# ATAQUE Y DEFENSA COMO TÉCNICAS DE SEGURIDAD CONTRA AMENAZAS EN SISTEMAS DE INFORMACIÓN

Huertas Acosta Wilmer Fabián
huertas.wilmer@gmail.com
Universidad Piloto de Colombia

***Resumen***—En este artículo se describen dos técnicas que hacen parte de la Seguridad Informática: el hacking ético y la defensa en profundidad. El propósito no es determinar cuál es mejor, sino darlas a conocer y que cada experto en seguridad se sienta en la capacidad profesional de decidir cuál usar de acuerdo con las situaciones que enfrente en su entorno laboral.

***Abstract***—This article describes two techniques that are part of Computer Security: ethical hacking and in-depth defense. The purpose is not to determine which is better, but to make them known and that each security expert feels in the professional capacity to decide which one to use according to the situations that they face in their work environment.

***Índice de Términos***—Amenaza informática, barrera, defensa en profundidad, hacking ético, pentest, vulnerabilidad informática.

## I. INTRODUCCIÓN

Conforme avanzan y evolucionan las tecnologías de información, así mismo lo hace el entorno de las amenazas cibernéticas, el cual está presente en cada uno de los sistemas informáticos. Aunque se dice que no se puede garantizar la seguridad al 100%, se hace necesario desarrollar mejores métodos de protección frente a dichas amenazas. Con la aparición de nuevos vectores de ataques y amenazas persistentes avanzadas, queda más que claro que se le debe dar un enfoque más moderno a la ciberseguridad. Las técnicas tradicionales simplemente ya no resultan adecuadas para proteger la información frente a los ciberataques.

Lo que actualmente se conoce como "amenazas persistentes avanzadas", han evidenciado la capacidad que tienen para burlar las defensas de seguridad y mantenerse ocultas por mucho tiempo mientras se llevan a cabo acciones criminales. La única manera de descubrir el "cómo", "cuándo" y "dónde" es recrear las maniobras que un hacker malintencionado (más adelante veremos que el término, aunque muy usado, está mal empleado) llevaría a cabo dentro de un sistema de información. Es aquí donde nace el hacking ético y su método de pentest, el cual permite recrear paso a paso cada uno de los movimientos que llevaría a cabo un atacante si quisiera ingresar a un sistema. Aunque esta técnica es efectiva, no es la única, ya que también se puede optar por defender en vez de atacar, y es aquí donde sale a flote la defensa en profundidad, una técnica que consiste en fortalecer la defensa ya existente dentro de un sistema, haciendo uso de barreras que conforman líneas de defensa contra el atacante.

En este artículo, tanto el hacking ético como la defensa en profundidad se explicarán partiendo de una corta reseña histórica; luego se definirán ciertos conceptos que se deben tener claros antes de adentrarse en las dos técnicas; seguido de los tipos de pentest y las fases que lo componen. Y para finalizar, se hablará sobre la defensa en profundidad y el método que normalmente se utiliza.

## II. BREVE HISTORIA

No hay mejor forma de afrontar el presente y el futuro que conociendo el pasado. A través de los años, se han forjado historias de personajes que han llevado a cabo hazañas -tanto gloriosas como ilegales- dentro de sistemas informáticos. Unos para probar que su ingenio y habilidad son capaces de burlar cualquier sistema de seguridad, pero otros, lo hacen con fines explícitamente ilícitos. Sin embargo, debido a la gran confusión –y mal entendido- que puede llegar a generar el término "hacker", se termina asociando la palabra con criminalidad y

ciberdelincuencia. Los medios de información también han contribuido en gran parte a esto debido a que aún no han aprendido la lección de que los hackers malintencionados se deben llamar "crackers".

Para iniciar, la palabra *hacker* es un neologismo[1] utilizado para referirse a un individuo que es experto en una o varias ramas de la informática (como por ejemplo bases de datos, redes de computadores o programación). Las acciones propias llevadas a cabo por un hacker suelen denominarse "hackear" y "hackeo".

Curiosamente, el nacimiento de la palabra "hacker" se remonta aproximadamente en el año de 1960 donde en los laboratorios de sistemas y computación del Instituto Tecnológico de Massachusetts (MIT) aparecieron los primeros ordenadores, esas enormes computadoras que llegaban a ocupar cuartos enteros y utilizaban tarjetas perforadas. Los estudiantes más inteligentes y curiosos –los mal llamados "nerds"- hacían lo que fuera por acceder a estas máquinas el mayor tiempo posible. Al mismo tiempo que aprendían, mejoraban sus programas de computación, llevando al extremo este nuevo "juguete". Estos personajes terminaron autodenominándose "hackers".

Por otro lado, la palabra "*cracker*" deriva del inglés *crack* (que en español significa *romper*). Una vez apareció la cultura hacker, se dio a conocer por sus seguidores: personas con grandes habilidades y con la capacidad de burlar la seguridad de cualquier sistema informático, siempre manteniéndose al margen del ámbito legal. Pero poco tiempo después empezaron a emerger personas que, utilizando sus conocimientos en informática, aprovechaban errores y debilidades de algunos sistemas y los "crackeaban", en pocas palabras, burlaban la seguridad pisando el terreno de la ilegalidad. A estas personas se les siguió denominando "hackers", por lo que alrededor del año 1985, los hackers originales empezaron a nombrarlos "*crackers*" en contraposición al término "hacker" alegando defensa por mal uso del término.

### A. *El primer hacker*

A principios de los años 70's, un joven llamado John Draper descubrió la forma de realizar llamadas gratuitas nacionales e internacionales gracias a un curioso juguete que venía dentro del cereal llamado "Cap'n Crunch". Resulta que un amigo ciego de Draper llamado Joe Engressia le contó que se podía modificar el pequeño silbato de juguete para emitir un tono a 2600 Hz, la misma frecuencia que usaba en ese entonces la compañía de telefonía estadounidense AT&T para indicar que la línea telefónica se encontraba lista para rutear una llamada. Una vez realizado esto, se podía entrar en modo "operador", lo que permitía explorar las propiedades del sistema telefónico.

A partir de este descubrimiento, Draper desarrolló la llamada *Blue Blox* –o caja azul-, un dispositivo electrónico capaz de emular los tonos usados por la compañía de teléfonos, lo que le permitía realizar llamadas gratuitas. Una vez terminado, probado y en funcionamiento, quiso compartirlo entre sus contactos y amigos más cercanos (tales como Steve Jobs y Steve Wozniak).


Fig. 1. Juguete promocional del cereal Cap'n Crunch.
Fuente: *John T. Draper, El Capitán Crunch (Dragonjar, 2008)*.

Debido al fraude telefónico del que fue acusado por un juzgado norteamericano, John Draper fue arrestado en el año de 1972. Gracias a esta hazaña, se ganó el apodo de "Capitán Crunch".

Actualmente, aunque Draper ya se ha jubilado, rara vez se le ve trabajando como conferencista y consultor de seguridad informática.

### B. *El hacker más famoso*

Kevin Mitnick nació el 6 de agosto de 1963 en Estados Unidos. Desde muy pequeño tuvo gran pasión y habilidades con los sistemas y la informática. En la época de los 90's, llegó a ser considerado el cibercriminal más buscado por el FBI. Su fama se debía a sus innumerables accesos y penetraciones a los sistemas informáticos de diversas organizaciones gubernamentales y no

[1] Neologismo: (De neo-, el gr. λόγος lógos 'palabra' e –ismo): Vocablo, acepción o giro nuevo en una lengua.

gubernamentales. Durante su carrera como criminal informático, el método que más utilizó para tener acceso a los sistemas de manera ilegal fue la ingeniería social.

Su primer arresto fue en el año de 1983, cuando fue descubierto por un policía de la Universidad del Sur de California utilizando un computador para acceder por medio de ARPAnet[2] al sistema informático del Pentágono. Fue sentenciado a seis (6) meses de cárcel en una prisión juvenil de California.

Después de esto, tuvo otros problemas con la justicia americana, ya que en el año 1988 fue nuevamente arrestado por el FBI con una condena mínima de un (1) año y seis (6) meses. En 1992 fue objeto de otra investigación llevada a cabo por el FBI ya que se le acusó de ingresar ilegalmente a la base de datos comercial de la agencia de detectives TelTec donde él trabajaba. Pero cuando fueron a arrestarlo, había desaparecido sin dejar rastro.

Luego de quedar en libertad en el año 2000 y de una "rehabilitación", Mitnick fundó su propia compañía de consultoría llamada *Mitnick Security Consulting LLC*. Ha publicado varios libros referentes a la seguridad informática y al igual que Draper, se desempeña en algunas ocasiones como conferencista.

### *C. El ejército romano y la defensa en profundidad*

Originalmente el término defensa en profundidad -también conocido como "defensa elástica"- es una palabra proveniente de la jerga militar. El arquitecto italiano Vitruvio, alrededor del siglo I a.C. fue quien lo utilizó por vez primera y sostenía que "el acceso a las plazas debe dificultarse mediante diversos métodos entre los que necesariamente deberían incluirse la combinación de fosos y murallas".

Esta estrategia de defensa consiste en colocar varias líneas consecutivas en vez de una línea única muy fuerte. De este modo, el empuje inicial del atacante se va perdiendo conforme intenta avanzar y superar las líneas de defensa colocadas, logrando así que se disperse su fuerza y al mismo tiempo se debilite. Así, el defensor logra ganar tiempo para reorganizarse y posteriormente, atacar el punto más debilitado de su enemigo.

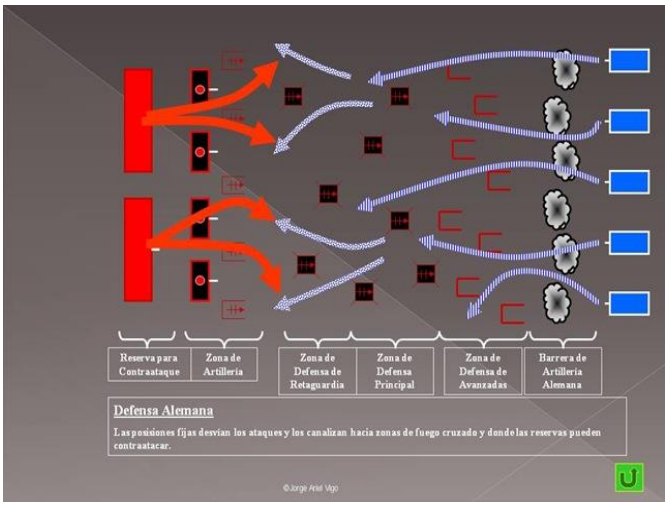


Fig. 2. Modelo base de la defensa en profundidad.
Fuente: *Defensa en profundidad – Defensa elástica (Salazar, 2012).*

La defensa en profundidad fue utilizada por el ejército romano, cuyo objetivo era ambiguo: el primero persuadir a su enemigo, y el segundo, si éste decidía llevar a cabo un ataque, que se fuese debilitando al intentar quebrantar las diferentes líneas de defensa y de este modo, lograr su aprehensión.

## III. CONCEPTOS

### *A. Hacker*

Individuo con una o más habilidades en el campo de la informática –tales como lenguaje de programación, bases de datos o redes de computador- las cuales usa para acceder a sistemas informáticos (algunas veces lo hace contando con autorización del dueño del sistema). Actualmente, los hackers se pueden clasificar en tres (3) tipos: hacker de sombrero blanco (White Hat), hacker de sombrero negro (Black Hat) y hacker de sombrero gris (Grey Hat).

### *B. White Hat (sombrero blanco)*

Persona que utiliza sus conocimientos para detectar vulnerabilidades en un sistema para posteriormente reportarlas al responsable y contribuir a la solución de las mismas. Sus actos no se desarrollan bajo fines ilícitos ya que normalmente actúan bajo consentimiento del propietario del sistema atacado.

[2] ARPAnet (Advanced Research Projects Agency Network): fue una red de computadoras creada por el Departamento de Defensa de los Estados Unidos y fue usada para intercomunicar instituciones estatales y académicas. El primer nodo se desarrolló en la Universidad de California.

### *C. Black Hat (sombrero negro)*

Persona que utiliza sus conocimientos para detectar vulnerabilidades y debilidades en un sistema informático. A diferencia de los White Hat, sus fines son la gran mayoría de veces lucrativos, extorsivos y destructivos.

### *D. Grey Hat (sombrero gris)*

Persona que se dedica a traspasar y burlar los niveles de seguridad de un sistema informático de una empresa, para luego ofrecer sus servicios como consultor. Es decir, atacan los sistemas para demostrar su habilidad y luego lo defienden. Se puede decir que un sombrero gris se encuentra entre el limbo entre un sombrero blanco y un sombrero negro, pero solamente su actitud y ética le permite tomar la mejor decisión sobre los comportamientos más adecuados de acuerdo a la situación a la que se enfrenta.

### *E. Cracker*

Individuo que utiliza sus conocimientos para detectar vulnerabilidades en un sistema y aprovecharse de las mismas para lucrarse de ello –normalmente monetario-. Los crackers son también conocidos como Black Hat (sombrero negro), aunque ninguno de estos dos términos suele usarse correctamente, por lo que constantemente se les confunde con los hackers.

### *F. Hacking ético*

Se puede definir como la utilización de los conocimientos relacionados con seguridad informática para ejecutar pruebas en sistemas informáticos, redes de telecomunicaciones o dispositivos electrónicos, con el propósito de detectar vulnerabilidades que explotar, reportarlas para tomar medidas sin poner en riesgo el sistema y tomar decisiones para solventar dichas vulnerabilidades. Este tipo de pruebas normalmente las lleva a cabo un hacker *White hat (sombre blanco)* y se les denomina “pentest” (en español *pruebas de penetración*).

### *G. Amenaza informática*

Una amenaza informática es todo evento, circunstancia y/o persona que tiene la capacidad y posibilidad de causar daño a un sistema en diversos modos (modificación, divulgación, destrucción o negación).

### *H. Vulnerabilidad informática*

Debilidad existente dentro de un sistema informático, que permite a un atacante violar los 3 principios de la seguridad de la información: *confidencialidad*, *integridad* y *disponibilidad*. Las vulnerabilidades son el resultado de defectos o fallos en el diseño del sistema. Aunque en un sentido más amplio, también pueden ser el resultado de limitaciones tecnológicas, porque en principio, no existe un sistema 100% seguro.

### *I. Exploit*

Programa informático malicioso (también conocido como *malware*) que tiene como objetivo utilizar y sacar provecho de una debilidad en otro programa o sistema. Los exploits suelen utilizar vulnerabilidades. Normalmente se corrigen mediante actualizaciones de software o parches de seguridad.

### *J. Ataque informático*

Cualquier acción que atenta contra la seguridad de un sistema informático.

### *K. Pentest*

Procedimiento sistemático y metodológico que intenta mediante diversos pasos recrear las acciones ofensivas de un atacante (del mismo modo en que éste las haría sobre un sistema informático) para lograr acceder a él, con el fin de descubrir y reparar problemas de seguridad. La persona que ejecuta dichas pruebas suele denominarse *pentester*.

### *L. Defensa en profundidad*

En el campo de la ingeniería de sistemas y de la información, es una técnica que representa el uso de múltiples metodologías de seguridad informática para cooperar a mitigar el riesgo de que un componente de la defensa esté en riesgo o sea evadido. Dicho enfoque de la seguridad que se ejecuta por numerosas capas, se realiza desplegando diversos productos de seguridad de varios proveedores (sea software o hardware), para defenderse de los numerosos vectores de ataque potencialmente conocidos, reduciendo así que el posible fallo en una defensa implique a un fracaso mayor.

### *M. Gravedad de un hecho de seguridad*

Calcula el impacto real del hecho en función de la criticidad del bien cuando un hecho tiene una

derivación directa sobre un bien, o el impacto potencial de este hecho sobre el bien amenazado en función de la cantidad de líneas de defensa restantes y de la criticidad de dicho bien. El hecho no tiene impacto sobre el bien sino sobre sus medios de defensa.

*N. Barrera*

Medio de seguridad idóneo que tiene por objetivo proteger una parte del sistema de información contra al menos una amenaza. Una barrera puede ser de tipo técnico o de procedimiento, dinámico o estático, automático o manual –incluso hasta humano-. Debe beneficiarse con un medio de control de su estado.

*O. Línea de defensa*

Agrupación de barreras que, situadas en un mismo lugar, tienen el objetivo de anular un posible ataque llevado a cabo por una amenaza a un sistema informático.

La superación de dichas barreras provoca un incidente cuya gravedad depende de la cantidad de barreras que queden en pie por superar por la amenaza (o las amenazas) para alcanzar el bien (o los bienes protegidos), y depende también del valor de estos bienes, es decir que un incidente de seguridad está asociado a un nivel de gravedad que indica si la línea de defensa fue superada. Para ser una línea y no un conjunto de medios de protección, toda línea de defensa debe contar con medios de detección/monitoreo, de notificación y dispositivos.

## IV. TIPOS DE PENTEST

El pentest es llevado a cabo por un hacker ético profesionalmente calificado y con las habilidades pertinentes para ejecutar las distintas fases que comprenden este procedimiento. Hace uso de herramientas tanto libres como comerciales (no hay restricción alguna). Lo más importante es tener claro el objetivo: descubrir la mayor cantidad de fallos de seguridad como sea posible. Actualmente se conocen 5 tipos de pentest y son:

*A. Por el conocimiento del objetivo*

- **Pruebas de caja blanca:** en este escenario el pentester no cuenta con ningún tipo de información acerca de la estructura o la red de la organización que está intentando penetrar. Bajo sus propios medios intenta descubrir la información que necesita.
- **Pruebas de caja gris:** pruebas donde el pentester cuenta con información parcial acerca de la organización y su red (por ejemplo, el nombre del servidor de dominio).
- **Pruebas de caja negra:** acá el pentester es provisto con toda la información necesaria para llevar a cabo el proceso de pentest.

*B. Por el origen de las pruebas*

- **Pruebas internas:** este tipo de pruebas se enfoca principalmente en la red, infraestructura, servidores o software que esté ejecutándose en la infraestructura. En este caso, el pentester ético intenta atacar usando redes públicas a través de Internet. Se intenta piratear la infraestructura de la organización atacando páginas web, servidores web, servidores DNS públicos, etc.
- **Pruebas externas:** en estas pruebas el pentester ya se encuentra dentro de la red de la organización y conduce sus pruebas desde allí.

## V. FASES DEL PENTEST

Como todos los proyectos alineados a la ingeniería, el hacking ético cuenta también con diversas metodologías y un set de fases que más allá de indicarle “el cómo”, le ayuda al experto en seguridad a estructurar mucho mejor su trabajo.

Las fases del pentest varían unas de otras dependiendo de la metodología y/o autor. Sin embargo, lo que realmente importa es tener claro el objetivo de cada fase y sus respectivas salidas:

1) **Reconocimiento:** el reconocimiento es la fase donde se obtiene información acerca del objetivo usando medios activos o pasivos. Las herramientas más comunes para llevar a cabo esta tarea son NMAP, Hping, Maltego y Google Dorks.
2) **Escaneo:** en esta fase se comienza a probar el sistema objetivo (o red) en busca de vulnerabilidades que puedan ser explotadas. Las herramientas más comunes para esta labor son Nessus, Nexpose y NMAP.
3) **Obtener acceso:** cuando se tiene la vulnerabilidad detectada, se intenta explotarla para conseguir acceso al sistema objetivo.

Metasploit es una herramienta útil para lograr el acceso.

4) **Mantener acceso:** en esta fase ya se ha logrado el acceso al sistema. Una vez allí, se instala algún software (como un backdoor) para entrar al sistema cada vez que se requiera. Metasploit es una herramienta que puede hacer dicha tarea.
5) **Borrar huellas:** este proceso se considera una actividad "anti-ética", ya que el objetivo es borrar todos los logs de las actividades que tomaron lugar durante el proceso de hacking. Suele ejecutarse únicamente por el black hat.
6) **Reporte final:** aquí se termina el proceso del pentest. Se consolida un reporte con los hallazgos y el trabajo realizado, así como las herramientas utilizadas, la tasa de éxito, vulnerabilidades encontradas y el proceso de explotación de estas.

A continuación, se detalla cada una de las fases anteriormente mencionadas:

*A. Reconocimiento*

También conocido como "descubrimiento", es el preparativo del pentest. El propósito es conseguir la mayor cantidad de información del sistema objetivo como sea posible (por ejemplo, dominios y subdominios, servicios publicados, información personal, correos electrónicos, archivos con información sensible, identificar máquinas activas, descubrir puertos abiertos y puntos de acceso). El reconocimiento normalmente puede ser de dos tipos:

- **Reconocimiento activo:** en este proceso se interactúa directamente con el sistema para obtener información. Esta información puede ser relevante y precisa. Pero existe el riesgo de llegar a ser detectado si se está planeando un reconocimiento activo sin permiso. Si se detecta, entonces el administrador del sistema puede tomar medidas severas contra el autor de la acción y rastrear las actividades posteriormente.
- **Reconocimiento pasivo:** a diferencia del reconocimiento activo, en este no se está conectado directamente al sistema informático. Este proceso es utilizado para recopilar información esencial sin tener que interactuar con los sistemas objetivo.

Las técnicas más comunes en la fase de reconocimiento son:

- **Google Hacking:** técnica de obtención de información (en inglés *information gathering*) que hace uso de las altas capacidades del motor de búsqueda Google para buscar información. Las búsquedas pueden refinarse para lograr encontrar datos específicos por medio del uso de operadores avanzados y operadores lógicos (tales como AND, OR o NOT).
- **Ingeniería social:** técnica que consiste en manipular psicológicamente a las personas para que compartan información sensible o para que lleven a cabo acciones inseguras. En la mayoría de casos, los ataques se realizan mediante correo electrónico o por teléfono. Los atacantes se hacen pasar por otra persona y convencen a la víctima para entregar información confidencial de la organización (o sus usuarios y contraseñas). Como es un tema más humano que tecnológico, ni el hardware ni el software que implementan las compañías pueden prevenir los ataques. Debido a esta vulnerabilidad, los atacantes se aprovechan y recurren a este tipo de tácticas para vulnerar sistemas seguros y muy complejos.
- **Escaneo de puertos:** técnica que permite analizar por medio de un programa el estado de los puertos de una máquina que se encuentra conectada a una red de telecomunicaciones. Se puede llegar a detectar si un puerto está abierto, cerrado, o protegido por un cortafuegos. Esta técnica se utiliza para detectar qué servicios comunes está ofreciendo la máquina y las posibles vulnerabilidades de seguridad que pueden haber de acuerdo a los puertos que se encuentren abiertos. En algunos casos también se puede llegar a detectar el sistema operativo que está corriendo sobre la máquina.

*B. Escaneo*

En esta fase se aplica la información obtenida en la fase de reconocimiento con el propósito de

detectar posibles vectores de ataque dentro de la infraestructura del sistema de información. Para esto, se puede utilizar el escaneo de puertos y el escaneo de servicios del objetivo.

Se determinan qué puertos se encuentran abiertos y después, se asocia el puerto a un servicio en particular. Una vez finalizado este proceso, se procede a realizar el escaneo de vulnerabilidades (éste permitirá encontrar vulnerabilidades en el o los equipos objetivo, tanto de las aplicaciones como del sistema operativo).

Conceptualmente, esta fase se puede dividir en seis sub-etapas. En cada una de éstas se tiene como objetivo hallar la mayor cantidad de información posible, desde los equipos que se encuentran online en una red o segmento de red, hasta la planificación del propio ataque. En algunos casos, ciertas herramientas cubren varias etapas juntas en un mismo análisis. Estas etapas son:

1) Detección de sistemas informáticos activos.
2) Escaneo de puertos.
3) Detección del sistema operativo.
4) Identificación de servicios.
5) Escaneo de vulnerabilidades.
6) Planificación del ataque.

Inicialmente, la manera más sencilla de comprobar si un host está activo o no es a partir del "ping sweep", técnica que consiste en enviar paquetes ping por broadcast a los hosts de una red. Si responde, significa que está online y que es un objetivo claro y vulnerable para atacar.

En dado caso que el escaneo realizado con ping sweep no detecte hosts activos, no significa que éstos no existan. Suele combinarse como complemento de otras técnicas, ya que por sí sola no muestra información muy precisa.

En la segunda etapa del análisis de los puertos abiertos es el complemento perfecto que se mencionaba anteriormente para el ping sweep: si a un equipo se le pueden analizar los puertos, esto significa que se encuentra activo. Para este análisis se pueden usar distintos tipos de escaneos que utilizan diversas propiedades del protocolo TCP tales como *SYN stealth scan, FIN scan, XMAS tree scan, NULL scan, FIN scan*, entre otros.

La tercera etapa -la de detección del sistema operativo- se realiza a partir de las respuestas que el host brinda frente a ciertos paquetes. Todo sistema operativo tiene su implementación del protocolo TCP, y responde de manera autónoma y diversa a ciertos paquetes que son interpretados por la aplicación una vez son recibidos.

Llegando a la cuarta etapa, está la identificación de servicios. Esto se puede obtener a partir del *"banner grabbing"*, que implica obtener información de la aplicación con la lectura de banners[3] predeterminados.

Una vez se tengan los datos recopilados en las anteriores etapas, se inicia el escaneo de vulnerabilidades –también conocido como *análisis de vulnerabilidades*-. Depende de los servicios que se estén ejecutando (web, e-mail, FTP, etc.) del sistema operativo del equipo objetivo (Windows, Linux, Solaris, Mac OSX) y la aplicación (IIS, Apache, entre otros), se podrá identificar la existencia de vulnerabilidades conocidas y de este modo llegar a explotarlas posteriormente.

Para finalizar, la planificación del ataque tendrá como propósito llevar a cabo el proceso de ocultación de huellas del ataque. En pocas palabras, no dejar rastros de lo que se hizo ni cómo se hizo.

### *C. Obtener acceso*

Cuando se tengan detectadas las vulnerabilidades, el gran paso es obtener acceso al sistema definido como objetivo. En el caso en que esto se realice bajo el marco de una simulación parte del pentest y llevado a cabo por profesionales calificados, no se suele tomar control sobre el sistema sino más bien se enfoca en detectar las vulnerabilidades y proponer soluciones. Pero si fuese un ataque o simulación más realista, esta fase será quizá la más desafiante, ya que aquí se utilizan todos los recursos y conocimientos técnicos.

En el momento en que sea detectada una vulnerabilidad, se buscará un exploit que permita explotarla y obtener el control del objetivo. Este proceso puede llevarse a cabo de forma manual o mediante algún programa de explotación (tales como Immunity Canvas, Metasploit Framework o Core Impact). Actualmente, existen varios recursos online donde se puede conseguir información sobre las vulnerabilidades y los exploits (por ejemplo,

[3] Banner: un banner es una leyenda que traen las aplicaciones donde se brinda información sobre esta mismas, como la arquitectura o la versión.

Common Vulnerability Scoring System, Open Source Vulnerability Database, Milw0rm, BugReport, Bugtraq, Common Vulnerabilities and Exposures y Packet Storm).

De acuerdo al tipo de exploit ejecutado, puede ser que el acceso obtenido no brinde los privilegios que se desean, y será necesario escalar privilegios con el fin de poseer control total del sistema atacado. Una de las maneras más típicas de escalar privilegios es, cuando se esté ingresando al sistema, usar otro exploit local que otorgue privilegios de administrador (Administrador o System para Windows y Root para Unix/Linux).

Al momento de obtener los privilegios deseados, el siguiente paso suele ser ejecutar aplicaciones o comandos de forma remota en el sistema atacado (se pueden usar herramientas como PsExec de Sysinternals). Para esto, es necesario haber establecido previamente un canal de comunicación entre el equipo atacante y víctima.

Si lo anterior no llegase a funcionar, se suele utilizar la ingeniería social, donde se engaña al usuario solicitándole por algún medio (e-mail, mensajería instantánea, etcétera) que realice una determinada acción. Lo que el usuario no sabe es que dicha acción explotaría una vulnerabilidad y brindaría acceso remoto al atacante.

### *D. Mantener acceso*

Una vez se obtiene el acceso al objetivo, lo que realmente desea un atacante es mantener el equipo comprometido. Para ello busca la forma en que el acceso conseguido sea perdurable el tiempo que requiera. La mayoría de veces esto se consigue a partir de la instalación y ejecución de algún software malicioso (tales como troyanos, keyloggers, backdoors, spyware, entre otros). Si bien el comportamiento puede variar de acuerdo al software, el resultado siempre será el mismo: el atacante podrá retomar el acceso al equipo comprometido cuantas veces y cada vez que lo desee.

### *E. Reporte final*

La presentación del reporte final es la última etapa del pentest donde se detallan los resultados obtenidos durante la ejecución de cada fase de las pruebas de penetración.

Se debe realizar de una forma asertiva, clara, completa, ordenada y considerando el perfil, conocimiento e interés del lector a quien va dirigido. El reporte final puede subdividirse en dos:

1) **Reporte técnico:** dirigido especialmente a grupos encargados de la remediación de problema, a líderes técnicos del proyecto, analistas del área de TI o de seguridad. Contiene un compilado detallado técnico y debe ser exhaustivo. Esta clase de reportes son una herramienta útil para la toma de decisiones de tipo técnico. Un reporte de este tipo consta de lo siguiente:

- **Introducción:** se describen los antecedentes, entorno y partes interesadas del proyecto. Se detalla una breve descripción de la empresa o del consultor.
- **Objetivos:** se describe brevemente los objetivos del proyecto. Si se requiere, incluir requerimientos normativos.[4]
- **Alcance:** en esta sección se deben especificar los tipos de pruebas llevados a cabo (análisis de vulnerabilidades, pentest, interno o externo, caja blanca o caja negra, etc.). Mencionar el lugar donde se llevaron a cabo las pruebas, número de aplicaciones probadas, redes o activos involucrados, tiempo y periodicidad de ejecución de las pruebas.
- **Metodología:** se detallan las etapas y una descripción de cada una (descubrimiento y enumeración, análisis de vulnerabilidades, pruebas de penetración, etc.). Mencionar las herramientas que se utilizaron (Nessus, Nikto, Accunetix, etc.). Se mencionan las metodologías o guías utilizadas (Metodología del EC-Council, OSSTMM, OWASP, etc.).
- **Resultados:** en esta etapa se detallan los resultados técnicos obtenidos en cada una de las etapas. Adicional, se coloca el inventario de activos y una descripción de la información obtenida en la etapa de descubrimiento. También se coloca el inventario de vulnerabilidades encontradas con descripción, código CVE, el puntaje CVSS[5], información adicional, links de referencia,

[4] Requerimientos normativos: normas que sustentan la aplicación y ejecución de pruebas de penetración y análisis de vulnerabilidades (circular 052, PCI DSS, ISO 27001)

[5] CVSS: Es un sistema de puntaje de vulnerabilidades diseñado para proporcionar un método estandarizado y abierto para calificar vulnerabilidades de TI.

recomendaciones de remediación, evidencia de resultados de penetración.
Se recomienda apoyarse en gráficas (como distribución de vulnerabilidades de acuerdo a su criticidad, servidores y puertos más vulnerables, vulnerabilidades más comunes, clasificación por tipo de vulnerabilidad, parches de sistema operativo, configuraciones por defecto, vulnerabilidades de productos, etc.

- **Conclusiones y recomendaciones:** es el análisis de los resultados. Discusión de los aspectos más relevantes, principales problemas o situaciones críticas. Se detallan recomendaciones de remediación (no es una lista de lo que entregan los reportes de las herramientas, sino la unificación de un análisis global de los resultados y una guía de cuál es el mejor camino a seguir). Se describen las acciones más contundentes y de menor costo.
- **Anexos:** se recomienda anexar distintos soportes que ayuden a sustentar el reporte tales como tablas dinámicas o archivos Excel.

2) **Reporte ejecutivo:** presentación resumida de resultados relevantes. Dirigido a gerentes y directores. Se debe minimizar el uso de lenguaje técnico especializado. Debe ser comprensible para un lector sin conocimientos en el tema. Contiene las mismas secciones que el reporte ejecutivo, pero acá se presentan resultados resumidos teniendo en cuenta el público a quien va dirigido. Es recomendable usar nombres de aplicaciones en lugar de direcciones IP o describir los servidores de acuerdo a los servicios que presta. También se usan gráficas estadísticas, pero de aspectos generales como la cantidad de vulnerabilidades, número de equipos comprometidos, facilidad de la explotación, etc. Los resultados se deben presentar en términos del nivel de riesgo y del tipo de consecuencias para la organización.

## VI. DEFENSA EN PROFUNDIDAD

La defensa en profundidad de un sistema de información es una defensa global y dinámica que acopla de una forma ordenada varias líneas de defensa que abarca todo el sistema. El concepto "profundidad" se requiere comprender en su noción más extensa, es decir, en la constitución del sistema de información, en su implementación y, por último, en las tecnologías involucradas y utilizadas. Lo que significa facultar medidas de neutralización de los atentados contra la seguridad a un costo menor, por medio de la correcta y efectiva gestión de los riesgos, un sistema idóneo de informes, la correcta planificación de las acciones y reacciones y el constante enriquecimiento gracias a la experiencia adquirida.

La defensa en profundidad tiene doble propósito: i) ofrecer un canal de comunicación que proporcione a los directos responsables de la toma de decisiones y a los usuarios en particular, concientizarse de la gravedad e importancia de los incidentes de seguridad que se presentan dentro y fuera de la organización ii) fortalecer la protección del sistema de información mediante un enfoque cualitativo que posibilite verificar la finalización y la calidad del dispositivo final.

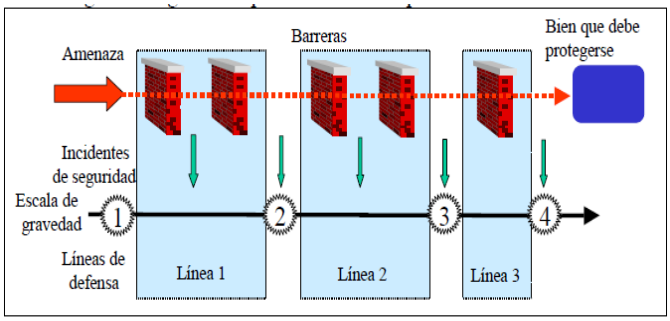


Fig. 3. Procedimiento de identificación de líneas de defensa.
Fuente: *La defensa en profundidad aplicada a los sistemas de información (Secrétariat général de la défense nationale Direction centrale de la sécurité des systèmes d'information, 2004).*

El término de defensa en profundidad obedece a 6 grandes principios generales. Cada uno de estos principios puede existir de forma individual, pero la profundidad de la defensa la proporciona la combinación de éstos. A continuación, se detalla cada uno:

TABLA I
PRINCIPIOS DE LA DEFENSA EN PROFUNDIDAD

| Título | Naturaleza |
|---|---|
| *Coordinación* | **La defensa debe ser dinámica, lo que significa que el sistema de información dispone de una política de seguridad que identifica:**<br>a) una capacidad de reacción<br>b) una planificación de las acciones<br>c) una escala de gravedad. |
| *Demostración* | **La defensa debe ser demostrada, lo que significa que:**<br>a) se califica a la defensa<br>b) existe una estrategia de homologación |

| | |
|---|---|
| | c) la homologación acompaña al ciclo de vida del sistema de información. |
| *Dinamismo* | **La defensa debe ser dinámica, lo que significa que el sistema de información dispone de una política de seguridad que identifica:**<br>a) una capacidad de reacción<br>b) una planificación de las acciones<br>c) una escala de gravedad. |
| *Exhaustividad* | **La defensa debe ser completa, lo que significa que:**<br>a) los bienes que deben protegerse se protegen en función de su criticidad<br>b) que cada uno de ellos está protegido, como mínimo, por tres líneas de defensa<br>c) se formaliza la difusión de la experiencia adquirida. |
| *Globalidad* | **La defensa debe ser global, lo que significa que engloba todas las dimensiones del sistema de información:**<br>a) aspectos organizacionales<br>b) aspectos técnicos<br>c) aspectos de implementación. |
| *Suficiencia* | **La defensa debe ser suficiente, lo que significa que cada medio de protección (organizacional o técnico) debe contar con:**<br>a) una protección propia<br>b) un medio de detección<br>c) procedimientos de reacción. |

Fuente: *La defensa en profundidad aplicada a los sistemas de información (Secrétariat général de la défense nationale Direction centrale de la sécurité des systèmes d'information, 2004).*

## VII. EL MÉTODO DE DEFENSA EN PROFUNDIDAD

La palabra "defensa" –en lugar de seguridad- implica fuertes ideas, ya que contribuye las nociones de iniciativa, libertad de acción y dinámica, de funcionamiento en modo funcionalidad reducida, etc., y no se limita al uso de medios de protección pasivos. El concepto de defensa en profundidad se puede adaptar a todos los niveles de un sistema de información, desde el más microscópico, hasta el más macroscópico (como por ejemplo la implementación de un algoritmo o la evaluación de un producto).

Una barrera (y una línea de defensa) puede cubrir una o más amenazas y su superación causa un denominado "incidente de seguridad", cuya gravedad depende únicamente de la cantidad de líneas de defensa que hagan falta por superar, y por supuesto, del valor de los bienes que se estén protegiendo. El método faculta al experto en seguridad integrar los principios anteriormente nombrados. Dicha integración permite calificar el sistema y en cierto modo, medir su nivel de defensa. Para poder cumplir este objetivo, el método parte de la hipótesis de que ya se ha hecho un análisis de riesgos previamente. A continuación, se detalla cada una de las etapas del método:

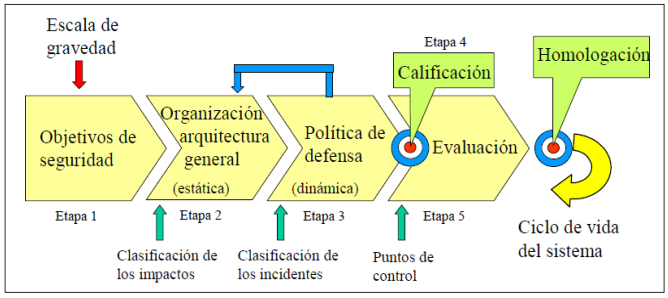


Fig. 4. Etapas del método de defensa en profundidad.
Fuente: *La defensa en profundidad aplicada a los sistemas de información (Secrétariat général de la défense nationale Direction centrale de la sécurité des systèmes d'information, 2004).*

### A. *Primera etapa: determinación de los bienes y de los objetivos de seguridad*

En esta primera etapa se requiere determinar los bienes que se van a defender y su grado de criticidad (el análisis de riesgos debe permitir medir el valor de la defensa: la fiabilidad de un equipamiento debe ponderarse por medio del valor de la consecuencia de su pérdida para así poder graduar el nivel de alerta). Una vez concluida esta tarea, se identifican los actores del modelo y se definen las necesidades de seguridad. Es importante tener en cuenta la escala de gravedad para clasificar los hechos de seguridad en función del impacto sobre el sistema informático. Dicha escala está inspirada en la escala INES[6], pero se basa únicamente en el impacto del hecho:

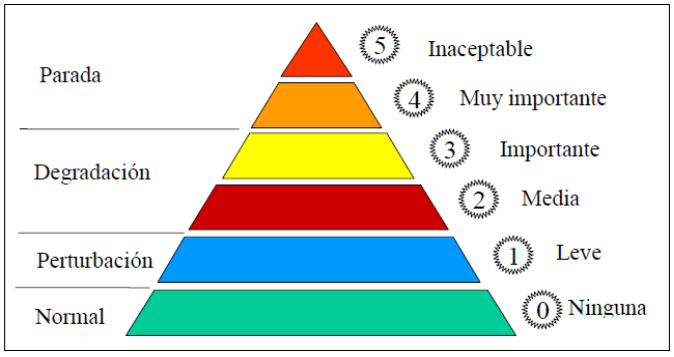


Fig. 5. Escala de gravedad.
Fuente: *La defensa en profundidad aplicada a los sistemas de información (Secrétariat général de la défense nationale Direction centrale de la sécurité des systèmes d'information, 2004).*

[6] INES: (International Nuclear Event Scale) fue introducida por el Organismo Internacional de Energía Atómica (OIEA) para permitir la comunicación sin falta de información importante de seguridad en caso de accidentes nucleares y facilitar el conocimiento de los medios de comunicación y la población de su importancia en materia de seguridad

TABLA II
ESCALA DE GRAVEDAD EN UN SISTEMA DE INFORMACIÓN

| Categoría | Nivel | Gravedad | Criterio |
|---|---|---|---|
| Parada | 5 | Inaceptable | El hecho cuestiona la supervivencia de la empresa (el hecho temido ocurre) |
| | 4 | Muy importante | El hecho presenta un riesgo muy importante y necesita medidas de urgencia inmediatas. |
| Degradación | 3 | Importante | El hecho no ocasiona riesgo importante alguno pero se toca una parte significativa del sistema |
| | 2 | Media | El hecho tiene una consecuencia sobre el funcionamiento normal y debe generar una reacción inmediata |
| Perturbación | 1 | Leve | El hecho no tiene consecuencias notables pero debe tratarse para restablecer un funcionamiento normal |
| Funcionamiento normal | 0 | Ninguna importancia desde el punto de vista de la seguridad | Funcionamiento normal |

Fuente: *La defensa en profundidad aplicada a los sistemas de información (Secrétariat général de la défense nationale Direction centrale de la sécurité des systèmes d'information, 2004).*

Es significativo que el análisis llevado a cabo en esta etapa sea el resultado de la combinación y de la validación mutua de un enfoque deductivo (por los recursos) luego inductivo (por las amenazas) y que el factor humano sea tenido en cuenta.

### *B. Segunda etapa: arquitectura general del sistema*

Se determina la profundidad del sistema y se realizan elecciones sobre la organización, procedimientos de seguridad y las tecnologías involucradas. Para llevar a cabo dichas elecciones y lograr identificar los puntos más críticos y sensibles a las distintas amenazas, este método aconseja usar un enfoque natural –y el más comúnmente empleado- que consiste en partir de la amenaza y prever las distintas líneas de defensa hasta llegar al bien que se pretende defender. Luego el experto en seguridad se encarga de desarrollar un enfoque deductivo partiendo del bien que se quiere defender hacia la amenaza, con el propósito de implementar provisionalmente nuevas líneas y al mismo tiempo identificar dentro del sistema los puntos más expuestos. Es importante identificar lo siguiente:

- Distribución de las zonas en ámbitos de confianza.
- Repartición privada/común en cada ámbito y entre ámbitos.
- Determinación de las barreras (medio humano, de procedimiento y técnico).
- Clasificación de las zonas en función de su sensibilidad y la determinación de las reglas de paso de una a la otra.
- División de las zonas en función de los actores, riesgos, y las principales funciones de la organización.

En esta etapa es imprescindible constituir un "cuadro de medidas" tomadas con el objetivo de exponer los medios de defensa en toda la profundidad. Así mismo, configurar los sistemas críticos con el objetivo de evaluarlos y determinar los incidentes (superación de una barrera) en una escala de gravedad –la misma escala fijada en la primera etapa de este método- en función de la clasificación de los impactos, ya que facultará contribuir a nivel de la política operativa, la graduación de las acciones y especificar las líneas de defensa.

Esta etapa debe llevarse a cabo normalmente al inicio del proyecto, lo que significa que un estudio de seguridad previo debe estar integrado en el proyecto. Si el sistema ya existe, el método se aplica de la siguiente manera:

- Analizar la topología que se encuentra implementada dentro del sistema de información (tanto técnica como funcional).
- Valorar la arquitectura existente para fijar las nuevas modificaciones que se deben contribuir con el propósito de responder a las amenazas.
- Identificar las barreras existentes.
- Modelizar los procesos más críticos e importantes.

### *C. Tercera etapa: elaboración de la política de defensa*

Se compone de dos (2) sub-etapas:

1) Determinación de la defensa global y coordinada:

- Detección de los ataques y determinación de los puntos de control.
- Correlación de los hechos.
- Envío de la información.
- Alerta.

2) Planificación:

- Determinar si existen nuevas configuraciones (con funcionamiento normal y con funcionamiento en modo degradado).
- Planes de reacción.

La defensa global se da de acuerdo a los tres (3) ejes (tecnológico, organizacional e implementación) que constituyen las líneas de defensa empleadas en las zonas definidas en la etapa dos (2) del presente método. Cada una de estas líneas dispone de tres (3) funciones de seguridad:

- Protección.
- Detección.
- Reacción.

Para cada uno de los incidentes de seguridad que surjan, la política de seguridad debe decretar su nivel de gravedad con el propósito de beneficiarse con "el aporte pedagógico" del método que posibilita una mayor sensibilización por parte del personal. De acuerdo a la cantidad de líneas de defensa restantes, se deducirán los niveles de gravedad de los incidentes. Dicha gravedad depende mucho más de los medios de defensa restantes que de aquellos que han sido superados.

La defensa tiene –y debe- ser coordenada y global (todos los medios participan por cumplir con el objetivo de seguridad). Esta coordinación concierne primordialmente a los medios de información –*posibilita precisar la amenaza real por medio del análisis de diversas informaciones relacionadas a un ataque en curso*- y de reacción -*configuración nueva de medios de defensa a partir de la localización de otro medio de defensa*- (la coordinación concierne más a las barreras que a las mismas líneas de defensa).

Tanto los accidentes como los incidentes deben clasificarse de acuerdo a la escala de gravedad y emprender obligatoriamente una reacción:

- De nivel técnico (respuesta automática).
- De procedimiento (aplicación del procedimiento o del correspondiente plano).
- De tipo humano (iniciativa, decisión, etc.).

Ciertamente, en el marco de la defensa en profundidad, se debe predecir la consideración de varios incidentes al mismo tiempo. Los planos de reacción deben ser acoplados en el mismo sentido que los ataques a la seguridad, con el fin de fortificar las medidas en función del nivel de gravedad.

Entre las medidas no técnicas que se deben tener en cuenta llevar a cabo, se requiere prever aquellas acciones que atentan la integridad contra personal externo, al igual que aquellas previstas en el reglamento interno contra el personal de la organización.

### *D. Cuarta etapa: calificación de la defensa en profundidad*

En esta etapa lo que se quiere conseguir es la calificación del sistema –validar la organización y la arquitectura-. Se realiza desde dos (2) enfoques: *cualitativo* y *demostrativo*, y se lleva a cabo por medio del estudio de las situaciones aplicables:

- **Enfoque cualitativo:** este enfoque se centra principalmente en verificar el cumplimiento de los principios de la defensa en profundidad estipulados en el presente método. Se relaciona de forma similar al procedimiento de calidad tratado en el capítulo 7 de la norma ISO 15408[7], que permite argumentar el carácter exhaustivo de los objetivos de seguridad respecto de las amenazas seleccionadas.
- **Enfoque demostrativo:** este enfoque apunta a que el método de calificación debe ser coherente con el método de defensa global de defensa en profundidad tal y como fue diseñado, y debe basarse en los resultados producidos a lo largo de las diferentes etapas del método.

[7] ISO/IEC 15408-1:2009: norma que establece los conceptos y principios generales de la evaluación de seguridad de TI y especifica el modelo general de evaluación dado por varias partes de ISO / IEC 15408 que en su totalidad debe utilizarse como base para la evaluación de las propiedades de seguridad de los productos de TI.

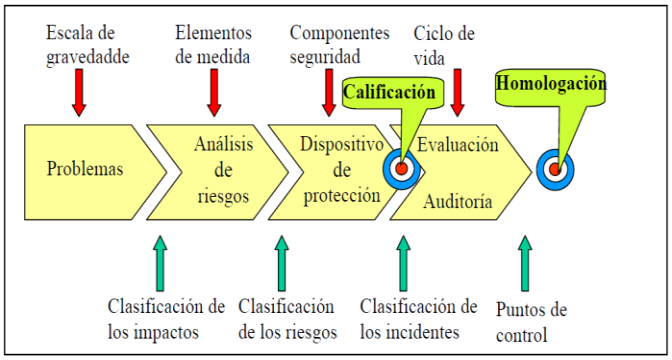


Fig. 6. Principios de una evaluación.
Fuente: *La defensa en profundidad aplicada a los sistemas de información (Secrétariat général de la défense nationale Direction centrale de la sécurité des systèmes d'information, 2004).*

La primera etapa permite clasificar los impactos eventuales sobre la escala de gravedad en función de los retos y definir los elementos de medida para catalogar los riesgos.

La segunda etapa tiene como resultado una separación de los incidentes de seguridad en función de los factores deficientes.

La tercera etapa identifica los puntos de control que se emplearán para la evaluación permanente del dispositivo durante la etapa de calificación.

El método de calificación de defensa en profundidad emplea dos (2) métodos demostrativos de análisis y son:

- **Análisis por situación envolvente:** consiste en instaurar una situación que cubra el riesgo máximo y evidenciar que las demás situaciones están incorporadas en el caso "envolvente" y que, por lo tanto, la solución elegida las cubre. Este análisis permite verificar la coherencia del número de barreras con la gravedad del hecho tenido.
- **Análisis por componente defectuoso:** reside en postular un incidente de seguridad y un fallo de forma aleatoria de otro componente ubicado entre el incidente y el hecho temido para analizar la protección restante y verificar que ésta sea suficiente.

### *E. Quinta etapa: evaluación permanente y periódica*

La evaluación debe ser permanente y periódica (una vez puesto en marcha el proyecto) y de revisión constante. Esta etapa tiene como objetivo evaluar la defensa en forma sistémica:

- Esquema orientativo.
- Retroacción (ver lo que figura a continuación).
- Estudio estático de los componentes.
- Auditoría periódica.
- Dinámica sobre incidente (experiencia).

Los resultados de esta etapa deben permitir enseñar a los responsables de la toma de decisiones las medidas tomadas para cumplir las necesidades de seguridad pactadas en la primera etapa y constatar que se alcanzaron los objetivos. Esta etapa debe converger en una decisión de homologación de seguridad que permita exponer que el sistema de información se considera apto para procesar información de determinada sensibilidad.

## VIII. CONCLUSIONES

1) Las ciberamenzas siempre estarán presentes y prestas a atacar un sistema de información. Por eso, sin importar la técnica que se escoja para contrarrestar dichas amenazas –sea ataque o defensa- se debe tener claro cuál es el objetivo primordial: y es el de evitar que se materialicen las amenazas y que éstas atenten contra el bien mayor de un sistema, que es la información.
2) El hacking ético y la defensa en profundidad son una de tantas técnicas que se pueden implementar en el campo de la seguridad informática. Aunque ninguna es mejor que la otra, juntas pueden garantizar un buen nivel de seguridad dentro de un sistema de información.
3) Para poder garantizar una cultura de seguridad, es importante que tanto directivos, gerentes y empleados sean conscientes de los problemas y amenazas a las que está expuesta la información y así, poder tomar las medidas preventivas necesarias.

## IX. REFERENCIAS

[1] S Calderón. (2012, mayo). "Hacking Ético". [En línea]. Disponible: http://hackinge.blogspot.com.co/2012/05/antecedentes-de-la-etica-del-hacker.html

[2] J D Berrio López. (2017, noviembre). "Hacking Ético vs Defensa en Profundidad". [En línea]. Disponible: http://www.dsteamseguridad.com/museo/HACKIN%20ETICO_VS_DEFENSA_PROFUNDIDAD_JUANBERRIO.pdf

[3] Secrétariat général de la défense nationale Direction centrale de la sécurité des systèmes d'information. (2004,

julio). “La defensa en profundidad aplicada a los sistemas de información” [En línea]. Disponible: https://www.ssi.gouv.fr/archive/es/confianza/documents/methods/mementodep-V1.1_es.pdf

[4] “Diccionario de informática”. [En línea]. Disponible: http://www.alegsa.com.ar/Diccionario/Cat/38.php

[5] “Glosario de seguridad” [En línea]. Disponible: https://www.symantec.com/es/mx/theme.jsp?themeid=glosario-de-seguridad

[6] O Mogollón Salazar. (2012, agosto). [En línea]. Disponible: http://2.bp.blogspot.com/-gVMfhAtilp0/UDm7DyvGoUI/AAAAAAAAATU/1go8AMwdR0M/s640/692649f56cedabab8269b60fbf0f6cd3.jpg

[7] Dragonjar. [En línea]. Disponible: http://www.dragonjar.org/wp-content/uploads/2011/03/silvato-capn-crunch-300x119.jpg

**Autor**

Wilmer Fabián Huertas Acosta, aspirante al título de Especialista en Seguridad Informática – Universidad Piloto de Colombia.