Las nuevas tecnologías y los delitos informáticos

Por Lic. Benigno Víctor Sánchez Curbelo
Especialista en Ciencias Informáticas, Subgerencia de Sistemas Informáticos, UNR, ETECSA
ben@etecsa.cu

"Todo delito que no se convierte en escándalo no existe para la sociedad".
Heinrich Heine

El desarrollo de las nuevas tecnologías de la información y su incorporación en casi todas las áreas de la sociedad, la evidente influencia que tiene la informática en la cotidianeidad de las personas y organizaciones, y su preponderancia en el progreso de un país, han traído consigo una serie de comportamientos ilícitos, a los que de manera general se les denomina **delitos informáticos**.

En el Undécimo Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal que se celebró en abril de 2005, se hizo mención al cambio que está produciendo en la sociedad la introducción de las tecnologías de la información y las comunicaciones en las disímiles facetas de la vida y los negocios; pero que, al mismo tiempo, trae consigo nuevas formas de delincuencia informática.

Los delitos informáticos se encuentran tipificados como tales en muchos países, están contemplados en sus legislaciones y son penados con sanciones que varían entre unos y otros. A pesar de esto, y lamentablemente, todavía un sector de la población tiene una visión romántica para la actividad de **piratería informática** o **delincuencia cibernética** —para englobar a las distintas variantes que la conforman y aunque poseen puntos de contactos, tienen acciones muy diferentes; ver más información en el Anexo 1—. Para este sector, un pirata informático, sería la persona que se apasiona por las computadoras y se dedica a ellas más allá de los límites.

Según la mayoría de los *hackers* famosos, la diferencia básica entre los *hackers* y *crackers* es que los unos construyen cosas, los otros las destruyen. Inicialmente, en los llamados *hackers* tradicionales primaba la curiosidad intelectual y el reto, esto se ha ido transformando en objetivos más mercantiles; por lo tanto, en la actualidad podría decirse que *hacker* es toda persona que se introduce ilegalmente en un sistema informático, que está involucrada en actos que atentan en contra de la propiedad intelectual, roba información, atenta contra la seguridad en las redes, son autores de virus, intrusos de servidores, interceptadores de mensajes de correo, vándalos del ciberespacio, etc.

Otras acepciones, según la jerga de Internet, es la persona que disfruta con la exploración de los detalles de los sistemas programables y cómo aprovechar sus posibilidades más allá de lo permisible por sus fabricantes, lo cual conduciría a la interrogante: ¿cuándo es más allá de lo permisible, según la ley de cada país y se hablaría, entonces, de delito informático?

En el análisis de la mayoría de los casos judiciales famosos sobre delitos informáticos, está presente el factor humano como fuente de información y el empleo de la ingeniería social como método para la obtención de los datos. No es el uso de tecnología sofisticada sino las debilidades internas, tanto humanas como de una incorrecta utilización de los recursos informáticos, lo que ha propiciado la comisión del delito.

Al convertirse en delito, se refiere ya a su impacto social e inciden en los cambios que han debido adoptar las instituciones gubernamentales para prevenir y penalizar las diferentes actividades que surgieron relacionadas con los delitos informáticos y que no estaban tipificadas en las leyes existentes.

Sociedad

La seguridad informática es una necesidad latente que abarca toda la sociedad, y repercute, entre otros factores, en un gasto extra en el que debe incurrirse para proteger los recursos y capacitar al personal que trabaja con las nuevas tecnologías. La sociedad actual tiende a ser cada vez más dependiente de las Tecnologías de la Información y las Comunicaciones (TICs). Ya es común manejar los términos Sociedad de Información y Aldea Global; pero esta dependencia trae consigo peligros latentes. Los sistemas de información son vulnerables a diversas amenazas y atentados.

En la Sociedad de la Información, la información y el conocimiento son insumos fundamentales. Se afirma

que la acción del conocimiento sobre el conocimiento es la fuente fundamental de productividad. La información, las tecnologías de la información van a ser un elemento protagonista; e Internet, su principal medio de transmisión y comunicación a nivel mundial. La sociedad de la información ya afecta a muchos aspectos de la vida, por lo que en ella inciden políticas tan diversas como la reglamentación del sector o la protección de la privacidad.

Un ejemplo del desarrollo abarcador de las nuevas tecnologías está en el llamado *e-government* o gobierno electrónico, que se entiende como la gestión que concentra el empleo intensivo de Tecnologías de la Información y Comunicación, con las modalidades de gestión y administración como una nueva forma de gobierno, es decir, llevar los servicios y trámites del gobierno a Internet, con la posibilidad de integrar las dependencias estatales y de obtener información y servicios mediante la red.

En la región americana pueden citarse ejemplos como la República Bolivariana de Venezuela, Brasil y Chile —política de Estado, según instructivo presidencial del 11 de mayo de 2001—. Sus objetivos en cuanto a gestión pública son el aumento de los niveles de eficiencia en la gestión pública, la disminución significativa de los costos de transacción y coordinación en la interacción entre entes públicos, la generación de incentivos y prácticas que faciliten modalidades de gestión innovadoras y creativas, la agregación de mayor valor público como horizonte permanente de las actividades del sector, y ofrecer mantenimiento y constante superación de los grados de transparencia de esas actividades.

Organizaciones

A nivel mundial se han creado diversas organizaciones con objetivos afines a la protección de la información, además de la comisión de delitos como un medio más para alertarnos y protegernos ante el desarrollo y proliferación de nuevas estrategias para cometer delitos informáticos. Por ejemplo:

- En la Unión Europea existe la ENISA —*European Network and Information Security Agency*—, para tratar los temas de seguridad en las redes y en los sistemas de información europeos, así como los llamados Libros Verdes y Libros Blancos.
- El instituto SANS —*System Administration, Networking and Security*—. Según su sitio Web, es la mayor fuente confiable y la más grande para el entrenamiento de la seguridad de la información y certificación en el mundo. También almacena, clasifica y mantiene disponibles, sin ningún coste adicional, la colección más grande de documentos relacionados con investigaciones sobre varios aspectos de la seguridad de la información, y en ella funciona el sistema de detección temprana del Internetcentro de la tormenta del Internet. Sus programas ahora alcanzan más de 165,000 profesionales de la seguridad, interventores, administradores de sistema o de red, los principales oficiales de seguridad de la información, y ejecutivos que comparten las lecciones aprendidas y encuentran soluciones en común a los desafíos que enfrentan.
- IC3 —Centro de Denuncias de Delitos en Internet— ofrece el servicio de tramitación y remisión de denuncias presentadas por individuos en los Estados Unidos y el resto del mundo.
- CVE —*Common Vulnerabilities and Exposures* / Vulnerabilidades y Exposiciones Comunes— tiene la meta de hacer más fácil el compartimiento de datos, a través de bases de datos, de la vulnerabilidad y de las herramientas, separadas de la seguridad. A pesar de que CVE puede facilitar la búsqueda de información en otras bases de datos, no se debe considerar una base de datos de vulnerabilidades.

Es importante resaltar que el 27 de marzo de 2006, la Asamblea General aprobó la Resolución A/RES/60/252, en la que se proclamaba el 17 de mayo como el Día Mundial de la Sociedad de la Información. Este día contribuirá a sensibilizar sobre las posibilidades que aportan el empleo de Internet y otras tecnologías de la información y las comunicaciones a las sociedades y economías, así como las formas de reducir la brecha digital.

Delitos y Leyes

Internet aún está considerado como un territorio sin ley y sin límites, la digitalización es cada día mayor, y se incorporan nuevos sistemas con la realización de actividades de operaciones y control en ramas tan diversas como el tráfico aéreo y el sistema bancario. El creciente mundo cibernético permite deducir que el delito informático tiende a aumentar y diversificarse.

Este progreso tecnológico ha traído consigo un derrumbe de las fronteras tradicionales de los países dificultando el punto de origen de los servicios. Internet está considerada en estos momentos por la mayoría como imparable e incontrolable, aunque existen partidarios de que debe regularse por los delitos que se generan, lo cual es difícil de perseguir debido a la naturaleza del entorno y a la falta de tipificación de las modalidades de comisión y de los medios empleados.

El Derecho Informático está en evolución y constituye una rama atípica de Derecho, trata de buscar

protección y soluciones jurídicas a nuevas instituciones informáticas. Es el conjunto de normas, aplicaciones, procesos, relaciones jurídicas que surgen como consecuencia de la aplicación de la informática.

Algunas actividades negativas que pueden ser realizadas mediante el uso de las herramientas que ofrecen las tecnologías informáticas y que, actualmente, se consideran delito, son:

- El acceso no autorizado a equipos de cómputo, la modificación o realización de acciones sin autorización de los dueños o fabricantes.
- El vandalismo o la falsificación de identidad —sea o no con fines de lucro—.
- El robo o fraude electrónico.
- Los mensajes no deseados con ánimo de colapsar o causar daños a los sistemas informáticos.
- La difusión de material contrario a la moral o a los principios de un país, una cultura, religión, etc.

El decálogo confeccionado por la Comisión Federal de Comercio de los Estados Unidos (FTC) informa acerca de los fraudes considerados más comunes que se pueden realizar a través de Internet, acorde con las denuncias de los clientes:

Las subastas: algunos mercados virtuales ofrecen una amplia selección de productos a precios muy bajos. Una vez que el consumidor ha enviado el dinero, puede ocurrir que reciban algo con menor valor de lo que creían o, peor aún, que no reciban nada.

Acceso a servicios de Internet: el consumidor recibe una oferta de servicios gratuitos. La aceptación lleva implícita el compromiso de contrato a largo plazo, con altas penalizaciones en caso de cancelación.

Las tarjetas de crédito: en algunos sitios de Internet, especialmente para adultos, se pide el número de la tarjeta de crédito con la excusa de comprobar que el usuario es mayor de 18 años. El objetivo verdadero es cobrar cargos no solicitados.

Llamadas internacionales: en algunas páginas, por lo general de material para adultos, se ofrece acceso gratuito a cambio de descargar un programa que en realidad desvía el módem a un número internacional o a un 906. La factura se incrementa notablemente en beneficio del propietario de la página.

Servicios gratuitos: se ofrece una página personalizada y gratuita durante un período de 30 días. Los consumidores descubren que se les han cargado facturas a pesar de no haber pedido una prórroga en el servicio.

Ventas piramidales: consisten en ofrecer a los usuarios falsas promesas de ganar dinero de manera fácil, sólo por vender determinados productos a nuevos compradores que estos deben buscar.

Viajes y vacaciones: algunas páginas de Internet ofrecen destinos maravillosos a precios muy asequibles que, a menudo, encubren una realidad completamente diferente o inexistente.

Oportunidades de negocio: en la red abundan las ofertas para ganar fortunas con la inversión en una aparente oportunidad de negocio y acaba convirtiéndose en una estafa.

Inversiones: las promesas de inversiones que rápidamente se convierten en grandes beneficios no suelen cumplirse y comprenden grandes riesgos para los usuarios. Como norma general, no es recomendable fiarse de las páginas que garantizan inversiones con seguridad del 100 %.

Productos y servicios milagro: algunas páginas de Internet ofrecen productos y servicios que aseguran curar todo tipo de dolencias. Hay quienes ponen todas sus esperanzas en estas ofertas que normalmente están lejos de ofrecer garantías de curación.

Otras actividades consideradas delictivas y sancionadas en las leyes vigentes de varios países son: la difusión de virus, los gusanos y *dialers*, la violación del trabajo con la información clasificada, molestias o amenazas y la violación del derecho de autor.

Existen acciones delictivas que están bien tipificadas en correspondencia con la forma de actuar y la técnica que utiliza, por ejemplo, *carding* —uso ilegal de tarjetas de crédito—, *trashing* —obtención de información en cubos de basura, por ejemplo, números de tarjetas de crédito, contraseñas, directorios o recibos—, *phreaking* y *foning* —uso ilegal de las redes telefónicas—, y los llamados piratas que copian software, música, etc. con el objetivo de venderlos y obtener ganancia.

La divulgación del empleo de la red de redes generó un submundo que no está limitado por las fronteras y donde el traspaso de información, para bien o para mal, no está regulado ni depende de reglamentos, culturas, tradiciones, etc. de los países y en el que es posible intercambiar documentación, herramientas, programas que facilitan y propician la actividad delictiva, debido a la ausencia de uniformidad de criterios con relación al delito informático.

Las referencias a delitos informáticos incluyen los cometidos contra el sistema y los que se realizan mediante el uso de sistemas informáticos. En muchos países ya están tipificados en sus disposiciones legales, fundamentalmente, los derechos de propiedad intelectual, protección de datos e intención de destruir o inutilizar los datos de un sistema de información que impida su funcionamiento correcto, conducta maliciosa que provoque daños o alteraciones en un sistema de información, etc.

En Cuba, Lourdes Pérez Navarro en un artículo publicado en el periódico *Granma* el 4/1/2005,

titulado "Criminalidad informática", refiere que, en el caso del Código Penal Cubano, los hechos delictivos instruidos y procesados por atacar a los sistemas informáticos, o por utilizar tecnologías para realizar actos ilícitos, han sido resueltos porque están incluidos dentro de la legislación vigente, es el caso de los delitos contra los derechos patrimoniales —robo, apropiación indebida, estafa, entre otros— y daños."

En la medida en que avance el desarrollo informático de la sociedad, el Código Penal Cubano tendrá que adecuarse e identificar los nuevos delitos específicos —por ejemplo, el creador de virus informáticos, el distribuidor y el intruso—, los cuales de alguna manera alteran o ponen en riesgo la seguridad informática.

Conclusiones

La cultura de Internet durante los primeros años creó una especie de aureola alrededor de la entrada ilegal a sitios cada vez más seguros convirtiéndose en un reto y un triunfo para los que lo lograban. Esto hizo que para algunos jóvenes fuera una meta la actividad de *hackeo* —actualmente es imprescindible que la sociedad concientice y asocie estas acciones como delitos al igual que cualquier otro de los llamados tradicionales—.

No son los grandes sistemas de información los que afectan la seguridad personal o de las empresas, sino la manipulación o el consentimiento de ellos, por parte de individuos poco conscientes e irresponsables de los datos que dichos sistemas contienen, por lo tanto, es necesario contar con leyes que penalicen a todas aquellas personas que empleen técnicas de *hackeo* para fines lucrativos o destructivos.

Es vital tener presente que el eslabón más débil en la cadena de seguridad es el factor humano; la mejor herramienta de un *hacker* es la ingeniería social, de ahí que la preparación del personal es un factor esencial en la elaboración de cualquier esquema de seguridad informática.

Bibliografía

"Aspectos legales del comercio electrónico". Disponible en: http://www.eurociber.es/index.php?mostrar=hackers7. (Consulta: octubre/2006).

"Ausencia de políticas públicas en la prevención de delitos informáticos". Disponible en: http://www.misionesonline.net/paginas/opinion.php?id=2298%20. (Consulta: octubre/2006).

"Confiare". Disponible en: http://www.confiare.cl. (Consulta: octubre/2006).

"Criminalidad Informática". Disponible en: http://www.granma.cubaweb.cu/2005/01/04/nacional/articulo06.html. (Consulta: octubre/2006).

"Cumbre Mundial sobre la Sociedad de la Información (CMSI)". Disponible en: http://www.itu.int/wsis/index-es.html y http://www.itu.int/wisd/2006/index-es.html. (Consulta: octubre/2006).

"Delitos_electrónicos". Disponible en: http://www.canalfiscal.com/delitos_electronicos.htm. (Consulta: octubre/2006).

"Delitos electrónicos / Legislación". Disponible en: http://www.gdt.guardiacivil.es/legislacion.php. (Consulta: octubre/2006).

"Delitos informáticos". Disponible en: http://www.iabogado.com/esp/guialegal/guialegal.cfm?IDCAPITULO=18050000. (Consulta: octubre/2006).

"Delitos informáticos". Disponible en: http://www.monografias.com/trabajos6/delin/delin.shtml. (Consulta: octubre/2006).

"Delitos informáticos". Disponible en: http://www.eurociber.es/index.php?mostrar=hackers7. (Consulta: octubre/2006).

"Delitos informáticos". Disponible en: http://www.iabogado.com/esp/guialegal/guialegal.cfm?IDCAPITULO=18050000. (Consulta: octubre/2006).

El Instituto Nacional de Tecnologías de la Comunicación. Disponible en: http://inteco.red.es/. (Consulta: octubre/2006).

Gobierno Bolivariano de Venezuela. Disponible en: http://www.gobiernoenlinea.gob.ve/. (Consulta: octubre/2006).

Instituto Nacional de Normas y Tecnología —*National Institute of Standards and Technology* (NIST)—. Disponible en: http://www.nist.gov/public_affairs/general2_spanish.htm. (Consulta: octubre/2006).

Las vulnerabilidades y las exposiciones comunes (CVE). Disponible en: http://cve.mitre.org/about/. (Consulta: octubre/2006).

Legislación. Disponible en: http://www.contract-soft.com/leyes.htm. (Consulta: octubre/2006).

Legislación sobre delitos informáticos. Disponible en: http://www.monografias.com/trabajos/legisdelinf/legisdelinf.shtml. (Consulta: octubre/2006).

"Posición de Cuba sobre la pornografía infantil". Disponible en: http://www.cubaminrex.cu/CDH/60cdh/POSICI%D3N%20DE%20CUBA%20SOBRE%20LA%20PORNOGRAF%CDA%20INFANTIL.htm. (Consulta: octubre/2006).

Resolución 6 del 96 del MININT. Disponible en: http://athenea.fcf.uh.cu/auditoria/manual%20del%20auditor/tomo1Cap2/resol6del96minint.htm. (Consulta: octubre/2006).

Sbampato, Ignacio. Disponible en: http://ignacio-sbampato.neurona.com/. Sbampato. (Consulta: octubre/2006).

Seguridad en las TICs. Disponible en: http://www.mic.gov.cu/hticentity.aspx. (Consulta: octubre/2006).

Anexo I

Notas sobre algunos términos usados y que se comentan sin la intención de ser absolutos en la explicación ofrecida.

Adware: es una palabra inglesa que nace de la contracción de las palabras *Advertising Software,* es decir, programas que muestran anuncios. Se denomina *adware* al software que muestra publicidad, a través del empleo de cualquier tipo de medio**:** ventanas emergentes, *banners*, cambios en la página de inicio o de búsqueda del navegador, etc. La publicidad está asociada a productos o servicios ofrecidos por los propios creadores o por terceros.

Alias: nombre usualmente corto y fácil de recordar que se utiliza en lugar de otro nombre por lo general largo y difícil de recordar (ver Nick).

Bug —bicho, insecto—: son conocidos como agujeros o huecos de seguridad. Son defectos del software y el hardware que, supuestamente no han sido descubiertos por los creadores o diseñadores de los mismos. El proceso para corregirlos se llama Debuggins. A través de un bug, las personas con ciertos conocimientos pueden introducirse en los sistemas ajenos o manipular alguna información de estos.

Ciberespacio: término concebido por el escritor William Gibson en su novela de ciencia ficción *Neuromante* (1984) con el propósito de describir un mundo de redes de información. Actualmente es utilizado para referirse al conjunto de información digital y a la comunicación que se realiza a través de las redes, un espacio en el cual casi todo lo que contiene información o puede transmitirla, debe ser incluido.

Cookies —galletitas o chivatos—**:** son datos intercambiados entre un usuario de Internet y un servidor Web que quedan archivados en el disco duro del usuario, registra las actividades que realiza en un sitio. Puede constituir un medio de control de las actividades del usuario.

Cracker: aquel que rompe con la seguridad de un sistema. Hacer daño, desproteger un programa con su propios medios y modificar la programación para usarlo sin pagar los derechos o para venderlo y obtener beneficios personales. Por ejemplo, intrusión de redes, acceso ilegal a sistemas gubernamentales, robo de información, distribuir material ilegal o moralmente inaceptable, fabricación de virus, herramientas de *Crackeo*, etc. *Crackear* es saltarse las protecciones —generalmente a nivel software—, que se introducen en los programas con el fin de impedir (o dificultar) su copia.

Dialers: es un programa que, sin el consentimiento del usuario, cuelga la conexión telefónica que está utilizándose en ese momento y establece otra, marcando un número de teléfono de tarificación especial. Esto supondrá un notable aumento del importe en la factura telefónica**.**

Firewall: se trata de un mecanismo de seguridad en Internet frente a accesos no autorizados. Hay firewalls por hardware o por software. Básicamente consiste en un filtro que mira la identidad de los paquetes y rechaza todos aquellos que no estén autorizados o correctamente identificados. Su traducción podría ser cortafuegos.

Freeware: cualquier programa que es gratuito. Por lo general trae una licencia de uso, que especifica los derechos y obligaciones de los usuarios con ese programa.

GII —*Global Information Infrastructure* / Infraestructura Global de Información—: es el nombre que se ha dado a la autopista de datos que cubrirá todo el planeta.

Hacker: persona que ve los sistemas informáticos como un reto y se dedica a su interioridades aprendiendo a usarlos al máximo más allá de un usuario normal y disfruta del reto intelectual de superar las limitaciones impuestas, por lo que tiene la capacidad y el talento de *crackear* un sistema programado. Puede acceder a un sistema protegido como si se tratara de un reto personal, sin intentar causar daños y buscar los fallos de seguridad para corregirlos; pero puede también obtener una información que el

propietario considera valiosa. Y es aquí cuando una actividad de *hackeo* se convierte en delito. Entre ellos también pueden diferenciarse en:

Sombrero Negro: calificados como terroristas y mercenarios.

Sombrero Gris: capacidad para vulnerar sistemas. Su intención no es causar daño.

Sombrero Blanco: detectar errores y fallas en los sistemas de seguridad y advertir cómo remediar el problema.

Hackerismo (hackear): así se le denomina al acto que hacen los hackers en una computadora.

Hoax (engaño): se refiere a un mensaje de correo electrónico con un contenido engañoso o falso. Es una variante del Spam que valiéndose de la ingeniería social informa sobre un virus desastroso o apelan a la solidaridad con una niña enferma o cualquier otra causa noble que toque la sensibilidad del destinatario o lo incite a ganar mucho dinero o mantener una cadena de suerte, etc. Pero realmente el objetivos es captar direcciones de correo, saturar la red o los servidores de correo, propagar un virus, etc.

Ingeniería Social: consiste en convencer a otra persona para que facilite información útil o que realice alguna acción determinada, normalmente sin revelar la identidad propia y suplantando una falsa; parte del principio que el eslabón más débil de la seguridad es el eslabón humano.

Jargon File: algo así como "archivo de la jerga hacker", contiene gran cantidad de definiciones de términos relacionados con Internet y se actualiza regularmente. Es un diccionario sobre la 'jerga hacker', la versión Web de un libro publicado por Eric S. Raymond.

Lammer: vocablo usado despectivamente para definir a aquellos que presumen de ser hackers y no lo son, sólo se aprovecha del conocimiento adquirido y publicado por los expertos.

Nick: es aquel nombre que se utiliza para ser conocido en el ciberespacio, necesariamente no tiene que ser el nombre verdadero de la persona, de por sí, los hackers nunca revelan su nombre siempre andan escondidos detrás de los *nicks*.

Phreaker: arte y ciencia de *crackear*, más bien de estafar la red telefónica para obtener beneficios personales, por ejemplo, llamadas gratis de larga distancia.

Phishing (pescando datos): técnica utilizada para captar datos personales, principalmente, los datos bancarios de los usuarios a través de la utilización de la imagen de la entidad bancaria mediante correos electrónicos o páginas Web que imitan/copian la imagen o apariencia de una entidad bancaria/financiera o empresa reconocida internacionalmente, etc. Por ejemplo, un correo electrónico indicando que nuestra cuenta o usuario está por ser deshabilitado y que deben reingresarse los datos, o en caso contrario se dará de baja, y se muestra un enlace donde podemos introducir los datos, remitiéndonos a un sitio falso destinado a obtener información personal y suplantar al verdadero usuario con fines de lucro.

Pirata: que se dedica a distribuir software ilegalmente —copiado o *crackeado*— y con ánimo de lucro.

Shareware: es el software que es distribuido exclusivamente para ser probado o evaluado por lo que pueden estar restringidas ciertas características y tiene un tiempo de uso limitado por el fabricante.

Sniffer: es una aplicación de monitorización y de análisis para el tráfico de una red para detectar problemas, lo hace buscando cadenas numéricas o de caracteres en los paquetes. Puede usarse ilegalmente para recibir datos privados en una red. Es el programa encargado de obtener los datos que circulan por una red.

Spam: el correo que recibimos sin haberlo solicitado. Por lo general contiene información basura.

Spyware: programas espías, son aplicaciones informáticas que recopilan datos sobre los hábitos de navegación, preferencias y gustos del usuario. Los datos recogidos son transmitidos a los propios fabricantes o a terceros, bien directamente, bien después de ser almacenados en el ordenador.

Trashing: es la técnica de recuperar o investigar sobre información que ha sido abandonada o eliminada.

Virus: un virus informático es un programa o segmento de código que puede interferir en el funcionamiento de una computadora, y es capaz de realizar algunas acciones, por ejemplo:

1. Tiene la capacidad de causar daño.
2. Replicarse a sí mismo.
3. Propagarse a otras computadoras.
4. Registrar, dañar o eliminar datos.
5. Infectar a otros ficheros.

XPloit: grupo de programas que emplean los *bugs* de seguridad para conseguir información de una máquina remota.