CAI4. CONSULTA SOBRE LA CONFIDENCIALIDAD DE LA INFORMACIÓN EN UNA ENTIDAD HOSPITALARIA II

Escuela Técnica Superior de
Ingeniería Informática

Índice

Alcance y Objetivos de la Consultoría

Como se explicó en la anterior consultoría, el principal objetivo de es es hacer que unos datos sean ininteligibles para un tercero en caso de que se pierda el control de la información. Para esto se nos ha pedido hacer un estudio sobre la esteganografía como método de ocultación.

Además, se tiene la sospecha que un trabajador está realizando envíos no autorizados de forma ajena al hospital usando este mismo método.

Por otra parte, también se ha realizado de forma paralela otra consulta sobre la seguridad de los clientes web y la realización de dos manuales de configuración para aumentar la seguridad de los mismos.

Recursos de la Consultoría

Para esta auditoría se harán uso de los siguientes recursos.

Recursos Humanos

El equipo de seguridad para esta asignatura se compone de los siguientes miembros:

- Barragán Candel, Marina - estudiante de Ing. Informática – Tecnología Informática, en la mención de Tecnologías de la información
- Calcedo Vázquez, Ignacio - estudiante de Ing. Informática – Tecnología Informática, en la mención de Sistemas de Información
- Polo Domínguez, Jorge - estudiante de Ing. Informática – Ingeniería de Computadores
- Sala Mascort, Jaime Emilio - estudiante de Ing. Informática – Tecnología Informática, en la mención de Computación

Recursos Tecnológicos

El equipo ha reunido un conjunto de herramientas con el objetivo de realizar la consultoría.

VSL

Se trata de una herramienta gráfica de diagramación en bloques que permite la fácil configuración del proceso esteganográfico de ocultación, extracción y análisis de los estegos.

Clientes Web

Para la segunda parte de esta consultoría, se harán uso de dos clientes web, Chrome y Firefox, que suponen un gran porcentaje de los exploradores utilizados a nivel mundial.

Estudio Inicial

La esteganografía consiste en el estudio y aplicaciones de distintas técnicas que permiten la ocultación de cualquier tipo de información en otros objetos, llamados portadores, para así crear un canal de comunicación encubierto, a lo largo de la historia se ha tratado de múltiples formas desde letras en un libro a usar los puntos de las íes como código morse, sin embargo, ahora en la época digital es sencillo ocultar información en cualquier objeto, ya sea un vídeo, un texto o una imagen.

En este estudio, nos centraremos en la ocultación de información en imágenes de un formato concreto, BMP, con el método más común, Least Significant Bit, o LSB, donde se oculta la información en el bit

menos significativo de un byte, de forma que apenas se altere el portador y también tenemos otro algoritmo llamado F5 que consiste en una revision de los algorttmos F3 y F4, donde se prioriza que la densidad de uso del portado sea la misma en todas las zonas y oculta la información en los coeficientes de la transformada discreta coseno, DCT.

Actividades de la Consultoría

Para poder realizar esta consultoría se han llevado a cabo las siguientes actividades:

Análisis de las técnicas de ocultación

Como se comentó en el estudio inicial, se analizarán las técnicas de LSB y F5 como métodos de ocultación.

Least Significant Bit, LSB

LSB es un método que usa la posición menos significativas de los bytes de la imagen para guardar un solo bit del objeto a ocultar, debido a ello, tiene una serie de limitaciones, por ejemplo,en la cantidad de información que se puede almacenar como máximo un 12,5% en relación al tamaño del portador sin que se afecte drásticamente al portador, además si no se incluye ninguna técnica de cifrado de la información, no supone un gran avance con respecto a guardar la imagen en un texto plano.

Pese a sus desventajas, se puede combinar con un algoritmo de cifrado para mejorar la confidencialidad y con ello se tiene un método confidencial, sin embargo hay que realizar más pruebas para comprobar la robustez y la velocidad de ocultación y recuperación

F5

F5 es un método de ocultación más complejo que usa coeficientes matemáticos que rebasan el nivel de esta consultoría, sin embargo, si podemos asegurar que se garantiza un mejor aprovechamiento de los objetos portadores, además introduciendo un coeficiente de aleatoriedad para que sea más difícil la detección de los estegos, además a su vez también se garantiza la confidencialidad de los estegos.

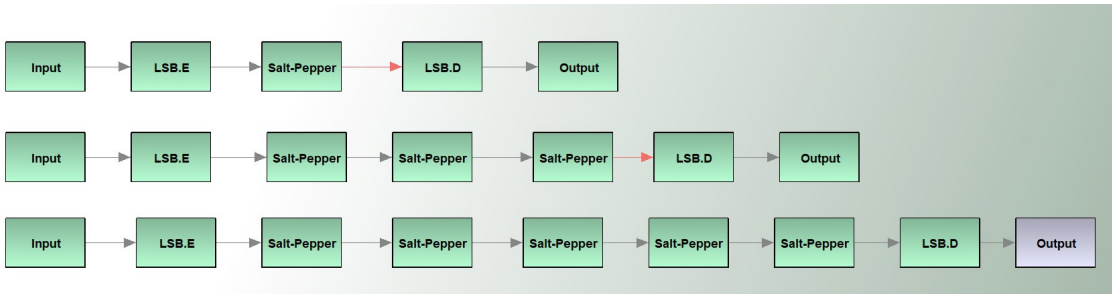
Con este método, se puede conseguir más del 13,5% de capacidad de ocultación, sin embargo debemos hacer las pruebas para saber su velocidad de ocultación y recuperación.

Pruebas de las técnicas de ocultación

Para las pruebas, hemos de usar firmas de entre 128 y 512 bytes, por tanto necesitamos imágenes de al menos 4096 pixeles, además debemos tener en las cabeceras de los formatos bmp se deben conservar, por tanto serán ficheros de algo mas de 4KB.

Para la realización de las pruebas usaremos VSL como herramienta de análisis.

Los diagramas utilizados para la generación de las pruebas son las siguientes:



El algoritmo de LSB ofrece las siguiente tasas de ocultación y recuperación:

Ocultación por LSB				
Tamaño\Nº Paginas	5	10	15	20
128 Bytes	1.61 s	1.71 s	2.25 s	2.71 s
512 Bytes	0.91 s	1.55 s	2.29 s	3.12 s

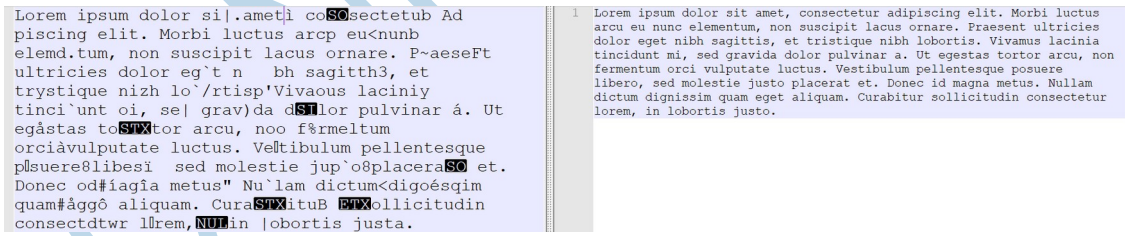
Extracción por LSB				
Tamaño\Nº Paginas	5	10	15	20
128 Bytes	0.36 s	0.83 s	1.11 s	1.60 s
512 Bytes	0.45 s	1.04 s	1.10 s	1.47 s

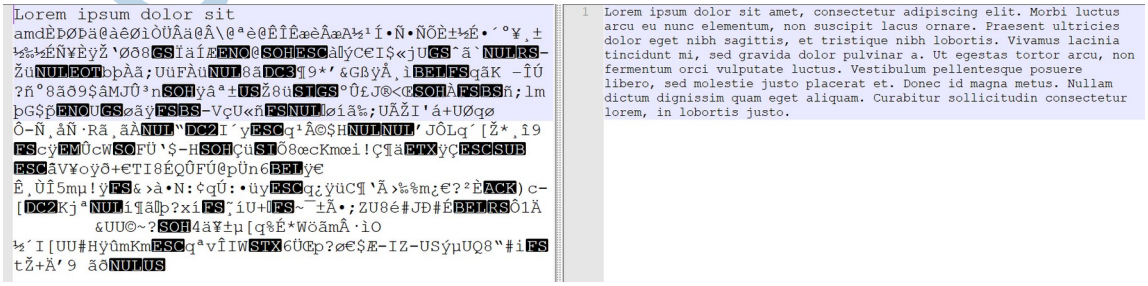
Por otra parte los resultados que nos ofrece F5 son:

Ocultación por LSB				
Tamaño\Nº Paginas	5	10	15	20
128 Bytes	2.10 s	2.75 s	3.54 s	4.98 s
512 Bytes	1.37 s	2.56 s	3.88 s	4.73 s

Extracción por LSB				
Tamaño\Nº Paginas	5	10	15	20
128 Bytes	1.46 s	2.21 s	3.26 s	4.12 s
512 Bytes	1.21 s	2.31 s	3.21 s	4.35 s

Como podemos observar, LSB es un método mucho más rápido debido a su simplicidad, sin embargo, su robustez no es la mejor, ya que como se puede observar en las dos siguientes imágenes aplicando un Salt-Pepper o un Crop, dejan gravemente dañado el mensaje original.





Como se puede comprobar su robustez es bastante limitada ya que su misma sencillez le hace muy sensible a los cambios de tamaño en la imagen.

Estegoanálisis de las imágenes sospechosas

El cliente en primer lugar solicita que se realice un estegoanálisis sobre la evidencia proporcionada en la imagen "dibujo.bmp". Para ello se da total libertad a la hora de realizar el proceso de análisis, siempre y cuando se recoja el proceso seguido para llegar a las conclusiones que se estimen oportunas.

Al comienzo de la investigación se decidió optar por la herramienta VSL 1.1, la cual permite analizar dos tipos de análisis distintos: Análisis LSB-RS y el análisis BSM-SVM . Sin embargo, tras un proceso de búsqueda de alternativas el equipo de análisis encontró un estudio, *"A Comparison Study Using StegExposefor Steganalysis by Eric Olson, Larry Carter, and Qingzhong Liu"*, que recomendaba una alternativa mejor: StegExpose.

En resumen, el estudio concluía que esta alternativa resultaba ser mucho más viable de cara a realizar estegoanálisis ya que VSL tiene muchos problemas para detectar mensajes ocultos en estegos no confeccionados con VSL. Partiendo de aquí, el plan de acción resultó ser utilizar esta nueva herramienta para obtener resultados.

Siguiendo los pasos que indican los desarrolladores de la herramienta, es necesario clonar el repositorio para obtener una aplicación java ejecutable del programa o bien compliar el código desde 0 para obtener un ejecutable. Una vez obtenido dicho ejecutable, el módo de empleo es el siguiente:

```
java -jar StegExpose.jar [directory] [speed] [threshold] [csv file]
```

,donde directory es el directorio donde se encuentran las imágenes a analizar para detectar si son sospechosas o no, speed permite configurar la intensidad del análisis, treshold es un parámetro que indica a partir de qué punto el fichero es susceptible de contener información oculta, y csv file es el fichero que generará el ejecutable tras realizar el análisis.

Resultados	
Filename	Dibujo.bmp
Above stego Threshold?	True
Secret message size	36406 Bytes
Primary Sets	0.31364411892356336
Chi Square	0.3496662168559932
Sample Pairs	0.2975282472564884
RS analysis	0.3111286214276572
Fusion (mean)	0.3179918011159255

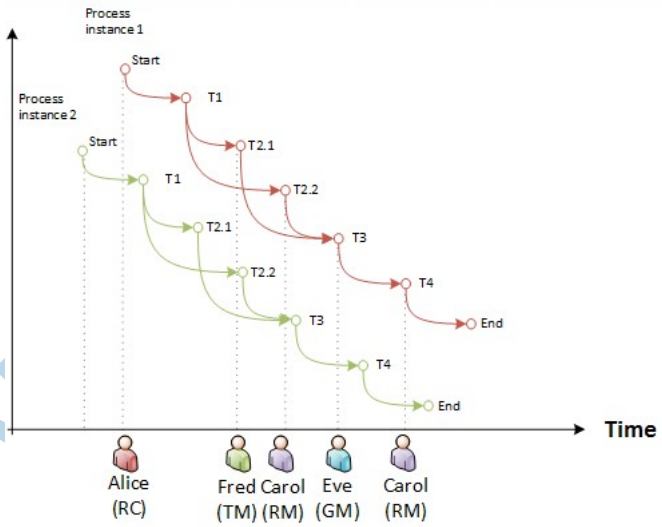
Observando la salida de la aplicación, se puede concluir que dentro de la evidencia presentada existe un mensaje oculto, pues todos los analizadores de la herramienta han sobrepasado el umbral para determinar que dentro de la imagen estudiada se encuentra un posible mensaje oculto. Por tanto, se recomienda tomar las medidas oportunas para cortar de lleno las transmisiones de información mediante este canal.

Una vez que se ha decretado que se está produciendo una comunicación oculta mediante esteganografía, se procede a intentar extraer el mensaje/imagen oculta dentro de la imagen proporcionada como evidencia. Para cumplir con este objetivo, se utilizará la herramienta de esteganografía VSL 1.1, la cual proporciona 3 métodos de decodificación distintos, entre ellos un decodificador de LSB.

El procedimiento de extracción es simple. Una vez abierta la aplicación, se colocan dentro del panel de trabajo un módulo de input, un módulo de LSB.D y finalmente un módulo de output.

Una vez seleccionada la imagen a decodificar, ejecutamos el workflow haciendo click sobre la flecha verde de la barra de iconos situada abajo a la izquierda de la ventana de la aplicación. A partir de aquí el software se encargará de desvelar el mensaje oculto, colocando el resultado en la carpeta "results" dentro del directorio de la aplicación, donde se encuentran los logs y otros archivos de configuración. VSL tras realizar esta decodificación deja como resultado un archivo plano, el cual si se abre con una herramienta de edición de texto mostrará un texto ilegible en casi su totalidad. Sin embargo, se proporciona una pista importante en la primera linea del fichero: %PNG. A partir de esta pista se deduce que el mensaje oculto se trataba de una imagen en formato PNG. Al abrir el fichero con un programa de visualización de imágenes podemos obtener la imagen oculta en la evidencia proporcionada:

Por tanto, se concluye que las sospechas del cliente sobre las filtraciones de información mediante esteganografía eran fundamentadas, y se presenta en este informe el mensaje descubierto, así como los motivos para fundamentar la sospecha.



Análisis de la seguridad en clientes web

Se ha realizado un anexo lleno de información relativa a la seguridad en los navegadores web, Anexo I: Seguridad en Navegadores Web.

Investigación de los ataques indicados

Se ha realizado un estudio de los ataques mencionados, realizando un anexo con la información que se nos pedía, Anexo II: Ataques Informáticos.

Como conclusiones a esta consultoría, debemos desrecomendar el uso de la esteganografía como método de ocultación, ya que a pesar de que haya técnicas más sofisticadas para garantizar su integridad es muy complicado su ocultación, ya que el estegoanálisis permite detectar la gran mayoría de los estegos en imágenes, extinguiendo una de las pocas razones por las que podríamos usarlas.

Anexo I: Seguridad en Navegadores Web

Google Chrome

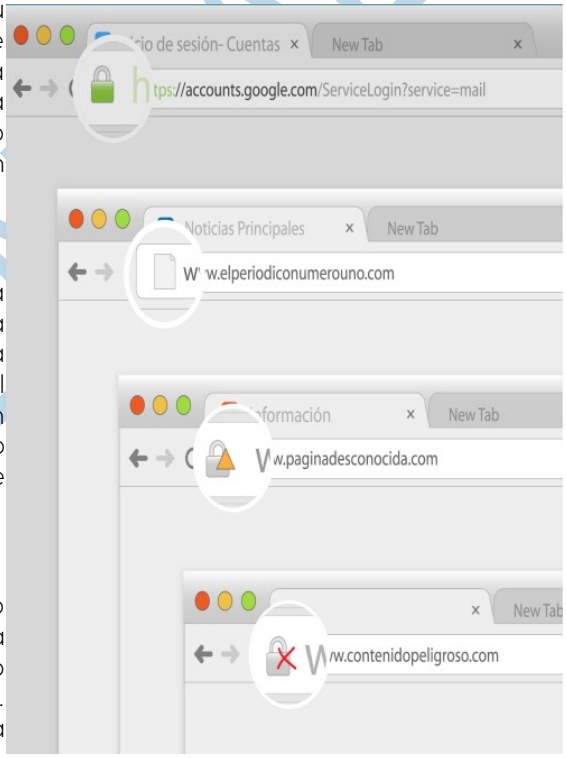
Para asegurar este navegador con una seguridad en general, podemos tener en cuentas las siguientes opciones:

Iconos de Google Chrome

- Chrome estableció una conexión segura:

Si Chrome ha establecido una conexión segura con el sitio que estás visitando, entonces aparecerá un candado verde en la Barra de direcciones, antecediendo a la dirección web.

Al ingresar la información en la web, como el número de tu tarjeta de crédito o tu fecha de nacimiento, verifica siempre que este ícono aparezca. Una conexión segura hace que sea mucho más difícil que otras personas puedan tener acceso a tu información personal o confidencial, especialmente si junto al ícono tiene el nombre de la organización dentro de un rectángulo de color verde.



- El sitio no usa SSL:

En la mayoría de las páginas te aparecerá un hoja blanca antes de la dirección web. Significa que el sitio no está utilizando una conexión segura. Esto no es importante para muchos sitios web, como una página de noticias o un canal musical, pero debes evitar escribir información personal en estas páginas. SSL significa "Capa de conexión segura" o Secure Sokcet Layer, que es un protocolo criptográfico que te proporciona comunicaciones seguras en internet.

- Chrome ha detectado contenido no seguro:

Te saldrá un candado con un triángulo amarillo sobrepuesto cuando ingreses a una página en la que Chrome detecta contenido peligroso, a pesar de que tiene SSL. Ten mucho cuidado al introducir información personal en esta página. Ese contenido peligroso podría ser la puerta de entrada para que alguien obtenga los datos que ingreses allí.

- Riesgo alto de contenido no seguro:

No introduzca ningún tipo de información en páginas que aparezca un candado con una X roja encima. Puede indicar que alguien está intentado manipular tu conexión al sitio web.

Malware y protección contra Phishing.

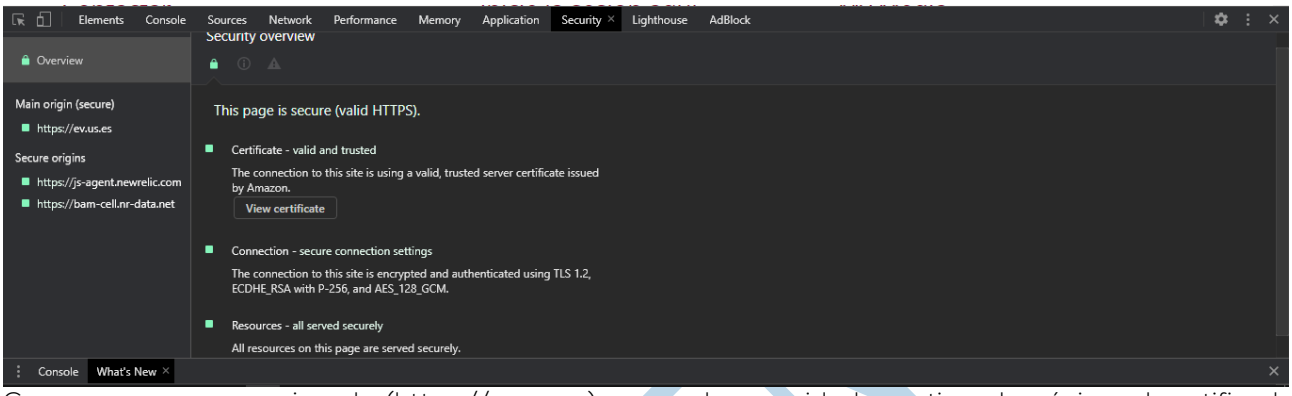
Con el fin de mantenerte a ti y a tu equipo protegidos contra sitios web dañinos, Chrome descarga automáticamente una lista de sitios web peligrosos y maliciosos, almacenando esa lista en tu computador. Cada vez que vayas a una página web, esa página se comparará con la lista.

Si hay sospechas de que una página web es un "malware" o un sitio de "phishing", Chrome mostrará una página de advertencia en lugar de entrar a la página web. Si ves esta página de advertencia, haz clic en Ir atrás para ir a la última página visitada.

Es importante tener en cuenta que Chrome no tiene una lista de todos los sitios web que visitas en Google. Debido a que la lista de sitios web peligrosos se almacenan en tu equipo, Google no necesita saber cuál página estás visitando para advertirte que puede ser peligrosa. Este proceso mantiene el historial de navegación privado y seguro.

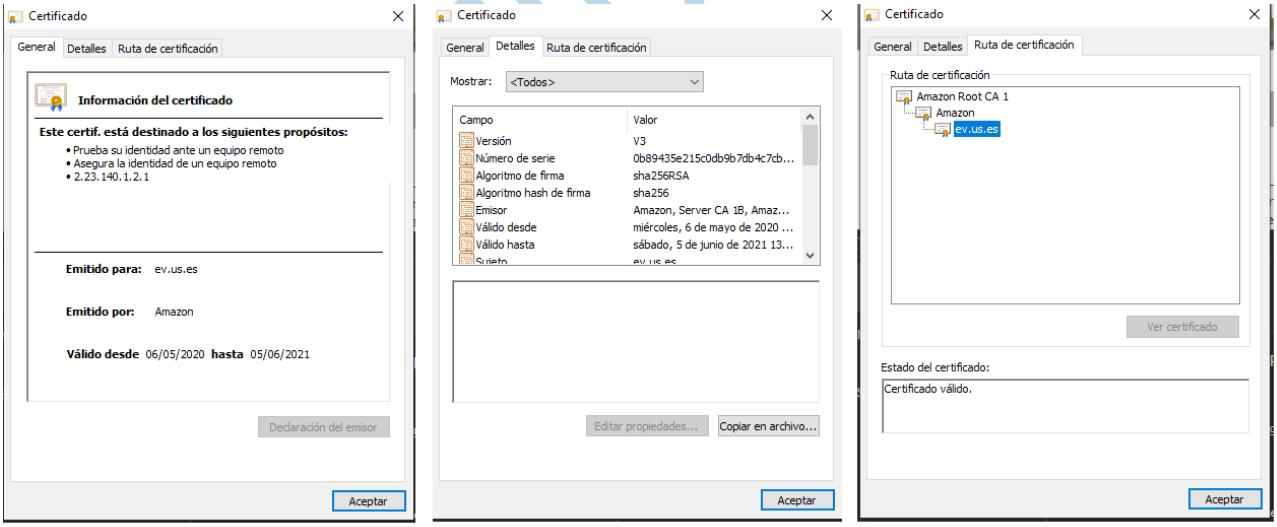
Certificados digitales para verificar la seguridad de la pagina.

En la pagina que queramos operar, pulsando F12 o inspeccionando la pagina con los comandos Ctrl + Mayús + I, podemos observar si la pagina es o no segura y si tiene certificados.



Como vemos en ese ejemplo (https://ev.us.es), vemos la seguridad que tiene la página, el certificado, la conexión segura que está encriptada y autenticada usando TLS 1.2 y que los recursos de la pagina son seguros.

Al abrir ese certificado, nos detalla la versión del certificado digital, la fecha de emisión y duración, clave pública, el algoritmo que se ha utilizado, etc.



Configuración de privacidad

Chrome te permite controlar parte de la información que compartes en la web, mediante la Configuración de Privacidad.

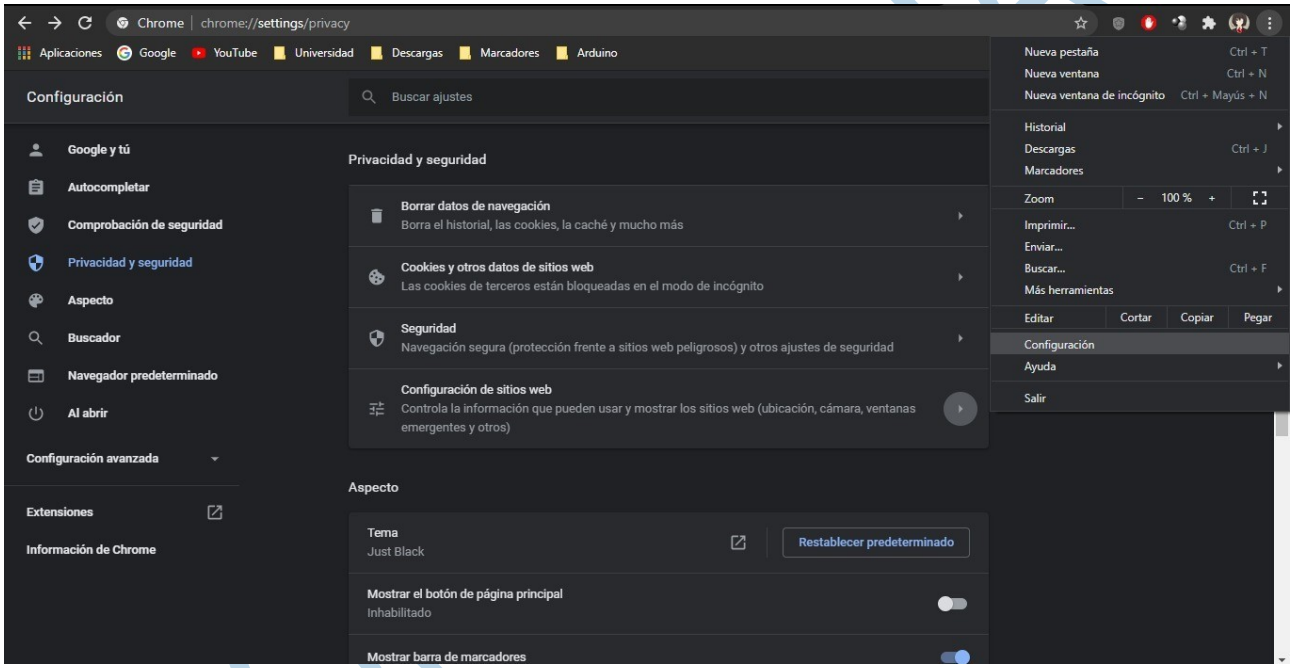
Sin embargo, te recomendamos dejar los valores preestablecidos en Chrome, ya que te permiten tener un equilibrio entre privacidad y seguridad.

Para ingresar a la configuración de privacidad del navegador sigue estos pasos:

1) Haz clic en el botón Configurar que está en la esquina superior derecha del navegador.
2) Se abrirá un menú desplegable. Allí, haz clic en la opción Configuración.
3) Se abrirá el panel de configuración del navegador. Allí busca y haz clic sobre la opción Mostrar configuración avanzada, que estará al final de la página.
4) Aparecerán diversas opciones para configurar tu navegador, entre las que encontrarás la opción Privacidad y seguridad.

Para modificar la configuración básica de privacidad, como permitir el envío detallado de tu uso de Chrome a Google, haz clic en las casillas junto a cada opción.

Para modificar opciones específicas de configuración de privacidad, como permitir que el navegador guarde cookies de las páginas web que visitas o éstas accedan a tu ubicación, haz clic en el botón de Configuración de sitios web.



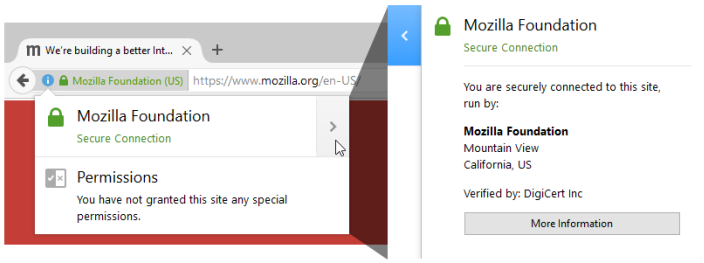
Mozilla Firefox

Seguridad de conexión

Cuando visitas una página, el icono de un candado en la barra de direcciones suele indicar que la conexión a la página es completamente segura.

Para saber más sobre la seguridad de la conexión, haz clic en el botón 'Site Info button' para acceder al Centro de control. La sección superior del panel te informa si la conexión actual está clasificada y es segura y si hay algún contenido no seguro que Firefox esté bloqueando en una página que se presupone segura.

Para saber más sobre el emisor de certificados de conexión segura y el propietario de una página (en el caso de que la información esté disponible) o para desactivar el bloqueo de contenido no seguro en una página, haz clic en la flecha de la derecha del Centro de control.



Bloqueo de contenido

Cuando la función de bloqueo de contenido está activada, el Centro de control indica si una página contiene o no elementos que pueden rastrearte, además de información sobre la conexión. La función de bloqueo de contenido de Firefox también detecta y bloquea automáticamente los rastreadores conocidos. El Centro de control te permite deshabilitar la función, si quieres.

Permisos

La sección de permisos del Centro de control te muestra cualquier permiso especial que hayas garantizado a una página en el pasado y te permite administrarlos.

Para poder editar cualquier otro permiso a una página, haz clic en la flecha derecha del Centro de control y haz clic en el botón 'Más información'.

Se abrirá la página de información, que incluye la sección de permisos.

Anexo II: Ataques Informáticos

Tipo de Ataque	Causa del ataque	Efecto del ataque	Contramedidas recomendadas
BEAST	Se incrusta código en el navegador que obliga a enviar texto sin formato por un canal SSL, se captura el tráfico del usuario mediante rastreador o Man In The Middle.	El atacante tiene la capacidad de descifrar parte de los mensajes codificados y es capaz de averiguar las cookies.	-Cerrar la sesión al terminar. -El atacante necesita acceso al sistema del usuario, el software de seguridad es útil para evitar este tipo de ataque. -Asociar las cookies de la sesión a la dirección IP con la que inicia conexión -Invalidar las cookies al cerrar la sesión
POODLE	Uso de cifrado CBC y servidor indica padding OK/incorrecto.	Se obtiene el texto plano a partir del texto cifrado.	·No uso de SSL, sino TLS. ·Uso de GCM.
FREAK	Usa pares de claves públicas RSA de 512 bits o menos. También ocurre que en equipos de gama media-baja, el ataque es capaz de desencriptar ese tipo de claves.	Los atacantes pueden acceder a la seguridad de la web mediante recursos, relativamente limitados.	·No usar el cifrado tipo EXPORT. ·Utilizar navegadores invulnerables, como puede ser Firefox. ·Usar TLS 1.2 o posterior, desacctivando antes SSL.
SWEET32	Sistemas que cifran por bloques, como AES, para encriptar datos cliente-servidor. Si son bloques pequeños, se van a considerar vulnerables a ataques de tipo 'BIRTHDAY'. Esto puede usarse si la clave que quieren averiguar es enviada en cada petición. Un MITM puede generar muchos mensajes con las caracteristicas dichas anteriormente. Ataque a los cifrados simétricos de bloques de 64-bit, TLS y OpenVPN están afectados.	Para efectuar el ataque en cifrado por bloques de 64 bits, se necesitan capturar por lo menos 32 GB en la red. En caso de SSL/TLS esto significaría una versión SSL/TLS individual. . Por lo tanto, las conexiones de larga duración podrían ser vulnerables. Se puede acabar descifrando partes de los bloques enviados entre el cliente y el servidor.	·Actualizar las claves con frecuencia, para que no sean vulnerables. ·Aumentar el tamaño de los bloques de 64 bits y actualizar el codigo.
SLOTH	Este ataque aprovecha el uso de algoritmos de hash que estén obsoletos, como son MD5 o SHA-1, en base a una serie de ataques complejos.	Como tiene partes vulnerables los sistemas que usen MD5 o SHA-1, se consigue acceso al sistema y esto puede producir la vulnerabilidad de las partes más importantes del sistema y con eso, hacen al sistema mas inseguro.	·Usar TLS posterior a 1.3 ·No usar MD5 o SHA-1 al estar obsoletos, y actualizar las partes es las que usen por código.