

1. CRITERIOS GENERALES COMÚNMENTE ACEPTADOS SOBRE AUDITORÍA INFORMÁTICA

Contenido

1. CRITERIOS GENERALES COMÚNMENTE ACEPTADOS SOBRE AUDITORÍA INFORMÁTICA	1
¿QUÉ ES UNA AUDITORÍA INFORMÁTICA?	3
CÓDIGO DEONTOLÓGICO DE LA FUNCIÓN DE AUDITORÍA.....	5
RELACIÓN DE LOS DISTINTOS TIPOS DE AUDITORÍA EN EL MARCO DE LOS SISTEMAS DE INFORMACIÓN	12
CRITERIOS A SEGUIR PARA LA COMPOSICIÓN DEL EQUIPO AUDITOR.....	15
EL INFORME DE AUDITORÍA	16
FASES GENERALES DE UNA AUDITORÍA.....	18
FASES DE UNA AUDITORÍA DE HACKING ÉTICO	22
TIPOS DE AUDITORÍAS DE HACKING ÉTICO, METODOLOGÍAS, NORMAS Y LEYES.....	40
APLICACIÓN DE CRITERIOS COMUNES PARA CATEGORIZAR LOS HALLAZGOS COMO OBSERVACIONES O NO CONFORMIDADES	70

¿QUÉ ES UNA AUDITORÍA INFORMÁTICA?

Una auditoría informática *es un proceso que permite evaluar y medir si el sistema de seguridad informático implantado realiza sus funciones adecuadamente, permitiendo poner de manifiesto y mejorar cualquier incidencia que se pueda presentar y que afecte a la triada CIA, confidencialidad, integridad y disponibilidad.*

Esto nos da la capacidad de tomar las medidas adecuadas para *minimizar el riesgo de materialización de una vulnerabilidad* tomando medidas para eliminar esos riesgos o minimizarlos, incluso a veces permitiendo aceptar el riesgo, esto ocurre en sistemas Legacy, donde a veces tenemos equipos o sistemas operativos que ya no pueden actualizarse, pero que contienen aplicaciones vitales para los procesos de negocio de la empresa, y que muchas veces la migración a sistemas más actuales supone una gran inversión económica que es mayor a asumir el riesgo de que se materialice una vulnerabilidad.

Además, nos permite *comprobar el cumplimiento* (compliance) *de leyes, normas y procedimientos de obligado cumplimiento* para proteger el activo más importante de las empresas que son los datos, en las dimensiones **CIA**, especialmente en materia de protección de datos, cumpliendo con leyes como la **LOPD** y **RGPD**.

Se evalúan aspectos tanto técnicos como humanos.

Las auditorías *se deben hacer de forma periódica, y tienen un carácter preventivo y proactivo* donde se analiza la seguridad de la empresa y se actúa en base a los resultados obtenidos.

Las **ventajas** de realizar estas auditorías periódicas son muchas, entre ellas:

- Optimizar los procesos informáticos de negocio.
- Detectar y conocer las vulnerabilidades existentes de forma que podamos eliminar o reducir el riesgo.
- Permite actuar antes de que se materialice un incidente de seguridad.
- Permite crear procedimientos de actuación en caso de sufrir el incidente, como, por ejemplo, poder recuperar la información si hemos hecho copias de seguridad en caso de que suframos un ataque de tipo Ransomware o cualquier otro que afecte a la integridad y disponibilidad de los datos.
- Permite optimizar, mejorar y actualizar las políticas de seguridad existentes en la empresa, así como los procedimientos a seguir.
- Evita multas y sanciones debidas al incumplimiento de leyes, buenas prácticas y normativas de protección de datos.
- Reduce costes a futuro, y hace que hagamos un mejor uso de los recursos.
- Mejora la imagen de empresa.
- Siguen procesos de mejora continua como el ciclo **PDCA** (Plan, do, check, act), en los que básicamente planificamos lo que vamos a hacer, lo hacemos, comprobamos que funciona y

lo ponemos en práctica, y con los resultados positivos o negativos que obtenemos en la puesta en práctica, volvemos a iniciar el proceso.

CÓDIGO DEONTOLÓGICO DE LA FUNCIÓN DE AUDITORÍA

Es necesaria la existencia de un **código deontológico**, basado en cuestiones como la moral y la ética profesional que se compone de varios principios:

1. Principio de beneficio del auditado

1. La actividad realizada por el auditor debe estar orientada a sacar el máximo beneficio para su cliente.
2. No deben anteponerse aspectos o intereses personales.
3. No debe existir por parte del auditor ningún tipo de interés o beneficio por parte de marcas, productos o fabricantes.
4. El auditor debe abstenerse de recomendar actuaciones innecesarias o que vayan a generar riesgos que estén injustificados.

2. Principio de calidad

1. Si existe algún impedimento por parte de la empresa o por su propia parte, como no tener las licencias de las herramientas necesarias para hacer la auditoría de forma satisfactoria, o no tener el suficiente conocimiento, el auditor debe negarse a realizar

la auditoría, para no comprometer la calidad del servicio prestado y ofrecer las máximas garantías en este sentido.

2. Dicho lo anterior si el auditor considera que el informe de auditoría debe ser hecho por un profesional más capacitado deberá remitirlo al mismo para una mejor calidad de la auditoría. Supongamos, por ejemplo, que somos especialistas en auditorías de sistemas Microsoft Windows, y que conocemos Linux, pero no en profundidad, en este caso, deberíamos delegar esa auditoría a un especialista e Linux, que garantice una correcta auditoría.

3. Principio de capacidad

1. El auditor debe realizar formación continua, algo que es muy evidente en el cambiante mundo IT.
2. El auditor debe de incidir en la toma de decisiones del cliente con cierta libertad.
2. Debe ser consciente del grado de conocimientos, capacidades y aptitudes para desarrollar el proceso de auditoría, siendo consciente de sus limitaciones sin hacer una valoración personal sobreestimada que pueda derivar en el incumplimiento total o parcial de la auditoría o crear deficiencias en la misma.
3. El auditor tiene que evolucionar con el desarrollo de las TI, es decir, estar actualizado en sus conocimientos.

4. Principio de cautela

1. Las recomendaciones efectuadas han de estar basadas en la experiencia.

2. El auditor está al corriente de la evolución tecnológica y es capaz de informar al cliente.
3. Debe actuar con humildad.

5. Principio de comportamiento personal

1. El auditor actuará conforme a las normas implícitas o explícitas dignas de la profesión.
2. NO debe exponer juicios de valor personales.
3. Debe estar seguro de sus conocimientos para el trabajo solicitado.

6. Principio de concentración en el trabajo

1. El auditor debe evitar el exceso de trabajo que influya en su capacidad de concentración y precisión en las tareas ejecutadas.
2. Debe estimar las posibles consecuencias del trabajo acumulado.
3. Evitar copiar conclusiones de trabajos anteriores para ahorrar tiempo, ya que además cada empresa es un mundo, y dispone de diferentes procesos de negocio y tecnologías asociadas.

7. Principio de confianza

1. El auditor fomenta la confianza siendo transparente en su forma de actuar.
2. Las auditorías requieren confianza y diálogo entre ambas partes para solucionar posibles dudas.
3. Se debe adecuar el lenguaje al nivel de comprensión del auditado, ya que el cliente no tiene por qué comprender nuestro "mismo idioma" o lenguaje técnico, es por ello que

además en toda auditoría se realizan dos informes, uno técnico para los miembros de TI y otro ejecutivo con un lenguaje más simple y cercano a una persona que no tienen conocimientos técnicos.

8. Principio de criterio propio

1. Este principio está relacionado con el principio de independencia, el auditor debe actuar con criterio propio y no dejarse llevar por otros.
2. Si por alguna razón existen discrepancias de criterio con otros profesionales, el auditor debe reflejar esas diferencias en su informe poniendo de manifiesto su criterio.

9. Principio de economía

1. El auditor debe evitar generar gastos innecesarios al cliente auditado.
2. Debe delimitar adecuada y concretamente el alcance, objetivos y límites de la auditoría.
3. Debe rechazar ampliaciones del trabajo que no estén directamente relacionadas con la auditoría.

10. Respeto por la profesión

1. El auditor debe reconocer y dar valor a su trabajo.
2. LA remuneración por la auditoría debe estar de acuerdo con los conocimientos, preparación y experiencia del auditor.
3. Evitar la competencia desleal poniendo precios más baratos que los del mercado.

4. Promover el respeto mutuo por los compañeros de profesión.

11. Principio de integridad moral

1. El auditor debe ser leal, honesto y diligente en su desempeño, dedicado y preciso.
2. Evitar participar de forma consciente o inconsciente en actos de corrupción.
3. No puede aprovechar los conocimientos adquiridos de la auditoría de la empresa para usarlos en su contra.

12. Principio de legalidad

1. El auditor debe evitar el uso de sus conocimientos en pro de la desobediencia de la legalidad en vigor.
2. No consentirá ni colaborará en cualquier acto que implique acciones no legales como borrado de archivos, manipulación de evidencias, obtención de claves de acceso restringidas, etc.
3. El auditor debe abstenerse de intervenir líneas de comunicación que impliquen la vulneración de la privacidad.

13. Principio de precisión

1. Este principio se relaciona directamente con el de calidad del servicio prestado, no se debe establecer una conclusión hasta que no estamos totalmente seguros y tenemos todas las evidencias que permite dar esa conclusión como válida.

2. Debe ser crítico.
3. Debe indicar en todo momento cómo se ha realizado la evaluación, el procedimiento seguido, su validez, y herramientas usadas que evidencian lo observado de forma absoluta.

14. Principio de responsabilidad

1. El auditor se responsabiliza de todo lo que haga, diga o aconseje.
2. Está obligado a hacerse cargo de los daños o perjuicios que haya podido ocasionar a su cliente derivados de una actuación culpable.

15. Principio de secreto profesional

1. La confidencialidad respecto al proceso de auditoría es una característica esencial en la relación entre cliente-auditor.
2. El auditor en su deber de secreto profesional no debe difundir a terceros información del cliente, de nada de lo visto, deducido u oído durante el desarrollo de su actividad.
3. Es responsabilidad del auditor tomar las medidas de seguridad necesarias para garantizar que la información documentada está a salvo.

16. Principio de veracidad

1. El auditor debe asegurar la veracidad de sus conclusiones y manifestaciones.

Adicionalmente ,voy a mencionar el **código de ética profesional de ISACA**, Information Systems Audit and Control Association (Asociación de Auditoría y Control de Sistemas de Información), asociación de ámbito internacional que patrocina el desarrollo de metodologías y certificaciones para auditorías y control en sistemas de información. Los miembros de las certificaciones de **ISACA** en materia de auditoría deben:

1. Soportar la implementación de procedimientos y fomentar el cumplimiento de normas, procedimientos y controles adecuados para los sistemas de información.
2. Ejecutar las tareas y deberes de forma objetiva y con la debida diligencia y profesionalidad conforme a las normas y mejores prácticas profesionales (ISO 27000, ITIL, COBIT, etc.).
3. Servir al interés de la empresa de forma legal y honesta manteniendo estándares altos de conducta y carácter sin cometer actos que pudieran deshonorar la profesión.
4. Mantener la privacidad y confidencialidad de toda información obtenida durante la auditoría, a excepción de que una autoridad legal requiere la revelación del secreto. Dicha información no se dará a terceros ni será usada para el beneficio personal.
5. Mantener competencia en el campo a auditar y emprender únicamente las acciones que podamos realizar en base a nuestro conocimiento.
6. Informar a las personas responsables y adecuadas del curso de la auditoría.
7. Aumentar la comprensión y conocimiento del cliente en la seguridad y control de los sistemas de información.

RELACIÓN DE LOS DISTINTOS TIPOS DE AUDITORÍA EN EL MARCO DE LOS SISTEMAS DE INFORMACIÓN

Como bien sabes, el mundo de la tecnología es muy extenso y variado y es imposible tener un conocimiento de todo, por lo que existen especialistas en diferentes áreas relacionadas con **IT** y ciberseguridad, por lo que existen multitud de tipos de auditorías en función del área.

Una auditoría como has podido extraer de los puntos anteriores es un procedimiento sistemático, independiente y documentado donde obtenemos evidencias objetivas que determinan el grado de cumplimiento de los criterios previamente marcados en el plan de seguridad de la empresa y el nivel de cumplimiento legal en función de la información que se tiene que asegurar en cada caso, acorde a la **LOPD** (Ley orgánica de protección de datos).

Inicialmente las auditorías pueden ser de dos tipos:

1. **Internas:** cuando son realizadas por el personal de la propia empresa.
2. **Externas:** la auditoría la hace un agente externo a la empresa. A su vez puede ser de dos tipos:
 1. **Auditoría externa de segundas partes:** ocurre cuando un cliente quiere comprobar si sus proveedores cumplen los requisitos esperados (calidad y seguridad de los servicios, leyes, normas, procedimientos estipulados, ISO, etc.) De forma que contrata una entidad externa para la evaluación.

2. **Auditoría de terceros:** en este caso, es una entidad certificadora independiente la que comprueba el cumplimiento, emitiendo un certificado final de cumplimiento si todo está conforme, por ejemplo, para que una empresa pueda obtener la certificación **ISO 27001** debe someterse a una auditoría externa por parte de entidades como por ejemplo **AENOR**, que confirma si se cumplen con todos los requisitos establecidos en dicha **ISO**.

Por otra parte, también podemos tener auditorías **según la metodología empleada**, estas pueden ser:

1. **De cumplimiento:** verifican cumplimiento de leyes, normas, procedimientos, estándares de seguridad, políticas y procedimientos internos.
2. **Técnicas:** auditorías en las que se revisan aspectos técnicos de seguridad acotadas generalmente a un sistema o sistemas específicos.

Como ya hemos mencionado pueden existir diferentes tipos de auditorías **en función del área a auditar**, entre las que destacan:

- Auditoría de redes y comunicaciones.
- Auditoría de sistemas operativos.
- Auditoría de aplicaciones.
- Auditoría forense.
- Hacking ético (Pentesting).
- Auditoría de vulnerabilidades.

- Análisis de código.
- Auditorías de seguridad lógica.
- Auditorías de seguridad física.
- Auditorías Web.

CRITERIOS A SEGUIR PARA LA COMPOSICIÓN DEL EQUIPO AUDITOR

Dado que las auditorías pueden versar de algo muy concreto como puede ser auditar un servidor o auditar toda la infraestructura de la empresa, hay que tener en cuenta que uno no puede tener todos los conocimientos de absolutamente todo, por lo que normalmente las auditorías se realizan por un equipo multidisciplinar, cada integrante con su “expertise” en la materia a auditar.

EL INFORME DE AUDITORÍA

Los resultados de la auditoría se deben documentar, se realizarán 2 informes, uno técnico y otro ejecutivo que puedan entender las personas que no tengan conocimientos técnicos informáticos. En este informe debemos:

- **Documentar** leyes, normativas y procedimientos que se han utilizado.
- Realizar un pequeño **glosario de palabras** y siglas para una mejor comprensión del lector del informe.
- **Documentar todo el procedimiento** realizado con la información recopilada adjuntando pantallazos, fotos de las evidencias que pueden incluirse en un anexo. Especificando también fecha y hora de realización. Estas evidencias deben ser objetivas, tangibles y bien documentadas con detalle.
- Los criterios de la auditoría vienen dados por la norma o metodología que estemos utilizando. Por ejemplo, la **ISO 27001**.
- Hay que documentar las no conformidades o desviaciones.
- Todo lo que esté conforme a la norma estará documentado, pero no es necesario incluirlo en el informe final de conclusiones, salvo que lo requiera el cliente.
- Este **informe de conclusiones** será un resumen de todas las valoraciones y no conformidades que debe ser firmado por el auditor y entregado al cliente.
 - En el anexo A 16.1 de la ISO 27001 se define el término de no conformidad como el incumplimiento de un requisito específico de dicha norma, que por otra parte

también puede tratarse de un incumplimiento legal que implica la implementación de una acción correctiva formal.

- Uno de los objetivos del informe es que cualquiera que use la misma metodología y herramientas pueda llegar a las mismas conclusiones que nosotros.
- Tendremos que **hacer unas recomendaciones de las medidas correctoras** que se pueden aplicar para cada no conformidad. Por ejemplo, si hemos detectado una vulnerabilidad CVE-XXXX-XXXX podemos consultar la web de cve-mitre, donde encontraremos una descripción de la misma y enlaces a documentos que permiten solventar esa vulnerabilidad, o en la propia web de los fabricantes, por ejemplo, en la web de Microsoft, Cisco, etc
- Con el informe realizado la gerencia de la empresa debe poder conocer el estado real de la seguridad de su infraestructura y sistemas, así como del cumplimiento o no de sus políticas de seguridad, y de esta forma poder tomar las decisiones oportunas en cada momento para mitigar o minimizar el riesgo.
- En el informe se puede hacer una evaluación del riesgo.

FASES GENERALES DE UNA AUDITORÍA

En este punto vamos a describir cuáles son las fases de una auditoría de forma general, más adelante veremos de forma específica las fases de una auditoría de hacking ético (pentesting).

Planificación inicial, objetivos y alcance

Lo primero es establecer una reunión con el cliente donde se definen aspectos como el alcance de la auditoría, esto es sistemas por auditar, límites como por ejemplo si accedemos a un equipo a través de una vulnerabilidad explotada, si ese es el fin de nuestra misión o podemos avanzar, por ejemplo, tratando de ver la información del equipo auditado, u otras acciones.

Se establecen las ventanas horarias en las que se va a realizar la auditoría, quien o quienes la van a realizar, el tipo de auditoría.

Se hará necesario realizar un inventario de los equipos a auditar, así como fotos de los recursos TI, también debemos conocer el plan de seguridad y procedimientos de la empresa, así como cuál es la formación de los trabajadores y sus funciones con respecto a los equipos auditados, su conocimiento de los procedimientos y del plan de seguridad y el nivel de cumplimiento.

En esta fase se establece también la duración de la auditoría que depende del tipo de auditoría a realizar, los equipos a auditar, así como del tipo de auditoría, si es de caja blanca, gris o negra, que describiremos en los siguientes puntos.

También se deben establecer los recursos humanos y técnicos necesarios.

Aquí es importante resaltar que con todo lo que hemos detallado hay que realizar un contrato entre auditor y cliente, con la debida autorización por parte de la empresa a auditar, ya que, si hacemos una auditoría sin permiso, estaríamos cometiendo una ilegalidad, con sus correspondientes consecuencias, por otra parte, también se firmarán acuerdos de confidencialidad.

Análisis de riesgos y amenazas

En esta fase realizaremos un análisis de los riesgos y amenazas a los que está expuesta la empresa, identificando vulnerabilidades y el nivel de amenaza, evaluando las consecuencias en caso de que se materializase esa amenaza.

Los puntos a analizar serían:

- Analizar la seguridad del hardware, sistemas operativos, aplicaciones y redes.
- Cumplimiento en cuanto a políticas y procedimientos.
- Cumplimiento de las normativas vigentes en cuanto a protección de datos y ciberseguridad.

- Análisis de la formación del personal implicado en las tareas de seguridad informática de la empresa, teniendo en cuenta que este suele ser el eslabón más débil, generalmente por la falta de formación adecuada para el puesto.
- Análisis del correcto funcionamiento de los protocolos de actuación en caso de que ocurra un incidente. Por ejemplo, si cae un servidor qué plan tenemos para su pronta recuperación y comprobar que funciona adecuadamente, lo entenderás mejor con las copias de seguridad, si por la razón que sea alguien accede a nuestros sistemas y cifra su información ¿Podemos recuperarla? ¿Tenemos un procedimiento de copias de seguridad y restablecimiento de las mismas? ¿Funciona? Esto es lo que hay que comprobar.

Definir las soluciones necesarias

Con toda la información obtenida de la fase anterior e identificados los riesgos, proponer las soluciones adecuadas y objetivas para mitigar el riesgo o eliminarlo, estableciendo prioridades en función de la severidad del riesgo encontrada.

En esta fase se determinan las medidas a tomar, los tiempos necesarios para su implementación, el coste y se actualizan los protocolos en caso de que sea necesario (revisiones).

Implantar los cambios necesarios

En aras de incrementar la seguridad de la empresa y de gestionar los riesgos se deben implementar las soluciones aportadas en la fase anterior y realizar un calendario de implementación.

Estos cambios suelen ser actualizaciones de software y hardware, aplicación de las correctas configuraciones, impartir formación adecuada a los empleados, actualizar las políticas de seguridad, adopción de nuevas tecnologías, instalación de software de seguridad como firewalls, IDS, IPS, sistemas de monitorización del tráfico de red, etc.

Monitorización y evaluación de resultados

Tras las modificaciones necesarias se hace necesario evaluar los resultados y monitorizar el correcto funcionamiento de los sistemas, para verificar si alcanzan el objetivo perseguido, aumentar el nivel de seguridad.

En algunos casos, se vuelve a realizar todo el proceso de auditoría para verificar que realmente se han cumplido los objetivos perseguidos a la hora de mejorar la seguridad y el cumplimiento.

Por supuesto, esto es un proceso de mejora continua, los planes de seguridad, los procedimientos, la propia tecnología no es estática, sino que está en constante evolución y cada vez más rápido por lo que hay que repetir estos procesos constantemente. Al menos hay que hacer una auditoría anual.

FASES DE UNA AUDITORÍA DE HACKING ÉTICO

El término hacking ético hace referencia al proceso de verificar la seguridad de una entidad y poder detectar las potenciales vulnerabilidades a través de las cuales un atacante podría alterar el buen funcionamiento de los equipos afectando a la triada CIA.

Un Pentesting o test de penetración simula un ataque al igual que lo haría un atacante con el objetivo de verificar el estado de la seguridad, y poder tomar las medidas adecuadas con los resultados obtenidos, y consta de las siguientes fases:

Fase 1: reconocimiento (Reconnaissance)

En esta fase trataremos de recopilar toda la información acerca de nuestro objetivo (empresa a auditar).

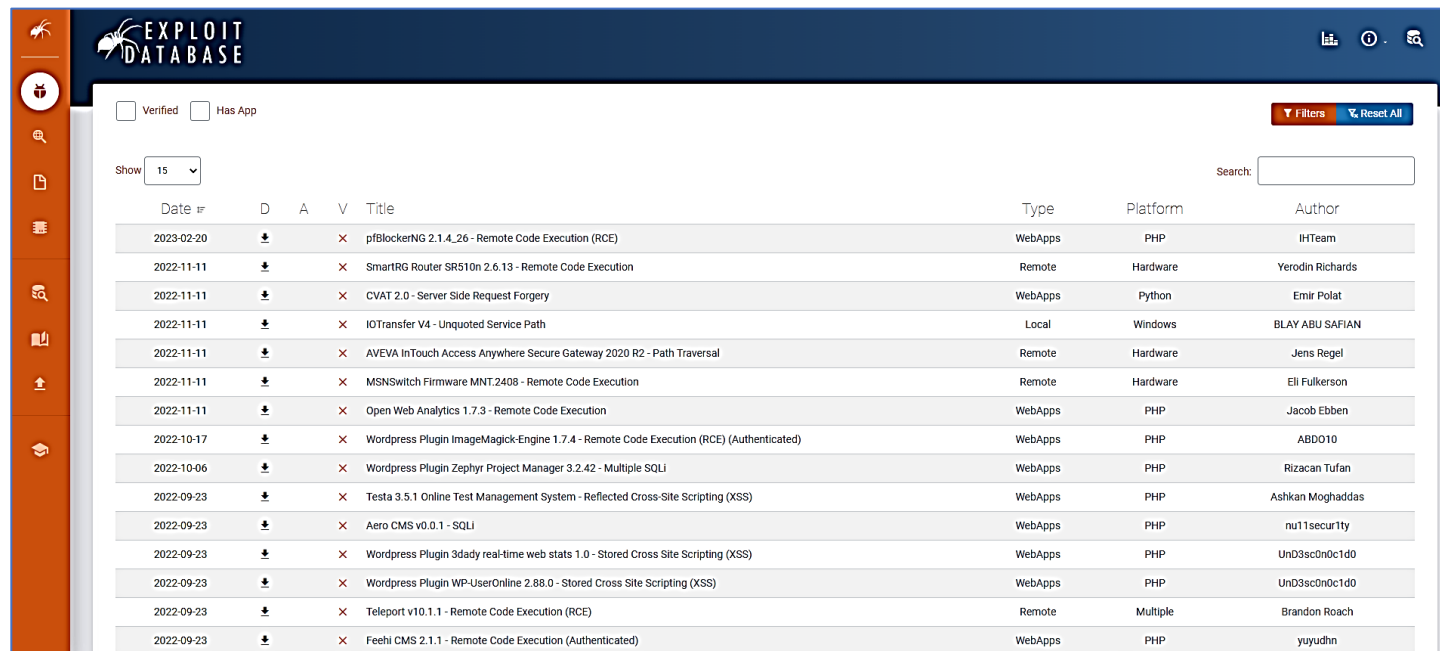
Obtendremos información sobre todo de fuentes abiertas, es decir, información pública en internet que podemos obtener a través de buscadores como Google, Bing, Yahoo, DuckDuckGo, etc.

La información a recopilar será:

- Nombre de personas que trabajan en la empresa, sus puestos, responsabilidades, teléfonos emails corporativos, redes sociales que usan, por ejemplo, es común encontrar en redes profesionales como LinkedIn este tipo de información, además

muchas veces los trabajadores aclaran en sus perfiles tecnologías concretas con las que trabajan que nos pueden dar una idea de la infraestructura de la empresa objetivo.

- Ubicaciones físicas de las instalaciones.
- Análisis de direcciones IP y rangos.
- Análisis de sistemas autónomos (ASNs).
- Dominios, subdominios y relaciones.
- Se usan técnicas como **Browser Hacking**, es decir usar los operadores adecuados para realizar búsquedas muy finas en buscadores como Google, lo que se conoce como **Google hacking**, y en concreto, las búsquedas son los **Dorks de Google** que podemos encontrar en bases de datos como Exploit-db.



The screenshot shows the Exploit Database website interface. It features a dark blue header with the 'EXPLOIT DATABASE' logo and navigation icons. Below the header, there are filters for 'Verified' and 'Has App', a 'Show' dropdown set to '15', and a search bar. The main content is a table listing various exploits with columns for Date, D (Download), A (Add), V (Verify), Title, Type, Platform, and Author.


Date	D	A	V	Title	Type	Platform	Author
2023-02-20	↓		×	pfblockerNG 2.1.4.26 - Remote Code Execution (RCE)	WebApps	PHP	IHTeam
2022-11-11	↓		×	SmartRG Router SR510n 2.6.13 - Remote Code Execution	Remote	Hardware	Yerodin Richards
2022-11-11	↓		×	CVAT 2.0 - Server Side Request Forgery	WebApps	Python	Emir Polat
2022-11-11	↓		×	IoTTransfer V4 - Unquoted Service Path	Local	Windows	BLAY ABU SAFIAN
2022-11-11	↓		×	AVEVA InTouch Access Anywhere Secure Gateway 2020 R2 - Path Traversal	Remote	Hardware	Jens Regel
2022-11-11	↓		×	MSNSwitch Firmware MNT2408 - Remote Code Execution	Remote	Hardware	Eli Fulkerson
2022-11-11	↓		×	Open Web Analytics 1.7.3 - Remote Code Execution	WebApps	PHP	Jacob Ebben
2022-10-17	↓		×	Wordpress Plugin ImageMagick-Engine 1.7.4 - Remote Code Execution (RCE) (Authenticated)	WebApps	PHP	ABD010
2022-10-06	↓		×	Wordpress Plugin Zephyr Project Manager 3.2.42 - Multiple SQLi	WebApps	PHP	Rizacan Tufan
2022-09-23	↓		×	Testa 3.5.1 Online Test Management System - Reflected Cross-Site Scripting (XSS)	WebApps	PHP	Ashkan Moghaddas
2022-09-23	↓		×	Aero CMS v0.0.1 - SQLi	WebApps	PHP	nu11secuR1ty
2022-09-23	↓		×	Wordpress Plugin 3dady real-time web stats 1.0 - Stored Cross Site Scripting (XSS)	WebApps	PHP	UnD3sc0n0c1d0
2022-09-23	↓		×	Wordpress Plugin WP-UserOnline 2.88.0 - Stored Cross Site Scripting (XSS)	WebApps	PHP	UnD3sc0n0c1d0
2022-09-23	↓		×	Teleport v10.1.1 - Remote Code Execution (RCE)	Remote	Multiple	Brandon Roach
2022-09-23	↓		×	Feehi CMS 2.1.1 - Remote Code Execution (Authenticated)	WebApps	PHP	yuyudhn

Podemos usar herramientas como **Shodan**, un buscador muy especial que tiene cacheados todos los sistemas públicos en internet y servicios que corren en los mismos, con vulnerabilidades, donde podemos encontrar desde servidores, webcams, routers, sistemas SCADA, centrales nucleares, etc. y que nos da información acerca de banners, puertos, servicios, versiones como puedes observar a continuación.

Shodan
Maps
Images
Monitor
Developer
More...

SHODAN
Explore
Downloads
Pricing
webstore
Account

TOTAL RESULTS
381

TOP COUNTRIES


United States	123
Germany	60
France	30
Netherlands	29
China	19
More...	

TOP PORTS

443	95
3001	69
80	63
5001	10
8081	10
More...	

TOP ORGANIZATIONS

A100 ROW GmbH	29
---------------	----

View Report
View on Map

Partner Spotlight: Looking for a place to store all the Shodan data? Check out [Gravwell](#)

Site: [Specialty Sites](#)

103.149.202.31
webstore-ist02.cochlear.com
webstore-usf.cochlear.com
slm-ist02.cochlear.com
slm-ist.cochlear.com
webstore-ist.cochlear.com
COCHLEAR LIMITED
Australia, Sydney

SSL Certificate

HTTP/1.1 200 OK
Date: Sat, 18 Mar 2023 10:41:57 GMT
Content-Type: text/html; charset=UTF-8
Set-Cookie: T581baa379=813f13f259f7e97fe39bd845d29a6e09399e0d253d59ad9286ee519f6cf7cd0f9f666db3d2ff70cc051ef6a7b4d288cf24d7fe9; Path=/; Domain=...

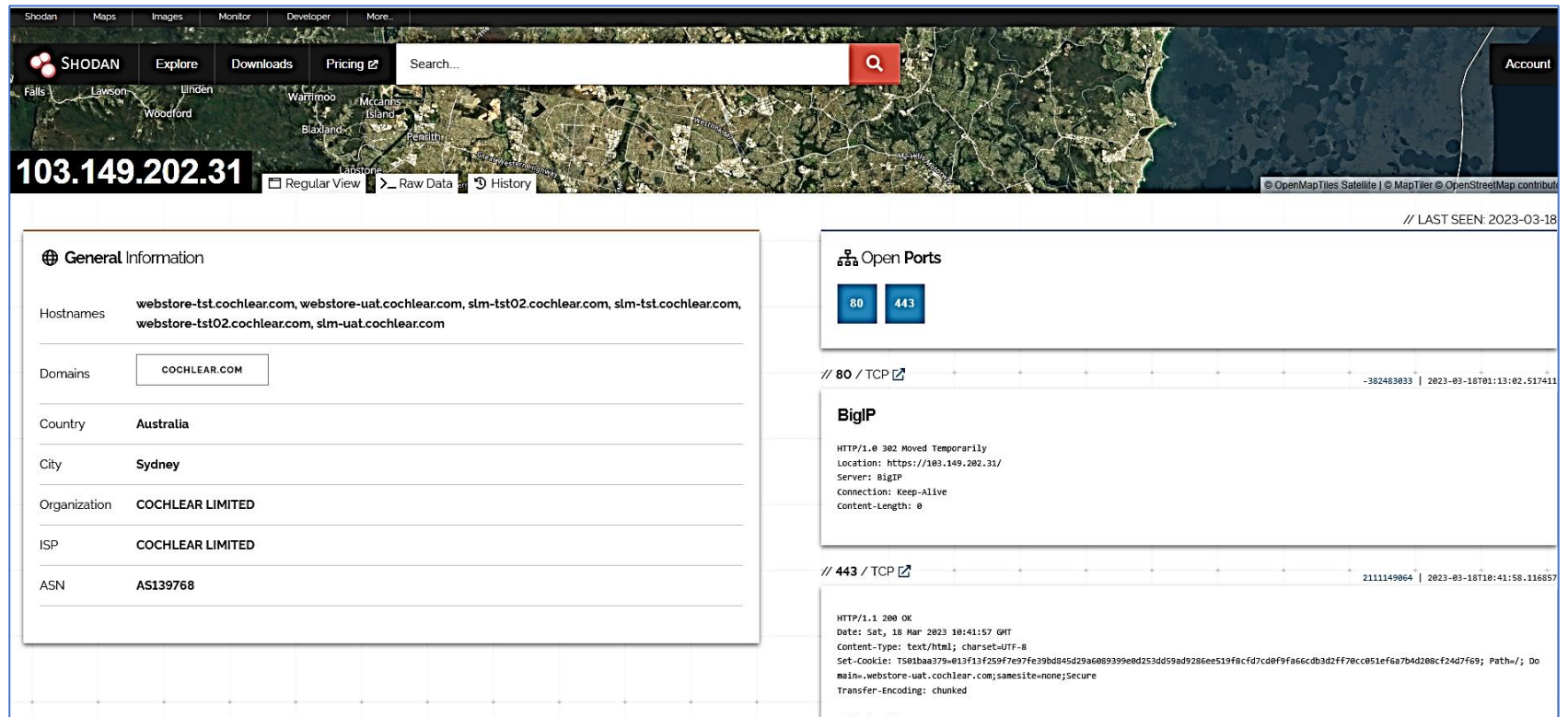
91.232.12.90
smtp4.rosman.ru
Summit Systems Ltd.
Russian Federation, Moscow

<!doctype html>
<html>
<head>
<title>UniFi Video</title>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
<meta name="description" content="">
<meta name="author" content="">
<meta name="viewport" content="w...

52.204.199.74
vkkearmesaparts.com
www.vkkearmesaparts.com

SSL Certificate

HTTP/1.1 301 Moved Permanently



The screenshot shows the Shodan search engine interface. At the top, there's a navigation bar with links like Shodan, Maps, Images, Monitor, Developer, and More. Below this is a search bar with the IP address 103.149.202.31 entered. The search results are displayed in a grid. The first result is for the IP 103.149.202.31, which is associated with the domain COCHLEAR.COM. The result is categorized as 'General Information' and shows details such as Hostnames, Domains, Country (Australia), City (Sydney), Organization (COCHLEAR LIMITED), ISP (COCHLEAR LIMITED), and ASN (AS139768). To the right of the main result, there's a section for 'Open Ports' showing ports 80 and 443. Below this, there's a detailed view of the port 80/TCP, showing the BigIP service and its location. The interface also includes a map of the location and a sidebar with various filters and options.

Existen herramientas de recopilación automática como **Maltego**, capaz de extraer mucha información de internet a través de sus transformadas. Puedes descargar esta herramienta tanto para Linux como para Windows, aunque ya está incorporada en frameworks de seguridad como Kali Linux y Parrot.

Podemos recopilar información sobre exfiltraciones de cuentas de usuario y credenciales en lugares como **PasteBin**, simplemente haciendo una búsqueda en Google.

Proceso temporal de desarrollo

NEZF00 FEB 5TH, 2023 25 0

Ruby 4.05 KB | History | 0 0 report view

... su papel en la difusión de explotaciones de seguridad informática y la realización de ataques cibernéticos contra objetivos ... de prevenir y m

Tags: FCYE

Untitled

A GUEST FEB 22ND, 2023 21 0

text 3.07 KB | None | 0 0 report view

... /2023</fecha>

<datos_emisor>

<nombre>Seguridad Informatica,S.L.</nombre>

<ci>B1522231< ... /2023</fecha>

<datos_emisor>

<nombre>Seguridad Informatica,S.L.</nombre>

<ci>B1522231< ...

Untitled

A GUEST JUL 22ND, 2022 30 0

text 96.00 KB | None | 0 0 report view

... de verificación (los «Procedimientos de seguridad»). Los Procedimientos de seguridad tienen por objeto confirmar que usted ... o sus filiales.

Riesgo de seguridad informática. Existe un riesgo para la seguridad y el funcionamiento técnico del ...

Untitled

A GUEST FEB 1ST, 2023 10 0

text 59.13 KB | None | 0 0 report view

... > Gestión de redes

 Seguridad informática

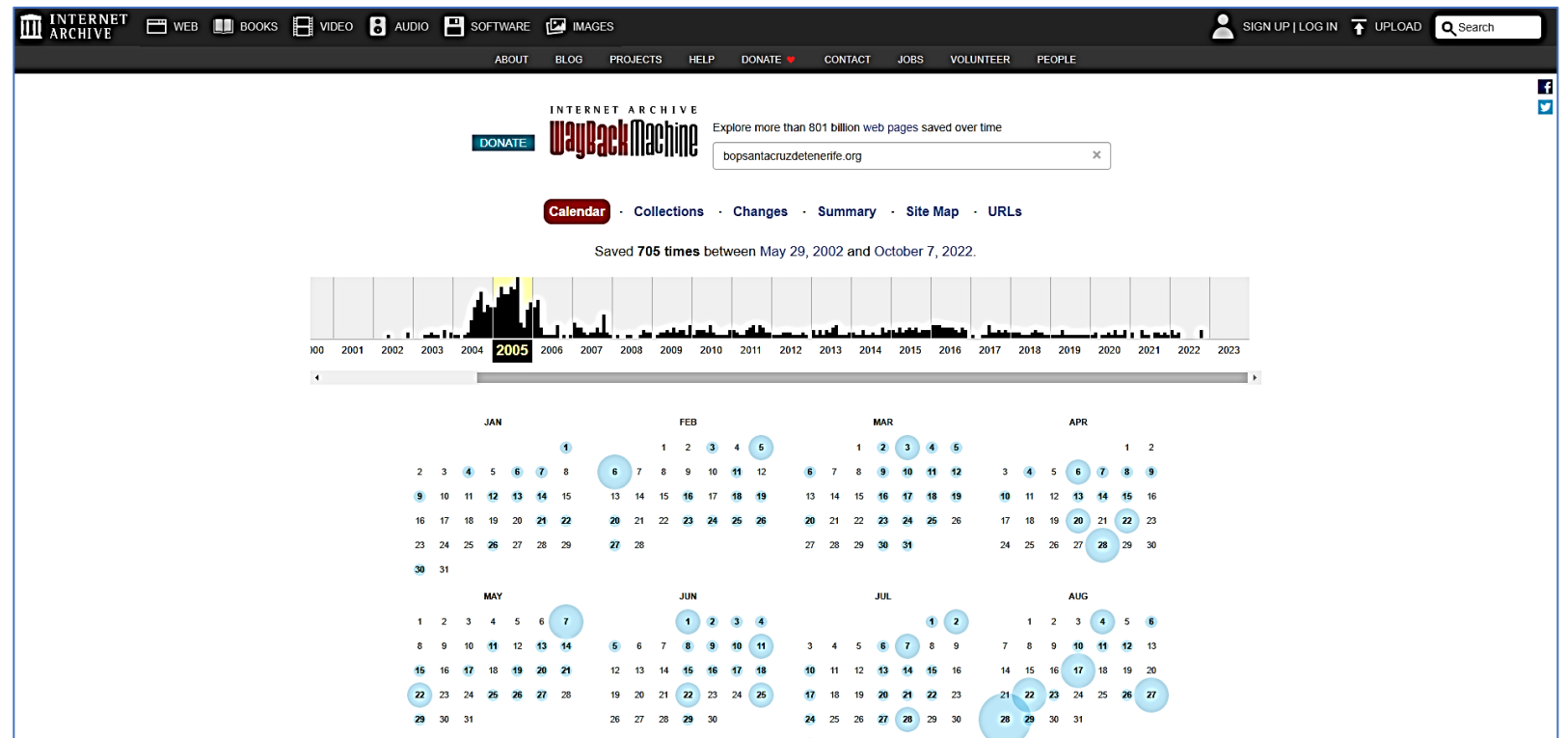
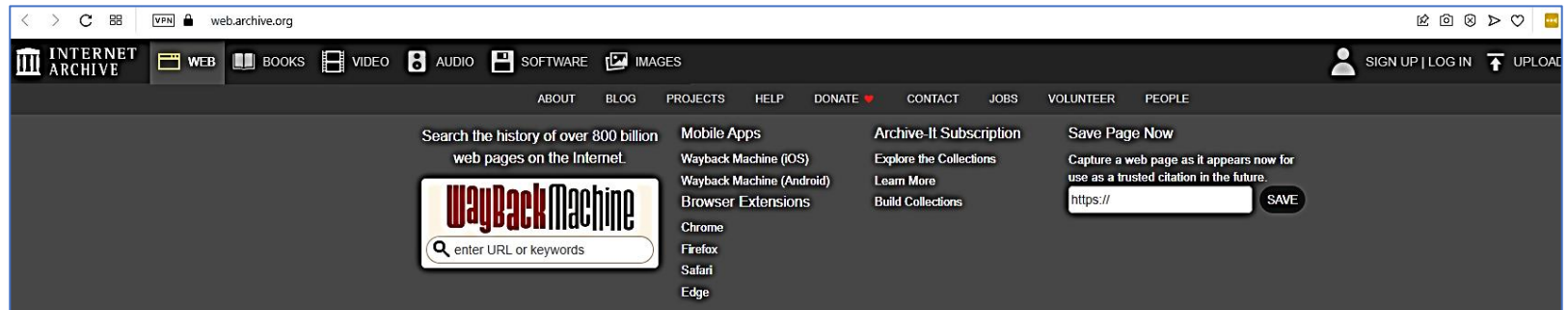
 Configuración de sistemas y ... ; Revisión y mantenimiento de los sistemas de seguridad informática. Instalación y configuraci

Advertisement

Advertise Here

Advertise Here

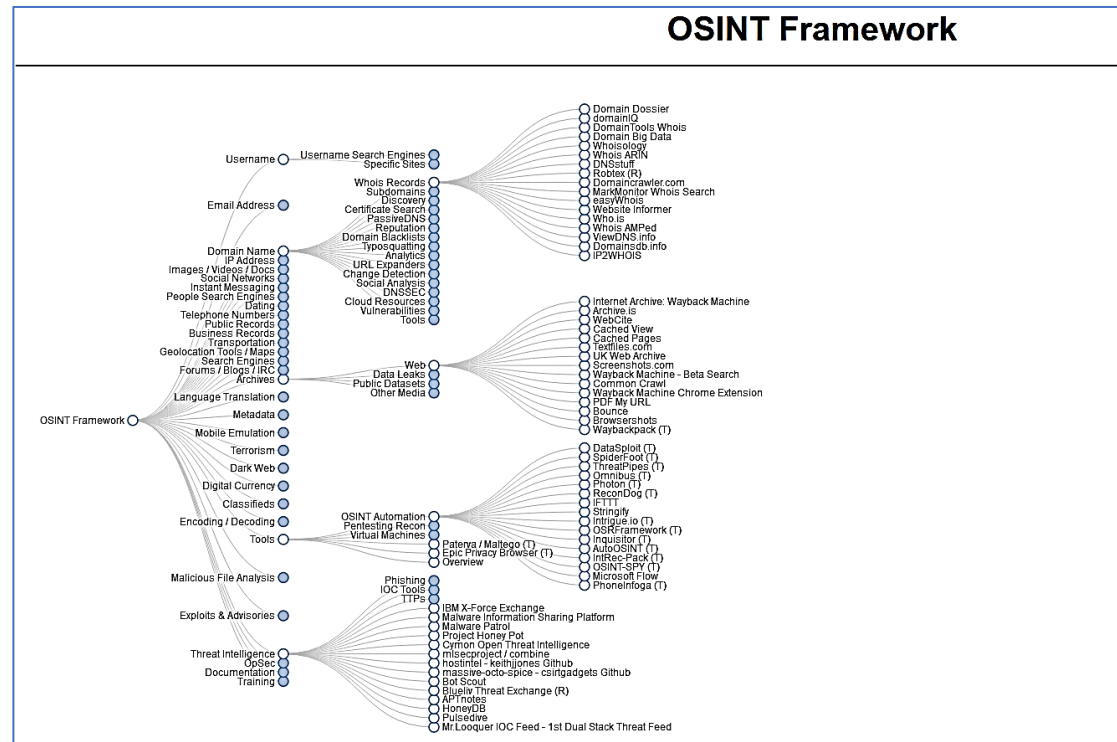
Encontraremos más información a recopilar buscando históricos de páginas web, es decir, versiones antiguas de una web donde podía existir información que en la versión actual no existe, y que puede ser valiosa para nuestra recopilación de información. En este sentido hay una web muy buena, en la que además encontrarás otras joyas que es **archive.org (WayBackMachine)**. En esta web podemos acceder a todas las versiones de la web solicitada como puedes ver a continuación:



Otra herramienta que nos puede proporcionar información valiosa son los metadatos, y en concreto una de las más usadas es **FOCA** (de Chema Alonso), donde puedes extraer

información adjunta en los metadatos de los archivos como nombres de usuarios, correos electrónicos, dominios, subdominios, direcciones IP, documentos, etc.

Y por supuesto, para mí la gran herramienta que es la metodología **OSINT (Open Source Intelligence)** y su **Osint Framework**, donde te vas a volver loco/a con la cantidad de herramientas de recopilación de información que hay. Es más, muchas de estas herramientas son online con lo cual ni siquiera tienes que realizar ningún tipo de instalación, y otras muchas, las que hay que instalar suelen venir incorporadas en los frameworks de seguridad como Kali Linux.



Es importante que sepas que hasta el momento no estamos haciendo nada ILEGAL, obviamente no, ya que tendremos autorización por parte de la empresa para realizar nuestra auditoría, pero, en cualquier caso, podríamos usar libremente estas herramientas en el sentido de que toda esta información la podríamos obtener Googleando. Eso sí el uso que ya después des a esa información podría ser ILEGAL.

No obstante, al hacer estas búsquedas, y por supuesto para las siguientes fases, es conveniente **hacer uso del anonimato**, mediante VPN, proxies o la red TOR.

Fase 2: escaneo y enumeración (scanning)

En esta fase podemos distinguir entre **dos tipos de análisis**, el **pasivo** y el **activo**.

En **el análisis pasivo no tenemos interacción directa con nuestro objetivo**, en cambio, cuando realizamos un **análisis activo ya estamos teniendo interacción con la máquina objetivo** y esto ya sí es ILEGAL, y lo recalco en mayúsculas porque es importante que sepas que el uso de estas herramientas no es un juego, y que pueden tener consecuencias legales.

En esta fase se realizan las siguientes actividades:

- **Análisis pasivo de sistemas vivos**, o lo que es lo mismo, que están activos, en el que no tenemos interacción directa con los equipos objetivo, ya que estaremos usando

herramientas online para la obtención de información, eso sí, como ya te expliqué anteriormente es conveniente que hagas uso del anonimato, ya que estas webs pueden guardar registros (logs) de tus visitas y búsquedas, así mismo Google acaba mosqueándose y vas a tener que estar todo el rato buscando aviones, autobuses y motos en los captchas.

- **Análisis pasivo de servicios habilitados**, también con herramientas online.
- **Escaneo de red mediante ARP**, para identificar equipos vivos dentro de la red, aquí ya estamos haciendo un análisis activo.
- **Escaneos de red**, con el objetivo de conocer los puertos que están abiertos en un equipo, los servicios que corren detrás de esos puertos, sus versiones, con lo que podemos saber si son o no vulnerables o si hay puertos inseguros que pudieran ser un vector de ataque. Aquí principalmente haremos uso de NMAP, aunque existen otras muchas herramientas, que no sólo de NMAP vive el hombre. En este caso también estamos haciendo análisis o reconocimiento activo.
- **Enumeración mediante DNS**, identificando dominios y subdominios, realizando transferencias de zona AXFR si es posible, etc.

Fase 3 Análisis de vulnerabilidades

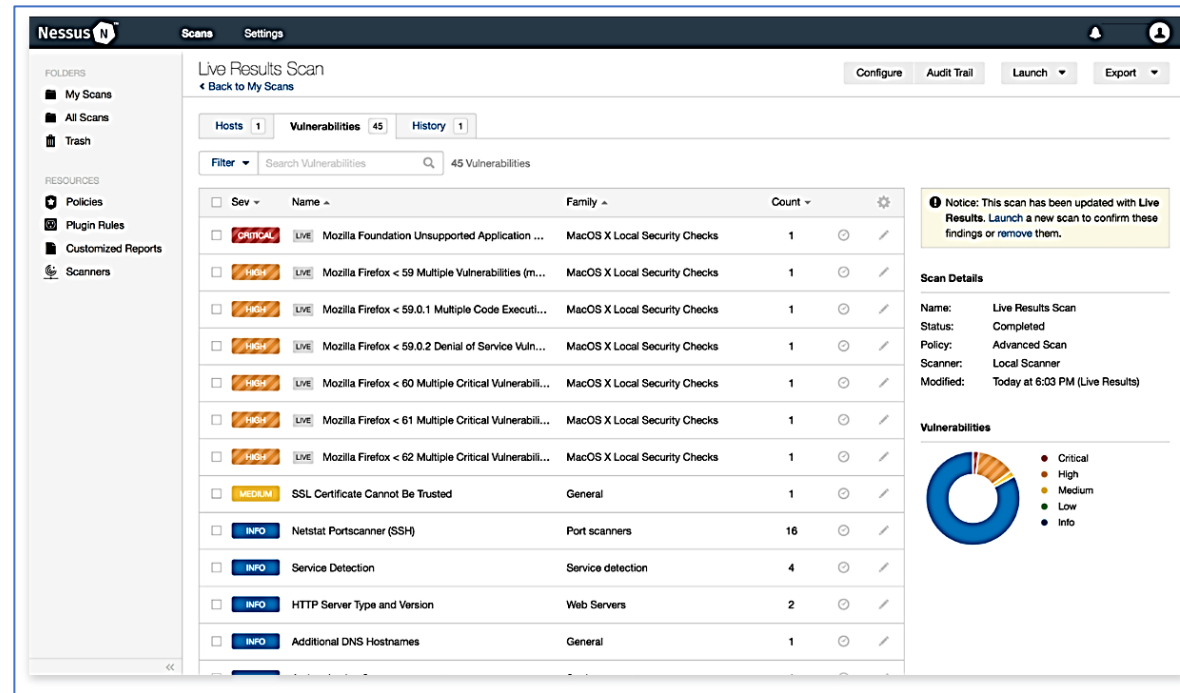
El análisis de vulnerabilidades tiene como objetivo conocer y evaluar las debilidades de un sistema, aplicación, sistema operativo, etc., con el objetivo de conocer los **CVE** a los que se

está expuesto, puertos, servicios vulnerables, etc., que pueden impactar en la continuidad del negocio.

Puede ser que nuestra auditoría acabe aquí, con lo que estaríamos haciendo una auditoría de vulnerabilidades (**vulnerability assesment**) que realmente finalizaría con los informes técnico y ejecutivo ya mencionados anteriormente. Pero si estamos realizando un Pentesting, avanzaremos a las siguientes fases.

Lo bueno de un análisis de vulnerabilidades es que no requiere que la persona que lo ejecuta tenga tantos conocimientos, es rápido y barato ya que se suelen emplear herramientas que lo realizan de forma automática, que nos generan reportes con las vulnerabilidades encontradas, que además podemos descargar en un formato adecuado para poderlos incluir en nuestro informe. Usaremos herramientas como **Nessus, Acunetix, OpenVas, GFI LANguard, o Qualys** entre otras.

En la siguiente imagen puedes ver la pantalla inicial de la herramienta de análisis de vulnerabilidades **Nessus**, donde podemos escoger entre diferentes tipos de análisis, que tendrás disponibles dependiendo de la versión.



The screenshot shows the Nessus web interface for a 'Live Results Scan'. The left sidebar contains navigation links for Folders (My Scans, All Scans, Trash) and Resources (Policies, Plugin Rules, Customized Reports, Scanners). The main content area displays a table of vulnerabilities with columns for Severity, Name, Family, and Count. A filter bar at the top allows searching for vulnerabilities. On the right, a 'Scan Details' panel shows the scan name, status, policy, scanner, and modification time. Below this, a 'Vulnerabilities' donut chart shows the distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

Sev	Name	Family	Count
Critical	Live Mozilla Foundation Unsupported Application ...	MacOS X Local Security Checks	1
Critical	Live Mozilla Firefox < 59 Multiple Vulnerabilities (m...	MacOS X Local Security Checks	1
Critical	Live Mozilla Firefox < 59.0.1 Multiple Code Executi...	MacOS X Local Security Checks	1
Critical	Live Mozilla Firefox < 59.0.2 Denial of Service Vuln...	MacOS X Local Security Checks	1
Critical	Live Mozilla Firefox < 60 Multiple Critical Vulnerabili...	MacOS X Local Security Checks	1
Critical	Live Mozilla Firefox < 61 Multiple Critical Vulnerabili...	MacOS X Local Security Checks	1
Critical	Live Mozilla Firefox < 62 Multiple Critical Vulnerabili...	MacOS X Local Security Checks	1
Medium	SSL Certificate Cannot Be Trusted	General	1
Info	Netstat Portscanner (SSH)	Port scanners	16
Info	Service Detection	Service detection	4
Info	HTTP Server Type and Version	Web Servers	2
Info	Additional DNS Hostnames	General	1

Scan Details

- Name: Live Results Scan
- Status: Completed
- Policy: Advanced Scan
- Scanner: Local Scanner
- Modified: Today at 6:03 PM (Live Results)

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

En la siguiente imagen puedes ver el resultado de un análisis de vulnerabilidades con Nessus donde nos indica las vulnerabilidades encontradas, cuánto de críticas son, ofreciéndonos su CVSS que es el nivel de riesgo, así como su CVE y la descripción de la vulnerabilidad, así como los enlaces a las posibles soluciones cuando pinchamos en una de las vulnerabilidades.

Nessus Scans Settings

Lab Scan
← Back to My Scans

Configure Launch Export

Hosts 9 Vulnerabilities 144 Remediations 216 History 1


1 Filter Search Vulnerabilities 144 Vulnerabilities

Sev	Name	Family	Count
CRITICAL	Bash Incomplete Fix Remote Code Execution Vulner...	Gain a shell remotely	3
CRITICAL	Bash Remote Code Execution (CVE-2014-6277 / CV...	Gain a shell remotely	3
CRITICAL	Bash Remote Code Execution (Shellshock)	Gain a shell remotely	3
CRITICAL	CentOS 4 / 5 / 6 : firefox (CESA-2012:0079)	CentOS Local Security Checks	1
CRITICAL	CentOS 4 / 5 : firefox / xulrunner (CESA-2011:1164)	CentOS Local Security Checks	1
CRITICAL	CentOS 4 / 5 : krb5 (CESA-2011:1851)	CentOS Local Security Checks	1
CRITICAL	CentOS 5 / 6 / 7 : bash (CESA-2014:1293)	CentOS Local Security Checks	1
CRITICAL	CentOS 5 / 6 / 7 : bash (CESA-2014:1306)	CentOS Local Security Checks	1
CRITICAL	CentOS 5 / 6 : java-1.6.0-openjdk (CESA-2013:0770)	CentOS Local Security Checks	1
CRITICAL	CentOS 5 / 6 : java-1.6.0-openjdk (CESA-2013:1014)	CentOS Local Security Checks	1
CRITICAL	CentOS 5 / 6 : samba (CESA-2012:0465)	CentOS Local Security Checks	1
CRITICAL	CentOS 5 : java-1.6.0-openjdk (CESA-2012:0730)	CentOS Local Security Checks	1

Scan Details

Name: Lab Scan
Status: Completed
Scanner: Local Scanner
Start: Today at 5:31 PM
End: Today at 6:01 PM
Elapsed: 30 minutes

Vulnerabilities



- Critical
- High
- Medium
- Low
- Info

Como contrapartida un análisis de vulnerabilidades aporta poco valor al cliente, ya que el hecho de que encontremos vulnerabilidades no necesariamente implica que puedan ser explotables, ya que pueden existir sistemas intermedios que protejan la infraestructura como Firewalls, IPS, entre otros, además de que estas herramientas nos pueden reportar falsos positivos o no encontrar vulnerabilidades que realmente existan y que puedan tener un gran impacto en la continuidad del negocio.

Por lo que resulta más interesante, aunque por contrapartida más costoso, en tiempo, dinero y recursos la realización de un Pentesting de forma ofensiva como si fuéramos un atacante real que ataca al objetivo poniendo a prueba su seguridad, a sus trabajadores para conocer lo concienciados o no que están en materia de seguridad informática, por ejemplo, haciendo uso de técnicas como la ingeniería social.

Fase 3: obtener acceso /explotación (Gaining Access)

Una vez que ya tenemos la suficiente información sobre las posibles vulnerabilidades, tenemos que buscar la forma de aprovecharlas para ganar acceso al sistema objetivo, y poder explotar esa vulnerabilidad con diferentes objetivos, como puede ser escalar privilegios, obteniendo una cuenta de administrador que me permite hacer más cosas, hacer una denegación de servicios (ataque DoS), etc.

Un exploit es una pieza de código que puede estar escrita en diferentes lenguajes de programación como puede ser Ruby, Python u otros, que nos permite aprovechar una debilidad o vulnerabilidad, que se puede ejecutar de dos formas:

- **Exploit Local:** que se ejecuta localmente en el sistema, cuyo objetivo suele ser escalar privilegios una vez ya estamos dentro del sistema ya que hemos tenido éxito con un Exploit Remoto.
- **Exploit Remoto:** Este se ejecuta desde el equipo atacante, comúnmente vía internet.

Si tenemos en cuenta dónde va a impactar nuestro Exploit, tenemos dos modalidades:

- **Server Side:** nos aprovechamos de una vulnerabilidad de una aplicación, protocolo o servicio a la que se puede acceder de forma directa.
- **Cliente Side:** se explota una vulnerabilidad del lado del cliente, teniendo en cuenta que este como ya hemos mencionado, es el eslabón más débil de la cadena, o sea, el usuario final, que generalmente tiene sus equipos desactualizados, que se fía de correos electrónicos tipo Phishing, etc., etc.

Es importante que conozcas mi lema No Todo Es Metasploit. **Metasploit** es la herramienta que se suele usar para lanzar los exploits, pero como te digo, no todo es Metasploit, ya que se pueden explotar vulnerabilidades mediante ingeniería social, o simplemente acceder a un router porque el usuario ha dejado el usuario y las claves por defecto, con lo que no hace falta ninguna herramienta en particular, ya tenemos las puertas de la casa abiertas, en otras ocasiones las contraseñas de los usuarios son muy predecibles, o lo más aberrante a mis ojos, es cuando están pegadas en un Post-it en la pantalla a la vista de todo el mundo.

Pero bueno, quiero aclarar que mi lema No Todo Es Metasploit, realmente viene por otra razón, y es que al final Metasploit cuando lo manejas es una herramienta fácil de usar, incluso tienes muchos tutoriales por internet, pero una vez que has accedido al sistema tienes que tener unos conocimientos muy grandes de muchas cosas para realmente hacer algo de provecho, como por ejemplo sistemas operativos, saber dónde se almacenan los logs, contraseñas, conocer el funcionamiento de las bases de datos, importantísimo más

aún es tener un sólido conocimiento de redes y protocolos, en fin, que a veces nos creemos que con Metasploit ya está todo hecho y la realidad no es así, y requiere que estemos formándonos de forma continua en cosas muy diversas, al menos para conocer lo básico de cada área, porque por supuesto luego tendrás que especializarte en algo, porque quien mucho abarca poco aprieta, y no podemos ser maestros de todo.

Como ya sabrás la herramienta más conocida para esta fase es Metasploit o la versión gráfica **Armitage**, aunque los verdaderos hackers hacen sus propias herramientas y exploits.

Fase 4: mantener acceso (maintaining Access)

Esta fase también la podemos llamar fase de Post Explotación, es decir lo que vamos a hacer una vez tenemos acceso al sistema y buscar la forma de poder acceder cuando quiera sin tener que realizar todo el proceso de Explotación de nuevo.

En esta fase, haremos un análisis del entorno comprometido, elevación de privilegios, extracción de credenciales, control del sistema, obtención de información y modificación de tiempos, exfiltración de información, suplantación y análisis mediante sniffers de red como Wireshark para capturar el tráfico de red, Pivoting o movimiento lateral a otras redes.

Por supuesto, en esta fase se procede a la instalación de puertas traseras (Backdoors), Rootkits y Troyanos que me garanticen un posterior acceso al equipo.

Fase 5: limpiar huellas (clearing tracks)

Esta fase es muy importante, ya que no queremos dejar rastro de nuestra estancia y acciones en el equipo objetivo, por lo que, echando mano de nuestro conocimiento de los sistemas, realizaremos acciones que nos permitan no dejar rastro como:

- Borrar caché y cookies.
- Ocultar ficheros: ADS Streams.
- Modificar algunos valores del registro.
- Volver a habilitar auditorías que hayamos deshabilitado previamente.
 - Auditpol.exe /disable
 - Auditpol.exe /enable
- Borrar alertas que se hayan generado en el visor de sucesos (Event Viewer).
 - Hay que tener en cuenta que se borran todos los sucesos, pero queda un registro de log referente a la acción del borrado.
 - Herramientas como Elsave o Winpazer permiten el borrado del registro de sucesos de forma remota, obviamente teniendo los privilegios adecuados.
- Borrar correos enviados, si por ejemplo hemos usado técnicas de Phishing.
- Borrar la papelera de reciclaje, caché del navegador, historiales, temporales, etc.
 - Se pueden usar herramientas como Evidence Eliminator.
- Ocultar ficheros con el uso de los atributos de ficheros o mediante esteganografía.
- Borrar logs que nos comprometan.

- Cerrar los puertos abiertos.
- Desinstalación de aplicaciones usadas para lograr nuestros objetivos.
- Borrar usuarios creados en el sistema.

Aprovecho para dejarte una reflexión de Sun Tsu que escribió en su tratado “El Arte de la Guerra”

“Conoce a tu enemigo y a ti mismo y en cien batallas nunca serás derrotado; Si eres ignorante de tu enemigo, pero te conoces a ti mismo, las probabilidades de ganar o perder serán las mismas; si eres ignorante de tu enemigo y de ti mismo, saldrás derrotado siempre”

Fase 6: Documentación, conclusiones y recomendaciones (Documentation)

Como ya dijimos, hay que documentar todo el proceso, y es aquí donde vamos a plasmar nuestra evaluación de seguridad, hallazgos, no conformidades, lo que se puede mejorar, nuestras conclusiones finales y recomendaciones, teniendo en cuenta la realización de dos informes el técnico y el ejecutivo, este último de vital importancia, ya que si la gerencia de la empresa, que no tiene por qué tener conocimientos técnicos no entiende lo que le queremos transmitir, de poco sirve el trabajo realizado, ya que finalmente son ellos los que tienen que dar el visto bueno para implementar y afrontar los costes de las mejoras que sean necesarias.

TIPOS DE AUDITORÍAS DE HACKING ÉTICO, METODOLOGÍAS, NORMAS Y LEYES

Tipos de auditorías de hacking ético

Cuando hablamos de tipos de auditorías de hacking ético, comúnmente hacemos referencia a las 3 principales que son, **caja blanca, caja gris y caja negra**, pero existen más tipos que hacen la auditoría aún más compleja.

- **Blind/BlackBox:** el auditor o analista de seguridad no tiene conocimiento del objetivo, y dispone de casi nada de información, probablemente apenas el nombre de la empresa, pero el cliente sí que sabe que le van a realizar una auditoría y el momento y ventanas horarias en que será realizada.
- **Double Bind/Blackbox:** parecido a lo anterior, sólo que en este caso el cliente tampoco sabe quién ni cómo ni cuándo se ejecutará la auditoría.
- **GrayBox:** el auditor dispone de pocos datos sobre el objetivo, eso sí alguno más que en la BlackBox, por ejemplo, puede tener una IP del objetivo, o un usuario, y con esa poca información debe ir tirando del hilo, obteniendo toda la información necesaria. El cliente si conoce el alcance de la auditoría, los test que se van a realizar y la ventana horaria.
- **Double GrayBox:** similar al anterior, pero como en el caso del Doble Bind/BlackBox, el cliente tampoco sabe cuándo se realizará el análisis.

- **WhiteBox:** el auditor dispone de toda la información necesaria para realizar su trabajo, IPs, infraestructura de red, usuarios, contraseñas, correos, etc. En este caso, ambas partes, auditor y cliente saben el tipo de test a realizar, cuándo se hacen, su alcance, etc.
- **Reversal:** similar al anterior, el auditor dispone de toda la información necesaria pero el cliente no sabe ni cómo ni cuándo se realizará el análisis.

Obviamente los análisis BlackBox y GrayBox, son los más largos, costosos y que requieren de más recursos, pudiendo durar entre 3 y 6 meses, ya que hay que buscar toda la información necesaria, en cuanto que un WhiteBox puede durar pocas semanas, de 1 a 3 semanas aproximadamente. Estos tiempos dependen de muchos factores, entre otros el alcance de la auditoría, y del número de cosas que vayamos a auditar, no es lo mismo 1 servidor que 20 o que toda la infraestructura de la empresa.

A estas fases habría que añadir al inicio la fase de planificación de la auditoría, que incluía las reuniones con el cliente, para definir aspectos como el alcance de la auditoría, lo que se va a auditar, cómo se va a hacer, que impacto tendrán los test a ejecutar sobre los procesos de negocio, ventanas horarias de realización de los test, contratos, autorizaciones, etc.

Metodologías comúnmente usadas

Para realizar las auditorías de seguridad se usan metodologías, esto es importante porque tenemos que seguir un procedimiento, y usar unas herramientas que permitan que si otro auditor usa la misma metodología y las mismas herramientas pueda llegar a las mismas conclusiones, esto también es importante en otras ramas como el análisis forense. Piensa que es lo mismo que cuando se usa el método científico.

Vamos a describir brevemente algunas de las metodologías más usadas, ya que, en sí, son un mundo a estudiar de forma detenida, la mayoría son metodologías abiertas, de libre acceso, y te recomiendo que las estudies ya que nos aportan mucha información desde los procedimientos a seguir, explicación de muchos aspectos técnicos de gran valor para ampliar nuestro conocimiento y las herramientas y el uso que tenemos que hacer de ellas.

OSSTM (OPEN-SOURCE SECURITY TESTING METHODOLOGY MANUAL)

OSSTMM es una metodología abierta de ISECOM (Institute for security and Open Methodologies) para pentesting, test de seguridad, análisis y medida de la seguridad operacional para poder defender nuestra organización. Actualmente se encuentra en su versión 3 (OSSTMM3), en su web puedes descargar el libro con la metodología. Es una metodología que se queda un poco antigua pero que aún usan muchas empresas, donde se explica cómo hacer varios tipos de auditorías, web, de sistemas, de redes,

física, ingeniería social, pero que no explica en detalle cómo hacer las cosas muy en detalles.

Personalmente, no es una metodología que me guste, ya que es muy genérica, y existen otras metodologías que son más especializadas como OWASP específicamente para aplicaciones Web o OWISAM para redes inalámbricas, que además de estar especializadas en un tipo de auditoría específica, nos detallan los controles que tenemos que hacer y herramientas a usar.



En la siguiente imagen tienes un extracto del índice de contenidos para que te hagas una idea de los temas que trata.

Table of Contents

Instructions.....	2
Quick Start.....	2
Upgrading from Older Versions.....	2
Version Information.....	3
About this Project.....	3
Restrictions.....	4
Primary Developers.....	5
Primary Contributors.....	5
Contributors, Reviewers, and Assistants.....	6
Foreword	7
Introduction.....	11
Purpose.....	13
Document Scope.....	13
Liability.....	13
Certification and Accreditation.....	14
Related Projects.....	17
Chapter 1 – What You Need to Know.....	20
1.1 Security.....	23
1.2 Controls.....	24
1.3 Information Assurance Objectives.....	27
1.4 Limitations.....	28
1.5 Actual Security.....	31
1.6 Compliance.....	31
Chapter 2 – What You Need to Do.....	33
2.1 Defining a Security Test.....	33
2.2 Scope.....	34
2.3 Common Test Types.....	36
2.4 Rules Of Engagement.....	38
2.5 The Operational Security Testing Process.....	41
2.6 Four Point Process.....	43
2.7 The Trifecta.....	44
2.8 Error Handling.....	46
2.9 Disclosure.....	51
Chapter 3 – Security Analysis.....	53
3.1 Critical Security Thinking.....	54
3.2 Recognize the OpSec Model.....	56
3.3 Look for Pattern Matching as a Sign of Errors.....	57
3.4 Characterize the Results.....	57
3.5 Look for Signs of Intuition.....	58
3.6 Transparent Reporting.....	59
Chapter 4 – Operational Security Metrics.....	62
4.1 Getting to Know the Rav.....	63
4.2 How to Make a Rav.....	67
4.3 Turning Test Results into an Attack Surface Measurement.....	70
4.4 The Operational Security Formula.....	79
4.5 The Controls Formula.....	80
4.6 The Limitations Formula.....	83
4.7 The Actual Security Formula.....	85

Chapter 5 – Trust Analysis.....	87
5.1 Understanding Trust	87
5.2 Fallacies in Trust.....	89
5.3 The Ten Trust Properties.....	90
5.4 The Trust Rules.....	91
5.5 Applying Trust Rules to Security Testing.....	94
Chapter 6 – Work Flow.....	96
6.1 Methodology Flow.....	97
6.2 The Test Modules	99
6.3 One Methodology.....	103
Chapter 7 - Human Security Testing.....	105
Chapter 8 - Physical Security Testing.....	120
Chapter 9 - Wireless Security Testing.....	138
Chapter 10 - Telecommunications Security Testing.....	151
Chapter 11 - Data Networks Security Testing.....	167
Chapter 12 - Compliance.....	185
Regulations.....	186
Chapter 13 – Reporting with the STAR.....	192
Chapter 14 – What You Get.....	204
The Möbius Defense.....	205
Get What We Need.....	206
Chapter 15 – Open Methodology License.....	208
The OML 3.....	208

Esta metodología incluye un marco de trabajo donde podemos encontrar las fases de realización de una auditoría, en la que se revisan los siguientes aspectos.

Sección A -Seguridad de la Información

- Revisión de la Inteligencia Competitiva.
- Revisión de Privacidad.
- Recolección de Documentos.

Sección B - Seguridad de los Procesos

- Testeo de Solicitud.
- Testeo de Sugerencia Dirigida.
- Testeo de las Personas Confiables.

Sección C - Seguridad en las tecnologías de Internet

- Logística y Controles.
- Exploración de Red.
- Identificación de los Servicios del Sistema.
- Búsqueda de Información Competitiva.
- Revisión de Privacidad.
- Obtención de Documentos.
- Búsqueda y Verificación de Vulnerabilidades.
- Testeo de Aplicaciones de Internet.

- Enrutamiento.
- Testeo de Sistemas Confiados.
- Testeo de Control de Acceso.
- Testeo de Sistema de Detección de Intrusos.
- Testeo de Medidas de Contingencia.
- Descifrado de Contraseñas.
- Testeo de Denegación de Servicios.
- Evaluación de Políticas de Seguridad.

Sección D - Seguridad en las Comunicaciones

- Testeo de PBX.
- Testeo del Correo de Voz.
- Revisión del FAX.
- Testeo del Modem.

Sección E - Seguridad Inalámbrica

- Verificación de Radiación Electromagnética (EMR).
- Verificación de Redes Inalámbricas [802.11].
- Verificación de Redes Bluetooth.
- Verificación de Dispositivos de Entrada Inalámbricos.
- Verificación de Dispositivos de Mano Inalámbricos.
- Verificación de Comunicaciones sin Cable.

- Verificación de Dispositivos de Vigilancia Inalámbricos.
- Verificación de Dispositivos de Transacción Inalámbricos.
- Verificación de RFID.
- Verificación de Sistemas Infrarrojos.
- Revisión de Privacidad.

Sección F - Seguridad Física

- Revisión de Perímetro.
- Revisión de Monitoreo.
- Evaluación de Controles de Acceso.
- Revisión de Respuesta de Alarmas.
- Revisión de Ubicación.
- Revisión de Entorno.

Muchas de estas metodologías, son certificables, y sabrás que esto de las certificaciones en IT es muy importante, ya que avalan o garantizan que conoces un producto o en este caso una metodología, que es un estándar en la industria. Dado que el mundo de la tecnología es bastante cambiante, estas certificaciones se deben realizar cada 3 años. Verás que en muchas ofertas de trabajo se solicita tenerlas. OSSTMM dispone de las siguientes certificaciones:



OSSTMM Professional Security Analyst

The OPSA is a technical, skills-based certification designed to accredit professional security analysts.



OSSTMM Professional Security Tester

The OPST is a technical, skills-based certification designed to accredit professional penetration testers.



OSSTMM Professional Security Expert

The OPSE is an introductory, knowledge-based certification designed to accredit security professionals working with the OSSTMM.



OSSTMM Wireless Security Expert

The OWSE is a technical, knowledge-based certification designed to accredit professional penetration testers.



OSSTMM Certified Trust Analyst

The CTA is a knowledge-based certification designed to accredit professionals measuring trust or making trust-based decisions either in a business or security capacity.



Certified Security Awareness Instructor

The SAI is a knowledge-based certification designed to accredit professionals teaching cybersecurity awareness.



Certified Hacker Analyst

The CHA is an introductory, technical, knowledge-based certification designed to accredit students for a well-rounded foundation in professional cybersecurity.



Certified Hacker Analyst Trainer

The CHAT is a technical, knowledge-based certification designed to accredit teachers teaching cybersecurity training such as the Certified Hacker Analyst and Hacker Highschool.



Certified Cyber Trooper

The CCT is a hands-on cyberwarfare certification to show a deep knowledge of the technical aspects of cybersecurity exclusively for military personnel.

ISSAF (INFORMATION SYSTEMS SECURITY ASSESSMENT FRAMEWORK)

ISSAF es una metodología desarrollada por OISSG (Open Information Systems Security Group) que clasifica la evaluación de seguridad en varios dominios cada uno con sus criterios de prueba.

En esta metodología se incluyen controles de ISO 27000, Sarbanes Oxley, CoBIT, COSO y SAS70.

Se basa en los siguientes criterios a evaluar y documentar:

- Descripción de los criterios de evaluación.
- Objetivos y finalidad.
- Prerrequisitos para las evaluaciones.
- Presentación de resultados (Informes).
- Recomendaciones y contramedidas.
- Referencias a documentos de fabricantes.

Esta metodología considera las siguientes fases para un Pentesting:

- FASE 1: Planteamiento.
- FASE 2: Evaluación.
- FASE 3: Tratamiento.

- FASE 4: Acreditación.
- FASE 5: Mantenimiento.

Estas fases contienen procesos como la recopilación de información, identificación e inventario de los recursos, riesgos, compliance (regulaciones legales), mapeo de la red, políticas de seguridad de la empresa, identificación de vulnerabilidades, explotación, escalada de privilegios, mantenimiento del acceso y borrado de huellas.

ISSAF (INFORMATION SYSTEMS SECURITY ASSESSMENT FRAMEWORK)

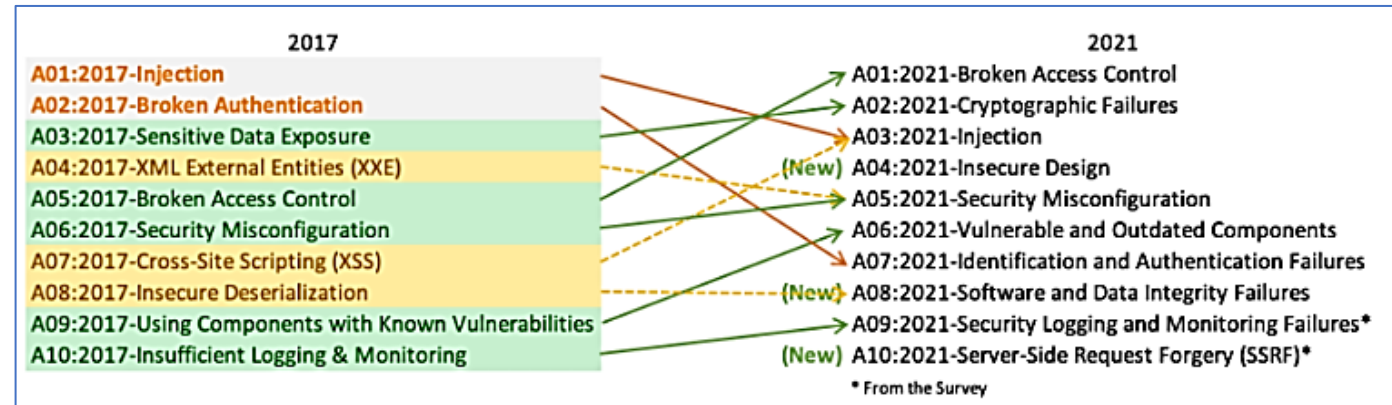
Esta metodología está especializada en aplicaciones Web e importante especialmente para los desarrolladores, también es de código abierto.

OWASP promueve el desarrollo de software seguir, centrado principalmente en aplicaciones web, concretamente en el Back-End.

Dispone de una amplia documentación a cerca de las brechas de seguridad más comunes y de varios proyectos de interés, todos de forma gratuita, como son:

- Tool projects.
- Code projects.
- Documentation projects.
- OWASP TOP TEN.
- OWASP AntiSamy Project.

Destaca su proyecto OWASP TOP TEN Web Application Security Vulnerabilities, que es una lista de los 10 fallos de seguridad más comunes.



Las herramientas que proporciona para la realización de auditorías también son libres y de código abierto, entre ellas destacan las siguientes.

- OWTF: herramienta de pentesting.
- WebGoat: aplicación de pruebas para encontrar vulnerabilidades que ilustra escenarios reales.
 - Cross Site Scripting.
 - Inyecciones SQL.
 - Robo de sesiones.
 - Inyecciones XPath.
 - Mecanismos de autenticación.
 - Manipulación de parámetros.

- WebScarab: framework de análisis de tráfico HTTP/HTTPS.
- Zed Attack Proxy: Análisis de vulnerabilidades en aplicaciones.
- Dependency Check: permite comprobar las dependencias de las aplicaciones y sus vulnerabilidades.
- SSL advanced forensic tool: muestra información acerca de SSL/TLS y certificados.
- Mobile security Project: para pentesting en aplicaciones móviles.

Enlace web OWASP: <https://owasp.org/>

Enlace a guía de desarrollo OWASP en Español:

[https://owasp.org/www-pdf-archive/OWASP Development Guide 2.0.1 Spanish.pdf](https://owasp.org/www-pdf-archive/OWASP_Development_Guide_2.0.1_Spanish.pdf)

Enlace a guía de pruebas OWASP:

[https://owasp.org/www-pdf-archive/Gu%C3%ADa de pruebas de OWASP ver 3.0.pdf](https://owasp.org/www-pdf-archive/Gu%C3%ADa_de_pruebas_de_OWASP_ver_3.0.pdf).

CEH (CERTIFIED ETHICAL HACKING)

CEH es una de las certificaciones más conocida y solicitada por los reclutadores, desarrollada por EC-Council (International Council of Electronic Commerce). Actualmente (año 2022) se encuentra en su versión 11.

En esta certificación se tratan todos los aspectos de la ciberseguridad y hacking ético reconociendo las siguientes fases:

- Fase de reconocimiento.
- Fase de escaneo.
- Fase de análisis de vulnerabilidades.
- Fase de Hackeo de sistemas.

Así mismo trata temas como tipos de código malicioso usado por los atacantes, Sniffing, ingeniería social, ataques DoS (Denial of service) o denegación de servicio, técnicas y herramientas para el secuestro de sesiones de usuarios legítimas, hacking web, Firewalls, IDS o sistemas de detección de intrusos, IPS o sistemas de prevención de intrusos, hacking de servidores web, ataques de inyección SQL, IoT, Cloud computing, criptografía, etc.



OFFENSIVE SECURITY

Otra de las metodologías importantes y deseadas en torno al mundo del Pentesting y seguridad ofensiva. Permite conocer de forma práctica como explotar sistemas buscar brechas de seguridad y formas en que un atacante actuaría. Se podría definir como Un proceso evaluativo a nivel de seguridad informática, comprobación de vulnerabilidades dentro d ellos sistemas de información e infraestructuras tecnológicas, donde se realizan ataque a diferentes tipos de entornos para descubrir fallos de seguridad.

Hace uso de herramientas como el framework de seguridad Kali Linux y su certificación más relevante es OSCP (certificado profesional de seguridad ofensiva) donde nos enseñan atacar un sistema de varias formas dentro de un ambiente seguro, es una certificación bastante exigente, ya que requiere mostrar tus habilidades de forma real.



OWISAM

OWISAM (Open Wireless Security Assessment Methodology) es una metodología abierta que permite la realización de auditorías de seguridad Wireless, creada por dos hermanos españoles Andrés y Miguel Tarrasco.

Al igual que OWASP, también tiene su OWISAM TOP TEN donde se ponen de manifiesto los principales riesgos en redes inalámbricas, que actualmente son:

- OWISAM-TR-001: red de comunicaciones Wi-Fi abierta.
- OWISAM-TR-002: presencia de cifrado WEP en redes de comunicaciones.
- OWISAM-TR-003: algoritmo de generación de claves del dispositivo inseguro (contraseñas y WPS).
- OWISAM-TR-004: Clave WEP/WPA/WPA2 basada en diccionario.
- OWISAM-TR-005: mecanismos de autenticación inseguros (LEAP, PEAP-MD5,).
- OWISAM-TR-006: dispositivo con soporte de Wi-Fi protected setup PIN activo (WPS).
- OWISAM-TR-007: red Wi-Fi no autorizada por la organización.
- OWISAM-TR-008: portal hotspot inseguro.
- OWISAM-TR-009: cliente intentando conectar a red insegura.
- OWISAM-TR-010: rango de cobertura de la red demasiado extenso.

En su web puedes encontrar tanto la metodología en sí como los controles a realizar, las herramientas y su uso, de una forma bastante detallada, te recomiendo mucho que indagues en ella ya que te va a aportar muchísimo conocimiento tecnológico a cerca de las redes inalámbricas.

En la siguiente imagen verás la Wiki de OWISAM, donde en su panel izquierdo puedes encontrar la metodología, sus controles y el software a usar.



Inicio - Start

Top 10

Controles - Controls

Metodología - Methodology

802.11

Security Scoring

Software

Distros

Lista de correo - Mailing list

Material adicional - Additional Resources

Autores - Authors

Wiki links

Página principal

Actualidad

Cambios recientes

Página aleatoria

Herramientas

Lo que enlaza aquí

Cambios relacionados

Páginas especiales

Versión para imprimir

Enlace permanente

Información de la página

Citar esta página

[Página principal](#)
[Discusión](#)

[Leer](#)
[Ver código](#)
[Ver historial](#)

Página principal

OWISAM (Open WIREless Security Assessment Methodology)

Otros idiomas:

English  **español** 

La presencia cada vez mayor de redes de comunicaciones inalámbricas, así como el uso de equipos portátiles y dispositivos móviles, conectados a redes domésticas y corporativas, expone el perímetro de las organizaciones a un gran número de ataques contra su infraestructura. En la actualidad, tanto las empresas como los analistas de seguridad informática, no disponen de un mecanismo estandarizado con el que analizar y clasificar el riesgo de las redes Wi-Fi.

Existen otras metodologías de seguridad, como OWASP [1] y OSSTMM [2], que referencian aspectos de seguridad relativos a las redes inalámbricas, sin analizar en profundidad los riesgos existentes. El enfoque de OWISAM es diseñar de una metodología ágil y usable que ayude a realizar con éxito un análisis de seguridad sobre estos entornos.

OWISAM, acrónimo de **Open Wireless Security Assessment Methodology** (Metodología de evaluación de seguridad wireless abierta), surge con el objetivo de cubrir una necesidad existente, poner en común con la comunidad los controles de seguridad que se deben verificar sobre redes de comunicaciones inalámbricas y definir una metodología abierta y colaborativa que ayude a administradores de redes, administradores de sistemas y a analistas de seguridad informática a identificar riesgos, a minimizar el impacto de los ataques informáticos y a garantizar la protección de las infraestructuras Wireless basadas en el estándar 802.11 [3].

La licencia de la metodología **OWISAM** es Creative Commons Attribution ShareAlike 3.0 license (CC-BY-SA) [4], permitiendo su uso, modificación y reproducción por cualquier individuo.

Esta licencia ayuda a que toda la comunidad colabore en el desarrollo de esta metodología, uniendo conocimientos y asegurando que todos los puntos de vista han sido contemplados.

Algunos recursos de interés integrados en OWISAM:

- **Controles OWISAM:** Lista de controles de seguridad definidos por OWISAM.
- **OWISAM Top 10:** Análisis de los principales riesgos de seguridad existentes en redes inalámbricas.
- **Metodología:** Información sobre la metodología OWISAM.
- **Mailing:** Listas de correo electrónico.
- **Twitter:** sigue las novedades de #owisam con Twitter en @owisam_org.

En esta edición de la metodología han colaborado los siguientes Autores.

Buscamos tu colaboración para que OWISAM crezca. Contacta con nosotros por [Twitter](#) o en la [lista de correo](#).

¡Anímate a colaborar en el wiki.

En lo que se refiere al software generalmente es software libre, aunque hay alguna aplicación comercial como Acrylic WIFI, que te recomiendo que pruebes, ya que es bastante interesante.

El software y las distros usadas en esta metodología son las siguientes:

- Aplicaciones gratuitas libres (Open source / free)
- Airodump-ng <http://www.aircrack-ng.org>
- Acrylic WiFi Free <https://www.acrylicwifi.com/acrylic-wifi-gratuito/>
- Reaver WPS <http://code.google.com/p/reaver-wps/>
- inSSIDer <http://www.metageek.net/products/inssider/>
- aircrack-ng <http://aircrack-ng.org>
- AirTraf <http://airtraf.sourceforge.net/>
- Kismet <http://www.kismetwireless.net/>
- Void11 <http://www.wirelessdefence.org/Contents/Void11Main.htm>

Aplicaciones Comerciales

- Acrylic WiFi heatmaps <https://www.acrylicwifi.com/acrylic-wifi-heatmaps-mapas-de-cobertura/>
- Wi-SPY: <http://www.metageek.net/products/wi-spy-wireless-spectrum-analysis/>
- Silica <http://www.immunityinc.com/products-silica.shtml>

Distros Linux

- Kali Linux: <https://kali.org>
- Wifi Slax: <http://www.wifislax.com/>
- Wifi way: <http://www.wifiway.org/>

PTES

Por último, PTES (Penetration Testing Execution Standard), una de las metodologías estandarizadas para Pentesting, ofrece un lenguaje común para los pentesters a la hora de hacer sus evaluaciones de seguridad.

Enfocada principalmente a la ejecución técnica de un Pentesting, por lo que se define de forma detallada los objetivos para cada prueba realizada en cada una de sus fases, y se acompaña de una guía con multitud de herramientas para cada prueba, además de determinar las pautas y alcance de cada una.



Las fases de esta metodología son muy similares a las ya comentadas.

Planeación e interacciones previas al compromiso.

Se definen aquí cosas como el alcance de la prueba, lo que se permite o no se permite hacer, ventanas horarias, inicio de las pruebas y cierre. Firma de contratos entre empresa y auditor, así como de terceros involucrados. Reuniones y resolución de dudas y preguntas.

Recopilación de información.

Recopilación de toda la información necesaria sobre activos o procesos.

Modelado de amenazas.

Identificación de los activos que tienen más probabilidades de ser atacados, determinando su valor, impacto y los procesos críticos a los que se afecta.

Análisis de vulnerabilidades.

Descubrir las brechas de seguridad, vulnerabilidades en sistemas y aplicaciones que pueden ser aprovechadas por un atacante, mediante la realización de pruebas activas, análisis del tráfico y análisis de vulnerabilidades. Una vez identificamos las vulnerabilidades podemos investigar cómo explotar esa vulnerabilidad, si existen exploits disponibles, etc.

Explotación.

Se accede al recurso evadiendo los sistemas de seguridad como antivirus, cortafuegos, etc. Siempre teniendo en cuenta el alcance establecido en el contrato.

Se usan exploits específicos para esas vulnerabilidades o incluso se aprovechan vulnerabilidades de día 0.

Explotación posterior.

Mantener acceso y control de la máquina.


Establecemos el valor del activo que viene determinado por el valor de los datos que contiene el activo, y si nos permite comprometer otras máquinas de la red, exfiltración de información, instalación de puertas traseras, creación de usuarios, etc.

Informes.

Como siempre realizaremos un informe técnico y otro ejecutivo, describiendo todas las pruebas realizadas para cada fase, sus resultados, etc.

Métricas de riesgo.

Existen herramientas y metodologías para la evaluación del riesgo, PTES no lo es pero nos sugiere cómo calcular el riesgo mediante la metodología FAIR.



[Main page](#)
[PTES Technical Guideline](#)
[In the Media](#)
[FAQ](#)

[Tools](#)
[What links here](#)
[Related changes](#)
[Special pages](#)
[Printable version](#)
[Permanent link](#)
[Page information](#)

Log in

[Main page](#)
[Read](#)
[View source](#)
[View history](#)

Main Page

High Level Organization of the Standard

The penetration testing execution standard consists of seven (7) main sections. These cover everything related to a penetration test - from the initial communication and reasoning behind a pentest, through the intelligence gathering and threat modeling phases where testers are working behind the scenes in order to get a better understanding of the tested organization, through vulnerability research, exploitation and post exploitation, where the technical security expertise of the testers come to play and combine with the business understanding of the engagement, and finally to the reporting, which captures the entire process, in a manner that makes sense to the customer and provides the most value to it.

This version can be considered a v1.0 as the core elements of the standard are solidified, and have been "road tested" for over a year through the industry. A v2.0 is in the works soon, and will provide more granular work in terms of "levels" - as in intensity levels at which each of the elements of a penetration test can be performed at. As no pentest is like another, and testing will range from the more mundane web application or network test, to a full-on red team engagement, said levels will enable an organization to define how much sophistication they expect their adversary to exhibit, and enable the tester to step up the intensity on those areas where the organization needs them the most. Some of the initial work on "levels" can be seen in the intelligence gathering section.

Following are the main sections defined by the standard as the basis for penetration testing execution:

- Pre-engagement Interactions
- Intelligence Gathering
- Threat Modeling
- Vulnerability Analysis
- Exploitation
- Post Exploitation
- Reporting

As the standard does not provide any technical guidelines as far as how to execute an actual pentest, we have also created a technical guide to accompany the standard itself. The technical guide can be reached via the link below:

- Technical Guidelines

For more information on what this standard is, please visit:

- The Penetration Testing Execution Standard: FAQ

Normas y Leyes

NORMA ISO 27000 SERIES

Las normas ISO de la familia ISO/IEC27000 conforman un conjunto de estándares orientados a las buenas prácticas, seguridad de la información y mitigación del riesgo, relacionadas con la implementación, gestión y mantenimiento de un SGSI o sistema de gestión de la información y que también sigue la filosofía de mejora continua, conocida como Ciclo Deming o PDCA, (Plan-Do-Check-Act), que es la abreviatura de las fases de este ciclo que son Planificar, Hacer, Verificar y Actuar.

La hemos llamado familia de normas ISO porque en realidad se compone de varias ISOs relacionadas entre sí.

- **ISO 27001:** especifica los requisitos para implantar y gestionar un SGSI. Esta norma es certificable.
- **ISO 27002:** conjunto de buenas prácticas para la implantación del SGSI mediante 114 controles, estructurados en 14 dominios y 35 objetivos de controles.
- **ISO 27003:** guía para la correcta implantación de un SGSI.
- **ISO 27004:** define y establece métricas que permiten evaluar el rendimiento del SGSI.
- **ISO 27005:** gestión de riesgos en los sistemas de gestión de la información.
- **ISO 27006:** requisitos a cumplir por las organizaciones que quieran acreditarse y para certificar a otras en el cumplimiento de la ISO/IEC-27001.
- **ISO 27007:** guía de procedimientos para realizar auditorías internas o externas basadas en la ISO/IEC-27001 .
- **ISO 27008:** evaluación de los controles del SGSI para revisar la adecuación técnica para que sean eficaces a la hora de mitigar los riesgos.
- **ISO 27009:** complementa la norma 27001 incluyendo nuevos requisitos y controles de aplicación en sectores específicos.
- **ISO 27010:** tratamiento de la información cuando es compartida con terceros, explica qué riesgos pueden suceder y los controles a establecer para mitigarlos, especialmente en infraestructuras críticas.

- **ISO 27011:** establece los principios para implantar, mantener y gestionar un SGSI en el ámbito de las organizaciones de telecomunicaciones.
- **ISO 27013:** establece cómo integrar las normas 27001 (SGSI) y 20000 Sistema de Gestión de Servicios (SGS) en aquellas organizaciones que implementan ambas.
- **ISO 27014:** principios para el gobierno de la seguridad de la información, para evaluar, monitorizar y comunicar las actividades relacionadas con la seguridad de la información.
- **ISO 27015:** principios de implantación de un SGSI en empresas prestadoras de servicios financieros, bancarios o banca electrónica.
- **ISO 27016:** toma de decisiones económicas vinculadas a la gestión de la seguridad de la información.
- **ISO 27017:** 37 controles específicos para los servicios en la nube, basados en la norma 27002.
- **ISO 27018:** complementa a las normas 27001 y 27002 en la implantación de procedimientos y controles para proteger datos personales en la nube para empresas que prestan servicios a terceros.
- **ISO 27019:** basada en la norma 27002 de aplicación a las industrias del sector energéticos a la hora de implantar un SGSI.

LEYES A NIVEL EUROPEO

- Directiva 2016/1148, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad en las redes y sistemas de información de la Unión.

- Reglamento Europeo de Protección de Datos 2016/679 (RGPD).
- Ley de Seguridad Cibernética (Cybersecurity Act). Aprobada el 27 de junio de 2019 por la UE.

NORMAS DE SEGURIDAD NACIONAL

- Ley 36/2015, de 28 de septiembre, de Seguridad Nacional. Regula los principios, organismos y funciones desempeñadas para la defensa de la Seguridad Nacional.
- Orden TIN/3016/2011, de 28 de octubre. Por la que se crea el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo e Inmigración.

LEYES DE SEGURIDAD

- Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana.
- Ley 5/2014, de 4 de abril, de Seguridad Privada.

LEYES REFERIDAS A LAS TELECOMUNICACIONES

- Ley 34/2002, de 11 de julio, de servicios a la sociedad de la información y comercio electrónico.
- Real Decreto 381/2015, de 14 de mayo, por el que se establecen medidas contra el tráfico no permitido o irregular con fines fraudulentos en comunicaciones electrónicas.
- Ley 50/2003, de 19 de diciembre, de firma electrónica.
- La Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

LEYES ASOCIADAS A CIBERDELINCUENCIA

- Código Penal.
- Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores.
- Real Decreto de aprobación de la Ley de Enjuiciamiento Criminal.

NORMATIVA DE PROTECCIÓN DE DATOS

- La Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD) y el Reglamento General de Protección de Datos o RGPD, son las normas en España de protección y privacidad de datos personales.

LEY SOBRE SEGURIDAD DE LAS REDES DE INFORMACIÓN

- El Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información tiene por objeto regular la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y de los servicios digitales, y establecer un sistema de notificación de incidentes.

Para ello, la nueva normativa sobre ciberseguridad en España se adapta al ordenamiento jurídico español la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo conocida como “Directiva europea sobre ciberseguridad”.

LSSI-CE

Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico, su objetivo es regular el régimen jurídico de los servicios relacionados con Internet y la contratación electrónica. Se aplica en los siguientes supuestos siempre que el prestador del servicio (empresario), obtenga algún tipo de beneficio:

- Comercio electrónico.
- Contratación en línea.
- Información y publicidad.
- Servicios de intermediación.

OTRAS NORMAS Y LEYES DE APLICACIÓN EXTRANJERAS

En este punto te voy a introducir en las leyes principalmente de Estados Unidos, que, aunque no estamos allí, dado que muchas veces las empresas tienen sus infraestructuras virtualizadas en la nube, y estos equipos de la nube se pueden encontrar en diferentes países, con lo que muchas veces no sólo se hace necesario conocer nuestras propias leyes sino también las de otros países. En cualquier caso, algunas de estas leyes también son de cumplimiento en nuestro país.

Las regulaciones más importantes en Estados Unidos son:

- **HIPPA:** (Health Insurance Portability and Accountability Act).

Ley de Transferencia y Responsabilidad de Seguro Médico.

Los profesionales de la salud deben tomar medidas para preservar la confidencialidad de la información médica personal, en función de las preferencias del paciente. Se reconoce el derecho a la confidencialidad a las personas a menos que autoricen revelar esa información. Esta ley trata sobre la confidencialidad, el acceso y la divulgación de la información médica identificable individualmente, o lo que es lo mismo, información sanitaria protegida.

- **PCI-DSS:** (Payment Card Industry Data Security Standard).

Es un estándar de seguridad para gestionar y mejorar la seguridad en cuanto a los pagos online, con los requisitos para proteger la información sensible de las tarjetas de crédito y débito.

Es obligatorio para todas las empresas que aceptan, procesan o transmiten los datos de tarjetas de crédito o débito.

PCI SSC propone 12 requisitos a cumplir por las empresas para los pagos seguros:

- Instalación y mantenimiento de cortafuegos que permita proteger los datos de los propietarios de tarjetas.

- No usar contraseñas por defecto provistos por los proveedores.
- Proteger los datos almacenados de los propietarios de tarjetas.
- Cifrar los datos de las tarjetas y la información confidencial que se transmite mediante redes públicas abiertas.
- Usar y actualizar un software antivirus.
- Desarrollo y mantenimiento de sistemas y aplicaciones seguras.
- Restringir el acceso a los datos.
- Asignar una identificación única a cada persona que tenga acceso a los equipos con información a proteger.
- Restricción del acceso físico a los datos de los propietarios de tarjetas.
- Trackear el acceso a los recursos de la red y datos de los propietarios de tarjetas mediante registros y logs.
- Auditar regularmente los sistemas y procesos de seguridad.
- Mantener políticas que contemplen la seguridad de la información.

- **GLBA.**

La Ley Gramm-Leach-Bliley de 1999 (GLBA) es una ley federal de los EE. UU para la protección de la privacidad y la seguridad de la información financiera de identificación personal (PII) relacionada con las personas.

- **SOX-Sarbanes Oxley.**

La Ley Sarbanes-Oxley, también se conoce como SarOx o SOA (Sarbanes Oxley Act), y regula las funciones financieras contables y de auditoría penalizando severamente, el crimen corporativo y blanqueo de capitales a todas las empresas que coticen en la bolsa de valores de Estados Unidos.

- **FERPA.**

Derechos Educativos de la Familia y Ley de Privacidad, es una ley federal que protege la privacidad de los estudiantes.

APLICACIÓN DE CRITERIOS COMUNES PARA CATEGORIZAR LOS HALLAZGOS COMO OBSERVACIONES O NO CONFORMIDADES

Una no conformidad se define en la ISO 27001 como el incumplimiento de un requisito que atiende a la norma y que además puede serlo también legalmente o por imposición del propio plan de seguridad de la empresa, y que por tanto es algo que hemos dejado de hacer pero que deberíamos, y que implica una acción correctiva formal que elimine el problema de base y su recurrencia, así como que podamos monitorear y evaluar su nivel de eficacia.

Una forma en la que podemos definir el nivel de hallazgo en una auditoría es usar un enfoque que esté basado en el riesgo y las posibles consecuencias en caso de que ocurra un incidente. Este enfoque nos proporciona una mayor transparencia en los esquemas de impacto y probabilidad de ocurrencia, en base a esto se establecen los siguientes niveles de hallazgos:

- **Crítico:** cuando hay una no conformidad en la que falla algo por completo en algún área. Se trata de una no conformidad que requiere acciones inmediatas.
- **Grave o mayor:** no conformidad o fallo en uno o más procesos del SGSI al no seguir correctamente las políticas o controles establecidos. Esta no conformidad puede dar lugar a una crítica si no se aplican las medidas correctivas de mejora.
- **Moderado o medio:** faltas que aún no causan un impacto negativo, que se registran como observaciones y que se deben de analizar y hacer un seguimiento de la evolución del problema en sucesivas auditorías.

- **Baja o menor:** esta no conformidad no tiene un gran impacto negativo, pero sí oportunidades de mejora.

La organización debe reaccionar ante las no conformidades, tomando las medidas correctivas necesarias que previamente habrá evaluado. Los incidentes de seguridad de la información no implican necesariamente que exista una no conformidad, pero pueden servir como indicador de una no conformidad. Existen varios tipos de no conformidades como:

- Incumplimiento de un requisito (total o parcialmente) de ISO / IEC 27001 en el SGSI.
- Implementación incorrecta de requisitos, reglas o controles establecido por el SGSI.
- Incumplimiento parcial o total de los requisitos legales o contractuales.
- Personas que no se comportan como se espera de los procedimientos y políticas.
- Proveedores que no proporcionan productos o servicios acordados.
- Controles que no funcionan según el diseño.
- Controles ineficaces o incompletos.
- Análisis de incidentes de seguridad de la información, mostrando el incumplimiento de un requisito del SGSI.
- Alertas de usuarios o proveedores.
- Resultados de seguimiento y medición que no cumplen con los criterios de aceptación, etc.