# Informática y seguridad

## El tratamiento de la información y nuestro comportamiento

# Contenidos

## Artículos



## Referencias



## Licencias de artículos

# Automatización de información y ética

## Infoética

La **infoética** o la **ética de la información** es el campo que investiga los asuntos éticos que surgen del desarrollo y aplicación de las tecnologías informáticas. Da un marco crítico para consider los asuntos morales sobre la privacidad informacional, la agencia moral (por ejemplo, si los agentes artificiales pueden ser morales), nuevos asuntos medioambientales (especialmente como los agentes deberían comportarse en la infoesfera), problemas que surgen del ciclo vital (creación, colección, grabación, distribución, procedimiento, etc.) de información (especialmente la propiedad y copyright, la brecha digital). La infoética es relacionada con los campos de la ética informática[1] y la filosofía de la información.

Dilemas en cuanto a la vida de información son cada vez más importantes en una sociedad que se define como "la sociedad de información". La transmisión y el alfabetismo informáticos son asuntos esenciales en establecer una fundación ética que promueve las prácticas justas, equitables y responsables. En términos generales, la infoética examina los asuntos relacionados con la propiedad, el aceso, la privacidad, la seguridad y la comunidad.

La informática afecta a los derechos fundamentales que involucran la protección de copyright, la libertad intelectual, la contabilidad y la seguridad.

Existen códigos profesionales que ofrecen una base para tomar decisiones éticas y aplicar soluciones éticas a situaciones que involucran la provisión y uso de información que reflejan la dedicación de una organización al servicio informático responsable. La evolución de los formatos y necesidades informáticos requiere reconsideración continua de los principios éticos y como se aplican estos códigos. La consideraciones en cuanto a la infoética influencian "las decisiones personales, la práctica profesional y la política pública".[2] Por lo tanto, el análisis ético debe proveer una base para tomar en consideración "muchos y varios dominios" en cuanto a como se distribuye la información.

## Referencias


[1] Luciano Floridi (1999). "Information Ethics: On the Theoretical Foundations of Computer Ethics" (http://www.wolfson.ox.ac.uk/~floridi/pdf/ieotfce.pdf), *Ethics and Information Technology* 1.1, 37-56.

[2] E. Elrod and M. Smith (2005). "Information Ethics", in *Encyclopedia of Science, Technology, and Ethics*, ed. by Carl Mitcham. Vol. 2: D-K (1004-1011). Detroit: Macmillan Reference USA.

3. Rafael Capurro. **ETICA DE LA INFORMACION. Un intento de ubicación**. Traducción de un artículo en alemán publicado en la International Review of Information Ethics (1/2004). Esta traducción, hecha por el autor, fue publicada en la revista Códice : Revista de la Facultad de Sistemas de Información y Documentación. Universidad de la Salle (Bogotá, Colombia). Vol. 1, no. 2 (jul.-dic., 2005); p. 87-95 ISSN 1794-9815.

## Bibliografía


- Adam D. Moore ed (2005). "Information Ethics: Privacy, Property, and Power", University of Washington Press.
- Richard A. Spinello and Herman T. Tavani (eds.) (2004). *Readings in Cyberethics*, second ed. Mass.: Jones and Bartlett Publishers.
- Herman T. Tavani (2004). *Ethics & Technology: Ethical Issues in an Age of Information and Communication Technology*. New Jersey: John Wiley and Sons, Inc..


## Enlaces externos

- (http://research.microsoft.com/ero/icd/phd/2006SummerSchool/default.aspx#Ethics_in_research) Luciano Floridi, *What Is Information Ethics?*, *Microsoft Research Research Summer School 2006*. PPT (http://research.microsoft.com/ero/phd/2006SummerSchool/Luciano Floridi.ppt?0sr=a)
- (http://www.computersandsociety.org/sigcas_ofthefuture2/sigcas/subpage/sub_page.cfm?article=925&page_number_nb=1) Luciano Floridi, "Information Ethics, its Nature and Scope", *Computers & Society*, 34.5, 2005. en español (http://www.wolfson.ox.ac.uk/~floridi/pdf/edlisnya.pdf) en Isegoría (http://www.ifs.csic.es/Isegoria/isg.htm).
- (http://www.ub.es/bid/13froel2.htm) Thomas Froehlich, "A brief history of information ethics", *BiD: textos universitaris de biblioteconomia i documentació*, número. 13, 2004.
- (http://www.cpsr.org/) Computer Professionals for Social Responsibility
- (http://web.comlab.ox.ac.uk/oucl/research/areas/ieg/) IEG, the Information Ethics research Group en la Universidad de Oxford
- (http://www.infoethicist.blogspot.com) Information Ethicist
- (http://icie.zkm.de) International Center for Information Ethics
- (http://www.sir.arizona.edu/ier/) Information Ethics Roundtable
- (http://redeticainformacion.ning.com/) Red Latinoamericana de Ética de la Información

# Cómputo forense

El **cómputo forense**, también llamado **informática forense**, **computación forense**, **análisis forense digital** o **examinación forense digital** es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

Dichas técnicas incluyen reconstruir el bien informático, examinar datos residuales, autenticar datos y explicar las características técnicas del uso aplicado a los datos y bienes informáticos.

Como la definición anterior lo indica, esta disciplina hace uso no solo de tecnología de punta para poder mantener la integridad de los datos y del procesamiento de los mismos; sino que también requiere de una especialización y conocimientos avanzados en materia de informática y sistemas para poder detectar dentro de cualquier dispositivo electrónico lo que ha sucedido.

La importancia de éstos y el poder mantener su integridad se basa en que la evidencia digital o electrónica es sumamente frágil. El simple hecho de darle doble clic a un archivo modificaría la última fecha de acceso del mismo.

Adicionalmente, un examinador forense digital, dentro del proceso del cómputo forense puede llegar a recuperar información que haya sido borrada desde el sistema operativo.

## Dispositivos a analizar

La infraestructura informática que puede ser analizada puede ser toda aquella que tenga una Memoria (informática), por lo que se pueden analizar los siguientes dispositivos:

- Disco duro de una Computadora o Servidor
- Documentación referida del caso.
- Logs de seguridad.
- Credenciales de autentificación
- Trazo de paquetes de red.
- Teléfono Móvil o Celular, parte de la telefonía celular,
- Agendas Electrónicas (PDA)
- Dispositivos de GPS.
- Impresora
- Memoria USB

## Definiciones

- **Cadena de Custodia**:La identidad de personas que manejan la evidencia en el tiempo del suceso y la ultima revision del caso. Es responsabilidad de la persona que maneja la evidencia asegurar que los articulos son registrados y contabilizados durante el tiempo en el cual estan en su poder, y que son protegidos, llevando un registro de los nombres de las personas que manejaron la evidencia o articulos con el lapso de tiempo y fechas de entrega y recepción.
- **Imagen Forense**: Llamada también "Espejo" en ingles "Mirror", la cual es una copia bit a bit de un medio electronico de almacenamiento. En la imagen quedan grabados los espacios que ocupan los archivos, areas borradas incluyendo particiones escondidadas.
- **Analisis de Archivo**: Examina cada archivo digital descubierto y crea una base de datos de informacion relacionada al archivo (metadatos, etc..), consistente entre otras cosas en la firma del archivo o hash (indica la integridad del archivo), autor, tamaño, nombre y ruta, asi como su creacion, ultimo acceso y fecha de modificacion.

## Pasos del cómputo forense

El proceso de análisis forense a una computadora se describe a continuación:

### Identificación

Es muy importante conocer los antecedentes, situación actual y el proceso que se quiere seguir para poder tomar la mejor decisión con respecto a las búsquedas y la estrategia de investigación. Incluye muchas veces la identificación del bien informático, su uso dentro de la red, el inicio de la cadena de custodia (proceso que verifica la integridad y manejo adecuado de la evidencia), la revisión del entorno legal que protege el bien y del apoyo para la toma de decisión con respecto al siguiente paso una vez revisados los resultados.

### Preservación

Este paso incluye la revisión y generación de las imágenes forenses de la evidencia para poder realizar el análisis. Dicha duplicación se realiza utilizando tecnología de punta para poder mantener la integridad de la evidencia y la cadena de custodia que se requiere. Al realizar una imagen forense, nos referimos al proceso que se requiere para generar una copia “bit-a-bit” de todo el disco, el cual permitirá recuperar en el siguiente paso, toda la información contenida y borrada del disco duro. Para evitar la contaminación del disco duro, normalmente se ocupan bloqueadores de escritura de hardware, los cuales evitan el contacto de lectura con el disco, lo que provocaría una alteración no deseada en los medios.

### Análisis

Proceso de aplicar técnicas científicas y analíticas a los medios duplicados por medio del proceso forense para poder encontrar pruebas de ciertas conductas. Se pueden realizar búsquedas de cadenas de caracteres, acciones específicas del o de los usuarios de la máquina como son el uso de dispositivos de USB (marca, modelo), búsqueda de archivos específicos, recuperación e identificación de correos electrónicos, recuperación de los últimos sitios visitados, recuperación del caché del navegador de Internet, etc.

### Presentación

Es el recopilar toda la información que se obtuvo a partir del análisis para realizar el reporte y la presentación a los abogados, la generación (si es el caso) de una pericial y de su correcta interpretación sin hacer uso de tecnicismos.

## Herramientas de Cómputo Forense

- Sleuth Kit (Forensics Kit)
- Py-Flag (Forensics Browser)
- Autopsy (Forensics Browser for Sleuth Kit)
- dcfldd (DD Imaging Tool command line tool and also works with AIR)
- foremost (Data Carver command line tool)
- Air (Forensics Imaging GUI)
- md5deep (MD5 Hashing Program)
- netcat (Command Line)
- cryptcat (Command Line)
- NTFS-Tools
- qtparted (GUI Partitioning Tool)
- regviewer (Windows Registry)
- Viewer
- X-Ways WinTrace

- X-Ways WinHex
- X-Ways Forensics
- R-Studio Emergency (Bootable Recovery media Maker)
- R-Studio Network Edtion
- R-Studio RS Agent
- Net resident
- Faces
- Encase
- Snort
- Helix

## Herramientas para el análisis de discos duros

- AccessData Forensic ToolKit (FTK)
- Guidance Software EnCase

## Herramientas para el análisis de correos electrónicos

- Paraben

## Herramientas para el análisis de redes

E-Detective - Decision Computer Group SilentRunner - Accessdata

Herramientas para filtrar y monitorear el trafico de una red tanto interna como a internet.

## Herramientas para el análisis de USB

- USBDeview

## Notas

Es muy importante mencionar que la informática forense o cómputo forense no tiene parte preventiva, es decir, la informática forense no se encarga de prevenir delitos, para ello que encarga la seguridad informática, es importante tener claro el marco de actuación entre la informática forense, la seguridad informática y la auditoría informática.

## Enlaces externos

- Reto Forense RedIRIS (España) y UNAM-CERT (México) (http://www.seguridad.unam.mx/eventos/reto/)
- Laboratorio de informatica forense en España (http://www.informaticosforenses.es)
- El mundo de la Informática Forense I (http://www.xombra.com/go_news.php?articulo=1942)
- El mundo de la Informática Forense II (http://www.xombra.com/go_articulo.php?articulo=60)

# Amenazas digitales vs. métodos de proteccion

## Delito informático

El **delito informático**, o crimen electrónico, es el término genérico para aquellas operaciones ilícitas realizadas por medio de Internet o que tienen como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet. Sin embargo, las categorías que definen un delito informático son aún mayores y complejas y pueden incluir delitos tradicionales como el fraude, el robo, chantaje, falsificación y la malversación de caudales públicos en los cuales ordenadores y redes han sido utilizados. Con el desarrollo de la programación y de Internet, los delitos informáticos se han vuelto más frecuentes y sofisticados.

Existen actividades delictivas que se realizan por medio de estructuras electrónicas que van ligadas a un sin número de herramientas delictivas que buscan infringir y dañar todo lo que encuentren en el ámbito informático: ingreso ilegal a sistemas, interceptado ilegal de redes, interferencias, daños en la información (borrado, dañado, alteración o supresión de datacredito), mal uso de artefactos, chantajes, fraude electrónico, ataques a sistemas, robo de bancos, ataques realizados por hackers, violación de los derechos de autor, pornografía infantil, pedofilia en Internet, violación de información confidencial y muchos otros.

### Generalidades

El delito informático incluye una amplia variedad de categorías de crímenes. Generalmente este puede ser dividido en dos grupos:

1. Crímenes que tienen como objetivo redes de computadoras, por ejemplo, con la instalación de códigos, gusanos y archivos maliciosos, Spam, ataque masivos a servidores de Internet y generación de virus.
2. Crímenes realizados por medio de ordenadores y de Internet, por ejemplo, espionaje, fraude y robo, pornografía infantil, pedofilia, etc.

Un ejemplo común es cuando una persona comienza a robar información de websites o causa daños a redes o servidores. Estas actividades pueden ser absolutamente virtuales, porque la información se encuentra en forma digital y el daño aunque real no tiene consecuencias físicas distintas a los daños causados sobre los ordenadores o servidores. En algunos sistemas judiciales la propiedad intangible no puede ser robada y el daño debe ser visible. Un ordenador puede ser fuente de pruebas y, aunque el ordenador no haya sido directamente utilizado para cometer el crimen, es un excelente artefacto que guarda los registros, especialmente en su posibilidad de codificar los datos. Esto ha hecho que los datos codificados de un ordenador o servidor tengan el valor absoluto de prueba ante cualquier corte del mundo.

Los diferentes países suelen tener policía especializada en la investigación de estos complejos delitos que al ser cometidos a través de internet, en un gran porcentaje de casos excede las fronteras de un único país complicando su esclarecimiento viéndose dificultado por la diferente legislación de cada país o simplemente la inexistencia de ésta.

# Crímenes específicos

## Spam

El Spam o los correos electrónicos, no solicitados para propósito comercial, es ilegal en diferentes grados. La regulación de la ley en cuanto al Spam en el mundo es relativamente nueva y por lo general impone normas que permiten la legalidad del Spam en diferentes niveles. El Spam legal debe cumplir estrictamente con ciertos requisitos como permitir que el usuario pueda escoger el no recibir dicho mensaje publicitario o ser retirado de listas de email.

## Fraude

El fraude informático es inducir a otro a hacer o a restringirse en hacer alguna cosa de lo cual el criminal obtendrá un beneficio por lo siguiente:

1. Alterar el ingreso de datos de manera ilegal. Esto requiere que el criminal posea un alto nivel de técnica y por lo mismo es común en empleados de una empresa que conocen bien las redes de información de la misma y pueden ingresar a ella para alterar datos como generar información falsa que los beneficie, crear instrucciones y procesos no autorizados o dañar los sistemas.
2. Alterar, destruir, suprimir o robar datos, un evento que puede ser difícil de detectar.
3. Alterar o borrar archivos.
4. Alterar o dar un mal uso a sistemas o software, alterar o reescribir códigos con propósitos fraudulentos. Estos eventos requieren de un alto nivel de conocimiento.

Otras formas de fraude informático incluye la utilización de sistemas de computadoras para robar bancos, realizar extorsiones o robar información clasificada.

## Contenido obsceno u ofensivo

El contenido de un website o de otro medio de comunicación puede ser obsceno u ofensivo por una gran gama de razones. En ciertos casos dicho contenido puede ser ilegal. Igualmente, no existe una normativa legal universal y la regulación judicial puede variar de país a país, aunque existen ciertos elementos comunes. Sin embargo, en muchas ocasiones, los tribunales terminan siendo árbitros cuando algunos grupos se enfrentan a causa de contenidos que en un país no tienen problemas judiciales, pero sí en otros. Un contenido puede ser ofensivo u obsceno, pero no necesariamente por ello es ilegal.

Algunas jurisdicciones limitan ciertos discursos y prohíben explícitamente el racismo, la subversión política, la promoción de la violencia, los sediciosos y el material que incite al odio y al crimen.

## Hostigamiento / Acoso

El hostigamiento o acoso es un contenido que se dirige de manera específica a un individuo o grupo con comentarios derogativos a causa de su sexo, raza, religión, nacionalidad, orientación sexual, etc. Esto ocurre por lo general en canales de conversación, grupos o con el envío de correos electrónicos destinados en exclusiva a ofender. Todo comentario que sea derogatorio u ofensivo es considerado como hostigamiento o acoso.

## Tráfico de drogas

El narcotráfico se ha beneficiado especialmente de los avances del Internet y a través de éste promocionan y venden drogas ilegales a través de emails codificados y otros instrumentos tecnológicos. Muchos narcotraficantes organizan citas en cafés Internet. Como el Internet facilita la comunicación de manera que la gente no se ve las caras, las mafias han ganado también su espacio en el mismo, haciendo que los posibles clientes se sientan más seguros con este tipo de contacto. Además, el Internet posee toda la información alternativa sobre cada droga, lo que hace que el cliente busque por sí mismo la información antes de cada compra.

### Terrorismo virtual

Desde 2001 el terrorismo virtual se ha convertido en uno de los novedosos delitos de los criminales informáticos los cuales deciden atacar masivamente el sistema de ordenadores de una empresa, compañía, centro de estudios, oficinas oficiales, etc. Un ejemplo de ello lo ofrece un hacker de Nueva Zelandia, Owen Thor Walker (AKILL), quien en compañía de otros hackers, dirigió un ataque en contra del sistema de ordenadores de la Universidad de Pennsylvania en 2008.

La difusión de noticias falsas en Internet (por ejemplo decir que va a explotar una bomba en el Metro), es considerado terrorismo informático y es procesable.-

## Sujetos activos y pasivos

Muchas de las personas que cometen los delitos informáticos poseen ciertas características específicas tales como la habilidad para el manejo de los sistemas informáticos o la realización de tareas laborales que le facilitan el acceso a información de carácter sensible.

En algunos casos la motivación del delito informático no es económica sino que se relaciona con el deseo de ejercitar, y a veces hacer conocer a otras personas, los conocimientos o habilidades del delincuente en ese campo.

Muchos de los "delitos informáticos" encuadran dentro del concepto de "delitos de cuello blanco", término introducido por primera vez por el criminólogo estadounidense Edwin Sutherland en 1943. Esta categoría requiere que: (1) el sujeto activo del delito sea una persona de cierto estatus socioeconómico; (2) su comisión no pueda explicarse por falta de medios económicos, carencia de recreación, poca educación, poca inteligencia, ni por inestabilidad emocional.

El sujeto pasivo en el caso de los delitos informáticos puede ser individuos, instituciones crediticias, órganos estatales, etc. que utilicen sistemas automatizados de información, generalmente conectados a otros equipos o sistemas externos.

Para la labor de prevención de estos delitos es importante el aporte de los demanificados que puede ayudar en la determinación del *modus operandi*, esto es de las maniobras usadas por los delincuentes informáticos.

## Regulación por países

### Argentina

#### La ley vigente

La Argentina sancionó el 4 de junio del 2008 la Ley 26.388 (promulgada de hecho el 24 de junio de 2008) que modifica el Código Penal a fin de incorporar al mismo diversos delitos informáticos, tales como la distribución y tenencia con fines de distribución de pornografía infantil, violación de correo electrónico, acceso ilegítimo a sistemas informáticos, daño informático y distribución de virus, daño informático agravado e interrupción de comunicaciones.

#### Definiciones vinculadas a la informática

En el nuevo ordenamiento se establece que el término "documento" comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión (art. 77 Código Penal).

Los términos "firma" y "suscripción" comprenden la firma digital, la creación de una firma digital o firmar digitalmente (art. 77 Código Penal).

Los términos "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente (art. 77 Código Penal).

**Delitos contra menores**

En el nuevo ordenamiento pasan a ser considerados delitos los siguientes hechos vinculados a la informática:

- Artículo 128: Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.

Será reprimido con prisión de cuatro (4) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización.

Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años.

**Protección de la privacidad**

- Artículo 153: Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.

En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.

La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica.

Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena.

- Artículo 153 bis: Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.

La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.

- Artículo 155: Será reprimido con multa de pesos un mil quinientos ($ 1.500) a pesos cien mil ($ 100.000), el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros.

Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público.

- Artículo 157: Será reprimido con prisión de un (1) mes a dos (2) años e inhabilitación especial de un (1) a cuatro (4) años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos.
- Artículo 157 bis: Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que:

1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;

2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.

3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años.

**Delitos contra la propiedad**

- Artículo 173 inciso 16: (Incurre en el delito de defraudación)...El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.
- Artículo 183 del Código Penal: (Incurre en el delito de daño)...En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.
- Artículo 184 del Código Penal: (Eleva la pena a tres (3) meses a cuatro (4) años de prisión, si mediare cualquiera de las circunstancias siguientes):

Inciso 5: Ejecutarlo en archivos, registros, bibliotecas, museos o en puentes, caminos, paseos u otros bienes de uso público; o en tumbas, signos conmemorativos, monumentos, estatuas, cuadros u otros objetos de arte colocados en edificios o lugares públicos; o en datos, documentos, programas o sistemas informáticos públicos;

Inciso 6: Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público.

**Delitos contra las comunicaciones**

Artículo 197: Será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida.

**Delitos contra la administración de justicia**

Artículo 255: Será reprimido con prisión de un (1) mes a cuatro (4) años, el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo.

Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de pesos setecientos cincuenta ($ 750) a pesos doce mil quinientos ($ 12.500).

## Colombia

En Colombia el 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “De la Protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evita incurrir en alguno de estos tipos penales.

No hay que olvidar que los avances tecnológicos y el empleo de los mismos para apropiarse ilícitamente del patrimonio de terceros a través de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos, entre otras, son conductas cada vez más usuales en todas partes del mundo. Según estadisticas, durante el 2007 en Colombia las empresas perdieron más de 6.6 billones de pesos a raíz de delitos informáticos.

De ahí la importancia de esta ley, que adiciona al Código Penal colombiano el Título VII BIS denominado "De la Protección de la información y de los datos" que divide en dos capítulos, a saber: “De los atentados contra la

confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos" y "De los atentados informáticos y otras infracciones".

En Colombia existen instituciones de educación como UNICOLOMBIA que promueven capacitaciones en temas relacionados con Delitos Informáticos, el mejor manejo y uso de la prueba digital, establecer altos estándares científicos y éticos para Informáticos Forenses, Llevar a cabo investigación y desarrollo de nuevas tecnologías y los métodos de la ciencia del análisis forense digital e Instruir a los estudiantes en diversos campos específicos sobre nuevas tecnologías aplicadas a la informática Forense, la investigación científica y el proceso tecnológico de las mismas.

## España

En España, los delitos informáticos son un hecho sancionable por el Código Penal en el que el delincuente utiliza, para su comisión, cualquier medio informático. Estas sanciones se recogen en la Ley Orgánica 10/1995, de 23 de Noviembre en el BOE número 281, de 24 de Noviembre de 1.995. Estos tienen la misma sanción que sus homólogos no-informáticos. Por ejemplo, se aplica la misma sanción para una intromisión en el correo electrónico que para una intromisión en el correo postal.

El Tribunal Supremo emitió una sentencia el 12 de junio de 2007 (recurso Nº 2249/2006; resolución Nº 533/2007) que confirmó las penas de prisión para un caso de estafa electrónica (phishing).

## México

En México los delitos de revelación de secretos y acceso ilícito a sistemas y equipos de informática ya sean que estén protegidos por algún mecanismo de seguridad, se consideren propiedad del Estado o de las instituciones que integran el sistema financiero son hechos sancionables por el Código Penal Federal en el titulo noveno capítulo I y II.

El artículo 167 fr.VI del Código Penal Federal sanciona con prisión y multa al que intencionalmente o con fines de lucro, interrumpa o interfiera comunicaciones alámbricas, inalámbricas o de fibra óptica, sean telegráficas, telefónicas o satelitales, por medio de las cuales se transmitan señales de audio, de video o de datos.

La reproducción no autorizada de programas informáticos o piratería esta regulada en la Ley Federal del Derecho de Autor en el Título IV, capítulo IV.

También existen leyes locales en el código penal del Distrito Federal y el código penal del estado de Sinaloa.

## Venezuela

Concibe como bien jurídico la protección de los sistemas informáticos que contienen, procesan, resguardan y transmiten la información. Están contemplados en la Ley Especial contra los Delitos Informáticos, de 30 de octubre de 2001.

La ley tipifica cinco clases de delitos:

- Contra los sistemas que utilizan tecnologías de información: acceso indebido (Art.6); sabotaje o daño a sistemas (Art.7); favorecimiento culposos del sabotaje o daño. (Art. 8); acceso indebido o sabotaje a sistemas protegidos (Art. 9); posesión de equipos o prestación de servicios de sabotaje (Art. 10); espionaje informático (Art. 11); falsificación de documentos (Art. 12).
- Contra la propiedad: hurto (Art. 13); fraude (Art. 14); obtención indebida de bienes o servicios (Art. 15); manejo fraudulento de tarjetas inteligentes o instrumentos análogos (Art. 16); apropiación de tarjetas inteligentes o instrumentos análogos (Art. 17); provisión indebida de bienes o servicios (Art. 18); posesión de equipo para falsificaciones (Art. 19);
- Contra la privacidad de las personas y de las comunicaciones: violación de la privacidad de la data o información de carácter personal (Art. 20); violación de la privacidad de las comunicaciones (Art. 21); revelación indebida de

data o información de carácter personal (Art. 22);
- Contra niños y adolescentes: difusión o exhibición de material pornográfico (Art. 23); exhibición pornográfica de niños o adolescentes (Art. 24);
- Contra el orden económico: apropiación de propiedad intelectual (Art. 25); oferta engañosa (Art. 26).

### Estados Unidos

Este país adoptó en 1994 el Acta Federal de Abuso Computacional que modificó al Acta de Fraude y Abuso Computacional de 1986.

En el mes de Julio del año 2000, el Senado y la Cámara de Representantes de este país -tras un año largo de deliberaciones- establece el Acta de Firmas Electrónicas en el Comercio Global y Nacional. La ley sobre la firma digital responde a la necesidad de dar validez a documentos informáticos -mensajes electrónicos y contratos establecidos mediante Internet- entre empresas (para el B2B) y entre empresas y consumidores (para el B2C).

## Enlaces externos

- Introducción a los delitos informáticos, tipos y legislación [1]

Legislación

- Modificación al Código Penal sobre la incorporación de los Delitos Informáticos [2] (Argentina)
- Delitos Informáticos [3] (Chile)
- Legislación vigente en España [4] (España)
- Ley Especial de Delitos Informáticos [5] (Venezuela)

## Referencias

[1] http://www.delitosinformaticos.com/delitos/delitosinformaticos.shtml
[2] http://infoleg.mecon.gov.ar/infolegInternet/anexos/140000-144999/141790/norma.htm
[3] http://www2.udec.cl/contraloria/docs/materias/delitosinformaticos.pdf
[4] http://delitosinformaticos.com/legislacion/espana.shtml
[5] http://www.tsj.gov.ve/legislacion/ledi.htm

# Seguridad informática

La **seguridad informática** es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo la información contenida). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pudiendo encontrar información en diferentes medios o formas.

## Objetivos de la seguridad informática

La seguridad informática está concebida para proteger los activos informáticos, entre los que se encuentran:

La información contenida

> Se ha convertido en uno de los elementos más importantes dentro de una organización. La seguridad informática debe ser administrada según los criterios establecidos por los administradores y supervisores, evitando que usuarios externos y no autorizados puedan acceder a ella sin autorización. De lo contrario la organización corre el riesgo de que la información sea utilizada maliciosamente para obtener ventajas de ella o que sea manipulada, ocasionando lecturas erradas o incompletas de la misma. Otra función de la seguridad informática en esta área es la de asegurar el acceso a la información en el momento oportuno, incluyendo respaldos de la misma en caso de que esta sufra daños o pérdida producto de accidentes, atentados o desastres.

La infraestructura computacional

> Una parte fundamental para el almacenamiento y gestión de la información, así como para el funcionamiento mismo de la organización. La función de la seguridad informática en esta área es velar que los equipos funcionen adecuadamente y prever en caso de falla planes de robos, incendios, boicot, desastres naturales, fallas en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática.

Los usuarios

> Son las personas que utilizan la estructura tecnológica, zona de comunicaciones y que gestionan la información. La seguridad informática debe establecer normas que minimicen los riesgos a la información o infraestructura informática. Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática minimizando el impacto en el desempeño de los funcionarios y de la organización en general y como principal contribuyente al uso de programas realizados por programadores.

## Las amenazas

Una vez que la programación y el funcionamiento de un dispositivo de almacenamiento (o transmisión) de la información se consideran seguras, todavía deben ser tenidos en cuenta las circunstancias "no informáticas" que pueden afectar a los datos, las cuales son a menudo imprevisibles o inevitables, de modo que la única protección posible es la redundancia (en el caso de los datos) y la descentralización -por ejemplo mediante estructura de redes- (en el caso de las comunicaciones).

Estos fenómenos pueden ser causados por:

- El usuario: causa del mayor problema ligado a la seguridad de un sistema informático (porque no le importa, no se da cuenta o a propósito).
- Programas maliciosos: programas destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema. Es instalado (por inatención o maldad) en el ordenador abriendo una puerta a intrusos o bien modificando los datos. Estos programas pueden ser un virus informático, un gusano informático, un troyano, una bomba lógica o un programa espía o Spyware.
- Un intruso: persona que consigue acceder a los datos o programas de los cuales no tiene acceso permitido (cracker, defacer, script kiddie o *Script boy, viruxer, etc.).*
- Un siniestro (robo, incendio, inundación): una mala manipulación o una malintención derivan a la pérdida del material o de los archivos.
- El personal interno de Sistemas. Las pujas de poder que llevan a disociaciones entre los sectores y soluciones incompatibles para la seguridad informática.

## Tipos de amenaza

El hecho de conectar una red a un entorno externo nos da la posibilidad de que algún atacante pueda entrar en ella, con esto, se puede hacer robo de información o alterar el funcionamiento de la red. Sin embargo el hecho de que la red no sea conectada a un entorno externo no nos garantiza la seguridad de la misma. De acuerdo con el Computer Security Institute (CSI) de San Francisco aproximadamente entre 60 y 80 por ciento de los incidentes de red son causados desde adentro de la misma. Basado en esto podemos decir que existen 2 tipos de amenazas:

- Amenazas internas: Generalmente estas amenazas pueden ser más serias que las externas por varias razones como son:

-Los usuarios conocen la red y saben cómo es su funcionamiento.

-Tienen algún nivel de acceso a la red por las mismas necesidades de su trabajo.

-Los IPS y Firewalls son mecanismos no efectivos en amenazas internas.

**Esta situación se presenta gracias a los esquemas ineficientes de seguridad con los que cuentan la mayoría de las compañías a nivel mundial, y porque no existe conocimiento relacionado con la planeación de un esquema de seguridad eficiente que proteja los recursos informáticos de las actuales amenazas combinadas.**

El resultado es la violación de los sistemas, provocando la pérdida o modificación de los datos sensibles de la organización, lo que puede representar un daño con valor de miles o millones de dólares.

- Amenazas externas: Son aquellas amenazas que se originan fuera de la red. Al no tener información certera de la red, un atacante tiene que realizar ciertos pasos para poder conocer qué es lo que hay en ella y buscar la manera de atacarla. La ventaja que se tiene en este caso es que el administrador de la red puede prevenir una buena parte de los ataques externos.

## La amenaza informática del futuro

Si en un momento el objetivo de los ataques fue cambiar las plataformas tecnológicas ahora las tendencias cibercriminales indican que la nueva modalidad es manipular los significados de la información digital. El área semántica, era reservada para los humanos, se convirtió ahora en el núcleo de los ataques debido a la evolución de la Web 2.0 y las redes sociales, factores que llevaron al nacimiento de la generación 3.0.

- Se puede afirmar que "la Web 3.0 otorga contenidos y significados de manera tal que pueden ser comprendidos por las computadoras, las cuales -por medio de técnicas de inteligencia artificial- son capaces de emular y mejorar la obtención de conocimiento, hasta el momento reservada a las personas".
- Es decir, se trata de dotar de significado a las páginas Web, y de ahí el nombre de Web semántica o Sociedad del Conocimiento, como evolución de la ya pasada Sociedad de la Información

En este sentido, las amenazas informáticas que viene en el futuro ya no son con la inclusión de troyanos en los sistemas o softwares espías, sino con el hecho de que los ataques se han profesionalizado y manipulan el significado del contenido virtual.

- “La Web 3.0, basada en conceptos como elaborar, compartir y significar, está representando un desafío para los hackers que ya no utilizan las plataformas convencionales de ataque, sino que optan por modificar los significados del contenido digital, provocando así la confusión lógica del usuario y permitiendo de este modo la intrusión en los sistemas”, La amenaza ya no solicita la clave de homebanking del desprevenido usuario, sino que directamente modifica el balance de la cuenta, asustando al internauta y, a partir de allí, sí efectuar el robo del capital”.

Para no ser presa de esta nueva ola de ataques más sutiles, Se recomienda:

- Mantener las soluciones activadas y actualizadas.
- Evitar realizar operaciones comerciales en computadoras de uso público.
- Verificar los archivos adjuntos de mensajes sospechosos y evitar su descarga en caso de duda.

## Tipos de Virus

Los virus se pueden clasificar de la siguiente forma:

### Virus residentes

La característica principal de estos virus es que se ocultan en la memoria RAM de forma permanente o residente. De este modo, pueden controlar e interceptar todas las operaciones llevadas a cabo por el sistema operativo, infectando todos aquellos ficheros y/o programas que sean ejecutados, abiertos, cerrados, renombrados, copiados. Algunos ejemplos de este tipo de virus son: Randex, CMJ, Meve, MrKlunky.

### Virus de acción directa

Al contrario que los residentes, estos virus no permanecen en memoria. Por tanto, su objetivo prioritario es reproducirse y actuar en el mismo momento de ser ejecutados. Al cumplirse una determinada condición, se activan y buscan los ficheros ubicados dentro de su mismo directorio para contagiarlos.

### Virus de sobreescritura

Estos virus se caracterizan por destruir la información contenida en los ficheros que infectan. Cuando infectan un fichero, escriben dentro de su contenido, haciendo que queden total o parcialmente inservibles.

### Virus de boot(bot_kill) o de arranque

Los términos boot o sector de arranque hacen referencia a una sección muy importante de un disco (tanto un disquete como un disco duro respectivamente). En ella se guarda la información esencial sobre las características del disco y se encuentra un programa que permite arrancar el ordenador. Este tipo de virus no infecta ficheros, sino los discos que los contienen. Actúan infectando en primer lugar el sector de arranque de los disquetes. Cuando un ordenador se pone en marcha con un disquete infectado, el virus de boot infectará a su vez el disco duro.

Los virus de boot no pueden afectar al ordenador mientras no se intente poner en marcha a éste último con un disco infectado. Por tanto, el mejor modo de defenderse contra ellos es proteger los disquetes contra escritura y no arrancar nunca el ordenador con un disquete desconocido en la disquetera.

Algunos ejemplos de este tipo de virus son: Polyboot.B, AntiEXE.

### Virus de enlace o directorio

Los ficheros se ubican en determinadas direcciones (compuestas básicamente por unidad de disco y directorio), que el sistema operativo conoce para poder localizarlos y trabajar con ellos.

### Virus cifrados

Más que un tipo de virus, se trata de una técnica utilizada por algunos de ellos, que a su vez pueden pertenecer a otras clasificaciones. Estos virus se cifran a sí mismos para no ser detectados por los programas antivirus. Para realizar sus actividades, el virus se descifra a sí mismo y, cuando ha finalizado, se vuelve a cifrar.

### Virus polimórficos

Son virus que en cada infección que realizan se cifran de una forma distinta (utilizando diferentes algoritmos y claves de cifrado). De esta forma, generan una elevada cantidad de copias de sí mismos e impiden que los antivirus los localicen a través de la búsqueda de cadenas o firmas, por lo que suelen ser los virus más costosos de detectar.

### Virus multipartites

Virus muy avanzados, que pueden realizar múltiples infecciones, combinando diferentes técnicas para ello. Su objetivo es cualquier elemento que pueda ser infectado: archivos, programas, macros, discos, etc.

### Virus del Fichero

Infectan programas o ficheros ejecutables (ficheros con extensiones EXE y COM). Al ejecutarse el programa infectado, el virus se activa, produciendo diferentes efectos.

### Virus de FAT

La Tabla de Asignación de Ficheros o FAT es la sección de un disco utilizada para enlazar la información contenida en éste. Se trata de un elemento fundamental en el sistema. Los virus que atacan a este elemento son especialmente peligrosos, ya que impedirán el acceso a ciertas partes del disco, donde se almacenan los ficheros críticos para el normal funcionamiento del ordenador.

## Análisis de riesgos

**Véase también: Análisis de riesgo informático**

El activo más importante que se posee es la información y, por lo tanto, deben existir técnicas que la aseguren, más allá de la seguridad física que se establezca sobre los equipos en los cuales se almacena. Estas técnicas las brinda la seguridad lógica que consiste en la aplicación de *barreras y procedimientos* que resguardan el acceso a los datos y sólo permiten acceder a ellos a las personas autorizadas para hacerlo.

Existe un viejo dicho en la seguridad informática que dicta: *"lo que no está permitido debe estar prohibido"* y ésta debe ser la meta perseguida.

Los medios para conseguirlo son:

1. Restringir el acceso (de personas de la organización y de las que no lo son) a los programas y archivos.
2. Asegurar que los operadores puedan trabajar pero que no puedan modificar los programas ni los archivos que no correspondan (sin una supervisión minuciosa).
3. Asegurar que se utilicen los datos, archivos y programas correctos en/y/por el procedimiento elegido.
4. Asegurar que la información transmitida sea la misma que reciba el destinatario al cual se ha enviado y que no le llegue a otro.
5. Asegurar que existan sistemas y pasos de emergencia alternativos de transmisión entre diferentes puntos.

6. Organizar a cada uno de los empleados por jerarquía informática, con claves distintas y permisos bien establecidos, en todos y cada uno de los sistemas o aplicaciones empleadas.
7. Actualizar constantemente las contraseñas de accesos a los sistemas de cómputo.

### Elementos de un análisis de riesgo

Cuando se pretende diseñar una técnica para implementar un análisis de riesgo informático se pueden tomar los siguientes puntos como referencia a seguir:

- Planes para reducir los riesgos.

## Análisis de impacto al negocio

El reto es asignar estratégicamente los recursos para equipo de seguridad y bienes que intervengan, basándose en el impacto potencial para el negocio, respecto a los diversos incidentes que se deben resolver. Para determinar el establecimiento de prioridades, el sistema de gestión de incidentes necesita saber el valor de los sistemas de información que pueden ser potencialmente afectados por incidentes de seguridad. Esto puede implicar que alguien dentro de la organización asigne un valor monetario a cada equipo y un archivo en la red o asignar un valor relativo a cada sistema y la información sobre ella. Dentro de los Valores para el sistema se pueden distinguir: Confidencialidad de la información, la Integridad (aplicaciones e información) y finalmente la Disponibilidad del sistema. Cada uno de estos valores es un sistema independiente del negocio, supongamos el siguiente ejemplo, un servidor Web público pueden poseer los requisitos de confidencialidad de baja (ya que toda la información es pública),pero de alta disponibilidad y los requisitos de integridad. En contraste, un sistema de planificación de recursos empresariales (ERP), sistema puede poseer alto puntaje en los tres variables. Los incidentes individuales pueden variar ampliamente en términos de alcance e importancia.

## Puesta en marcha de una política de seguridad

Actualmente las legislaciones nacionales de los Estados, obligan a las empresas, instituciones públicas a implantar una política de seguridad. Ej: En España la Ley Orgánica de Protección de Datos o también llamada LOPD y su normativa de desarrollo.

Generalmente se ocupa exclusivamente a asegurar los derechos de acceso a los datos y recursos con las herramientas de control y mecanismos de identificación. Estos mecanismos permiten saber que los operadores tienen sólo los permisos que se les dio.

La seguridad informática debe ser estudiada para que no impida el trabajo de los operadores en lo que les es necesario y que puedan utilizar el sistema informático con toda confianza. Por eso en lo referente a elaborar una política de seguridad, conviene:

- Elaborar reglas y procedimientos para cada servicio de la organización.
- Definir las acciones a emprender y elegir las personas a contactar en caso de detectar una posible intrusión
- Sensibilizar a los operadores con los problemas ligados con la seguridad de los sistemas informáticos.

Los derechos de acceso de los operadores deben ser definidos por los responsables jerárquicos y no por los administradores informáticos, los cuales tienen que conseguir que los recursos y derechos de acceso sean coherentes con la política de seguridad definida. Además, como el administrador suele ser el único en conocer perfectamente el sistema, tiene que derivar a la directiva cualquier problema e información relevante sobre la seguridad, y eventualmente aconsejar estrategias a poner en marcha, así como ser el punto de entrada de la comunicación a los trabajadores sobre problemas y recomendaciones en término de seguridad informática.

## Técnicas para asegurar el sistema

- Codificar la información: Criptología, Criptografía y Criptociencia, contraseñas difíciles de averiguar a partir de datos personales del individuo.
- Vigilancia de red. Zona desmilitarizada
- Tecnologías repelentes o protectoras: cortafuegos, sistema de detección de intrusos - antispyware, antivirus, llaves para protección de software, etc. Mantener los sistemas de información con las actualizaciones que más impacten en la seguridad.
- Sistema de Respaldo Remoto. Servicio de backup remoto

## Respaldo de Información

La información constituye el activo más importante de las empresas, pudiendo verse afectada por muchos factores tales como robos, incendios, fallas de disco, virus u otros. Desde el punto de vista de la empresa, uno de los problemas más importantes que debe resolver es la protección permanente de su información crítica.

La medida más eficiente para la protección de los datos es determinar una buena política de copias de seguridad o backups: Este debe incluir copias de seguridad completa (los datos son almacenados en su totalidad la primera vez) y copias de seguridad incrementales (sólo se copian los ficheros creados o modificados desde el último backup). Es vital para las empresas elaborar un plan de backup en función del volumen de información generada y la cantidad de equipos críticos.

Un buen sistema de respaldo debe contar con ciertas características indispensables:

- **Continuo**

  El respaldo de datos debe ser completamente automático y continuo. Debe funcionar de forma transparente, sin intervenir en las tareas que se encuentra realizando el usuario.

- **Seguro**

  Muchos softwares de respaldo incluyen cifrado de datos (128-448 bits), lo cual debe ser hecho localmente en el equipo antes del envío de la información.

- **Remoto**

  Los datos deben quedar alojados en dependencias alejadas de la empresa.

- **Mantención de versiones anteriores de los datos**

  Se debe contar con un sistema que permita la recuperación de versiones diarias, semanales y mensuales de los datos.

Hoy en día los sistemas de respaldo de información online (Servicio de backup remoto) están ganando terreno en las empresas y organismos gubernamentales. La mayoría de los sistemas modernos de respaldo de información online cuentan con las máximas medidas de seguridad y disponibilidad de datos. Estos sistemas permiten a las empresas crecer en volumen de información sin tener que estar preocupados de aumentar su dotación física de servidores y sistemas de almacenamiento.

### Consideraciones de software

Tener instalado en la máquina únicamente el software necesario reduce riesgos. Así mismo tener controlado el software asegura la calidad de la procedencia del mismo (el software obtenido de forma ilegal o sin garantías aumenta los riesgos). En todo caso un inventario de software proporciona un método correcto de asegurar la reinstalación en caso de desastre. El software con métodos de instalación rápidos facilita también la reinstalación en caso de contingencia.

Existe un software que es conocido por la cantidad de agujeros de seguridad que introduce. Se pueden buscar alternativas que proporcionen iguales funcionalidades pero permitiendo una seguridad extra.

### Consideraciones de una red

Los puntos de entrada en la red son generalmente el correo, las páginas web y la entrada de ficheros desde discos, o de ordenadores ajenos, como portátiles.

Mantener al máximo el número de recursos de red sólo en modo lectura, impide que ordenadores infectados propaguen virus. En el mismo sentido se pueden reducir los permisos de los usuarios al mínimo.

Se pueden centralizar los datos de forma que detectores de virus en modo batch puedan trabajar durante el tiempo inactivo de las máquinas.

Controlar y monitorizar el acceso a Internet puede detectar, en fases de recuperación, cómo se ha introducido el virus.

## Algunas afirmaciones erróneas comunes acerca de la seguridad

- **Mi sistema no es importante para un cracker**

Esta afirmación se basa en la idea de que no introducir contraseñas seguras en una empresa no entraña riesgos pues ¿quién va a querer obtener información mía?. Sin embargo, dado que los métodos de contagio se realizan por medio de programas *automáticos*, desde unas máquinas a otras, estos no distinguen buenos de malos, interesantes de no interesantes, etc. Por tanto abrir sistemas y dejarlos sin claves es facilitar la vida a los virus.

- **Estoy protegido pues no abro archivos que no conozco**

Esto es falso, pues existen múltiples formas de contagio, además los programas realizan acciones sin la supervisión del usuario poniendo en riesgo los sistemas.

- **Como tengo antivirus estoy protegido**

En general los programas antivirus no son capaces de detectar todas las posibles formas de contagio existentes, ni las nuevas que pudieran aparecer conforme los ordenadores aumenten las capacidades de comunicación, además los antivirus son vulnerables a desbordamientos de búfer que hacen que la seguridad del sistema operativo se vea más afectada aún.

- **Como dispongo de un firewall no me contagio**

Esto únicamente proporciona una limitada capacidad de respuesta. Las formas de infectarse en una red son múltiples. Unas provienen directamente de accesos al sistema (de lo que protege un firewall) y otras de conexiones que se realizan (de las que no me protege). Emplear usuarios con altos privilegios para realizar conexiones puede entrañar riesgos, además los firewalls de aplicación (los más usados) no brindan protección suficiente contra el spoofing.

- **Tengo un servidor web cuyo sistema operativo es un Unix actualizado a la fecha**

Puede que este protegido contra ataques directamente hacia el núcleo, pero si alguna de las aplicaciones web (PHP, Perl, Cpanel, etc.) está desactualizada, un ataque sobre algún script de dicha aplicación puede permitir que el atacante abra una shell y por ende ejecutar comandos en el unix.

## Organismos oficiales de seguridad informática

Existen organismos oficiales encargados de asegurar servicios de prevención de riesgos y asistencia a los tratamientos de incidencias, tales como el **CERT/CC** [1] (*Computer Emergency Response Team Coordination Center*) del *SEI* [2] (Software Engineering Institute) de la Carnegie Mellon University el cual es un centro de alerta y reacción frente a los ataques informáticos, destinados a las empresas o administradores, pero generalmente estas informaciones son accesibles a todo el mundo.

## Enlaces externos

Wikilibros

- Wikilibros alberga un libro o manual sobre **Seguridad informática**.
- CCN-CERT [3] Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN), dependiente del Centro Nacional de Inteligencia (CNI). Este servicio se creó a principios de 2007 como CERT gubernamental español y está presente en los principales foros internacionales en los que se comparte objetivos, ideas e información sobre la seguridad de forma global.
- UNAM-CERT [4] Subdirección de Seguridad de la Información UNAM-CERT (noticias, documentos, información para usuarios, revista .Seguridad, alertas de seguridad, Malware UNAM, Honeynet UNAM, etc.)
- CriptoRed [5] Red Temática de Criptografía y Seguridad de la Información (más de 400 documentos, libros, software y vídeos freeware)
- INTECO-CERT [6] Centro de Respuesta a Incidentes de Seguridad cuya finalidad es servir de apoyo preventivo y reactivo en materia de seguridad en tecnologías de la información y la comunicación tanto a PYMES como a ciudadanos de España.
- [7] Elementos de diseño de análisis de riegos informáticos
- Oficina de Seguridad del Internauta [8] Información sobre seguridad informatica para usuarios finales

## Referencias

[1] http://www.cert.org
[2] http://www.sei.cmu.edu/
[3] http://www.ccn-cert.cni.es
[4] http://www.seguridad.unam.mx
[5] http://www.criptored.upm.es/
[6] http://cert.inteco.es/
[7] http://seguridad.internet2.ulsa.mx/congresos/2003/esime/ariesgo.pdf
[8] http://www.osi.es

# Fuentes y contribuyentes del artículo

**Infoética** *Fuente*: http://es.wikipedia.org/w/index.php?oldid=44935488 *Contribuyentes*: Bethan 182, Gusgus, Maperez324, 1 ediciones anónimas

**Cómputo forense** *Fuente*: http://es.wikipedia.org/w/index.php?oldid=52262787 *Contribuyentes*: Andy.qaf, Avelaz, Diegusjaimes, Eduardohome, Farnabol, Francisco974, Gabriel Acquistapace, Gacq, Grosalesu, Gusgus, Jkbw, Manuel-jrs, Petruss, Rafael moncada, Sergio Andres Segovia, Vitamine, Xombra, Yakoo, 42 ediciones anónimas

**Delito informático** *Fuente*: http://es.wikipedia.org/w/index.php?oldid=55276433 *Contribuyentes*: -jem-, Abogadosrosarinos, Airunp, Albeiror24, Allan Javier Aguilar Castillo, Andreasmperu, Armenta isai, Arym, Açipni-Lovrij, Banfield, Beaire1, Braian87b, Chessa, Cinabrium, ColdWind, Copy Paco, David0811, Diegusjaimes, Draugmor, Emiduronte, Emilyum, Equi, Facundoherrera, Filipo, Firewall, Frank ug, GermanX, HNfrancisco, Handradec, Héctor Guido Calvo, Internetsinacoso, Irus, J. A. Gélvez, Javi the man, Jkbw, Ldfv, Loco085, Madgc, Maleiva, Matdrodes, Muro de Aguas, Pertile, RelliKuscof, Ricardogpn, Rubpe19, Rœge, Savh, Segedano, Technopat, Tidsa, Yakoo, 177 ediciones anónimas

**Seguridad informática** *Fuente*: http://es.wikipedia.org/w/index.php?oldid=55254900 *Contribuyentes*: -jem-, 333, AchedDamiman, Acorletti, Adrruiz, Agox, Aikurn, Airunp, Alakasam, Alex299006, Alexav8, Alhen, Allan Javier Aguilar Castillo, Amadís, Andreasmperu, Angel GN, Antonorsi, Aosoriod, Arcibel, Aziku, B3rN9, BL, Baiji, Banfield, Bernard, Bk26, BlackBeast, BrWriter2, Bucephala, Cad, Cansado, Centroamericano, Ciencia Al Poder, Cinabrium, Cratón, Crisborghe, Cxocommunity, Cybermeis, Damianiencowiki, Daniel121, Death Master, Deleatur, Demex, Diegusjaimes, Dodo, Draugmor, Eduardosalg, Edub, Edupedro, Egaida, Elabra sanchez, Emari, Emijrp, Er Komandante, Flores,Alberto, Fran89, FrancoGG, Gabriel Acquistapace, Galandil, GermanX, Gerval, Giannii, Ginés90, Greek, Gustavodiazjaimes, H4l9k, HECTOR ARTURO AZUZ SANCHEZ, HUB, Halfdrag, House, Hprmedina, Humberto, Héctor Guido Calvo, ILoveSugar, Iescriva, InfoAudit, Ing.armandolopez, Intecocert, Internetsinacoso, Inu, Irbian, Isha, Iulius1973, JEDIKNIGHT1970, JUANCARLOSMTZT, Javiergtz, Javierito92, Jihernandez, Jkbw, Jmquintas1973, JoanCalderón, JorgeGG, Jramio, Jugones55, Jurgens, K-F.U.N 2, Kizar, Kordas, KrumVik, Laozmdq, Leugim1972, Loco085, Lucien leGrey, Luis 414, Luis1970, M3thod.mdf, MIGUEL OJEDA, MadriCR, Magister Mathematicae, Magrox, Maleiva, Mansoncc, Manwë, MarcosJHofer, Matdrodes, McMalamute, Mecamático, Mel 23, Mjsoto, Montejo, Mortadelo2005, Mpeinadopa, Muro de Aguas, Mushii, NaSz, NathyMig, Netito777, Nicop, Nihilo, Nubecosmica, OMenda, OboeCrack, Oscar ., Oscarif, P kos, Palissy, Pan con queso, Pchamorro, Petruss, Pitlik, Platonides, Poco a poco, Pólux, Queninosta, Rafa2386, RamonVeres, Renly, Rennatot, Retama, Ricardo abarca, Rimac, Roberpl, Rodri cyberdog, Rodriguemus, Rogeliowar, Romel.rivas, Romz, RoyFocker, Sanbec, Santi1212, Santiperez, Sarampión, Sausaf, Savh, Seanver, Seguridad informática, SergioN, Snakeyes, Soniautn, Superzerocool, Tano4595, Technopat, Thr41N, Tigerfenix, Tirithel, Tomatejc, Tostadora, Uncorreotemporal, Urruedelp, Vanessaalexandra, Vitamine, Vituzzu, Wilfredor, Yeza, 765 ediciones anónimas

# Fuentes de imagen, Licencias y contribuyentes

**Archivo:Wikibooks-logo.svg** *Fuente*: http://es.wikipedia.org/w/index.php?title=Archivo:Wikibooks-logo.svg *Licencia*: logo *Contribuyentes*: User:Bastique, User:Ramac et al.

# Licencia