**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

| PROGRAMA DE FORMACIÓN | Hacking ético en sistemas y redes |
| --- | --- |

| COMPETENCIA | 220501111. Controlar sistema de seguridad de la información de acuerdo con los procedimientos y normativa técnica. | RESULTADOS DE APRENDIZAJE | 220501111-01. Comprender los componentes teóricos del Hacking, la seguridad informática y la ciberseguridad para su aplicación en entornos determinados. |
| --- | --- | --- | --- |

| NÚMERO DEL COMPONENTE FORMATIVO | CF001 |
| --- | --- |
| NOMBRE DEL COMPONENTE FORMATIVO | Fundamentos de *hacking* ético y seguridad informática |
| BREVE DESCRIPCIÓN | Las malas prácticas, configuraciones incorrectas y el uso inadecuado de las tecnologías son procesos que se ejecutan día a día enmarcados por los ataques informáticos. Comprender el ecosistema de los ciberdelincuentes contribuye a mitigar los ataques de gran y pequeña escala, logrando minimizar la afectación a las organizaciones, esto conlleva a conocer aspectos fundamentales sobre el *hacking* ético y la seguridad informática. |
| PALABRAS CLAVE | Ataque, ciberseguridad, *hacker*, *hacking*, vulnerabilidad. |

| ÁREA OCUPACIONAL | 2 - Ciencias Naturales, aplicadas y relacionadas |
| --- | --- |
| IDIOMA | Español |

1. **Tabla de contenidos**

**Introducción**

* 1. **Fundamentos de *hacking***
  2. Conceptos y generalidades (triada de la seguridad)
  3. Fases de *hacking*
  4. *Hacking* ético
  5. Investigación de vulnerabilidades
  6. Tipos de ataques
  7. **Leyes y normas de la seguridad de información**
  8. Aspectos legales de *hacking* ético
  9. Normatividad legal vigente
  10. **Metodologías del *hacking* ético**

3.1 Estándares y metodologías

3.2 Buenas prácticas

**Introducción**

El *software* y el *hardware* son indicadores del crecimiento T.I en el mundo y con este crecimiento la ciberdelincuencia también lo hace exponencialmente siguiendo sus pasos. Las malas prácticas, configuraciones incorrectas y uso inadecuado de las tecnologías son procesos que se ejecutan día a día enmarcados por los ataques informáticos. Comprender el ecosistema de los ciberdelincuentes contribuye a mitigar los ataques de gran y pequeña escala, logrando minimizar la afectación de las organizaciones. A continuación, puede revisar la introducción de este componente.

****

1. **Desarrollo de contenidos**

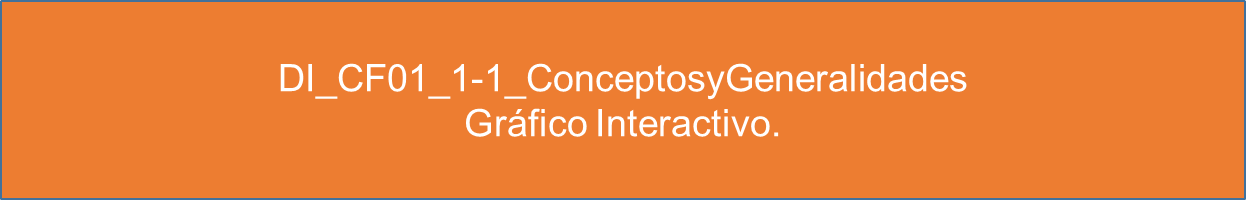
**1. Fundamentos de *hacking***

Los sistemas de gestión, planes de continuidad del negocio son de vital importancia; sin embargo, los aspectos técnicos son la base sostenible de la ciberseguridad y de la seguridad informática. Los ataques informáticos lamentablemente pueden ser llevados a cabo por personas sin gran experiencia, quienes por medio de herramientas básicas pueden conseguir objetivos de fácil acceso. Es importante resaltar que tener conocimiento del *modus operandi* de la ciberdelincuencia, articulado a conocimientos técnicos marcan la diferencia en cargos relacionados con la ciberseguridad y la seguridad informática, ya que de esta manera se puede evidenciar un ataque difícil de ser detectado.

Por lo anterior, la inversión en capacitación de personal es indiscutiblemente el pilar fundamental de toda implementación de seguridad, teniendo en cuenta que adquirir sistemas de seguridad con altas capacidades y características lleva a las organizaciones a entrar en un estado de falsa seguridad, dando un segundo lugar a las capacidades humanas.

* 1. **Conceptos y generalidades** (triada de la seguridad)

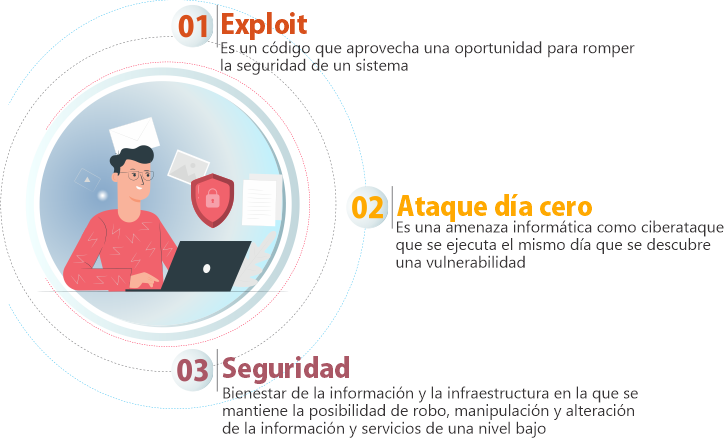
Cuando se escucha la palabra *“hacker”* en el mundo digital se ha asociado a prácticas indebidas por ciberdelincuentes, lo cual no es del todo cierto, ya que muchos de ellos se dedican a buenas prácticas en pro de salvaguardar la información de una persona, individuo u organización, poniendo a prueba todos sus organismos de control de seguridad, con el fin de determinar debilidades, amenazas y riesgos a los cuales pueden estar expuestos los sistemas de información, a esto comúnmente se le conoce como ***hacking* ético** y, para conocerlo y apropiarlo debe conocer la terminología necesaria para que se determine la respectiva importancia de este tema, por ello, revise los conceptos más importantes.



En la siguiente figura se presentan algunos de los conceptos importantes en el ***hacking* ético.**

**Figura 1**

*Conceptos importantes en el hacking ético*



Antes de entrar a hablar sobre los métodos efectivos de realizar un buen *hacking* ético debe de conocer y apropiar tres conceptos básicos de la seguridad de la información, que conforman el llamado **triángulo o triada de la seguridad de la información**, la cual se integra por la **confidencialidad, integridad y disponibilidad**, comúnmente conocida como la tríada CID (seguridad de la información), esta da el modelo base por el cual se incluye la terminología usada en seguridad, centrada en los datos y en la información, ver figura 2.

**Figura 2**

*Triada de la seguridad de la información*



* **Confidencialidad:** se puede equiparar con la privacidad que tiene un usuario o empresa, radica en todas las medidas que se toman para que los datos solo lleguen a personas autorizadas y no caigan en manos de terceros o ciberdelincuentes, igualmente, se diseña de cierta manera para que la información esté cifrada y solo pueden acceder a ella personal autorizado bajo claves o contraseñas; el poder salvaguardar la información tiene la visión ética de cada una de las personas que tienen acceso, y de ser conscientes de los riesgos, amenazas y vulnerabilidades a las cuales están expuestos.

La confidencialidad se refiere a los esfuerzos de una organización por mantener sus datos en privado o en secreto, en la práctica, se trata de controlar el acceso a los datos para impedir su divulgación no autorizada, por lo general, se trata de asegurar que solo las personas autorizadas tengan acceso a determinados bienes y que se impida activamente el acceso de las personas no autorizadas.



La confidencialidad puede violarse de muchas maneras, como ataques directos destinados a obtener acceso no autorizado a sistemas, aplicaciones y bases de datos, con el fin de robar o manipular datos, el reconocimiento de redes y otros tipos de escaneos, las escuchas electrónicas (mediante un ataque de hombre en medio) y la escalada de los privilegios del sistema por parte de un atacante son solo algunos ejemplos, pero la confidencialidad también puede ser violada sin querer, por error humano, descuido o controles de seguridad inadecuados, entre los ejemplos cabe citar la incapacidad (por parte de los usuarios o de la seguridad de la tecnología de la información) de proteger adecuadamente las contraseñas; el uso compartido de cuentas de usuario; la escucha física (también conocida como “*shoulder surfing*"); la no codificación de los datos (en proceso, en tránsito y cuando están almacenados); los sistemas de autenticación deficientes, débiles o inexistentes; y el robo de equipo físico y dispositivos de almacenamiento.

* **Integridad:** está inmersa en poder dar a los datos características como precisión, confiabilidad y consistencia, estos a su vez no deben ser alterados en su paso y se toman medidas de seguridad que garanticen que no se deben modificar, se realiza a través de permisos y controles de cada uno de los usuarios autorizados al acceso.

En el uso diario, la integridad se refiere a la calidad de algo que está entero o completo, se refiere a asegurar que los datos no han sido manipulados y, por lo tanto, se puede confiar en ellos, es correcto, auténtico y fiable, como ocurre con la confidencialidad, la integridad puede verse comprometida directamente a través de un vector de ataque (como la manipulación de los sistemas de detección de intrusos, la modificación de los archivos de configuración o el cambio de los registros del sistema para eludir la detección) o involuntariamente, por error humano, falta de cuidado, errores de codificación o políticas, procedimientos y mecanismos de protección inadecuados.

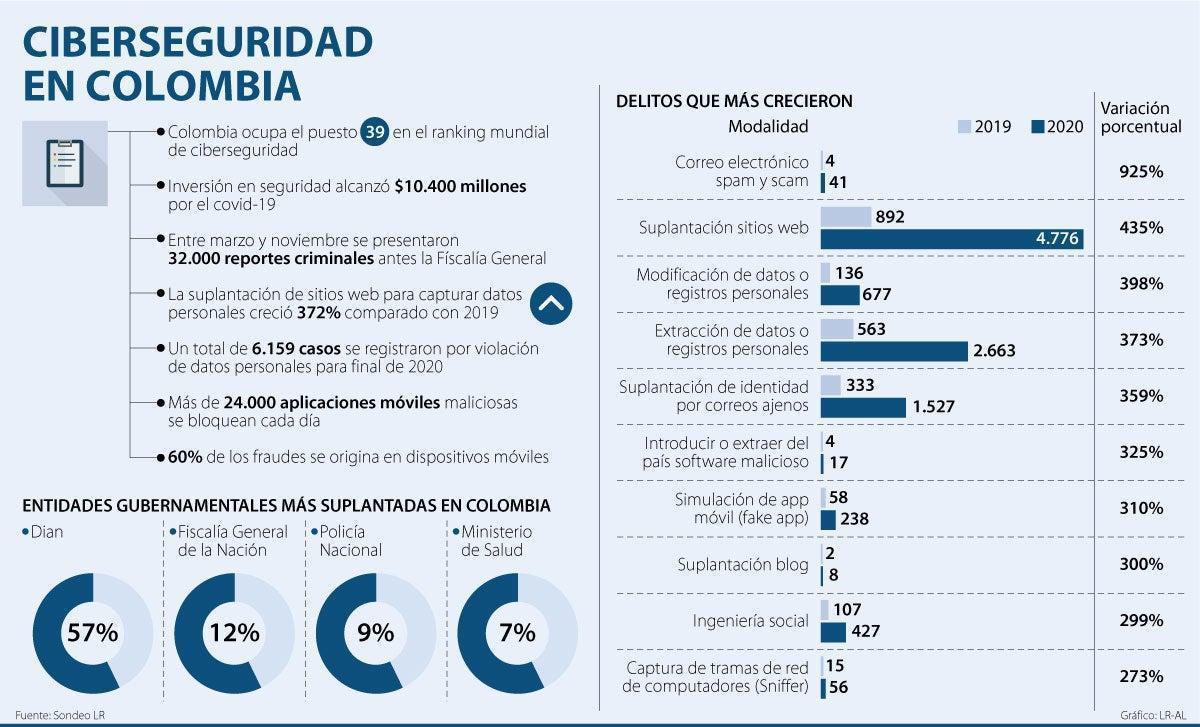
* **Disponibilidad**: radica en que la infraestructura de la información debe estar controlada rigurosamente, manteniendo el *hardware* en debido funcionamiento sin errores, para que de esta manera siempre que se necesite el acceso a la información esté disponible, evitando cuellos de botella y otros factores que pongan en riesgo la información.

Es por ello que los sistemas, las aplicaciones y los datos tienen poco valor para una organización y sus clientes si no son accesibles cuando los usuarios autorizados los necesitan, es por ello que la disponibilidad significa que las redes, los sistemas y las aplicaciones están en funcionamiento, garantizando que los usuarios autorizados tengan acceso oportuno y fiable a los recursos cuando los necesiten.

Muchas cosas pueden poner en peligro la disponibilidad, entre ellas las fallas de *hardware* o *software*, los cortes de energía, los desastres naturales y los errores humanos, tal vez el ataque más conocido que amenaza la disponibilidad sea el de negación del servicio, en el que el rendimiento de un sistema, un sitio web, una aplicación o un servicio basado en la web se degrada de forma intencionada y maliciosa, o el sistema se vuelve completamente inalcanzable. En la siguiente figura se pueden observar las estadísticas de la ciberseguridad en Colombia.

**Figura 3**

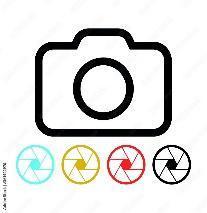
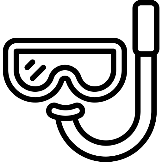
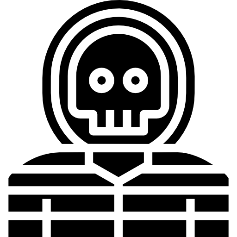
*Estadísticas de la ciberseguridad en Colombia*



* 1. **Fases de *hacking***

La seguridad de la información es una creciente preocupación para las personas y las empresas, la protección de sus datos se ha convertido en una premisa, ya que los ataques por parte de ciberdelincuentes cada vez son más comunes; sin embargo, los riesgos y constantes amenazas dejan al desnudo los sistemas de información y los peligros que en la era digital se están afrontando en el mundo de hoy, es por ello que se ha hecho fundamental que tenga conocimientos informáticos y de seguridad para poder aplicarlos en los sistemas y redes, para poder solventar fallos a tiempo, documentarlos y atacarlos de forma efectiva.

Para ello, se usan pruebas de penetración o conocidas comúnmente como *pentesting*, las cuales se usan para poder detectar riesgos en sus sistemas de información o redes, su uso pretende encontrar fallas en la seguridad de la información, saltándose las medidas de seguridad adoptadas por un individuo, empresa u organización, existen principalmente 5 fases del *hacking*, un *hacker* no necesariamente tiene seguirlas de forma secuencial; pero cuando se lleva de forma secuencial se obtienen mejores resultados.



En esta fase de reconocimiento la huella proporciona información importante como:

* + - El nombre de dominio.
    - Los servicios TCP y UDP.
    - Los nombres de los sistemas y las contraseñas.

Igualmente, hay otras formas de realizar la huella, como la suplantación de la identidad de un sitio web mediante su duplicación, el uso de motores de búsqueda para encontrar información sobre la organización e incluso el uso de la información de los empleados actuales para la suplantación.

En la siguiente tabla se presenta un comparativo entre la recolección activa y la recolección pasiva.

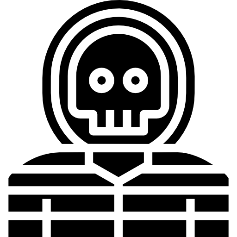
**Tabla 1**

*Tipos de reconocimiento*

| Recolección activa | Recolección pasiva |
| --- | --- |
| Es de gran efectividad, pero no es la mejor aliada si de anonimato se quiere hablar, porque puede llamar mucho la atención del objetivo:   * Campañas de ingeniería social (llamadas falsas). * *Metasploitable*. * Ataques al objetivo u escaneos invasivos. | Es cuando se tiene un contacto directo con el objetivo, es decir, cuando existe el apoyo de fuentes públicas para obtener información, lo cual ayuda a mantener el anonimato y es menos “ruidosa” que la activa; estas fuentes pueden ser:   * Sitios web relacionados con el objetivo. * Motores de búsqueda. * Redes sociales. * Blogs. |



















En la siguiente tabla puede observar algunas características de cada método.

**Tabla 2**

*Métodos de escaneo*

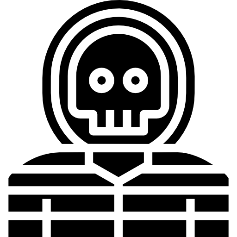
| Fase de pre-ataque | Rastreo de puertos | Extraer información |
| --- | --- | --- |
| Escaneo se refiere a la fase de pre-ataque cuando el atacante busca en la red para obtener información específica sobre la base de la información recopilada durante el reconocimiento. | La exploración puede incluir el uso de marcadores, analizadores de puertos, la cartografía de la red, barrido, escáneres de vulnerabilidades, entre otros. | Los atacantes extraen información como los nombres de equipos, direcciones IP y cuentas de usuario para lanzar ataques posteriores. |



















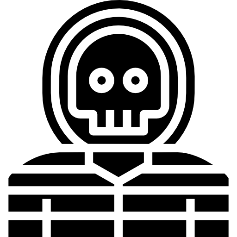
























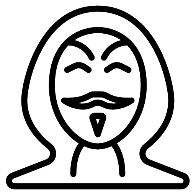




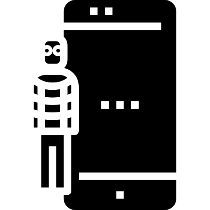






























* 1. ***Hacking* ético**

Es muy frecuente que las personas, empresas u organizaciones instalen sistemas de seguridad para mantener sus propiedades y activos a salvo, que compren un seguro en caso de desastre o hurto; sin embargo, cuando se encuentra que ese activo **es la información** es muy poco común encontrarse que las empresas inviertan en el sistema de seguridad informática; que es igual o hasta muchas veces más importante que los mismos activos, es por ello que hoy por hoy, es la que los propietarios de las empresas pueden implementar con programas y procedimientos para proteger los computadores de la empresa de los piratas informáticos y de los virus, el pirateo en general cuesta a las empresas miles de millones de dólares cada año, pero hay más que dinero en juego si su empresa se encontrará con un *hacker* informático.

Es probable que las empresas tengan información como tarjetas de crédito y cuentas confidenciales, por no mencionar la información financiera personal de sus clientes archivada en una base de datos informática, además de esto, también es probable que haya otra información personal de los empleados como números de seguridad social, direcciones de casa e información de atención médica en el archivo y todo tipo de información, un pirata informático puede acceder a esta información sensible, lo que a su vez podría conducir al robo de identidad y múltiples ataques ciberdelincuenciales que ponen en riesgo inminente a una persona o empresa, esto no solo puede ser perjudicial para sus empleados y clientes actuales, sino también para la reputación de su empresa.

* **Problemas de ciberseguridad**

Pueden variar desde cosas tan granulares como *software* desactualizado hasta luchas a gran escala como la falta de apoyo de los equipos de liderazgo; las medidas que deben adoptar con relación a la seguridad a aplicar dentro de una organización dependerán del tipo de sistemas a proteger o salvaguardar, de la información que produzcan, de las condiciones intrínsecas de cada empresa y de los riesgos y amenazas a las que se exponen. A continuación, en la tabla 3, podrá observar los problemas más comunes que cualquier empresa debería tener en cuenta independientemente de su actividad.

**Tabla 3**

*Problemas de ciberseguridad*

| La evolución de la tecnología se centró en la facilidad de uso |  | La creciente complejidad de la administración y gestión de infraestructura informática |
| --- | --- | --- |
| Cumplimiento con las leyes y regulaciones del gobierno | El impacto directo de la violación de la seguridad en la base de activos de las empresas y la buena voluntad |
| Aumento del número de aplicaciones basadas en la red | Es difícil para centralizar la seguridad en un entorno de computación distribuido |

* **Desafíos de la ciberseguridad**

Dentro del *hacking* ético se deben tener en cuenta algunos aspectos de la ciberseguridad, tales como son los retos de la seguridad y los riesgos asociados a la misma, y de esta manera poder actuar con programas pertinentes a la hora de realizar actuaciones frente a un ataque o vulneración de un sistema o red. Revise a continuación los retos y riesgos de seguridad más comunes.

**Retos de la seguridad**

* Aumento de la sofisticación en los cibercriminales.
* La fuga de datos, los *insiders* maliciosos y los trabajadores remotos.
* La seguridad móvil, la adaptación de autenticación, estrategias de medios sociales.
* Vulnerabilidades explotadas, seguridad operacional.
* Fuerza de trabajo de seguridad cibernética. Estrategias de acceso, identidad y de ciclo de vida.
* Vulnerabilidades explotadas, seguridad operacional.
* Equilibrio de intercambio con los requisitos de privacidad.

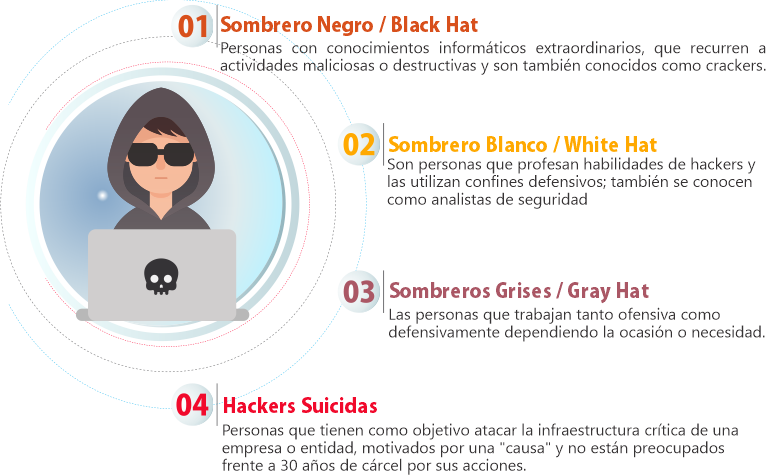
**Riesgos de la seguridad**

* Robo /venta de identidades mercado negro.
* *Botnets* (red de computadoras infectadas por *malware* que están bajo el control de una sola parte atacante, conocida como "*bot-herder*") Fast Flux.
* Datos transportables (USB, ordenadores portátiles, cintas de seguridad).
* Redes zombies (ordenador conectado a Internet que ha sido comprometido por un pirata informático, un virus informático o un troyano y que puede ser utilizado para realizar tareas maliciosas de un tipo u otro bajo dirección remota).
* *Exploits* en nuevas tecnologías.
* Las redes sociales.
* Ciberespionaje, *exploits* de día cero.
* Troyanos / robo de información / *keyloggers.*
* Pérdida / brechas de datos.
* Las amenazas internas.
* Delito cibernético organizado.
* Ingeniería *phishing (vishing)/* social.
* Virtualización y *cloud computing.*

Aunado a lo anterior, se puede dar cuenta que los riesgos asociados a la seguridad informática a la cual se expone como individuo, como empresa o como organización, son múltiples y es allí que se deben generar contingencias especializadas para poder salvaguardar la información sensible, a lo cual las organizaciones mundiales de seguridad informática desarrollaron el “***hacking* ético**”. Como aprendiz SENA debe estar a la vanguardia de este tipo de actividades y es pertinente que genere habilidades que permitan apoyar los sistemas y redes de información, ya sea de tipo personal o empresarial dentro del mundo digital al cual se enfrenta con las nuevas tecnologías emergentes.

**Tipos de *hackers***

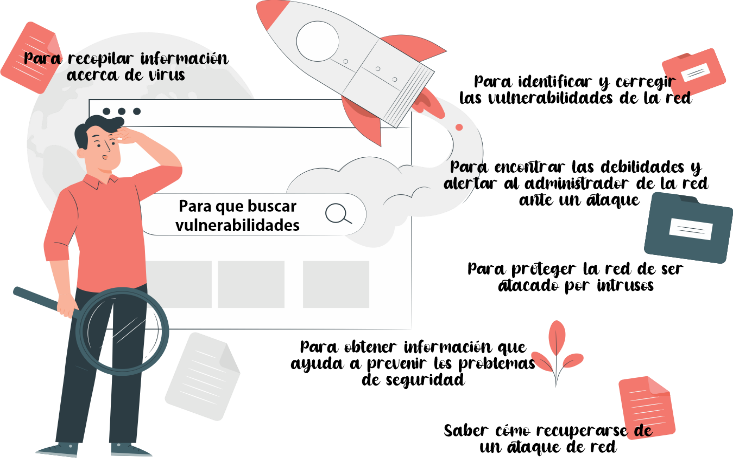
Para describir los tipos de *hackers* existentes se debe definir de forma sencilla qué son:



En el siguiente recurso podrá revisar las características de los diferentes tipos de *hackers*.





* El *hacking* ético es necesario, como piratería implica el pensamiento creativo, las pruebas de vulnerabilidad y auditorías de seguridad que no pueden garantizar que sean seguras.
* Como estrategia de la defensa en profundidad, para ello, las organizaciones deben implementar este tipo de estrategia para penetrar en sus redes y así poder estimar las vulnerabilidades y exponerse.
* Para contrarrestar los ataques es necesario, ya que permite la lucha contra los ataques de los *hackers* mediante la prevención de intrusos en el sistema.
  1. **Investigación de vulnerabilidades**

Es el proceso de descubrimiento de vulnerabilidades y fallos de diseño que abrirá un sistema operativo y sus aplicaciones a los ataques o al mal uso, las vulnerabilidades se clasifican según el nivel de gravedad (bajo, medio o alto) y el rango que explotan (local o remota). A continuación, se presentan los casos de vulnerabilidades más comunes.

* + - * 1. **El equipo del administrador está infectado por un virus**

El *hacker* puede haber instalado *software* espía en el equipo del administrador infectado por el virus para registrar sus combinaciones de teclas.

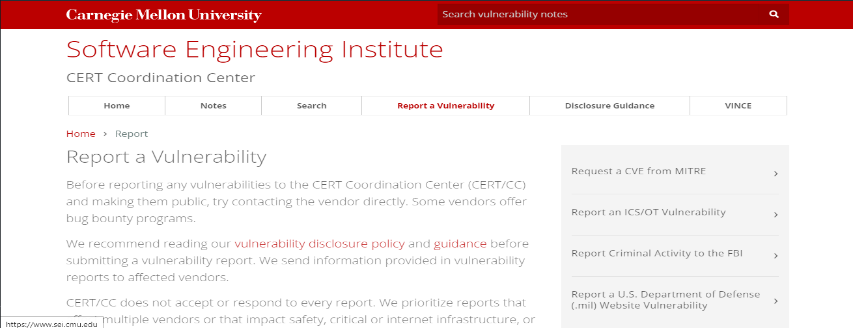
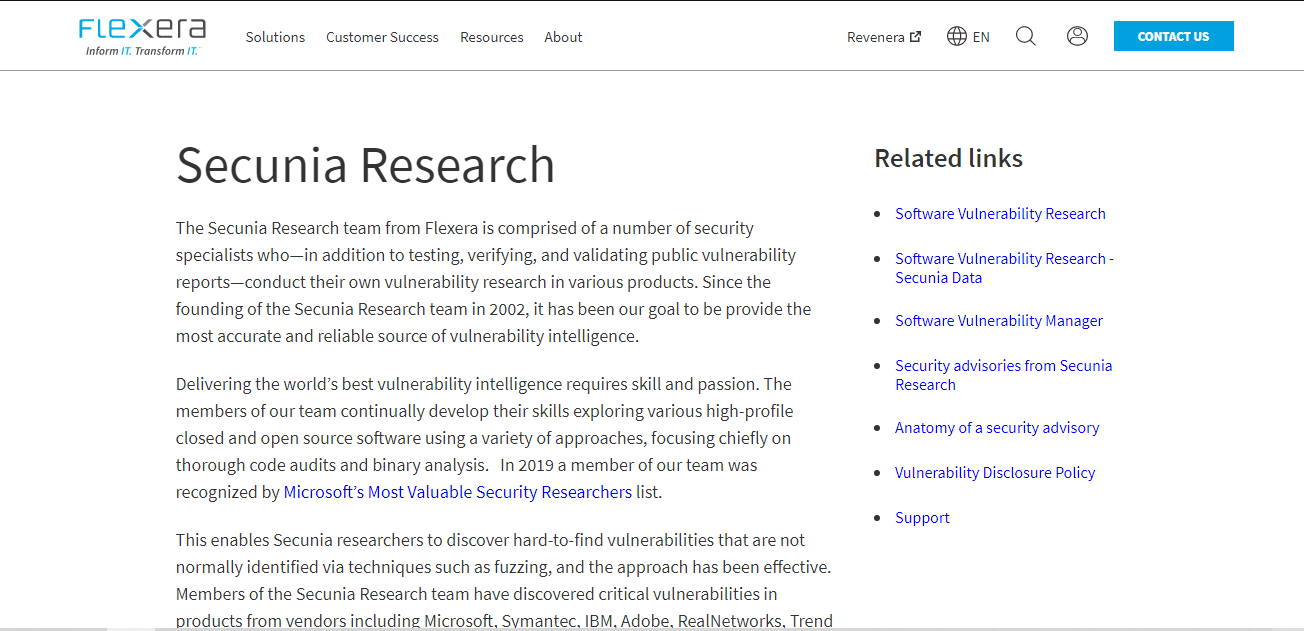
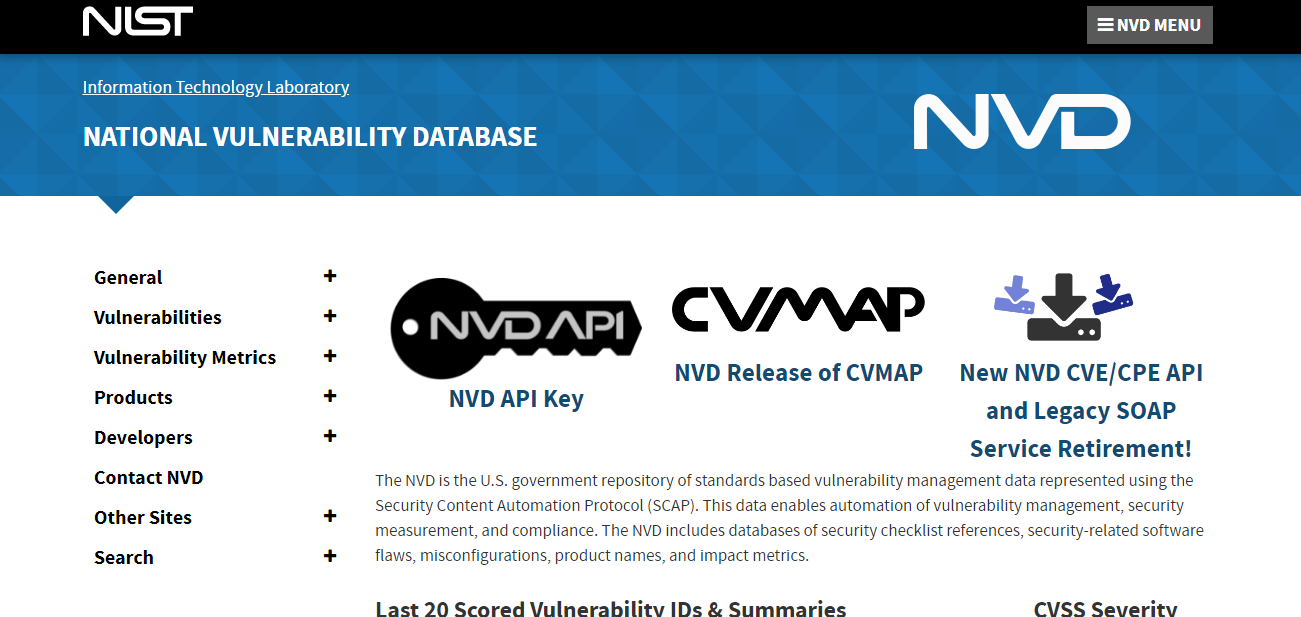
* Compruebe si hay virus en los sistemas del administrador, se recomienda que ejecute varios escáneres con antivirus de prestigio en todos los equipos que el administrador use para iniciar sesión en el sitio web, esta acción no es un método infalible de detección de virus, ya que constantemente se diseñan nuevas infecciones de *software* malicioso para evadir los análisis, es posible que los análisis antivirus informen sobre falsos positivos, por esta razón, la ejecución de varios análisis puede proporcionar distintos datos para determinar si existe una vulnerabilidad.
* Si el análisis antivirus detecta *spyware*, virus, troyanos o cualquier otro programa sospechoso, investigue los registros del servidor para comprobar la actividad del administrador propietario del equipo infectado.
* Es posible que el *hacker* haya alterado los archivos de registro, si no es así, la correlación del nombre de usuario del administrador con comandos sospechosos en el archivo de registro es una prueba más de que la causa de la vulnerabilidad ha sido un virus en el sistema del administrador.
  + - * 1. **Contraseñas débiles o reutilizadas**

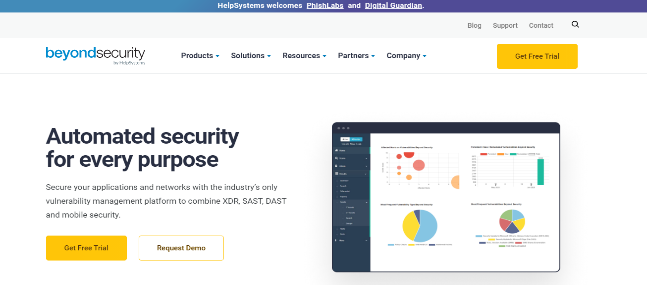
A los *hackers* les puede resultar relativamente fácil descifrar una contraseña débil, y esto le proporciona acceso directo a tu servidor, todas las contraseñas seguras están formadas por una combinación de letras, números y signos de puntuación, y no incluyen palabras, ni jerga que se puedan encontrar en un diccionario.

* Las contraseñas se deben utilizar para una única aplicación, no se deben reutilizar para todos los servicios, Si se reutilizan las contraseñas, con una sola infracción de la seguridad en una aplicación el *hacker* consigue el nombre de usuario y la contraseña, y puede intentar reutilizarlos en otros lugares.
* En el registro del servidor comprueba si hay actividad no deseada, por ejemplo, que un administrador haya hecho varios intentos para iniciar sesión o haya utilizado comandos inesperados. Anote cuándo ocurrió la actividad sospechosa. Es importante saber cuándo se pirateó el sitio web por primera vez para poder determinar qué copias de seguridad pueden estar limpias.
  + - * 1. ***Software* desactualizado**

Comprueba que los servidores tengan instalada la última versión del sistema operativo, del sistema de gestión de contenido, de la plataforma de *blogs,* de las aplicaciones, de los complementos, entre otros.

Existen sitios web de investigación de vulnerabilidades, como:

* El **Software Engineering Institute (SEI)**, que es un instituto federal estadounidense de investigación y desarrollo, fundado por el Congreso de los Estados Unidos en 1984 para desarrollar modelos de evaluación y mejora en el desarrollo de *software*, que dieran respuesta a los problemas que generaba al ejército estadounidense la programación e integración de los sub-sistemas de *software* en la construcción de complejos sistemas militares. Financiado por el Departamento de Defensa de los Estados Unidos y administrado por la Universidad Carnegie Mellon. Es un referente en Ingeniería de *software* por realizar el desarrollo del modelo SW-CMM (1991) que ha sido el punto de arranque de todos los que han ido formando parte del modelo que ha desarrollado sobre el concepto de capacidad y madurez, hasta el actual CMMI.
* Por otro lado, el equipo de investigación de **Secunia de Flexera** está compuesto por varios especialistas en seguridad que, además de probar, verificar y validar los informes públicos de vulnerabilidad, realizan su propia investigación de vulnerabilidad en varios productos, desde la fundación del equipo de investigación de Secunia en 2002, el objetivo ha sido proporcionar la fuente más precisa y fiable de inteligencia sobre vulnerabilidades.
* La Base de Datos Nacional de Vulnerabilidad (NVD) es el repositorio del gobierno de los EE.UU. de datos de gestión de vulnerabilidades basados en estándares representados mediante el Protocolo de Automatización de Contenidos de Seguridad (SCAP), estos datos permiten la automatización de la gestión de la vulnerabilidad, la medición de la seguridad y el cumplimiento; el NVD incluye bases de datos de referencias de listas de control de seguridad, fallas de *software* relacionadas con la seguridad, configuraciones erróneas, nombres de productos y métricas de impacto.



* SecuriTeam es un pequeño grupo dentro de Beyond Security dedicado a traer las últimas noticias y utilidades en seguridad informática.



Existen múltiples herramientas en Internet que permitirán reconocer las vulnerabilidades que puede tener su sistema o red, e igualmente, están a la disposición para poder mitigarlas, en la siguiente tabla se deja una cantidad de direcciones que pueden ser de mucha ayuda.

**Tabla 4**

*Herramientas para conocimiento de vulnerabilidades*

| Nombre | Sitio web / URL |
| --- | --- |
| Security Magazine | <http://securitymagazine.com> |
| Pentest Tools | <https://pentest-tools.com/website-vulnerability-scanning/website-scanner> |
| HackerWatch | <http://www.hackerwatch.org> |
| CodeRed Center | <http://eccouncil.org> |
| TechNet | <http://blogs.technet.com> |
| Common Vulnerabilities and Exposures | <https://cve.mitre.org/> |
| Hackerstorm Vulnerability Database Tool | <http://www.hackerstorm.com> |
| CNET Blogs | <http://www.new.cnet.com> |

Dentro de la investigación de vulnerabilidades se realizan las **pruebas de penetración** **(o *pentesting)*,** comoun ejercicio de seguridad en el que un experto en seguridad cibernética intenta encontrar y explotar las vulnerabilidades de un sistema informático, el propósito de este ataque simulado es identificar cualquier punto débil en las defensas de un sistema que los atacantes podrían aprovechar (Gaviria, 2015).





Lo mejor es que el *pentest* lo realice alguien con poco o ningún conocimiento previo de cómo se asegura el sistema, ya que puede ser capaz de exponer los puntos ciegos que no han sido detectados por los desarrolladores que construyeron el sistema, por esta razón, se suele traer a contratistas externos para que realicen las pruebas, a estos contratistas se les suele denominar "*hackers* éticos", ya que se les contrata para piratear un sistema con permiso y con el fin de aumentar la seguridad.

Muchos *hackers* éticos son desarrolladores experimentados con títulos avanzados y una certificación para pruebas de pluma, por otro lado, algunos de los mejores *hackers* éticos son autodidactas, pero el SENA por medio de estos programas de formación logra formar bases teórico – prácticas sobre estas prácticas, incluso, algunos son *hackers* criminales reformados, que ahora utilizan su experiencia para ayudar a arreglar los fallos de seguridad en lugar de explotarlos. Son los mejores candidatos para llevar a cabo una *pentest* que puede variar enormemente, dependiendo de la empresa objetivo y del tipo de *pentest* que quieran iniciar.



**En qué consiste una prueba de penetración**

* Las pruebas de intrusión son un método de evaluación de forma activa. Se mide la seguridad de un sistema de información o red mediante la simulación de un ataque de tipo malicioso.
* Las medidas de seguridad son analizadas activamente por deficiencias de diseño, fallas técnicas, y vulnerabilidades.
* Las pruebas de caja negra, (Black Box) simulan un ataque de alguien que no esté familiarizado con el sistema, y las pruebas de caja blanca (White Box) simulan un atacante que tiene pleno conocimiento sobre el sistema que ataca.
* Los resultados se entregan ampliamente en informes ejecutivos, de gestión y técnicos.

En la siguiente tabla se presenta un comparativo entre las pruebas de penetración y el *hacking* ético.

**Tabla 5**

*Comparativo pruebas de penetración – hacking ético*

| Pruebas de penetración | *Hacking* ético |
| --- | --- |
| * El objetivo principal es encontrar vulnerabilidades dentro del entorno objetivo. * Las pruebas de penetración se centran en la seguridad del área específica definida para las pruebas. * Se espera que el *pentester* sea consciente de ejecutar diferentes metodologías y conocer el propósito de cada metodología, cómo y cuándo ejecutar. * Se requiere experiencia previa en *hacking* ético para ser un buen *pentester*. * Un *pentester* puede funcionar en un dominio y red específicos, el conocimiento esperado es más específico a nivel experto. | * Su objetivo es abarcar varios ataques a través de diferentes técnicas de *hacking* para encontrar fallas de seguridad. * El *hacking* ético es un término integral y las pruebas de penetración son una de las funciones del *hacker* ético. * El *hacker* ético debe tener un conocimiento integral de las metodologías de *hacking.* * El *hacking* ético es un paso hacia las pruebas de penetración, a menos que uno conozca las metodologías, no pueden realizar un *pentest*. * Al ser un *hacker* ético debe tener en cuenta los aspectos técnicos del *software* y el *hardware* de los dispositivos digitales conectados a la red. |

El *ethical* *hacking* compromete los sistemas informáticos para evaluar la seguridad y actuar de buena fe informando a la parte vulnerable, el *hacking* ético es una habilidad clave para muchos puestos de trabajo relacionados con la seguridad de los activos en línea de una organización. Los profesionales que trabajan en estas funciones laborales mantienen las computadoras, los servidores y otros componentes de la infraestructura de la organización en condiciones de trabajo que impiden el acceso no autorizado a través de canales no físicos.

La gente cree que "*hacking"* significa *hackear* cualquier sitio web en un minuto, este concepto proviene de ver películas, por lo que ni siquiera conocen el concepto básico original de lo que significa *hackear* o cómo hacerlo. ¿Descifrar contraseñas o robar datos? No, el "*ethical* *hacking*" es mucho más que eso; el *hacking* *ético* es escanear las vulnerabilidades y encontrar amenazas potenciales en una computadora o red, un hacker ético encuentra los puntos débiles o lagunas en un computador, aplicaciones web o red y los reporta a la organización.

* 1. **Tipos de ataques**

Hay varias maneras en que un atacante puede obtener acceso a un sistema, estos deben ser capaz de explotar una debilidad o vulnerabilidad en un sistema, entre los tipos de ataque más populares se encuentran:

* **Ataques al sistema operativo:** el sistema operativo ejecuta muchos servicios como interfaces gráficas de usuario (GUI) que soportan aplicaciones y herramientas del sistema, y permiten el acceso a Internet, en los ataques a sistemas operativos, "los atacantes buscan vulnerabilidades en el sistema operativo de tal manera que puedan explotarlas a través de las vulnerabilidades y obtener acceso al sistema o red objetivo".

Las vulnerabilidades en el sistema operativo pueden ser puertos y servicios abiertos, ya que la mayoría de los sistemas operativos instalan estos servicios y puertos por defecto, estas son las vulnerabilidades más comunes encontradas por los atacantes para obtener acceso a un sistema operativo; por lo tanto, para prevenir los ataques al sistema operativo se necesita eliminar o deshabilitar aquellos servicios y puertos que son innecesarios por el momento.

* **Ataques a nivel de aplicación**: a veces un entorno seguro de una organización construida por varios interesados (administradores de sistemas, administradores de bases de datos o desarrolladores) queda con lagunas vulnerables, incluso después de haber pensado que el trabajo está completo, ya que no todos los interesados están al tanto o son responsables de asegurar la aplicación web y/o la infraestructura. Estas lagunas de seguridad llevan, entonces, a la organización a graves riesgos más adelante, incluyendo costosas multas y daños a la reputación. Incluso dejando sus aplicaciones a la merced de los ciberdelincuentes, esto se ve que en el *software* se encuentra:
* Sistemas sin parches.
* Archivos no encriptados.
* Aplicaciones web antiguas y desactualizadas.
* La aplicación web y la mala configuración de la nube
* Insuficiente protección de los cortafuegos.

Como bien se sabe, el desafío de un entorno heterogéneo para las empresas y la falta de conciencia de seguridad pueden aumentar el riesgo de estas peligrosas anomalías de seguridad y las amenazas que afectan a su negocio. Las debilidades de seguridad deben ser abordadas a través de todas las capas de su entorno diversificado.

* **Ataques por mala configuración:** las malas configuraciones de seguridad surgen cuando no se definen, implementan o mantienen los valores predeterminados de la configuración de seguridad, por lo general, esto significa que los ajustes de configuración no cumplen con los estándares de seguridad de la industria (puntos de referencia de la CEI, OWASP top 10, etc.) que son fundamentales para mantener la seguridad y reducir el riesgo empresarial, la mala configuración normalmente ocurre cuando un administrador o desarrollador de sistemas o bases de datos no configura adecuadamente el marco de seguridad de una aplicación, sitio web, escritorio o servidor, lo que conduce a peligrosas vías abiertas para los *hackers.*

Las configuraciones erróneas suelen considerarse un blanco fácil, ya que pueden ser fáciles de detectar en servidores web, nubes y aplicaciones mal configurados y luego se convierten en explotables, causando un daño significativo y provocando problemas catastróficos de fuga de datos para las empresas, una vez que un sistema es presa de una vulnerabilidad o falta de seguridad, sus datos sensibles corren el riesgo de ser robados o alterados muy a menudo, el mayor problema al que se enfrentan las organizaciones es que estos fallos no se identifican o abordan con la suficiente antelación de acuerdo con las mejores prácticas de higiene de seguridad.

* **Ataques *srhink / wrap:*** cuando se instala un sistema operativo / aplicaciones viene una gran cantidad de *scripts* de ejemplo para hacer la vida de un administrador más fácil, el problema no es el afinamiento o la personalización de estos *scripts,* lo cual llevará a un código predeterminado o a ataques de código *shrink wrap*, para lo cual se considera un ataque de este tipo a solo el acto de explotar agujeros en *software* sin parches o mal configurado. Para utilizar el término de otra manera, una "vulnerabilidad de *shrink wrap"* sería aquella que solo debería verse en un producto inmediatamente después de su instalación inicial "recién salido del *shrink wrap*", se podría decir.

La mayor parte de Internet depende de un número relativamente pequeño de aplicaciones, marcos y sistemas operativos diferentes, dado que estas plataformas se comparten entre una gran base de destinatarios y que tantas organizaciones y/o administradores optan por ignorar el "fruto de la casualidad", este tipo de vulnerabilidades suelen ser las primeras a las que recurrirá un atacante para explotar rápidamente un sistema.

* + - 1. **Leyes y normas de la seguridad de información**

Cada país puede tipificar los delitos informáticos de forma diferente, pero en general cuando se contrata un servicio de *hacking* ético los límites están más determinados por lo que la organización esté buscando, si simplemente quiere conocer sus fallas o que también las exploten y saber el impacto real de esta actividad que, como se decía hace un momento, se está anticipando a que un atacante la pueda llevar a cabo.

* 1. **Aspectos legales de *hacking* ético**

La siguiente historieta recrea algunos aspectos legales del *hacking* ético, revísela.



Por otra parte, analice los problemas profesionales y códigos de ética para el *hacking* ético.

* + **Problemas profesionales del *hacking* ético**

Los problemas profesionales del *hacking* ético incluyen un posible desempeño ineficaz en el trabajo, el *hacking* ético puede estar limitado por la sensibilidad de la información involucrada en la organización del cliente. Los clientes tienden a imponer requisitos y límites a las actividades del *hacker* ético.

Para que el *hacking* ético se desempeñe adecuadamente, puede ser necesario el acceso a todo el sistema o la red, debido a la necesidad de profesionalidad, el *hacker* ético no debe violar los límites impuestos por el cliente para reducir al mínimo las cuestiones profesionales.

Las empresas son hostiles a la investigación en materia de seguridad con una frecuencia alarmante. He aquí un ejemplo de cómo una compañía de drones DJI, que tiene un programa de control de errores, amenazó a un investigador con presentar cargos por violar la Ley de fraude y abuso informático por presentar a la compañía una vulnerabilidad y PoC. Otra empresa hostil, River City Media, demandó a un investigador por localizar una gran operación de spam originada en sus servidores. El director de seguridad de Oracle también escribió una famosa carta hostil sobre cómo la ingeniería inversa de su *software* viola su licencia y lo demandarán por reportar errores.

* + **Códigos de ética**

Los códigos de ética o conducta para el *hacking* ético se centran en los deberes, responsabilidades y límites del *hacker* ético en el desempeño de su trabajo. El *hacker* ético se asegura de que el sistema o la red del cliente se evalúa adecuadamente para los problemas de seguridad y las vulnerabilidades.

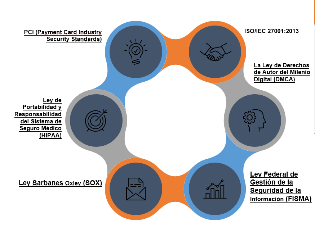
Debido a la naturaleza del *hacking* ético no es de extrañar que el hacker ético pueda encontrarse con información sensible, personal, confidencial o de propiedad exclusiva. A este respecto, el código de ética de la piratería ética debería guiar las acciones del *hacker* ético en el manejo de esa información. El código de ética debe centrarse en la protección del sistema o la red del cliente, así como en la eficacia del *hacker* ético en el desempeño de su trabajo.

¿Qué hace que el *hacking* ético sea "**ético**"? A continuación, verá cómo la piratería ética puede ayudar a proteger a las empresas de los ataques, así como examinar las formas en que puede asegurarse de que está trabajando con auténticos *hackers* éticos.

* **Realizado con consentimiento:** el *hacking* ético siempre se realiza con consentimiento. Si bien el objeto de los compromisos es reproducir con precisión las tácticas, técnicas y procedimientos utilizados por los ciberdelincuentes, nunca se diseña para que sea malicioso y tiene por objeto evitar daños y trastornos en las empresas. Antes de llevar a cabo una evaluación, una empresa profesional de seguridad cibernética se asegurará de que exista un acuerdo oficial que defina claramente el alcance de las evaluaciones y mantenga la confidencialidad del cliente.
* **Realizada por expertos:** el pirateo ético siempre debe ser realizado por profesionales capacitados que comprendan las últimas herramientas y técnicas de piratería informática y que realicen evaluaciones según las normas técnicas, legales y éticas más elevadas.
* **Realizadas por consultores con certificación de seguridad:** al encargar una evaluación ética del *hacking* es importante tener plena confianza en las personas involucradas. Cuando una prueba con bolígrafo implica el acceso a información altamente confidencial y/o clasificada, las empresas pueden considerar garantías adicionales, como el uso de probadores con una autorización de seguridad de alto nivel.
* **Realizada de acuerdo con las leyes actuales:** hay muchos aspectos legales que deben ser considerados cuando se experimenta el *hacking* ético. Los probadores pueden, a través del proceso normal de un compromiso, acceder a datos altamente sensibles. Para lograr un objetivo acordado pueden tener la necesidad de extraer esta información.
* **Realizado de forma transparente:** es esencial que las evaluaciones éticas del *hacking* sean lo más transparentes posible. Un *hacker* ético siempre compartirá los hallazgos y ofrecerá consejos de reparación para asegurar que las vulnerabilidades sean reportadas y tratadas. Debe estar localizable durante los compromisos y proporcionar informes escritos claros para resumir las conclusiones y recomendaciones. Hay muchas cosas a considerar cuando se encarga un *hacker* ético para su negocio. En cualquier caso, es una buena idea trabajar con un proveedor muy experimentado que esté dispuesto a hablarle de los riesgos y a asegurarse de que todo el proceso se lleve a cabo de la forma más segura posible y ofrezca resultados tangibles.
  1. **Normatividad legal vigente**

La normatividad para que se pueda realizar hacking ético depende de la legislación del país donde se ejecute, en la siguiente figura se presentan algunas leyes que pueden permitirse y ser aplicadas a nivel global.

**Figura 4**

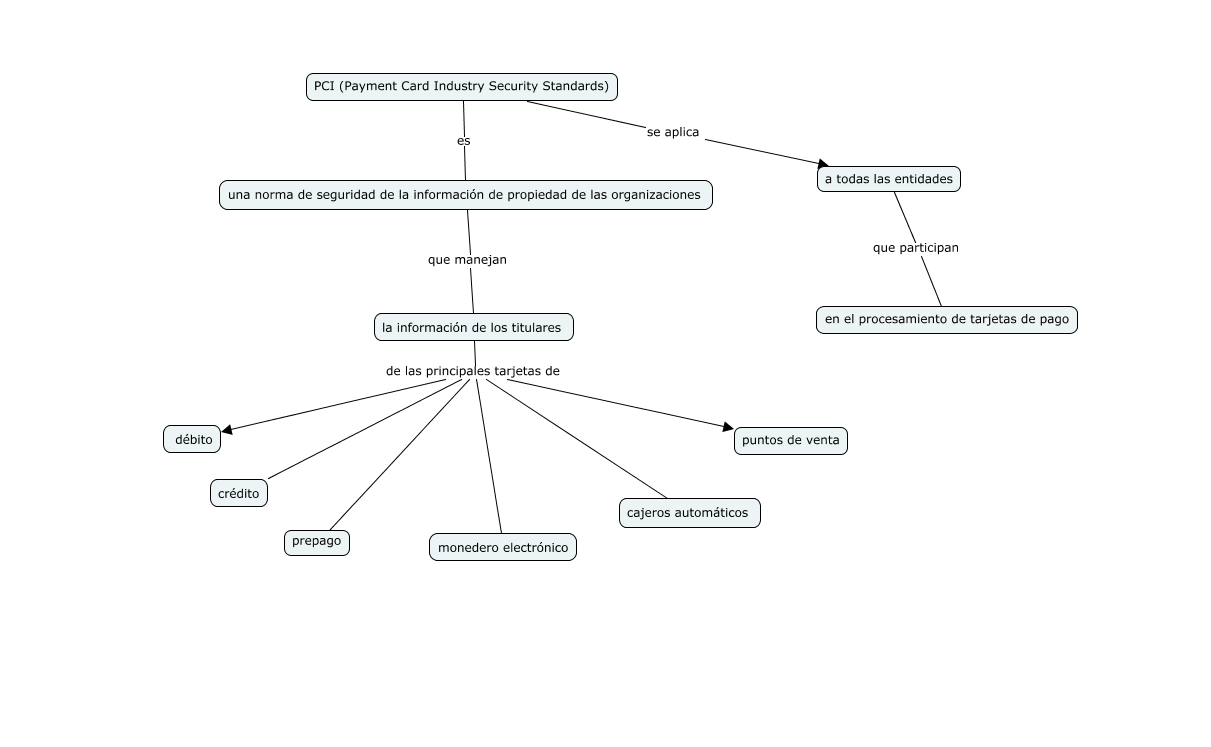
*Normatividad legal vigente*



A continuación, se realizará la descripción de cada una.

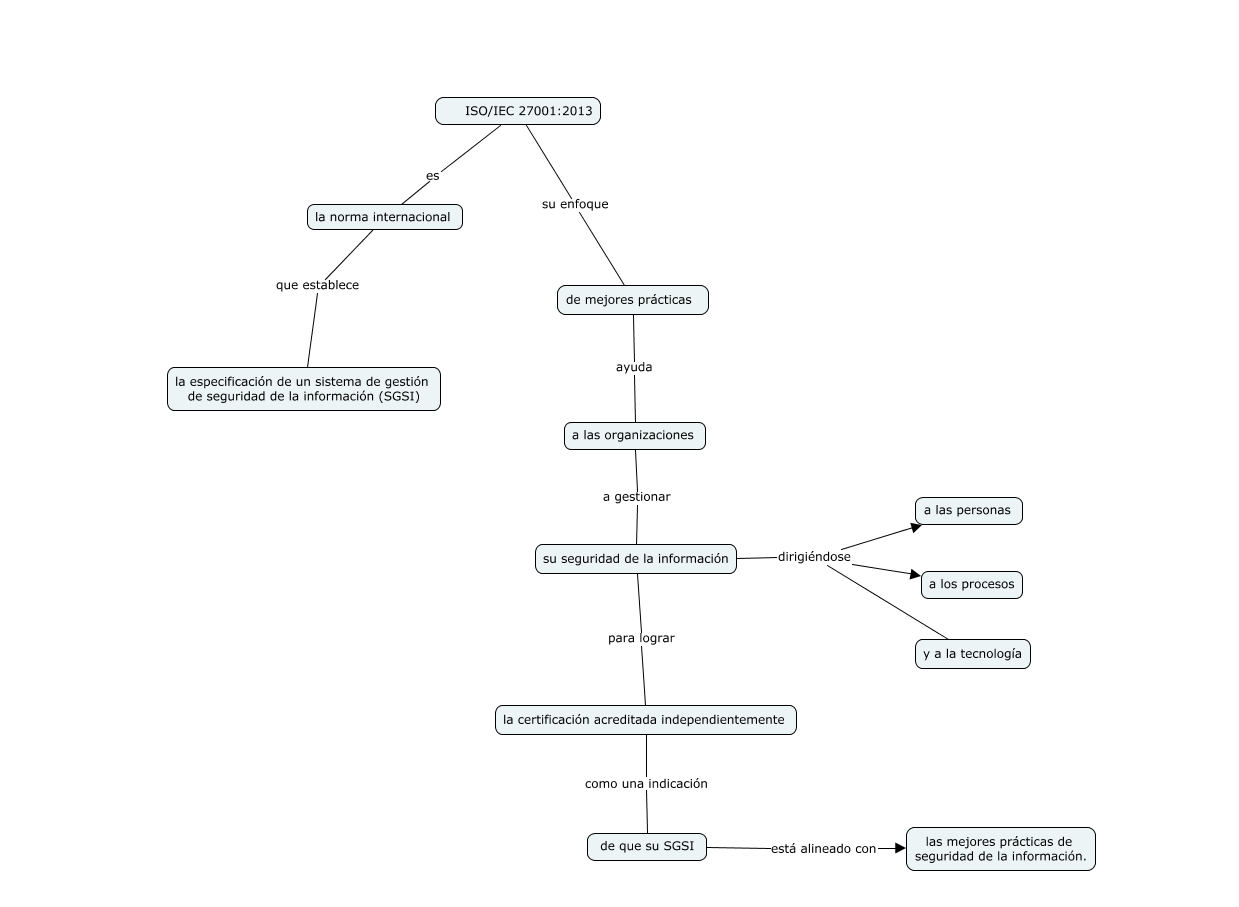
* **PCI (Payment Card Industry Security Standards)**

También conocida como la norma de seguridad de datos de la industria de las tarjetas de pago (PCI DSS).



* **ISO/IEC 27001:2013**

También conocida como ISO27001.



* **Ley de Portabilidad y Responsabilidad del Sistema de Seguro Médico (HIPAA)**

HIPAA es el acrónimo de la Ley de Portabilidad y Responsabilidad del Seguro Médico que fue aprobada por el congreso americano en 1996. La HIPAA hace lo siguiente:





* **Ley Sarbanes Oxley (SOX)**

La Ley Sarbanes-Oxley de 2002. 







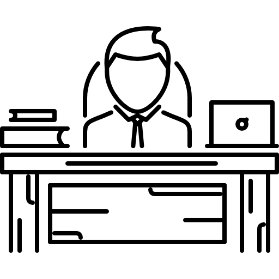












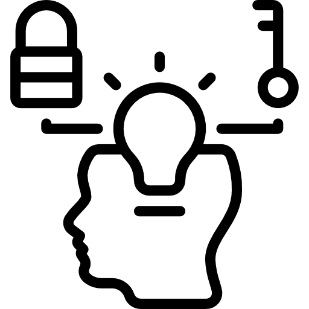


* **La Ley de Derechos de Autor del Milenio Digital (DMCA)**

Es una ley de derechos de autor de los Estados Unidos.























* **Ley Federal de Gestión de la Seguridad de la Información (FISMA)**

FISMA es la Ley Federal de Gestión de la Seguridad de la Información aprobada por el Congreso de los Estados Unidos en 2002, exige a los organismos federales que apliquen planes de seguridad de la información para proteger los datos sensibles.



Más concretamente, el NIST:

* Establece los requisitos mínimos para los planes y procedimientos de seguridad de la información.
* Recomienda los tipos de seguridad (sistemas, programas informáticos, etc.) que los organismos deben aplicar y aprueba a los proveedores.
* Estandariza el proceso de evaluación de riesgos y establece diversas normas de seguridad de la información basadas en las evaluaciones de riesgos de los organismos. Cada organismo tiene diferentes niveles de requisitos de seguridad: el Organismo Nacional de Seguridad y el Organismo de Vivienda y Desarrollo Urbano, por ejemplo, tienen diferentes niveles de riesgo y, por consiguiente, diferentes requisitos de seguridad.
  + - 1. **Metodologías del *hacking* ético**

Se le invita a revisar el siguiente recurso que hace una introducción a las metodologías del *hacking* ético.

****

* 1. **Estándares y metodologías**

A continuación, puede revisar algunas de las metodologías más populares usadas por los *hackers* éticos.

* + **OSSTMM**

El “Manual de la Metodología Abierta de Testeo de Seguridad” se ha convertido en un estándar de facto. Sin duda supuso el primer acercamiento a una estructura global del concepto de seguridad. Si bien las pruebas incluidas y los *test* que se ejecutan no son especialmente innovadores, se ha convertido en una auténtica referencia para los organismos que quieren desarrollar un *testing* de calidad, ordenado y eficiente.

Para organizar y estructurar su contenido, la metodología se subdivide en los aspectos más importantes de los sistemas de información. Se destacan los siguientes aspectos como:













De manera sencilla se identifican una serie de actividades de testeo específicas por área, sobre las que se comprueban las especificaciones de seguridad, integradas con las verificaciones realizadas en las revisiones rutinarias.

****

Un aspecto importante de esta metodología es que no solo se centra en los aspectos eminentemente técnicos de seguridad tradicionales, sino que abarca aspectos sobre los responsables del testeo, trata de estandarizar las credenciales del desarrollador a cargo del *test*, el formato de los resultados, crear un código ético, un plan temporal de ejecución, entre otros, un aspecto muy importante de la metodología, es la incorporación del concepto de valores de evaluación de riesgo, que permiten diferenciar y clasificar las diferentes problemáticas (Caballero, 2015).

OSSTMM plantea categorizaciones estándar, que permiten identificar claramente el alcance de cada una de las actividades, evitando inconvenientes en tal sentido:

1. **Búsqueda de vulnerabilidades**: orientado principalmente a realizar comprobaciones automáticas de un sistema o sistemas dentro de una red.
2. **Escaneo de la seguridad**: orientado a las búsquedas principales de vulnerabilidades en el sistema que incluyen verificaciones manuales de falsos positivos, identificación de los puntos débiles en el sistemas y análisis individualizado.
3. ***Test* de intrusión**: se plantean *test* de pruebas que se centran en romper la seguridad de un sistema determinado.
4. **Evaluación del riesgo**: se refiere a los análisis de seguridad a través de entrevistas e investigación de nivel medio que incluye la justificación negocios, las justificaciones legales y las justificaciones específicas de la industria.
5. ***Auditoría de seguridad****:* se refiere a la continua inspección que sufre el sistema por parte de los administradores que controlan que se cumplan las políticas de seguridad definidas.
6. ***Hacking* ético**: orientado a tratar de obtener, a partir de los *test* de intrusión, objetivos complejos dentro de la red de sistemas.
   * **ISSAF**

El ISSAF (*Information System Security Assessment Framework*) es un enfoque especializado y estructurado para las pruebas de penetración, más importante aún, el *framework* proporciona metodologías avanzadas que están personalizadas para el contexto.

Estos estándares le permiten al *pentester* planificar y ejecutar cada paso del proceso de prueba de penetración, por lo tanto, satisface todos los requisitos del proceso de prueba de penetración. Como *hacker* ético si está utilizando diferentes herramientas, ISSAF es un framework crucial, por ejemplo, vincula cada paso a una herramienta específica y, por lo tanto, reduce la complejidad.

ISSAF ofrece información adicional sobre varios vectores de ataque, así como el resultado de la vulnerabilidad después de la explotación, toda esta información permite a los evaluadores planificar un ataque avanzado que garantiza beneficios al tiempo que protege los sistemas de los ataques cibernéticos.

* + **OWASP**

“OWASP Testing Project”Project” (está muy orientado a realizar pruebas sobre aplicaciones web y está en el camino de convertirse en uno de los proyectos referencia en su ámbito OWASP, ha conseguido ser una referencia habitual para cualquier desarrollador en el ámbito de la seguridad OTP en particular, se encuentra enfocado a responder preguntas tales como ¿qué?, ¿por qué?, ¿cuándo?, ¿dónde? y ¿cómo? Al testear una aplicación web se cubren los siguientes puntos:

* El alcance de qué testear.
* Principios del testeo.
* Explicación de las técnicas de testeo.
* Explicación general acerca del *framework* de testeo de OWASP.
  + OTP incorpora en su metodología de testeo, aspectos clave relacionados con el “Ciclo de vida del desarrollo de *software*” a fin de que el “testeo a realizar comience mucho antes de que la aplicación web se encuentre en producción, de este modo, y teniendo en cuenta que un programa efectivo de testeo de aplicaciones web, debe incluir elementos como testear personas, procesos y tecnologías, OTP delinea en su primer parte conceptos claves a la vez que introduce un *framework* específicamente diseñado para evaluar la seguridad de aplicaciones web a lo largo de su vida.
  + **CEH**

Acrónimo de “*Certified Ethical Hacker* “ es uno de los más reconocidos internacionalmente en el campo del *hacking* ético y la auditoría de sistemas informáticos, es una metodología de pruebas de seguridad desarrollada por el *International Council of Electronic Commerce Consultants (*EC Council) algunas de las fases enunciadas en esta metodología son:

* Obtención de información.
* Obtención de acceso.
* Enumeración.
* Escalamiento de privilegios.
* Reporte.
* **Offensive Security**

Metodología líder a nivel mundial para el desarrollo de pruebas de penetración y estudios de seguridad, la metodología contempla principalmente los métodos para el desarrollo de estudios de seguridad enfocados en seguridad ofensiva y teniendo como marco la posibilidad real de explotación, independientemente de los indicadores de riesgos y vulnerabilidades, las principales

ventajas de adoptar este marco metodológico son:

* Enfoque sobre la explotación real de las plataformas.
* Enfoque altamente intrusivo.
* Enfoque orientado a resultados tangibles y no a estadísticas generadas por herramientas.
  1. **Buenas prácticas**

Se utiliza para identificar los riesgos y poner de relieve las acciones correctivas, y también reduce los

costos de las Tecnologías de la Información y la Comunicación (TIC); sin embargo, a menos que las empresas primero sepan que es lo que buscan, y por qué están contratando a un proveedor externo para hackear los sistemas en primer lugar, lo más probable es que no se gane mucha experiencia del ejercicio, un *hacker* ético, solo puede ayudar a la organización a entender mejor sus sistemas de seguridad, pero está de parte de la organización el colocar las salvaguardas en sus redes.

El *hacking* ético es un componente crucial para desarrollar las mejores prácticas y el buen gobierno para resolver las vulnerabilidades, desde:









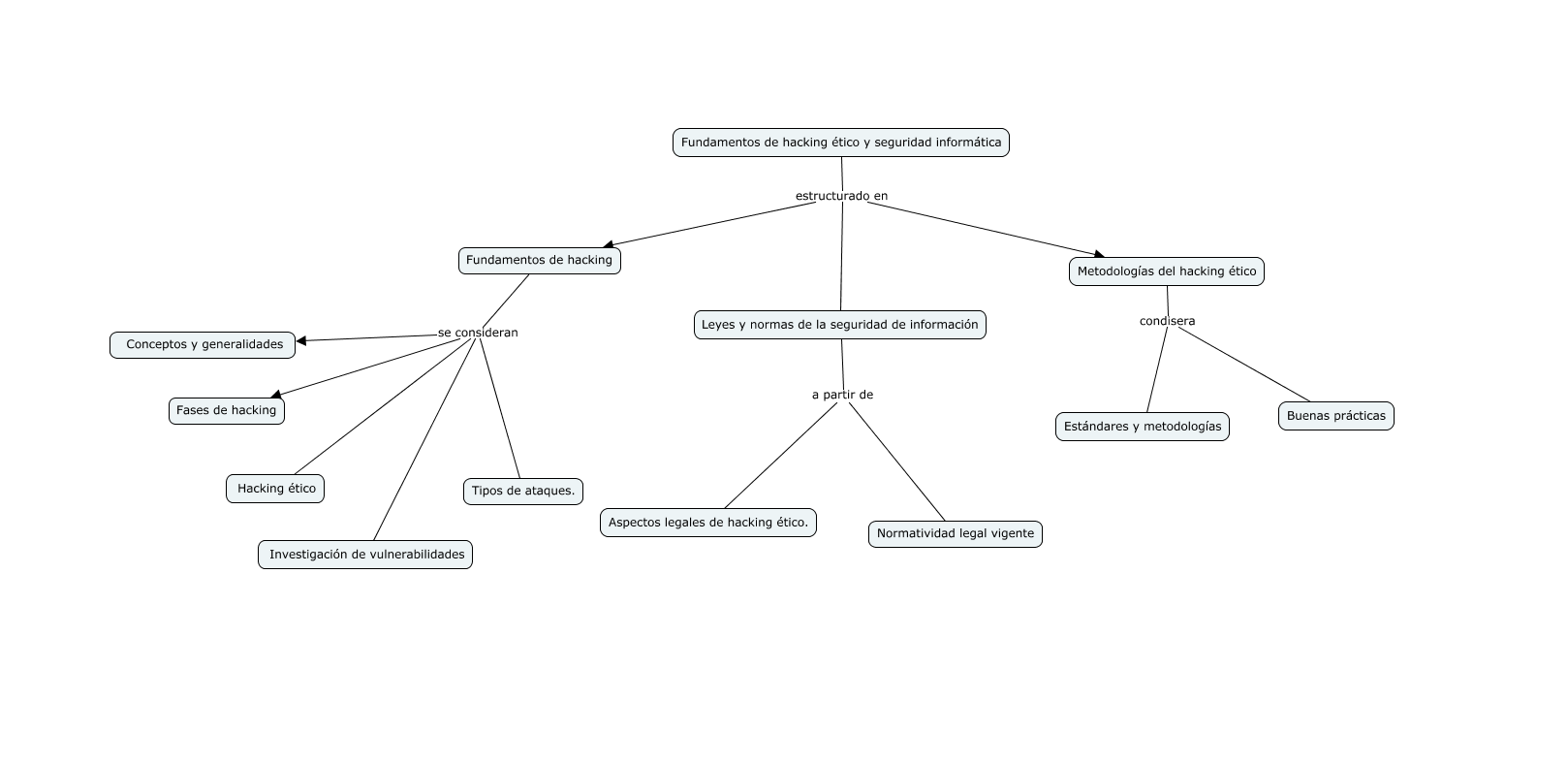


Dentro de las buenas prácticas de un *hacker* ético encontrará que ellos tratan de responder las siguientes preguntas:

* **¿Qué puede ver un intruso en el sistema de destino?** (reconocimiento y fases de exploración)
* **¿Qué puede hacer un intruso con esa información?** (obtención de acceso y permanencia)
* **¿Hay alguien en el objetivo que pueda detectar los intentos y aciertos de los intrusos?** (reconocimiento y cubrimiento de huellas)

1. **Síntesis**

En el siguiente mapa se presenta la síntesis de los *ítem* abordados en el componente formativo.



1. **Actividades didácticas (entre 1 y 2 actividades)**

| DESCRIPCIÓN DE LA ACTIVIDAD DIDÁCTICA | |
| --- | --- |
| Nombre de la actividad | Crucigrama de las características de las TIC |
| Objetivo de la actividad | Apropiar el contenido de las conceptos y generalidades del *hacking* ético para buenas prácticas de la seguridad informática y redes |
| Tipo de actividad sugerida | Crucigrama |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | Actividad\_Didactica 1 |

1. **Material complementario**

Relacionar el material de apoyo o complementario de los temas abordados en este recurso.

| Tema | Referencia APA del Material | Tipo de material  (Video, capítulo de libro, artículo, otro) | Enlace del Recurso o  Archivo del documento o material |
| --- | --- | --- | --- |
| Ethical hacking | Perú Hacking. (2020). *Fases del Ethical Hacking* [video]. YouTube. <https://www.youtube.com/watch?v=HG1N1kMj8cM> | Videoconferencia | <https://www.youtube.com/watch?v=HG1N1kMj8cM> |
| *Hackers* éticos | Betancourth, J. (2020). *Herramientas fundamentales para el hacking ético*. Universidad Piloto de Colombia. <http://polux.unipiloto.edu.co:8080/00001610.pdf> | Artículo científico | <http://polux.unipiloto.edu.co:8080/00001610.pdf> |
| Triada de la seguridad | Ontek. (2020). ¿Qué es? Tríada CID (Confidencialidad, Integridad y Disponibilidad <https://www.ontek.net/que-es-triada-cid/> | Sitio web | <https://www.ontek.net/que-es-triada-cid/> |

**g. Glosario**

| TÉRMINO | SIGNIFICADO |
| --- | --- |
| Cifrado | Esconder información, la cual se utiliza con el fin de proteger la estructura de los datos e información de una empresa o persona. |
| *Exploit* | Término acuñado en informática para explotar o aprovechar una vulnerabilidad de un sistema o red, se realiza a través de fragmentos de código. |
| *Insider* | Es una amenaza interna, un riesgo para la seguridad que se origina dentro de la organización objetivo, esto no significa que el responsable deba ser un empleado u oficial actual de la organización. Puede ser un consultor, exempleado, socio comercial o miembro de la junta. |
| *Sniffing* | Técnica de un *hacker* que se realiza por medio de “escuchar” para poder captar información importante tales como contraseñas o datos sensibles. |
| Vulnerabilidad | Se puede determinar cómo errores de un sistema o red que puede conllevar a que un tercero se aproveche de ella para hacer robo, manipulación o eventos inesperados en el sistema. |

**h. Referencias bibliográficas**

Borges, E. (2019). Servidor FTP. <https://blog.infranetworking.com/servidor-ftp/>

Borges, S. (2019). Servidor web. <https://blog.infranetworking.com/servidor-web/>

Caballero, A. (2015). Introducción a OSSTMM (Open Source Security Testing Methodology Manual). <http://www.reydes.com/d/?q=Introduccion_a_OSSTMM_Open_Source_Security_Testing_Methodology_Manual>

Castillo, J. (2018). Active directory qué es y para qué sirve. <https://www.profesionalreview.com/2018/12/15/active-directory/>

Echeverry, J. (2009). Metodología para el diagnóstico continuo de la seguridad informática de la red de datos de la Universidad Militar Nueva Granada.

<https://pdfs.semanticscholar.org/60c7/dbe2abab31a25422c92ead74085fd7093715.pdf>

Gaviria, R. (2015). Guía práctica para pruebas de *pentest* basada en la metodología OSSTMM V2.1 y la guía OWASP V3.0. [http://repositorio.unilibrepereira.edu.co:8080/pereira/bitstream/handle/123456789/622/GUÍA%20PRÁCTICA%20PARA%20PRUEBAS.pdf?sequence=1](http://repositorio.unilibrepereira.edu.co:8080/pereira/bitstream/handle/123456789/622/GU%C3%8DA%20PR%C3%81CTICA%20PARA%20PRUEBAS.pdf?sequence=1)

INCIBE. (2017). Amenaza vs. vulnerabilidad, ¿sabes en qué se diferencia? <https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian>

Martínez, E. (2018). Las diferentes amenazas de seguridad informática. <https://sites.google.com/site/lasamenazaslainformatica/>.

Zuluaga, A. (2017). *Hacking* ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la rama judicial, seccional Armenia. <https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17410/1/94288061.pdf>

**i. Control del documento**

|  | Nombre | Cargo | Dependencia  *(Para el SENA indicar Regional y Centro de Formación)* | Fecha |
| --- | --- | --- | --- | --- |
| Autor (es) | Pedro Javier Lozada Villota | Experto temático | Regional Cauca - Centro de Teleinformática y Producción Industrial | Noviembre de 2021 |
| Alix Cecilia Chinchilla Rueda | Diseñadora instruccional | Regional Distrito Capital - Centro de Gestión Industrial | Noviembre de 2021 |
| Rafael Neftalí Lizcano Reyes | Asesor pedagógico | Regional Santander - Centro Industrial del Diseño y la Manufactura | Noviembre de 2021 |
| Carolina Coca Salazar | Revisora metodológica y pedagógica | Regional Distrito Capital - Centro de Diseño y Metrología | Diciembre de 2021 |
| Julia Isabel Roberto | Diseñadora y evaluadora instruccional | Regional Distrito Capital – Centro para la Industria de la Comunicación Gráfica | Diciembre de 2021 |

**j. Control de cambios**

**(Diligenciar únicamente si realiza ajustes a la Unidad Temática)**

|  | Nombre | Cargo | Dependencia | Fecha | Razón del Cambio |
| --- | --- | --- | --- | --- | --- |
| Autor (es) |  |  |  |  |  |