SDA Ciberseguridad

2º Bachillerato ipepCórdoba Situación de Aprendizaje

TIYC II

Seguridad informática

Imagen generada con IA (Bing). Seguridad informática (CC BY-SA <http://creativecommons.org/licenses/?lang=es>)

En el vertiginoso mundo digital del siglo XXI, la seguridad informática se erige como un pilar fundamental para salvaguardar nuestra información en un entorno cada vez más interconectado. En esta era de avances tecnológicos acelerados, nuestra asignatura se presenta como el terreno fértil donde cultivar el entendimiento y las habilidades necesarias para enfrentar los desafíos inherentes a la ciberseguridad.

La seguridad informática se presenta como un viaje fascinante y esencial, donde explorarán los principios fundamentales que subyacen a la protección de datos y sistemas. Desde comprender las amenazas cibernéticas más comunes hasta analizar las estrategias de defensa, seréis guiados hacia un entendimiento significativo de la importancia de mantener la integridad, confidencialidad y disponibilidad de la información.

Este proceso de aprendizaje no solo potenciará la destreza técnica, sino también fomentará el pensamiento crítico y ético necesario para tomar decisiones informadas en un mundo digital en constante evolución. Al finalizar esta SdA, los estaréis mejor equipados para navegar en el ciberespacio con conciencia y confianza, contribuyendo así a la construcción de un entorno en línea más seguro y resiliente.

1. Seguridad informática

Imagen generada con IA (Bing). Ciberladrón (CC BY-SA <http://creativecommons.org/licenses/?lang=es>)

Hoy en día es difícil concebir una empresa que no posea ordenadores y una conexión a Internet. Y no solo empresas, sino también a nivel particular como herramienta de ocio o trabajo. Las empresas basan gran parte de su actividad en datos almacenados en equipos informáticos o en datos e información que viaja por la red.

Por un lado será importante garantizar que la información almacenada no se pierda, se degrade o se altere de forma incorrecta (seguridad) y por otro, el garantizar que datos de carácter personal o privados por la actividad de la empresa sean accesibles por personas no autorizadas (privacidad).

Ofrecer protección frente a estos dos tipos de vulnerabilidad es de suma importancia, tanto para la actividad y funcionamiento de organismos y empresas como para individuos particulares.

¿Qué sientes cuándo se te estropea el disco duro de tu equipo y pierdes todas tus fotos de los últimos 5 años?, ¿y si alguien suplanta tu identidad y accede a tus datos bancarios? , ¿y si tu empresa rival accede a tus datos con los diseños de los últimos prototipos que aún no habéis lanzado?.

Alerta con los delitos

El acceso a datos privados y la suplantación de identidad son delitos penados por la ley.

Todo este tipo de delitos que se realizan contra sistemas informáticos o a través de ellos , se conocen como cibercrimen y existe una unidad de la Guardia Civil encargada de su investigación.

Grupo de Delitos Telemáticos (G.D.T) <https://www.gdt.guardiacivil.es/webgdt/pinformar.php> : si tienes curiosidad en esta página se describe su actividad, así como algunas normas básicas de seguridad y se proporcionan una serie de formularios para denunciar o informar de posibles delitos telemáticos.

¿Qué es el hacking?

Seguro que habrás escuchado la palabra "hackear" en multitud de ocasiones. Pues básicamente consiste en acceder sin autorización a un sistema informático con el fin de obtener información confidencial.

Imagen generada con IA (Bing). Hacker (CC BY-SA <http://creativecommons.org/licenses/?lang=es>)

Como habrás deducido, estamos hablando de un hecho que constituye un delito, por lo que las consecuencias derivadas del hacking pueden ser muy graves. Por lo que, en primer lugar, te recomendamos que te abstengas de hacer pruebas absurdas, y no caigas en el "lado oscuro de la fuerza".

Pero te preguntarás..."si yo quiero convertirme en un experto en seguridad, ¿cómo lo puedo hacer?"

No te preocupes, iremos poco a poco.

Siempre es mejor empezar por el principio (como dijo un maestro Zen), asentar las bases y practicar en entornos de pruebas controlados.

Reflexiona sobre las siguientes cuestiones:

¿Que es hackear?

A continuación te invitamos que veas el siguiente video sobre hacking:

Se ha producido un error.

Prueba a ver el vídeo en www.youtube.com o habilita JavaScript si está desactivado en tu navegador.

En los años 60, ¿a quién se designaba con el término hacker?

Eran los programadores más avanzados que trabajan en el MIT (Massachusetts Institute of Technology) <https://www.mit.edu/>

Año 1975. ¿Qué significado tenía el término hacker?

En el manifiesto conocido como "Jargon File" <https://es.wikipedia.org/wiki/Jargon_File> se define como "una persona que disfruta explorando los detalles de sistemas programables y como aumentar sus capacidades al máximo, a diferencia de la mayoría de los usuarios, que prefieren aprender lo mínimo indispensable.

¿En qué año el término hacker se convirtió en sinónimo de cibercriminal?

En el año 1980. En ese momento apareció el término cracker, ya que la comunidad hacker se esforzó en diferenciar a los hackers buenos de los malos.

Es decir a partir de ese momento, lo correcto es referirse a los delincuentes informaticos como cracker y a los expertos en informática que exploran los límites de los sistemas informáticos, que buscan vulnerabilidades en los sistemas, pero sin aprovecharse ilicitamente como hacker.

¿Qué famosos se vieron implicados en el caso de los Papeles de Panamá?

Los Papeles de Panamá <https://es.wikipedia.org/wiki/Papeles_de_Panam%C3%A1> fueron un sonado caso de hackeo donde se publicó información de personas que presuntamente habían cometido delitos de evasión de impuestos en personajes públicos de todo el mundo

1. Jackie Chan, actor.
2. Bachar al Asad, presidente de Siria.
3. Diego Forlán, futbolista.
4. Àlex Crivillé, piloto español de motociclismo.
5. Lionel Messi, futbolista del F. C. Barcelona y de la selección nacional de Argentina.
6. José Luis Núñez, presidente del F. C. Barcelona.
7. Club de fútbol Real Sociedad.
8. Emma Watson, actriz, modelo y activista británica.

Así un total de hasta 200.000 nombres.

Ciberseguridad

La ciberseguridad se entiende como el conjunto de técnicas que se aplican para defender a las redes, dispositivos (equipos, servidores, móviles, etc.) así como a los datos de posibles ataques maliciosos.

Es importante entender la envergadura de dichas técnicas, ya que abarcan muchos aspectos. Ten en cuenta que la resistencia y fortaleza de una cadena es la del eslabón más débil. (Enlace a blog INCIBE

<https://www.incibe.es/ciudadania/blog/sabias-que-el-95-de-las-incidencias-en-ciberseguridad-se-deben-errores>)

En el siguiente video profundizamos más en esta cuestión:

Se ha producido un error.

Prueba a ver el vídeo en www.youtube.com o habilita JavaScript si está desactivado en tu navegador.

Actividad 1. Noticia sobre ciberseguridad

Busca en Internet alguna noticia relacionada con ciberseguridad en la que se haya comprometido la información de una organización / empresa / organismo público en el último año. No serán validas las noticias con más de un año de antigüedad. Ha un comentario crítico de 100 palabras sobre dicha noticia.

¿Necesitas ayuda?

Haz uso de la herramienta de filtro de Google y prueba a buscar ataques en organizaciones públicas concretas, como ayuntamientos.

Entrega de la tarea

Ve a la plataforma Moodle y entrega la actividad "Actividad 1. Noticia sobre ciberseguridad", además debes pegar el enlace a la noticia en el foro de Dudas y consultas de nuestro curso.

Objetivos de la Seguridad Informática

Imagen generada con IA (Bing). Seguridad informática (CC BY-SA <http://creativecommons.org/licenses/?lang=es>)

Según el estándar para la seguridad de la información ISO/IEC 27001, que fue aprobado y publicado en octubre de 2005 por la International Organization for Standardization (ISO) y por la comisión International Electrotechnical Commission (IEC):

“La seguridad informática consiste en la implantación de un conjunto de medidas técnicas destinadas a preservar la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como

la autenticidad, la autorización, la auditoría y el no repudio."

Tenemos que definir estos terminos:

- La confidencialidad de la información: que nadie no autorizado pueda verla.
- La integridad de la información: que nadie no autorizado pueda modificarla y alterarla.
- La disponibilidad de la información: que quien esté autorizado pueda acceder a ella siempre y consultarla.
- Autenticidad: permite validar la identidad del emisor. Verificando que es quien dice ser. El método más conocido es el de controlar el acceso mediante usuario y contraseña. Existen otros métodos más seguros como el certificado digital, tarjetas magnéticas, huella dactilar, reconocimiento facial, etc..
- Autorización: controla el acceso de los usuarios a información, equipos o procesos restringidos, tras pasar un proceso de autenticación. Deberemos definir sobre qué puede actuar, cuándo puede actuar y cómo puede hacerlo (p.ej. acceso a ficheros en modo de solo lectura o lectura/escritura, acceso a bases de datos con permisos de inserción, borrado o modificación, etc.) Siempre será más recomendable dar autorizaciones más restringidas y abrirlas cuando sea necesario, que dar autorizaciones muy abiertas que pueden comprometer la seguridad del sistema en caso de accesos con permisos inadecuados, bien intencionadamente o bien por error.
- Auditoría: debemos llevar un control sobre los sistemas y servicios que nos permita determinar qué acciones se han llevado a cabo y quién y cuándo las ha llevado a cabo. Periódicamente se revisará está información para analizarla y sacar conclusiones que permitan detectar posibles fallos de seguridad o mejorar los procedimientos.
- No repudio: mecanismo para asegurar que nadie pueda decir que él no fue. El emisor no podrá negar que fue él quien envió el mensaje, puesto que el receptor tendrá pruebas de ello o el receptor no podrá negar que recibió el mensaje porque el receptor tendrá información que lo confirma.

Sopa de letras sobre seguridad

2

Hallar las palabras ocultas relacionadas con la seguridad informática.

%E9%B0%E6%EB%E2%F7%D5%F3%FF%F7%B0%A8%B0%C1%FD%E2%F3%B0%BE%B0%FB%FC%E1%E6%E0%E7
0123456
Su navegador no es compatible con esta herramienta.

2. Seguridad activa y pasiva

Imagen generada con IA (Bing). Coches (CC BY-SA <http://creativecommons.org/licenses/?lang=es>)

En un vehículo nos encontramos con dos tipos de seguridad:

- La seguridad activa, que es la que trata de evitar que se produzca un accidente, como pude ser el sistema de frenado o la adherencia de los neumáticos.
- Y la seguridad pasiva, que trata de minimizar los daños una vez que el accidente ya se ha producido o es inevitable, como pueden ser los cinturones de seguridad o airbags.

En seguridad informática nos encontramos con algo parecido. Por un lado la seguridad activa, que tratará de prevenir y evitar que ocurran daños en los sistemas informáticos, y por otro lado, la seguridad pasiva que tratará de minimizar los efectos causados por un accidente, un error o un ataque.

Conoce más sobre la seguridad activa

Algunas de las técnicas de seguridad activa son:

- Contraseñas seguras: Previene el acceso a recursos a personas no autorizadas
- Encriptación: Los datos a proteger se cifran usando una clave de cifrado, de forma que las personas que no conozcan la clave no puedan interpretar esos datos.
- Software específico: (antivirus, antiespías, cortafuegos, etc.): Previenen frente a los virus informáticos y entradas indeseadas al sistema.
- Firma digital y certificado digital: Permiten verificar el origen de los datos, su integridad y su autenticidad

Conoce más sobre la seguridad pasiva

Entre las técnicas de seguridad pasiva tenemos:

- Instalaciones adecuadas (conexiones eléctricas, refrigeración del sistema, etc.): Reaccionan ante problemas eléctricos como subidas de tensión, derivación a tierra, humedades en los sistemas, etc...
- SAI (Sistema de Alimentación Ininterrumpida): Estos dispositivos proporcionan energía eléctrica almacenada en sus baterías durante un tiempo limitado ante un apagón. Otras de sus posibles funcionalidades es la de mejorar la calidad de la energía eléctrica, filtrando frente a subidas y bajadas de tensión.
- Conjunto de discos redundantes (RAID, Redundant Array of Independent Disks): Nos permiten restaurar información que no es válida o consistente a partir de la repetición de los datos en distintos grupos de discos.
- Copias de seguridad: Copias de los datos en distintos soportes físicos y en distintas ubicaciones físicas.

Juega con la seguridad activa y pasiva

3. Seguridad física y lógica

Imagen generada con IA (Bing). Hardware y Software (CC BY-SA <http://creativecommons.org/licenses/?lang=es>)

Se pueden clasificar los mecanismos de seguridad atendiendo a si protegen el hardware <https://es.wikipedia.org/wiki/Hardware> o el software <https://es.wikipedia.org/wiki/Hardware> .
Aquellos mecanismos que protegen el hardware o medio físico en que se ubica el sistema frente a amenazas que pueden ser causadas por el hombre o por la naturaleza, se conocen como seguridad física.
Los mecanismos que protegen el software, es decir, aplicaciones y datos frente a posibles amenazas serán los que implementen la seguridad lógica.

Seguridad física

La seguridad física, como ya hemos dicho es la que trata de proteger el hardware frente a posibles amenazas. En la siguiente tabla se recogen algunas de estas amenazas y los mecanismos de protección que podemos usar:

- Incendios:
  - Mobiliario ignífugo en CPD (centro de procesos de datos).
  - Mecanismos antiincendios (detectores, extintores, etc..)
  - No estar cerca de material inflamable
- Inundaciones:
  - No ubicar los servidores en salas subterráneas con riesgo de inundación.
  - Sistemas de evacuación de agua.
  - Impermeabilización y sellado de posibles vías de entrada de agua
- Robos:
  - Vigilante
  - Cámaras de seguridad
  - Sistemas de control de acceso
- Sobrecargas y apagones:
  - SAI (Sistemas de alimentación ininterrumpida).
- Caídas en la línea:
  - Línea de backup.
- Otros desastres naturales (terremotos, maremotos, etc..)
  - Consultar datos meteorológicos.
  - En áreas con alta probabilidad de movimientos sísmicos, edificaciones preparadas para ello.

Seguridad lógica

La seguridad lógica trata de proteger las aplicaciones o programas y los archivos y datos frente a distintas amenazas, mediante distintas medidas de seguridad. En la siguiente tabla puedes ver algunas de estás amenazas y los mecanismos de protección con los que se intenta eliminar o minimizar dicha amenaza:

- Modificaciones no autorizadas:
  - Restringir el acceso a programas y archivos mediante contraseñas.
  - Limitar permisos de forma que los usuarios no puedan modificar por error o intencionadamente programas ni archivos.
  - Listas de control de acceso.
  - Cifrado de la información.
- Ataques desde la red (Internet o red local):
  - Firewalls.

    - Servidores Proxys.
    - Sistemas de monitorización de la red.
    - Listas de control de acceso (por IP p por MAC).
- Pérdidas de información:
    - Copias de seguridad.
    - Sistemas tolerantes a fallos.
    - Discos redundantes.
- Virus:
    - Programas antivirus que eviten que estos programas malintencionados se instalen en los equipos.
- Suplantación de identidad:
    - Contraseñas
    - Sistemas de reconocimiento (voz, digitales, faciales, etc.)
    - Certificados

¿Eres capaz de encontrar la solución a una amenaza?

—

Malware

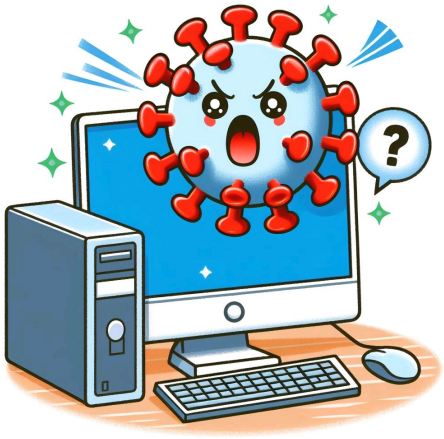


Imagen generada con IA (Bing). Malware (CC BY-SA <http://creativecommons.org/licenses/?lang=es>)

Las amenazas lógicas también se las conoce con la palabra malware proviene de las palabras (en inglés) MALicious softWARE, que se traduce como software malicioso.

Cuando hablamos de malware, no nos referimos a ningún software defectuoso (un bug en una aplicación no es algo que se haga con intencionalidad ni buscando fines dañinos).

Malware engloba todo aquel software creado para infiltrarse en un equipo informático con la finalidad de modificar su funcionamiento o la información que almacena, modificándola, eliminándola o reenviándola a terceros sin el consentimiento de su propietario.

Los efectos de este tipo de software son muy diversos, y pueden ir desde una simple molestia para el usuario a ser muy perjudiciales y dañinos.

Virus, gusanos, troyanos, spyware, adware y otros, no son más que distintos tipos de software malicioso que iremos conociendo a lo largo de este tema.

A continuación puedes conocer más sobre distintos tipos de malware

Virus

Un virus es un programa o fragmento de código que se carga en un equipo sin consentimiento ni conocimiento del propietario. Algunos son solo molestos, pero otros pueden llegar a ser muy dañinos, destruyendo información o tomando el control del sistema. Sus efectos pueden ir desde rotar la pantalla hasta controlar totalmente el equipo infectado. Este código malicioso puede venir en archivos ejecutables descargados de sitios poco fiables o en algún archivo adjunto a un correo. Cuando ejecutemos el programa infectado, el virus se instalará en la memoria RAM. Es importante tener en cuenta que para que el virus comience a funcionar y a extenderse, debe haber alguien que ejecute ese código. Una vez en la RAM, el virus infectará otros archivos ejecutables y los grabará en disco. Aún después de apagar el ordenador, cuando algunos de estos programas se ejecuten, se repetirá la acción.

¿Quiere conocer más sobre uno de los primeros virus de la historia? Se llamaba Jerusalen o Viernes 13 <https://es.wikipedia.org/wiki/Jerusalem_(virus_inform%C3%A1tico)>

Gusanos

Los gusanos o worms se diferencian de los virus en su forma de propagarse. Este malware no necesita de la ejecución del programa infectado para su propagación, pues puede autopropagarse sin necesidad de ninguna acción por parte del usuario.

Sus efectos también suelen ser distintos a los de los virus, mientras que los virus pretenden alterar o destruir archivos los gusanos van encaminados a consumir recursos causando generalmente problemas de saturación en la red.

Los gusanos aprovechan vulnerabilidades de Sistemas Operativos y aplicaciones para autopropagarse de un equipo a otro.

Un gusano es considerada una de las primeras armas cibernéticas de la historia, se llama Stuxnet <https://cronicaseguridad.com/2022/09/05/stuxnet-primera-ciberarma-historia/>

Troyano

Los troyanos, toman su nombre del famoso caballo de Troya:

El caballo de Troya fue un artilugio con forma de enorme caballo de madera que se menciona en la historia de la guerra de Troya y que según este relato fue usado por los griegos como una estrategia para introducirse en la ciudad fortificada de Troya.

Al igual que hicieron los griegos para entrar en la ciudad de Troya ocultos en el caballo de madera, los troyanos son un tipo de malware que se introduce en el equipo camuflado en un programa aparentemente inofensivo.

De hecho al ejecutar el programa en cuestión, este parecerá funcionar correctamente, sin embargo en segundo plano, y sin que nos percatemos de ello, se instalará el troyano, cuya misión no es la de infectar ficheros como los virus para propagarse, ni hacerlo de forma autónoma como los gusanos, sino la de realizar distintas acciones y configuraciones con el fin de facilitar el control externo de nuestro equipo sin nuestra autorización.

El troyano tendrá dos partes, un cliente que es el que se instala en el equipo atacante y un servidor que es el instalado en el equipo atacado, que será el que reciba las ordenes del cliente y realice las operaciones oportunas en el equipo en el que se aloja.

En wikipedia <https://es.wikipedia.org/wiki/Troyano_(inform%C3%A1tica)#Troyanos_m%C3%A1s_famosos> han recopilado varios troyanos famosos de la historia

Ransomware

Su nombre proviene de ransom (rescate) y software.

Este malware "secuestra" archivos y pide un rescate por liberarlos.

Lo que hace es encriptar archivos (también de le conoce como criptovirus) y no facilita la clave para su desencriptación hasta que se paga una determinada cantidad de dinero.

Recomendaciones

Para evitar pérdidas asociadas a este tipo de ataque se recomienda:

- Tener instaladas herramientas de detección de malware, si la amenaza se detecta de forma temprana es posible eliminarla antes de que actúe sobre archivos (encriptándolos) o bloquee el acceso a partes del sistema.
- Tener copias de seguridad de los ficheros importantes en algún tipo de almacenamiento externo.

Protegete

Después de conocer algunas de las múltiples amenazas que nos encontramos en la red, podríamos pensar que estamos totalmente desprotegidos, pero no es así, existen multitud de herramientas, que junto con algunas de las buenas prácticas que hemos ido viendo, protegerán a nuestro equipo. Aunque, desgraciadamente, ninguna herramienta protege al 100%, puesto que los desarrolladores de malware están constantemente evolucionando.

Algunas de estas herramientas antimalware son:

- Antivirus: que nos permitirán detectar, eliminar y prevenir virus informáticos. Es importante que la base de datos de virus que usa se actualice frecuentemente.
- Antspyware: eliminan y previenen frente a software espía.
- Antirootkit: estas herramientas van dirigidas a localizar rootkits, que como ya vimos es un tipo de malware que un antivirus no detectaría.
- Filtros antispam: analizan los correos de la bandeja de entrada para localizar publicidad no deseada y correos masivos o sospechosos, que mueven a otra carpeta para su posterior chequeo y borrado por parte del usuario.
- Antiphising: van más allá de los filtros antispam, analizan los correos para detectar links fraudulentos o dominios falsos.
- Filtros de contenido: permiten o deniegan el acceso a páginas en función de su contenido, según reglas previamente establecidas.
- Control parental: con el fin de proteger al menor, es posible instalar filtros que permitan o denieguen el acceso a determinadas páginas o utilidades, según la url, según contenido, etc. Que bloqueen el acceso a redes sociales o registren su actividad o que limiten el tiempo y horarios de uso.

Imagen generada con IA (Bing). Ordenador protegido (CC BY-SA <http://creativecommons.org/licenses/?lang=es>)

- Firewall: O cortafuegos, nos permite limitar el acceso desde internet a una parte de la red o a nuestro equipo, estableciendo ciertas reglas de filtrado, por paquetes o aplicaciones.
- Suites de seguridad: agrupan todas o varias de las herramientas anteriores con el fin de proteger al equipo.
- Actualizaciones de los navegadores y sistema operativo: es recomendable tener siempre actualizados tanto el S.O. como los navegadores que usemos, pues muchas veces estas actualizaciones resuelven problemas detectados en la seguridad del software.
- Copias de seguridad: copias de los ficheros y datos más importantes en algún soporte externo, de forma que permanezcan intactos tras cualquier ataque a la máquina original que provoque la destrucción, encriptación o modificación no deseada de estos.

Otras precauciones:

- Desconfiar siempre de correos desconocidos.
- No hacer click en URL sospechosas que se nos adjunten en mensajes o correos. Por ejemplo si tu banco es bbva su dominio es https://bbva.es <https://bbva.es/> es muy común encontrar enlaces del tipo https://bbva.es.xyz/accesoCliente o similar que cualquier persona puede confundir, por eso es tan importante no acceder desde enlaces que te envié tu banco, mejor acceder directamente desde su app o su web, o revisarlos muy bien antes de pulsar en ellos.
- No abrir ficheros ejecutables que nos lleguen por correo.
- Jamás dar nuestros datos personales a ninguna "supuesta" entidad. La entidad real (banco, policia, etc.) jamás nos pedirá nuestros datos y menos por esas vías.
- Al entrar en páginas de compras, bancos, etc. verificar que la conexión es segura (https://...) los accesos no seguros (http://) fijaos que falta la s, pueden estar puenteados y nuestra información y credenciales circular por el equipo de un atacante que guardará todas nuestras credenciales.
- No descargar software de páginas no confiables.
- Si vas a instalar un software descargado, lee atentamente todas las pantallas (evita hacer click en siguiente, siguiente). En este tipo de instalaciones suele venir marcada por defecto (hay que desmarcar o elegir instalación personalizada en lugar de típica) la instalación de software adicional, generalmente con fines publicitarios.

---

4. Seguridad de contraseñas

Imagen generada con IA (Bing). Contraseñas (CC BY-SA <http://creativecommons.org/licenses/?lang=es>)

Es fundamental el controlar que cualquier persona que acceda al sistema esté autorizado y que solo pueda acceder a los recursos para los que tiene autorización.

Una de las formas más usuales de autorizar los accesos es mediante un usuario y contraseña (o password) y asociando a dicho usuario una serie de permisos (qué acciones podrá realizar y cuáles no y sobre qué recursos).

Recomendaciones para elegir Contraseña

No es recomendable elegir contraseñas que por ser fáciles de recordar, sean también fáciles de averiguar, no se recomienda nuestra fecha de nacimiento, NIF, nombre, nombre de nuestra mascota, nombre de algún familiar, etc.

Existen además ataques por diccionario o fuerza bruta que que se dificultan si se siguen algunas normas como longitud mínima o caracteres especiales.

Algunas normas básicas a la hora de elegir nuestra contraseña son:

- No elegir palabras relacionadas con nuestro entorno (NIF, nombre de nuestra mascota, fecha de nacimiento, nombre de tu hijo, etc.)
- Usar combinaciones de letras, mayúsculas, minúsculas, números y caracteres especiales (no usar palabras con significado).
- Longitud mínima de 8 caracteres.
- Intentar usar contraseñas distintas para servicios distintos.
- No usar nunca la contraseña por defecto, cambiarla en el primer acceso.

Para recordar una contraseña segura (mínimo 8 caracteres que incluyan números, letras y caracteres especiales) podemos recurrir al truco de usar una frase, por ejemplo: ¿Yo nací en febrero de 1980?, y quedarnos con los dos últimos caracteres de cada palabra: Yocíenrode80?

Obviamente, ninguna de estas precauciones será de utilidad si después anotamos la contraseña en un postit y la pegamos en la pantalla de nuestro ordenador. Las contraseñas deben almacenarse de forma segura (existen programas gestores de contraseñas) y tener cuidado en su distribución, cómo y a quién se facilita, como norma general una contraseña es de uso privado, por lo que no se debe facilitar a nadie. En caso necesario, debemos ser cuidadosos con el medio que usamos y si es necesario cifrar la información , de forma que solo la persona que posea la clave de cifrado pueda recuperar esa contraseña.

Soy administrador de un sistema, ¿Que puedo hacer?

A la hora de configurar nuestros sistemas debemos forzar a los usuarios a tomar ciertas medidas de seguridad con respecto a sus contraseñas:

- Obligar al usuario a cambiar la contraseña inicial en su primer acceso.
- Numero máximo de intentos permitidos, tras el cual el sistema se bloquea.
- Que no se admitan contraseñas de menos de 8 caracteres y que estos obligatoriamente incluyan mayúsculas, minúsculas, números y caracteres especiales.
- Que las contraseñas expiren cada cierto tiempo y haya que cambiarlas, tampoco se permitirá repetir ninguna de las tres últimas.

Tipos de ataques

Existen diversos sistemas para averiguar contraseñas. Algunos de los más conocidos son:

- Sniffers: programas que interceptan las comunicaciones de los equipos en una red pudiendo extraer contraseñas de las comunicaciones "escuchadas".
- Keyloggers: Programas que capturan las teclas pulsadas.
- Fuerza bruta: Programas que prueban todas las combinaciones (cuanto más larga sea la contraseña, más tiempo requieren).
- Ataque por diccionario: Programas que usan palabras del idioma del usuario.
- Suplantación de identidad: Se trata de engañar al usuario haciéndole creer que es su banco, o alguien conocido, o algún organismo público, para que se le faciliten las claves.

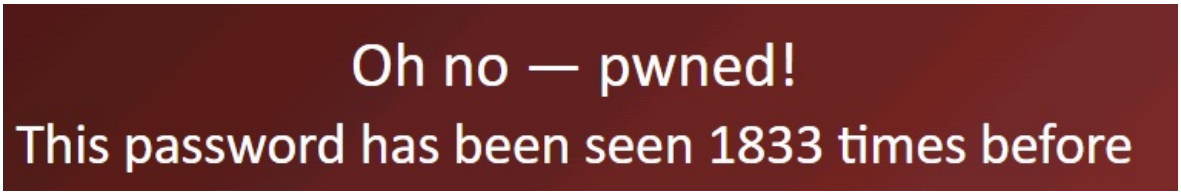
Actividad 2.1 Navegamos seguros

Mi contraseña no la sabe nadie. ¿Seguro?

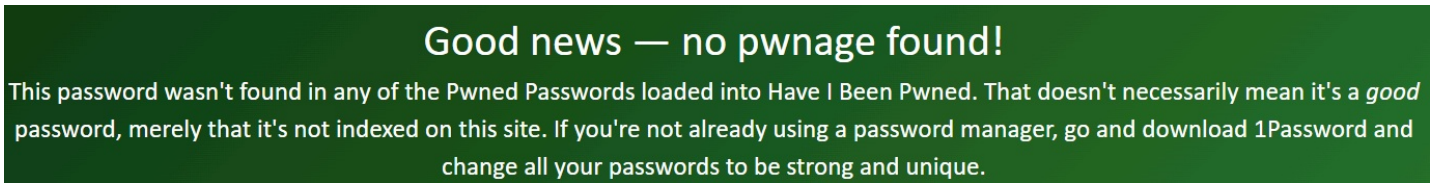
La percepción de seguridad falsa en torno a las contraseñas es una ilusión peligrosa. A menudo, las personas optan por combinaciones predecibles o reutilizan contraseñas, creyendo que están a salvo. Sin embargo, este sentido de seguridad es engañoso, ya que las tácticas de hacking evolucionan constantemente. Contraseñas débiles o comunes son vulnerabilidades evidentes. La realidad es que la seguridad reside en la complejidad y la singularidad de las contraseñas. Ignorar esta realidad crea una falsa sensación de protección, exponiendo a los individuos a riesgos innecesarios de violación de datos y comprometiendo la integridad de la información personal.

Decenas de empresas son comprometidas cada año, algunas de ellas empresas muy grandes con millones de datos de sus usuarios, puede que entre esos datos filtrados este ¿nuestra contraseña?, ¿Cómo saberlo? Tenemos una web que nos lo va a decir. Introduce tus contraseñas en esta página https://haveibeenpwned.com/Passwords <https://haveibeenpwned.com/Passwords>

Si nuestra contraseña ha sido filtrada en alguna ocasión nos aparecerá el siguiente mensaje indicando que esta comprometida, y la cantidad de veces que ha sido filtrada, en este ejemplo escribí como contraseña "contraseña":



Si nuestra contraseña no ha sido filtrada nunca, nos aparecerá el siguiente mensaje.



Introduce tus contraseñas en esta página y haz una captura de pantalla con el resultado de alguna de ellas. Ahora guarda esta captura en un documento de texto, te servirá más adelante.

---

5. Seguridad en las redes

Spam

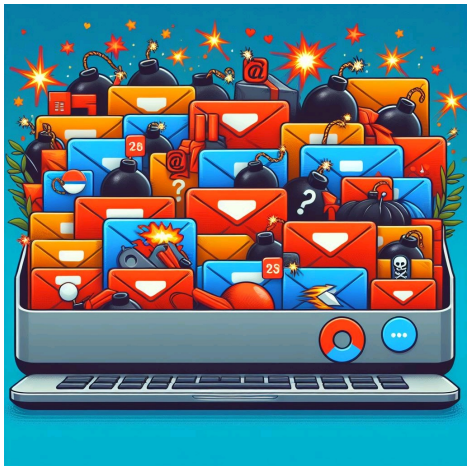


Imagen generada con IA (Bing). Spam (CC BY-SA <http://creativecommons.org/licenses/?lang=es>)

El spam, correo electrónico no solicitado, en apariencia inofensivo plantea graves amenazas a la seguridad informática. Al inundar bandejas de entrada con mensajes engañosos, los ciberdelincuentes buscan robar datos confidenciales o distribuir malware. Estos correos fraudulentos pueden contener enlaces maliciosos, comprometiendo la integridad de sistemas y redes. La ingeniería social utilizada en spam puede engañar a usuarios para revelar información personal, facilitando el robo de identidad. Además, la propagación de spam a menudo se vincula con campañas de phishing, llevando a ataques más sofisticados. La lucha contra el spam se convierte así en una necesidad crucial para salvaguardar la ciberseguridad.

¿De donde viene esa palabra?

El término spam tiene su origen en una comida enlatada. Los Monty Python hicieron una parodia llamada "Spam" en 1970, el término "Spam" en la pieza de teatro, prácticamente todos los platillos contenían Spam. La repetición del término en la canción "Lovely Spam, Wonderful Spam" llevó a que, en la década de 1990, "Spam" se adoptara para referirse a mensajes electrónicos no solicitados, especialmente correos electrónicos no deseados. La asociación con la canción resalta cómo la repetición de la palabra "spam" ahoga cualquier otra comunicación, inspirando su uso en el contexto de la mensajería no deseada.

Cypher789 <https://de.wikipedia.org/wiki/User:Cypher789> . Lata de SPAM <https://en.wikipedia.org/wiki/Spam_(food)#/media/File:Spam_2.jpg> (CC BY-SA <http://creativecommons.org/licenses/?lang=es>)

Se ha producido un error.

Prueba a ver el vídeo en www.youtube.com o habilita JavaScript si está desactivado en tu navegador.

Weidmoo <https://www.youtube.com/@Weidmoo> . Monty Python - Spam

<https://www.youtube.com/watch?v=ycKNt0MhTkk> (Licencia estándar de YouTube <https://www.youtube.com/static?template=terms>)

...

Pishing

Imagen generada con IA (Bing). Pishing (CC BY-SA <http://creativecommons.org/licenses/?lang=es>)

Toma su nombre del inglés phising (pesca), pues se trata de técnicas para conseguir que la víctima "muerda el anzuelo".

Podría llegarnos un correo o mensaje al móvil de nuestro banco informándonos de que se han detectado problemas de seguridad, o de que necesitan verificar nuestros datos o número de cuenta o tarjeta por mantenimiento de la base de datos de clientes, o cualquier otro motivo, y para ello se nos facilita un enlace. Al hacer click en este enlace nos aparecerá una página, falsa, con el mismo aspecto que la de nuestro banco real. Es complicado darse cuenta de que no es la página verdadera puesto que la interfaz es la misma, tan solo si observamos la url o dirección de la página veremos que aunque muy similar, no es exactamente la de nuestro banco. Pero si no nos percatamos de esto al introducir nuestros datos, el atacante los tendrá en su poder y habremos caído en el engaño.

Puesto que la página es falsa, una vez tengan los datos que buscaban, nos saltará alguna página informándonos de algún error en el servidor o en la conexión, para evitar levantar sospechas.

Recomendaciones

- Sospechar siempre de correos o mensajes en que se nos soliciten datos. Las entidades implicadas deberían tenerlos y en caso de necesitar alguna verificación no sería por este medio.
- Nunca pulsar en un enlace que se nos facilite en correos o mensajes, hacerlo siempre desde la web oficial.
- Verificar la URL antes de introducir datos.
- Sospechar de URL con el carácter @ pues lo que hace es dirigirnos de una página a otra.
- Verificar que la conexión es segura (precedida de https).
- Sospechar de mensajes cuyo remitente no provenga del correo oficial de la entidad.
- Utilizar filtros antispam en el correo.

Pishing real

El siguiente es un pishing real recibido en mi correo electrónico. Se han borrado algunos datos para no exponer las direcciones originales, que son direcciones reales gubernamentales que han sido usadas en el pishing sin permiso.

Este es el cuerpo y el asunto del email, que recibí en mi cuenta de email personal en la carpeta general, no fue marcado como Spam:

De: **Leonardo** [redacted] **Gonzales** <[redacted]@tschool.edu.pe>
Date: vie., 2 feb. 2024 7:31
Subject: Convocatoria: Respuesta inmediata
To:

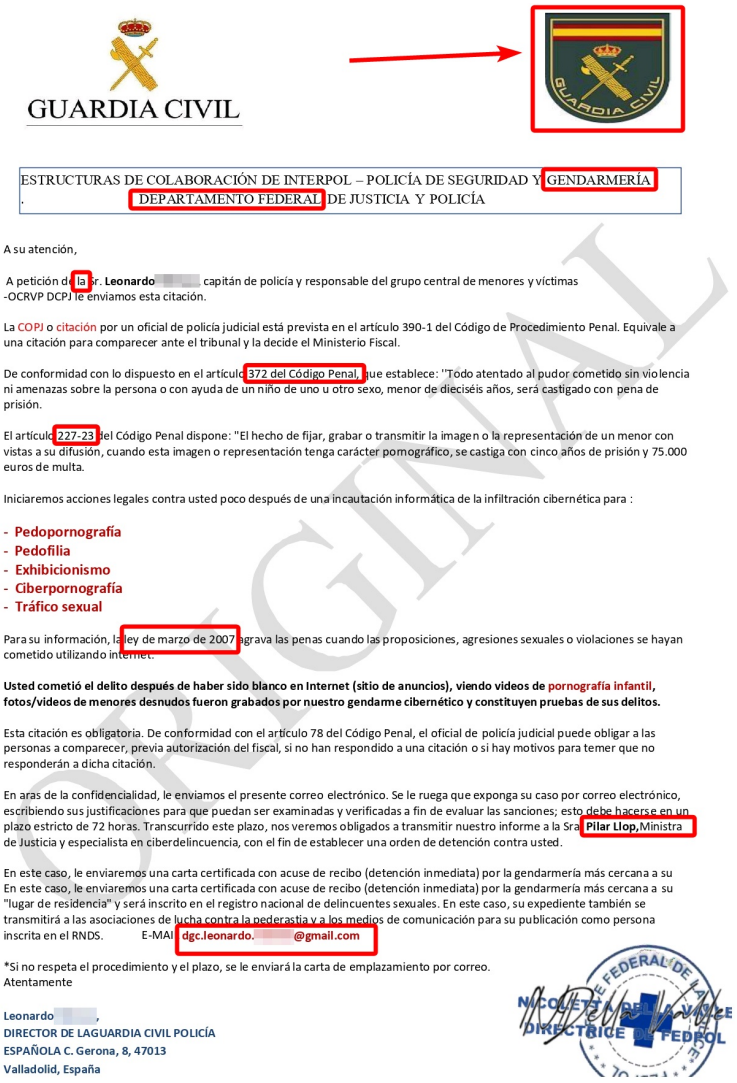
Tome nota de esta invitación y responda a la dirección de correo electrónico indicada en la invitación adjunta.

Atentamente

Imagen de elaboración propia. Pishing real (CC BY-SA <http://creativecommons.org/licenses/?lang=es>)

Fijaos que la dirección es una dirección real del gobierno de perú, por lo que en teoría el archivo pdf que me adjuntaban tenía que ver con ese país. Primera situación extraña, ya que yo no tengo ninguna relación con Perú, pero bueno podía ser alguna invitación a una colaboración en materia educativa...

Al abrir el pdf cuyo nombre de archivo es "CONVOC...TORIA.pdf" otro elemento con el que desconfiar me encuentro con lo siguiente:



GUARDIA CIVIL

ESTRUCTURAS DE COLABORACIÓN DE INTERPOL – POLICÍA DE SEGURIDAD Y GENDARMERÍA
DEPARTAMENTO FEDERAL DE JUSTICIA Y POLICÍA

A su atención,

A petición de la Sr. **Leonardo** capitán de policía y responsable del grupo central de menores y víctimas -OCRVP DCPJ le enviamos esta citación.

La COPJ o citación por un oficial de policía judicial está prevista en el artículo 390-1 del Código de Procedimiento Penal. Equivale a una citación para comparecer ante el tribunal y la decide el Ministerio Fiscal.

De conformidad con lo dispuesto en el artículo 372 del Código Penal, que establece: "Todo atentado al pudor cometido sin violencia ni amenazas sobre la persona o con ayuda de un niño de uno u otro sexo, menor de dieciséis años, será castigado con pena de prisión.

El artículo 227-23 del Código Penal dispone: "El hecho de fijar, grabar o transmitir la imagen o la representación de un menor con vistas a su difusión, cuando esta imagen o representación tenga carácter pornográfico, se castiga con cinco años de prisión y 75.000 euros de multa.

Iniciaremos acciones legales contra usted poco después de una incautación informática de la infiltración cibernética para :

- **Pedopornografía**
- **Pedofilia**
- **Exhibicionismo**
- **Ciberpornografía**
- **Tráfico sexual**

Para su información, la ley de marzo de 2007 agrava las penas cuando las proposiciones, agresiones sexuales o violaciones se hayan cometido utilizando internet.

Usted cometió el delito después de haber sido blanco en Internet (sitio de anuncios), viendo videos de pornografía infantil, fotos/videos de menores desnudos fueron grabados por nuestro gendarme cibernético y constituyen pruebas de sus delitos.

Esta citación es obligatoria. De conformidad con el artículo 78 del Código Penal, el oficial de policía judicial puede obligar a las personas a comparecer, previa autorización del fiscal, si no han respondido a una citación o si hay motivos para temer que no responderán a dicha citación.

En aras de la confidencialidad, le enviamos el presente correo electrónico. Se le ruega que exponga su caso por correo electrónico, escribiendo sus justificaciones para que puedan ser examinadas y verificadas a fin de evaluar las sanciones; esto debe hacerse en un plazo estricto de 72 horas. Transcurrido este plazo, nos veremos obligados a transmitir nuestro informe a la Sra **Pilar Llop,** Ministra de Justicia y especialista en ciberdelincuencia, con el fin de establecer una orden de detención contra usted.

En este caso, le enviaremos una carta certificada con acuse de recibo (detención inmediata) por la gendarmería más cercana a su
En este caso, le enviaremos una carta certificada con acuse de recibo (detención inmediata) por la gendarmería más cercana a su
"lugar de residencia" y será inscrito en el registro nacional de delincuentes sexuales. En este caso, su expediente también se transmitirá a las asociaciones de lucha contra la pederastia y a los medios de comunicación para su publicación como persona inscrita en el RNDS. E-MAIL: **dgc.leonardo.@gmail.com**

*Si no respeta el procedimiento y el plazo, se le enviará la carta de emplazamiento por correo.
Atentamente

Leonardo
DIRECTOR DE LAGUARDIA CIVIL POLICÍA
ESPAÑOLA C. Gerona, 8, 47013
Valladolid, España

Imagen de elaboración propia. Pishing (CC BY-SA <http://creativecommons.org/licenses/?lang=es>)

Elementos que nos tienen que poner alerta:

1. El primero y más importante, recordad que el email venia de un organismo de Perú, y me encuentro con una carta de la Guardia Civil.
2. El logo de la Guardia Civil esta claramente estirado
3. Gendarmería no existe en España. Ni departamentos federales.
4. Confunde el género habla en femenino cuando el nombre del supuesto Guardía Civil es un hombre
5. El articulo 372 y 227 del Código Penal Español no hablan de nada de pornografía
6. Las leyes nunca se nombran como "la ley de marzo de 2007" cada ley tiene un número o una denominación. La Ley de Orgánica por la que se módifica la LOE, o la Ley Orgánica 3/2020, de 29 de diciembre.
7. Cuando me llego el email Pilar Llop ya no era ministra, lo había dejado de ser meses antes.
8. y por último El email donde me indican que me dirija es un email de "gmail" ningún organismo de seguridad pública como la Guardia Civil nos va a pedir información por Gmail... y lo peor al pulsar en el email, me lleva a otra dirección diferente también de gmail con el nombre de una mujer.

Buscando información de los nombres que aparecen en el email, de los email a los que en principio debería mandar información y otros elementos de la carta, veo que el pishing que recibí es una ligera modificación de este pishing <https://blogs.publico.es/bulocracia/2022/03/03/la-directora-de-la-guardia-civil-no-manda-amenazas-por-email/?

doing_wp_cron=1707342937.0029680728912353515625> del que se hicieron eco los medios.

Redes inalámbrica

Wikipedia <https://commons.wikimedia.org/wiki/File:WiFi_Logo.svg>. WiFi (Dominio público)

La protección de la red WiFi en el hogar es esencial para salvaguardar la privacidad y seguridad digital. Una red no segura puede ser vulnerable a intrusiones, robo de datos y acceso no autorizado a dispositivos conectados. Es crucial cambiar la contraseña por defecto proporcionada por el proveedor, ya que estas contraseñas son conocidas y pueden ser explotadas por ciberdelincuentes.

Cambiar la contraseña regularmente fortalece la seguridad. Se debe utilizar una combinación de letras, números y caracteres especiales para hacerla más resistente a ataques de fuerza bruta. Además, es recomendable utilizar el protocolo de seguridad WPA3, que proporciona un cifrado más fuerte que las versiones anteriores.

Otra medida importante es cambiar el nombre de la red (SSID) para evitar que los atacantes identifiquen fácilmente el modelo del enrutador y utilicen vulnerabilidades específicas.

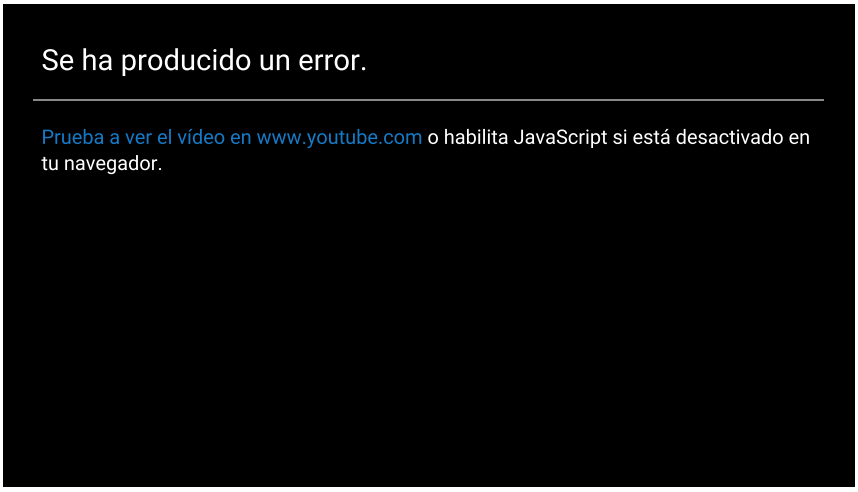
Redes públicas

Imagen generada con IA (Bing). Ladrón en WiFi pública (CC BY-SA <http://creativecommons.org/licenses/?lang=es>)

La vulnerabilidad asociada con el uso de redes inalámbricas públicas plantea serios riesgos para la seguridad de la información. Las conexiones Wi-Fi en lugares públicos, como cafeterías o aeropuertos, son propensas a ataques cibernéticos, exponiendo datos personales a posibles amenazas.

Es muy recomendable no utilizarlas y utilizar el servicio de Internet proporcionado por el operador telefónico como alternativa más segura. Estas conexiones suelen contar con medidas de seguridad más avanzadas, proporcionando una barrera adicional contra intrusiones no autorizadas y ataques malintencionados.

A continuación tienes un estupendo video donde se explican todos estos problemas y donde se realizan pruebas reales, aunque pueda parecer un vídeo antiguo, todo lo que se comenta es de plena actualidad:



Salvados - La Sexta <https://www.youtube.com/@laSexta> . Seguridad de las redes públicas <https://www.youtube.com/watch?v=WY6g-KzeMNw> (Licencia estándar de YouTube <https://www.youtube.com/static?template=terms>)

Navegador

Imagen generada con IA (Bing). Navegadores (CC BY-SA <http://creativecommons.org/licenses/?lang=es>)

Configurar adecuadamente el navegador es esencial, ya que actúa como la puerta principal al mundo de Internet. Ajustes de seguridad en el navegador son como un cerrojo digital, protegiendo contra amenazas cibernéticas. Asegurarse de tener actualizaciones automáticas habilitadas, utilizar extensiones de seguridad y gestionar las cookies y permisos con precaución son pasos vitales. Un navegador bien configurado no solo mejora la experiencia de navegación, sino que también fortalece la defensa contra posibles riesgos de seguridad en línea, creando una conexión más segura con el ciberespacio.

Navegación privada

La navegación en modo privado es como cerrar la cortina digital al explorar Internet. Protege la privacidad al evitar que se registren historiales, cookies o contraseñas. Esto es esencial, especialmente al realizar transacciones financieras o acceder a información sensible. Además, en entornos compartidos, evita que otros vean tu actividad en línea. Navegar de manera privada también ayuda a evitar la personalización no deseada de anuncios basada en el historial de búsqueda. En resumen, activar la navegación privada no solo preserva la intimidad en línea, sino que también añade una capa de seguridad esencial al proteger datos personales de miradas indiscretas. Aquí tienes los pasos para hacerlo en Chrome <https://support.google.com/chrome/answer/95464?hl=es&co=GENIE.Platform%3DDesktop> y Firefox <https://support.mozilla.org/es/kb/navegacion-privada-Firefox-no-guardar-historial-navegacion>

Publicidad en Internet

La publicidad en Internet, si bien es una herramienta vital para financiar servicios digitales, ha generado inquietudes significativas en relación con la invasión de la privacidad del usuario. La creciente sofisticación de las técnicas de

seguimiento y segmentación ha llevado a una intrusión sin precedentes en la vida digital de las personas. La recolección constante de datos personales para dirigir anuncios específicos ha creado un entorno en el que la privacidad se ve comprometida en aras de estrategias publicitarias más efectivas.

Los usuarios experimentan una invasión constante al ser perseguidos por anuncios personalizados que reflejan sus actividades en línea. La sensación de que la privacidad está siendo constantemente vulnerada ha llevado al aumento del uso de bloqueadores de anuncios y medidas de protección de datos.

La monetización de la información personal ha generado una brecha significativa entre la necesidad de los anunciantes de llegar a audiencias específicas y el derecho fundamental de los individuos a la privacidad. La falta de transparencia en la recopilación y el uso de datos personales plantea interrogantes éticos y resalta la urgencia de reformas en la regulación de la publicidad en línea para salvaguardar la privacidad del usuario. En este contexto, la publicidad en Internet se ve envuelta en una creciente controversia que destaca la necesidad crítica de abordar las preocupaciones de privacidad en el entorno digital.

Actividad 2.2 Navegamos seguros

---

1. Accede a la web de ipepcordoba.com <http://www.ipepcordoba.com/> desde una sesión privada del navegador y realiza una captura.
2. Anuncios en Internet
    a. Accede a una web que tenga anuncios, haz una captura de pantalla
    b. Instala un bloqueador de anuncios en el navegador
    c. Realiza una captura de de pantalla con los anuncios ya bloqueados.

Finalmente tendrás 4 capturas de pantalla, no es que no sepa contar, ¿recuerdas la captura de pantalla que hiciste en el apartado anterior comprobando si tu contraseña había sido filtrada o no? pues debes añadirla también junto con las 3 que acabas de hacer ahora. Añadelas a un documento de texto y conviertelo a pdf para subirlo a la plataforma, en la tarea correspondiente.

---

6. Criptografía

Introducción

Imagen generada con IA (Bing). Criptografía en el Antigüo Egipto (CC BY-SA <http://creativecommons.org/licenses/?lang=es>)

La necesidad de compartir mensajes privados y que no sean interceptados es una necesidad que se remonta hasta el Antiguo Egipto, hace más de 4500 años.

Es por ello que se hace necesario diseñar reglas o códigos para encriptar esos mensajes y, en el caso de que sean interceptados, no puedan ser revelados fácilmente. Esto es precisamente el objetivo de la criptografía, desarrollar técnicas para ocultar información.

Sin embargo, la historia, o nuestra propia naturaleza, nos ha forzado a intentar descrifrar esos mensajes, teniendo una relevancia mayúscula en, por ejemplo, la II Guerra Mundial. Ese es precisamente el objetivo del criptoanálisis.

Te has dado cuenta.....

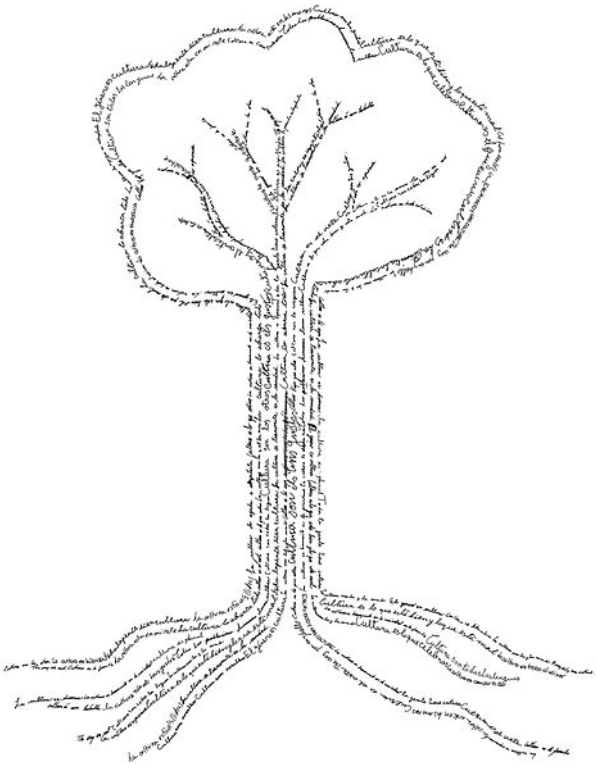
Seguro que en algún momento de tu vida, has creado con tus amigos un sistema para comunicarte con ellos de forma secreta. ¿Te atreves a desvelarlo?

¿Qué es la esteganografía?

La esteganografía, una técnica ancestral de ocultamiento de información dentro de otro tipo de datos, abarca una gama diversa de medios, desde imágenes y videos hasta archivos de audio y texto. Su propósito principal es eludir la detección por parte de observadores no autorizados, camuflando la información dentro de un contexto aparentemente inocuo.

A diferencia de la criptografía, cuyo enfoque radica en proteger la información mediante la aplicación de algoritmos de cifrado, la esteganografía va más allá, no solo ocultando el contenido, sino también la misma existencia de la información oculta. Este aspecto es crucial, ya que la presencia del mensaje secreto no es detectable a simple vista, a menos que se realice una búsqueda minuciosa o se cuente con conocimientos especializados en la materia.

Los métodos digitales de esteganografía son diversos y versátiles, incluyendo la ocultación de datos dentro de archivos de texto, imágenes, audio, video e incluso en archivos de cualquier tipo. Estos métodos pueden ser aplicados de forma



Museu Valencià d'Etnologia <https://en.wikipedia.org/wiki/Museu_Valenci%C3%A0_d%27Etnologia> . Caligrama (CC BY-SA <http://creativecommons.org/licenses/?lang=es>)

independiente o combinados entre sí para aumentar el nivel de seguridad y complejidad del ocultamiento.

Además, la esteganografía puede ser complementaria a la criptografía, donde el mensaje oculto puede estar previamente cifrado antes de ser insertado en el medio portador. Esta combinación ofrece una capa adicional de protección, ya que no solo se oculta la información, sino que también se protege mediante técnicas de cifrado, dificultando aún más su detección y decodificación por parte de terceros no autorizados.

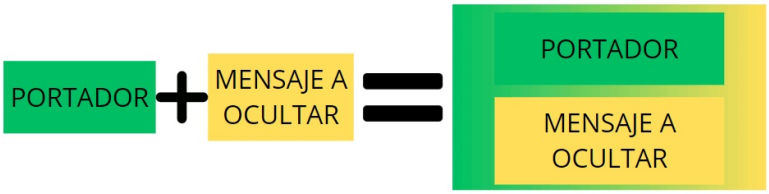


Imagen de elaboración propia. Esteganografía (CC BY-SA <http://creativecommons.org/licenses/?lang=es>)

¿Quieres saber más?

Se ha producido un error.

Prueba a ver el vídeo en www.youtube.com o habilita JavaScript si está desactivado en tu navegador.

Estegoanálisis

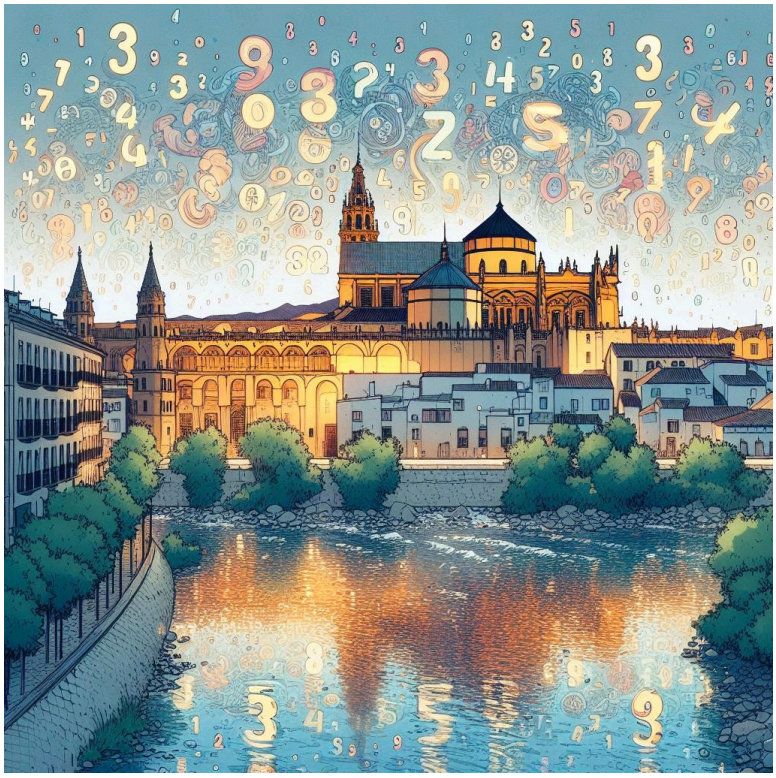


Imagen generada con IA (Bing). Estegoanálisis (CC BY-SA <http://creativecommons.org/licenses/?lang=es>)

El estegoanálisis, un proceso meticuloso y complejo, implica la detección, análisis y, en ocasiones, la decodificación de información clandestina empleando las sofisticadas técnicas de la esteganografía.

Este campo del análisis se presenta como un desafío continuo, dado que las estrategias esteganográficas se han vuelto cada vez más intrincadas. Para abordar este desafío, los estegoanalistas deben mantenerse al día con los avances más recientes en técnicas y herramientas, con el fin de identificar con eficacia la presencia de información oculta. Además, la naturaleza del estegoanálisis puede exigir un enfoque multidisciplinario, que integre conocimientos de informática forense, criptografía y teoría de la información, entre otros campos relacionados.

La gama de técnicas empleadas en el estegoanálisis es sumamente variada, abarcando desde métodos simples como la inspección visual o auditiva, hasta complejos algoritmos matemáticos y estadísticos. Esta diversidad de enfoques refleja la necesidad de adaptabilidad y versatilidad por parte de los

estegoanalistas en su labor de revelar información oculta.

¿Sabías que?

Un artista famoso que incluyó mensajes ocultos en sus obras fue Michelangelo Buonarroti. Este renombrado artista del Renacimiento italiano, conocido principalmente por su maestría en la escultura y la pintura, también empleó la técnica de la esteganografía para transmitir mensajes ocultos en algunas de sus obras más emblemáticas.

Un ejemplo destacado es la famosa pintura del techo de la Capilla Sixtina en el Vaticano, donde Michelangelo incorporó una serie de significados simbólicos y referencias religiosas en sus frescos. Además, se especula que Michelangelo pudo haber incluido representaciones ocultas de la anatomía humana y mensajes simbólicos en varias de sus esculturas, aunque estos detalles pueden ser objeto de interpretaciones diversas y controvertidas.

Te lo digo con música

Te gusta la música? Aquí tienes una canción que habla sobre el estegoanálisis y la estenografía. Esta canción ha sido generada con IA con la herramienta Suno <https://app.suno.ai/>

Canción generada con IA (Suno). Entre Claves y Enigmas ( )

Si quieres puedes descargarte la canción para escucharla offline.

Herramientas

Pero basta de teoria, vamos a trabajar con herramientas concretas que permitirán que tu y tus amigos y familiares podáis compartir información oculta en mensajes aparentemente inofensivos.

Te recomendamos dos herramientas que debes explorar y conocer. Oculta mensajes en imagenes y audios y revelalos después. Te serán muy útiles en un futuro:

- Esteganografía de imágenes <https://stylesuxx.github.io/steganography/> de stylesuxx en github
- Stegonaut <https://www.stegonaut.com/> Oculta y revela información en archivos de audio MP3

Actividad 3. Descifra la invitación

–

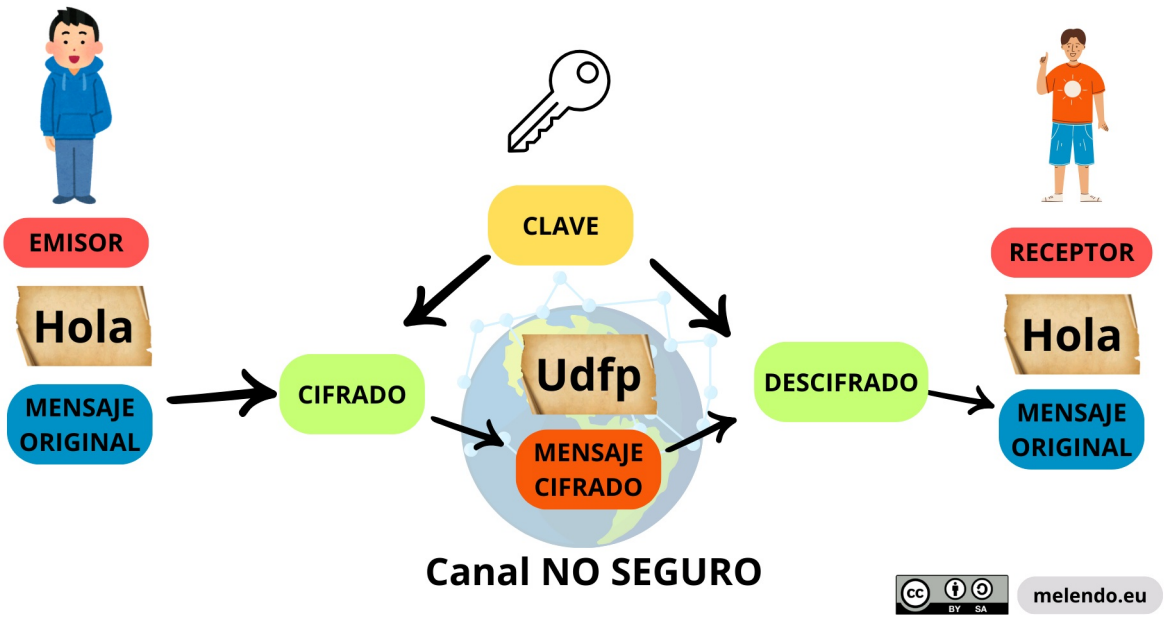
7. Criptografía simétrica

Fundamentos

La criptografía clásica, también conocida como criptografía simétrica, constituye un método de cifrado fundamental en el que una única clave se emplea tanto para el cifrado como para el descifrado de los datos. Esta clave compartida entre el remitente y el destinatario garantiza la confidencialidad de la información transmitida, ya que es utilizada de manera simultánea para ocultar (cifrar) y revelar (descifrar) el mensaje.

En este contexto, es esencial destacar que la seguridad de la comunicación en criptografía simétrica radica en la confidencialidad de la clave compartida. Por lo tanto, la generación, distribución y gestión adecuadas de esta clave son aspectos críticos para asegurar la integridad y la autenticidad de la información transmitida. Además, se ha avanzado en el desarrollo de protocolos y algoritmos criptográficos eficientes para mejorar la resistencia contra posibles ataques, como el uso de algoritmos de cifrado de bloque y de flujo, así como técnicas de autenticación de mensajes.

Asimismo, cabe mencionar que la criptografía simétrica se utiliza ampliamente en una variedad de aplicaciones, incluyendo la protección de datos en redes informáticas, la seguridad de las comunicaciones en línea y el almacenamiento seguro de información confidencial. Sin embargo, a pesar de sus ventajas en términos de eficiencia y velocidad, la criptografía simétrica presenta desafíos en lo que respecta a la distribución segura de claves y la escalabilidad en entornos de comunicaciones a gran escala. Por tanto, su implementación efectiva requiere un enfoque cuidadoso y la combinación con otras técnicas criptográficas, como la criptografía asimétrica, para garantizar un nivel óptimo de seguridad en las comunicaciones digitales.



Proceso de Cifrado (CC BY-NC-SA <http://creativecommons.org/licenses/?lang=es>)

En el contexto de un sistema de criptografía simétrica, el proceso operativo se desenvuelve en las siguientes etapas detalladas:

1. Generación de clave privada: Este primer paso implica la creación de una clave secreta que será compartida exclusivamente entre el remitente y el destinatario para asegurar la confidencialidad de la comunicación. Esta clave se genera mediante algoritmos criptográficos específicos y debe ser lo suficientemente robusta para resistir posibles intentos de descifrado por parte de terceros no autorizados.

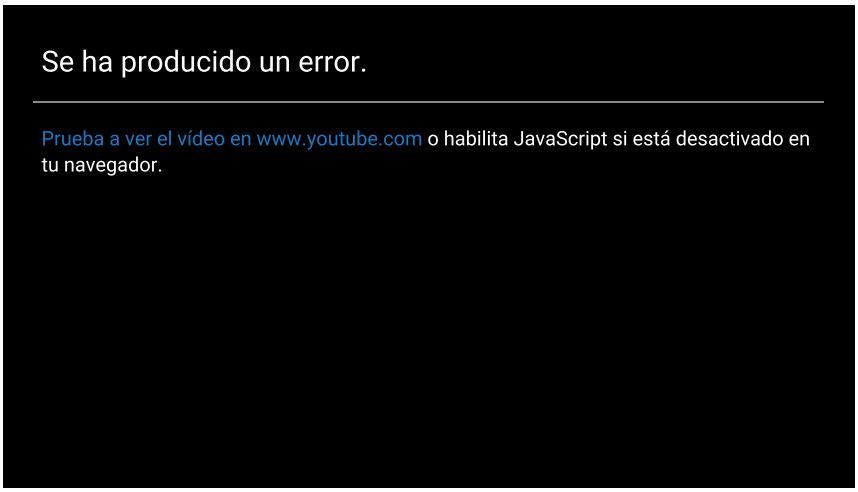
2. Cifrado del mensaje: En esta fase, el remitente emplea la clave compartida previamente establecida para cifrar el mensaje antes de su transmisión. Durante este proceso, el mensaje original se somete a transformaciones matemáticas mediante algoritmos criptográficos, convirtiéndolo en una forma ilegible y aparentemente aleatoria para cualquier individuo que no posea la clave correspondiente. Esta técnica de cifrado garantiza la confidencialidad de la información durante su transmisión a través de canales no seguros, como redes de comunicación pública o internet.

3. Transmisión del mensaje cifrado: Una vez que el mensaje ha sido cifrado con éxito, se transmite al destinatario a través del canal de comunicación previamente establecido. Durante esta etapa, se pueden implementar medidas adicionales de seguridad, como el uso de protocolos de comunicación seguros (por ejemplo, HTTPS), para proteger la integridad y la autenticidad de los datos durante su tránsito.

4. Descifrado del mensaje: Al recibir el mensaje cifrado, el destinatario utiliza la misma clave compartida que fue empleada por el remitente para descifrar el mensaje y recuperar la información original. Este proceso de descifrado implica la aplicación de algoritmos criptográficos inversos que deshacen las transformaciones realizadas durante el cifrado, restaurando así el mensaje a su forma legible y comprensible para el destinatario autorizado.

Es fundamental destacar que la seguridad del sistema de criptografía simétrica depende en gran medida de la confidencialidad y la integridad de la clave compartida. Por lo tanto, se deben implementar prácticas sólidas de gestión de claves para garantizar su protección contra posibles amenazas y ataques cibernéticos. Además, es importante mencionar que la criptografía simétrica ofrece un alto rendimiento y eficiencia en términos computacionales, lo que la convierte en una opción preferida para aplicaciones que requieren un procesamiento rápido y seguro de datos, como la comunicación en tiempo real y el almacenamiento de información sensible.

Vamos a verlo con más detalle....

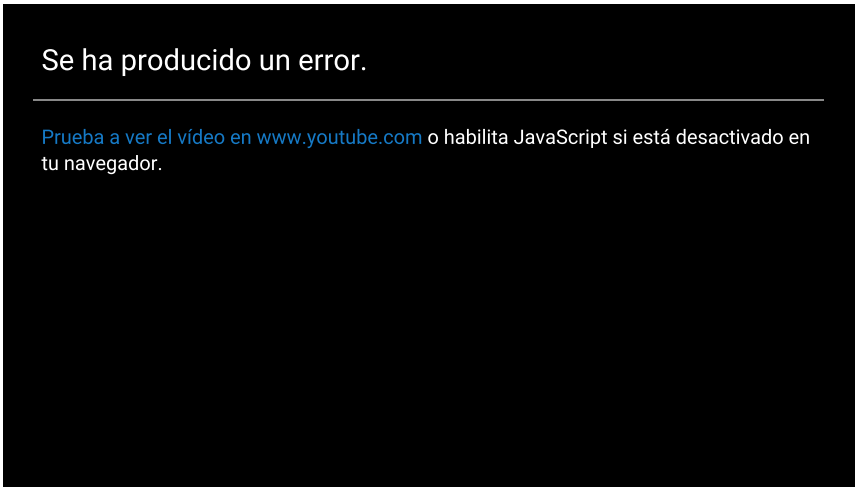


Vídeo de Los números de Fran <https://www.youtube.com/@losnumerosdefran> . Criptografía simétrica <https://www.youtube.com/watch?v=aeFPuqW9OCM> (Licencia estándar de YouTube <https://www.youtube.com/static?template=terms>)

¿Este sistema es seguro?

La eficacia y robustez de la criptografía simétrica se sustentan en la confidencialidad y la integridad de la clave compartida entre las partes autorizadas. La relevancia de este aspecto se hace evidente al considerar que, en caso de que un tercero no autorizado logre acceder a la clave, podría comprometer la seguridad del sistema y descifrar con facilidad los mensajes cifrados, vulnerando así la confidencialidad de la información transmitida. En consecuencia, la protección y la gestión segura de la clave simétrica se convierten en aspectos críticos para garantizar la integridad del sistema criptográfico y mantener la confidencialidad de las comunicaciones. Es fundamental implementar medidas de seguridad robustas, como el uso de algoritmos de cifrado sólidos y protocolos de gestión de claves seguros, con el fin de prevenir posibles vulnerabilidades y asegurar la confidencialidad de la información en todo momento.

Cuando en la siguiente sección veamos la criptografía asimétrica, veremos como se pueden combinar ambos sistemas para hacer un sistema que hasta el día de hoy es inquebrantable, y que siga así muchos años, porque sino vamos a tener un problema muy grande en internet y en la sociedad en general... por ahora el único peligro para este sistema son los ordenador cuánticos, pero tranquilos que aún estan muy lejos de conseguirlo:



Vídeo de Derivando <https://www.youtube.com/@Derivando> . ¿Los ordenador cuanticos romperán nuestras claves? (Licencia estándar de YouTube <https://www.youtube.com/static?template=terms>)

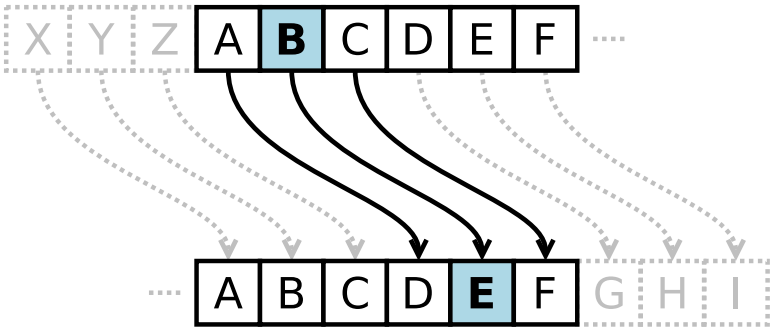
Repasamos

Cifrado César

Durante el apogeo del Imperio Romano, la comunicación segura era vital para mantener el poder y control. Julio César, uno de los líderes más reconocidos de la historia, utilizó una técnica de cifrado simple pero efectiva, conocida hoy como el cifrado César. Aunque simple, este método fue revolucionario en su época y marcó el comienzo de la criptografía como la

conocemos hoy.

El cifrado César es una técnica de criptografía que consiste en sustituir cada letra de un mensaje por otra que se encuentra un número fijo de posiciones más adelante o más atrás en el alfabeto. Por ejemplo, si el desplazamiento es de 3, la letra A se reemplaza por la D, la B por la E, y así sucesivamente. Este método se llama así porque lo usaba Julio César para comunicarse con sus generales de forma secreta. El cifrado César es muy fácil de descifrar, ya que solo hay un número limitado de combinaciones posibles. Se puede usar el análisis de frecuencias o la fuerza bruta para encontrar la clave. El cifrado César es un tipo de cifrado por sustitución monoalfabética, que se puede mejorar usando varios alfabetos, como en el cifrado de Vigenère



Cepheus <https://commons.wikimedia.org/wiki/User:Cepheus~commonswiki> . Cifrado cesar <https://es.wikipedia.org/wiki/Cifrado_C%C3%A9sar#/media/Archivo:Caesar3.svg>

(Dominio público)

Para facilitar el trabajo de cifrado y descifrado se puede utilizar una rueda de cifrado. Puedes pulsar en inner y outer y desplazar las ruedas, shift le indica el número de clave del cifrado. De esa forma quedan emparejadas las letras originales y las cifradas. Cuidado porque esta rueda no tiene Ñ, el alfabeto que se usa en el cifrado Cesar es fundamental, en Español tenemos la Ñ y en Francés por ejemplo tienen la Ç. Así que en el cifrado Cesar además de la clave es fundamental saber el alfabeto

Rueda de cifrado Cesar <https://www.geogebra.org/material/show/id/SRdYhZ2J#>

(CC BY-SA <http://creativecommons.org/licenses/?lang=es>)

Además hoy día a muchas web que nos pueden ayudar a cifrar descifrar mensajes con este tipo de cifrado. Una muy popular es Cryptii <https://cryptii.com/pipes/caesar-cipher>

Actividad 4. Enviamos un email cifrado

8. Criptografía asimétrica

Fundamentos

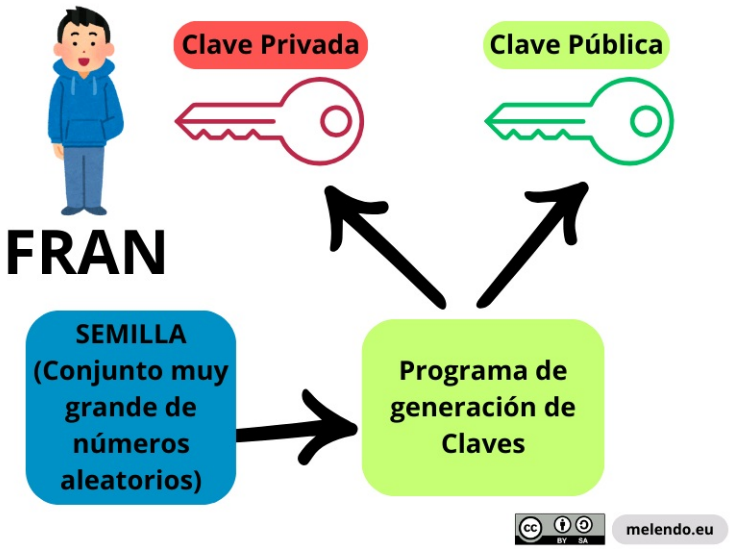
La criptografía asimétrica, también denominada criptografía de clave pública, es una rama de la seguridad informática que se centra en el uso de un par de claves interconectadas para realizar operaciones de cifrado y descifrado. Este método es fundamental en la protección de la información sensible en entornos digitales.

A diferencia de la criptografía simétrica, donde una sola clave se emplea tanto para cifrar como para descifrar los datos, la criptografía asimétrica se basa en un enfoque de claves distintas pero complementarias. Cada usuario o entidad en un sistema de criptografía asimétrica posee un conjunto único de claves: una clave pública y una clave privada. Estas claves están matemáticamente relacionadas, pero son diferentes en su aplicación y propósito.

La clave pública, como su nombre indica, se comparte abiertamente y se utiliza para cifrar los datos que solo pueden ser descifrados por el poseedor de la clave privada correspondiente. Por otro lado, la clave privada se mantiene en secreto y se utiliza para descifrar los datos cifrados con la clave pública asociada.

Tomemos como ejemplo a un usuario ficticio llamado Fran para ilustrar el funcionamiento de este sistema. Supongamos que Fran desea enviar un mensaje seguro a otro usuario, Antonio. Fran utiliza la clave pública de Antonio para cifrar el mensaje, lo que garantiza que solo Antonio , que posee la clave privada correspondiente, pueda descifrar y leer el mensaje. Este método asegura la confidencialidad de la comunicación incluso si el mensaje es interceptado durante su transmisión.

Además de la seguridad que ofrece en las comunicaciones, la criptografía asimétrica también se utiliza en la autenticación de usuarios y la firma digital de documentos, entre otros usos. Su aplicación es fundamental en la seguridad de la información en entornos digitales, donde la protección de los datos es de suma importancia.



Las claves empleadas en este proceso son generadas mediante algoritmos de cierta complejidad, los cuales utilizan patrones numéricos aleatorios para garantizar un alto nivel de imprevisibilidad y dificultar la identificación de cualquier patrón predecible.

Supongamos que Fran desea enviar un mensaje cifrado a Antonio. En este escenario, Fran utilizará la clave pública de Antonio para cifrar el mensaje, siguiendo el estándar de la criptografía asimétrica. Es importante destacar que cada usuario tiene su propia clave pública, lo que asegura un cifrado único y exclusivo para cada destinatario.

Cuando Antonio recibe el mensaje cifrado, procede a utilizar su clave privada única y exclusiva para descifrarlo. Esta clave privada es de su propiedad exclusiva y no debería ser compartida con ningún otro usuario. Al descifrar el mensaje con su clave privada, Antonio puede acceder al contenido original enviado por Fran.

A continuación tienes una animación de todo este proceso

Este proceso garantiza un alto nivel de seguridad y confidencialidad en la comunicación entre Fran y Antonio, ya que solo el destinatario autorizado puede descifrar el mensaje utilizando su clave privada correspondiente. De esta manera, se protege la integridad y privacidad de la información transmitida en el intercambio de mensajes cifrados mediante el uso de claves públicas y privadas en la criptografía asimétrica.

Otra funcionalidad del cifrado asimétrico, igual de importante que el envío de mensajes cifrados es el de la validación de firma, esto quiere decir, que nuestro amigo Fran puede firmar un documento electrónico y que Antonio o cualquier otra persona tendrá la seguridad que dicho mensaje ha sido elaborado y firmado por Fran tal y como nos ha llegado a nosotros y que nadie puede alterarlo, ya que si lo altera en el descifrado podremos detectar que dicho mensaje no es el original. A continuación hay una animación que ilustra el proceso.

Algunos ejemplos de algoritmos empleados son:

- Diffie-Hellman <https://es.wikipedia.org/wiki/Diffie-Hellman>
- RSA <https://es.wikipedia.org/wiki/RSA>
- DSA <https://es.wikipedia.org/wiki/DSA>
- Cifrado ElGamal <https://es.wikipedia.org/wiki/Cifrado_ElGamal>
- Criptografía de curva elíptica <https://es.wikipedia.org/wiki/Criptograf%C3%ADa_de_curva_el%C3%ADptica>
- Criptosistema de Merkle-Hellman <https://es.wikipedia.org/wiki/Criptosistema_de_Merkle-Hellman>

Ventajas

1. Seguridad Mejorada:
    - La criptografía asimétrica proporciona un alto nivel de seguridad, ya que la clave privada nunca se comparte y es necesaria para descifrar la información cifrada con la clave pública.
2. Autenticación:
    - Permite la autenticación de mensajes y la verificación de identidad. Un mensaje firmado con una clave privada puede ser verificado por cualquier persona con la clave pública correspondiente, asegurando que el mensaje proviene del remitente esperado.
3. No Repudio:
    - Proporciona no repudio, lo que significa que el remitente de un mensaje no puede negar haberlo enviado, ya que se puede verificar con su clave pública.
4. Facilidad de Gestión de Claves:
    - Es más fácil manejar las claves públicas ya que pueden ser distribuidas libremente sin comprometer la seguridad del sistema.
5. Intercambio Seguro de Claves:
    - Permite el intercambio seguro de claves para sesiones de comunicación cifrada sin necesidad de compartir previamente una clave secreta.

6. Escalabilidad:
    - Es adecuada para entornos con múltiples usuarios y sistemas, ya que cada usuario solo necesita su propio par de claves.

Problemas

Rendimiento:

Los algoritmos de criptografía asimétrica tienden a ser más lentos y computacionalmente intensivos que los algoritmos de criptografía simétrica, especialmente en el cifrado y descifrado de grandes volúmenes de datos.
Longitud de Clave:

Para alcanzar un nivel de seguridad comparable al de la criptografía simétrica, las claves asimétricas necesitan ser significativamente más largas, lo que puede incrementar la complejidad y el tiempo de procesamiento.
Complejidad Operacional:

La implementación y gestión de la criptografía asimétrica pueden ser más complejas debido a la necesidad de generar y administrar pares de claves y certificados digitales.
Ataques a la Infraestructura:

La infraestructura de clave pública (PKI) puede ser un punto débil. Si la autoridad de certificación (CA) es comprometida, la seguridad del sistema entero puede verse afectada.
Problemas de Confianza:

La confianza en la autoridad de certificación es crucial. Si los usuarios no confían en la CA, pueden cuestionar la validez de las claves públicas distribuidas.
Almacenamiento y Protección de Claves Privadas:

La clave privada debe ser almacenada de manera extremadamente segura. Si es comprometida, toda la seguridad basada en ese par de claves se ve comprometida.

Ampliación

A continuación tienes un video para conocer un poco más qué es la criptografía asimétrica

Se ha producido un error.

Prueba a ver el vídeo en www.youtube.com o habilita JavaScript si está desactivado en tu navegador.

Vamos a repasar

—

Actividad 5. Trabajamos con el certificado digital

El certificado digital, piedra angular de la seguridad en línea, emplea la criptografía asimétrica para salvaguardar la información. Seguro que lo has usado muchas veces sin saber que guardaba este secreto, si no lo has usado, ahora es el momento.

Obtenemos el certificado

Si tienes un certificado valido y sin caducar, puedes saltarte este primer paso, si tu certificado esta caducado, debes seguir todos los pasos como si fuese la primera vez que lo solicitas.

Dirígete a la web del certificado digital de la FNMT <https://www.sede.fnmt.gob.es/certificados/persona-fisica/obtener-certificado-software> y sigue los pasos. Recuerda que debes usar el mismo ordenador en todo el proceso.

1. Debes comprobar que tu ordenador cumple los requisitos, en la web que hemos enlazado antes tienes todos los requisitos y una aplicación que autoconfigura tu ordenador.
2. Tendrás que solicitar el certificado con los datos de tu DNI. En este proceso obtendrás un número.
3. Debes ir a una oficina <http://mapaoficinascert.appspot.com/> a acreditarte con tu DNI físico y el número que obtuviste en el paso anterior, llama antes de ir pues muchas requieren cita previa.
4. Por último debes volver a tu ordenador, debe ser el mismo ordenador y el mismo navegador que usaste en el paso 2, y con el código que obtuviste en dicho paso podrás instalar y descargar el archivo de firma digital, guarda a buen recaudo dicho archivo, es tu identificación digital, si alguien se apodera de él, se esta apoderando de tu identidad en Internet

Accedemos a ClicSalud

Accede a la web de ClicSalud+ <https://www.sspa.juntadeandalucia.es/servicioandaluzdesalud/clicsalud/> con tu certificado digital, simplemente tienes que entrar a la web de ClicSalud+ <https://www.sspa.juntadeandalucia.es/servicioandaluzdesalud/clicsalud/> y pulsar en la parte superior donde indica Certificado Digital seleccionas tu certificado y haces una captura donde se vea que el acceso ha sido correcto, como se puede ver en la siguiente imagen:

Imágen de elaboración propia. Acceso a ClicSalud (CC BY-SA <http://creativecommons.org/licenses/?lang=es>)

Instalamos Autofirma

Descarga e instala la aplicación de AutoFirma de la Junta de Andalucia <https://ws024.juntadeandalucia.es/clienteafirma/autofirma/autofirma.html> , te dará acceso a muchos tramites electrónicos con la administración andaluza, local y estatal.

Imagen de elaboración propia. Autofirma (CC BY-SA <http://creativecommons.org/licenses/?lang=es>)

Firma un archivo pdf

Genera un documento pdf con tu nombre y apellidos y firmalo con autofirma, simplemente tienes que seleccionar el fichero en el programa y pulsar en firmar. Una vez firmado, podrás guardar el nuevo archivo con el nombre que desees.

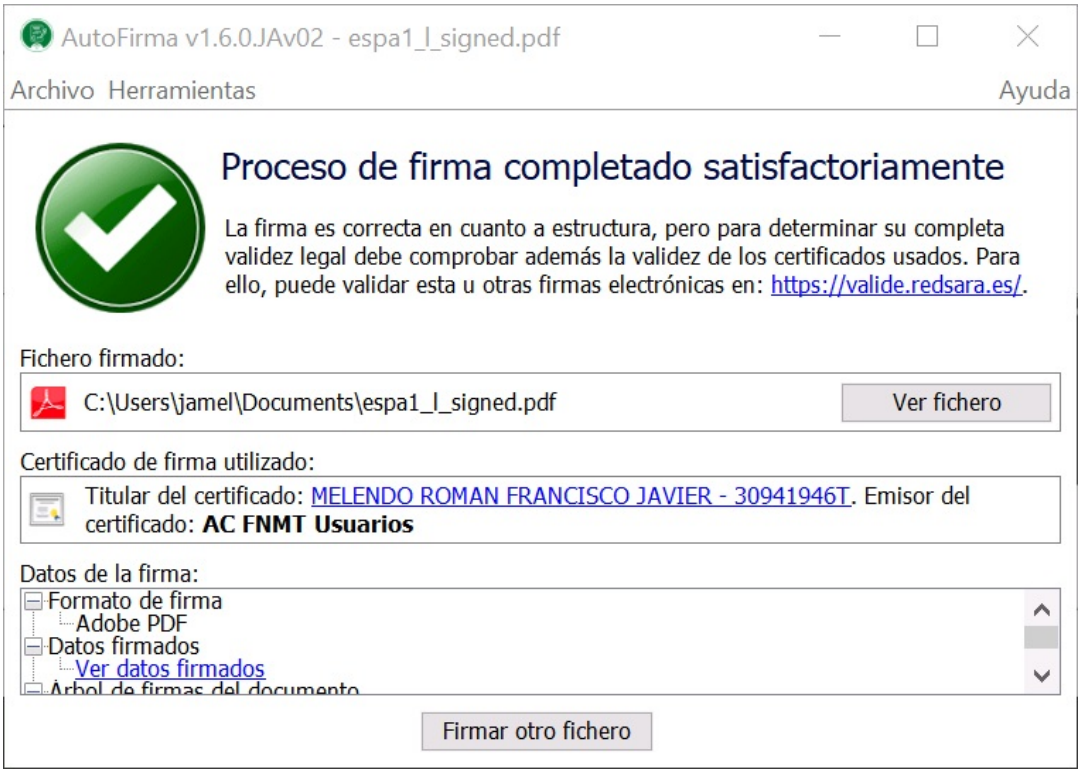


Imagen de elaboración propia. Firmamos (CC BY-SA <http://creativecommons.org/licenses/?lang=es>)

Validar firma

Ahora cuando abras el documento pdf, el programa en tu ordenador te informará de que esta firmado:

Imagen de elaboración propia. Validamos firma (CC BY-SA <http://creativecommons.org/licenses/?lang=es>)

Abre el pdf en tu ordenador y haz una captura de pantalla donde se muestre esa información.

Aunque es muy posible que el programa no conozca a la FNMT como entidad validadora, y te indique que no puede vertificar la firma. Así que cuando recibas documentos firmados la mejor forma de comprobar su autenticidad es ir a la web de validación de redsara.es <https://valide.redsara.es/valide/validarFirma/ejecutar.html> y subir nuestro archivo pdf. Hazlo con tu archivo pdf y realiza una captura de pantalla.

Imagen de elaboración propia. Firma valida (CC BY-SA <http://creativecommons.org/licenses/?lang=es>)

¿Que entregamos?

En la plataforma debéis entregar:

- Un pantallazo de acceso a ClicSalud
- Un archivo pdf firmado con vuestro certificado digital
- Una captura de pantalla con la validación de la web redsara.es

---

Otros formatos y Autoria

Versión eXeReader

Si quieres ver este material en un móvil o tablet Android sin conexión a internet, debes instalar la App eXeReader <https://play.google.com/store/apps/details?id=net.exelearning.exereader&hl=es&gl=US> de tu tienda de aplicaciones y bajarte este archivo

Versión imprimible PDF

Este material esta diseñado para ser leido y trabajado en una pantalla, preferiblemente en un ordenador, pero si quieres imprimir este material para su consulta, en este archivo puedes descargarte el material en pdf

Autoria

Título	SDA Ciberseguridad
Descripción	Situación de aprendizaje sobre seguridad informática para la asignatura TIYC2
Autor	Francisco Javier Melendo Román
Licencia	Creative Commons BY-SA 4.0 <https://creativecommons.org/licenses/by-sa/4.0/>
Fuente	Si eres docente y quieres modificar este material con exelearning bajate este archivo y cambia la extensión zip a elp

Este contenido fue creado con eXeLearning <http://exelearning.net/> , el editor libre y de fuente abierta diseñado para crear recursos educativos.

Criterios de Evaluación

A continuación tenemos todas las Competencias específicas, Criterios de evaluación y Saberes básicos relacionados de la materia Tecnología de la Información y la Comunicación II de 2º de Bachillerato. En negrita encontraras los Criterios de Evaluación que serán calificados en esta SdA

Competencias específicas	Criterios de evaluación	Saberes básicos

1. Reconocer el proceso de transformación como agente de cambio, analizando aspectos positivos y negativos de dicho proceso para entender el papel principal de las tecnologías de la información y la comunicación en la sociedad actual, su impacto en los ámbitos social, económico y cultural, y su importancia en la innovación y el empleo. STEM2, CD2, CD3, CD4, CPSAA1.2, CC1, CE1.	1.1. Analizar y valorar el impacto de la industria de desarrollo de soware en la sociedad actual, en especial en la innovación y el empleo.	TICO.2.A.4.
2. Configurar ordenadores y equipos informáticos, utilizando de forma segura, responsable y respetuosa dichos dispositivos, para comprender el funcionamiento de los componentes hardware y soware que conforman ordenadores y equipos digitales. CCL1, CP2, STEM2, CD2, CD3,CD4, CPSAA1.2.	2.1. Emplear medidas de seguridad informática necesarias para la protección de las personas y de sus datos, comprendiendo los principios de la ciberseguridad, identificando amenazas y riesgos.	TICO.2.C.1.
	2.2. Proteger la privacidad en Internet y reconocer contenido, contactos o conductas inapropiadas, sabiendo informar al respecto.	TICO.2.C.2.
3. Usar, seleccionar y combinar múltiples aplicaciones informáticas, atendiendo a cuestiones de diseño, usabilidad y accesibilidad, incluyendo la creación de un proyecto web, para crear producciones digitales que cumplan unos objetivos determinados. CCL1, CP2, STEM2, CD2,CD3,CD4, CPSAA1.2, CC1, CE1, CCEC4.1.	3.1. Elaborar y publicar contenidos en la web, integrando información textual, gráfica y multimedia, teniendo en cuenta a quién va dirigida y el objetivo que se pretende conseguir, midiendo, recogiendo y analizando datos de uso.	TICO.2.B.1.
4. Comprender el funcionamiento de Internet y de las tecnologías de búsqueda, analizando de forma crítica los contenidos publicados y fomentando un uso compartido de la información, para permitir la producción colaborativa y la difusión de conocimiento. CCL1, CP2, STEM2, CD2, CD3, CD4, CPSAA1.2, CC1, CE1.	4.1. Trabajar colaborativamente en la creación de contenidos digitales, usando herramientas de comunicación y productividad, comprendiendo y respetando los derechos de autor en el entorno digital.	TICO.2.B.2.
5. Comprender qué es un algoritmo y cómo son implementados en forma de programa, analizando y aplicando los principios de la ingeniería del soware, para desarrollar y depurar aplicaciones informáticas y resolver problemas. STEM2, CD2, CD3, CD4, CPSAA1.2, CC1, CE1.	5.1. Desarrollar una variedad de aplicaciones informáticas en las que se emplee una aproximación modular y diferentes estructuras de datos.	TICO.2.A.1.
	5.2. Aplicar los principales pasos del ciclo de vida de una aplicación, trabajando de forma colaborativa, empleando un entorno de desarrollo integrado.	TICO.2.A.2.
	5.3. Analizar y resolver problemas de tratamiento de la información, dividiéndolos en subproblemas, empleando mecanismos de abstracción, definiendo algoritmos que los resuelvan e identificando problemas y soluciones similares.	TICO.2.A.3.