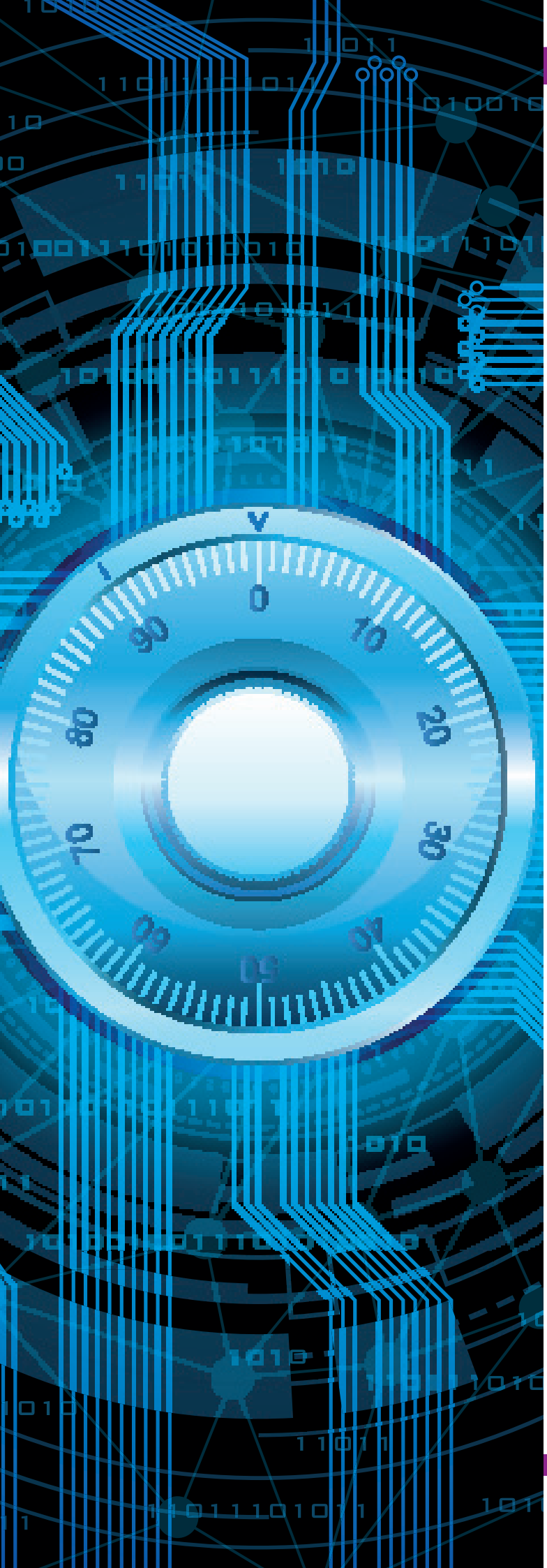

unidad 1

Introducción a la seguridad informática

SUMARIO

- Seguridad de la información y seguridad informática
- Conceptos básicos relacionados con la seguridad informática
- Principios básicos de la seguridad informática
- Políticas de seguridad
- Planes de contingencia

OBJETIVOS

- Conocer las diferencias entre seguridad de la información y seguridad informática.
- Aprender los conceptos básicos relacionados con el mundo de la seguridad informática.
- Describir cuáles son los principios básicos de la seguridad.
- Conocer qué son y qué utilidad tienen las políticas de seguridad.
- Aprender en qué consisten los planes de contingencia.

Ideas clave

Hispasec

Inteco

Hackhispano

Websecurity

Seguridad en la red

Intypedia

Historia secreta de los hackers

Hispasec

Enciclopedia de la seguridad de la información

Sugerencias didácticas

•• El objetivo principal de esta unidad es aproximarse al concepto de seguridad informática, analizar por qué ha llegado a ser tan necesaria hoy en día y hacer hincapié en lo que la distingue de la seguridad de la información

En esta unidad el alumnado realiza una primera toma de contacto con los conceptos básicos relacionados con la seguridad informática, como cuáles son los activos más valorados, qué son las vulnerabilidades y de qué modo pueden estas afectarles. Además aprenderán a nivel general qué tipo de amenazas y ataques se pueden sufrir, qué se ha de tener en cuenta en un análisis de riesgos y qué impactos y desastres puede provocar un ataque.

También se ofrece un análisis de los principios de la seguridad de la información que tratan de protegerla y del sistema que se utiliza para ofrecer un buen nivel de seguridad a los usuarios.

Por último se abordan los conceptos de políticas de seguridad y planes de contingencia, para que el alumnado sea consciente de la importancia de la seguridad tanto a nivel personal como a nivel empresarial.

Para introducir los conceptos y contenidos que van a ser analizados en la unidad, puede ser útil llevar a cabo una presentación de la misma a través de distintas actividades.

– Algunas páginas web donde se pueden encontrar noticias actuales son:
  - Hispasec Sistemas. Seguridad y tecnologías de la información: www.hispasec.com
  - Instituto Nacional de Tecnologías de la Información: www.inteco.es/landing/Seguridad/
  - Hackhispano: www.hackhispano.com
  - Websecurity. Red social sobre seguridad informática: www.websecurity.es
  - Seguridad en la red, de la Asociación de Intenautas: www.seguridadenlared.org
  - Enciclopedia de la seguridad de la información: www.intypedia.com
– También puede ser interesante utilizar algún video para despertar la curiosidad del alumnado, por ejemplo:
  - Documental *Historia secreta de los hackers:* www.youtube.com/watch?v=-E3JIOedIgw
  - Cualquiera de los presentados en el canal YouTube de Hispasec: www.youtube.com/user/Hispasec
  - Cualquiera de los presentados en la Enciclopedia de la seguridad de la información: www.intypedia.com
– Presentaciones PowerPoint de la unidad.
– Con el fin de fijar los conceptos estudiados en la unidad, es aconsejable realizar un repaso utilizando el documento de ideas clave incluido al final de la unidad.

Así mismo recomendamos realizar varios test del CD *Generador de pruebas de evaluación* para comprobar si el alumnado ha alcanzado los objetivos propuestos.

A continuación se muestra una tabla resumen con todos los recursos de esta unidad.

Recursos de la unidad 1	
CD *Recursos multimedia*	Presentaciones multimedia
CD *Generador de pruebas de evaluación*	

Solucionario de las actividades propuestas

Página 7

1 >> Seguridad informática y seguridad de la información

1·· Debate con tus compañeros de clase la siguiente cuestión: ¿a qué se deben la mayoría de los fallos de seguridad?

La respuesta puede variar según cada alumno y centro de estudios.

La mayoría de los fallos de seguridad se deben a descuidos en las medidas de seguridad, acciones voluntarias o involuntarias del personal de la empresa o ajeno a ella, factores externos como los medioambientales, etc.

2·· Realiza una tabla comparando ejemplos de seguridad pasiva y activa del campo de la informática y del campo de los vehículos.

Informática		Vehículos	
Seguridad pasiva	Seguridad activa	Seguridad pasiva	Seguridad activa
Uso de sistemas de alimentación ininterrumpida	Uso de contraseñas	*Airbags*	Sistemas de frenado
Uso de sistemas RAID	Cortafuegos	Cinturones de seguridad	Neumáticos
Copias de seguridad	Sistemas de vigilancia	Reposacabezas	Sistemas de control de estabilidad

Página 8

2 >> Conceptos básicos en materia de seguridad

3·· ¿Cuál es el activo más valioso para una empresa?

Su activo más importante es la información.

a) ¿Qué vulnerabilidades podrían afectarle?

Los robos, debido por ejemplo a carecer de contraseñas fuertes, a la alteración del contenido o a la destrucción por acceso indebido.

b) ¿Qué amenazas podrían afectarle? Clasifícalas.

- **Amenazas naturales o físicas:** desastres naturales o condiciones medioambientales.
- **Amenazas de tipo involuntario:** provocadas por dejar sin protección determinados ficheros con información sensible o por borrar o modificar accidentalmente algún fichero o parte de la información que contiene. Estas pueden acarrear, por ejemplo, que se interrumpa el sistema en el momento en el que se está usando la información.
- **Amenazas intencionadas:** procedentes de personas, ya sean empleados o no. Un ejemplo es el uso de software ajeno a la empresa para interceptar, borrar o bloquear información protegida.

4·· ¿Crees que la evaluación de riesgos es igual para todas las empresas? ¿Por qué?

No es igual para todas las empresas, ya que depende de las medidas de seguridad que se hayan previsto para proteger los activos de vulnerabilidades y amenazas.

5·· Enumera varias preguntas de las que pueden hacerse en la realización de una evaluación de riesgos.

Algunas de las preguntas que pueden hacerse son las siguientes:

- ¿Qué puede ir mal? ¿Con qué frecuencia puede ocurrir?
- ¿Qué activos hay que proteger?
- ¿Qué consecuencias tendrían lugar si les ocurriese algo no deseado a los activos a proteger?
- ¿Está protegido el sistema informático de posibles desastres naturales o condiciones medioambientales adversas?

- ¿Existen medidas que impidan el acceso físico no autorizado a las instalaciones?
- ¿Se sabe cuál es el nivel de acceso de cada empleado a los activos a proteger?
- ¿Poseen las instalaciones algún tipo de vigilancia cómo cámaras, guardias de seguridad, etc.?
- ¿Poseen las instalaciones sistemas de contingencia como extintores, cámaras, etc.?
- ¿Cómo se actuaría si la seguridad fuera violada?

6·· Busca en Internet aplicaciones comerciales que permitan realizar una evaluación de riesgos.

R-Box

IBM

PILAR

Algunos ejemplos son la herramienta comercial R-Box (http://www.r-box.com.ar/), que gestiona la información; IBM Rational AppScan (http://www-142.ibm.com/software/products/es/es/ibmsecuappsstan), que identifica y soluciona las vulnerabilidades más importantes; o la herramienta libre PILAR. http://www.ccn-cert.cni.es/. Seleccionar en el menú de la izquierda la opción *tools* y escoger la herramienta PILAR.

Página 15

3 >> Principios de seguridad informática

7·· A partir de los principios expuestos en este epígrafe:

a) Plantea un posible ataque contra cada uno de ellos.

b) Indica una posible solución para cada uno de los ataques planteados.

Los principios expuestos son:

Integridad

Un ejemplo sencillo de ataque es la modificación de la información que se transmite desde una base de datos. Otros ataques podrían ser alterar un programa para que funcione de forma diferente, modificar el contenido de los mensajes que están siendo enviados por la red o ataques en redes WiFi como *man in the middle*.

Algunas soluciones para estos ataques son cifrar la información o usar la firma electrónica.

Confidencialidad

Un ataque contra la confidencialidad es el uso de herramientas capaces de capturar información que circula a través de las tarjetas de red, por ejemplo los *sniffers*.

La solución podría ser utilizar comunicaciones cifradas mediante protocolos seguros como SSH o el uso de sistemas de cifrado de clave pública para el envío de correos electrónicos o transacciones bancarias.

Disponibilidad

Un posible ataque es la denegación de servicios (DoS). Para evitarlo puede utilizarse un cortafuegos que proteja tanto el sistema como la red.

Autenticación

Los ataques podrían ser la suplantación de la identidad o el robo de contraseñas. Contra estos podrían emplearse los sistemas de cifrado de clave pública, las soluciones biométricas como sustitución de las contraseñas o el uso de contraseñas fuertes, entre otras soluciones.

8·· Busca más información sobre los sniffers en Internet. ¿Qué son? ¿Qué utilidad tienen?

Son herramientas capaces de capturar información que circula por la red a través de las tarjetas de red.

Sus utilidades se clasifican del siguiente modo:

Utilidades legítimas: resolución de problemas en la red, analizando la red y detectando posibles problemas, o detección de intrusos.

Utilidades ilegítimas: captura de nombres de usuario y contraseñas o de información privada (como números de tarjetas bancarias, PIN, etc.).

Página 16

4 >> Políticas de seguridad

9·· ¿Crees que determinar que los usuarios de una organización tengan una contraseña de acceso segura es una buena política de seguridad?

Sí, es un requisito fundamental.

10·· Indica qué políticas de seguridad establecerías para evitar la caída de los servidores de una organización.

Las políticas de seguridad deben prevenir situaciones no deseadas que puedan derivarse de catástrofes naturales (terremotos, tormentas, etc.), personal tanto interno como externo a la organización (accesos indebidos, mal uso, etc.) o fallos técnicos (problemas derivados del suministro eléctrico, el hardware, el software, etc.).

Algunos ejemplos de políticas de seguridad son tener servidores de respaldo, disponer de tecnología de almacenamiento redundante y distribuido (sistemas RAID), situar los servidores en un entorno físico que los proteja de accesos no autorizados, de factores medioambientales y de catástrofes naturales, poseer buenas instalaciones eléctricas (como sistemas de alimentación ininterrumpida para el caso de fallos eléctricos) o poner en marcha una buena política de copias de seguridad.

Página 17

5 >> Planes de contingencia

11·· ¿Quiénes crees que deben elaborar el plan de contingencia para una empresa?

El personal del departamento de sistemas junto con los responsables de cada área de la organización y aquellos usuarios implicados en los aspectos a reflejar en el plan de contingencia.

12·· ¿Crees que un plan de contingencia, una vez creado, sirve para toda la vida?

No, debe ser revisado y actualizado periódicamente (al menos anualmente).

Solucionario de las actividades finales

Página 18

.:CONSOLIDACIÓN

1·· ¿En qué se diferencian la seguridad activa y la seguridad pasiva?

Seguridad activa: se encarga de prevenir, detectar y evitar cualquier incidente en los sistemas informáticos antes de que se produzca (medidas preventivas). Un ejemplo es la utilización de contraseñas.

Seguridad pasiva: comprende todas aquellas técnicas o procedimientos necesarios para minimizar las consecuencias de un incidente de seguridad (medidas correctoras). Un ejemplo son las copias de seguridad.

2·· Indica algunas razones por las que a alguien le puede interesar realizar un ataque contra la seguridad informática de una empresa.

Para obtener información, para hacer daño, para demostrar que el sistema es vulnerable, para buscar esas vulnerabilidades, por diversión, por venganza de algún empleado descontento, etc.

3·· Enumera posibles activos asociados a una organización.

Los activos de una organización son la información (bases de datos, ficheros, documentos, etc.), los equipos informáticos, los equipos de comunicaciones, el cableado, el software (aplicaciones), el mobiliario, el personal y los vehículos, entre otros.

4·· ¿Cuáles son los posibles puntos débiles en los sistemas informáticos de una organización?

Son puntos débiles las contraseñas débiles, las comunicaciones no cifradas, las aplicaciones y sistemas operativos no actualizados, las aplicaciones no autorizadas, el mantenimiento inadecuado del hardware, la ausencia de sistemas de vigilancia, la ausencia de sistemas contra incendios, la ausencia de sistemas de alimentación ininterrumpida, etc.

5·· ¿Qué recomendaciones harías para evitar en una organización el acceso no autorizado a su información?

Utilizar contraseñas adecuadas, emplear sistemas de usuarios con privilegios de acceso a la información, usar autorizaciones para el acceso físico de los usuarios a las instalaciones de los sistemas informáticos, utilizar sistemas seguros (bajo llave, cifrado, etc.) para almacenar las copias de seguridad, aumentar la formación del personal, etc.

6·· Enumera posibles vulnerabilidades asociadas a las estaciones de trabajo en una organización.

Ubicación insegura de los equipos, contraseñas débiles, uso de software no autorizado por la organización, uso de dispositivos no autorizados o no libres de virus o software malicioso, software no actualizado, antivirus no actualizado, ausencia de protector de pantallas de bloqueo o ausencia de configuraciones de seguridad y de copias de seguridad.

7·· Indica, para los siguientes supuestos, qué principios de la seguridad se están violando:

a) Destrucción de un elemento hardware.

Disponibilidad

b) Robo de un portátil con información de interés de la empresa.

Confidencialidad

c) Robos de direcciones IP.

Autenticación

d) Escuchas electrónicas.

Confidencialidad

e) Modificación de los mensajes entre programas para variar su comportamiento.

Integridad

f) Deshabilitar los sistemas de administración de archivos.

Disponibilidad

g) Alteración de la información que se transmite desde una base de datos.

Integridad

h) Robos de sesiones.

Autenticación

8·· Pon un ejemplo de ataque por ingeniería social. ¿Cómo crees que se puede proteger una organización ante este tipo de ataque?

Un ejemplo de ataque por ingeniería social es el uso de archivos adjuntos en correos electrónicos, a menudo aparentemente provenientes de alguna persona conocida y que dicen contener fotos "íntimas" de alguna persona famosa, algún programa supuestamente gratuito o información de este tipo, pero que en realidad ejecutan código malicioso con la intención, por ejemplo, de usar la máquina de la víctima para enviar cantidades masivas de *spam*.

Algunas medidas preventivas para este tipo de ataques son la utilización de filtros *antispam* en el correo electrónico, antivirus, y programas *antimalware* diversos, concienciación a los empleados de la organización para la buena utilización del correo (no abrir si se sospecha, utilizarlo solo para fines corporativos, etc.).

9·· Analiza el grado que puede alcanzar el impacto a una organización ocasionado por una amenaza meteorológica como un huracán.

El incidente puede ser muy grave, pero si la empresa cuenta con la protección adecuada en su infraestructura, el impacto puede ser leve.

10·· ¿En qué consisten y qué aspectos deben cubrir las políticas de seguridad?

Las políticas de seguridad informática determinan normas y protocolos a seguir en los que se detallan diferentes medidas para proteger la seguridad del sistema. Establecen también los mecanismos necesarios para controlar su correcto funcionamiento.

Toda política de seguridad debe tener en cuenta:

- La protección física, lógica, humana y de comunicación.
- Todos los distintos componentes de la organización.
- El entorno del sistema.

11·· ¿Por qué crees que es importante que una organización tenga un plan de contingencia? ¿Qué consecuencias podrían tener lugar si no se dispusiera de él?

El plan de contingencia es importante ya que, incluso habiendo tomado medidas preventivas, podría producirse algún desastre o acontecimiento no deseado.

La consecuencia que acarrea el no disponer de él es estar expuesto a sufrir pérdidas, que podrían llegar a ser irreparables o al menos mucho más costosas que la implantación de un plan.

12·· ¿En qué consiste el análisis de riesgos y para qué sirve realizarlo?

El análisis de riesgos consiste en estudiar los activos que hay que proteger y cuáles son sus vulnerabilidades y amenazas, así como la probabilidad de que estas se produzcan. Además tiene en cuenta durante cuánto tiempo y qué esfuerzo y dinero se está dispuesto a invertir.

Sirve para saber qué medidas deberán tomarse para conocer, prevenir, impedir, reducir o controlar los riesgos previamente identificados y para reducir al mínimo su potencialidad o sus posibles daños.

13·· ¿Qué utilidad tienen para las organizaciones los planes de contingencia?

Los planes de contingencia aportan medidas detalladas para lograr la recuperación del sistema cuando este falle.

.: APLICACIÓN :.

1·· Suponemos que el hospital X está ubicado cerca de un cauce de río que prácticamente no lleva agua. Su centro de cálculo está situado en el sótano. Se han anunciado lluvias fuertes y por tanto existe una alta posibilidad de desbordamiento del río que pasa cerca de la zona debido a la falta de limpieza de su cauce.

Identifica los activos, las amenazas y las vulnerabilidades del sistema.

Activo: centro de cálculo. **Amenaza:** desbordamiento del río. **Vulnerabilidad:** el hecho de que el activo esté situado en el sótano. Esta vulnerabilidad también está determinada por la frecuencia con la que se desborda el río.

2·· ¿Qué tipo de aplicaciones se pueden utilizar para comprometer la confidencialidad del sistema?

Los *keyloggers*, el *spyware* o los *sniffers*.

3·· Una empresa ha sido atacada y su página web ha sido modificada sin previa autorización. ¿Qué tipo de ataque se ha producido? ¿Qué principios de la seguridad se han visto violados?

Se ha producido un ataque de modificación que afecta a la confidencialidad y la integridad de la empresa.

4·· ¿Qué soluciones se podrían aplicar para que el sistema informático de una entidad bancaria no se viera afectado por un desastre que afectara a sus clientes?

La respuesta puede variar según cada alumno. Sería interesante que primero se enumeraran las vulnerabilidades que pueden detectarse para luego buscar sus soluciones.

Algunas de las vulnerabilidades que pueden proponerse son las relacionadas con el acceso físico a las instalaciones (cámaras de vigilancia, entrada con autorización, etc.) o con el acceso a los sistemas (servidores, estaciones de trabajo, cajeros automáticos, comunicaciones, etc.), las derivadas de la instalación, mantenimiento y uso de las aplicaciones informáticas (incluyendo bases de datos), las de tipo medioambiental o derivadas de catástrofes naturales (fuego, inundación, humedades, etc.), así como otras vistas a lo largo de la unidad.

Algunas posibles soluciones son el acceso físico a las instalaciones por parte del personal mediante tarjetas identificativas o códigos personales; el uso de contraseñas fuertes, sistemas operativos y aplicaciones actualizadas y protegidas mediante un sistema antivirus y antiespía; no permitir la instalación de aplicaciones externas sin previa autorización; mantener protegidas las bases de datos y disponer de un buen plan de copias de seguridad; poseer extintores, sistemas contra inundaciones y sistemas antihumedades en perfecto estado, etc.

Solucionario de las actividades de la revista de informática

Página 23

1·· ¿Por qué crees que las empresas no están implementando las medidas de protección apropiadas para salvaguardar su información?

Piensan que solo son las grandes organizaciones las que están en el punto de mira de los ataques y, por tanto, no se consideran objetivo de los mismos.

2·· Según el texto, ¿qué amenazas a la seguridad pueden sufrir las pymes? ¿Qué otras amenazas añadirías?

Las amenazas que pueden sufrir son el acceso a sus cuentas de banca *online* por no proteger sus máquinas, la usurpación de su identidad y la pérdida de información por no usar antivirus en todos los equipos, el acceso a sus correos electrónicos por no disponer de seguridad en los servidores de correo, la inserción de software malicioso por no tener los antivirus actualizados, la manipulación de la configuración por no tener actualizados los sistemas operativos y errores de usuarios por no proporcionarles una formación adecuada.