Material para a formación profesional inicial

UD01. Introdución á seguridade informática

Familia profesional	IFC	Informática e comunicacións
Ciclo formativo	CMIFC01	Sistemas microinformáticos e redes
Grao		Medio
Módulo profesional	MP0226	Seguridade informática
Unidade didáctica	UD01	Introdución á seguridade informática
Actividade	**A01**	**Introdución á seguridade informática**
Autoras		Amalia Falcón Docampo Laura Fernández Nocelo Marta Rey López

1. Seguridade informática

O espectacular auxe de Internet e dos servizos telemáticos fixo que a nosa vida se convertera en dixital: empregamos o teléfono móbil, a tablet, o ordenador e a televisión para conectarnos a Internet e enviar emails, whatsapps, comprar, estudar, contactar con empresas ou organizacións a través das súas páxinas web, etc.

Isto fai que sexa moi importante asegurar un correcto funcionamento dos sistemas e das redes informáticas, xa que calquera erro nos mesmos pode supoñer unha grande perda económica, ou xa non digamos de privacidade, ao estar exposta toda a información que hoxe en día está almacenada nos equipos e servidores das empresas.

Principalmente polo uso de Internet, o tema de la protección da información transfórmase nunha necesidade.

Cunhas boas políticas de seguridade, tanto físicas como lóxicas, conseguiremos que os nosos sistemas sexan menos vulnerables ás distintas ameazas.

Dado que a seguridade informática 100% é imposible, temos que intentar lograr un nivel de seguridade máximo en base ás nosas posibilidades e estar preparados para que, cando se produzan os ataques, os danos poidan ser evitados ou en caso contrario ter sido o suficientemente precavidos para realizar copias.

Que é a seguridade informática

Segundo a R.A.E. o termo Seguridade significa *"Estar libre y exento de todo peligro, daño o riesgo"*

Se aplicamos este concepto aos sistemas de información e informáticos, podemos definir a seguridade informática como a disciplina que se encarga de deseñar as normas, procedementos, métodos e técnicas destinadas a conseguir un sistema de información ou informático seguro e fiable.

Así, segundo a **ISO27002** a seguridade da información pódese caracterizar pola preservación de **("CIA", *Confidentiality, Integrity, Availability*):**

- **Confidencialidade:** Asegura que o acceso á información está adecuadamente autorizado
- **Integridade:** Salvagarda a precisión e completitude da información e os seus métodos de proceso
- **Dispoñibilidade**: Asegura que os usuarios autorizados poidan acceder á información cando a necesitan.

A norma **ISO 7498** define a Seguridade Informática como "una serie de mecanismos que minimizan la vulnerabilidad de bienes y recursos en una organización"

Segundo **INFOSEC Glossary 2000:** *«Seguridad Informática son las medidas y controles que aseguran la confidencialidad, integridad y disponibilidad de los activos de los Sistemas de Información, incluyendo hardware, software, firmware y aquella información que procesan, almacenan y comunican»*

Polo tanto, a seguridade non é un **produto** senón que é un **proceso.**

Como a seguridade absoluta é indemostrable, fálase de *fiabilidade*, que é a probabilidade de que un sistema se comporte tal e como se espera de el.

Principios da seguridade informática

Os tres principios básicos da seguridade informática son:

- 1. Principio do **acceso máis sinxelo**: O intruso ao sistema empregará o artiluxio que faga máis sinxelo o seu acceso e posterior ataque. O *punto máis débil* é a vulnerabilidade máis seria, polo que os expertos en seguridade informática deben considerar todas as posibles formas de acceso.
- 2. Principio da **caducidade do secreto**: Os datos confidenciais deben protexerse soamente ata que ese secreto perda o seu valor como tal.
- 3. Principio da **eficiencia** das medidas tomadas: As medidas de control impleméntanse para que teñan un comportamento **efectivo**, **eficiente**, sexan sinxelas de usar e **apropiadas** ao medio.

Os especialistas en seguridade informática deben ter en conta estes tres principios básicos dado que o destino dos ataques informáticos pode ser calquera activo do sistema informático: *hardware, software, datos e persoas,* de xeito que a seguridade é unha cadea, tan débil como o máis débil dos seus elos.

Obxectivos da seguridade informática

En base ás definicións dadas para a seguridade informática podemos deducir os obxectivos principais da mesma:

- **Confidencialidade:** garante que os recursos soamente estean dispoñibles para as persoas ou máquinas (en diante, *axentes*) debidamente autorizadas.
- **Dispoñibilidade:** intenta que os axentes poidan acceder aos servizos con normalidade no horario establecido. Para iso invertese en sobredimensionar os recursos.
- **Integridade:** garante que os recursos do sistema soamente poidan ser modificados polos axentes autorizados, é dicir, os datos teñen que quedar almacenados tal e como espera o usuario: que non sexan alterados sen o seu consentimento.

Fonte: MONOGRÁFICO: *Introducción a la seguridad informática*. INTEF. Ministerio de Educación.

A seguridade consiste en manter o equilibrio axeitado entre estes tres factores. Non ten sentido conseguir a confidencialidade para un arquivo se é a costa de que nin tan sequera o usuario administrador poida acceder a el, xa que se está negando a dispoñibilidade.

Dependendo do entorno de traballo e as súas necesidades pódese dar prioridade a un aspecto da seguridade ou a outro. Así por exemplo, en ambientes militares sempre é prioritaria a confidencialidade da información fronte á dispoñibilidade.

Xunto a estes tres obxectivos principais estúdase tamén a *autenticación* e o *non repudio*:

- **Autenticación.** Intenta confirmar que unha persoa ou máquina é quen di ser.
- **Non repudio:** garante a participación das partes nunha comunicación, é dicir, ante unha relación entre dúas partes, intentaremos evitar que calquera delas poida negar que participara nesa relación.

Estes obxectivos están relacionados entre si de xeito que uns dependen da existencia dos outros. É ao que se lle chama CIDAN (polas súas siglas)

Para conseguir estes obxectivos empréganse os seguintes mecanismos:

- **Autorización.** Unha vez autenticado, os distintos usuarios da información terán distintos privilexios sobre ela: só lectura, ou lectura e modificación.
- **Encriptación.** A información estará cifrada para que sexa inútil a quen non supere a autenticación.
- **Auditoría.** Rexistra e analiza as accións desenvolvidas polos distintos axentes do sistema.
- **Copias de seguridade e imaxes de respaldo**
- **Antivirus, antispyware,..**
- **Devasas e proxys**
- **Sistemas de identificación dixital**. Firma electrónica e certificado dixital.
- **Normativa e leis sobre seguridade informática.**

Elementos vulnerables no sistema informático

A seguridade debe protexer todos os **activos** das empresas, de xeito que teremos que ter en conta todos os recursos do sistema:

- **Hardware**: elementos físicos do sistema informático, tales como procesadores, electrónica e cableado de rede, medios de almacenamento (cabinas, discos, cintas, DVDs,...).
- **Software**: elementos lóxicos ou programas que se executan sobre o hardware, tanto se é o propio sistema operativo como as aplicacións.
- **Datos**: A información lóxica que procesa o software facendo uso do hardware. En xeral serán informacións estruturadas en bases de datos ou paquetes de información que viaxan pola rede.
- **Outros:** funxibles, persoas, infraestruturas,.. aqueles que se 'usan e gastan' como pode ser a tinta e papel nas impresoras, os soportes tipo DVD ou incluso cintas se as copias se fan nese medio, etc.

Deles os máis críticos son os datos, o hardware e o software. É dicir, os datos que están almacenados no hardware e que son procesados polas aplicacións software. Aínda podemos concluír que o **máis crítico son os datos**, pois o resto podemos repoñelos con facilidade, mentres que os datos dependerá de que se fixeran as copias de seguridade.

Fonte: MONOGRÁFICO: *Introducción a la seguridad informática*. INTEF. Ministerio de Educación.

Conceptos de seguridade informática

Para poder protexer os recursos ou activos do sistema informático e minimizar os riscos, debemos coñecer cales son as ameazas e ataques ás que están expostos. Para iso, definamos os seguintes conceptos básicos:

- ***Exposición:*** Forma de posible perda ou dano nun sistema de computación.
- ***Vulnerabilidade:*** Debilidade do sistema de seguridade que pode ser empregada para causar unha perda ou dano.
- ***Ataque:*** Acción de provocar un dano ao sistema de forma intencionada.
- ***Ameaza:*** Presenza de factores que atacarían ao sistema causando un dano ou unha perda mediante a exposición, modificación ou destrución de información ou mediante a denegación de servizos críticos (os ataques por parte de persoas son exemplos de ameazas, o mesmo que os desastres naturais, os erros humanos, e os erros internos no hardware ou no software).
- ***Dano:*** Consecuencia dunha vulnerabilidade, ameaza ou ataque
- ***Control:*** Medida de protección -unha acción, un dispositivo, un procedemento, ou unha técnica- que reduce unha vulnerabilidade.

Se consideramos como risco a probabilidade de que se materialice unha ameaza aproveitando unha vulnerabilidade, debemos avaliar os riscos considerando o impacto que poidan ter os danos que se produzan sobre os activos e vulnerabilidades do sistema.

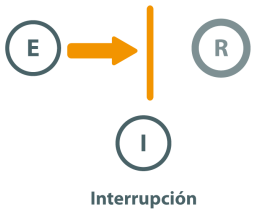
Tipos de ataques aos recursos

Faremos unha clasificación segundo os obxectivos de seguridade que vulneran e outra clasificación segundo a acción que realizan.

Segundo os obxectivos de seguridade que vulneran

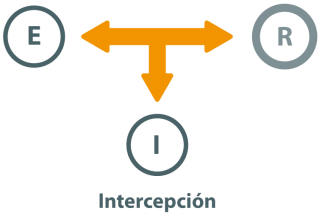
Hai catro formas de ameazas á seguridade dun sistema de computación:

- **Interrupción**: Vulnera o obxectivo de dispoñibilidade. Un recurso do sistema é destruído ou se volve non dispoñible. Tamén é denominado Negación de Servizo. Por exemplo, destrución dun dispositivo hardware, borrado dun programa ou dun ficheiro de datos, ou fallo do Sistema Operativo.



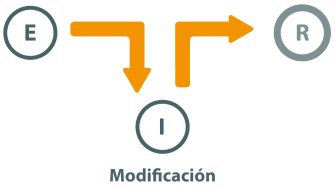
Interrupción

- **Intercepción**: Vulnera o obxectivo de confidencialidade. Unha entidade non autorizada consegue acceso a un recurso. Por exemplo, copia ilícita de programas ou datos, escoita non autorizada nunha rede, etc.



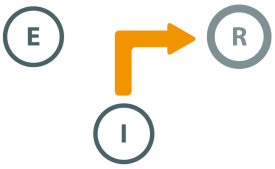
Intercepción

- **Modificación**: Vulnera o obxectivo de integridade. Unha entidade non autorizada non só consegue acceder a un recurso, senón que é capaz de manipulalo. Por exemplo, modificar valores nunha base de datos, modificar os datos que se están transmitindo pola rede, etc.



Modificación

- **Fabricación**: Vulnera a autenticidade. Trátase dunha modificación na que o obxecto fabricado é idéntico ao orixinal: unha entidade non autorizada insire obxectos falsificados no sistema. Por exemplo, o *phising*.



Fabricación

Segundo a forma de actuar dos ataques:

- **Spoofing ou suplantación de identidade**: O atacante modifica a dirección IP (IP Spoofing), a dirección MAC (MAC Spoofing), ou a IP do DNS (DNS spoofing) de orixe dos paquetes de información que envía á rede, falsificando a súa identificación para facerse pasar por outro usuario. Deste xeito, o atacante pode asumir a identificación dun usuario válido da rede, obtendo os seus privilexios.
- **Sniffing ou análise de tráfico:** Consiste en capturar paquetes de información que circulan pola rede coa utilización dunha ferramenta para devandito fin, instalada nun equipo conectado á rede; ou ben mediante un dispositivo especial conectado ao cable. En redes sen fíos a captura de paquetes é máis simple, xa que non require de acceso físico ao medio.
- **Introdución de Código Malicioso – Malware** (*mal*icious soft*ware*): Todo programa ou fragmento do mesmo que xera algún tipo de problema no sistema no cal se executa sen o coñecemento do seu propietario, interferindo desta forma co normal funcionamento do mesmo. Existen diferentes tipos de código malicioso:
  - **Virus:** secuencia de código que se insire nun ficheiro executable (denominado hóspede), de forma que cando o arquivo se executa, o virus tamén o fai, inseríndose a si mesmo noutros programas.
  - **Vermes:** programa capaz de executarse e propagarse por si mesmo a través da rede, en ocasións portando un virus ou aproveitando *bugs* dos sistemas aos que conecta. Ao ser difíciles de programar o seu número non é moi elevado, pero o dano que poden causar é moi grande. Un verme pode automatizar e executar nuns segundos todos os pasos a seguir por un atacante humano para acceder ao noso sistema: mentres que unha persoa, por moitos coñecementos e medios que posúa, tardará como mínimo horas en controlar a nosa rede completa (un tempo máis que razoable para detectalo), un verme pode facer iso mesmo en poucos minutos.
  - **Bombas lóxicas**: son programas daniños que se activan en determinadas circunstancias. As bombas lóxicas son partes de código de certos programas que permanecen sen realizar ningunha función ata que son activadas; nese punto, a función que realizan non é a orixinal do programa, senón que xeralmente trátase dunha acción prexudicial.

- **Troianos**: son programas aparentemente inofensivos, cunha determinada función ou utilidade, pero que contén código oculto para executar accións non esperadas polo usuario.
- **Portas traseiras (backdoors):** son "atallos" que habitualmente deixando os progamadores mentres desenvolven as aplicacións ou os sistemas operativos para conseguir maior velocidade á hora de detectar e depurar fallos. Algúns programadores poden deixar estes atallos nas versións definitivas do *seu software* para facilitar un mantemento posterior, para garantir o seu propio acceso, ou simplemente por descoido. A cuestión é que si un atacante descobre unha destas portas traseiras vai ter un acceso global a datos aos que non debería poder acceder.
- **Rootkits**: son un tipo de troianos utilizados para ocultar portas traseiras que faciliten o acceso e control do sistema infectado cos máximos privilexios posibles.
- **Espías (Spyware)**: son aplicacións que recollen e envían información sobre as páxinas web que máis frecuentemente visita un usuario, tempo de conexión, datos relativos ao equipo no que se atopan instalados (sistema operativo, tipo de procesador, memoria, etc.) e, ata, hai algúns deseñados para informar de si o software que utiliza o equipo é orixinal ou non.
- **Adware:** son programas que abren ventás emerxentes mostrando publicidade de produtos e servizos. Normalmente o usuario é consciente diso e dá o seu permiso. Estes programas xeralmente están relacionados cos spyware, e envían a información recompilada ao servidor remoto que lles devolve máis publicidade que presentar.
- **Programas coello ou bacterias:** son programas que non fan nada útil, senón que simplemente dedícanse a reproducirse ata que o número de copias acaba cos recursos do sistema (memoria, procesador, disco. . .), producindo unha negación de servizo.
- **Técnicas salami:** consiste no roubo automatizado de pequenas cantidades de bens (xeralmente diñeiro) dunha gran cantidade orixe. O feito de que a cantidade inicial sexa grande e a roubada pequena fai extremadamente difícil a súa detección: si dunha conta con varios millóns de pesetas róubanse uns céntimos, ninguén vaise dar conta diso.
- **Keylogger**: é unha aplicación destinada a rexistrar todas as teclas que un usuario teclea na súa computadora. Algúns deles ademais rexistran outro tipo de información útil para un atacante, como ser, imaxes de pantalla.
- **Hijacker ou secuestro**: é un programa que modifica as páxinas de inicio do navegador e redirecciona as páxinas de procura.
- **Bromas (Joke):** é un código que non realiza ningunha acción prexudicial para o equipo pero que gasta unha "broma" ao usuario facéndolle pensar que o seu ordenador está infectado.
- **Exploit:** é un código que se aproveita dun bug ou dunha vulnerabilidade no sistema para poder atacalo.
- **Rogueware:** é un falso antivirus, fanche crer que o sistema está infectado e cobran para a suposta desinfección.
- **Hoaxes**: son *bulos* que se distribúen a través de Internet, recorrendo as mensaxes de correo que informan sobre a aparición dun novo virus

extremadamente perigoso, cando en realidade trátase dunha información totalmente falsa.

- **Ramsonware**: é un programa que cifra arquivos e pide ao usuario que pague un rescate se quere o contrasinal para recuperar os arquivos orixinais.
- **Bots**: os sistemas infectados son "zombies" que conforman unha "botnet" ou rede de bots; esta rede está controlada polos hackers de chapeu negro para que realicen ordes de forma remota

- **Conexións non autorizadas:** o seu obxectivo é conectarse a servidores e equipos sen autorización a través de exploits, portas traseiras, rootkits,...
- **Denegación de Servizo:** O seu obxectivo é degradar considerablemente ou deter o funcionamento dun servizo ofrecido por un sistema ou dispositivo de rede. Existen diferentes técnicas para a explotación deste tipo de ataques:
  - **Envío de paquetes de información mal conformados** de xeito de que a aplicación que debe interpretalo non pode facelo e colápsase.
  - **Inundación da rede** con paquetes (por exemplo, paquetes ping) que non permiten que circulen os paquetes de información de usuarios.
  - **Bloqueo de contas** por excesivos intentos de login errados.
- **Enxeñaría Social:** Consiste en utilizar artiluxos, tretas e outras técnicas para o engano das persoas logrando que revelen información de interese para o atacante, como poden ser contrasinais de acceso. Diferénciase do resto das ameazas basicamente porque non se aproveita de debilidades e vulnerabilidades propias dun compoñente informático para a obtención de información.
- **Phishing*:*** Consiste no envío masivo de mensaxes electrónicas que finxen ser notificacións oficiais de entidades/empresas lexítimas co fin de obter datos persoais e bancarios dos usuarios. Xeralmente, as mensaxes redireccionan aos usuarios cara a páxinas web falsas que imitan ás orixinais dos servizos bancarios que pretenden suplantar.
- **Pharming**: Trátase de redirixir un nome de dominio a outra máquina distinta falsificada e fraudulenta.
- **Cross-Site Scripting (XSS):** consiste en executar código script nun navegador de maneira que poidan enganar ao usuario, por exemplo reenchendo formularios con datos confidenciais.
- **Inxección de código SQL**: consiste en inserir novas sentenzas SQL que o servidor non debería de aceptar.
- **Cracking de passwords:** consiste en descubrir os contrasinais utilizando ataques por dicionario ou por forza bruta.
- **Escaneo de portos:** consiste en verificar os servizos que presta unha máquina por medio da revisión dos portos abertos.

Tipos de atacantes

Os atacantes clasifícanse en:

- **Hackers**: persoas expertas en programación (con grandes coñecementos informáticos e telemáticos) que se dedican a investigar os sistemas de seguridade para descubrir as súas vulnerabilidades e informar aos propietarios do sistema para que as solucionen. Non buscan danar os sistemas nin un beneficio económico, polo que tamén se coñecen como hackers de chapeu branco.
- **Crackers ou hackers de chapeu negro**: persoas que intentan acceder aos sistemas e recursos da rede con fins maliciosos, ben para beneficio persoal ou ben con fins económicos. O término *cracker* creárono os hackers para diferenciarse deles: provén das palabras *cr*iminal h*acker.*
- **Programadores de malware**: persoas expertas en programación que crean programas maliciosos e que poñen na rede conseguindo que se distribúan rapidamente para ocasionar o máximo dano posible.
- **Phreakers**: persoas expertas en telefonía. Manipulan a rede telefónica para realizar chamadas gratuítas.
- **Spammers**: persoas que envían millóns de mensaxes de correo electrónico non desexado (coñecido como *spam)*, colapsando os servidores de correo e os buzóns dos destinatarios, provocando diariamente custos incalculables de tempo. Normalmente utilizan virus para realizar o envío masivo de correos a todos os destinatarios da libreta de direccións.
- **Estafador**: utiliza o correo electrónico ou outro medio para enganar a outras persoas para que brinden información confidencial como número de conta ou contrasinais.
- **Ciberterroristas**: persoas expertas en informática e telemática que están ao servizo de países e organizacións con obxecto de espiar ou sabotar sistemas informáticos.
- **Sniffers**: persoas que escoitan o tráfico da rede con obxecto de descifralo.
- **Lammers**: son xóvenes que sen grandes coñecementos informáticos créense auténticos hackers. Estes mozos descargan programas de Internet para realizar os seus ataques sen saber moi ben como funcionan, o que fai que sexa fácil rastrexalos.
- **Newbie**: son os hackers novatos.
- **Kiddies**: son persoas sen ningún coñecemento informático que instalan calquera cousa que descargan de Internet, infectándose de malware e poñendo en risco aos demais equipos .
- **Persoal interno**: son persoas que traballan nunha empresa ou organización que de xeito voluntario ou involuntaria perpretan un ataque á seguridade do sistema.
- **Ex-empregados**: son persoas que pertenceron á empresa ou organización e que por vinganza atacan á súa antiga empresa.

Exemplos de signos de ataque

- O sistema párase
- Intentos de escritura nos arquivos do sistema
- Algúns arquivos desaparecen
- Denegación de servicio (o sistema pasa a monousuario, e nin sequera o administrador pode entrar)
- As prestacións do sistema son inexplicablemente baixas
- Inestabilidade do sistema, con frecuentes caídas
- Apertura inusual de portos
- Incremento do tráfico de rede
- Desactivación de algunhas aplicacións: antivirus, cortafuegos,...
- Logins desde lugares ou a horas non habituais
- Arquivos con nomes sospeitosos
- Cambios nos arquivos de contrasinais, listas de grupos, etc.
- Cambios nos arquivos de configuración do sistema, en bibliotecas, en executables, etc.
- Cambios nos datos: páxinas WWW, servidores FTP…
- Ferramentas deixadas atrás polo atacante: Cabalos de Troia, Sniffers, etc.
- Procesos periódicos ou transferencias periódicas (ftp, mail) non xustificables
- Incremento repentino do envío de mensaxes a outros usuarios

Exemplos de buratos na seguridade

- Contrasinais sinxeñass de adiviñar, ou contrasinais por defecto
- Contas inactivas ou non usadas, contas innecesarias ou con privilexios excesivos, contas de grupo
- Protocolos mal deseñados
- Servizos non seguros mal configurados (tftp, sendmail, ftp)
- Servizos non seguros e inútiles (finger, rusers, rsh)
- Arquivos de configuración da rede ou de acceso non seguros (“entradas +” en configuración NIS)
- Consolas inseguras (telnet, rlogin)
- Protección de acceso e propiedade de arquivos sensibles mal configurada
- Versións non actualizadas do sistema operativo ou das aplicacións instaladas
- Conexións telefónicas inseguras
- Política de copias de seguridade inexistente ou mal deseñada

…

Mecanismos de protección

Partindo da premisa de que ningún mecanismo pode garantirnos a seguridade ao 100%, podemos poñer en práctica as seguintes medidas de protección:

- Manter actualizado o sistema operativo e as aplicacións instaladas: É a única forma de previr e corrixir vulnerabilidades. Todo o noso software debe estar actualizado, pero especialmente o sistema operativo e os programas que utilizamos en Internet.
- Utilizar sempre un antivirus: Non basta con instalalo, debemos realizar revisións periódicas do noso ordenador (a maioría de antivirus permiten programar estas revisións de xeito automático). Ademais é esencial mantelo actualizado (estímase que aparecen da orde de 20 virus novos cada día ...).
- Utilizar software antispyware/antiadware: A maioría de programas antivirus non detectan nin eliminan correctamente aos programas espía, polo que é preciso utilizar un software específico para o seu detección e eliminación.
- Eliminar a conta de invitado e cambiar o nome á conta de administrador, xa que son contas coñecidas por todos.
- Utilizar contrasinais seguras e diferentes para cada un dos servizos: As contrasinais de acceso aos servizos deben ser fortes para evitar a suplantación de identidade. Ademais deben ser distintas para cada servizo para que no caso de que consigan pescudar unha, non se vexan afectados o resto de servizos.
- Non visitar sitios web potencialmente perigosos e evitar descargas de arquivos dende lugares non seguros: A maioría dos secuestros de navegador prodúcense ao visitar páxinas que ofrecen descargas de música, películas, software pirata ou pornografía. En xeral debemos desconfiar de descargas gratuítas dende sitios web descoñecidos. Se queremos baixar programas freeware ou shareware, é preferible facelo desde portais especializados, ou ben acudir directamente á páxina do fabricante correspondente. Do mesmo xeito, para descargar drivers ou actualizacións de programas, a opción máis segura tamén é visitar o servidor web do fabricante correspondente. O risco de infectarse ao instalar software legal é normalmente moi baixo. Pola contra, os programas manipulados para saltarse protecións ou os cracks poden esconder troianos ou outras clases de virus.
- Evitar os programas de intercambio de arquivos (P2P): Á marxe de discusións sobre a legalidade do seu uso, desde o punto de vista da seguridade, este tipo de programas normalmente esconden software espía ou adware.
- Instalar devasas: As devasas ou firewall persoais protéxennos de accesos indebidos desde/a Internet.
- Ser especialmente coidadoso co correo e a mensaxería instantánea: O correo electrónico é con diferenza o medio preferido polos virus actuais. As principais precaucións a tomar son:
    - Borrar inmediatamente o spam e as mensaxes de orixe dubidosa. Se o noso cliente de correo permite filtralos automaticamente, mellor.

- Non abrir NUNCA un arquivo achego se non estamos absolutamente seguros do seu contido. Coñecer ao remitente non é unha garantía, xa que moitos virus len a libreta de direccións do ordenador infectado.
- Cortar as pirámides e cadeas de correo. Aínda que fosen certas compórtanse como hoaxes ou spam, polo que non debemos difundilas.
- Non dar crédito aos *bulos* e falsas alarmas, por convincentes que resulten.

- Coidado coa enxeñaría social. Moitos hackers recompilan información relevante para os ataques facéndose pasar por usuarios novatos que piden axuda en toda clase de chats. Non debemos aceptar ficheiros de descoñecidos, nin tampouco acceder a enviarllos.
- Debemos sospeitar si observamos calquera comportamento estraño, ou calquera cambio que non foi realizado por nós, especialmente se instalamos novos programas recentemente. Algúns síntomas sospeitosos poderían ser:
  - Diminución notable do rendemento, inestabilidade, colgues ou reinicios inesperados.
  - Aumento inexplicable da ocupación de disco duro ou do consumo de memoria.
  - Elevado consumo de CPU ou sospeitosos accesos a disco ata en períodos de suposta inactividade.
  - "Fenómenos estraños" nos que a unidade de CD-ROM, o teclado ou outros periféricos parecen cobrar "vida propia"
  - Estraños cambios na aparencia do escritorio, o fondo de pantalla, as iconas, o funcionamento do rato, etc ... Ou na visualización (a pantalla vese investida ou aparecen carácteres ou mensaxes estrañas)
  - Episodios de secuestro do navegador web

No enlace https://www.osi.es/es/herramientas-gratuitas tes unha lista de ferramentas de protección gratuítas.

Clasificación da seguridade informática

Podemos facer diversas clasificacións da seguridade informática en función de distintos criterios:

- Segundo **que** activo se quere protexer :
  - Seguridade física: protexe o hardware
  - Seguridade lóxica: protexe o software e datos
- Segundo **cando se actúa** para protexer:
  - Seguridade activa (Prever): actúase antes do ataque evitando os danos nos sistemas
  - Seguridade pasiva (Curar): actúase despois do ataque minimizando os danos ocasionados.

Algúns mecanismos de defensa ante ameazas ás seguridade física:

Amezas	Mecanismos de defensa
Sobrecarga na rede eléctrica. Apagóns	SAI, Grupos Electróxenos, Baterías, Regretas protectoras Desenchufar equipos
Fogo	Sistemas antiincendios, extintores. Armarios ignífugos Alonxar de salas con transformadores, motores, etc.
Roubo	Portas seguridade. Alarmas. Cámaras vixilancia. Pechaduras. Control de acceso (vixiantes)
Golpes, tiróns	Colocar o equipo e cableado fora de sitios de paso. Protexelo en armarios, falso chan, canaletas, etc. Empregar periféricos a proba de golpes Empregar cables de lonxitude suficiente
Humidade, Entrada de auga	Localización lonxe de ventás Sistemas extractores de humidade (A/A) Paredes que no dean ao exterior Non poñer os equipos no chan. Non poñer bebidas enriba da mesa do equipo Non poñer equipos baixo consolas de A/A (desaugan)
Inundacións	Investigar sobre o historial de inundacións na zona Non poñer en planta baixa a sala dos equipos
Calentamento	Aire acondicionado Localización lonxe de ventás ou zonas calurosas Limpeza periódica da sala e equipos Sistemas de refrixeración
Deterioro do hardware	Limpeza, Mantemento

Mecanismos de defensa ante ameazas á seguridade lóxica:

Amezas	Mecanismos de defensa
Virus, spyware…	Antivirus, antispyware Non executar o sistema operativo con permisos de administrador
Roubo de información	Contrasinais de acceso seguras ACL`s Cifrado Backups (copias de seguridade)
Crackers	Antivirus, firewall, IDS, …
Perda de integridade do sistema Avarías	Ferramentas de chequeo do equipo. Comprobadores md5 Backups. RAID (Discos redundantes)
Mal uso por parte de usuarios	Contrasinais seguras. Contas de usuario con permisos limitados.

Das medidas indicadas anteriormente podemos clasificar como medidas de seguridade pasiva a realización de copias de seguridade, instalación de SAIs, e os RAID, e as demais medidas podémolas clasificar como medidas de seguridade activa.

Políticas de Seguridade

Unha boa *Política de Seguridade* ten como obxectivo definir como se vai a protexer unha organización ante os posibles ataques. Consta de dúas partes:

- Política xeral: Define o enfoque xeral:
  - Análise de vulnerabilidade
  - Identificación das ameazas
- Regras específicas: Definen as características e accións concretas, para cada servizo ou sistema, orientada a cumprir os obxectivos da política xeral.

Polo tanto, a Política de Seguridade é o documento de referencia que define os obxectivos de seguridade e as medidas que deben implementarse para ter a certeza de alcanzar estes obxectivos.

Claves dunha boa política de seguridade

Unha boa política ten que ter definidos os seguintes aspectos:

- **Autoridade**: Quen é o responsable?
- **Ámbito**: A quen afecta?
- **Caducidade**: Cando remata?
- **Especificidade**: Que se require?
- **Claridade**: É entendible por todos?

Características dunha boa política de seguridade

- Tense que poder poñer en práctica mediante **procedementos concretos** de administración de sistemas, mediante a publicación de guías sobre o uso aceptable dos recursos informáticos ou mediante outro métodos prácticos apropiados.
- Non debe ser una entelequia. Debe ser **implementable**
- Débese obrigar o seu cumprimento mediante **ferramentas de seguridade**, onde sexa posible, e mediante **sancións**, onde a prevención no sexa posible tecnicamente.
- Non debe ter buratos, e se os te hai que poder detectalos
- Debe definir claramente as **áreas de responsabilidade** dos usuarios, os administradores e a dirección
- Ten que haber un **responsable** para toda situación posible.

Compoñentes dunha boa política de seguridade

- **Guía de compra de hardware e software**, onde se especifique as funcións relacionadas coa seguridade requiridas ou desexadas.
- Unha **política de privacidade** que asegure un nivel mínimo de privacidade en canto a acceso a correo electrónico, arquivos de usuario, arquivos de traza, etc.
- Unha **política de acceso** que defina os niveis de seguridade, os dereitos e privilexios, características das conexións ás redes internas e externas, mensaxes de aviso e notificación, etc.
- Unha **política de responsabilidade** que defina as responsabilidades dos usuarios, e do persoal técnico e de xestión. Debe definir os procedementos de auditoría e de xestión de incidentes (a quén avisar, cándo e cómo, etc.)
- Unha **política de autenticación** que estableza un esquema de contrasinais ou palabras de paso (passwords), que especifique modelos para a autenticación remota ou o uso de dispositivos de autenticación
- Unha **declaración de dispoñibilidade**, que aclare as expectativas dos usuarios en canto á dispoñibilidade dos recursos. Debe definir temas como a redundancia, a recuperación ante intrusións, información de contacto para comunicar erros nos sistemas /ou na rede, etc.
- Unha **política de mantemento** que describa cómo se leva a cabo o mantemento interno e externo, se se permite mantemento remoto e/ou mantemento por contratas externas, etc.
- Unha **política de comunicación de violacións** que defina qué tipos de ameazas, e cómo e a quén se deben comunicar.
- Información de apoio que indique aos usuarios, persoal técnico e administración cómo actuar ante calquera eventualidade, cómo discutir con elementos externos os incidentes de seguridade, qué tipo de información se considera confidencial ou interna, referencias a outros procedementos de seguridade, referencias a lexislación da compañía e externa, etc.

Referencias

- CESAR SEOANE RUANO e outros. *Seguridad Informática*. Ed. McGraw-Hill.
- ALFREDO ABAD DOMINGO. *Seguridad y alta disponibilidad*. Ed. Garceta. 2013
- XESUS COSTAS SANTOS. *Seguridad informática*. Editorial Ra-Ma. 2010
- STALLINGS, W. (2004). *Fundamentos de Seguridad en Redes. Aplicaciones y estándares. (2ª ed.)*. Editorial Pearson
- Web do *Instituto Nacional de Ciberseguridad*:

  https://www.incibe.es
- Web da *Oficina de seguridad del internauta (OSI)*:

  https://www.osi.es/es/
- INEF. Instituto Nacional de Tecnologías Educativas y Formación de Profesorado. *Monográfico: Introducción a la seguridad informática*. Ministerio de Educación, Cultura e Deporte.
- OSI. *Herramientas gratuitas*

  https://www.osi.es/es/herramientas-gratuitas
- Enlaces de interese:
  - *El Lado del Mal* - http://www.elladodelmal.com/
  - *Hispasec* - http://www.hispasec.com/
  - *Security by default* - http://www.securitybydefault.com/
  - *S21Sec* - http://blog.s21sec.com/