejor que el propio personal de la organización conoce mejor los sistemas... y sus debilidades), lo normal es que más que de ataques se trate de **accidentes** causados por un error o por desconocimiento de las normas básicas de seguridad.

- ***Ex-empleados.*** Generalmente, se trata de personas descontentas con la organización que pueden aprovechar debilidades de un sistema que conocen perfectamente, pueden insertar troyanos, bombas lógicas, virus... o simplemente conectarse al sistema como si aún trabajaran para la organización (muchas veces se mantienen las cuentas abiertas incluso meses después de abandonar la universidad o empresa), conseguir el privilegio necesario, y dañarlo de la forma que deseen, incluso chantajeando a sus ex-compañeros o ex-jefes.

- ***Curiosos.*** Junto con los *crackers,* los curiosos son los atacantes más habituales de sistemas. En la mayoría de ocasiones esto se hace simplemente para leer el correo de un amigo, enterarse de cuánto cobra un compañero, copiar un trabajo o comprobar que es posible romper la seguridad de un sistema concreto. Aunque en la mayoría de situaciones se trata de ataques no destructivos (a excepción del borrado de huellas para evitar la detección), parece claro que no benefician en absoluto al entorno de fiabilidad que podamos generar en un determinado sistema.

- ***Hacker***. Es un término general que se ha utilizado históricamente para describir a 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, aunque no siempre tiene que ser esa su finalidad.

- ***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.

- ***Intrusos remunerados.*** Se trata de piratas con gran experiencia en problemas de seguridad y un amplio conocimiento del sistema, que

son pagados por una tercera parte generalmente para robar secretos (el nuevo diseño de un procesador, una base de datos de clientes, información confidencial sobre las posiciones de satélites espía...) o simplemente para dañar la imagen de la entidad afectada.

- **Amenazas lógicas.** Bajo la etiqueta de "amenazas lógicas" encontramos todo tipo de programas que de una forma u otra pueden dañar a nuestro sistema, creados de forma intencionada para ello (*software* malicioso, también conocido como *malware*) o simplemente por error (*bugs* o agujeros).

  - ***Software incorrecto.*** A los errores de programación se les denomina *bugs*, y a los programas utilizados para aprovechar uno de estos fallos y atacar al sistema, *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 en la subred completa, un potencial intruso las puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar los equipos. Herramientas como NESSUS, SAINT o SATAN pasan de ser útiles a ser peligrosas cuando las utilizan *crackers* que buscan información sobre las vulnerabilidades de un *host* o de una red completa.

  - ***Puertas traseras.*** Durante el desarrollo de aplicaciones grandes o de sistemas operativos es habitual entre los programadores insertar "atajos" en los sistemas habituales de autenticación del programa o del núcleo que se está diseñando.

  - ***Bombas lógicas.*** Las bombas lógicas son partes de código de ciertos programas que permanecen sin realizar ninguna función hasta que son activadas; en ese punto, la función que realizan no es la original del programa, sino que generalmente se trata de una acción perjudicial.

  - ***Canales cubiertos.*** Los canales cubiertos (o canales ocultos, según otras traducciones) son canales de comunicación que permiten a un proceso transferir información de forma que viole la política de seguridad del sistema; dicho de otra forma, un proceso transmite información a otros (locales o remotos) que no están autorizados a leer dicha información.

- ***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. Todo el mundo conoce los efectos de los virus en algunos sistemas operativos de sobremesa como Windows; sin embargo, en GNU/Linux los virus no suelen ser un problema de seguridad grave.

- ***Gusanos.*** Un gusano 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 conecta para dañarlos. Al ser difíciles de programar su número no es muy elevado, pero el daño que pueden causar es muy grande: el mayor incidente de seguridad en Internet fue precisamente el *Internet Worm,* un gusano que en 1988 causó perdidas millonarias al infectar y detener más de 6.000 máquinas conectadas a la red.

- ***Caballos de Troya.*** Los troyanos o caballos de Troya son instrucciones escondidas en un programa de forma que éste parezca realizar las tareas que un usuario espera de él, pero que realmente ejecute funciones ocultas (generalmente en detrimento de la seguridad) sin el conocimiento del usuario; como el Caballo de Troya de la mitología griega, al que deben su nombre, ocultan su función real bajo la apariencia de un programa inofensivo que a primera vista funciona correctamente.

- ***Programas conejo o bacterias.*** Bajo este nombre se conoce a los programas que no hacen nada útil, sino que simplemente se dedican a reproducirse hasta que el número de copias acaba con los recursos del sistema (memoria, procesador, disco...), produciendo una negación de servicio.

- **Amenazas físicas.** Algunas de las amenazas físicas que pueden afectar a la seguridad y por tanto al funcionamiento de los sistemas son:

  - Robos, sabotajes, destrucción de sistemas.

  - Cortes, subidas y bajadas bruscas de suministro eléctrico.

  - Condiciones atmosféricas adversas. Humedad relativa excesiva o temperaturas extremas que afecten al comportamiento normal de los componentes informáticos.

- Las catástrofes (naturales o artificiales) son la amenaza menos probable contra los entornos habituales: simplemente por su ubicación geográfica. Un subgrupo de las catástrofes es el denominado de riesgos poco probables. Como ejemplos de catástrofes hablaremos de terremotos, inundaciones, incendios, humo o atentados de baja magnitud (más comunes de lo que podamos pensar); obviamente los riesgos poco probables los trataremos como algo anecdótico.

Hasta ahora hemos hablado de los aspectos que engloba la seguridad informática, de los elementos a proteger, de los tipos de amenazas que contra ellos se presentan y del origen de tales amenazas; parece claro que, para completar nuestra visión de la seguridad, hemos de hablar de las **formas de protección de nuestros sistemas**.

Para proteger nuestro sistema hemos de realizar un **análisis de las amenazas potenciales** que puede sufrir, las **pérdidas** que podrían generar, y la **probabilidad de su 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 los mecanismos utilizados para implementar esta política de seguridad se les denomina **mecanismos de seguridad** son la parte más visible de nuestro sistema de seguridad, y se convierten en la herramienta básica para garantizar la protección de los sistemas o de la propia red.

Se distinguirán y estudiarán en los próximos temas las medidas de seguridad:

- **Activas:** que 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.
  - El uso de software específico de seguridad informática. Antimalware.
- **Pasivas:** que minimizan el impacto y los efectos causados por accidentes, mediante:
  - Uso de hardware adecuado, protección física, eléctrica y ambiental.
  - Realización de copias de seguridad, que permitan recuperar los datos.

A lo largo de los siguientes temas analizaremos desde distintas perspectivas la seguridad informática:

- ✓ Capítulo 2: Seguridad física y ambiental.
- ✓ Capítulo 3: Seguridad lógica. Gestión de usuarios, privilegios, contraseñas, y actualizaciones.
- ✓ Capítulo 4: Software de seguridad, principalmente antimalware.
- ✓ Capítulo 5: Gestión de almacenamiento de la información, copias de seguridad y restauraciones.
- ✓ Capítulo 6: Seguridad en redes y comunicaciones.
- ✓ Capítulo 7: Encriptación de la información.
- ✓ Capítulo 8: Normativa legal en materia de seguridad. LOPD y LSSICE.
- ✓ Capítulo 9: Auditorías de seguridad informática.

ACTIVIDADES

✆ **Realiza un glosario de términos nuevos que encuentres en el siguiente artículo y busca sus definiciones formales en Internet. ¿Has recibido alguna vez un spam? ¿Podrías indicar algún ejemplo?**

Realiza un debate en el que se analicen las posibles amenazas existentes en los sistemas del aula y qué tipo de medidas de prevención preliminares se podrían tomar.

El término phishing aparece por primera vez en el año 1996 en las newsgroups de hackers y en la edición del Magazine 2600. Este término tiene dos orígenes: 1) Fishing o pesca, refiriéndose a la pesca de credenciales o a la pesca de ingenuos para intentos de fraude, 2) Phishing - Password Harvesting que viene a significar cosecha de contraseñas.

En 1996 un phisher se hizo pasar por técnico de AOL y envió mensajes haciendo uso de la ingeniería social en los que solicitaba que el usuario verificase su cuenta o confirmase una factura y así poder solicitar las credenciales personales de la víctima. Con estos datos ya podía realizar acciones como el envío de spam. Para intentar solucionarlo, AOL incluyó como texto por defecto en el intercambio de mensajes: AOL nunca le solicitará contraseñas o información de facturación.

En 2001 aparecen los primeros scam en Hotmail con el texto "Usted es uno de los 100 ganadores de Hotmail" junto con un formulario que solicitaba el usuario y la contraseña de la cuenta de la víctima. Aunque este mensaje aparecía firmado por el Staff de Hotmail, en realidad provenía de una dirección IP de Ucrania. También AOL informó de un caso similar en donde el usuario recibía un mensaje que le avisaba de un error en su registro y no podían facturarle, para evitar que se le diera de baja debería rellenar un formulario lo antes posible. Además, incluía un enlace a una página para realizar la facturación de AOL. Ese mismo año se recibieron mensajes informando que un grupo de hackers había accedido a la base de datos de MSN en donde solicitaban el envío de un correo con los datos personales y la cuenta (usuario y contraseña) porque de lo contrario serían borrados de la base de datos.

En 2002 fueron los usuarios de ICQ quienes recibieron mensajes simulando la imagen de ICQ, en los que les solicitaban sus datos personales en un formulario, y mediante un script redireccionaban sus datos a una dirección de Hotmail. A finales de año Yahoo informaba que varios de sus clientes habían recibido correos donde les solicitaban los datos de sus tarjetas de crédito.

En 2003 le tocó el turno a los usuarios de EBAY quienes recibieron correos que simulaban alertas de Paypal solicitando sus datos bancarios y los números de sus tarjetas de crédito. Después aparecieron los primeros phishing a entidades de banca online como Barclays Bank, BBVA, en donde los phishers usaron técnicas para la ofuscación de URL. También comenzaron a registrarse nombres de dominio similares a los de las entidades bancarias. A finales de año se detectaron los primeros correos dirigidos a banca online que incluían troyanos con técnicas de ocultación. Un caso fue un ataque que introducía un troyano embedido en código HTML e incluía un script en la máquina de la víctima. Ese troyano era una variante del Spy-Tofger.

Las técnicas que se usaron a partir de entonces se enfocan hacia intentos de fraude como:

- Correos electrónicos: masivos de spam, selectivos, acompañados por ingeniería social para captar la atención de la víctima, también podían hacer uso de webspoofing o falsas páginas web, algunas venían acompañadas de malware que redirige el nombre de dominio a otra máquina (pharming). Aparece por primer vez un troyano con capacidad para capturar las pulsaciones de teclado (Keylogger).
- Sitio web: malware que explotaba las vulnerabilidades sin parchear de los navegadores, en el sistema operativo, y una vez infectado redireccionaba a los usuarios a servidores web en donde

estaban las páginas que suplantaban a las originales. También se insertaba código malicioso en HTML, frames, scripts PHP, en donde se ocultaban keyloggers, capturadores de pantalla, backdoors. Banners publicitarios para redireccionar al usuario a sitios con confiables.

- IRC y mensajería instantánea: donde se enviaban imágenes, URL, a los usuarios con contenidos maliciosos. Se enviaba SPAM y se conectaban bots para propagar los contenidos.
- VoIP: simulación telefónica, uso de Bots-IVR que solicitaban las credenciales personales. Redirección a webspoofing, otros canales.
- Buscadores: que proporcionaban sitios maliciosos en respuesta a las búsquedas de comercio electrónico o banca online.
- Mensajes en foros, en redes sociales, tablones de anuncios, con mensajes con ingeniería social para captar a la víctima.
- Redes P2P, descarga de software desde páginas de descarga masiva.
- Plataformas de juegos online, recordamos los casos de phishing que han sufrido los jugadores del World of Warcraft.
- Falsos antivirus y antispyware, utilizando llamativos anuncios o pop-ups con avisos alarmantes que advierten al usuario que su sistema está infectado y debe comprar la solución que se le propone. Al usar su tarjeta para obtener este producto sus datos son capturados para su posterior uso fraudulento.
- Vía teléfono móvil (SMiShing), enviando un SMS al usuario en donde se le invita a enviar su información privada o visitar un sitio web con contenidos maliciosos.
- Botnets: que tratan de controlar un número masivo de máquinas para la captura de datos bancarios, cuentas de correo.

El objetivo de estas mafias es la búsqueda de usuarios y los datos de sus cuentas bancarias. Haciendo uso de la ingeniería social, el spam y el malware. Entrando en las redes sociales como Facebook o Twitter. Aprovechándose de mensajes con carga emocional, como por ejemplo la catástrofe en Haití (terremoto 2010), en donde ya se han detectado casos de phishing para lucrar a estas organizaciones.

Los usuarios y las entidades deben tener una actitud responsable y utilizar medidas de protección. Se debe concienciar y educar al ciudadano para estar alerta y evitar que sus datos personales y bancarios sean robados.

ACTIVIDADES

En esta actividad vamos a analizar el centro de seguridad de sistemas Windows. Verifica que tienes correctamente configuradas sus opciones.

Sistema operativo Windows XP. Ir a Panel de control / Seguridad / Centro de seguridad.

En esta ubicación podemos encontrar algunos aspectos centralizados sobre seguridad del sistema:

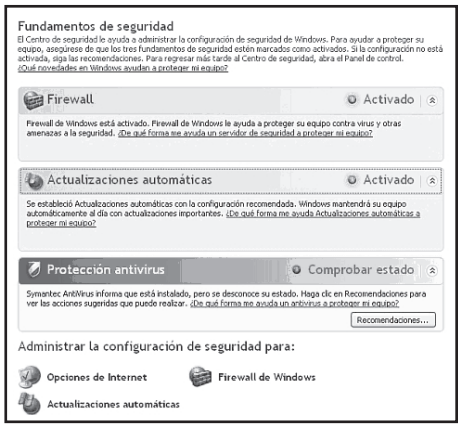
Para acceder al Centro de seguridad en Windows XP, debemos pulsar en el Inicio de Windows e ingresar al Panel de control.

Hacemos clic sobre "Centro de seguridad". A continuación, se abrirá la ventana del Centro de seguridad. Aquí encontraremos

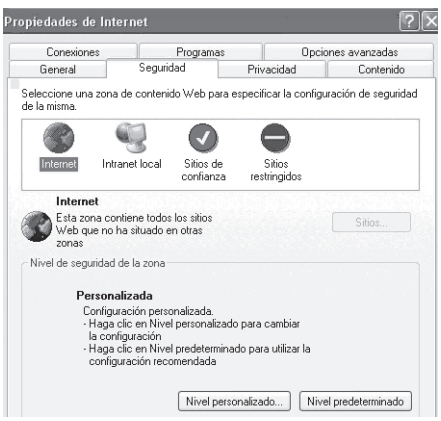
- Firewall.
- Actualizaciones automáticas.
- Protección antivirus.

Una luz verde nos indicará si están activados y una luz roja nos informará si están desactivados, o si hay que verificar su estado.

En la parte inferior de la ventana, tenemos tres opciones: Opciones de Internet, Firewall de Windows y Actualizaciones de Windows.



Ingresando a Opciones de Internet, en la solapa "Seguridad", podremos definir el nivel de seguridad de la navegación. Esta ventana, tiene botones que nos permiten agregar "Sitios de confianza" o definir una lista de "Sitios restringidos".



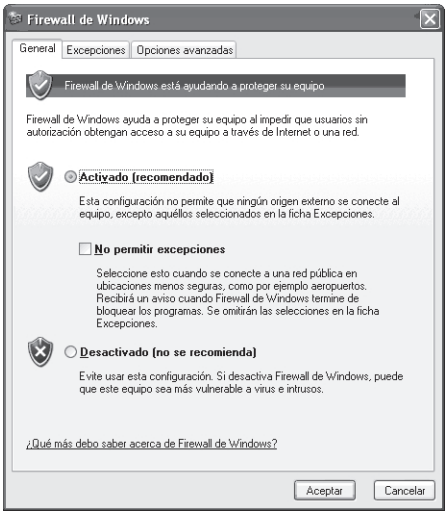
Si realizamos algún cambio en la configuración, debemos confirmarlo con el botón "Aplicar" y luego con "Aceptar".

Nuevamente, desde el Centro de seguridad de Windows, podremos configurar el Cortafuegos ingresando a "Firewall de Windows".

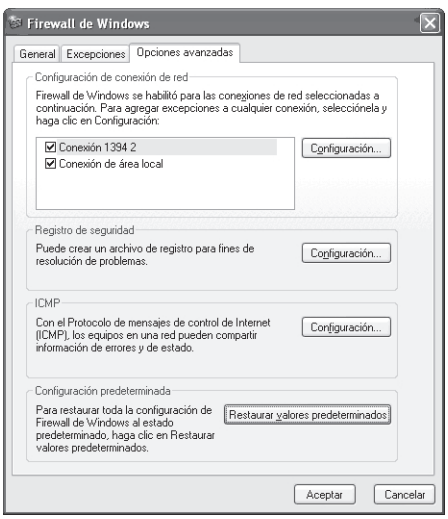
En esta ventana, podremos elegir entre tres opciones:

- Activado (es la opción por defecto).
- No permitir excepciones (es una alternativa útil cuando se necesita mayor seguridad), no permitiendo que ninguna aplicación tenga conexión de red.

- Desactivado (esta opción se puede utilizar si vamos a instalar un firewall distinto al que provee Windows).



Si ingresamos a la solapa "Excepciones" encontraremos una lista de programas que podremos marcar o desmarcar, para permitirles o prohibirles el acceso a la red.



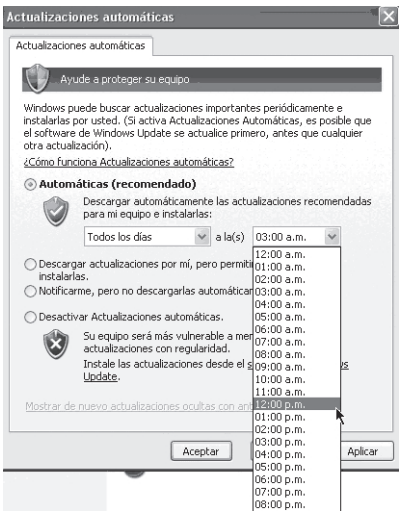
Podremos agregar nuevos programas a la lista y también puertos. Contamos con la posibilidad de configurar el firewall, para que nos advierta cuando está bloqueando un programa.

Dentro de la solapa "Opciones avanzadas" podremos habilitar o deshabilitar conexiones de red y configurar el registro de seguridad, entre otras opciones.

Si realizamos algún cambio, podremos confirmarlo con el botón "Aceptar".

Desde el Centro de seguridad de Windows, podremos ingresar a la opción "Actualizaciones automáticas". En esta ventana elegimos si deseamos que Windows descargue las actualizaciones de seguridad de manera automática.

Si escogemos esta alternativa, podremos indicar qué día y a qué hora, el equipo debe conectarse para verificar si hay alguna actualización.



También podremos optar para que se realice la descarga, pero elegir cuándo se instalan; notificación sin descarga automática; o desactivar la descarga automática, para manejar este tema por nuestra cuenta.

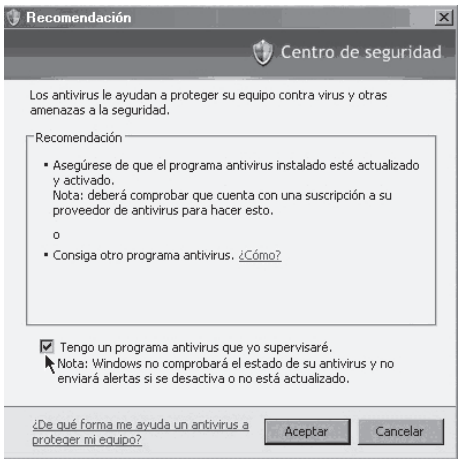
Si realizamos alguna modificación en la configuración, debemos confirmarlo con el botón "Aplicar" y luego con "Aceptar".

Nota: Si deseamos acceder a Microsoft Update para ver las últimas actualizaciones de nuestro sistema operativo, podremos hacerlo entrando con Internet Explorer 5 o superior a: http://www.update.microsoft.com/

En el ítem "Protección de virus" el sistema puede detectar si tenemos instalado un antivirus. Sin embargo, en algunos casos, nos puede alertar si no logra verificar al fabricante o las definiciones de virus.

Si preferimos manejar el antivirus por nuestra cuenta, sin que Windows nos

muestre las alertas del centro de seguridad para este ítem, hacemos clic en el botón "Recomendaciones" y accedemos a una ventana donde podemos tildar la opción "Tengo un programa antivirus que yo supervisaré".



De esta manera, el ítem "Protección antivirus" en el Centro de seguridad se pondrá de color amarillo y nos mostrará un cartel "Sin supervisión".

1.5 REFERENCIAS WEB

- ✓ Sitio web sobre seguridad informática de Microsoft: http://www.microsoft.com/spain/protect/default.mspx
- ✓ Sitio web sobre seguridad informática de GNU/Linux, de Criptonomicón, un servicio ofrecido libremente desde el Instituto de Física Aplicada del CSIC: http://www.iec.csic.es/CRIPTonOMICon/linux/
- ✓ *INTECO* - Instituto Nacional de Tecnologías de la Comunicación: www.inteco.es/
- ✓ Hispasec Sistemas: Seguridad y Tecnologías de información. Resúmenes anuales de noticias de actualidad sobre seguridad informática: http://www.hispasec.com/

RESUMEN DEL CAPÍTULO

En este capítulo se han analizado los fundamentos y conceptos de la seguridad informática.

Los principios que todo sistema informático debe contemplar son:

- **Confidencialidad**, es decir, no desvelar datos a usuarios no autorizados; que comprende también la privacidad (la protección de datos personales).
- **Disponibilidad**, esto es, que la información se encuentre accesible en todo momento a los distintos usuarios autorizados.
- **Integridad**, que permite asegurar que los datos no se han falseado.
- **Autenticación**, verificación de la identidad de un usuario, a partir de ese momento se considera un usuario autorizado.
- El **no repudio** o irrenunciabilidad, estrechamente relacionado con la autenticación, permite probar la participación de las partes en una comunicación.

Las amenazas a los sistemas que provienen de distintos ámbitos:

- **Personas:** como personal de la empresa, ex-empleados, curiosos, hacker, cracker, Intrusos remunerados
- **Amenazas lógicas**: software incorrecto, herramientas de seguridad, puertas traseras, bombas lógicas, canales cubiertos, virus, gusanos, caballos de Troya, programas conejo o bacterias
- **Amenazas físicas**: robos, sabotajes, destrucción de sistemas, cortes, subidas y bajadas bruscas de suministro eléctrico, condiciones atmosféricas adversas, catástrofes (naturales o artificiales como incendios).

Por otro lado en cuanto a las medidas para la prevención y recuperación se distinguen entre:

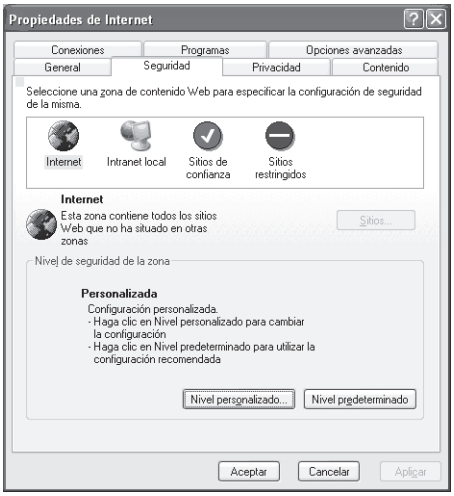
- **Activas:** contraseñas, encriptación y filtrado en las comunicaciones, uso de antimalware.
- **Pasivas:** protección física, eléctrica y ambiental, copias de seguridad, control de acceso físico.

Debemos ser conscientes de que las medidas de seguridad que deberán establecerse comprenden un conjunto de elementos que no pueden ser tratados dejando de lado o desprotegido ninguno de ellos: hardware, sistema operativo, comunicaciones (por ejemplo, medios de transmisión), medidas de seguridad físicas (ubicación de los equipos, suministro eléctrico, etc.), los controles organizativos (políticas de seguridad, niveles de acceso, contraseñas, normas, procedimientos, etc.) y legales (por ejemplo, la Ley Orgánica de Protección de Datos, LOPD).

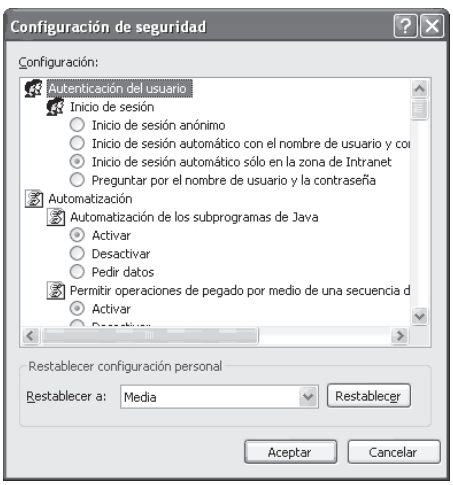
En los siguientes capítulos analizaremos dichas medidas para hacer de la seguridad la seña de identidad de nuestros sistemas.

EJERCICIOS PROPUESTOS

- **1.** Configura el firewall de tu sistema operativo para evitar contestar a peticiones de red de echo entrante.
- **2.** Configura el firewall para evitar que su navegador web tenga acceso a Internet.
- **3.** Contesta a las siguientes preguntas:
  ¿Qué nivel de seguridad posees en tu navegador web Internet Explorer? Puedes analizarlo en las propiedades de Internet / pestaña de privacidad.



En opciones avanzadas. Entre el nivel de configuración de seguridad a nivel medio y a nivel básico encuentra las diferencias de configuración de las opciones de seguridad. ¿Qué restricciones propone el nivel alto?



- **4.** ¿Dispones de restricciones de acceso a sitios web? Ver pestaña de seguridad en el apartado Sitios restringidos.

- **5.** ¿Tu sistema posee protección antivirus? ¿Te la proporciona el sistema operativo?

- **6.** Busca un software antivirus en línea y realiza un análisis de tu sistema.

TEST DE CONOCIMIENTOS

1 El servicio de no repudio:
- **a)** Se produce entre dos partes de una comunicación.
- **b)** Lo verifica el receptor.
- **c)** Se puede verificar por un tercero.
- **d)** Se realiza por emisor y un agente externo a la comunicación.

2 Indica qué sentencia es falsa:
- **a)** La integridad permite asegurar que los datos no se han falseado.
- **b)** Confidencialidad es desvelar datos a usuarios no autorizados; que comprende también la privacidad (la protección de datos personales).
- **c)** Disponibilidad es que la información se encuentre accesible en todo momento a los distintos usuarios autorizados.

3 ¿Cúal de estos principios no es aplicable a la seguridad informática?:
- **a)** Confidencialidad.
- **b)** Integridad.
- **c)** Disponibilidad.
- **d)** Verificación.
- **e)** No repudio.

4 ¿Qué elemento de un sistema informático se considera más crítico a la hora de protegerlo?:
- **a)** Comunicaciones.
- **b)** Software.
- **c)** Hardware.
- **d)** Datos.

5 Un hacker:
- **a)** Siempre tiene una finalidad maliciosa.
- **b)** La mayoría de las veces tiene una finalidad maliciosa.
- **c)** A veces posee una finalidad maliciosa, entonces se denomina cracker.
- **d)** Es un curioso con finalidad impredecible.

6 El phishing:
- **a)** Es un tipo de fraude bancario.
- **b)** Es un tipo de malware o virus.
- **c)** Se contrarresta con un spyware.
- **d)** Se propaga mediante correo electrónico siempre.