Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.
CONSEJERÍA DE ECONOMÍA, INNOVACIÓN, CIENCIA Y EMPLEO

AndalucíaCERT
CENTRO DE SEGURIDAD TIC

Informe de divulgación
Herramientas de seguridad

Tipo de documento:	*Informe*
Autor del documento:	*AndalucíaCERT*
Código del Documento:	*CERT-IF-6137-140903*
Edición:	*0*
Categoría	*Público*
Fecha de elaboración:	*03/09/2014*
N° de Páginas	*1 de 15*

1 TABLA DE CONTENIDOS

2 OBJETO Y ALCANCE

El objetivo de este documento es dar a conocer un conjunto diverso y amplio de herramientas disponibles en Internet que pueden resultar de utilidad para diferentes tareas relacionadas con el análisis de la seguridad TIC o para la protección de sus sistemas o puestos de trabajo.

Este documento va destinado al personal de la Junta de Andalucía y al público en general.

3 INTRODUCCIÓN

A día de hoy existen a nuestra disposición una gran cantidad de **herramientas** que nos pueden ayudar en diferentes tareas relacionadas con la seguridad TIC en general y con la de nuestro sistema en particular.

En este documento hemos querido hacer una pequeña recopilación de herramientas que pueden serles útiles a la hora de mejorar la seguridad de su sistemas, o de protegerse de los distintos peligros existentes tanto en Internet como en su entorno. Se ha intentado primar siempre que el programa sea software libre y/o gratuito, para facilitar su distribución y adquisición, así mismo nos hemos centrado prncipalmente en plataformas Windows y Linux, aunque muchas de las herramientas funcionan en entorno multiplataforma.

Las herramientas que vamos a mostrar han sido clasificadas en las siguientes categorías:

- Protección de la navegación
- Gestores de contraseñas
- Cifrados de archivos y volúmenes
- Comprobación de integridad de ficheros
- Copias de seguridad y clonado de discos
- Cifrado de correos
- Eliminación segura de información
- Comprobación del actualizaciones del sistema
- Particionado
- Control parental
- Suite de aplicaciones de recuperación

4 PROTECCIÓN DE LA NAVEGACIÓN

En este apartado vamos a mostrar una serie de plugins para los navegadores que nos permitirán proteger ciertos aspectos cuando naveguemos por Internet. Los plugins o complementos son programas que se instalan en los navegadores de Internet y que se encargan de proveer funcionalidades extras al mismo. Existen una gran cantidad de navegadores diferentes, las extensiones propuestas abarcan los más usados, haciendo especial hincapié en soluciones basadas en sofware libre.

4.1 NOSCRIPT

La extensión NoScript ofrece a los navegadores basados en Mozilla la posibilidad de permitir que sólo se ejecuten ciertos scripts como Javascript, Java, Flash y otros plugins en sitios de confianza a elección del usuario, además proporciona protección contra ataques XSS y anticlicking.

Sitio: http://noscript.net/

4.2 KB SSL ENFORCER

KB SSL Enforcer se encarga de comprobar y seleccionar la navegación segura en los sitios, en caso de que esta exista de manera automática y transparente.

Destacan las siguientes características:

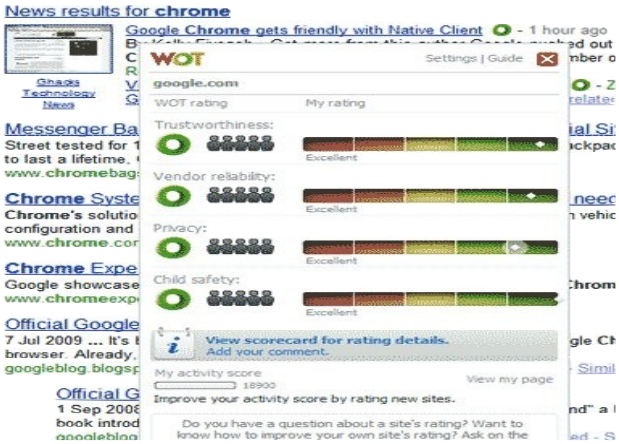
- Detección automática de soporte SSL
- Cacheo de sitios con soporte SSL
- Cambio automático a conexión SSL en caso de encontrarla
- Personalización de opciones para especificar cuándo cambiar

Sitio del proyecto: http://code.google.com/p/kbsslenforcer/

4.3 WOT

WOT es un servicio WEB que se usa para marcar páginas web dependiendo de su reputación, basandose en distintos factores como la presencia de malware, la identificación de páginas de phishing alojadas, la existencia de contenido ofensivo y, de una manera destacada la opinión de millones de usuarios.

El plugin permite integrar esta información en los navegadores mostrando la reputación de un sitio web como un icono de semáforo junto a los resultados de las búsquedas realizadas con Google, Yahoo!, Bing o cualquier otro motor de búsqueda.



Sitio: https://www.mywot.com/en/download

4.4 GHOSTERY

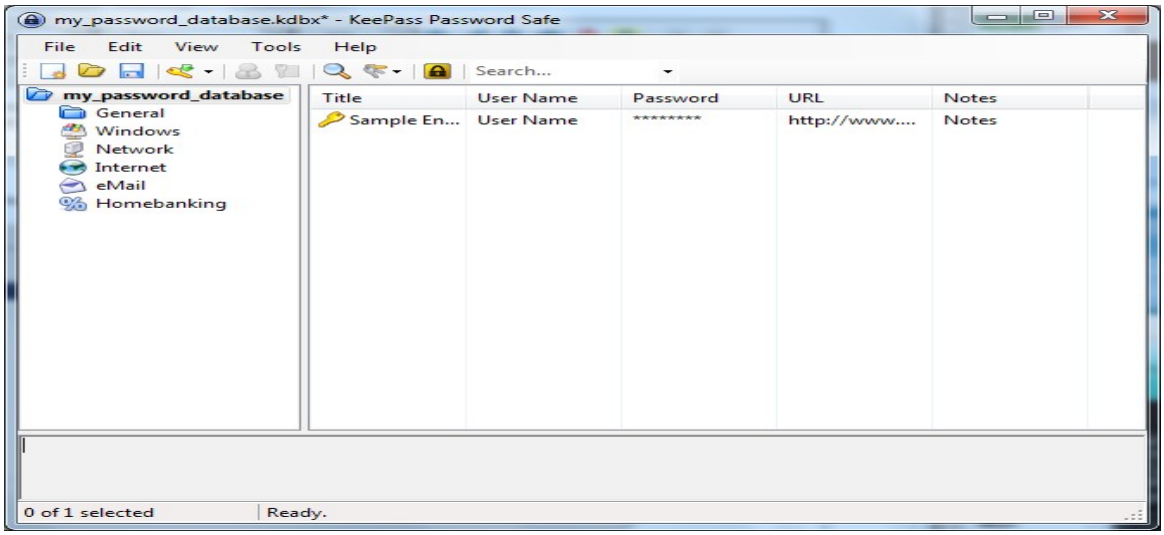
Ghostery permite bloquear scripts, imágenes, objetos y documentos insertados en marcos procedentes de empresas en las que no confíe. Esta extensión le permite detectar, rastreadores, balizas web, píxeles especiales e indicadores incluidos en páginas web por Facebook, Google y otros servicios, ofreciendo la posibilidad de evitar que se puedan recolectar tus datos de navegación. Hay empresas interesadas en la actividad de los usuarios como anunciantes, redes sociales, redes publicitarias, agencias de datos de comportamiento y editores de contenidos.

Sitio: https://www.ghostery.com/es/

5 GESTORES DE CONTRASEÑAS

5.1 KEEPASSX

KeePassX es un gestor de contraseñas libre y multiplataforma que permite guardar diversa información como nombres de usuario, contraseñas, direcciones web, archivos adjuntos, comentarios, etc, en una base de datos cifrada. Permite, además, generar contraseñas seguras automáticamente desde el mismo programa, facilitando de esta manera, la creación de nuevas credenciales.



Sitio: http://www.keepassx.org/

5.2 PASSWORD SAFE

Password Safe es un programa de código abierto para el almacenamiento de contraseñas en el sistema operativo Windows de forma segura, ya que utiliza un cifrado AES a 256 bits. De la misma manera que la aplicación anterior, los datos pueden ser organizados por categorías, ordenados y registrados.

Sitio:http://passwordsafe.sourceforge.net/

6 CIFRADO DE ARCHIVOS Y VOLÚMENES

6.1 AESCRYPT

AESCrypt es un software de cifrado de archivos libre disponible para distintas plataformas que utiliza AES (Advanced Encryption Standard) para cifrar archivos de manera segura, se integra de una manera simple en el sistema y permite su uso desde línea de comandos.

Descarga: http://www.aescrypt.com/

6.2 AXCRYPT

AxCrypt es un programa libre para Windows que se integra completamente en el sistemas para ofrecernos cifrado/descifrado seguro de ficheros.

Es un programa muy ligero, incrementa poco el tamaño del fichero cifrado, y está disponible desde el menú contextual (clic derecho), permitiendo incluso el descifrado del archivo aunque no se tenga el programa instalado. La última opción del menú contextual es el idioma, está en varios, entre ellos el español.

Descarga: http://www.axantum.com/AxCrypt/Downloads.html

7 COMPROBACIÓN DE INTEGRIDAD DE FICHEROS

En muchas ocasiones es necesario determinar si un fichero ha sido modificado, esto nos permite determinar, tanto para nuestros ficheros locales como los descargados de Internet, si se mantiene la integridad del mismo lo que podría ser indicativo de una posible modificación ilícita o de si el archivo ha podido ser dañado o no se ha descargado correctamente.

Para la comprobación de la integridad de un fichero habitualmente se usan funciones de resumen. Estas son algoritmos que consiguen crear a partir de una entrada (ya sea un texto, una contraseña o un archivo, por ejemplo) una salida alfanumérica de longitud normalmente fija que representa un resumen de toda la información que se le ha dado, por lo que cualquier modificación en la entrada, daría un valor de resumen totalmente distinta.

Los dos algoritmos de resumen (hash) que se usan habitualmente son MD5 y SHA256.

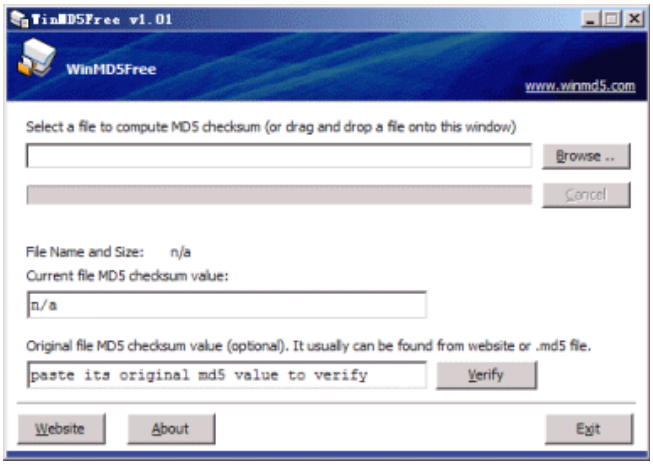
7.1 FILE CHECKSUM INTEGRITY VERIFIER (FCIV)

Herramienta gratuita disponible desde el sitio de soporte de Microsoft que, una vez ejecutada nos permite comprobar el hash tanto en MD5 como en SHA256

Sitio: http://support2.microsoft.com/kb/841290

7.2 WINMD5FREE

Una aplicación ligera, libre y gratuita que nos permite calcular de una manera rápida el MD5 de cualquier fichero que le indiquemos y que nos permite comprobar si coincide con cualquier otro valor que le indiquemos.



Sitio:http://www.winmd5.com/

8 COPIAS DE SEGURIDAD Y CLONADO DE DISCOS

8.1 CLONEZILLA

Clonezilla es un programa libre de particionado y clonado de discos que facilita el despliegue de sistemas, la realización de copias de seguridad y la recuperación frente a desastres. Existen dos tipos de versiones:

- **Clonezilla live:** Adecuado para la realización de copias de seguridad y restauración de sistemas individuales, permitiendo arrancar desde un CD o USB para la recuperación de particiones en caso de desastre.
- **Clonezilla SE (server edition):** Recomendado para despliegues de red masivos.

Descarga: http://clonezilla.org/downloads.php

9 CIFRADO DE CORREOS

GNU Privacy Guard (GnuPG o GPG) es una herramienta de cifrado y firmas digitales, que viene a ser un reemplazo del PGP (Pretty Good Privacy) pero con la principal diferencia que es software libre licenciado bajo la GPL. GPG utiliza el estándar del IETF denominado OpenPGP.

Aunque el programa tiene básicamente una interfaz textual, actualmente hay varias aplicaciones gráficas que integran GPG, como por ejemplo Kmail y Evolution o se proporciona un Plugin externo como es el caso de Mozilla y Thunderbird, lo que nos permite trabajar en Windows, GNU/Linux y otros sistemas operativos.

9.1 GPG/GPG4WIN

La implementación del programa para Windows se denomina GPG4WIN, este programa permite la integración GPG para este sistema operativo, se compone de los siguientes elementos:

- **GnuPG**: Núcleo de la herramienta de cifrado.
- **Kleopatra:** Gestor de certificados para OpenPGP y X.509 (S/MIME) y otros cifrados comunes.
- **GPA:** Un gestor de certificados alternativo para OpenPGP y X.509 (S/MIME).
- **GpgOL:** Plugin para el cifrado de correos para Microsoft Outlook 2003/2007/2010/2013.
- **GpgEX:** Plugin para Microsoft Explorer que provee cifrado de ficheros.
- **Claws Mail:** Aplicación de correo electrónico completa con soporte de cifrado.

Sitio:http://www.gpg4win.org/

9.2 ENIGMAIL (Mozilla/Thunderbird)

Enigmail es una extensión para Mozilla y Mozilla Thunderbird, lo que le permite funcionar tanto en sistemas Windows como de tipo Unix o GNU/Linux. Enigmail no es un motor criptográfico por sí mismo, sino que utiliza el GNU Privacy Guard (GnuPG o GPG) para realizar las operaciones de cifrado, integrándolo de una manera simple en el programa que usemos. Enigmail ofrece cifrado y descifrado automático de correos y una funcionalidad integrada de administración de las claves, lo que nos permitirá gestionar nuestras claves (creación, revocación, etc...) como las que obtengamos.

Sitio: https://www.enigmail.net/home/index.php

10 ELIMINACIÓN SEGURA DE LA INFORMACIÓN

La eliminación segura de datos no es tan fácil como se puede pensar. Cuando se elimina un archivo utilizando los comandos por defecto del sistema operativo la mayoría de estos sólo eliminan referencias al archivo, permaneciendo el contenido en el disco duro hasta que otro archivo es creado encima de él, e incluso después de ser sobreescrito puede ser posible recuperar datos usando ciertas técnicas forenses.

Mediante el uso de herramientas específicas, es relativamente sencillo recuperar archivos borrados de un disco duro, por ello que presentamos varias herramientas que realizan un borrado seguro de los datos mediante diferentes métodos.

10.1 SECURE-DELETE (LINUX)

Es una herramienta con una serie de programas especialmente útiles que utilizan técnicas avanzadas para eliminar definitivamente los archivos.

El paquete tiene diferentes comandos, dependiendo de nuestras necesidades:

- **srm (secure remove):** Eliminación segura de ficheros o directorios.
- **sdmem (secure memory wiper):** Eliminación segura de datos en la memoria RAM.
- **sfill (secure free space wiper):** Se usa para la limpieza del espacio libre en el disco.
- **sswap (secure swap wiper):** Permite eliminar de manera segura cualquier dato en la partición SWAP.

Sitio: http://sourceforge.net/projects/srm/

10.2 ERASER

Eraser es una herramienta avanzada de seguridad para Windows que le permite eliminar completamente los archivos de su disco duro, permite seleccionar varios niveles de seguridad para la eliminación de los datos siendo posible usar esta herramienta para borrar datos sensibles de discos duros, tarjetas de memoria, pendrives y, en general, cualquier dispositivo de almacenamiento de datos.

Sitio: http://eraser.heidi.ie/download.php

11 COMPROBACIÓN DE ACTUALIZACIONES DEL SISTEMA

Mantener el sistema actualizado nos protegerá de cualquier intento de explotación de vulnerabilidades conocidas para los distintos programas instalados. Sin embargo, en ocasiones, la gran cantidad de programas instalados y que muchos de ellos no comprueben la existencia de actualizaciones de manera automática hacen que esta tarea se vuelva ardua.

Los sistemas basados en Windows, al contrario que en otros sistemas operativos, carecen de un repositorio central de aplicaciones que les permita ser notificados y actualizar de una manera automática el software instalado.

Por estos motivos existen programas que se encargan de comprobar la existencia de nuevas versiones de los programas que tengamos instalados, con el objetivo de que mantengamos siempre nuestros sistemas actualizados a las últimas versiones.

11.1 SECUNIA-PSI

Secunia Personal Software Inspector (PSI) es una solución de seguridad gratuita que permite identificar en sistemas Windows vulnerabilidades en programas de terceros, esto es ajenos a Microsoft, que pueden dejar el PC vulnerable a ataques externos.

SecuniaPSI analiza el software instalado en el sistema e identifica los programas a los que es necesario aplicar actualizaciones de seguridad, permitiendo actualizarlos de una manera inmediata.

Sitio: http://secunia.com/vulnerability_scanning/personal/

11.2 FILEHIPPO UPDATE CHECKER

Filehippo Update Checker revisará el software instalado en tu ordenador, comprobará las versiones y después enviará esta información a FileHippo.com para ver si hay nuevas versiones. Éstas se muestran ordenadamente en tu navegador para que las descargues. Cuenta con la desventaja de que no todos los programas se encuentran soportados.

Sitio: http://www.filehippo.com/es/updatechecker/

12 PARTICIONADO

12.1 GPARTED

GParted es un editor de particiones para el entorno de escritorio GNOME. Esta aplicación es usada para crear, eliminar, redimensionar, inspeccionar y copiar particiones, como también los sistemas de archivos que se encuentran en ellas. Esto es útil para crear espacio para nuevos sistemas operativos, reorganizar el uso del disco y crear imágenes de un disco en una partición. Es posible arrancarlo desde un liveCD para la modificación de cualquier unidad de disco sin necesidad de instalar una distribución de Linux

Sitio: http://gparted.org/

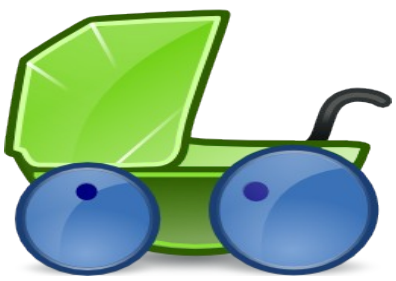
12.2 EASE PARTITION MASTER

EASEUS Partiton Master es una aplicación gratuita que nos permitirá gestionar y particionar nuestro disco duro, permite realizar distintas tareas con las particiones de un disco duro: Desde las operaciones más básicas como crear, eliminar y formatear las particiones en FAT32 y NTFS, hasta las operaciones más avanzadas como modificar el nombre y la letra, modificar el tamaño sin pérdida de información.

De la misma manera podremos reconfigurar nuestra tabla de particiones para crear nuevas particiones y guardar allí la información para, por ejemplo, formatear un equipo sin perder los datos o para instalar un nuevo sistema operativo sin eliminar el actual.

Sitio: http://www.easeus.com/partition-manager/epm-free.html

13 CONTROL PARENTAL



13.1 GNOME NANNY

Gnome Nanny es una aplicación de control parental que permite establecer ciertas restricciones en el sistema, como son el numero de horas que puede estar encendido el PC, los intervalos horarios de tiempo en los que se permite su uso, e incluso establecer filtros para la navegación por internet, el chat o el correo.

Sitio: https://wiki.gnome.org/Projects/Nanny

13.2 PARENTAL CONTROL BAR

Herramienta de control parental que se instala como barra en el navegador Internet Explorer, Mozilla Firefox y Safari (solo en Mac OS X). Cuando se instala la aplicación es necesario introducir una contraseña que servirá para la configuración de la aplicación así como una dirección de correo electrónico que serviría para la recuperación de la misma en caso de perdida.

Su funcionamiento se basa actualmente en listas blancas y negras, así mismo el programa incluye una serie de filtros predefinidos basados en material de carácter sexual, lenguaje explícito, violencia y otros criterios, siendo solamente necesario seleccionar el filtro adecuado.

Sitio: http://www.parentalcontrolbar.org/

14 SUITES DE APLICACIONES DE RECUPERACIÓN

En ocasiones, debido a problemas en el sistema, nos podemos encontrar con que nuestro equipo no arranque, por ejemplo porque el sector cero o MBR del Disco duro o de la unidad de estado sólido no está escrito correctamente, se ha perdido por algún problema físico, programa instalado o algún tipo de malware.

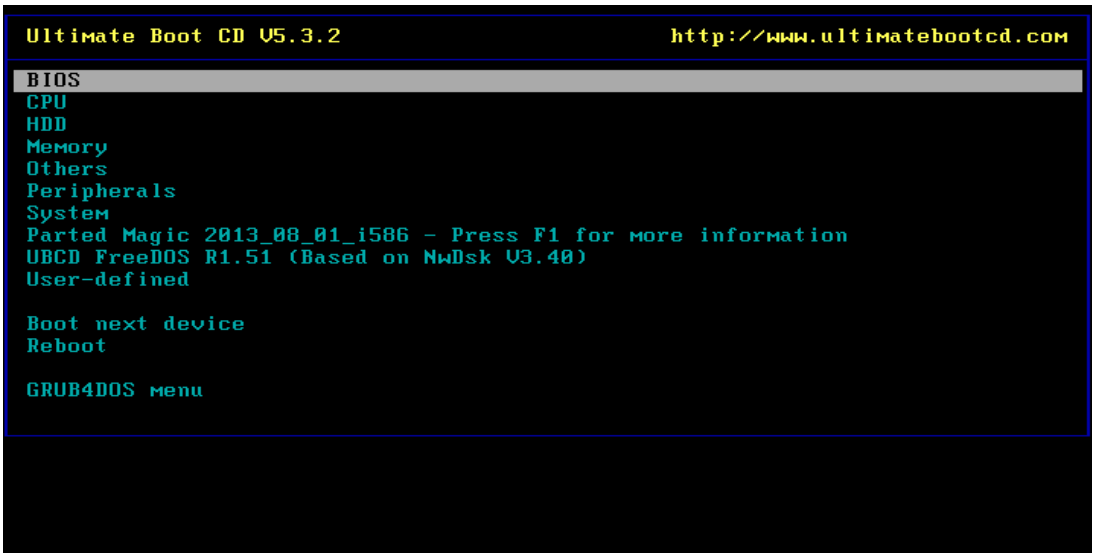
Para ayudarnos a solventar este y otros tipos de dificultades, se encuentran disponibles distintos sistemas de recuperación arrancables desde CD O USB que contienen software utilizado para reparar, restaurar y diagnosticar varios problemas informáticos.

14.1 ULTIMATE BOOT CD

Ultimate Boot CD es una recopilación de programas gratuitos bajo licencia GPL o Freeware que nos permite tener un conjunto de herramientas y utilidades con las que analizar y reparar ordenadores. Permite el arranque desde CD/DVD o USB en incluye una amplia selección de programas divididos por categorías.

Destacan las siguientes categorías:

- Utilidades para BIOS.
- Utilidades para CPU.
- Gestión del arranque del sistema.
- Recuperación de datos.
- Gestión e información de dispositivos.
- Herramientas de diagnostico de Discos Duros.
- Herramientas de clonación de Discos.
- Herramientas de edición de Discos.
- Borrado de Disco.
- Gestión de particiones.



Sitio: http://www.ultimatebootcd.com/

14.2 UBUNTU RESCUE REMIX

Basada en la popular distribución de Ubuntu, actualmente en la versión 12.04 ("Precise Pangolin"), nos provee de una amplia colección de utilidades de código abierto para la recuperación del sistema, de datos, así como de análisis forense. Su falta de interfaz gráfica, le permite trabajar incluso en sistemas con limitaciones de memoria y CPU.

Sitio: http://ubuntu-rescue-remix.org/

15 CONCLUSIONES

La oferta de herramientas que nos pueden ayudar a mejorar la seguridad de nuestro equipo es muy amplia, sobre todo si tenemos en cuenta además herramientas comerciales. Se ha querido en este documento, hacer una recopilación de las herramientas que pueden ser utilizadas para los distintos aspectos que un usuario medio pueda necesitar en su día a día relacionado con la seguridad general de su sistema.

Sin embargo, siempre hay que tener en cuenta, que la principal herramienta con la que dispone el usuario final es el sentido común y que al igual que en otros aspectos, cada usuario debe tomar la responsabilidad de velar porque sus sistemas sean seguros para evitar poder realizar acciones que puedan ver seriamente afectada la integridad, confidencialidad o disponibilidad de sus sistemas o de otros usuarios