7. ¿Qué es el Protocolo HTTPS?, ¿Cuáles son sus características? Ejemplifica.

Antes de nada, es importante que tengamos claro el significado de **HTTP**. Es el acrónimo de **Hypertext Transfer Protocol** (se puede traducir al español como *protocolo de transferencia de hiper texto*).

HTTPS es lo mismo, con la salvedad de que se le añade el término "**seguro**".
En ambos casos, estamos hablando de un protocolo que define la manera en la que viajan los datos a través de Internet.

- En el caso de que se utilice el protocolo HTTP, los datos serán accesibles para cualquier persona que pueda captar la comunicación, por lo que no se considera la forma más efectiva de hacerlo.
- Por su parte, el **protocolo HTTPS** utiliza una conexión segura ya que se basa en el sistema de cifrado **SSL**. Esto permite que los datos puedan viajar de manera segura de un dato a otro, y que no puedan ser captados por cualquiera.

Para entender mejor **qué es el protocolo HTTPS**, es importante saber cómo funciona:

- Abrimos una página de Internet y el navegador intentará conectarse a un sitio que ha sido protegido con SSL.
- El navegador requerirá que el servidor web se identifique.
- Será así como el servidor mandará una copia de su **certificado SSL** a nuestro navegador.
- El navegador, una vez ha recibido la copia, comprobará si el sitio web es de confianza. Si es así, manda un mensaje que lo acredita.
- El servidor mandará un **acuse de recibo con firma digital** que permitirá que se inicie la conexión cifrada.
- Así es como empezarán a transferirse datos cifrados entre el servidor y el navegador.

¿Cómo surgió HTTPS?

El **HTTP**, el protocolo clásico en el que se basa la navegación web, sería inventado entre los años **1989-1991** por **Tim Berners-Lee**. Este protocolo ha ido cambiando bastante a lo largo de los años debido a las necesidades emergentes.
En sus orígenes, este protocolo fue diseñado para intercambiar archivos en un entorno controlado, en un laboratorio. Ahora se utiliza para intercambiar todo tipo de ficheros (imágenes, textos, vídeos de alta resolución, entre un largo etcétera) a través de una red infinitamente más grande.
Ya te habrás dado cuenta de que al navegar en los sitios más conocidos (cómo puede ser el caso de **Google** o redes sociales como Twitter o Facebook), el protocolo que se emplea no es HTTP, si no **HTTPS**, combinándolo con el protocolo **TLS** (siglas de *Transport Layer Securitu*).

Para comprender el inicio del HTTPS es necesario hacer un viaje en el tiempo al año **1994**. Por aquel entonces, la compañía **Netscape**, conocida por haber diseñado el navegador homónimo, creó **SSL v2**.

Se trataba de un protocolo de cifrado que había sido diseñado con el objetivo de dar protección a las comunicaciones a través de Internet. Sin embargo, este protocolo todavía tardaría un año para ser integrado en el **navegador Netscape Navigator en su versión 1.1**.

Este momento del tiempo fue muy importante, ya que sería la primera vez que se podría navegar por Internet con un protocolo de cifrado. En aquel momento no era demasiado importante, pero hoy en día ya es imprescindible.

Como primera versión, **SSL v2 presentó importantes problemas de seguridad**. Netscape no tardaría demasiado en hacer las correcciones pertinentes, y es así como lanzaría la siguiente versión, la **SSL V3**.

Durante muchos años se estuvo usando este sistema de seguridad.
De hecho, las versiones más avanzadas todavía tienen su vale en **SSL 3.0**. Sin embargo, algunos expertos recomiendan el uso del protocolo TLS, que es una evolución del protocolo SSL.

¿Para qué sirve el protocolo HTTPS?

1. **Creación de un canal encriptado**

El HTTPS permite dar forma a un canal encriptado para trabajar con aquella información que es más sensible.
Eso sí, habrá que tener en cuenta que el nivel de cifrado estará supeditado al navegador que se utilice y el servidor remoto con el que se está interactuando.

2. **No hará falta usar ningún software adicional**

Al usar el protocolo no será necesario instalar ningún tipo de software o funcionalidad adicional. Por ello, será utilizable por cualquier tipo de navegante sin ninguna restricción. Tal y como veremos a continuación cuando hablemos de las ventajas del HTTPS, esto es muy interesante, ya que ayuda a fomentar la confianza en el cliente, elevando las posibilidades de que se produzca la conversión deseada.

3. **Total integración**

El protocolo HTTPS ser competible sin ningún tipo de problema con la mayoría de los navegadores web actuales, como:

- Mozilla Firefox
- Google Chrome
- Microsoft Edge
- Opera
- Safari

4. **Identificación inequívoca de que la web es segura**

Lo más habitual es que aparezca un rasgo distintivo en el navegador que nos indique que la página es segura. Suele ser un **pequeño candado que se sitúa en la zona izquierda en la barra de direcciones**.

Además, el término HTTPS aparecerá en la dirección URL, elevando todavía más la confianza del usuario.

5. **No almacena contenido en caché**

La información que se transmite a través del protocolo HTTPS no almacena ningún tipo de información en caché. Sin embargo, esto podría ser una ventaja o un inconveniente, dependiendo de la situación.
El hecho de que no se almacene en caché es interesante porque no quedan datos residuales a los que se pueda acceder para intentar vulnerarlos. A cambio, la página tardará más tiempo en cargarse (cuestión de milisegundos).

6. **Proceso de verificación complejo**

En el caso de que una persona no autorizada consiga obtener los datos que han sido transmitidos a través de este protocolo, no será capaz de descifrar la información debido a que le llegará encriptada.

Ventajas:

1. **Ayuda a mejorar la privacidad de los datos de tus clientes**

Si decides hacer el cambio a este protocolo, estarás incorporando una **capa de cifrado a los datos** que los usuarios van a introducir en tu web y con los que va a interactuar. Por ejemplo, podríamos estar hablando de sus datos personales, dirección, incluso de su información bancaria.
A nadie le gustaría que estos datos pudieran caer en malas manos, sin hablar de las responsabilidades legales que esto entrañaría.
Con el protocolo HTTPS se consigue que los datos de la web queden encriptados y que nadie pueda tener acceso a los mismos, aunque encontrase la manera de acceder.

También debemos tener en cuenta que no solo se protege el sitio web, sino también la **URL al completo**. Esto quiere decir que protege tanto los datos personales que se escriben en el momento del registro, las contraseñas introducidas, los parámetros que se envían y se reciben, las *cookies*, etc.

2. **Mejora la protección contra ataques externos**

Cómo ya hemos indicado en el apartado anterior, confiar en el **protocolo HTTPS** significa que dotaremos a nuestra web de una capa de protección extra que elevará la seguridad mediante el recurso de la encriptación.
Las defensas de la página se verán reforzadas, así que podrá defenderse mejor frente a ataques como *Ransomware*, *Malwares*, o cualquier otro tipo de software relacionado. Digamos que cerramos las vías de entrada que usan estos sistemas infecciosos para acceder a nuestra web.
El negocio online, más allá de a lo que se dedique y de su reputación, **tendrá más seguridad**. Así tendrá un camino más llano que le orientará hacia el éxito.

3. **Mejora la credibilidad y confianza de la plataforma**

Los usuarios cada vez se toman más en serio la seguridad al **comprar online**, y no es para menos. Hay muchas páginas fraudulentas que tan solo buscan hacerse con datos personales o con el dinero de los internautas.
Si entras a una página web y **te encuentras con el mensaje de no es seguro** (que es el que te puede indicar un navegador como *Chrome*) puede ser el motivo que haya que el visitante no confíe en la web y no complete la venta o ni tan siquiera llegue a registrarse.
Gracias al certificado SSL, y a hacer el cambio de **HTTP** a **HTTPS**, podremos presentar una web totalmente legítima que indicará que somos reales y que realmente se puede confiar en nosotros.
Así lograremos **mejorar la reputación online** y nuestra **imagen digital** en general.

4. **Ayuda a mejorar el posicionamiento SEO**

Aunque de esto hablaremos más adelante, en la sección correspondiente, es una ventaja que no podemos pasar por alto.
Google se toma muy en serio que Internet sea lo más seguro posible y pone todo su empeño en hacer que las páginas se cambien al protocolo seguro.
Por esta razón, podrías estar perdiendo posiciones en los resultados de búsqueda (o SERP) si todavía estás usando el protocolo HTTP. Por mucho que estés trabajando en otros criterios relativos al Posicionamiento SEO u orgánico, necesitas hacer el cambio a HTTPs ya mismo.

5. **Te encaminará hacia el éxito**

Las ventajas del protocolo HTTPS ya descritos harán que tu web sea un sitio seguro, legítimo, en el que se puede confiar y mejorará su posicionamiento SEO.
No importa qué tipo de tienda online, blog, web corporativa o proyecto tengas, ya que es necesario hacer el cambio a HTTPs (se tiene que ver como algo básico).
Y es que son muchas las cosas que están en juego, como es el caso de la imagen del negocio, el tráfico y elevar las posibilidades de que se produzcan conversiones.

Cualquier criterio que pueda mejorar el impacto de tu proyecto online debe ser tenido en cuenta.

Desventajas:

Sin embargo, también existen algunas desventajas del protocolo HTTPS, aunque no es algo que se pueda considerar irremediable.
Estas son las 3 desventajas más destacadas:

1. **Errores 404**

- **Si empiezas tu proyecto web directamente con el protocolo HTTPS** activo, puedes obviar este punto porque no te interesa.
- Sin embargo, si se hace la **migración del sitio web a HTTPS**, se cambiarán todas las URLs de la web (piensa qué en vez de comenzar por HTTP, empezarán por HTTPS). Esto es muy importante, ya que tu cliente se podría encontrar con errores 404 si no se han hecho las redirecciones adecuadas.

No es que sea algo muy complicado, pero requiere de unos conocimientos técnicos medios-avanzados que no tienen todos los usuarios.

2. **Dificultades a la hora de migrar**

El propio proceso de migración también entraña una serie de dificultades que habrá que solventar, y que no siempre son intuitivas. Por ejemplo, podríamos estar hablando de:

- Problemas de enlaces (cómo ya hemos indicado).
- Cómo manipular el archivo *robots.txt* (por si tenemos que bloquearlo para evitar contenido duplicado u otros problemas).
- Cualquier mensaje de alerta que pueda ocurrir en la web.

Todo esto se puede confiar en una empresa que se encargue de efectuar la migración por ella misma. Así, nos aseguramos de que la página sea plenamente funcional y no afecte a la experiencia del cliente.

3. **Cambios en el rendimiento web**

La verdad es que **el protocolo HTTPS requiere de más recursos que el protocolo HTTP**. Hay que tener en cuenta que, si nuestro rendimiento con este último protocolo no era bueno, lo más probable es que empeore todavía más a la hora de hacer el cambio.
No obstante, este es un problema urgente a arreglar, ya que nos va a afectar en más de lo que pensamos.
Por ejemplo, podría ser que la página fuese tan lenta que los clientes se desesperen cada vez que van a comprar, y que Google nos penalice por trabajar con velocidades tan reducidas.

¿Qué relación guarda el HTTPS con “SSL”?

El protocolo HTTPS pertenece a la capa de aplicación del modelo OSI. Para poder cumplir con su función de protección, necesita de un **certificado SSL/TLS**.

El certificado SSL se encuentra dentro de la capa de sesión en el modelo OSI, mientras que el protocolo TLS se localiza en la capa de transporte.

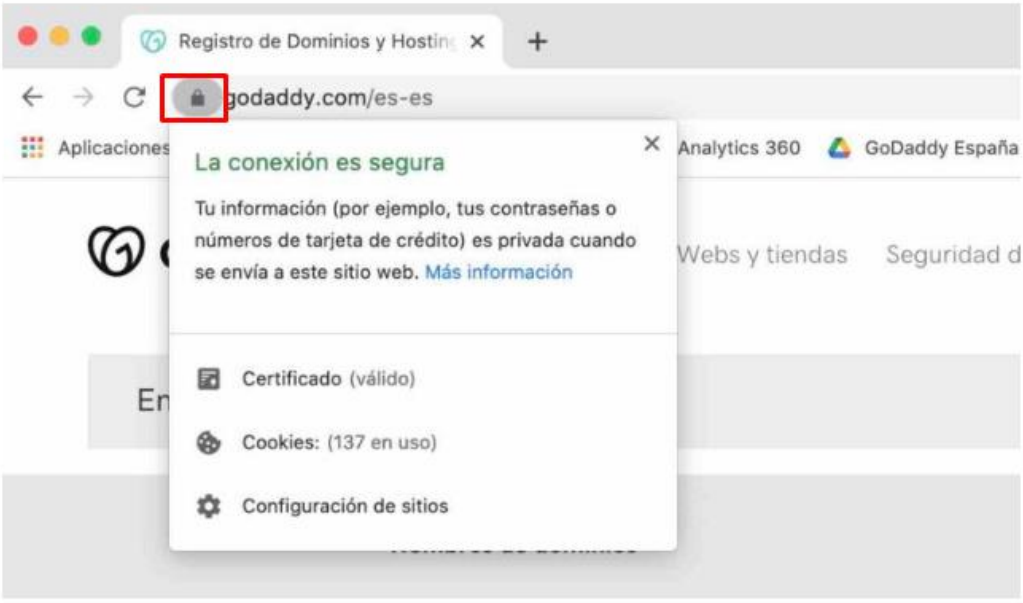
Estos certificados se emplean cuando se produce intercambio de información sensible o personal, cómo podría ser la introducción de contraseñas para acceder a páginas en donde los datos podrían ser robados (como la página web de una entidad bancaria).

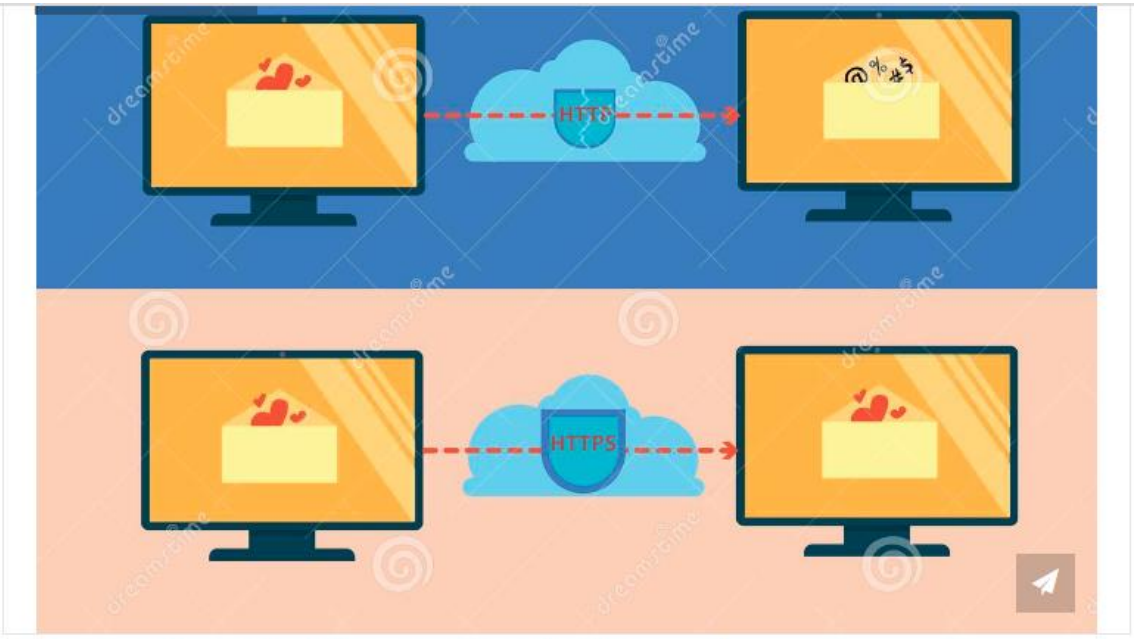
Con la combinación de HTTPS + SSL/TLS vas a poder conseguir mejorar la seguridad de los navegantes en tu sitio web.

¿Qué datos protege el protocolo SSL?

Este protocolo te protege de los siguientes 3 tipos de datos:

- **De cifrado:** al cifrar los datos que se intercambian en un sitio web conseguimos que estén protegidos ante *miradas indiscretas*. En otras palabras: mientras el usuario está navegando a través de una web, no habrá nadie que pueda tener acceso a la información con la que está interactuando. Tampoco podrá llevar a cabo un seguimiento de las actividades mediante las páginas que visita ni robar información.
- **Integridad de la información:** este protocolo también asegura que los datos no podrán ser modificados o sufrir algún tipo de daño mientras se están transfiriendo, con independencia de que este daño pueda haber sido intencionado o no. En determinados casos, sí que podría producirse un daño, pero el protocolo SSL sería capaz de detectarlo.
- **Autentificación:** la **autentificación** es un recurso que se emplea para demostrar que los usuarios se pueden comunicar con la página web en cuestión. Blinda la página ante ataques y ayuda a elevar la confianza del navegante. Esto redunda en que se eleve la posibilidad de que se produzca la conversión por parte del cliente.





Ejemplo de los ejemplos planos del vector de la seguridad del HTTP y de los https