Una perspectiva global de la seguridad

[1.1] ¿Cómo estudiar este tema?

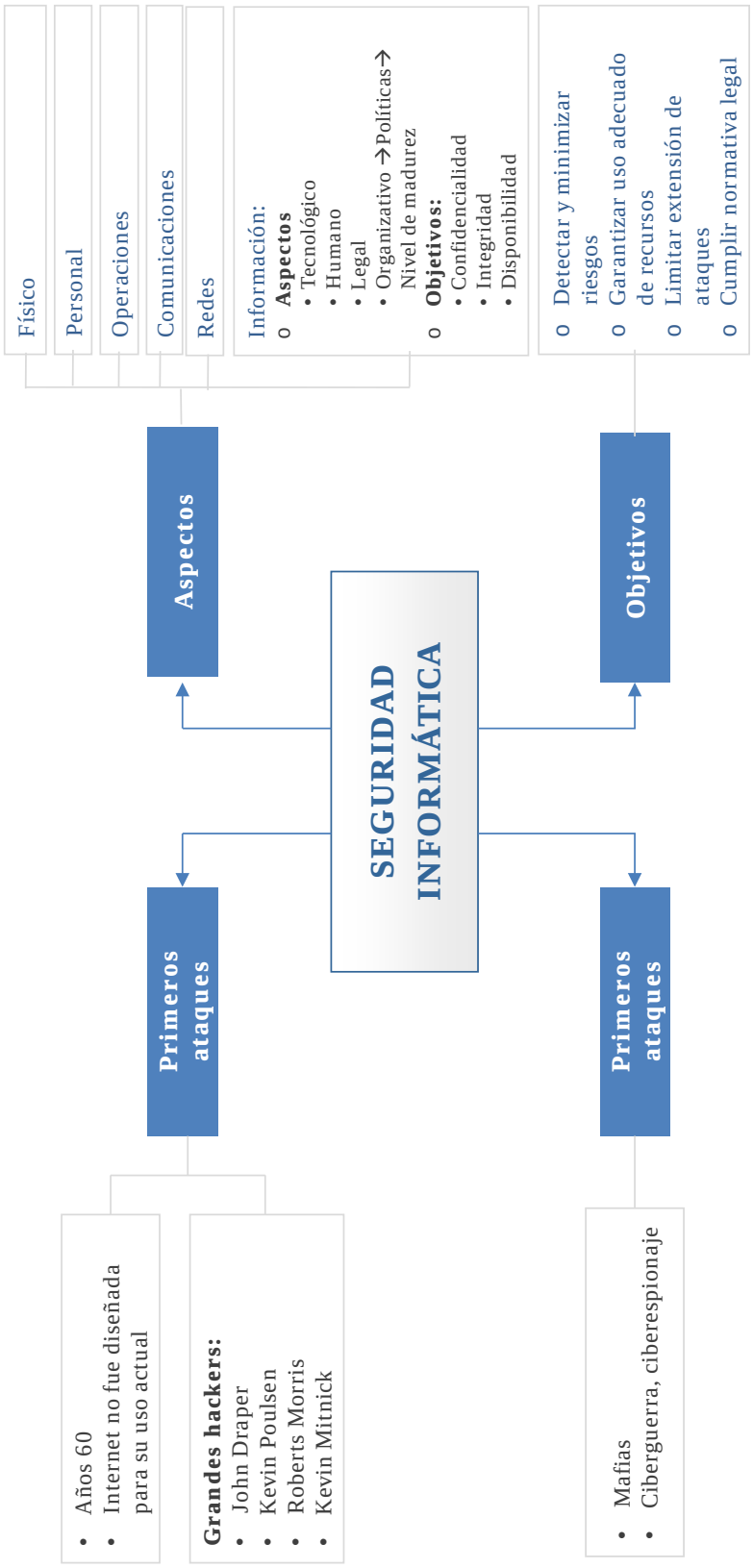
[1.2] La seguridad informática: perspectiva histórica

[1.3] Pero, ¿qué se entiende exactamente por seguridad?

[1.4] Otros conceptos importantes

TEMA 1

Esquema


SEGURIDAD INFORMÁTICA
Aspectos
Objetivos
Primeros ataques
Primeros ataques
Físico
Personal
Operaciones
Comunicaciones
Redes
Información:
Aspectos
Tecnológico
Humano
Legal
Organizativo → Políticas → Nivel de madurez
Objetivos:
Confidencialidad
Integridad
Disponibilidad
Detectar y minimizar riesgos
Garantizar uso adecuado de recursos
Limitar extensión de ataques
Cumplir normativa legal
Años 60
Internet no fue diseñada para su uso actual
Grandes hackers:
John Draper
Kevin Poulsen
Roberts Morris
Kevin Mitnick
Mafias
Ciberguerra, ciberespionaje

Ideas clave

1.1. ¿Cómo estudiar este tema?

El estudio de este tema se realiza a través de los contenidos desarrollados en las **Ideas clave** expuestas a continuación.

Este tema introductorio a la **seguridad informática** comienza con un breve repaso histórico de sus orígenes. Conoceremos, a los considerados «grandes hackers» de la historia, qué ataques llevaron a cabo y cómo estos despertaron la conciencia de toda la comunidad informática, provocando las primeras medidas de seguridad que terminarían convirtiéndose en el campo imprescindible que es hoy en día.

En este recorrido histórico llegaremos al momento actual, donde veremos cómo los ataques se han profesionalizado al participar mafias e incluso gobiernos, llevando a un auge sin precedentes al ***ciberterrorismo*** y ***ciberespionaje***.

Por último, presentaremos los primeros **conceptos sobre seguridad informática**, sus procedimientos y métodos. Analizaremos brevemente sus **objetivos, necesidades y formas de actuación**.

1.2. La seguridad informática: perspectiva histórica

La necesidad de la seguridad en el campo de la informática se hizo evidente desde sus mismos inicios. Se considera que el primer ordenador fue desarrollado durante la Segunda Guerra Mundial, y utilizado por Alan Turing y su equipo de matemáticos para romper los códigos secretos alemanes. Este es un tema apasionante, que estudiaremos con más profundidad en el siguiente tema de esta asignatura.

En este escenario surgió la necesidad de **limitar y proteger el acceso a las instalaciones** (hablamos de «instalaciones» porque el ordenador en cuestión era en realidad un conjunto de máquinas mecánicas que ocupaban varias habitaciones). Se implementaron varios niveles de seguridad, incluyendo barreras físicas, llaves y reconocimiento facial realizado por personal militar.

Vemos por tanto, que los verdaderos orígenes de la seguridad informática se encuentran en **medidas físicas** para limitar el acceso a los ordenadores. La situación no es en realidad, muy distinta a la actual, pues la ***seguridad física*** en una rama muy importante de la ***seguridad telemática***, y es absolutamente esencial en instalaciones de seguridad media y alta.

En aquellos momentos, las principales amenazas a la seguridad eran el robo físico de los equipos, el espionaje y el sabotaje. Uno de los primeros problemas de seguridad documentados que era de este tipo «físico» ocurrió a principios de los años 60, la época de los primeros *mainframes* de IBM, cuando un administrador de sistemas trabajaba en un fichero que contenía un MOTD (*Message Of The Day* - mensaje del día), y otro se encontraba editando el fichero de contraseñas del sistema. Un fallo en el software del sistema operativo mezcló ambos archivos, y todas las contraseñas se imprimieron junto con los datos de cada archivo del sistema.

Un **MOTD** es un viejo concepto proveniente de los primeros sistemas UNIX y consistía en mostrar los contenidos de determinado fichero después de un *login*, y justo antes de las ejecuciones de la *shell del sistema*. Normalmente, se incluían aforismos o mensajes divertidos.

La década de los años 60 y los orígenes de Internet

Durante la década de los años 60, en plena guerra fría entre EE.UU. y la antigua Unión Soviética, se detectó la necesidad de conectar los ordenadores entre sí, para que pudieran realizar en conjunto tareas más complejas y sofisticadas que las que podían abordar individualmente. La idea era evitar que un ataque soviético a un nodo, de los por entonces existentes y que funcionaban con el protocolo X.25 basado en el establecimiento de circuitos virtuales, dejara incomunicadas dos entidades.

Transportar físicamente enormes cintas magnéticas entre los centros de datos no era una opción viable, por lo que la famosa **Agencia para la Investigación Avanzada de Proyectos de Defensa (DARPA)** se puso a trabajar en la tarea.

El resultado fue una red comunicaciones por cable, lo más redundante y resistente posible, para el intercambio de información militar. Larry Roberts lideró el desarrollo del proyecto, conocido como **ARPANET**, y que terminaría desembocando en la primigenia Internet, cuando se abrió su acceso al mundo civil. Se habilitó un protocolo con capacidad de detectar un nodo caído y modificar su ruta de encaminamiento hasta destino (IP) y otro protocolo capaz de detectar en destino posibles errores (TCP). Todo funcionaba perfectamente... pero solo bajo la premisa inicial: que el atacante actuara desde fuera de la red. Si el atacante actuaba desde dentro, empezaban serios problemas para estas redes.

Durante la siguiente década, ARPANET se hizo cada vez más popular y su uso creció de forma exponencial entre las universidades, primeros usuarios civiles de la red. Por supuesto, este incremento de usuarios trajo consigo los primeros ataques y vulnerabilidades.

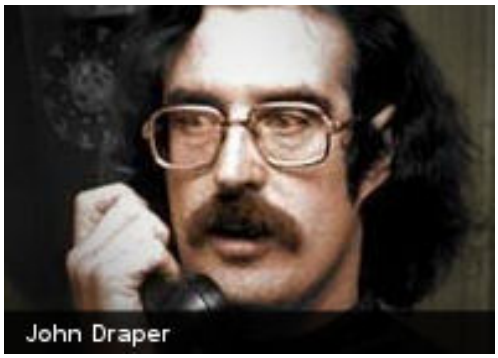
Ya en 1973, Robert Metcalfe, que más tarde desarrollaría el famoso ***protocolo Ethernet***, avisó de problemas de base y diseño en la seguridad de ARPANET. En descargo de los primeros diseñadores, es justo apuntar aquí que, como hemos visto, el encargo inicial sólo contemplaba un uso militar de la red, por usuarios que, por defecto, se consideraban autorizados. Nadie pudo prever el éxito exponencial e imparable que sufrió la red en pocos años y, como consecuencia, algunos de los grandes problemas de seguridad existentes hoy en día todavía en Internet se arrastran desde aquellos primeros días.

Años 80 y 90: grandes hackers de la historia

Debido a esta inherente falta de seguridad en el diseño de Internet y de los primeros protocolos de comunicaciones (como TCP/IP), durante la década de los años 80 y 90 hubo una gran aparición de ***hackers***, en principio mentes inquietas buscando conocimiento, que atacaron toda clase de sistemas, con mejores o peores intenciones.

Es interesante mencionar aquí algunos de ellos, pues sus acciones en muchos casos fueron el detonante para que la seguridad en esta clase de redes empezase a tomarse realmente en serio.

John Drape (*Capitán Crunch*). Tras contactar con un amigo ciego en 1969, Draper se enteró de que, taponando uno de los agujeros de un silbato distribuido como parte de una promoción de una marca de cereales llamada *Cap'n Crunch*, este producía un tono puro con una frecuencia de 2600 Hz, justo la que utilizaba la operadora norteamericana *AT&T* para señalizar el fin de la llamada. Tras esto, si uno de los extremos seguía conectado, este entraba en modo «operador», lo que permitía entre otras cosas, establecer parámetros del sistema telefónico y, por supuesto, hacer llamadas gratuitas.



Fuente: https://culturizando.com/el-primer-hacker-de-la-historia

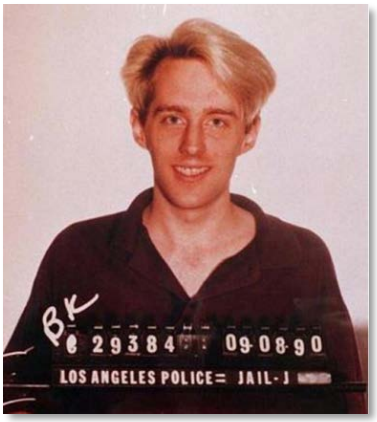
Con lo aprendido, Draper construyó la primera *blue box* de la historia, un dispositivo electrónico capaz de reproducir los tonos usados por la compañía telefónica y, de esta forma realizar llamadas telefónicas gratuitas a larga distancia.

Este era un aparato muy codiciado en un momento en el que estas llamadas eran de un sote muy elevado y sobre todo, el acceso a Internet era vía teléfono utilizando un *módem*.

Por supuesto, en cuanto la compañía telefónica advirtió este fallo de su sistema lo corrigió, haciendo lo que debería haber hecho desde el principio: usando circuitos diferentes para la voz y las señales (lo que se conoce como señalización **fuera de banda**). Posteriormente, la sustitución de la tecnología analógica por la digital eliminó de raíz la posibilidad de interferir en el sistema de conexión.

En cualquier caso, el famoso silbato de *Cap'n Crunch* sigue teniendo un gran valor como objeto de coleccionista. La historia del que muchos consideran el primer hacker de la historia dio lugar, además, al nombre a la revista de hackers más famosa de la historia, *The 2600 Magazine* (Disponible en: http://www.2600.com/) que todavía sigue publicándose.

Kevin Poulsen (*Dark Dante*). El siguiente de nuestros personajes, cuyo nick de «guerra» era Dark Dante, se llama Kevin Lee Poulsen, nació en 1965, y fue el primer hacker en ser acusado formalmente de espionaje cibernético en EE.UU.



Fuente: https://www.soldierx.com/hdb/Kevin-Poulsen-Dark-Dante

Aunque sus andanzas comenzaron con sólo 17 años, su episodio más conocido sucedió el 1 de junio de 1990, estando ya en busca y captura por parte del FBI. Poulsen tomó el control de la centralita telefónica de un concurso de radio, para asegurarse ser la llamada número 102 y obtener así el suculento premio de un Porsche 944. No contento con eso, usó la misma técnica para ganar un viaje a Hawaii. «Curiosamente» los teléfonos siempre funcionan mal al paso de Poulsen pues, en otra ocasión, justo cuando su imagen se iba a difundir en el famoso programa televisivo de la NBC norteamericana *Misterios sin resolver*, su centralita dejó de funcionar.

Poulsen fue finalmente arrestado en Febrero de 1995, acusado de siete delitos de espionaje cibernético y condenado a 51 meses de prisión, una condena ejemplar en aquella época.

Pero, como tantos otros *hackers* de pasado oscuro, Poulsen se reinventó a la salida de la cárcel. Trabajó, por ejemplo, en *Sun Microsystems* como administrador de red y formó parte del equipo del portal de seguridad *Securityfocus*. Además, en octubre de 2006, Poulsen hizo uso de sus habilidades y realizó una investigación sobre pederastas ocultos en la antigua red social *MySpace*. Su trabajo ayudó identificar 744 personas presuntamente culpables y condujo a la detención de uno de ellos.

«El gusano Morris» y el primer incidente global en Internet. El 2 de Noviembre de 1988 se observó el que se considera primer *gusano* de la historia, y que acabó afectando a más de 6000 máquinas (que componían el 10% de Internet entonces).

Fuente: http://www.nndb.com/people/466/000027385/

El responsable era un joven llamado Robert Morris, que escribió un programa que explotaba una serie de vulnerabilidades de los sistemas UNIX, y que era capaz de transmitirse de unos sistemas a otros a gran velocidad. En una Internet totalmente desprotegida y «virgen» a este tipo de ataques, en unas horas, miles de equipos tenían sus CPUs al 100%, siendo por tanto inoperativas. Este hecho fue especialmente importante porque propició el nacimiento del **CERT (*Computer Emergency Response Team*)**.

Por este episodio, Morris, cuyo padre era curiosamente uno de los desarrolladores iniciales de UNIX, y que en 1986 pasó a trabajar para la NSA norteamericana, fue condenado a 3 años de condena menor, 400 horas de servicios a la comunidad y los costes del juicio ($10,050). Actualmente es profesor en el MIT (Massachusetts Institute of Technology).

Kevin Mitnick. Pero, sin duda, el hacker más famoso de la historia sigue siendo Kevin Mitnick (que quizás no haya sido el mejor, pero sí el más mediático).

Conocido como **«El Cóndor» Mitnick** era especialmente hábil haciendo uso de la denominada *ingeniería social*. En esencia, está técnica no es más que aprovechar el eslabón más débil de la seguridad de todo sistema informático: las personas.

Por ejemplo, Mitnick fue capaz de, utilizando únicamente un mono de trabajo y mucho desparpajo, presentarse en una oficina de una compañía de teléfonos móviles y conseguir unos manuales confidenciales sobre su funcionamiento, que le permitieron generar multitud de ataques sobre ellos.

Fuente: https://twitter.com/kevinmitnick

Mitnick llegó a ser considerado «el hacker» más buscado del mundo y su foto llegó a estar en la lista de los delincuentes buscados por el FBI. Finalmente fue detenido en 1995, tras una persecución de película, gracias a la colaboración de Tsutomu Shimomura, actual miembro del Centro de Supercomputación de San Diego, que también había sufrido los ataques de Mitnick. (La historia completa es realmente interesante, por lo que te animamos a que consultes los detalles en el apartado **«No dejes de leer de este tema»**).

Tras cumplir su condena, Mitnick tuvo prohibido todo tipo de acceso a ordenadores, teléfonos móviles o cualquier otro equipo electrónico durante varios años. Finalmente se convirtió en un profesional respetado de la seguridad, fundó su propia compañía y actualmente viaja por el mundo impartiendo conferencias y seminarios.

El nuevo milenio y la profesionalización del *hacking*

La historia del *hacking* siguió siendo más o menos individual, centrada en individuos brillantes y muy habilidosos, hasta la llegada del año 2000. En este año comenzó un proceso de profesionalización de los atacantes, debido principalmente a la irrupción de las mafias tradicionales en el mundo digital.

Estas mafias se dieron cuenta de que Internet era el escenario perfecto para blanquear el dinero que conseguían con sus actividades delictivas «tradicionales» (tráfico de armas, de personas, drogas, etc.), para ocultar su rastro o para, por qué no, «ampliar» su negocio con versiones digitales de los timos y estafas que llevan años produciéndose fuera de la Red.

El *phishing*, las cartas nigerianas, las ofertas de trabajo falsas y muchas otras estafas son nuevas puestas en escena de viejos timos «analógicos». Más allá de estos timos de baja calidad y cualificación de los atacantes, lo cierto que existe una clara tendencia en los últimos años hacia la profesionalización de los atacantes y toda la infraestructura delictiva que los rodea. Y la joya de la corona estrella de esta nueva etapa es sin duda el ***malware***.

Estudiaremos con detalle esta cuestión más adelante en esta asignatura, pero para proporcionar una perspectiva del crecimiento que ha sufrido este fenómeno en los últimos años, ya que se estima que desde 2003 el número de nuevos especímenes de *malware* se ha ido doblando año a año, hasta llegar a los 100.000 diarios del año 2013. Esto significa que se crean 69 nuevas amenazas por minuto en todo el mundo. Como es previsible, la mayoría de este *malware* se focaliza en el robo de credenciales, bien bancarias para el robo de dinero o de autenticación, para la sustracción de información potencialmente valiosa.

Pero si el crecimiento del malware en plataformas PC (sobre todo en sistemas operativos Windows) ha sido espectacular, las cifras para los dispositivos móviles son sencillamente increíbles. Desde el lanzamiento del primer *iPhone* en 2007 y la primera plataforma *Android* en 2008, con crecimientos anuales que han llegado a superar el 3000% en 2013.

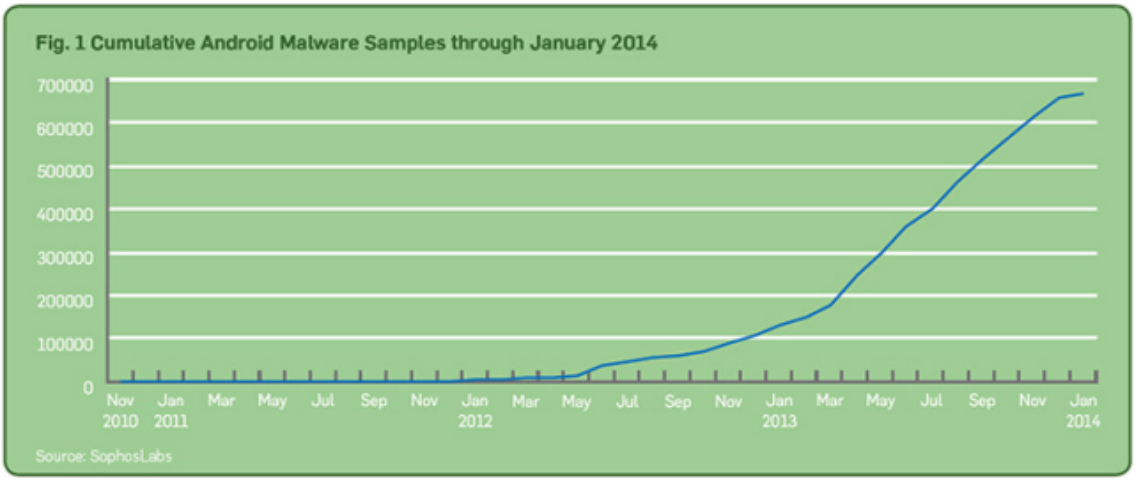


Figura 1. Crecimiento del número de ejemplares distintos de malware en la plataforma Android.

(Fuente: SophosLabs. Informe malware 2014)

Otro dato importante es que *Android* es, con enorme diferencia, la plataforma móvil más infectada, con un 99% de las amenazas. La razón crea controversia entre detractores y fans de dicha plataforma, pero lo más probable es que la causa no esté tanto relacionada con el nivel de seguridad de la plataforma como con su gran aceptación y número de usuarios.

¿Cuáles son los objetivos principales de este nuevo tipo de *malware*? Pues, por supuesto, no son precisamente cándidos y pueden dividirse en tres grandes grupos: **robo de información**, **creación de *botnets*** y ***troyanos* de envío de SMS**. Se estima que este último grupo representa alrededor del 40% del total de amenazas y funciona enviando mensajes SMS a números *premium*, que tienen un coste adicional y elevado para el usuario y que repercute en el atacante. Aunque comenzaron sobre todo en Europa del Este, en los últimos años se han expandido por todo el mundo.

En cuanto al robo de información, algunos especímenes se están volviendo realmente complejos. Por ejemplo, a principios de 2014 se detectó un tipo de *malware* para *Windows* que es capaz de infectar dispositivos *Android* a través de una conexión USB, descargar un *troyano* a dicho dispositivo para interceptar los mensajes SMS enviados por algunos bancos *online* como códigos de autenticación de doble factor.

Otra amenaza importante en los últimos años que merece la pena destacar, es el nuevo vector de ataque en el que se ha convertido el **lenguaje de programación *Java***. Desde 2012 ha sufrido una desastrosa serie de vulnerabilidades que lo han convertido en sinónimo de inseguridad.

Por ejemplo, más de 600.000 ordenadores fueron víctimas de una vulnerabilidad no resuelta durante meses en *Mac OS X* y, como consecuencia, fueron convertidos en máquinas *zombies* de una *botnet* global denominada *Flashback*.

La nueva guerra fría: «ciberguerra» y «ciberespionaje»

Como hemos visto, durante la década de 2000 el cibercrimen mundial se ha caracterizado básicamente por la profesionalización de sus atacantes y métodos. Sin embargo, en los últimos años han aparecido en escena otros actores con intenciones supuestamente más benévolas: **los gobiernos**.

En efecto, los gobiernos han empezado a ser conscientes de que la Tercera Guerra Mundial, si alguna vez se libra, no se hará con armas convencionales sino cibernéticas, con ordenadores y a través de Internet. Por esta razón y porque «no hay mejor defensa que un buen ataque», las grandes superpotencias especialmente EE.UU y China, han creado sus propios equipos de *hackers* y especialistas en seguridad.
Uno de los ejemplos más llamativos es desde luego, el de China. De acuerdo a un informe de inteligencia elaborado por la empresa de seguridad *Mandiant*, el gobierno chino cuenta con un equipo secreto de *hackers* de élite, encargados de infiltrarse en tantos objetivos como sea posible, especialmente norteamericanos.

Este grupo, conocido por el nombre *APT1* (el acrónimo *APT* hace referencia a la expresión inglesa «*Advanced Persistent Threat*»), salió a la luz en 2010 gracias a la conexión de cientos de incidentes inicialmente aislados por todo el mundo. Después de una investigación de varios años, era evidente que existía un grupo de *hackers* chinos muy organizado, bien financiado y con buenos contactos detrás de dichos ataques. Las sospechas de que este grupo no sólo contaba con el beneplácito del gobierno chino, sino que fue éste quien lo puso en marcha no tardaron en verse comprobadas.

De la estructura del grupo se conocen algunos detalles: su nombre en clave, ***unidad 61398 del Ejército de Liberación Chino***, y que su base de operaciones está situado probablemente en Shanghái. Se sabe que allí *China Telecom* proveyó a la unidad de comunicaciones de fibra óptica exclusivas en nombre del interés nacional.

Este grupo ha robado cientos de *terabytes* de datos de más de 140 organizaciones en todo el mundo (la mayoría de habla inglesa) y ha demostrado capacidad para atacar simultáneamente a decenas de objetivos, lo que hace pensar que debe ser un grupo numeroso en sus efectivos humanos (se cree que emplea a cientos, quizá miles de personas). Se sabe también que el proceso de selección es extremadamente riguroso, siendo una de las condiciones *sine qua non*, que los candidatos sean prácticamente bilingües en inglés.

Los objetivos del grupo son muy variados, pero en esencia se trata de **obtener toda la información posible sobre empresas, industrias y otros gobiernos para ayudar al servicio de inteligencia chino**. Por ejemplo, en la **Figura 2** puede observarse una línea temporal de las intrusiones de APT1, ordenados por tipo de industria; prácticamente no queda ninguna categoría sin comprometer. Llama especialmente la atención el interés en las redes de satélites y comunicaciones, pues no hay que olvidar que se trata de un grupo militar, y uno de sus objetivos principales es estar preparado ante una situación de ciberguerra.

En cuanto a sus métodos y herramientas, nos encontramos de nuevo con el secretismo. Se sabe sin embargo, que disponen de multitud de ***exploits zero-day*** para todo tipo de software, incluyendo navegadores y servidores Web, sistemas operativos y software ofimático. Un ***exploit*** es de tipo *zero-day* cuando aún no es conocido por el público (administradores de sistemas, principalmente), pero sí está siendo utilizado por los atacantes. Este estado es especialmente peligroso, pues al no ser conocido por las empresas, éstas no pueden generar parches que solucionen dicha vulnerabilidad. De hecho, muchas empresas de seguridad pagan miles de dólares por vulnerabilidades desconocidas, de forma que puedan añadirlas a sus bases de datos y disponer de su conocimiento de forma exclusiva.

Exploits. Un *exploit* es un software malicioso, escrito con el objetivo de **aprovechar una vulnerabilidad y ganar acceso a un sistema**. Si tiene éxito, un *exploit* **abrirá habitualmente una puerta trasera**, para que el atacante pueda **volver al sistema comprometido más tarde**.

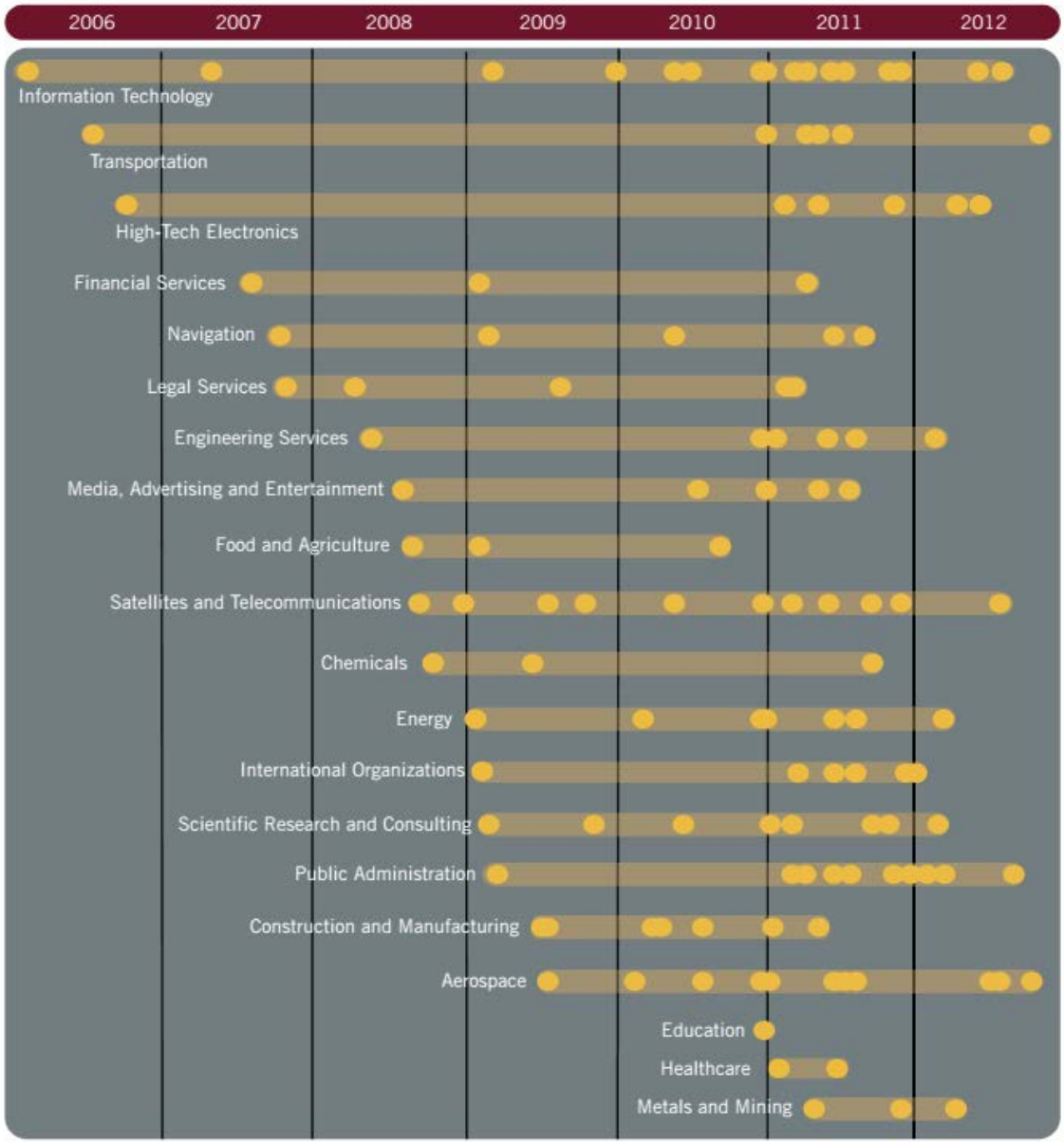


Ilustración 1. Línea de tiempo de las operaciones de *ciberespionaje* del grupo APT1, ordenadas por tipo de objetivo. Los puntos amarillos hacen referencia a la primera fecha conocida en la que el grupo comprometió un objetivo de cada categoría. Fuente: Informe sobre APT1 de Mandiant (Fuente: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf)

Se podría pensar que un grupo de élite como este utiliza técnicas muy sofisticadas para sus ataques. En parte es así, desde luego, pues conocen vulnerabilidades no públicas que utilizan para comprometer sus objetivos. Pero en muchas ocasiones utilizan métodos sencillos para romper la parte más débil de la cadena de la seguridad: **las personas**.

En un ejemplo de ataque real, este grupo envió correos electrónicos a su objetivo (los mismos miembros de la empresa de seguridad que les estaba investigando) con adjuntos maliciosos o enlaces a ficheros que contenían malware.

Para que tuviera más posibilidades de ser tomado en serio, los atacantes estudiaron bien el nombre del destinatario y trataron de encontrar un «Asunto:» del mensaje relevante y con sentido para él:

```
Date: Wed, 18 Apr 2012 06:31:41 -0700
From: Kevin Mandia <kevin.mandia@rocketmail.com>
Subject: Internal Discussion on the Press
Release

Hello,
Shall we schedule a time to meet next week?
We need to finalize the press release.
Details click here.

Kevin Mandia
```

A primera vista, el correo parecía haber sido enviado por el **CEO** (acrónimo de *Chief Executive Officer*, término de reciente aparición, pero muy utilizado ya por las empresas. **CTO** (Chief Technology Officer) y **CISO** (Chief Information Security Officer) son otros términos que conviene que conozcas de la empresa, Kevin Mandia). Sin embargo, si se observa con detalle, la dirección de correo es «kevin.mandia@rocketmail.com», que pertenece a un servicio de correo gratuito y no es la cuenta corporativa de la empresa. Es fácil no darse cuenta de un detalle así.

El adjunto, camuflado también como un archivo PDF cuando era en realidad un archivo comprimido ZIP, contenía un ejecutable que se habría instalado silenciosamente en la máquina si alguien lo hubiera abierto.

Hasta el momento hemos manejado en esta introducción a la historia de la seguridad y el *hacking* diversos conceptos, sin definirlos de forma rigurosa. Ha llegado el momento de hacerlo en el siguiente apartado.

1.3. Pero, ¿qué se entiende *exactamente* por seguridad?

Aunque es casi imposible encontrar una definición sobre el concepto de seguridad que genere consenso en todos los especialistas, utilizaremos aquí una muy extendida. Se entiende por **seguridad** la «*cualidad o estado de ser seguro, es decir, libre de peligro*». Obviamente, este es un concepto muy amplio, por lo que podemos hablar de diferentes aspectos:

- **Seguridad física**, con el fin de proteger equipamiento, personas o áreas del acceso no autorizado.
- **Seguridad del personal**, para organizar el acceso de individuos autorizados a las áreas o equipamiento que necesitan para realizar su trabajo.
- **Seguridad en las operaciones**, que protege los detalles de una serie de actividades, agrupadas bajo el nombre de operaciones.
- **Seguridad en las comunicaciones**, con el objetivo de proteger la información transmitida y el propio canal de comunicación.
- **Seguridad en las redes**, que protege el equipamiento de red, conexiones y autentica las partes involucradas.
- **Seguridad de la información**, que pretende asegurar la confidencialidad, integridad y disponibilidad de la información durante su almacenamiento, procesamiento o transmisión.

Todos los aspectos anteriores son esenciales si queremos plantear una política de seguridad seria y un nivel alto de protección. A lo largo de esta asignatura iremos estudiando cada uno de ellos, analizando sus principales características y dificultades.

Aunque en muchos manuales y libros se tiende a olvidar el resto de aspectos y centrarse únicamente en el último de ellos, la **seguridad de la información**, todos son necesarios para tener una visión global de la seguridad informática en una organización.

En este punto es apropiado presentar por primera vez uno de los axiomas de la seguridad informática, que todo profesional que se dedica a la misma ha oído repetir una y otra vez, casi como un mantra: ***la seguridad es como una cadena, y el nivel de toda ella es igual al del más débil de los eslabones***.

La metáfora es, desde luego, apropiada. La seguridad informática de una organización debería considerarse como una **cadena formada por los «eslabones»** enumerados anteriormente: seguridad física, en las comunicaciones, de la información, etc. Si uno de ellos falla, sólo uno, todo el sistema puede venirse abajo fácilmente. Es habitual encontrar empresas que dedican enormes partidas presupuestarias a la seguridad de la información, pero descuidan, por ejemplo, la seguridad del personal o física. El riesgo que corren es enorme, pues todos sus esfuerzos para asegurar la información confidencial de la empresa pueden verse comprometidos por un simple ladrón que robe un servidor físicamente, o un empleado despedido que copie la información en un *pendrive* USB antes de abandonar definitivamente la empresa.

Así pues, una buena **política de seguridad** debe ser «equilibrada» y contemplar y tener en cuenta todos los aspectos anteriores, en menor o mayor grado.

Objetivos de la seguridad informática

Una vez presentados el qué y el cómo de la seguridad, falta establecer el porqué. Es decir, cuáles son los principales objetivos de la misma:

- ***Detectar, minimizar y gestionar los riesgos*** y amenazas al estado seguro de los sistemas de información.
- ***Garantizar una utilización adecuada*** y autorizada de los recursos y aplicaciones del sistema.
- ***Limitar la extensión***, alcance y posibles pérdidas en caso de un *incidente* de seguridad, y planificar una recuperación del sistema lo más rápida y eficiente posible.
- ***Cumplir con la normativa legal vigente*** y con los requisitos organizativos, legales y de autorización impuestos por el cliente.

Como ya hemos visto, para cumplir con estos objetivos una política de seguridad tendría que actuar sobre todos (o la mayoría de ellos, dependiendo de las necesidades específicas) los aspectos expuestos anteriormente, que podrían resumirse en estos cuatro grandes planos de actuación:

Técnico, tanto a nivel lógico como físico.
Legal, cada vez más países obligan a cumplir leyes muy restrictivas en determinados sectores y para tratar determinados datos. En nuestro país, destaca la LOPD (Ley Orgánica de Protección de Datos), que contempla multas cuantiosas a quien no cumpla sus directivas sobre tratamientos de datos de carácter personal.
Humano, a través de la formación y sensibilización de empleados y directivos hacia la necesidad de la seguridad, la definición de sus funciones y obligaciones, etc.
Organizativo, a través de la definición e implantación de políticas de seguridad, planes, normas, procedimientos y buenas prácticas de actuación.

Es importante destacar en este punto que la seguridad informática debe ser entendida como un proceso y no únicamente como un producto o servicio que se pueda instalar y olvidarnos de él. Esta ha sido una máxima muy repetida por fabricantes de productos de seguridad, que aseguran en muchas ocasiones que su producto es poco menos que «mágico» y soluciona todos los problemas y amenazas de seguridad de una empresa.

Por supuesto esto nunca es exactamente y en todo caso, un producto solucionaría únicamente el aspecto técnico de los enunciados en la lista anterior; faltaría abordar, por tanto los aspectos legales, humanos y organizativos, tan importantes o más como el técnico.

La **seguridad debe considerarse, por tanto, como un proceso iterativo**, constante, que no acaba nunca durante la vida de una organización o sistema de información (véase **Figura 3**).

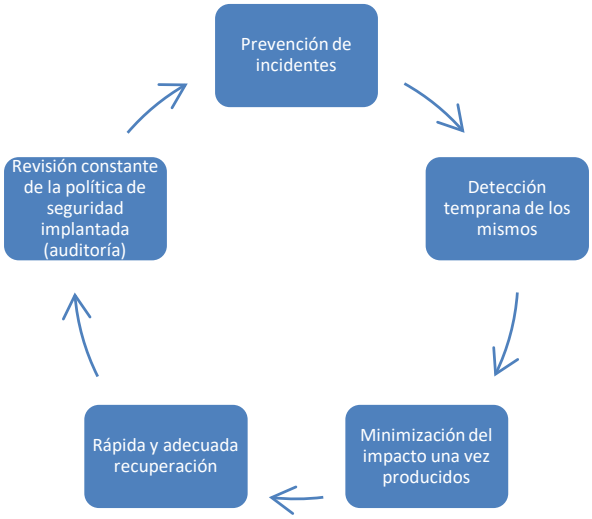


Figura 3. La seguridad como proceso

Objetivos de la seguridad de la información: el triángulo C.I.A.

Como comentamos en su presentación, los objetivos básicos de la seguridad de la información, una de las «patas» de la seguridad informática en general, son asegurar la **confidencialidad, integridad y disponibilidad** de la información.

Este principio básico es conocido como el ***triángulo CIA*** (de sus siglas en inglés, *confidentiality*, *integrity*, *availability*), y forma ya parte de todo tipo de estándares (como el ISO 17799).

Figura 4. Principios básicos de la seguridad de la información

Definamos ahora qué se entiende exactamente por cada uno de estos conceptos:

- **Confidencialidad:** este servicio garantiza que una comunicación, mensaje o dato sólo podrá ser leído por su dueño, y no por cualquier otro agente que tenga acceso a él. Es decir, la confidencialidad garantiza el secreto de los datos.
- **Integridad:** indica que un mensaje no ha sido modificado durante su transmisión, o que un dato no ha sido manipulado desde que fue creado durante su almacenamiento.
- **Disponibilidad:** como es fácil de entender, la disponibilidad debe asegurarse de los datos puedan ser accedidos siempre que se necesite. Esto incluye protección ante ataques de denegación de servicio, recuperación ante incidentes o desastres naturales. Aunque este aspecto suele ser menospreciado ante los dos primeros, ¿de qué sirve una información perfectamente protegida si no puedo acceder a ella o esta ha sido borrada?

1.4. Otros conceptos importantes

Finalizaremos este primer tema introductorio definiendo una serie de conceptos importantes, sobre los que suele haber ciertas dudas, incluso entre los profesionales de la seguridad informática. Iremos estudiándolos como todo detalles a lo largo de la asignatura, pero conviene sentar unas bases sólidas desde el principio:

- **Activo:** es un recurso de la organización que debe ser protegido. Un activo puede ser **lógico**, como un sitio Web, o un documento confidencial, o **físico**, como una persona, un ordenador o cualquier otro objeto tangible.
- **Ataque:** existe la definición obvia, que hemos estado ya utilizando implícitamente, que es la del acto intencionado de una persona contra un sistema de información con el fin de robar información, destruirla o ganar el control del mismo. Sin embargo, es importante destacar que los ataques pueden ser (la mayoría de las veces lo son) no intencionados y llevados a cabo por un empleado, en la forma de un mal uso del sistema (instalar un software de intercambio de archivos *P2P* en el ordenador corporativo, por ejemplo). Un ataque puede ser llevado a cabo también por la naturaleza, como un rayo producido durante una tormenta. Todos estos ejemplos se consideran ataques, de forma genérica, para poder actuar de forma conjunta ante ellos, sin distinciones de su origen o finalidad.

- **Amenaza**: un conjunto de personas, objetos o cualquier otra entidad que suponga un peligro para los activos de una organización. Es importante asumir que las amenazas en Internet están siempre presentes. En la **Figura 6** pueden verse algunos de los tipos de amenazas más comunes a los sistemas de información.
- **Vulnerabilidad**: es una debilidad o falla en un sistema o mecanismo de protección que facilita que se lleve a cabo un ataque. Quizás las más conocidas sean las existentes en el software, pero vulnerabilidades pueden ser también un cortafuegos mal configurado o una puerta de acceso a la habitación que aloja los servidores mal cerrada.
- **Riesgo**: por último, el riesgo es la probabilidad de que algo no deseado ocurra. En cierta manera, podríamos definirlo a través de la siguiente «ecuación»:

Riesgo = vulnerabilidades * amenazas

Esta fórmula hace referencia a que si no existen amenazas (cosa muy poco probable que no debería asumirse nunca) el riesgo es bajo, aunque existan vulnerabilidades, y si no existen vulnerabilidades, el riesgo también es bajo, aunque existan muchas amenazas.

Número	Tipo de amenaza	Ejemplos
1	**Ataques a la propiedad intelectual**	Copia ilegal de películas y música, sin respetar el copyright
2	**Ataques vía software**	Virus, gusanos, ataques de denegación de servicio
3	**Ataques a la calidad de servicio (*QoS, quality of service*)**	Cortes de electricidad, ataques al proveedor de servicio de Internet
4	**Espionaje o intrusión**	Acceso no autorizado y/o recolección de datos robados
5	**Catástrofes naturales**	Fuegos, inundaciones, terremotos, rayos
6	**Error humano**	Accidentes, fallos de los empleados
7	**Extorsión y/o secuestro de información**	Criptovirus, extorsión bajo amenaza de publicar información comprometedora
8	**Pérdidas de información**	Pérdidas completas o parciales de información debido a un plan de *backup* inadecuado
9	**Controles inadecuados**	Falta de cortafuegos o sistemas de detección de intrusión, mala configuración de los mismos.
10	**Sabotaje**	Destrucción o robo físico de sistemas de información
11	**Fallos hardware**	Fallos en el equipamiento hardware
12	**Fallos software**	Bugs, problemas de codificación o diseño
13	**Obsolescencia tecnológica**	Tecnologías o equipos anticuados

Figura 5. Tipos de amenazas más comunes a los sistemas de información

Lo + recomendado

No dejes de leer...

Informe de Sophos sobre _malware_ para plataformas móviles

Este informe contiene los últimos datos y tendencias del *malware* actual, completamente centrado ya en las plataformas móviles. Como dato curioso, basta decir que el 99% del *malware* afecta a la plataforma *Android*.

Accede al documento a través del aula virtual o desde la siguiente dirección web:
http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-mobile-security-threat-report.pdf

Informe de Mandiant sobre el grupo de hackers chino APT1

Este interesantísimo documento contiene todos los detalles que se conocen hasta la fecha del grupo de *hackers APT1*, amparado por el gobierno chino. Te proponemos la lectura del documento para ampliar lo que hemos visto sobre este grupo a lo largo del tema.

Accede al documento a través del aula virtual o desde la siguiente dirección web:
http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

No dejes de ver...

Juegos de guerra (Wargames)

Título original: *Wargames*
Año: 1983
Duración: 114 min.
País: EE.UU.
Director: John Badham
Interpretación: Matthew Broderick, Ally Sheedy, John Wood

Muchas veces una película es una buena manera de captar la verdadera esencia de un tema. Esta vieja película, todo un clásico para los aficionados a la informática, muestra muy bien cómo fueron los inicios del *hacking* y el miedo reverecencial que se les tenía durante los primeros años.

Historia Secreta de los Hackers Informáticos

Este interesante documental hace un exhaustivo recorrido por la historia de los grandes hackers, y cuenta de forma muy didáctica muchas anécdotas y datos sobre todos los personajes que hemos estudiado en el tema. No te lo pierdas si quieres profundizar más sobre ellos.

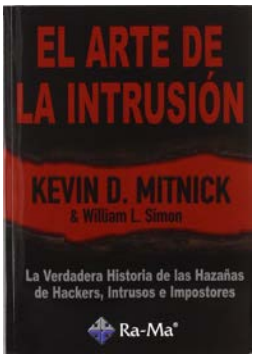
Accede al vídeo a través del aula virtual o desde la siguiente dirección web:
https://www.youtube.com/watch?v=Y47m1cOyKjA

+ Información

A fondo

El arte de la intrusión

Kevin Mitnick (2007). *El arte de la intrusión*. Madrid: RA-MA.



Este es un libro clásico escrito por el propio Kevin Mitnick, que cuenta muchas de sus «aventuras» y cómo fue finalmente detenido. Es un documento ameno de leer y proporciona una visión clara sobre las motivaciones que movían a los primeros hackers.

Test

1. La razón última de muchos de los problemas actuales en informática son debidos a que:

A. Internet tuvo un origen civil y no fue diseñado para un uso tan masivo

B. Internet tuvo un origen militar y no fue diseñado para ser utilizado por actores no autorizados

C. La seguridad se dejó fuera deliberadamente de los diseños porque degradaba mucho el rendimiento de la red

D. La seguridad

2. El sobrenombre del hacker que construyó las primeras *blue boxes*, dispositivos para conectarse gratuitamente al sistema telefónico, era:

A. Kevin Mitnick

B. Dark Dante

C. Capitán Crunch

D. Robert Morris

3. El principal rasgo distintivo del *hacking* moderno es:

A. El aumento de la capacidad técnica de los atacantes; su principal motivación es el reconocimiento y la fama

B. La profesionalización de todos los actores implicados, cuyo objetivo principal es el lucro económico

C. El auge de la creación de grupos de *hackers*, frente a los primeros años, donde el hacking era una actividad esencialmente individual

D. El aumento de la capacidad técnica de los atacantes, como consecuencia de un mayor acceso a los conocimientos de hacking, antes de difícil acceso

4. Un *exploit* es:

A. Cualquier tipo de ataque a un sistema que tenga éxito

B. Cualquier tipo de ataque a un sistema, independientemente de que tenga éxito o no

C. Un ataque a un sistema que todavía no es conocido por el público, sólo por los atacantes

D. Una porción de software escrito con el fin de explotar una vulnerabilidad y ganar acceso a un sistema

5. Uno de los grupos de hackers chinos más conocidos, con apoyo gubernamental, se denomina:

A. APT1
B. APT2
C. Ejército de liberación chino
D. Mandiant

6. ¿Cuál de las siguientes sentencias no es uno de los objetivos esenciales de la seguridad informática?

A. Detectar, minimizar y gestionar los riesgos y amenazas de los sistemas de información
B. Proporcionar los recursos materiales necesarios para el adecuado funcionamiento de una organización
C. Limitar la extensión, alcance y posibles pérdidas en caso de un incidente de seguridad
D. Cumplir con la normativa legal vigente y con los requisitos organizativos, legales y de autorización impuestos por el cliente

7. ¿Podríamos decir que seguridad de la información y seguridad informática son términos equivalentes?

A. Aunque suelen confundirse, la seguridad de la información es sólo un aspecto más de la seguridad informática, que engloba a éste y otros aspectos
B. Esencialmente sí, pues el objetivo último de la seguridad informática es la seguridad de la información
C. Aunque suelen confundirse, la seguridad informática es sólo un aspecto más de la seguridad de la información, que engloba a éste y otros aspectos
D. Son completamente equivalentes, y pueden utilizarse indistintamente

8. El responsable de asegurar la confidencialidad, integridad y disponibilidad de la información durante su almacenamiento es:

A. Seguridad en las operaciones.
B. Seguridad en las comunicaciones.
C. Seguridad en las redes.
D. Seguridad de la información.

9. El riesgo en un sistema informático puede definirse como:

A. Riesgo = amenaza * ataque
B. Riesgo = amenaza * vulnerabilidad
C. Riesgo = ataque * vulnerabilidad
D. Riesgo = activo * amenaza

10. El objetivo esencial de la seguridad de la información es asegurar:

A. La confidencialidad, secreto y disponibilidad
B. La confidencialidad, integridad y disponibilidad
C. La confidencialidad, integridad y no modificación
D. La confidencialidad, integridad y accesibilidad