**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 | 220501111-4. Documentar la información obtenida mediante formatos y criterios específicos para la organización. |
| --- | --- | --- | --- |

| NÚMERO DEL COMPONENTE FORMATIVO | CF005 |
| --- | --- |
| NOMBRE DEL COMPONENTE FORMATIVO | Controles, documentación y reportes en *hacking* ético |
| BREVE DESCRIPCIÓN |  |
| PALABRAS CLAVE | cifrar, clave, encriptar, llave, reporte |

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

1. **Tabla de contenidos**

**Introducción**

1. **Criptografía**
   1. Conceptos y generalidades
   2. Tipos y cifrados
   3. Herramientas criptográficas
   4. Firmas digitales
   5. Herramientas de cifrado y criptoanálisis
2. **Reportes**
   1. Tipos de reporte
   2. Elementos de un reporte

**Síntesis**

1. **Desarrollo de contenidos**

**Introducción**

Se le invita a revisar la introducción de este material de formación en el siguiente recurso:

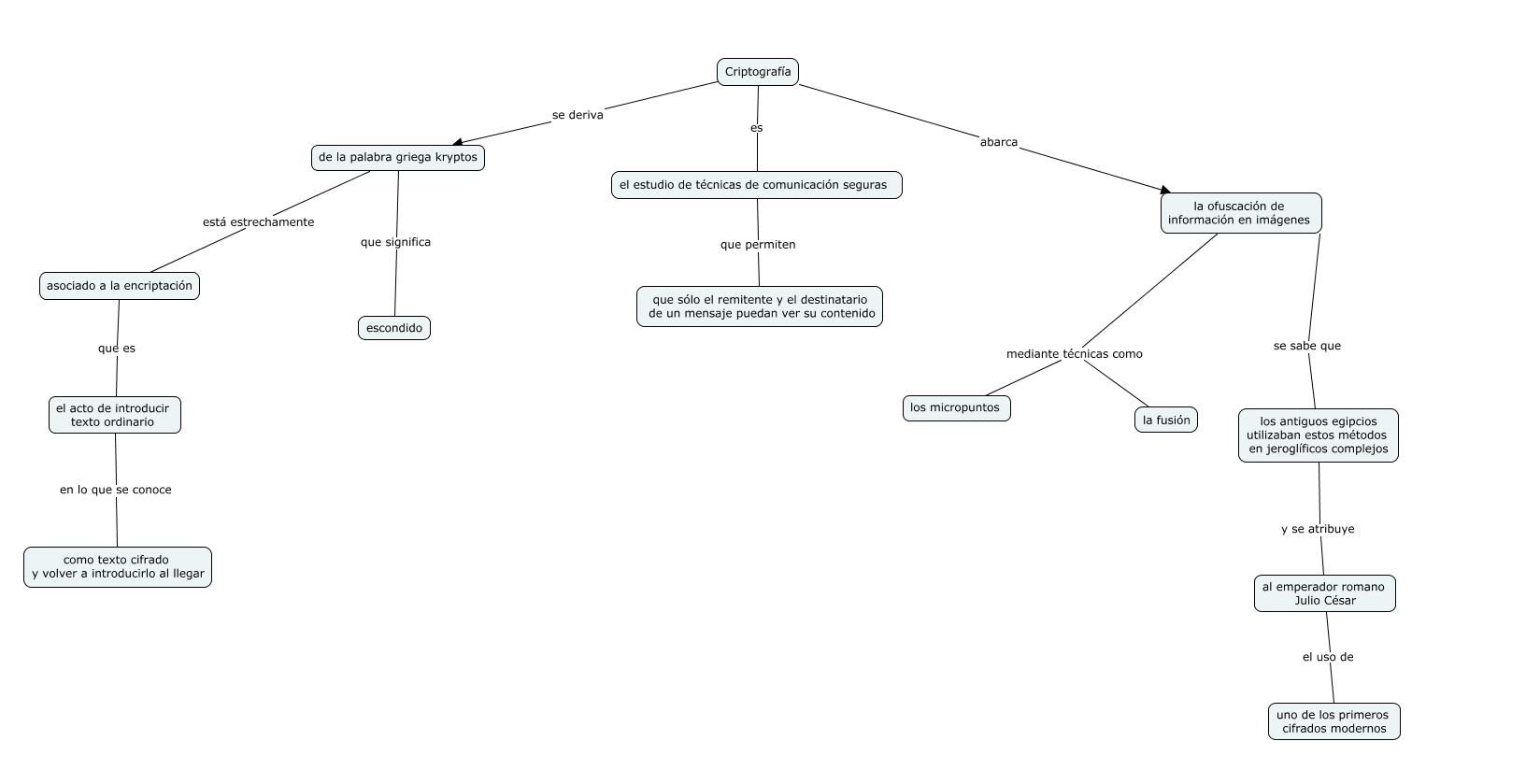


# **Criptografía**

Revise el siguiente mapa que trata el concepto de Criptografía

**Figura 1**

*Concepto de criptografía*



Cuando se transmiten datos electrónicos, el uso más común de la criptografía es cifrar y descifrar el correo electrónico y otros mensajes de texto plano. El método más simple utiliza el sistema simétrico o de "clave secreta"; en este caso, los datos se cifran utilizando una clave secreta, y luego tanto el mensaje codificado como la clave secreta se envían al destinatario para su descifrado.



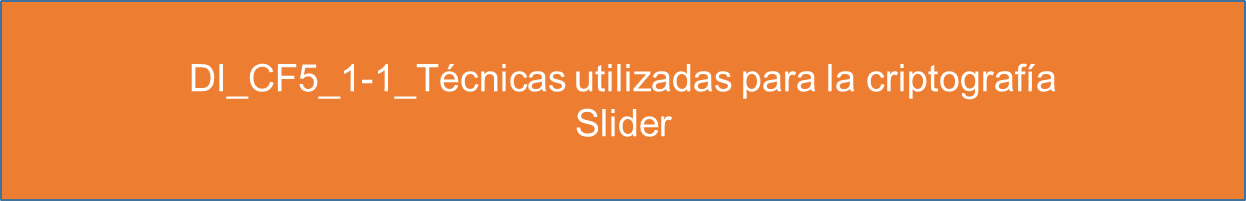
* 1. **Conceptos y generalidades**

La criptografía es la conversión de los datos en un código codificado que se descifra y se envía a través de una red privada o pública; se utiliza para proteger los mensajes de correo electrónico, información de tarjeta de crédito y datos corporativos.

* **Técnicas utilizadas para la criptografía:**

En la era actual de las computadoras, la criptografía suele asociarse con el proceso en el que un texto simple ordinario se convierte en texto cifrado, que es el texto hecho de tal manera que el receptor previsto del texto sólo puede decodificarlo y, por lo tanto, este proceso se conoce como cifrado. El proceso de conversión de un texto cifrado a texto plano se conoce como descifrado.

Las características de la criptografía son las siguientes:



* **Cifrado**

Se conoce como cifrado:

**Figura 2**

*Cifrado*















A continuación, se presenta un breve tratamiento de los cifrados, para un tratamiento completo.

**Figura 3**

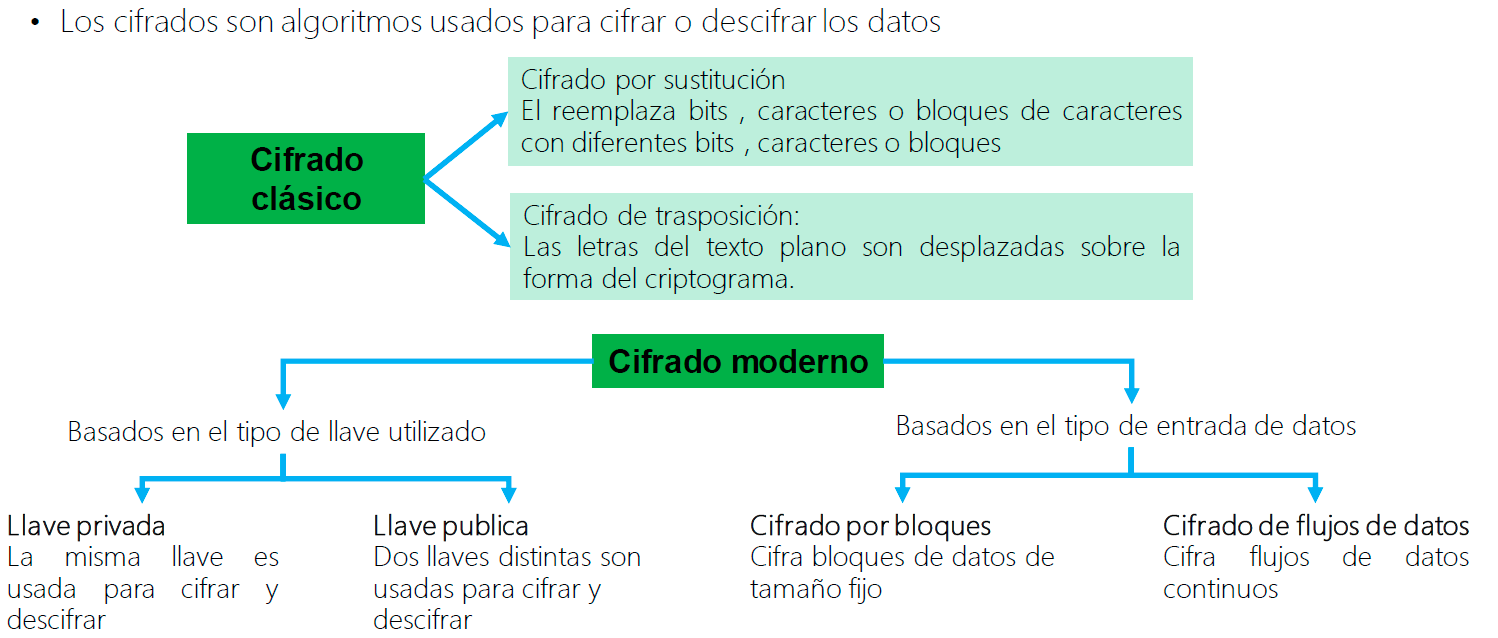
*Tratamiento de cifrado*





**Figura 4**

*Tipos de cifrado*



Se han utilizado comúnmente dispositivos o máquinas de cifrado para cifrar y descifrar mensajes. El primer dispositivo de cifrado parece haber sido empleado por los antiguos griegos alrededor del año 400 a.C. para las comunicaciones secretas entre los comandantes militares. Este dispositivo, llamado la guadaña, consistía en un bastón cónico alrededor del cual se envolvía en espiral un trozo de pergamino inscrito con el mensaje, cuando se desenvolvía, el pergamino llevaba un incomprensible juego de letras, pero cuando se envolvía alrededor de otro bastón de idénticas proporciones, el texto original reaparecía.

Otros dispositivos simples conocidos como discos cifrados fueron utilizados por los gobiernos europeos para las comunicaciones diplomáticas a finales de 1400. Estos dispositivos consistían en dos círculos concéntricos giratorios, ambos con una secuencia de 26 letras; un disco se usaba para seleccionar las letras de texto plano, mientras que el otro se usaba para el componente de cifrado correspondiente.

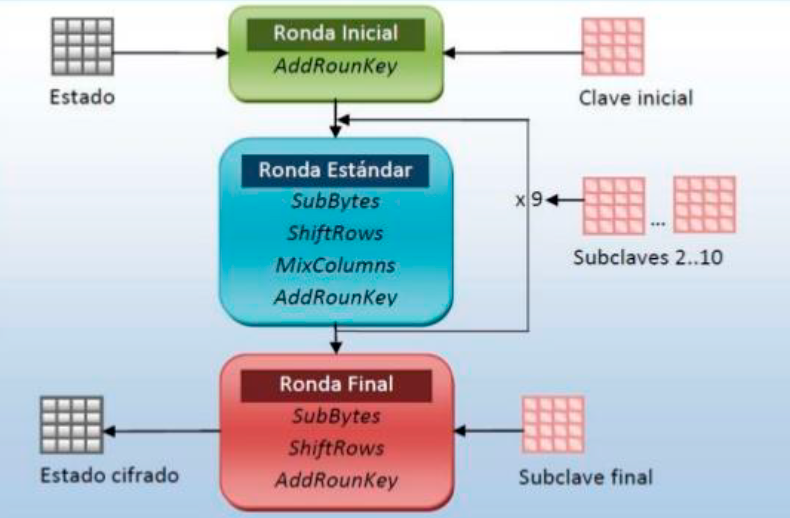
* 1. **Tipos y cifrados**

A continuación, estudiará los tipos de criptografía.



**Ahora aborde algunos estándares y algoritmos:**

* **Estándar de cifrado avanzado (AES)**

El cifrado AES fue establecido por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST) en 2001 y su objetivo es ofrecer una especificación para la encriptación de datos electrónicos.

Los desarrolladores del AES son dos criptógrafos belgas: Joan Deamen y Vincent Rijmen; se sabe que el dúo ha propuesto su cifrado en bloque al Instituto Nacional de Estándares y Tecnología durante el proceso de selección de un AES. Para seleccionar un AES seguro, el NIST consideró tres diferentes bloques de cifrado de la familia de cifrado Rijndael. Estos tres cifrados seleccionados eran todos de 128 bits, pero las longitudes de sus claves eran de 128, 192 y 265 bits.

Al final, se seleccionó el cifrado en bloque desarrollado por Rijmen y Daemen. Este AES fue adoptado por primera vez en los Estados Unidos, pero con el tiempo se convirtió en la corriente principal en todo el mundo; el AES se caracteriza por ser un cifrado en bloque simétrico, en otras palabras, utiliza la misma clave para el cifrado y el descifrado.

* **Estándar de encriptación de datos (DES**)

DES es el nombre del estándar FIPS (Federal Information Processing Standard) 46-3, el cual describe el algoritmo de cifrado de datos (DEA), que es un sistema criptográfico simétrico originalmente diseñado para implementación en el *hardware*; también es usado para encriptación de usuario simple para almacenar datos en el disco de forma encriptada, un algoritmo de cifrado en bloque que toma texto plano en bloques de 64 bits y los convierte en texto cifrado utilizando claves de 48 bits.

* **Algoritmos RC4, RC5, RC6**

RC4, RC5 y RC6 son los algoritmos de una encriptación simétrica. Estas soluciones son diferentes entre sí en cuanto a los métodos y enfoques utilizados para el cifrado de datos. Handy Backup puede proporcionar todas las funciones necesarias para respaldar los datos de su *software* RSA cuando lo necesite.

* El RC4 es un cifrado de flujo de tamaño de clave variable, con operaciones orientadas a los bytes. El algoritmo utiliza una permutación aleatoria para los datos.
* RC5 es un algoritmo parametrizado, que implementa un bloque de 32, 64 o 128 bits, un tamaño de clave variable y un número variable de rondas.
* El RC6 utiliza el RC5 con una suma de una multiplicación entera e implementando los cuatro registros de trabajo de 4 bits en lugar de los dos registros de 2 bits del RC5.

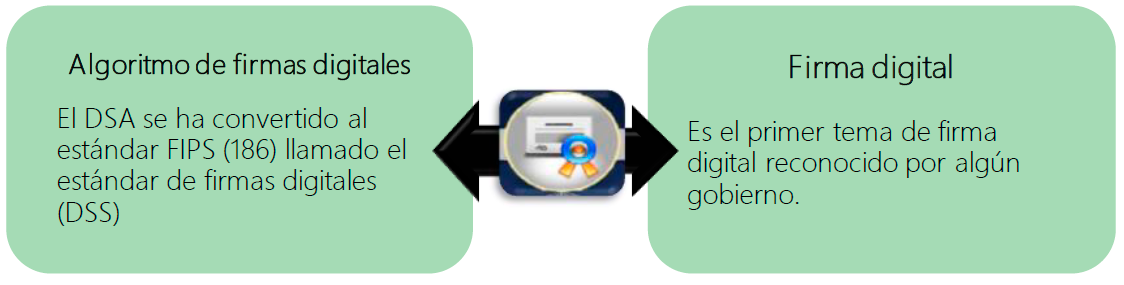
Estas soluciones de encriptación se aplican ampliamente en algunas áreas, incluyendo sitios web basados en Joomla CMS y algunas otras soluciones.

* **El DSA y los esquemas de firmas relacionados**

El Algoritmo de Firma Digital, o DSA, por sus siglas en inglés, utiliza un algoritmo diferente para la firma y la encriptación a RSA (Rivest Shamir Aldeman, el cual revisará más adelante), pero proporciona el mismo nivel de seguridad. Fue propuesto en 1991 por el Instituto Nacional de Estándares y Tecnología (NIST) y adoptado por el Estándar Federal de Procesamiento de Información (FIPS) en 1993; desde entonces, ha pasado por cuatro revisiones.

**Figura 5**

*Firma digital*



Un certificado de la DSA facilita el cumplimiento de las normas gubernamentales, ya que está avalado por los organismos federales, incluido el inminente paso a longitudes de clave de 2048 bits, incluso puede ejecutar RSA y DSA simultáneamente para mejorar aún más su seguridad, los servidores Apache, por ejemplo, pueden ejecutar los certificados RSA y DSA simultáneamente en un solo servidor web, esto beneficiará a las empresas que buscan maximizar el alcance de su ecosistema para su correspondencia comercial.

* **RSA (Rivest Shamir Aldeman)**

En la siguiente infografía, puede revisar el concepto



Como la mayoría de los criptosistemas, la seguridad de la RSA depende de cómo se implementa y se utiliza. Un factor importante es el tamaño de la llave, cuanto mayor es el número de bits de una llave (esencialmente la longitud de la misma), más difícil es romperla mediante ataques como la fuerza bruta y el factoraje.

Dado que los algoritmos de clave asimétrica como RSA pueden romperse mediante factorización de enteros, mientras que los algoritmos de clave simétrica como AES no pueden, las claves RSA necesitan ser mucho más largas para lograr el mismo nivel de seguridad. Actualmente, el mayor tamaño de clave que ha sido factorizado es de 768 bits de largo, esto fue hecho por un equipo de académicos durante un período de dos años, utilizando cientos de máquinas.

Dado que la factorización se completó a finales de 2009 y la potencia de computación ha crecido significativamente desde entonces, se puede asumir que un intento de intensidad similar podría ahora factorizar una clave RSA mucho más grande; a pesar de esto, el tiempo y los recursos necesarios para este tipo de ataque lo pone fuera del alcance de la mayoría de los hackers y en el ámbito de los estados nacionales. La mejor longitud de la clave a utilizar dependerá de su modelo de amenaza individual. El Instituto Nacional de Estándares y Tecnología recomienda un tamaño mínimo de clave de 2048 bits, pero también se utilizan claves de 4096 bits en algunas situaciones en las que el nivel de amenaza es mayor.

El factoraje es sólo una forma en la que el RSA puede romperse, otros ataques tienen el potencial de romper el cifrado con una cantidad menor de recursos, pero estos dependen de la aplicación y otros factores, no necesariamente del propio RSA.

* + **Funciones de resumen (*Bash* de una vía)**

A continuación, se presenta en qué consisten las funciones de resumen:



* + **Función de resumen del mensaje: MD5**

Revise ahora la función de resumen del mensaje, algoritmo MD5.



* **Algoritmo de Hashing Seguro (SHA)**

Los algoritmos *Secure* *Hash*, también conocidos como SHA, son una familia de funciones criptográficas diseñadas para mantener los datos seguros, funcionan transformando los datos mediante una función *hash*: un algoritmo que consiste en operaciones de bits, adiciones modulares y funciones de compresión.

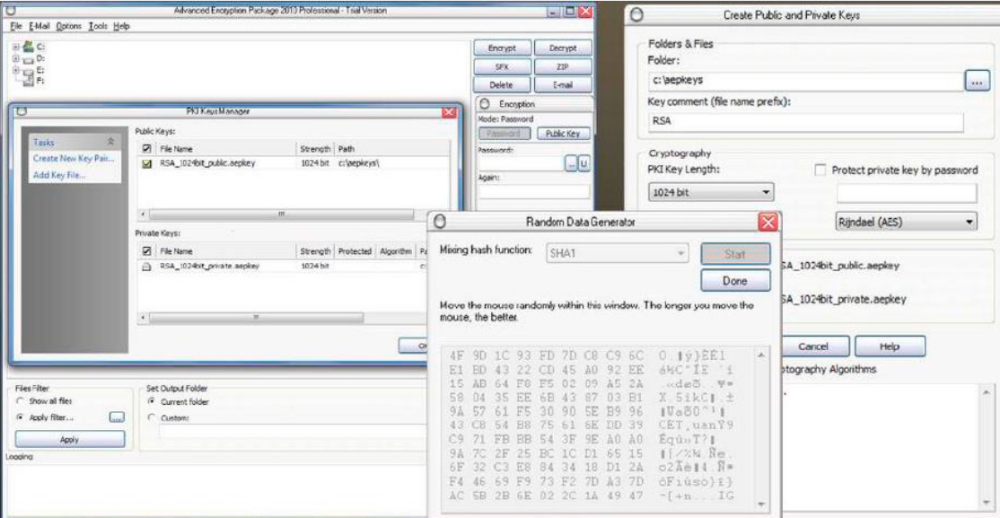


Además, las SHA exhiben el efecto de avalancha, en el que la modificación de muy pocas letras que se cifran provoca un gran cambio en la salida; o, por el contrario, cadenas drásticamente diferentes producen valores de *hash* similares. Este efecto hace que los valores *hash* no den ninguna información sobre la cadena de entrada, como su longitud original. Además, los valores de *hash* también se utilizan para detectar la manipulación de los datos por parte de los atacantes, en la que, si un archivo de texto se modifica ligeramente y apenas se nota, el valor de *hash* del archivo modificado será diferente del valor de *hash* del archivo original, y la manipulación será bastante notable.

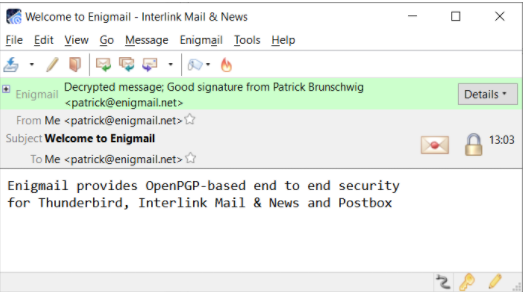
* 1. **Herramientas criptográficas**

Hoy en día, las organizaciones manejan información sensible y confidencial que es perentorio proteger y salvaguardar, ya que esta puede caer en manos de terceros. Es por ello que, para mitigar estos riesgos y amenazas, resulta imprescindible el conocer las diferentes herramientas de cifrado; en este módulo, se van a mirar algunas de ellas, que ayudan a cifrar y proteger la información; entre las que se pueden encontrar en la red y se pueden usar en las organizaciones están:

* **Herramienta de criptografía: Advanced Encryption Package**

Disponible en <http://www.aeppro.com>

* **Herramienta de cifrado: Enigmail**

****

Disponible en: <https://www.enigmail.net/index.php/en/>

Igualmente, existen un sinnúmero de herramientas y aplicaciones que pueden servirle para poder cifrar o encriptar su información que puede consultar en la red según las necesidades de la organización para poder proteger la información, hay desde protección de discos duros hasta protección de correos electrónicos.

* 1. **Firmas digitales**

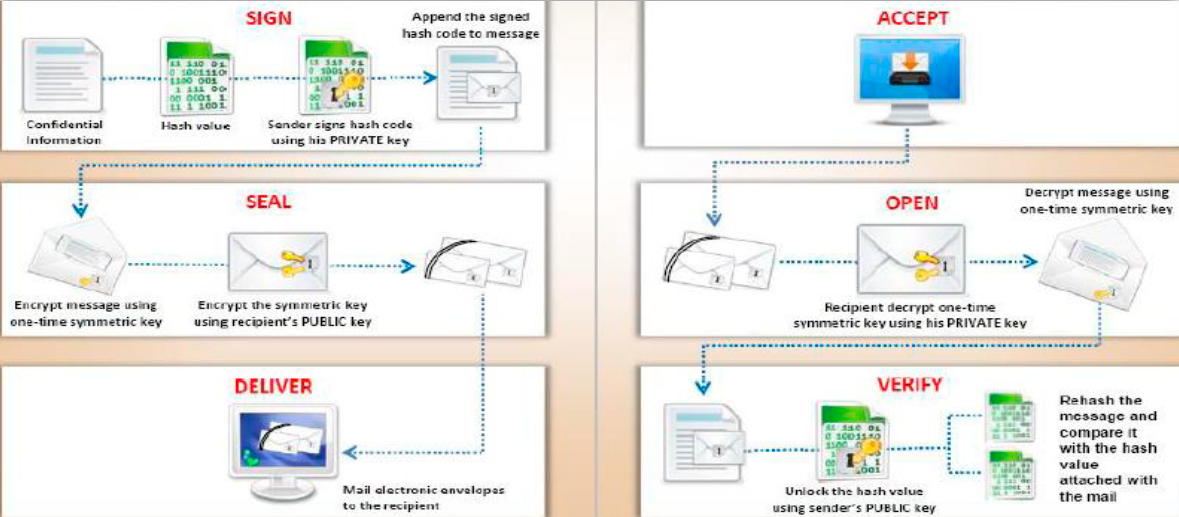
La firma digital utiliza un cifrado asimétrico para simular las propiedades de seguridad de la firma en digital por la forma que se escribió. Los esquemas de firma digital involucran dos algoritmos, una llave privada para firmar el mensaje y una llave pública para verificar las firmas.

Las firmas digitales funcionan utilizando un algoritmo matemático, los proveedores de soluciones de firma digital como Zoho Sign, generarán dos claves: una clave pública y una clave privada. Cuando un firmante firma digitalmente un documento, se genera un *hash* criptográfico para el documento.

Ese *hash* criptográfico se cifra entonces utilizando la clave privada del remitente, que se almacena en una caja HSM segura. A continuación, se adjunta al documento y se envía a los destinatarios junto con la clave pública del remitente.

**Figura 6**

*Clave pública*



El destinatario puede descifrar el *hash* codificado con el certificado de clave pública del remitente. Un *hash* criptográfico se genera de nuevo en el extremo del destinatario.

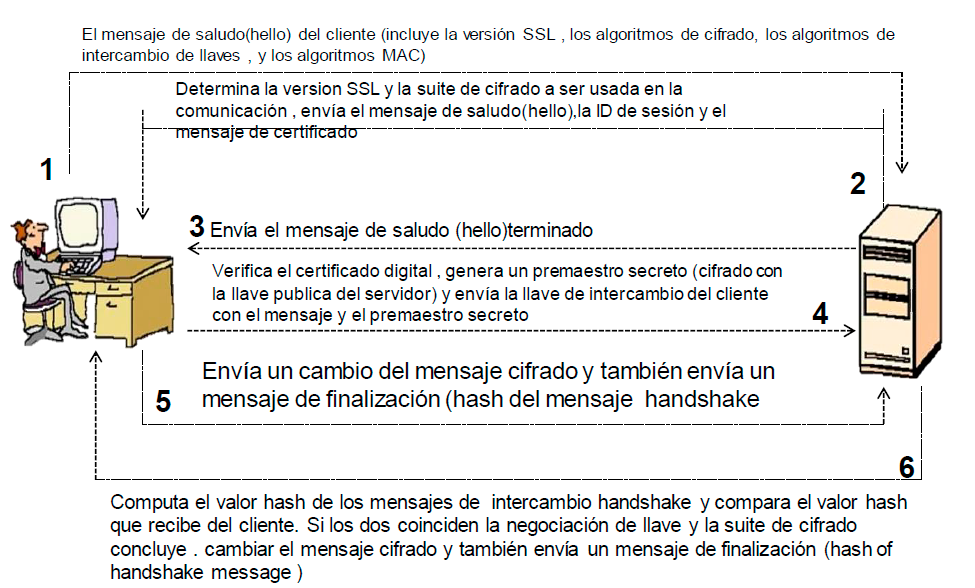
Ambos *hashes* criptográficos se comparan para comprobar su autenticidad. Si coinciden, el documento no ha sido manipulado y se considera válido.

* **Certificado SSL**

SSL es el acrónimo de Secure Sockets Layer (capa de sockets seguros), la tecnología estándar para mantener segura una conexión a Internet, así como para proteger cualquier información confidencial que se envía entre dos sistemas e impedir que los delincuentes lean y modifiquen cualquier dato que se transfiera, incluida información que pudiera considerarse personal. Los dos sistemas pueden ser un servidor y un cliente (por ejemplo, un sitio web de compras y un navegador) o de servidor a servidor (por ejemplo, una aplicación con información que puede identificarse como personal o con datos de nóminas).

**Figura 7**

*Certificado SSL*



Esto lo lleva a cabo asegurándose de que todos los datos que se transfieren entre usuarios y sitios web o entre dos sistemas sean imposibles de leer. Utiliza algoritmos de cifrado para codificar los datos que se transmiten e impedir que los hackers los lean al enviarlos a través de la conexión. Esta información podría ser cualquier dato confidencial o personal, por ejemplo, números de tarjeta de crédito y otros datos bancarios, nombres y direcciones.

* 1. **Herramientas de cifrado y criptoanálisis**

La encriptación de discos es una tecnología que protege la información convirtiéndola en un código ilegible que no puede ser descifrado fácilmente por personas no autorizadas. La encriptación de discos utiliza *software* o *hardware* de encriptación de discos para encriptar cada bit de datos que va en un disco o volumen de disco. Se utiliza para impedir el acceso no autorizado al almacenamiento de datos. Revise la siguiente figura:

**Figura 8**

*Herramientas de cifrado*



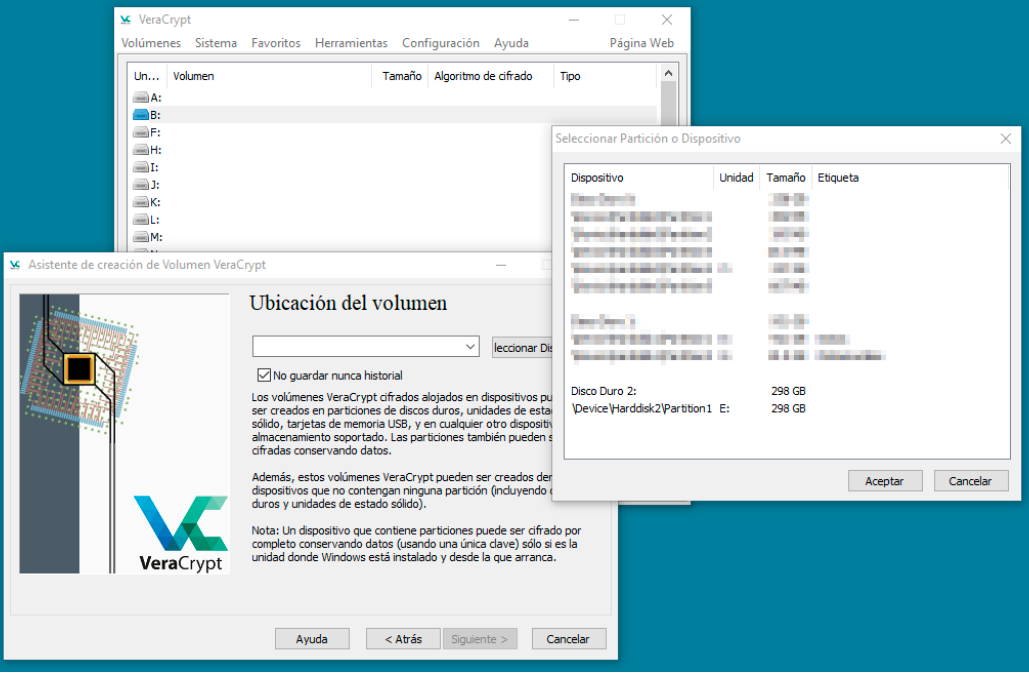




La expresión cifrado de disco completo (FDE) significa que todo lo que hay en el disco está cifrado, pero el registro de arranque maestro (MBR), o un área similar de un disco de arranque, con el código que inicia la secuencia de carga del sistema operativo, no está cifrado. Algunos sistemas de encriptación de disco completo basados en *hardware* pueden realmente encriptar un disco de arranque completo, incluyendo el MBR.

* **Herramienta de cifrado de datos: VeraCrypt**

VeraCrypt es una utilidad gratuita disponible en la fuente, que se utiliza para el cifrado sobre la marcha (OTFE). Puede crear un disco cifrado virtual dentro de un archivo o cifrar una partición o (en Windows) todo el dispositivo de almacenamiento con autenticación previa al arranque.

****

**Herramienta de cifrado de datos: BitLocker**

BitLocker es una característica de cifrado integrada en equipos que ejecutan Windows 10 Pro; si ejecuta Windows 10 Home no podrá usar BitLocker. Crea un entorno seguro para sus datos sin necesidad de realizar ningún esfuerzo adicional por su parte. De hecho, una vez que se configura.



Aquí están otros enlaces con algunas herramientas de criptoanálisis

* Cryptanalysis Tools <https://sourceforge.net/projects/cryptanalysisto/>
* Ganzua <http://ganzua.sourceforge.net/es/index.html>
* Crank <http://crank.sourceforge.net/downloads.html>
* AlphaPeeler <http://alphapeeler.sourceforge.net/me/?page_id=16>
* EverCrack <https://sourceforge.net/projects/evercrack/>
* CryptoBench <http://www.addario.org/cryptobench/>

1. **Reportes**

En las pruebas de penetración, la redacción de informes es una tarea exhaustiva que incluye la metodología, los procedimientos, la explicación adecuada del contenido y el diseño del informe, un ejemplo detallado del informe de la prueba y la experiencia personal del probador. Una vez preparado el informe, se comparte entre el personal directivo superior y el equipo técnico de las organizaciones objetivo; si en el futuro surgiera algún tipo de necesidad de este tipo, este informe se utiliza como referencia.

Un informe de *pentesting* o *ethical hacking* es un resumen del proceso de penetración, las vulnerabilidades identificadas y las recomendaciones para mitigarlas. Una prueba que tenga un proceso confirmado, regulado y observado puede representar un resumen de un informe eficaz e imparcial.

En gran medida, los informes están orientados a la técnica y carecen de recomendaciones prácticas, estos tampoco explican los impactos comerciales debido a la existencia de las vulnerabilidades enumeradas. Un tester bien cualificado no sólo encuentra las debilidades, sino que también explica su impacto en el cliente; es importante escribir un informe con un valor añadido real; el informe debe proporcionar al cliente soluciones realistas a los riesgos identificados; la parte final del informe del test debe incluir los detalles del proceso de despliegue.

* 1. **Tipos de reporte**

La planificación del informe comienza con los objetivos, que ayudan a los lectores a entender los puntos principales de las pruebas de penetración, esta parte describe por qué se realizan las pruebas, cuáles son los beneficios de las pruebas, con bolígrafo, etc. En segundo lugar, la planificación del informe también incluye el tiempo empleado en las pruebas, las cuales son consignadas en diferentes tipos de reportes que se deben entregar, los cuales se clasifican en:

* Informe ejecutivo
* Informe técnico
* Plan de mitigación
  1. **Elementos de un reporte**

Los principales elementos de la redacción del informe son:



**Estructura más común de un informe de test**

Para poder entregar a las organizaciones los hallazgos encontrados en las pruebas de penetración realizadas a sus sistemas, se debe de tener en cuenta la siguiente estructura:

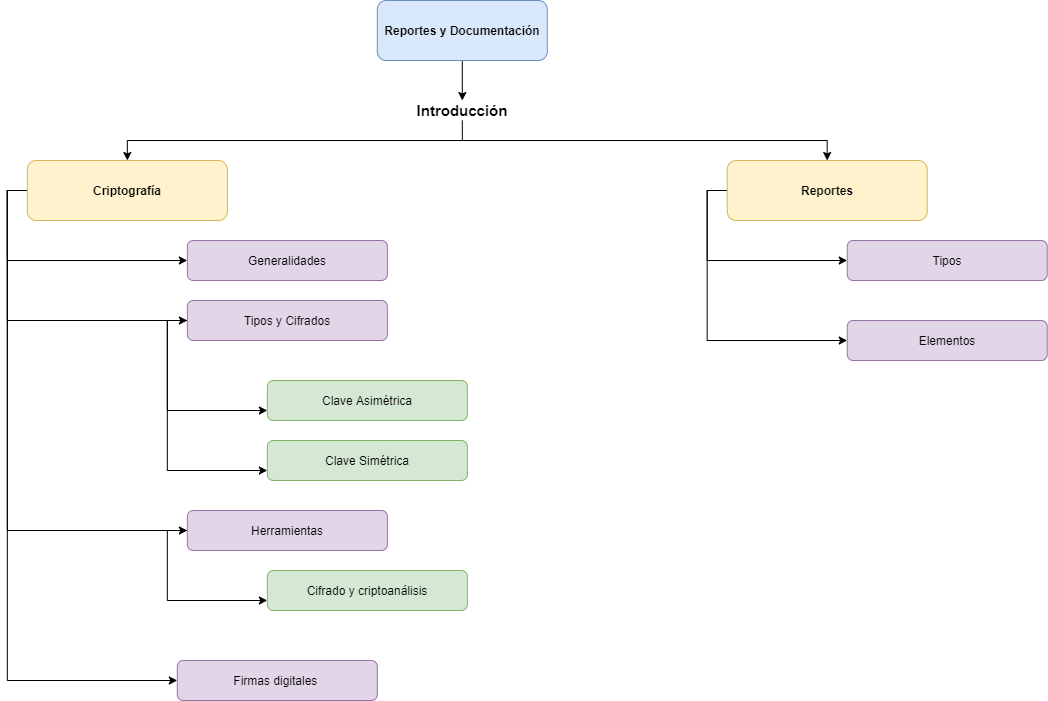
* Resumen ejecutivo del proyecto: El informe habla de la información del proyecto, sobre el propósito, objetivo y meta del proceso del test; resume el tema, los métodos de análisis, los resultados, las conclusiones, las recomendaciones y las limitaciones del informe. Aunque hay mucho que explicar sobre todo el proceso, el *pentester* o hacker ético debe mantenerlo conciso y preciso.
* Detalles del proyecto: En esta sección, el *pentester*, o hacker ético, describe el enfoque del proyecto, el proceso que utilizó y el alcance definido al inicio de la propuesta; detalla para qué ha sido contratado el *pentester* y establece las "reglas de combate", por ejemplo, qué es lo que probará, qué hará cuando lo haga, qué precauciones tomará, cómo se juzgará el éxito, a quién informará, etc.
* Información de la empresa: El informe también explica detalles de la organización, el tipo de negocio, los clientes a los que se dirige, el alcance del negocio y otra información legítima; incluye detalles de los miembros del equipo involucrados, sus calificaciones, funciones de trabajo, responsabilidades, etc. Gran parte de esto será opcional, ya que caerá en la información de acceso público. Sin embargo, algunos pueden ser incluidos, especialmente si esa información tiene que ver con el descubrimiento de vulnerabilidades posteriores que son explotadas posteriormente.
* Enumeración de los riesgos en función de la gravedad: Para hacer un informe estructurado, enumere los hallazgos con base en su gravedad, se debe dar prioridad a las vulnerabilidades de alto riesgo y enumerarlas arriba, seguidas de los hallazgos de bajo riesgo.

El formato puede ser el siguiente:

| Hallazgos | Descripción | Detalles | Gravedad | Recomendaciones |
| --- | --- | --- | --- | --- |

* + Descargo de responsabilidad: Una liberación de responsabilidades es una parte muy importante de un informe. Al ser un tester, es posible que enumere las vulnerabilidades, explique sus consecuencias y recomiende su mitigación, en el ámbito dado, las herramientas y los factores externos definidos; estas consecuencias pueden resultar en caso de que cambie alguno de los factores influyentes; una cláusula de exención de responsabilidad al final del informe resume la responsabilidad y define los límites de la prueba de penetración.

**Síntesis**



**C. Actividades didácticas**

| DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA | |
| --- | --- |
| Nombre de la Actividad | Crucigrama de las técnicas de la criptografía |
| Objetivo de la actividad | Repasar el contenido de los conceptos y generalidades de las técnicas de la criptografía y el cifrado de información 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\_didáctica\_1 |

**D. Material complementario**

| Tema | Referencia APA del Material | Tipo de material  (Video, capítulo de libro, artículo, otro) | Enlace del Recurso o  Archivo del documento o material |
| --- | --- | --- | --- |
| Encriptación simétrica y asimétrica | Profe Sang. (2021). *Encriptación (Cifrado) Simétrica y Asimétrica - Explicado Fácilmente* [Video]. YouTube. <https://www.youtube.com/watch?v=wDpqrasDmxM> | Video | <https://www.youtube.com/watch?v=wDpqrasDmxM> |

**E. Glosario**

| TÉRMINO | SIGNIFICADO |
| --- | --- |
| Activo | Componente o funcionalidad de un sistema, el cual puede ser atacado por parte de un ciberdelincuente, ya sea a nivel de *software* o de *hardware*. |
| Análisis de tráfico | Observación del comportamiento de los datos en una red por un canal de transmisión de información. |
| Antispam | Herramienta por la cual se infiere en las contramedidas en la contención de correos electrónicos. |
| Basura | Obtención de datos a base de la basura de las personas o empresas, los cuales pueden brindar información relevante para un posible ataque. |
| Ciberespionaje | Actividad que tienen los hackers en el mundo digital para poder obtener información y datos sensibles, los cuales pueden obtenerse de manera pasiva o activa. |
| Falso negativo | Son *bugs* o errores que se producen cuando un sistema puede diagnosticar como actividad normal un ataque de un ciberdelincuente |
| Reporte | Documento estructurado donde se organiza información relevante para dar a conocer los hallazgos durante un *pentesting.* |

**F. Referencias bibliográficas**

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

Borges, S. (2021). *Servidor web*. Infranetworking. <https://blog.infranetworking.com/servidor-web/>.

Castillo, J. (2018). *Active Directory Qué es y para qué sirve*. Profesional Review. <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*. Semantic Scholar.

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

Gaviria, R., Cárdenas, J. y Supelano, J. (2015). *Guía práctica para pruebas de pentest basada en la metodología OSSTMM V2.1 y la guía OWASP V3.0*. Universidad Libre Seccional Pereira. <https://repository.unilibre.edu.co/handle/10901/17296>

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

Jimenez, J. (2021). *Tipos de ataques de ingeniería social y cómo evitarlos*. Redes Zone. <https://www.redeszone.net/tutoriales/seguridad/tipos-ataques-ingenieria-social-consejos/>

LISA Institute. (2020). *Guía práctica contra la ingeniería social*. <https://www.lisainstitute.com/blogs/blog/guia-practica-ingenieria-social>

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

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

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

**G. 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 |
| Carolina Coca Salazar | Revisora Metodológica y Pedagógica | Regional Distrito Capital – Centro de Diseño y Metrología | Diciembre de 2021 |
| Rafael Neftalí Lizcano Reyes | Asesor pedagógico | Regional Santander - Centro Industrial del Diseño y la Manufactura | Noviembre de 2021 |
| Darío González | Corrección de estilo | Regional Distrito Capital – Centro de Diseño y Metrología | Febrero 2022 |

**H. Control de cambios**

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

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