

Pilares básicos

En este primer capítulo, nos introduciremos en los conceptos, terminologías y características que nos servirán de base para la comprensión de los restantes capítulos.

¿Qué es la seguridad?	18
Confidencialidad	18
Integridad	18
Disponibilidad	18
Autenticidad	18
¿Qué queremos proteger?	20
Importancia de los elementos	21
¿De qué nos protegemos?	24
Factores humanos	25
Factores no humanos	29
Resumen	29
Actividades	30

¿QUÉ ES LA SEGURIDAD?

La seguridad está finamente ligada a la certeza. Para entender esta definición, hay que aclarar que no existe seguridad absoluta, más bien, lo que se intenta es minimizar el impacto y/o riesgo. Por tal motivo, cuando hablamos de seguridad, debemos hacerlo en carácter de niveles, y lo que se intenta y se debe hacer es llevar a cabo una organización efectiva a fin de lograr llegar a los niveles más altos.

Las técnicas para llegar a una correcta organización están basadas en cuatro pilares fundamentales que hacen que la **INFORMACIÓN** se encuentre protegida. Estos pilares se ocupan principalmente de proteger cuatro aspectos de la información:

- **Confidencialidad**
- **Disponibilidad**
- **Integridad**
- **Autenticidad**

Confidencialidad

La información puede ser accedida **únicamente** por las personas que tienen autorización para hacerlo. Por ejemplo, cuando decimos que Internet es una Red de redes, estamos diciendo que hay **medios** que se entrelazan entre sí para lograr una vinculación. Es por ello que la confidencialidad se puede ver amenazada si alguien intercepta los paquetes que viajan de un lado al otro.

Integridad

Cuando nos referimos a integridad, queremos decir que estamos totalmente seguros de que la información no ha sido borrada, copiada o alterada, no sólo en su trayecto, sino también desde su origen. Por ejemplo, si un atacante modifica información confidencial para provecho propio, o si dicha información está codificada y el mismo atacante, al no poder leerla claramente, la borra.

Disponibilidad

Este término hace referencia al método de precaución contra posibles daños tanto en la información como en el acceso a la misma: ataques, accidentes o, simplemente, descuidos pueden ser los factores que obligan a diseñar métodos para posibles bloqueos.

Autenticidad

Algunos profesionales de la seguridad no incluyen este ítem cuando hablan de los pilares, sino que nombran los tres anteriores. Particularmente, creemos que no se

puede soslayar este concepto, debido al hecho de que **integridad** nos informa que el archivo, por ejemplo, no ha sido retocado ni editado, y **autenticidad** nos informa que el archivo en cuestión es el real.

No podemos dejar de nombrar, en un capítulo dedicado a esclarecer conceptos, el rol que cumple la **autenticación**. La autenticación de una computadora difiere con los términos de los humanos: para una PC, **autenticar** no es lo mismo que **identificar**. Por ejemplo, en un sistema de seguridad donde se verifica la voz, el sistema se encarga de buscar un patrón en su voz para distinguir quién es. Este reconocimiento es de identificación, pero todavía falta la parte en que el usuario dice una frase o palabra clave, y es aquí donde la autenticación tiene efecto.

Los métodos de autenticación para verificación de identidad pueden clasificarse en tres categorías, a saber:

- **Categoría 1: algo que el usuario sabe.**

Un dato esencial, puede tratarse de algo de su persona o bien de un simple o complejo password (contraseña).

```
login as: root
Using keyboard-interactive authentication.
Password:
Last login: Tue Jun 28 14:59:17 2005 from 192.168.1.2
test:~# █
```

Figura 1. Imagen que nos muestra un sistema de verificación por medio de usuario y password en el sistema operativo **Linux**.

- **Categoría 2: algo que el usuario lleva consigo.**

Puede ser un documento de identidad, una tarjeta o cualquier otro elemento que uno lleve consigo.

- **Categoría 3: propiedad física o acto involuntario.**

La pupila, la voz y la huella dactilar son ejemplos de propiedades físicas de un individuo y **firmar** es un acto involuntario, ya que uno no está pensando en hacer cada trazo, sino que los realiza en conjunto.

PRIMERO HAY QUE ENFOCARSE

La seguridad es un estado mental; si no estamos enfocados en el punto correcto, el mecanismo para asegurar nuestra red se va a ver afectado. Pensemos primero en los peligros y en las prioridades de sus elementos y, luego, en las soluciones.

Estos temas se hablarán en detalle en el capítulo **Seguridad física**; sólo se expusieron a modo de concepto, ya que cuando hablamos de seguridad informática, hablamos de fiabilidad y, por ende, de elementos que generen tal confianza.

¿QUÉ QUEREMOS PROTEGER?

Cuando hablamos de seguridad informática muchas veces se confunde diciendo **seguridad en Internet**, y estos términos no son sinónimos. **Informática** comprende otro contexto, como ser el de la seguridad física, mientras que el otro sólo se limita a hablar del entorno que a Internet se refiere. Por tales motivos, la seguridad informática intenta proteger cuatro elementos:

- **Hardware**

El hardware se encuentra compuesto por el conjunto de sistemas físicos del sistema informático, en otros términos, de nuestra computadora: gabinete, motherboard, microprocesador, disco duro, unidades de almacenamiento extraíble, monitor, mouse, teclado, cables, etc.

- **Software**

El software consiste en el conjunto de sistemas lógicos que hacen funcional al hardware: sistemas operativos, aplicaciones, programas, etc.

- **Datos**

Conjunto de sistemas lógicos que tienen como función manejar el software y el hardware (registros, entradas en base de datos, paquetes que viajan por los cables de red; hasta un bit es un dato).

Vale aclarar que **no es lo mismo dato que información**. Un dato no tiene coherencia por sí solo, sino que la tiene por medio de un entorno o contexto. Si bien el dato es esencial, el juicio sobre lo que se debe hacer con el mismo se realiza por medio de un programa o persona.



IMPORTANTE

Últimamente la tecnología se ve representada en dispositivos cada vez más pequeños. Esto hace que la seguridad física deba ser tenida muy en cuenta por el encargado de la seguridad.

A diferencia de los datos, la información sí tiene significado. Es más, los datos se convierten en información cuando su creador les añade significado.

- **Elementos fungibles**

Son elementos que se gastan o se desgastan con el uso continuo (papel, controladora fiscal, impresora/tóner, disquetes, insumos en general y todo lo que de alguna manera esté conectado a una máquina). Algunos administradores de seguridad no consideran estos elementos para protegerlos, y están equivocados.

Una buena administración se basa en controlar los recursos de la empresa, ya que los mismos no son infinitos ni el dinero con el que se cuenta es ilimitado, y menos para usarlo como gasto y no como inversión. Para lograr eficiencia y calidad se tiene que tomar conciencia y crear una política para el correcto uso de las herramientas con las que cuenta la empresa.

Importancia de los elementos

De los cuatro elementos, los datos son los principales a la hora de proteger. El hardware, el software y los elementos fungibles son recuperables desde su origen (comprándolos o instalándolos nuevamente), pero los datos **no tienen origen**, sino que son cambiados en el transcurso del tiempo y son el resultado del trabajo realizado. Ésta es la razón que convierte en muy importante el armado de una política de seguridad, y es el motivo por el cual el próximo capítulo está dedicado exclusivamente a confeccionar una política de seguridad. Una política consistiría en programar horarios y momentos para realizar copias de seguridad (*backups*), archivarlos, tener disponibilidad de espacio/privacidad y, además, poder hallar lo se necesite en tiempo y forma.

Los múltiples ataques que se pueden realizar sobre los datos –principalmente– se pueden categorizar en cuatro grupos.

- **Interrupción. Ataque contra la disponibilidad.**

Cuando los datos o la información de un sistema se ven corruptos, ya sea porque los mismos se han perdido, se han bloqueado o simplemente porque no están dis-



INFORMACIÓN PÚBLICA Y PRIVADA

Según el lema de los hackers, la información debe ser pública. Por eso es sumamente importante que los datos se protejan.

ponibles para su uso. Este tipo de ataque en la mayoría de las ocasiones no tiene mucha lógica por parte del atacante, salvo que se vea encerrado o perseguido.

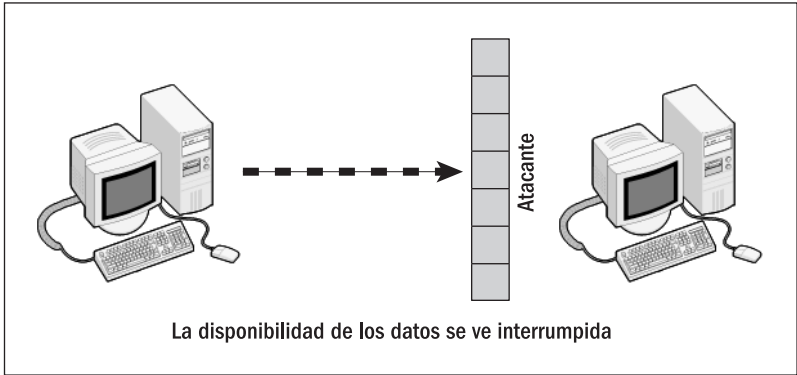


Figura 2. Cómo se paraliza el flujo de datos.

• **Interceptación. Ataque contra la confidencialidad.**

Con este tipo de ataque lo que se logra es que un usuario no autorizado pueda acceder a un recurso y, por ende, la confidencialidad se ve divulgada. Hay muchos tipos de interceptación, por ejemplo, cuando se intercepta las cabecera de los paquetes y logramos identificar usuarios tanto del lado del remitente como del receptor; eso es llamado **interceptación de identidad**, en cambio, el **sniffear** (ver ilegítimamente la información que pasa por un medio) se llama sencillamente **interceptación de datos**.

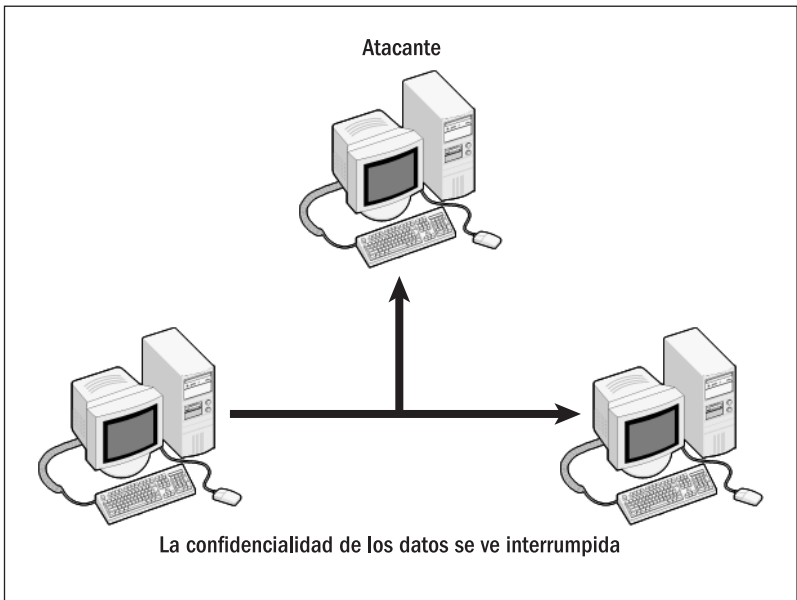


Figura 3. Desvío de los datos.

- **Fabricación. Ataque contra la autenticidad.**

El ataque contra la autenticidad tiene lugar cuando un usuario malicioso consigue colocar un objeto en el sistema atacado.

Este tipo de ataque puede llevarse a cabo con el objeto de hacer creer que ese archivo/paquete es el correcto o bien con la finalidad de agregar datos y obtener, de esta manera, un provecho propio.

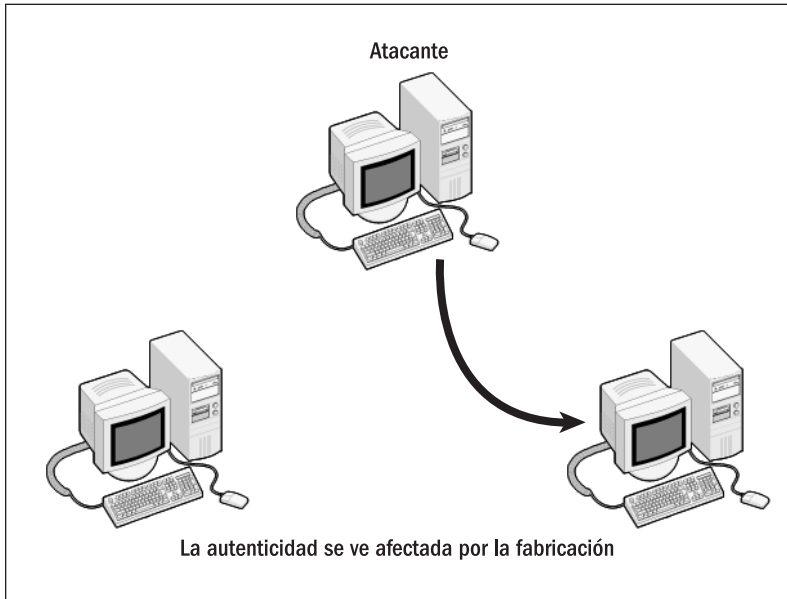


Figura 4. El momento del cambio de datos.

- **Modificación. Ataque contra la integridad.**

Un atacante, que puede contar o no con autorización para ingresar al sistema, manipula los datos de tal manera que la integridad se ve afectada por su accionar. Cambiar datos de archivos, modificar paquetes, alterar un programa o aplicación son sólo algunos ejemplos de este tipo de ataque que, sin ninguna duda, es el que reviste mayor grado de peligrosidad.



NUESTRA INFORMACIÓN PUEDE SER ESPIADA

El método que más fácil les resulta a los interesados es el de **sniffear** (o escuchar por el cable), que entra en la categoría de **interceptación**. El método trabaja sobre redes LAN, es sumamente efectivo pero, a la vez, sumamente peligroso.

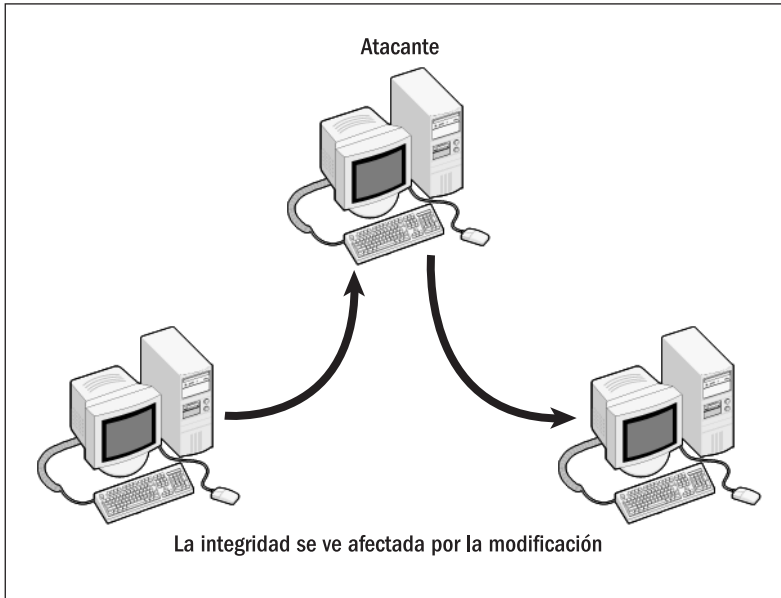


Figura 5. En esta imagen vemos un esquema que ilustra el flujo de datos inventado.

Hasta aquí, hemos nombrado los grupos más conocidos y más divulgados dentro del campo de la seguridad informática. Pero no son exactos, ya que algunos ataques no se encasillan en estos grupos, o bien entran en varios. Por ejemplo, cuando hablamos de **destrucción**, estamos hablando de un ataque contra la disponibilidad, por ende, se debería situar en el grupo **interrupción**, pero varios autores lo sitúan en **modificación**, haciendo referencia a que la destrucción inutiliza el objeto afectado.

¿DE QUÉ NOS PROTEGEMOS?

Esta pregunta es tan amplia como su respuesta. Hay muchas clasificaciones que van variando según cada autor y cada investigador del tema, pero la mayoría tienen un punto de vista en común: **nos protegemos de las personas.**

A esta altura de los tiempos y con las sociedades que evolucionan, suena raro decir que estamos cuidándonos de nosotros mismos y, más aún sabiendo que esos elementos que protegemos son, en su mayoría, cosas creadas por nosotros mismos. El factor más importante que incita a las personas a cometer actos en contra de los cuatro pilares (integridad, disponibilidad, confidencialidad y autenticidad) es, sin ninguna duda, el poder. Este poder reside en los datos y en la información, y son compartidos por el mundo, como explicaremos en capítulos posteriores cuando hablemos sobre los hackers.

Como hemos dicho anteriormente, muchos escritores difieren al referirse sobre de quién o de qué hay que protegerse, ya que para algunos, las **catástrofes** lo toman sin la debida atención y no como un motivo para hacer resguardos de información o hacer uso de mecanismos a fin de prevenirlos.

Si bien vamos a hablar más en detalle sobre quiénes y cómo son nuestros atacantes, clasificados dentro de la categoría **factores humanos**, no podríamos dejar de resumir y de explicar los **factores no humanos**.

Factores humanos

Al hablar de factores humanos, incluimos al software y/o malware, ya que los mismos fueron ideados y creados por personas. La responsabilidad no puede atribuirse a un programa por más que éste pueda reproducirse, actuar de forma independiente o tomar decisiones (de acuerdo con patrones) pues su génesis es humana.

El personal o los ex-empleados

Son los grupos más poderosos y los que más pueden sacar provecho de los datos. A propósito decimos **pueden**, ya que una amenaza no se da cuando el ataque cobra víctimas, sino cuando está en camino a concretarse.

Hackers, crackers y lamers

Se trata de muchos de los que intentan entrar en los sistemas de manera externa e interna. Si bien aquí han sido puestos en un mismo conjunto para poder manifestar los ataques más comunes externos e internos, estos grupos son muy diferentes entre sí y hasta se discriminan rotundamente.

- **Los hackers:** de por sí la palabra es un neologismo utilizado para referirse a un experto en las telecomunicaciones. El entendimiento que poseen estos atacantes es más profundo que el resto de las personas/técnicos, ya que tienen la habilidad de razonar igual o mejor que muchos de los programas o aplicaciones, y esto en realidad no es tan ilógico, ya que las computadoras y las utilidades que se encuentran instaladas en ellas fueron creadas por personas.



CONCIENTIZAR

Sin entrar en la paranoia, todo empleado es un posible atacante, ya que es la persona que tiene acceso a datos sensibles. Es por eso que hay que prevenir mediante la toma de conciencia y poniendo límites.

- **Los crackers:** cracker viene del inglés “crack”(romper) y justamente es lo que ellos hacen. Saben más o menos lo mismo que los hackers pero no comparten la ética. Por consiguiente, no les importa romper una arquitectura o sistema una vez dentro, ni tampoco borrar, modificar o falsificar algo; es por eso que la teoría habla de que: “los hackers son buenos y los crackers son malos”.
- **Los lamers:** se usa la palabra lamer o lammer para hablar en forma despectiva de de una persona que no posee los mismos conocimientos que tienen los expertos, pero que conserva la misma intención.
Más puntualmente, se denomina de esta manera a la persona que quiere aprender a ser un experto sin siquiera poner esfuerzo en aprender.
Más que nada, es una palabra que usan los hackers o crackers para discriminarse del “resto” y de los novatos que se quieren iniciar y no saben cómo, ni tampoco poseen la pasión que los expertos tenían cuando empezaron.
Hoy en día, también se emplea la palabra “luser” que es una mezcla del término “loser” (perdedor, fracaso) y el término “user”(usuario).

En la actualidad, un hacker puede romper un sistema, por ejemplo, porque lo despidieron del trabajo e impulsado por su deseo de venganza y en un ataque de furia, quiere demostrar lo que sabe de esa forma. Con este caso, queremos aclarar que se trata de personas, no hay malas o buenas, sino que a veces hay intenciones buenas y a veces hay intenciones malas.

Además, si vamos al caso, los hackers ya con meterse en un sistema están rompiendo “hipotéticamente” la seguridad, y **de principio**, el pilar de confidencialidad ya ha sido vulnerado por los propios “expertos”. No sólo están yendo en contravención con su ética, sino con la ley de propiedad, por ende, están cometiendo delito.

Otra forma más lógica de mostrar las relaciones no distantes entre ellos es de la siguiente manera:

El **hacker** pudo haber sido un lamer, y de vez en cuando puede usar mecanismos que usarían los crackers. Pero jamás volverá a ser un lamer. Un **cracker** de vez en cuando puede usar mecanismos de los hackers y, en realidad, a veces hace cosas pa-



DIVERSIFICACIÓN

Una intrusión puede no tener efecto usando los métodos individualmente. Por tal motivo muchas veces se combinan para sacar mayor provecho, y la persona encargada de la seguridad debe usar varios métodos para asegurar su sistema o red.

ra los lamers, por ende, ellos tampoco podrían serlo. Por último, los **lamers** pueden llegar a ser hackers y tener contacto con el cracking, pero generalmente esto sucede con una evolución radical o cuando el entorno –tanto laboral como familiar– hace posible que los libros estén a su alcance.

Los cliqueadores y los gecece

Esta diversificación salió del concepto **script-kiddie** (cliqueadores+gecece), pero es un concepto muy amplio; actualmente es necesario poder distinguir a las personas por el sistema operativo, porque el conocimiento no es igual. Una persona que sólo sabe manejar el mouse no sabe lo mismo que el que sabe escribir comandos y parámetros (que además sabe mover el mouse), aunque la facilidad de los mismos es semejante, la separación y la distinción de ambos es necesaria para saber qué grado de manejo de la computadora tienen.

Para un administrador un atacante es un atacante, no le va a importar las diferencias, pero cuando hablamos de novatos es importante diferenciar a los que “usan lo que le vino por defecto en la máquina (Windows)” contra “los que se animaron a cambiar y a probar otro sistema operativo (Unix)”.

Son personas que únicamente pueden lograr su cometido si son ayudadas por un programa. Este programa suele ser creado por hackers. Los denominamos así, diferenciando entre la gama Unix y la gama Windows. Los **cliqueadores**, en su gran mayoría, nunca usaron un entorno de consola, y si lo hicieron, fue en Microsoft DOS para poder usar el ping. En otras palabras, los cliqueadores sólo saben que haciendo clic (y muchas veces con un entorno gráfico demagógico) pueden explotar algunas vulnerabilidades, y así creerse y manifestarse como hacker.

Los **gecece** los denominamos así porque utilizan entorno de consola, aunque seguramente sólo por el hecho de que los programas para explotar vulnerabilidades están hechos en un lenguaje de programación que usa librerías no compatibles con el sistema operativo Windows.

Los programas para **explotar** (*exploits*), ya sean que estén escritos en Perl, C, Python o cualquier otro lenguaje, ponen a disposición de quien quiera su código fuente, es



PRIORIDADES DE LAS PREGUNTAS

En cualquier ataque o análisis de seguridad informática siempre hay que acordarse de que la primera pregunta nunca es ¿quién?, ¿por qué? o ¿de dónde?, sino que lo que hay que preguntarse es el **cómo**.

decir, que cualquiera que desee aprender una vulnerabilidad y saber cómo funciona ésta, sólo debería leer este código.

A esos jóvenes, que solamente saben ejecutar este código sin entenderlo, los llamamos aquí **gecece**, ya que **GCC** (*Gnu Compiler Collection*) es el compilador de lenguajes más difundido y conocido. Además, irónicamente, hemos puesto **gecece**, ya que la fonética sirve para los desentendidos de un idioma, y el GCC les convierte la ignorancia en un comando. Ejemplo: **gcc exploit.c** (siendo C el lenguaje) y, luego, con tan sólo ejecutarlo tienen la misma función que sus compañeros, los cliqueadores. Existe una palabra en la jerga que es utilizada para denominar a estos grupos: **script kiddie**.

Intrusos por paga

Este tipo de atacante tiene una particularidad muy especial: **sabe**.

A diferencia de la mayoría de las otras categorías, este individuo posee una sabiduría privilegiada y también es, por tal motivo, apto para recibir dinero por usar su experiencia en la seguridad en formas ilícitas.

Generalmente, no estamos hablando de una paga menor, sino que la mayoría de las veces la base de la retribución por el servicio comienza con cinco cifras. Y el trabajo que debe realizar o lo importante que es la empresa a la cual debe infiltrarse, es directamente proporcional a la paga. Habitualmente, las empresas que reciben este tipo de ataques son las más importantes que uno puede conocer.

Los cyberterroristas

Son personas que atacan con un fin específico: ya sea por ideologías o por puntos de vista. Por ejemplo, los cyberterroristas pueden atacar páginas que se manifiesten en contra de su religión o directamente pueden dejar inactivo servidores con ataques DoS.

Estas personas usan su conocimiento (bien puede tratarse de un lamer, un cliqueador o un **gecece**) para punto de vista personal en la concepción del entorno. En otras palabras, si él cree que en las elecciones tiene que ganar alguien, va a intentar manifestarlo anárquicamente.

El software con errores

Los programadores no son perfectos y, por ende, muchas veces el código con el que realizan sus trabajos contiene errores. Esos errores no son voluntarios y se encuentran en la mayoría de los códigos de cualquier programa, ya que la vulnerabilidad se debe a globalizar la manera en que programan para no acotar y que no funcionen ciertas cosas. Esas aberturas no están tan visibles y entendibles a código cerrado; por eso se encuentran más vulnerabilidades en los entornos Unix, que es de código abierto (**código fuente disponible**), razón por la cual un Unix actualizado es el sistema operativo más seguro.

Puertas traseras

Muchas veces los programadores dejan **atajos**, pero no de los que conocemos —como por ejemplo, **ALT+F4** para cerrar una ventana, o **CONTROL+ESC** para abrir el menú **Inicio** de Windows—, sino métodos no convencionales para traspasar autenticaciones, restricciones o simplemente métodos más largos para llegar al mismo lugar.

Otros métodos

Como hay muchos más métodos y factores, dejaremos las explicaciones de cada uno para más adelante y nombraremos a los restantes.

Los otros métodos pueden ser: virus, canales ocultos, gusanos, troyanos (caballos de Troya), conejos, bombas, etc.

Factores no humanos

Las amenazas ambientales, si bien dependiendo de la ubicación geográfica pueden tener más o menos periodicidad catastrófica, no son hechos que ocurran frecuentemente. Pero esto no es motivo suficiente para no considerar la circunstancia de que, si sucede, el daño será severo.

Las catástrofes más comunes son los terremotos, incendios, atentados, tormentas, etc. Existe un grupo poco conocido —más que nada por su arbitrariedad— denominado **riesgos de baja probabilidad**, que habla sobre los riesgos no comunes, que pueden ser desde que un avión se caiga sobre el edificio en donde están los servidores y la documentación, hasta que al encargado de la seguridad lo raptan personas de otro planeta. Obviamente, para este tipo de situaciones no hay contramedida.

RESUMEN

La seguridad informática abarca numerosas posibilidades de medidas y contramedidas, pero los pilares son siempre los mismos. En este capítulo, se explicó la base y se plantearon algunas terminologías y conceptos que hay que saber a la hora de poder armar una organización adecuada. Lo fundamental, más allá de la teoría, es poder tomar conciencia y analizar mentalmente cuáles son las posibilidades antes de que ocurra un ataque. El éxito de un administrador de seguridad es saber el cómo, para luego no tener que preguntarse el porqué.



TEST DE AUTOEVALUACIÓN

- 1** Mencione los cuatro pilares básicos de la seguridad informática y explique las diferencias que existen entre ellos.

- 2** ¿Cómo se llaman los códigos que explotan vulnerabilidades?

- 3** ¿Qué es una puerta trasera?

- 4** Cuando hablamos de una interceptación, ¿hablamos de un ataque contra qué pilar?

- 5** ¿Para qué se usa un sniffer?

- 6** El código abierto ¿tiene más bugs reportados que el cerrado?

- 7** ¿A qué clase de personas se las denominó gecece y por qué?

- 8** ¿Qué es lo fundamental a proteger?

- 9** Si hablamos de una tarjeta de identificación, ¿hablamos de un método de autenticación o de identificación?

- 10** Si han entrado en su sistema, ¿qué es lo primero que se pregunta?
