Auditoría de Seguridad Informática

CURSO PRÁCTICO

Silvia Clara Menéndez Arantes

Ra-Ma®

eduJ®

Auditoría de Seguridad Informática

Curso práctico

Silvia Clara Menéndez Arantes

Ra-Ma®
eduU®
Conocimiento a su alcance

Menéndez Arantes, Silvia Clara

Auditoría de seguridad informática / Silvia Clara Menéndez Arantes --. Bogotá: Ediciones de la U, 2023
220 p. ; 24 cm
ISBN 978-958-792-509-8 e-ISBN 978-958-792-510-4
1. Informática 2. Seguridad informática 3. Ciberseguridad 4. Incidentes informáticos I. Tít.
621.39 ed.

Edición original publicada por © Editorial Ra-ma (España)
Edición autorizada a Ediciones de la U para Colombia

Área: Informática
Primera edición: Bogotá, Colombia, abril de 2023
ISBN. 978-958-792-509-8

© Silvia Clara Menéndez Arantes
© Ra-ma Editorial. Calle Jarama, 3-A (Polígono Industrial Igarsa) 28860 Paracuellos de Jarama
www.ra-ma.es y www.ra-ma.com / E-mail: editorial @ra-ma.com
Madrid, España
© Ediciones de la U - Carrera 27 #27-43 - Tel. (+57) 601 6455049
www.edicionesdelau.com - E-mail: editor@edicionesdelau.com
Bogotá, Colombia

Ediciones de la U es una empresa editorial que, con una visión moderna y estratégica de las tecnologías, desarrolla, promueve, distribuye y comercializa contenidos, herramientas de formación, libros técnicos y profesionales, e-books, e-learning o aprendizaje en línea, realizados por autores con amplia experiencia en las diferentes áreas profesionales e investigativas, para brindar a nuestros usuarios soluciones útiles y prácticas que contribuyan al dominio de sus campos de trabajo y a su mejor desempeño en un mundo global, cambiante y cada vez más competitivo.

Coordinación editorial: Adriana Gutiérrez M.
Carátula: Ediciones de la U
Impresión: DGP Editores SAS
Calle 63 #70D-34, Pbx (+57) 601 7217756

Impreso y hecho en Colombia
Printed and made in Colombia

No está permitida la reproducción total o parcial de este libro, ni su tratamiento informático, ni la transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, por fotocopia, por registro y otros medios, sin el permiso previo y por escrito de los titulares del Copyright.

A tod@s los que aguantan mis largas horas delante de un ordenador,
mis ideas locas y mis teclados, y aun así me soportan,
especialmente a mis Padres, Hermana, a mi adorable quesito Annabelle,
Eli de cuatro patas (mi adorada perrita que siempre está a mi lado
y que también sabe un montón de Ciberseguridad)
y mi mejor amiga Eli de dos patas.

ÍNDICE

ACERCA DE LA AUTORA **11**

CAPÍTULO 1. CRITERIOS GENERALES COMÚNMENTE ACEPTADOS SOBRE AUDITORÍA INFORMÁTICA **13**

1.1 ¿QUÉ ES UNA AUDITORÍA INFORMÁTICA? 13
1.2 CÓDIGO DEONTOLÓGICO DE LA FUNCIÓN DE AUDITORÍA 14
1.3 RELACIÓN DE LOS DISTINTOS TIPOS DE AUDITORÍA EN EL MARCO DE LOS SISTEMAS DE INFORMACIÓN 19
1.4 CRITERIOS A SEGUIR PARA LA COMPOSICIÓN DEL EQUIPO AUDITOR 20
1.5 EL INFORME DE AUDITORÍA 21
1.6 FASES GENERALES DE UNA AUDITORÍA 23
1.6.1 Planificación inicial, objetivos y alcance 23
1.6.2 Análisis de riesgos y amenazas 24
1.6.3 Definir las soluciones necesarias 24
1.6.4 Implantar los cambios necesarios 25
1.6.5 Monitorización y evaluación de resultados 25
1.7 FASES DE UNA AUDITORÍA DE HACKING ÉTICO 25
1.7.1 Fase 1: reconocimiento (Reconnaissance) 26
1.7.2 Fase 2: escaneo y enumeración (scanning) 31
1.7.3 Fase 3 Análisis de vulnerabilidades 31
1.7.4 Fase 3: obtener acceso /explotación (Gainning Access) 33
1.7.5 Fase 4: mantener acceso (maintaining Access) 35
1.7.6 Fase 5: limpiar huellas (clearing tracks) 35
1.7.7 Fase 6: Documentación, conclusiones y recomendaciones (Documentation) 36
1.8 TIPOS DE AUDITORÍAS DE HACKING ÉTICO, METODOLOGÍAS, NORMAS Y LEYES 37
1.8.1 Tipos de auditorías de hacking ético 37

1.8.2 Metodologías comúnmente usadas 38
1.8.3 Normas y Leyes 51
1.9 APLICACIÓN DE CRITERIOS COMUNES PARA CATEGORIZAR LOS HALLAZGOS COMO OBSERVACIONES O NO CONFORMIDADES 56

CAPÍTULO 2. APLICACIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL 59

2.1 EVOLUCIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS 59
2.2 ASPECTOS DE LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL 60
2.2.1 Derechos ARCO 60
2.2.2 Niveles de seguridad de los ficheros de datos 61
2.2.3 Sanciones por incumplimiento 64
2.2.4 Recursos protegidos dentro de la LOPD 66
2.2.5 Agencia Española de Protección de Datos (AEPD) 67
2.2.6 Auditorias LOPD 69
2.2.7 El papel del DPO 71

CAPÍTULO 3. ANÁLISIS DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN 73

3.1 CONCEPTOS DE ANÁLISIS DE RIESGOS 73
3.2 METODOLOGÍAS DE ANÁLISIS DE RIESGOS Y GUÍAS DE BUENAS PRÁCTICAS 76
3.3 VULNERABILIDADES, MALWARE, ATAQUES, FALLOS DE PROGRAMA, PROGRAMAS MALICIOSOS Y CRITERIOS DE PROGRAMACIÓN SEGURA 77
3.3.1 Ingeniería social 77
3.3.2 Ataques de red 79
3.3.3 Ataques por contraseña 83
3.3.4 Ataques a aplicaciones 84
3.3.5 Amenazas físicas 85
3.3.6 Software malicioso 86
3.3.7 Amenazas al hardware 89
3.3.8 Vulnerabilidades en aplicaciones 93
3.4 GESTIÓN DE RIESGOS 95
3.4.1 Identificar los activos 95
3.4.2 Identificar las amenazas (Threat assessment) 96
3.4.3 Análisis del impacto 96
3.4.4 Priorización de las amenazas 97
3.4.5 Identificar las técnicas de mitigación del riesgo 97
3.4.6 Evaluar el riesgo residual 97
3.5 ESTRATEGIAS DE MITIGACIÓN DEL RIESGO 98
3.6 METODOLOGÍA NIST SP 800-30 99
3.7 METODOLOGÍA MAGERIT 101

CAPÍTULO 4. USO DE HERRAMIENTAS PARA LA AUDITORÍA DE SISTEMAS 107

4.1 HERRAMIENTAS DEL SISTEMA OPERATIVO TIPO PING, TRACEROUTE... 107
4.1.1 Ping 107
4.1.2 Tracert 112
4.1.3 Pathping 114
4.1.4 Netstat 115
4.1.5 Whois 119
4.1.6 Nslookup 122
4.1.7 Ipconfig 126
4.1.8 Getmac 129
4.1.9 Arp -a 131
4.1.10 Netsh 132
4.1.11 Hostname 137
4.1.12 Route 137
4.1.13 Nbtstat 138

4.2 HERRAMIENTAS DE ANÁLISIS DE RED, PUERTOS Y SERVICIOS: NMAP 140

4.3 HERRAMIENTAS DE ANÁLISIS DE VULNERABILIDADES 153
4.3.1 Nessus 153
4.3.2 MBSA 161
4.3.3 OpenVas 163

4.4 ANALIZADORES DE PROTOCOLOS 164
4.4.1 Wireshark 164
4.4.2 Otras aplicaciones de análisis de protocolos 175

4.5 ANALIZADORES DE PÁGINAS WEB 177
4.5.1 OWASP ZAP 177
4.5.2 Acunetix 180

4.6 ATAQUES DE DICCIONARIO Y FUERZA BRUTA TIPO BRUTUS, JOHN THE RIPPER 183
4.6.1 Ataques de fuerza bruta y de diccionario online. Contramedidas 187
4.6.2 Ataque de fuerza bruta y de diccionario Offline 190
4.6.3 Ataques de tablas Rainbow 191

CAPÍTULO 5. DESCRIPCIÓN DE LOS ASPECTOS SOBRE CORTAFUEGOS EN AUDITORÍAS DE SISTEMAS INFORMÁTICOS 193

5.1 TIPOS DE FIREWALL 193
5.1.1 Firewall proxy 193
5.1.2 Stateful inspection firewall 193
5.1.3 Firewall para gestión unificada de amenazas (UTM) 194
5.1.4 Firewall de última generación (NGFW) 194
5.1.5 Otras clasificaciones de firewall 194

5.2 FIREWALL EN ROUTERS 195

5.3 EL CORTAFUEGOS DE WINDOWS 196
5.3.1 Reglas de entrada y salida 201
5.3.2 Crear una regla personalizada Entrada o salida 201
5.3.3 Reglas de Puerto 204
5.3.4 Reglas personalizadas y personalizadas predefinidas 207
5.3.5 Propiedades del firewall 207
5.4 CORTAFUEGOS DOMÉSTICOS / SOFTWARE 209
5.4.1 ZoneAlarm Free Firewall 209
5.4.2 Sophos XG Firewall Home Edition 210
5.4.3 Comodo Firewall 210
5.4.4 AVS Firewall 211
5.5 CORTAFUEGOS EMPRESARIALES 212
5.5.1 Fortinet 212
5.5.2 Paloalto 213
5.5.3 Checkpoint 213
5.5.4 Sophos 213
5.5.5 Cisco 213
5.6 ESTABLECER FIREWALL MEDIANTE GPO EN WINDOWS SERVER 214

BIBLIOGRAFÍA Y WEBGRAFÍA 219

ACERCA DE LA AUTORA

Mi nombre es Silvia, aunque me llaman Zebra.

Llevo más de 22 años en el mundo de la informática, docencia y ciberseguridad, en realidad yo quería estudiar Ingeniería de Telecomunicaciones de Imagen y Sonido, que es algo que me apasiona, pero las causalidades de la vida me trajeron al mundo TI, me entró un virus en el ordenador de mi hermana al cual tenía el acceso absolutamente denegado, tuve que buscar la forma de arreglarlo antes de que llegara de su viaje de fin de curso, lo que de urgencia fue bastante caro, y días después alguien me ofreció un folleto paseando por Gran Vía de un curso de reparación de ordenadores y redes, y pensé esto no me vuelve a pasar, así comencé a arreglar ordenadores de amigos y poco después monte una empresa de informática.

Desde muy joven he sido muy inquieta, y me ha gustado aprender cosas nuevas, con 20 años monté junto a un amigo, Javier, una empresa de informática, CSR Soluciones Informáticas, lugar donde verdaderamente comprendí la importancia de lo que es aprender a la fuerza, trabajar duro, y que ser empresaria no siempre es un lujo. Sin muchos conocimientos, en aquel momento, solo un curso de Reparación de Ordenadores y Redes, pero con muchas ganas, juventud a raudales y ganas de ofrecer lo mejor a mis clientes comencé a estudiar Ingeniería Informática, y todo lo que podía y me permitía el tiempo.

El mundo de la informática, y más en la especialidad de Ciberseguridad, hace que estés en constante aprendizaje, así que me considero la eterna estudiante, ASIR, casi Ingeniera Informática, y casi Ingeniera de Telecomunicaciones, Master en Ciberseguridad y Hacking ético, certificaciones de varios fabricantes EC-

Council, COMPTIA, Microsoft, Cisco, Paloalto, Google IT, Fortinet, Ethical Hacker (CEH)…, y en definitiva en constante crecimiento mental y profesional.

Actualmente diversifico mi tiempo entre estudiar, impartir formación privada en Empresas (DHL, Registro de la Propiedad, COFRESCO, etc.) y en Certificados de profesionalidad del SEPE, como el de Seguridad informática entre otros relacionados con el mundo IT, colaborar en algunos proyectos de ciberseguridad, Ejército de Tierra en la especialidad de informática, mi canal de Youtube para apoyar y ayudar a mis alumnos y a quien lo necesite y mis nuevos proyectos HackingBytesZebra.com y la Producción musical. Como buena profesional IT duermo poco y necesito días más largos.

- LinkedIN: *https://www.linkedin.com/in/silviaclara/*
- Canal Youtube: *https://www.youtube.com/c/silviacma*
- Plataforma cursos de ciberseguridad: *https://www.HackingBytesZebra.com*

1

CRITERIOS GENERALES COMÚNMENTE ACEPTADOS SOBRE AUDITORÍA INFORMÁTICA

1.1 ¿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.

1.2 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.
   a. La actividad realizada por el auditor debe estar orientada a sacar el máximo beneficio para su cliente.
   b. No deben anteponerse aspectos o intereses personales.

c. No debe existir por parte del auditor ningún tipo de interés o beneficio por parte de marcas, productos o fabricantes.

d. El auditor debe de abstenerse de recomendar actuaciones innecesarias o que vayan a generar riesgos que estén injustificados.

2. Principio de calidad.

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

   b. 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.

   a. El auditor debe realizar formación continua, algo que es muy evidente en el cambiante mundo IT.

   b. El auditor debe de incidir en la toma de decisiones del cliente con cierta libertad.

   c. 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.

   d. El auditor tiene que evolucionar con el desarrollo de las TI, es decir, estar actualizado en sus conocimientos.

4. Principio de cautela.

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

   b. El auditor está al corriente de la evolución tecnológica y es capaz de informar al cliente.

   c. Debe actuar con humildad.

5. Principio de comportamiento personal.
   a. El auditor actuará conforme a las normas implícitas o explícitas dignas de la profesión.
   b. NO debe exponer juicios de valor personales.
   c. Debe estar seguro de sus conocimientos para el trabajo solicitado.
   d. Debe respetar la política empresarial del cliente auditado.
6. Principio de concentración en el trabajo.
   a. El auditor debe evitar el exceso de trabajo que influya en su capacidad de concentración y precisión en las tareas ejecutadas.
   b. Debe estimar las posibles consecuencias del trabajo acumulado.
   c. 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.
   a. El auditor fomenta la confianza siendo transparente en su forma de actuar.
   b. Las auditorías requieren confianza y diálogo entre ambas partes para solucionar posibles dudas.
   c. 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.
   a. Este principio está relacionado con el principio de independencia, el auditor debe actuar con criterio propio y no dejarse llevar por otros.
   b. 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.
   a. El auditor debe evitar generar gastos innecesarios al cliente auditado.

b. Debe delimitar adecuada y concretamente el alcance, objetivos y límites de la auditoría.

c. Debe rechazar ampliaciones del trabajo que no estén directamente relacionadas con la auditoría.

10. Respeto por la profesión.

a. El auditor debe reconocer y dar valor a su trabajo.

b. LA remuneración por la auditoría debe estar de acuerdo a los conocimientos, preparación y experiencia del auditor.

c. Evitar la competencia desleal poniendo precios más baratos que los del mercado.

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

11. Principio de integridad moral.

a. El auditor debe ser leal, honesto y diligente en su desempeño, dedicado y preciso.

b. Evitar participar de forma consciente o inconsciente en actos de corrupción.

c. No puede aprovechar los conocimientos adquiridos de la auditoría de la empresa para usarlos en su contra.

12. Principio de legalidad.

a. El auditor debe evitar el uso de sus conocimientos en pro de la desobediencia de la legalidad en vigor.

b. 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.

c. El auditor debe de abstenerse de intervenir líneas de comunicación que impliquen la vulneración de la privacidad.

13. Principio de precisión.

a. 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.

b. Debe ser crítico.

   c. 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.
    a. El auditor se responsabiliza de todo lo que haga, diga o aconseje.
    b. 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.
    a. La confidencialidad respecto al proceso de auditoría es una característica esencial en la relación entre cliente-auditor.
    b. El auditor en su debe 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.
    c. Es responsabilidad del auditor tomar las medidas de seguridad necesarias para garantizar que la información documentada está a salvo.

16. Principio de veracidad.
    a. 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 deshonrar 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.

1.3 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:

   a. **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.

   b. **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.

1.4 CRITERIOS A SEGUIR PARA LA COMPOSICIÓN DEL EQUIPO AUDITOR

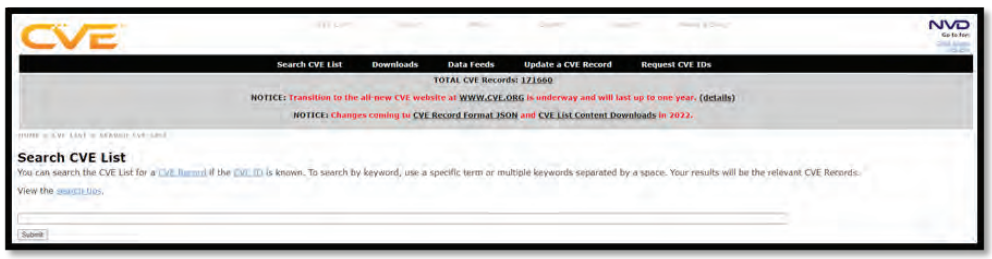
Dado que las auditorías pueden versar de algo muy concreto como puede ser auditar un servidor o auditar toda la infraestructura de la empresa, hay que tener en cuenta que uno no puede tener todos los conocimientos de absolutamente todo, por lo que normalmente las auditorías se realizan por un equipo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

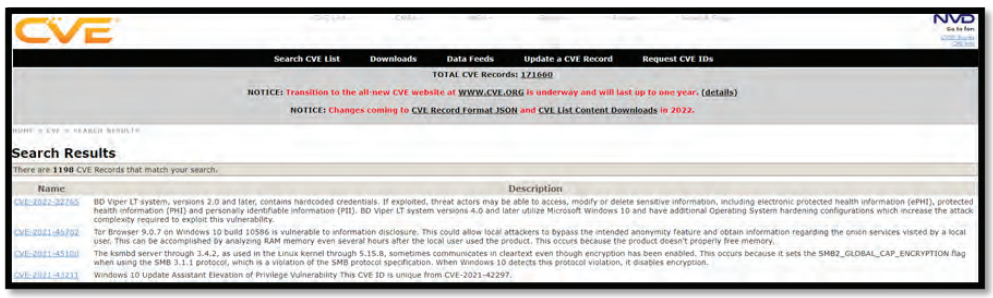
1.5 EL INFORME DE AUDITORÍA

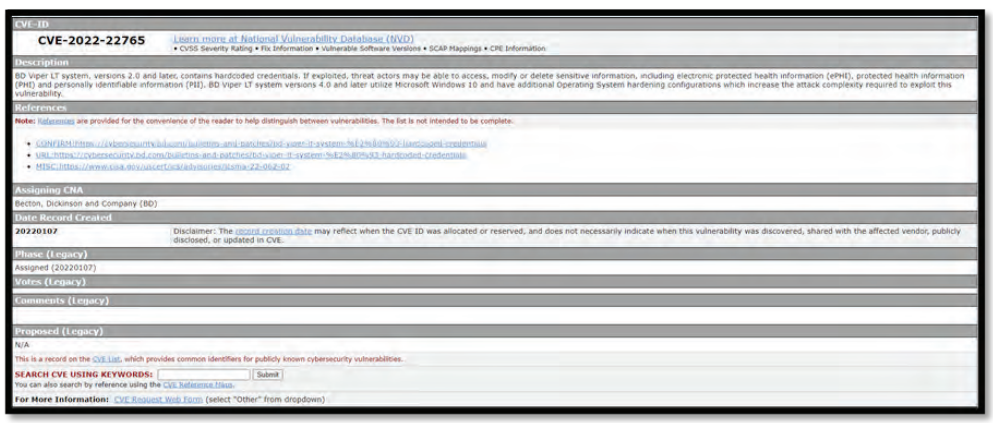
Los resultados de la auditoría se deben documentar, se realizarán 2 informes, uno técnico y otro ejecutivo que puedan entender las personas que no tengan conocimientos técnicos informáticos. En este informe debemos:

- **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.







Enlace a cve mitre: *https://cve.mitre.org/cve/search_cve_list.html*

- 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.

1.6 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).

1.6.1 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 a 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.