UNIVERSIDAD DE SALAMANCA

FACULTAD DE TRADUCCIÓN Y DOCUMENTACIÓN

GRADO EN INFORMACIÓN Y DOCUMENTACIÓN

TRABAJO DE FIN DE GRADO

SEGURIDAD DE LA INFORMACIÓN

Intercambio de datos seguro

Alumno: Henar Sánchez Peña

Tutor: Ángel Luis Sánchez Lázaro

Salamanca, 2017

UNIVERSIDAD DE SALAMANCA

FACULTAD DE TRADUCCIÓN Y DOCUMENTACIÓN

GRADO EN INFORMACIÓN Y DOCUMENTACIÓN

TRABAJO DE FIN DE GRADO

SEGURIDAD DE LA INFORMACIÓN

Intercambio de datos seguro

Alumno: Henar Sánchez Peña

Tutor: Ángel Luis Sánchez Lázaro

Salamanca, 2017

Asiento bibliográfico

SANCHEZ PEÑA, Henar

Seguridad de la información. Intercambio de datos seguro.

Sánchez Lázaro, Ángel Luis. P. 52

RESUMEN

Internet es una herramienta muy útil hoy en día, que permite realizar una gran variedad de gestiones sin salir de casa, pero también es un arma de doble filo, ya que la información que se introduce en los sitios web puede ser interceptada por personas malintencionadas para hacer un uso fraudulento de esos datos.

Para evitar esas acciones, intervienen los protocolos de seguridad, es por eso que son tan importantes los sistemas de cifrado y juegan un papel primordial en el intercambio de información.

Palabras clave: protección, internet, seguridad, protocolos, cifrado.

SUMMARY

Internet is a very useful tool today, that allows carry on a great variety of paperwork without go out of home, but also is a doublé-edged sword, because the information that it's being introducing on a web page could be intercept by malicious people to make fraudulent use of that data.

To avoid that actiones, intercede the security protocols,is because of that are so important the encrypted system and plays a essential role in the Exchange of information.

Key words: protection, internet, security, protocols, encode.

Sumario

INTRODUCCIÓN

El principal propósito de este trabajo ha sido demostrar la importancia que tienen las técnicas de cifrado hoy en día en que la mayoría de la gente realiza gestiones cotidianas, como consultar el saldo bancario o hacer comprar por internet, para proteger sus datos personales y que no puedan caer en manos de personajes ajenas que puedan utilizarlos para fines malintencionados.

Para la realización del trabajo, se ha hecho un recorrido por las distintas técnicas de cifrado y su evolución a lo largo del tiempo para demostrar que, no solo son útiles en la actualidad debido a la gran información que se almacena en los ordenadores, sino también a lo largo de la historia para la protección de información.

La metodología empleada ha sido la búsqueda de información sobre el cifrado y los distintos tipos que hay y ha habido para introducir en la materia de la protección de la información.

Una vez vista de forma teórica la materia, se ha realizado un pequeño trabajo de campo para dar a conocer las aplicaciones prácticas de los métodos de cifrado y como pueden variar de un navegador a otro en un mismo sitio web.

ENCRIPTACIÓN Y DESENCRIPTACION

La criptografía[1], cuyo significado "escritura oculta", proviene del griego *krypto,* «oculto», y *graphos*, «escritura», es un conjunto de técnicas y procedimientos utilizados para cifrar textos y que no puedan ser comprendidos por personas ajenas. Las técnicas de criptográficas han sido utilizadas a lo largo de la historia durante cientos de años, en los cuales ha ido evolucionando con los avances de la tecnología y sigue haciéndolo día a día gracias a internet y su gran expansión.
A su vez, exigido por los avances en internet, ha sido necesaria la creación de nuevas formas de encriptación ya que el acceso a la información está al alcance de un gran número de usuarios, además de datos de carácter personal, haciendo al mismo tiempo necesaria la formulación de nuevas leyes de protección de datos.

HISTORIA DE LA CRIPTOGRAFÍA

Inicios de la encriptación

Los inicios de la encriptación se remontan al siglo I a.C. con el general romano Julio César y la creación de un sistema de sustitución de letras, cuyo método de encriptación consistía en sustituir la letra que se quería escribir por la tercera letra que le seguía en el alfabeto (A- D, B- E, ...)
El siguiente gran momento de desarrollo para la criptografía tuvo lugar en la Edad Media, siglo VI d.C., en el cual se cifraban los textos con propósitos militares y políticos.

Primeros métodos de cifrado

La primera publicación sobre criptografía conocida fue la de León Battista Alberti, a quien se le considera el padre de la criptografía moderna, con su "*Tratado de cifras",* publicado en 1470.

Ilustración 1 - Disco de Alberti

En este libro aparece el primer encriptado por sustitución poli alfabético, cuyo método

[1] Otro término que se puede utilizar para hacer referencia a la criptografía y sus técnicas es el de cifrado.

de encriptado y desencriptado consistía en la utilización de unas herramientas llamadas *«discos de Alberti»*.

Estos discos consistían en dos piezas circulares, una fija exterior con los caracteres del alfabeto latín en mayúsculas grabados y a continuación los números de 1 al 4, y una pieza interior móvil con otro alfabeto grabado.
De esta forma, girando el disco móvil, emparejaba las letras del alfabeto fijo con la letra interna del disco que coincidiese, dependiendo del número de giros que la persona que quería ocultar el mensaje quisiese asignarle.

Posteriormente, aparecieron nuevas técnicas como la Tabla de Porta, cuyo creador es Giovanni Battista Porta o el Método de Vigenère, perteneciente al diplomático francés Blaise de Vigenère, en el que se utiliza una tabla de 26 alfabetos posibles con un desplazamiento unitario en cada fila.

	ENTRADA TEXTO PLANO																								
ENTRADA CLAVE	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Ilustración 2 - Cuadro de Vigenére

El cifrado y descifrado de textos utilizando esta tabla es relativamente sencillo: se sitúa el mensaje en una línea y la clave repetida tantas veces como sea necesario en la línea

siguiente, a la altura del mensaje original y empezando por la misma posición. El carácter cifrado vendrá dado por la intersección de los caracteres del mensaje en claro y la clave.
El descifrado se realiza de la misma manera únicamente variando la utilización del mensaje cifrado en lugar del original, y de la columna de clave de descifrado en lugar de la de cifrado.

De esta última técnica surgieron diversas variantes como el *Cifrado de Beaufor,* el *Cifrado Playfair* o el *Cifrado Hill*.

I y II Guerra Mundial

Durante la I Guerra Mundial, el descifrado del *Telegrama de Zimmerman* fue crucial, ya que, gracias al Servicio de Inteligencia Naval de Inglaterra, se pudo informar a Estados Unidos de que al embajador alemán que se encontraba en México se le concedía permiso para negociar un acuerdo con México, ofreciéndole los territorios de Nuevo México, Arizona y Texas a cambio de que interviniesen en el conflicto a favor de Alemania.

En la II Guerra Mundial también ejercicio un papel importante el cifrado, en este caso de la mano de la máquina enigma y su descifrador, Alan Turing. Se trata de una máquina utilizada por la Alemania nazi tanto para cifrar como para descifrar mensajes. Está compuesta por varios rotores conectados entre sí. Cada rotor era un disco circular plano con 26 contactos eléctricos en cada cara, uno por cada letra del alfabeto. Cada contacto está conectado por un circuito eléctrico con otro de otra cara, lo que hace que se ilumine el teclado eléctrico con una letra que, aparentemente, no tiene ninguna conexión con la pulsada.

Encriptación actual

En la época actual, en la en su mayoría la información se encuentra informatizada y en la que, prácticamente todo el mundo dispone desde sus dispositivos de conexión a internet, la encriptación sigue siendo un factor fundamental, principalmente durante el intercambio de información para evitar que esta sea interceptada en el proceso por terceras personas ajenas a esta.
Una de las formas más eficaces y seguras de proteger la información, es cifrándola como paso previo a su almacenamiento en los discos duros y Pen Drives. Existen

numerosos productos en el mercado que permiten tales funciones, basándose la mayoría de ellos en algoritmos conocidos y otros de algoritmos de propietarios desconocidos, de cuya eficacia no se puede estar seguro.
Los ordenadores realizan el cifrado de la información mediante la aplicación de un algoritmo a cada bloque de datos que se va a cifrar. Un algoritmo es simplemente un conjunto de reglas que define un método para realizar una tarea determinada.

SISTEMAS DE CIFRADO

Los algoritmos de cifrado no serían de mucha utilidad si siempre entregasen el mismo texto cifrado como salida de un texto claro determinado, para asegurar que esto no ocurre, cada algoritmo de cifrado necesita una clave de cifrado. El algoritmo utiliza, por tanto, la clave de cifrado que es cambiada regularmente, como parte del proceso de cifrado.
Otro punto importante del cifrado es el del tamaño del bloque de datos que se va a cifrar cada vez, y del tamaño de la clave que se va a utilizar. Esto influye en que el algoritmo de cifrado pueda ser quebrado o no y, por tanto, averiguado el texto original sin necesidad de conocer la clave de cifrado.
El cifrado se puede utilizar de forma muy efectiva para la protección de los datos almacenados en discos duros, de los datos transmitidos entre ordenadores, para asegurar la integridad de la información, confirmar la identidad de un usuario, ...
No obstante, el cifrado debe aplicarse sólo a aquella información que realmente necesita ser protegida, puesto que tanto el proceso de encriptación como de des encriptación conllevarían un largo periodo de tiempo que podría considerarse perdido.
Los tipos de cifrado serían dos:

- Cifrado simétrico
- Cifrado asimétrico

- ***Cifrado simétrico***

Un algoritmo simétrico de cifrado es aquel que requiere la misma clave para el cifrado que para el descifrado. Esta definición cubre la mayor parte de los algoritmos utilizados en la historia hasta la aparición de la criptografía de clave pública.
Las reglas que definen un algoritmo de cifrado simétrico, contienen la definición de longitud de clave que se va a utilizar, y la longitud de bloque que se va a cifrar para cada ejecución del algoritmo de cifrado.
El algoritmo de cifrado toma una clave de cifrado y un bloque de texto en claro, aplica el algoritmo de cifrado y produce un bloque de texto cifrado.

El descifrado simétrico toma un bloque de texto cifrado y la clave que se utilizó para realizar el cifrado, aplica el inverso del algoritmo de cifrado, obteniendo el bloque de texto original.

Algunos ejemplos de sistemas de cifrado simétrico son: AES, DES, IDEA, ...

- AES

AES (Advanced Encryption Standard) es un algoritmo de cifrado por bloques, inicialmente diseñado para tener longitud de bloque variable pero el estándar define un tamaño de bloque de 128 bits, por lo tanto, los datos a ser encriptados se dividen en segmentos de 16 bytes (128 bits) y cada segmento se puede ver como un bloque o matriz de 4x4 bytes.

- DES

DES (Data Encryption Standard) es un sistema de cifrado de clave simétrica de cifrado de bloques, quiere decir que opera sobre bloques de tamaño fijo. Convierte bloques de 64 bits de texto claro en bloques de 64 bits de texto cifrado y viceversa. Las claves que utiliza también son de 64 bits.

- IDEA

IDEA (International Data Encription Algorithm) es un algoritmo de cifrado similar, en su estructura general, al DES. Basa su fortaleza la utilización de tres operaciones diferentes: OR-exclusivo, adición modular y multiplicación modular. Adicionalmente utiliza una clave de 128 bits.

- ***Cifrado asimétrico***

Un cifrado asimétrico requiere un par de claves, una para el cifrado y otra para el descifrado. La clave de cifrado es pública y está libremente disponible para cualquiera que quiera utilizarla, mientras que la clave de descifrado se mantiene en secreto, esto significa que cualquiera puede utilizar la clave de cifrado para la realización del mismo, pero el descifrado únicamente lo podrá realizar aquella persona que conozca la clave de descifrado.
Esto implica que cualquiera que posea un sistema de este tipo, puede recibir mensajes cifrados con su clave pública provenientes de cualquier interlocutor, pero únicamente el propietario de la clave privada será capaz de descifrarlo.
Esta es una gran ventaja sobre el sistema de cifrado simétrico, ya que cuando se transmite información protegida entre dos ubicaciones no es necesario que ambas

tengan la misma clave, únicamente es necesario que el receptor posea la clave secreta, lo cual es ventajoso desde el punto de vista del administrador de claves.
La mayor desventaja del sistema se presentaría en el tiempo de cálculo y la potencia que requieren que se emplee, lo que hace que su utilización se centre, principalmente, en sistemas de distribución de claves.
El cifrado asimétrico, toma una clave de cifrado y un bloque de texto, aplica el algoritmo de cifrado y produce un bloque de texto cifrado.
El descifrado asimétrico toma un bloque de texto cifrado y la clave de descifrado, aplica el algoritmo de descifrado, obteniendo el bloque de texto original.

- RSA

RSA (Rivest, Shamir y Adleman) es el algoritmo asimétrico más conocido y usado de los sistemas de clave pública. Presenta todas las ventajas de los sistemas asimétricos, incluyendo la firma digital.

Firma digital

La firma digital es un mecanismo de cifrado que permite al receptor de un mensaje, firmado digitalmente, identificar a la entidad creadora de dicho mensaje y confirmar que el mensaje no ha sido alterado desde que fue firmado por el creador.
La firma digital es una de las ventajas que ofrece el cifrado asimétrico, ya que gracias a este sistema se comenzó su desarrollo.
Este método permite no solo verificar la originalidad del mensaje, sino también la identidad del receptor. Dado un texto, basta calcular su huella digital y cifrarla con la clave secreta del remitente para obtener simultáneamente la seguridad de que el contenido no se manipula (integridad), y de que el firmante es quien dice ser (autenticación).

Protección de las claves

Al estar tratando los tipos de cifrado con claves es conveniente añadir un punto, que puede considerarse importante, sobre las claves y su protección.
Una vez generadas las calves de cualquier sistema de cifrado la administración de estas es un factor clave ya que, aunque la información esté cifrada con el mejor sistema del mundo, de nada sirve para su confidencialidad si las claves no están a bien protegidas.
Las claves de cifrado deberán estar cifradas a su vez como paso previo a su distribución o almacenamiento, de esta forma se podrá utilizar cualquier canal para su distribución.
Normalmente se suele utilizar un sistema de cifrado de clave pública para realizar el cifrado de las claves.

Autentificación

El método más simple de actualización consiste en la utilización de contraseñas, que son claves secretas. El punto débil de este sistema es que un servidor malicioso puede usurpar la identidad del usuario.

La utilización de firmas digitales es un método más seguro debido a que solo el poseedor de la clave secreta puede firmar con esa clave, mientras que cualquiera que sea consciente de la clave pública puede comprobar la identidad del firmante.

Certificados

La certificación es lo que aporta la fiabilidad a la autentificación de las personas físicas asociando de forma correcta las claves públicas y privadas con las personas físicas o jurídicas correspondiente, se podría decir que, las autoridades de certificación son una especie de "notarios electrónicos", entes fiables y reconocidos que firman las claves públicas de los usuarios, rubricando con su firma de identidad.

PROBLEMAS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACION

La seguridad en la web es el conjunto de medidas de protección que se toman para proteger todos los elementos que forman parte de la red como infraestructura e información, que son las partes que se ven más afectadas por los ataques de los delincuentes cibernéticos.
La seguridad informática se encarga de crear métodos, procedimientos y normas que logren identificar y eliminar vulnerabilidades en el almacenamiento y los intercambios información y los equipos físicos.
Cuatro son los problemas principales que afectan a los sistemas de información:

- Interrupción
- Intercepción
- Modificación
- Fabricación

❖ ***Interrupción***

La información es corrompida para que los datos queden en un estado inutilizable, haciendo que el sistema quede detenido durante un periodo de tiempo más o menos largo

❖ ***Intercepción***

Una tercera persona, no autorizada, consigue acceder a la información o al sistema. Puede ser una persona, programa o sistema informático.
Una vez intervenida esa información puede ser utilizada de forma mal intencionada de múltiples formas, uno de los usos más frecuentes es el uso de los datos de acceso con la intención de hacer pensar al sistema que se está identificando un usuario de confianza para fines malintencionados.

❖ ***Modificación***

La parte no autorizada que ha conseguido acceder, toma control sobre los datos o el sistema realizando cualquier tipo de cambio en este.

❖ ***Fabricación***

Una parte no autorizada fabrica información o archivos falsificados y los introduce en el

sistema.

Algunos conceptos a tener en cuenta a la hora de hablar de seguridad en la red serían:

- Vulnerabilidad: es una debilidad del sistema de seguridad que puede ser explotada para causar pérdidas o daños.

- Amenazas: son circunstancias que constituyen una causa potencial de pérdida o daño: errores humanos inadvertidos y fallos internos de hardware o software.

- Medida de protección: acción, dispositivo, procedimiento o técnica que reduce una vulnerabilidad.

- Confidencialidad: la información será obtenida únicamente por los usuarios autorizados.

- Disponibilidad: la información será accesible por los usuarios autorizados con facilidad y en tiempo adecuado.

Niveles de seguridad

Según la "Guía de Seguridad de Datos" redactada por la *Agencia Española de Protección de datos*, existen tres niveles de seguridad, en la que se distribuyen los ficheros o datos atendiendo al tipo de datos que contengan en su interior. Estos niveles de seguridad, que se detallan a continuación, están determinados por el Reglamento de desarrollo de la Ley Orgánica de Protección de datos de carácter personal(RLOPD):

- **NIVEL ALTO.** Ficheros o tratamientos con datos:

  - de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual y respecto de los que no se prevea la posibilidad de adoptar el nivel básico;

  - recabados con fines policiales sin consentimiento de las personas afectadas;
  - derivados de actos de violencia de género.

- **NIVEL MEDIO.** Ficheros o tratamientos con datos:

  - relativos a la comisión de infracciones administrativas o penales;
  - que se rijan por el artículo 29 de la LOPD (prestación de servicios de solvencia patrimonial y crédito);
  - de Administraciones tributarias, y que se relacionen con el ejercicio de sus potestades tributarias;
  - de entidades financieras para las finalidades relacionadas con la prestación de servicios financieros;
  - de Entidades Gestoras y Servicios Comunes de Seguridad Social, que se relacionen con el ejercicio de sus competencias;
  - de mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social;
  - que ofrezcan una definición de la personalidad y permitan evaluar determinados aspectos de la misma o del comportamiento de las personas;
  - de los operadores de comunicaciones electrónicas, respecto de los datos de tráfico y localización

- **NIVEL BÁSICO.** Cualquier otro fichero que contenga datos de carácter personal. También aquellos ficheros que contengan datos de ideología, afiliación sindical, religión, creencias, salud, origen racial o vida sexual, cuando:

  - los datos se utilicen con la única finalidad de realizar una transferencia dineraria a entidades de las que los afectados sean asociados o miembros;
  - se trate de ficheros o tratamientos de estos tipos de datos de forma incidental o accesoria, que no guarden relación con la finalidad del fichero;
  - en los ficheros o tratamientos que contengan datos de salud, que se refieran exclusivamente al grado o condición de discapacidad o la simple declaración de invalidez, con motivo del cumplimiento de deberes públicos.

Las medidas de seguridad de nivel básico son exigibles en todos los casos. Las medidas de nivel medio complementan a las anteriores en el caso de ficheros clasificados en este nivel, y las de nivel alto, cuando deban adoptarse, incluyen también las de nivel básico y medio.

Objetivos de seguridad

La seguridad en informática es el conjunto de procedimientos, estrategias y herramientas que permiten garantizar la integridad, disponibilidad y la confidencialidad de la información.

- Integridad: es necesario asegurar que los datos no sufran cambios no autorizados, la perdida de integridad puede tener como consecuencia los fraudes, decisiones erróneas o nuevos ataques.

- Disponibilidad: hace referencia a la continuidad operativa de la entidad. La pérdida de disponibilidad puede implicar la pérdida de productividad o de credibilidad de la entidad. El sistema contiene información o proporciona servicios que pueden estar disponibles a tiempo para satisfacer requisitos o evitar pérdidas importantes.

- Confidencialidad: se refiere a la protección de datos frente a la difusión no autorizada. Su pérdida puede ocasionar problemas legales o pérdida de credibilidad. Los sistemas contienen información que necesita protección contra la divulgación no autorizada, como información de carácter personal o informes.

Estos aspectos, además de tener que hacer frente a los ataques potenciales por parte de agentes remotos, también se ven amenazados por empleados poco leales, virus o sabotajes, por ejemplo.

Estrategias de seguridad

Los sistemas de seguridad utilizan una metodología para diseñar modelos de protección para desarrollar una estrategia para proteger los tres puntos principales de la seguridad de la información, anteriormente vistos: integridad, disponibilidad y confidencialidad.
Esto es primordial para los administradores, directores y demás personal encargado de la seguridad, ya que son los encargados de establecer las directivas de seguridad.
La metodología ofrece unas bases para la realización de esta importante tarea que es la protección de la información. No obstante, se han de establecer también planes de

contingencia, para que en el caso de que el sistema falle se tenga un plan de actuación ya establecido, puesto que ningún sistema de protección es infalible.
El tiempo, dinero y esfuerzo que se ha de invertir para desarrollar las directivas y controles de seguridad apropiados, a de proceder de los administradores encargados de la seguridad de cada sistema.

A la hora de desarrollar la metodología para establecer los modelos de seguridad, es necesario tener en cuenta los siguientes puntos:

- **Identificar métodos, herramientas y técnicas que puedan utilizar en posibles ataques.**

La lista de amenazas, de la que suelen disponer la mayoría de las organizaciones, ayudan a los administradores de seguridad a identificar los distintos métodos, herramientas y técnicas que podían utilizar en los ataques. Los potenciales ataques varían desde virus o gusanos a la adivinación de contraseñas e interceptación de intercambio de información. Es de vital importancia de los administradores actualicen constantemente sus conocimientos en estas áreas, ya que también la metodología de ataque evoluciona constantemente.

- **Establecer estrategias de defensa y reparación**

En cada modelo, se han de incluir estrategias de defensa, para defender el sistema frente a cualquier ataque, y de reparación, para hacer uso en el caso de que no se haya podido repeler el ataque.
La estrategia de defensa es un conjunto de pasos que ayudan a reducir al mínimo la cantidad de puntos vulnerables existentes en las directivas de seguridad y para el desarrollo de planes de contingencia. La determinación del posible daño que un ataque pueda provocar en un sistema, las debilidades y los puntos vulnerables durante los ataques serán de ayuda a la hora de elaborar estas estrategias.
Las estrategias de reparación o estrategia post-ataque se refiere a las directrices a seguir tras un ataque para la evolución del daño causado por este y/o reparar los daños causados en el sistema.

Es importante documentar los ataques indicando como y porque se han producido para así poder mejorar el sistema de defensa y prevenirlos en el futuro.

- **Evaluación**

Poner a prueba ambos sistemas de defensa y post-ataque es algo fundamental para

tener un buen sistema de seguridad, ya que evaluando estos sistemas se pueden observar sus puntos débiles y así poder repararlos mejorando ambos sistemas para que, durante su utilización, puedan afrontar la mayoría de ataques potenciales sin que lleguen a causar daños en el sistema.
La realización de pruebas o ataques simulados permite localizar estas vulnerabilidades y ajustar así los controles de seguridad, en consecuencia.

PROTECCION DE DATOS

Según la Agencia de Española de protección de datos "sobre el responsable del fichero recaen las principales obligaciones establecidas por la LOPD y le corresponde velar por el cumplimiento de la Ley en su organización." El responsable debe:

- Notificar los ficheros ante el Registro General de Protección de Datos para que se proceda a su inscripción.
- Asegurarse de que los datos sean adecuados y veraces, obtenidos lícita y legítimamente y tratados de modo proporcional a la finalidad para la que fueron recabados.
- Garantizar el cumplimiento de los deberes de secreto y seguridad.
- Informar a los titulares de los datos personales en la recogida de éstos.
- Obtener el consentimiento para el tratamiento de los datos personales.
- Facilitar y garantizar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.
- Asegurar que en sus relaciones con terceros que le presten servicios, que comporten el acceso a datos personales, se cumpla lo dispuesto en la LOPD.
- Cumplir, cuando proceda, con lo dispuesto en la legislación sectorial que le sea de aplicación.

Asociada a la figura del responsable, está la figura del encargado, que es la persona o entidad, autoridad pública, servicio o cualquier otro organismo que, sólo o con otros, trate datos por cuenta del responsable del fichero.
La realización de un tratamiento por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado tratará los datos conforme a las instrucciones del responsable, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.
No se considera encargado del tratamiento a la persona física que tenga acceso a los datos personales en su condición de empleado dentro de la relación laboral que mantiene con el responsable del fichero.
Ambos, encargado y responsable del tratamiento, pueden ser sancionados de acuerdo a la LOPD si incumplen sus obligaciones.

Una persona facilita sus datos personales cuando abre una cuenta en el banco, cuando

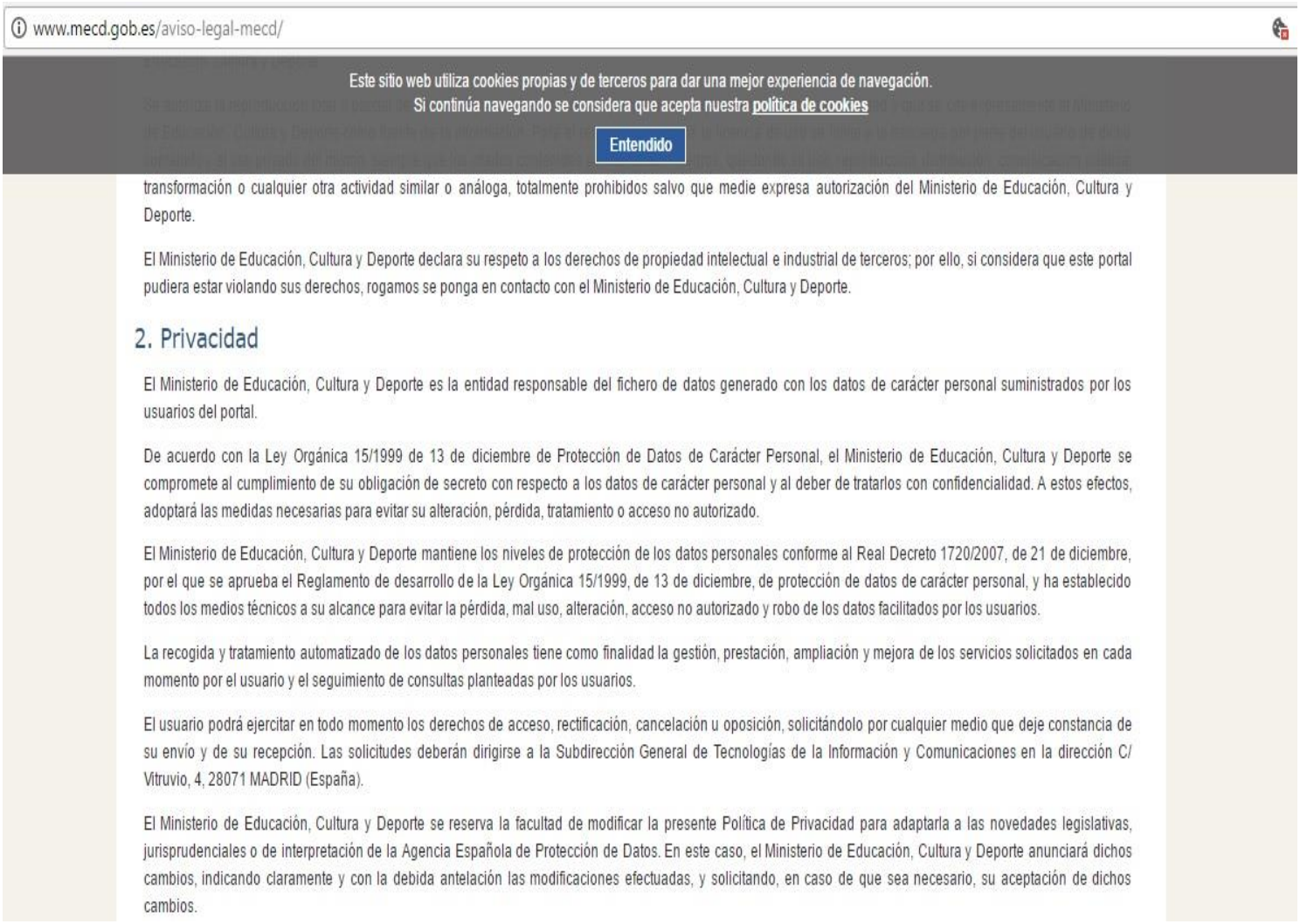
se matricula en un curso de idiomas, cuando se apunta al gimnasio, cuando solicita participar en un concurso, cuando reserva un vuelo o un hotel, cuando pide hora para una consulta médica, cuando busca trabajo, cada vez que efectúa un pago con su tarjeta de crédito, cuando navega por Internet….
La constante evolución de las nuevas tecnologías conlleva inevitablemente que toda la información se encuentre digitalizada, por lo que su tráfico, incluso a nivel global resulta mucho más sencillo. Los gobiernos nacionales y en especial la Unión Europea, han iniciado acciones conjuntas de cara a evitar, o en su caso frenar, el intercambio descontrolado y no autorizado de base de datos digitalizadas que contengan datos de carácter personal.

Legislación española sobre protección de datos
La normativa de protección parte de una serie de principios básicos dispuestos en los artículos 4, 5 y 6 de la LOPD que pueden resumirse en la obligación por parte de los Responsables de Fichero a que todas sus bases de datos deben cumplir con el principio de calidad de los datos, con el deber de información a los afectados, así como respecto a la regulación, legítima y no, del tratamiento que se lleve a cabo de dichos datos personales.
El Principio de Calidad de los datos, tiene como finalidad primordial evitar que se proceda a recopilar datos de forma masiva, sin ser estrictamente necesario para la finalidad originaria y que se aparte de la misma, destinándose a otras finalidades. Del mismo modo, es estrictamente obligatorio cancelar dicha base de datos, una vez haya desaparecido la finalidad para la cual fueron recabados y para la que el afectado prestó el consentimiento inicialmente.
Por otro lado, el principio de deber de información en la recogida de los datos obliga al responsable del Fichero, de forma previa a la recogida de los datos, a informar al titular respecto a:

- La existencia de un fichero en el que se tratan datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios.
- El carácter obligatorio de las respuestas a los apartados del formulario.
- Las consecuencias de la obtención de los da de la negativa a suministrarlos.
- La posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición.
- Los datos de la entidad que recaba los datos, o en su caso, de su representante.

Siempre debemos ser informados de forma previa respecto a cuál es la finalidad para la que se recaban nuestros datos de carácter personal, quién será el responsable del

Tratamiento y cuáles son los derechos de que disponemos.


www.mecd.gob.es/aviso-legal-mecd/

Este sitio web utiliza cookies propias y de terceros para dar una mejor experiencia de navegación.
Si continúa navegando se considera que acepta nuestra política de cookies

Entendido

transformación o cualquier otra actividad similar o análoga, totalmente prohibidos salvo que medie expresa autorización del Ministerio de Educación, Cultura y Deporte.

El Ministerio de Educación, Cultura y Deporte declara su respeto a los derechos de propiedad intelectual e industrial de terceros; por ello, si considera que este portal pudiera estar violando sus derechos, rogamos se ponga en contacto con el Ministerio de Educación, Cultura y Deporte.

2. Privacidad

El Ministerio de Educación, Cultura y Deporte es la entidad responsable del fichero de datos generado con los datos de carácter personal suministrados por los usuarios del portal.

De acuerdo con la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal, el Ministerio de Educación, Cultura y Deporte se compromete al cumplimiento de su obligación de secreto con respecto a los datos de carácter personal y al deber de tratarlos con confidencialidad. A estos efectos, adoptará las medidas necesarias para evitar su alteración, pérdida, tratamiento o acceso no autorizado.

El Ministerio de Educación, Cultura y Deporte mantiene los niveles de protección de los datos personales conforme al Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, y ha establecido todos los medios técnicos a su alcance para evitar la pérdida, mal uso, alteración, acceso no autorizado y robo de los datos facilitados por los usuarios.

La recogida y tratamiento automatizado de los datos personales tiene como finalidad la gestión, prestación, ampliación y mejora de los servicios solicitados en cada momento por el usuario y el seguimiento de consultas planteadas por los usuarios.

El usuario podrá ejercitar en todo momento los derechos de acceso, rectificación, cancelación u oposición, solicitándolo por cualquier medio que deje constancia de su envío y de su recepción. Las solicitudes deberán dirigirse a la Subdirección General de Tecnologías de la Información y Comunicaciones en la dirección C/ Vitruvio, 4, 28071 MADRID (España).

El Ministerio de Educación, Cultura y Deporte se reserva la facultad de modificar la presente Política de Privacidad para adaptarla a las novedades legislativas, jurisprudenciales o de interpretación de la Agencia Española de Protección de Datos. En este caso, el Ministerio de Educación, Cultura y Deporte anunciará dichos cambios, indicando claramente y con la debida antelación las modificaciones efectuadas, y solicitando, en caso de que sea necesario, su aceptación de dichos cambios.

Ilustración 3 - Privacidad de la página web de Ministerio de Cultura y Deporte

Como se puede ver en la ilustración anterior, las páginas web, por lo general, tiene un apartado dentro del sitio en el que aparece el uso que el sitio web puede hacer de los datos que los usuarios comparten con dicho sitio web y los derechos que tienen los usuarios sobre ellos.

PROTOCOLOS DE DEGURIDAD EN EL INTERCAMBIO DE INFORMACION

Es un hecho que las comunicaciones por medio de internet no son un medio seguro debido a que es vulnerable a ser interceptada por parte de atacantes informáticos. Los datos transmitidos entre dos puntos de la red son segmentados en pequeños paquetes, para facilitar su envío, que son transmitidos a través de nodos intermedios hasta llegar a su destino. En el transcurso del paso por cualquiera de estos puntos es posible que la información contenida en los paquetes sea interceptada para ser leída, destruida o modificada por atacantes, lo que pondría en riesgo la integridad y confidencialidad de los datos enviados. Por ello se crearon protocolos de seguridad, necesarios para garantizar el intercambio de datos seguros, sobre todo de carácter personal.
Uno de los protocolos más utilizados y que garantizan el mayor nivel de seguridad, en estos momentos, es el protocolo SSL (Secure Sockets Layer) que se va a ver en profundidad a continuación.

SSL (Secure Sockets Layer)

Se trata de una tecnología diseñada por NetScape Communications Inc. que dispone un nivel seguro de transporte entre el servicio clásico de transporte en Internet (TCP) y las aplicaciones que se comunican a través de él. Sin embargo, no fue hasta su tercera versión, conocida como SSL v3.0 que alcanzó su madurez, superando los problemas de seguridad y limitaciones de sus predecesores. SSL está incorporado a muchos navegadores, como por ejemplo el clásico Internet Explorer, entre otros.

Este protocolo, constituye la solución de seguridad implantada en la mayoría de los

Ilustración 4 - Sitio web seguro en varios navegadores

servidores web que ofrecen servicios de comercio electrónico.

En la imagen superior se muestra como los distintos navegadores tienen símbolos, más o menos similares, para indicar que el sitio web es seguro.
Las comunicaciones tienen lugar en dos fases. En una primera fase se negocia entre el cliente y el servidor una clave simétrica sólo válida para esta sesión. En la segunda fase, se transfieren datos cifrados con dicha clave. Este sistema es transparente para las aplicaciones finales, que simplemente saben que el canal se encarga de proporcionarles confidencialidad entre los nodos de inicio y fin.
La fase inicial se realiza muy cuidadosamente para evitar tanto la intercepción de terceras partes como para evitar suplantaciones de identidad por parte del servidor.
SSL está basado en la aplicación conjunta de criptografía simétrica (de llave secreta), criptografía asimétrica (de llave pública), certificados digitales y firmas digitales para conseguir un canal o medio seguro de comunicación a través de Internet.
Los sistemas simétricos de encriptación se utilizan como motor principal de la encriptación debido a su rapidez de operación. Por su parte, los sistemas asimétricos se usan para el intercambio seguro de las claves simétricas, consiguiendo con ello resolver el problema de la confidencialidad en la transmisión de datos.
La identidad de un sitio web seguro se consigue mediante el certificado digital correspondiente, del que se comprueba su validez antes de iniciar el intercambio de datos sensibles, mientras que de la integridad de los datos intercambiados se encarga la firma digital mediante funciones *hash* y la comprobación de resúmenes de todos los datos enviados y recibidos.
Un certificado digital es un documento digital generado por una autoridad de certificación (CA). Un certificado digital incluye el nombre del propietario del certificado (usuario que está siendo certificado), la clave pública de ese usuario, un número de serie, una fecha de expiración, la firma de los datos anteriores por la autoridad de certificación y cualquiera otra información relevante.
La autoridad de certificación es responsable de la autenticación, de manera que debe chequear cuidadosamente la información antes de publicar un certificado digital. Los certificados digitales están disponibles públicamente y son contenidos por las autoridades de certificación en repositorios de certificados.
La CA firma el certificado ya sea encriptado con la clave pública o un valor de hash de la clave pública, utilizando su propia clave privada. La CA tiene que verificar cada clave pública individual.

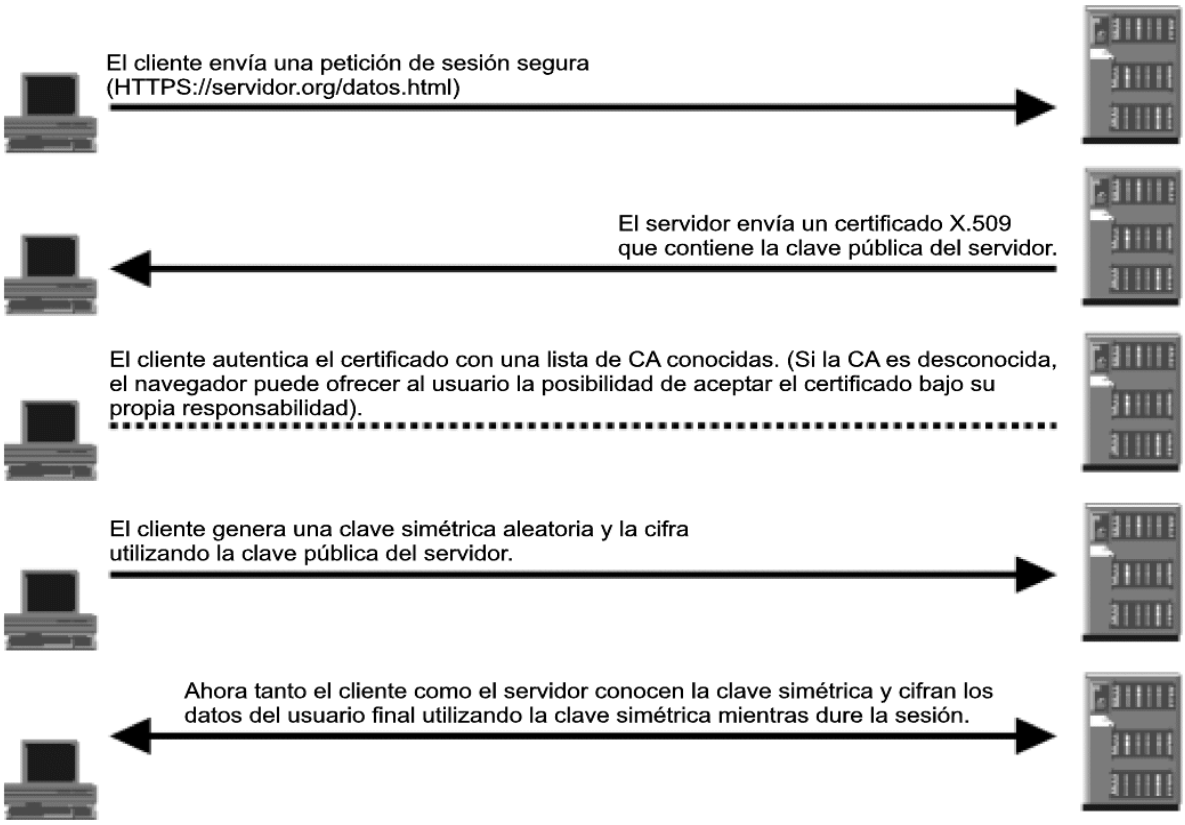


Ilustración 5 - SSL

Funcionamiento del protocolo

En el modelo TPC/IP, SSL se introduce como una capa adicional entre la capa de programa y la capa de transporte. Esto hace que se pueda utilizar con cualquier programa, es decir, no solo es utilizado para encriptar la comunicación entre un navegador y un servidor web, sino también en cualquier programa como FTP. También puede aplicar algoritmos de compresión a los datos transmitidos y fragmentar los bloques de mayor tamaño a 214 bytes, volviendo a reensamblarlos en el receptor.
SSL es flexible respecto al algoritmo de encriptación simétrico utilizado, la función de verificación de mensaje y el método de autenticación. La combinación de los elementos anteriores es conocida como suite de cifrado.
Para la encriptación simétrica SSL puede usar los algoritmos DES, Triple DES, RC2, RC4, Fortezza e IDEA; para la verificación de mensajes puede usar MD5 (Message Digest Algorithm 5) o SHA-1 (Secure Hash Algorithm) como algoritmos de hashing y para la autenticación puede usar algoritmos RSA (Rivest, Shamir, Adelman) u operar en modo anónimo en donde se usa el intercambio de claves de Diffie-Hellman. Los algoritmos, longitudes de clave y funciones hash usados en SSL dependen del nivel de seguridad que se busque o se permita.
A continuación, se comentarán algunos de los primeros protocolos y se estudiarán en mayor profundidad los nuevos protocolos en el siguiente punto.

MIME: Multipurpose Mail Enhancements

MIME es un protocolo de intercambio de objetos en Internet. Cada objeto se encierra en una concha que especifica tanto su semántica como el medio de codificación utilizado. La caracterización semántica permite asociar los datos con su mecanismo de transporte (codificación) con su significado, de forma que el remitente y el destinatario utilicen coordinadamente los datos intercambiados. MIME se desarrolló inicialmente para intercambios de mensajería electrónica, habiéndose extendido a muchos otros protocolos.

PEM (Privacy Enhanced Mail) and MIME Object Security Objects (MOSS)

PEM es un sistema similar a MIME y desarrollado en paralelo con este para crear objetos de mensajería garantizados. Con el desarrollo de MIME, PEM es de alguna forma repetitivo, por lo que se verá probablemente desplazado por MOSS que es una extensión de MIME que aporta exclusivamente lo que le falta a éste para obtener las garantías deseadas: claves, firmas, certificados, ...

Secure HTTP (S-HTTP)

Es este un protocolo propuesto por Enterprise Integration Technologies (EIT) y patrocinado por el consorcio CommerceNet. Constituye una extensión del protocolo básico de *www* (http) incorporando cabeceras MIME para aportar confidencialidad, autenticación, integridad e irrenunciabilidad de las transacciones *www*.
Utiliza un sistema inspirado en PEM, añadiendo suficientes cabeceras a cada transacción para lograr cada uno de los objetivos propuestos. Las transacciones HTTP constan simplemente de una petición por parte del cliente que induce una respuesta del servidor. Y punto. S-HTTP especifica que el cliente envíe directamente toda la información pertinente: claves, certificados, códigos de integridad, ... (incluyendo la posibilidad de referenciar secretos compartidos obtenibles exteriormente: intercambios
previos o bases de datos comunes). El servidor responde siguiendo la misma filosofía PEM.

A diferencia de SSL, S-HTTP sólo afecta a las transacciones HTTP, sin extender su cobertura a otros protocolos habituales en Internet. Por lo demás, S-HTTP y SSL pueden convivir, utilizándose uno u otro en diferentes instantes de una transacción comercial, o incluso utilizándose simultáneamente.

VISION PRACTICA SOBRE LA SEGURIDAD EN INTERNET

Como se ha podido observar, la protección de la información que se maneja en el día a día, es algo fundamental para que esta no caiga en las manos de personas ajenas que podrían hacer un uso indebido de la información que se guarda e intercambia. Sobre todo, es necesaria una gran seguridad durante el intercambio, ya que es más vulnerable a ataques de por parte de terceras partes. Por este motivo se han implantados protocolos de seguridad, en los que se incluye el cifrado de la información, que permiten un intercambio más fiable de los datos.
El intercambio de datos de forma electrónica es el intercambio entre sistemas, por medios electrónicos, de datos estructurados y enviados de acuerdo a unas normas de envío de datos.
Dentro de las redes informáticas se conoce bajo el nombre de protocolo de lenguaje, conjunto de reglas formales que permiten la comunicación de distintas computadoras entre sí. Dentro de las distintas redes, como internet, existen numerosos tipos de protocolos, entre ellos:

- TCP/IP

Este es definido como el conjunto de protocolos básicos para la comunicación entre redes y es por medio de él que se logra la transmisión de información entre computadoras pertenecientes a una red. Gracias al protocolo TCP/IP los distintos ordenadores de una red se logran comunicar con otros diferentes y así enlazar a las redes físicamente independientes en la red virtual conocida bajo el nombre de Internet. Este protocolo es el que prevé la base para los servicios más utilizados como por ejemplo transferencia de ficheros, correo electrónico y el login remoto.

- TCP (Transmision Control Protocol)

Este es un protocolo orientado a las comunicaciones y ofrece transmisión de datos confiable. El TCP es el encargado del ensamble de datos provenientes de las capas superiores hacia paquetes estándares, asegurándose que la transferencia de datos se realice correctamente.

- HTTP (Hypertext Transfer Protocol)

Este protocolo permite la recuperación de información y realizar búsquedas indexadas que permiten saltos intertextuales de manera eficiente. Por otro lado, permiten la transferencia de textos de los más variados formatos, no solo HTML. El protocolo HTTP fue desarrollado para resolver los problemas surgidos del sistema hipermedia

distribuidos en diversos puntos de la red.

- FTP (File Transfer Protocol)

Este es utilizado a la hora de realizar transferencias remotas de archivos. Lo que permite es enviar archivos digitales de un lugar local a otro que sea remoto o al revés. Generalmente, el lugar local es el ordenador, mientras que el remoto es el servidor.

- SSH (Secure Shell)

Este fue desarrollado con el fin de mejorar la seguridad de las comunicaciones en internet. Para lograr esto el SSH elimina el envío de aquellas contraseñas que no son cifradas y codificando toda la información transferida.

- UDP (User Datagram Protocol)

El protocolo de datagrama de usuario está destinado a aquellas comunicaciones que se realizan sin conexión y que no cuentan con mecanismos para transferir datagramas. Esto se contrapone con el TCP que está destinado a comunicaciones con conexión. Este protocolo puede resultar poco confiable excepto si las aplicaciones utilizadas cuentan con verificación de confiabilidad.

- SNMP (Simple Network Management Protocol)

Este usa el Protocolo Datagrama del Usuario (PDU) como mecanismo para el transporte. Por otro lado, utiliza distintos términos de TCP/IP como agentes y administradores en lugar de servidores y clientes. El administrador se comunica por medio de la red, mientras que el agente aporta la información sobre un determinado dispositivo.

- TFTP (Trivial File Transfer Protocol)

Este protocolo de transferencia se caracteriza por sencillez y falta de complicaciones. No cuenta con seguridad alguna y también utiliza el Protocolo de Datagrama del Usuario como mecanismo de transporte.

- SMTP (Simple Mail Transfer Protocol)

Este protocolo está compuesto por una serie de reglas que rigen las transferencias y el formato de datos en los envíos de correos electrónicos. SMTP suele ser muy utilizado por clientes locales de correo que necesiten recibir mensajes de e-mail almacenados en un servidor cuya ubicación sea remota.

- ARP (Address Resolution Protocol)

Por medio de este protocolo se logran aquellas tareas que buscan asociar a un

dispositivo IP, el cual está identificado con una dirección IP, con un dispositivo de red, que cuenta con una dirección de red física. ARP es muy usado por los dispositivos de red locales Ethernet. Por otro lado, existe el protocolo RARP y este cumple la función opuesta a la recién mencionada.

Ilustración 6 - Redes

CERTIFICADOS DE SEGURIDAD EN INTERNET

Una vez comprendidos, de forma general, los puntos básicos de la protección de datos, se puede ver la aplicación práctica que se hace de ellos en internet en el día a día que, para los usuarios cotidianos, pasa desapercibida.
Desde que se entra en el correo por la mañana en el ordenador o la Tablet hasta consultarla cuenta bancaria o realizar la reserva de un libro en una biblioteca, todo ello requiere de los servicios de la codificación para poder asegurar la confidencialidad de los datos de carácter personal de los usuarios y su integridad, además de impedir que se pueda hacer un uso indebido de ellos.
Hoy día, es aún más importante el que los sitios web tengan un buen sistema de seguridad, ya que, para comodidad de los usuarios, la gran mayoría de las gestiones que se realizan día a día se pueden llevar a cabo con internet, y es un método que la mayoría de los usuarios utilizan al poder llevarlo a cabo desde cualquier sitio prácticamente gracias a los datos móviles y les permite ahorrar tiempo en desplazamientos.

Otro punto importante es el sistema operativo que se utiliza y el navegador. Para ellos se van a comprobar en los sistemas operativos Windows, Android e iOS; y en los navegadores *Internet Explorer, Google Chrome, Opera* y *Mozilla Firefox* en el S.O. Windows 10; con la aplicación *Internet* en el S.O. Android 5.1.1 y *Safari* en el S.O. iOS 10.3.2.

Todos los navegadores utilizan símbolos que aparecen al lado del buscador donde aparece la dirección web del sitio, para que a primera vista el usuario que está navegando por ellos pueda saber si son sitios seguros, protegidos con cifrado; no seguros, que no poseen ningún tipo de cifrado y por lo tanto el intercambio de datos con el sitio no es seguro; e inseguros, en los que no solo no hay certificado, sino que además no se garantiza que el sitio web sea realmente ese sitio o que al entrar pueda haber terceras personas obteniendo acceso a tu información personal almacenada en el ordenador, son sitios de riesgo.

Certificados en el Sistema Operativo Windows

Este S.O., al ser uno de los más utilizados por los usuarios tiene un gran número de navegadores compatibles para ser utilizados, pero dentro de todos ellos, los principales y más utilizados son estos cuatro: Internet Explorer, Google Chrome, Opera y Mozilla Firefox.

Las páginas utilizadas para la realización de esta práctica han sido la página de las bibliotecas de la Universidad de Salamanca y la página web del catálogo de las bibliotecas del Ayuntamiento de Salamanca.

El uso de estas páginas como ejemplo es debido a que la primera, la perteneciente a las bibliotecas de la USAL, utiliza certificado para la página web y por lo tanto la información que se intercambia va a estar cifrada, esto se debe a que se puede iniciar sesión en ella con los datos de usuario.

Mientras que, en el caso del catálogo de las bibliotecas del ayuntamiento, no se utiliza ningún tipo de certificado ya que la información no está cifrada, lo cual sería algo a tener en cuenta puesto que los usuarios de estas bibliotecas pueden iniciar sesión en esta página web para la reserva de libros.

- **Internet Explorer**

La primera búsqueda que se va a realizar es la de la página de las bibliotecas de la Universidad de Salamanca. Una vez realizada la búsqueda en el navegador y se accede

a la página web, se puede ver en la parte superior, a la izquierda de la dirección web un candado, esto quiere decir que el sitio web es seguro y que el intercambio de datos con este va a estar cifrado. Para saber que tipo de certificados utiliza el sitio web se hace clic en el candado que aparece en la esquina derecha de la dirección del sitio web, donde se desplegará una pequeña venta donde se indica la "Identificación del sitio web" y en esta, en la parte inferior aparece un enlace a la ventana de con la información del certificado, "Ver certificado".

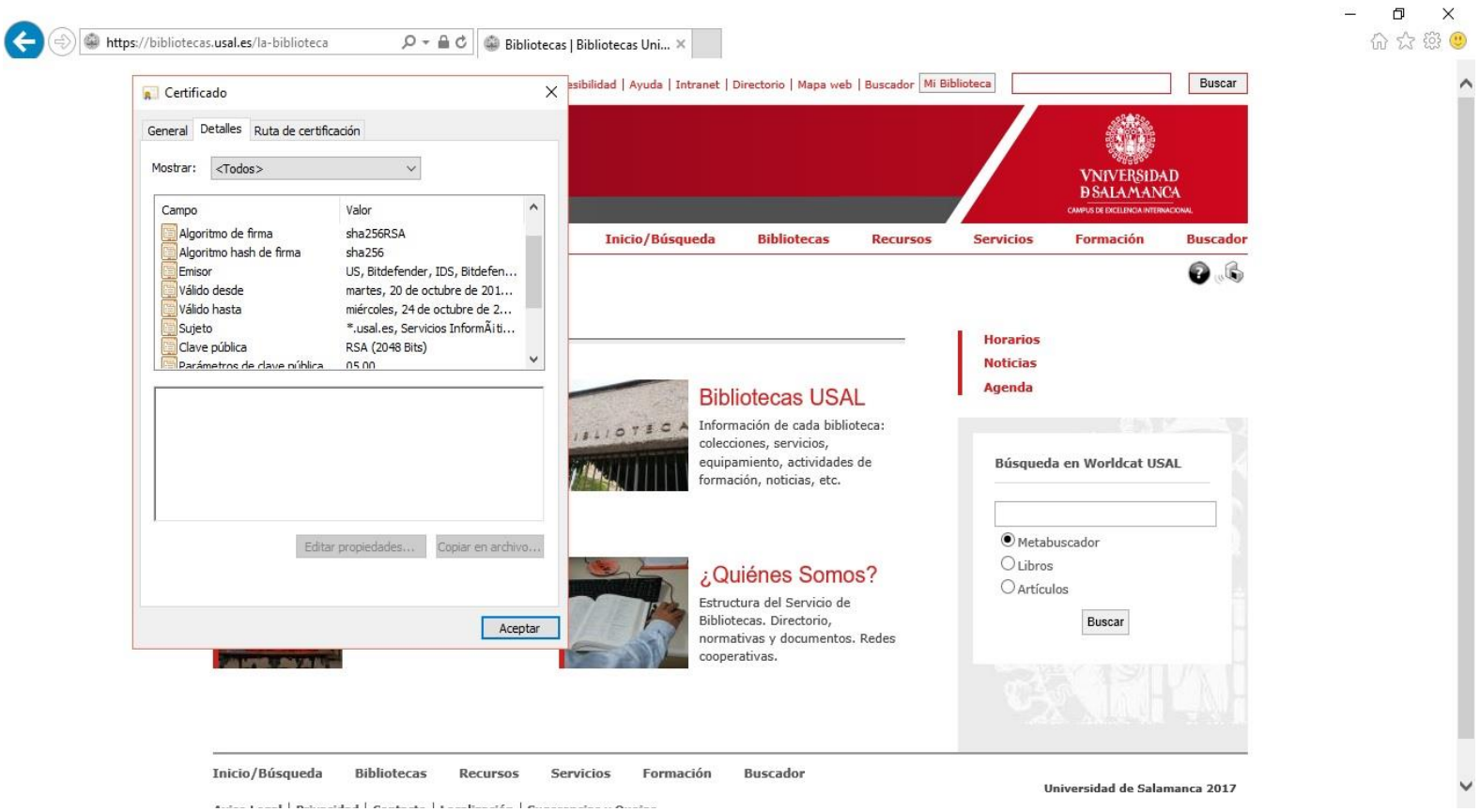


Ilustración 7 - Internet Explorer

En la imagen inferior se pueden comprobar los detalles del certificado de la web de las bibliotecas de la USAL. Se puede ver el algoritmo de firma, el algoritmo hash de firma, el emisor, la validez de este la entidad que está utilizando este certificado, el tipo de clave pública que utiliza.

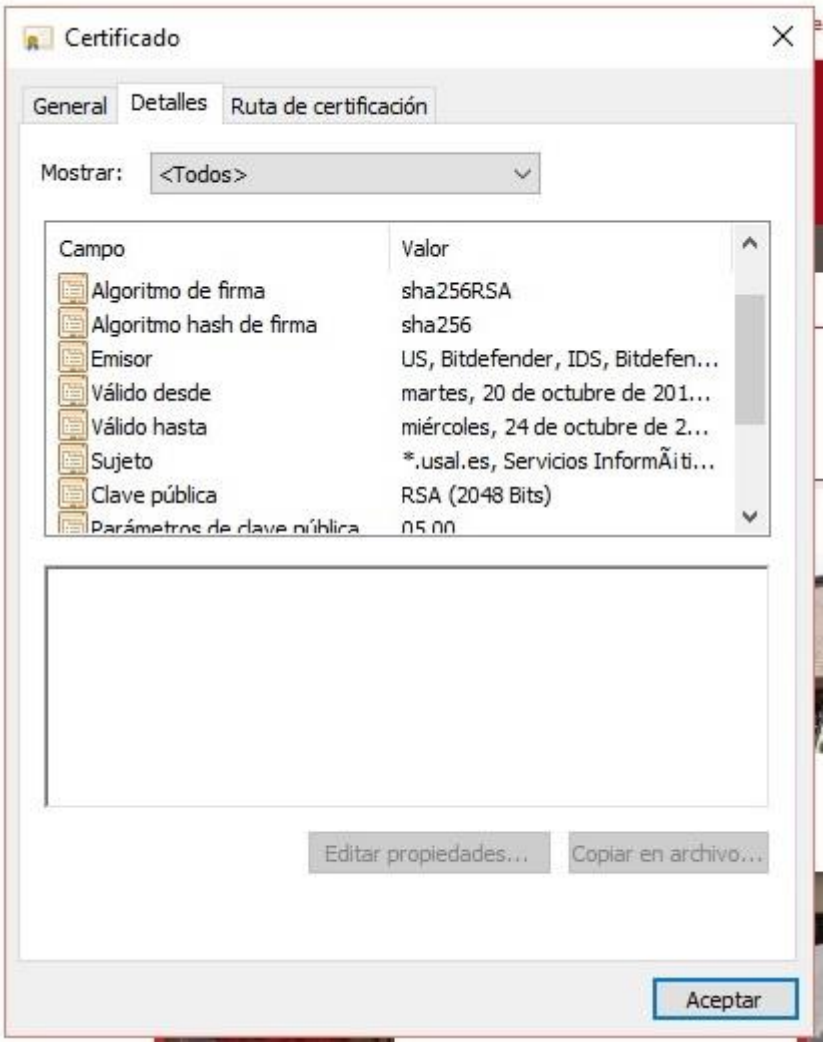


Ilustración 8 - Detalle Internet Explorer

Vista la información detallada del certificado de esta página, se pasa a la búsqueda del siguiente sitio web de estudio para comprobar la seguridad web del sitio.
En este caso, la página web del catálogo de las bibliotecas del ayuntamiento no aparece en la esquina derecha el candado que garantía que se está visitando un sitio seguro, sino que no aparece ningún símbolo. No obstante, se puede comprobar clicando con el botón derecho del ratón en la página y en el desplegable entrando en el aparatado "Propiedades".

En la nueva ventana se puede ver el tipo de protocolo, en este caso HTTP, el tipo de documento web y el tipo de conexión, en este caso no cifrado. En la parte inferior aparece un botón llamado "certificados" que al no poseer ninguno el sitio web no está activo. Esta información se puede ver en la siguiente imagen.

- **Google Chrome**

En este caso también se comienza buscando la página web de las bibliotecas de la USAL, al igual que en el caso anterior se realiza la búsqueda en el navegar para acceder al sitio web, aquí también aparece un candado, en este caso de color verde y al lado se puede leer en letras verdes "Es seguro".En este caso, para acceder a los certificados de seguridad del sitio web, se hace clic en la página con el botón con forma de flecha que aparece en la esquina de la parte superior derecha y en el desplegable se selecciona "Más herramientas", lo cual abrirá más opciones, y de estas nuevas opciones se hace clic en "Herramientas para desarrolladores". En este momento la página aparece reducida en la mitad izquierda de la pantalla y en la otra mitad derecha aparecerán

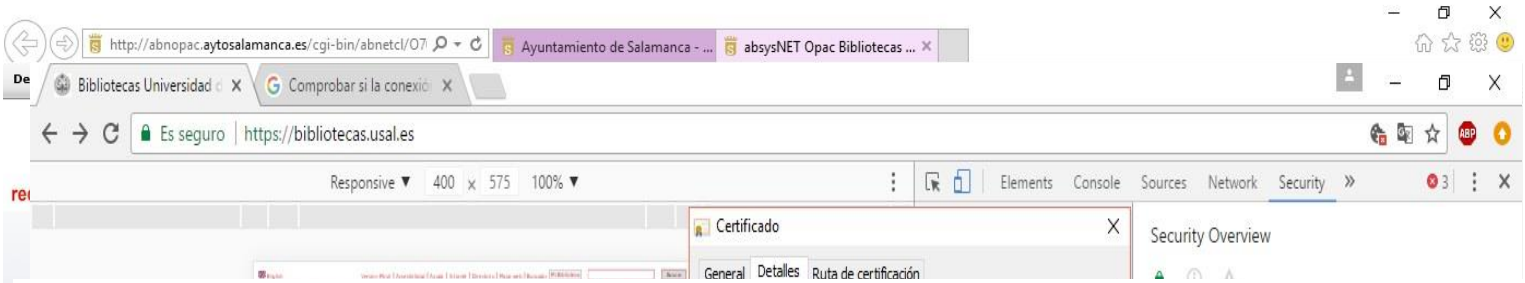


Ilustración 9 - Internet Explorer II

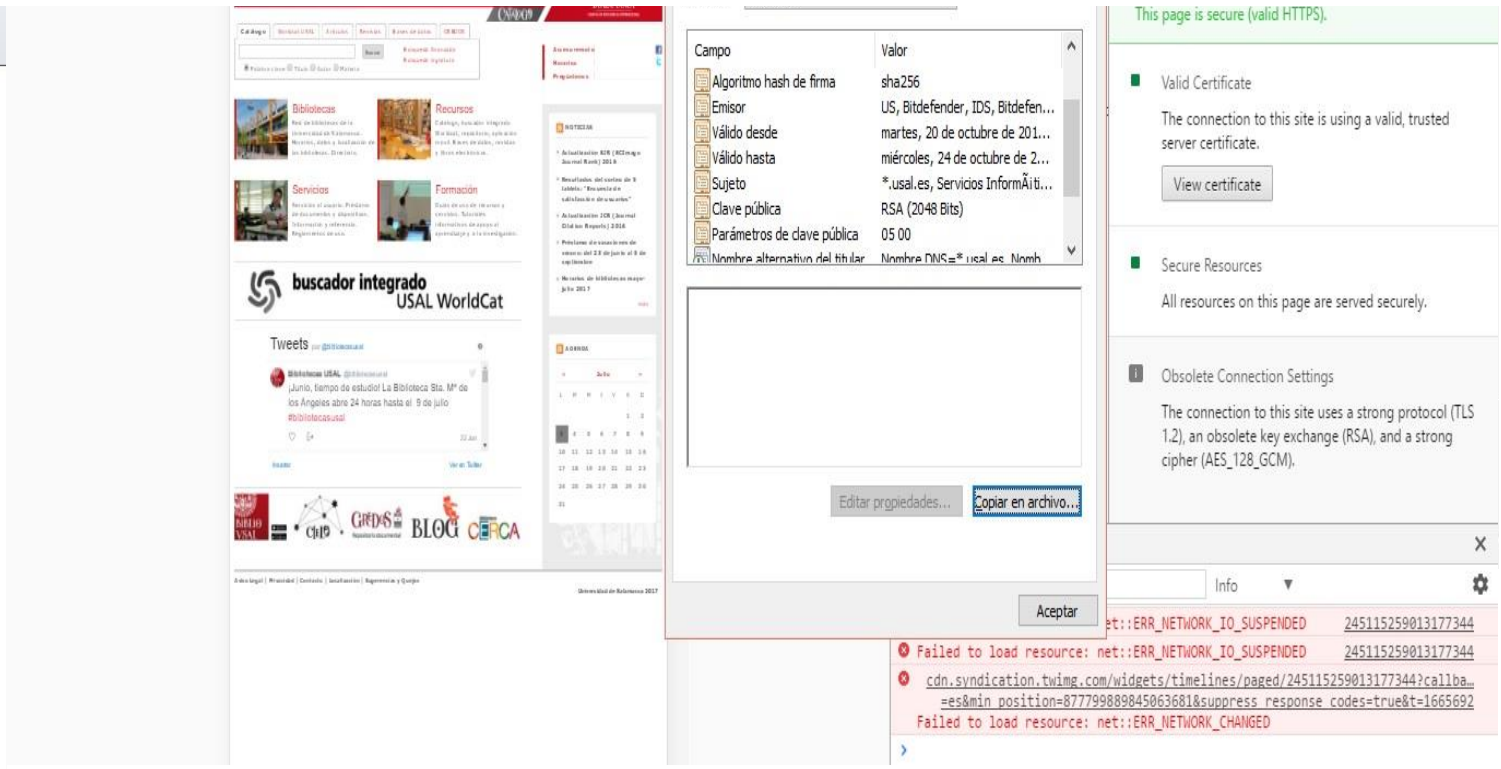


Ilustración 11- Google Chrome

estas herramientas que se han abierto. En la parte superior de estas herramientas hay un menú con opciones para ver, se hace clic en "Security" y en el desplegable que se ha abierto se pueden ver tres símbolos, en este caso aparece coloreado en verde el candado indicando que es un sitio web seguro, con una dirección HTTP válida. A continuación, se presiona el botón "View Certificate", ahora aparecerá una pequeña pantalla con toda la información del certificado. Para conocer la información detallada del certificado, se va a la pestaña "Detalles" y hay aparecerá la información acerca del certificado del sitio web.

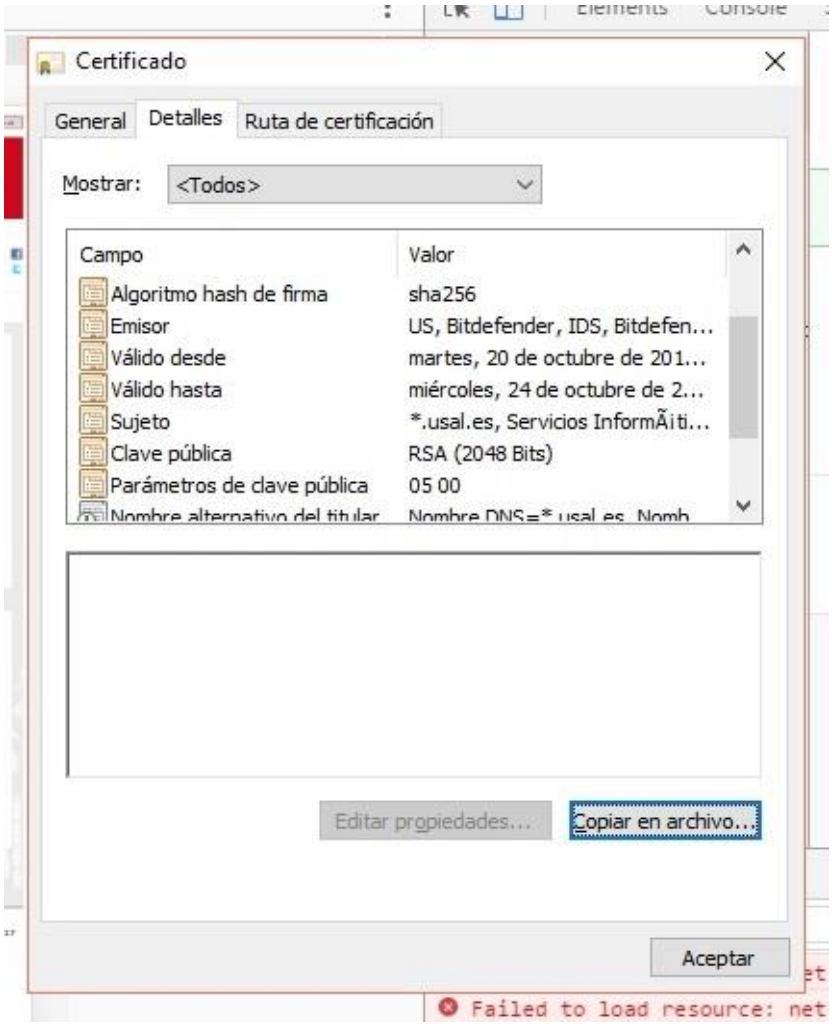


Ilustración 12 - Detalle Google Chrome

En la primera imagen, en la parte derecha, donde se abrió la parte de seguridad, se puede ver que aparece el tipo de protocolo que utiliza la página, TLS 1.2, el algoritmo de clave pública, RSA y el algoritmo de cifrado, AES 128 GCM.
Mientras que en esta segunda imagen aparece información más detallada: el algoritmo hash de firma que utiliza, el emisor del certificado, el inicio y el fin de la validez del

certificado, la entidad que está utilizando este certificado, el tipo de clave pública que utiliza, los parámetros de esta clave pública, ...
Viendo la página de los certificados, se puede apreciar que este navegador tiene una presentación y cantidad de datos sobre los certificados prácticamente idéntica a la de Internet Explorer.

El siguiente sitio web, es el de la página de las bibliotecas del ayuntamiento. A diferencia del sitio web anterior, en este en lugar del candado indicando que el sitio web estaba cifrado, en este se puede ver un circulo con una "i" dentro, señalando que no es seguro.
No obstante, se procede, al igual que en el caso anterior, a comprobar los certificados, si los hubiese, abriendo las herramientas para desarrolladores como se ha explicado en el caso anterior.
Aunque en este caso al no haber certificados simplemente el navegador indica que no hay certificados.

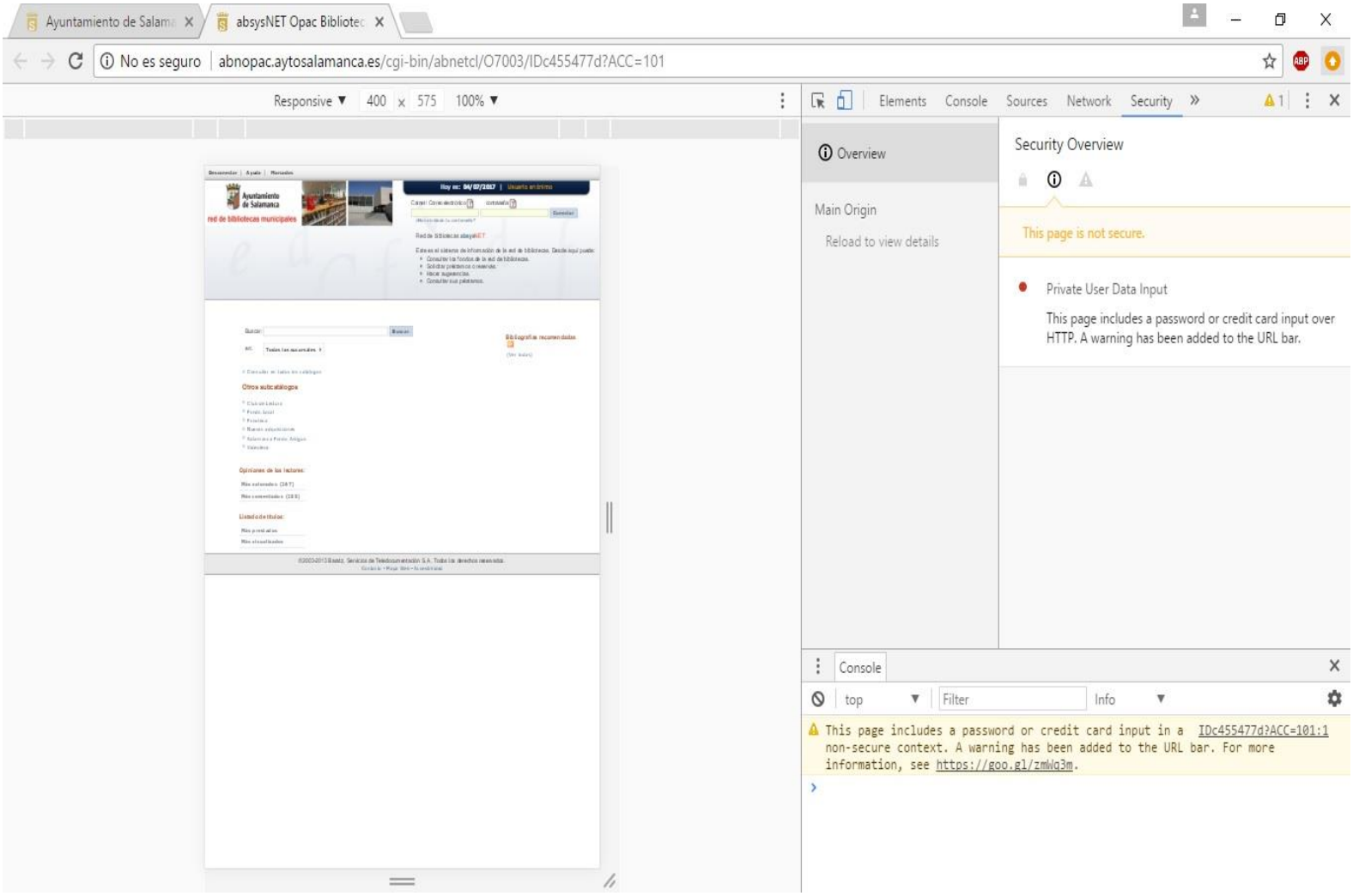


Ilustración 14 - Google Chrome II

En este caso se puede ver que el símbolo iluminado es el del círculo con la letra "i", al igual que el que aparece al lado de la dirección web del buscador. Aquí se indica que el sitio web no es seguro y que se van a introducir datos de acceso en una página web no segura.

- **Opera**

Tras abrir el navegador, se abre la página web de las bibliotecas de la USAL en primer

lugar. Al igual que en los sitios seguros de los demás navegadores, aparece el candado al lado de la dirección web del sitio, en este caso a la izquierda.
A continuación, para ver la seguridad del sitio web se hace clic encima del icono del cando y se desplegará una pequeña pantalla en la únicamente se informa de que el sitio es seguro, para ver más información se hace clic en "detalles" y ahora se puede ver quién es el autoridad que expide el certificado y a que empresa u organización; y el tipo de conexión, en el que aparece el protocolo, TSL 1.2 en este caso; el tipo de cifrado, AES 128 GCM; y el algoritmo de clave pública, RSA.

Ilustración 15 - Opera

Una vez vista la configuración de un sitio seguro con Opera, se abre el sitio web no seguro para visualizar como lo presenta el navegador.
Al abrir la página web del catálogo de bibliotecas del ayuntamiento, en el lugar que en el caso anterior aparecía el candado, en este caso se encuentra un circulo con una bola

dentro, en el que, al clicar en él, se despliega la información de que no es un sitio web seguro y aconseja al usuario que *"No deberías introducir información confidencial en este sitio web (por ejemplo, contraseñas o tarjetas de crédito) porque los atacantes podrían robarla."* Al pulsar en "detalles" se indica que la información no está cifrada.

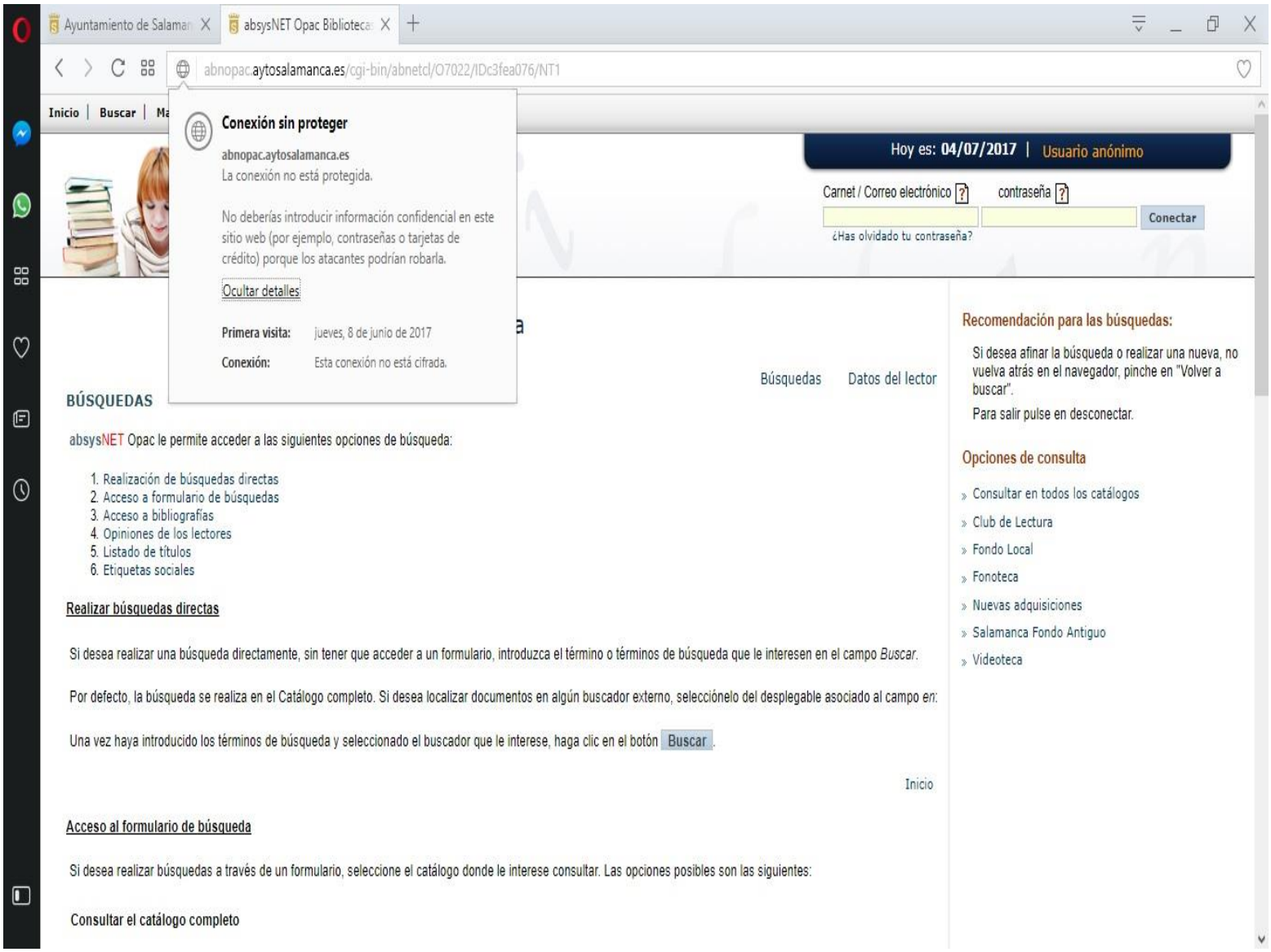


Ilustración 16 - Opera II

- **Mozilla Firefox**

Se realiza la búsqueda con el último de los navegadores de Windows, Mozilla Firefox, para comenzar con la página de las bibliotecas de la USAL.
El símbolo de sitio seguro aparece a la izquierda de la dirección web, en este caso vuelve a ser un candado del color verde. Para ver el certificado del sitio se hace clic sobre este candado y se desplegara una venta indicando "Conexión segura", para ver más detalles se hace clic en la flecha que aparece a la derecha, ahora aparece que es una conexión segura y quien lo verifica, en este caso "TERENA".
Aún se puede ampliar más la información haciendo clic en "Más información", abriéndose una ventana nueva con la información de seguridad de la página con la información de los "detalles técnicos" con: el tipo de protocolo, TLS 1.0, el modo de seguridad de la capa de transporte, DHE (es un protocolo de acuerdo de llave anónimo que proporciona las bases para una variedad de protocolos y se utiliza para promover confidencialidad directa en los modos efímeros de seguridad de la capa de transporte); el algoritmo de cifrado de clave pública, RSA; el algoritmo de cifrado AES 256 CBC; y el algoritmo hash de firma, SHA de 256 bits.
Este navegador amplía aún más la información al hacer clic en "Ver certificado", con lo que se muestra: el certificado del cliente, SSL; para quien se ha emitido (nombre común, organización, unidad organizativa y número de serie); por quien ha sido emitido (nombre común, organización y unidad organizativa); el periodo de validez, desde el martes 20 de octubre de 2015 hasta el miércoles 24 de octubre de 2018; y las huellas digitales.

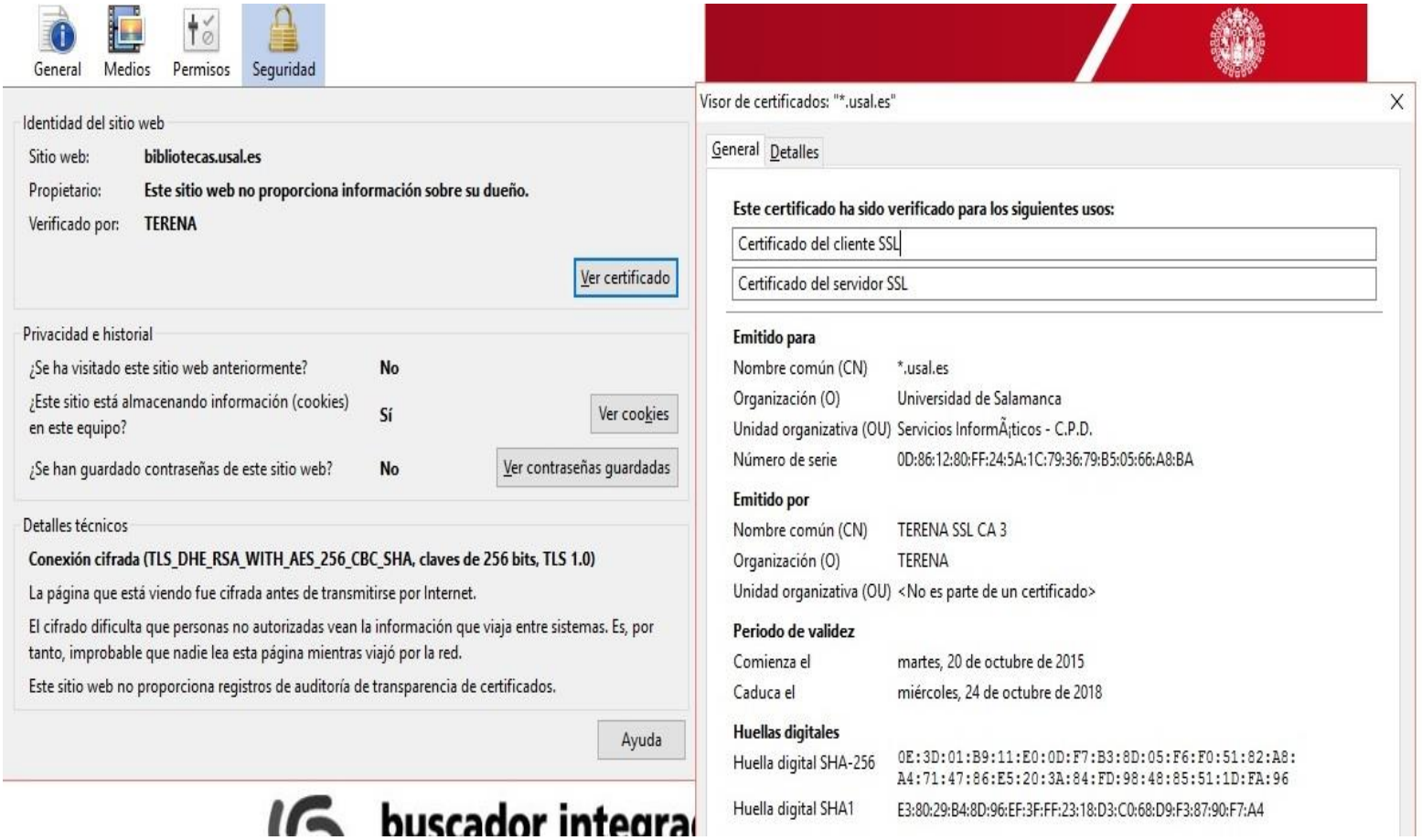


Ilustración 17 - Mozilla Firefox

Como se puede ver, este navegador muestra una información de la seguridad y el certificado del sitio web muy completa.

Visto el sitio seguro, se abre el siguiente sitio de estudio no seguro.

El símbolo que aparece sigue siendo un candado, pero en este caso en color gris y tachado con una barra roja, que, al hacer clic en él, muestra el desplegable e ir a "Más información" para ver la configuración de seguridad del sitio, simplemente se muestra que no se dispone información acerca del propietario del sitio web y que no ha sido verificado.

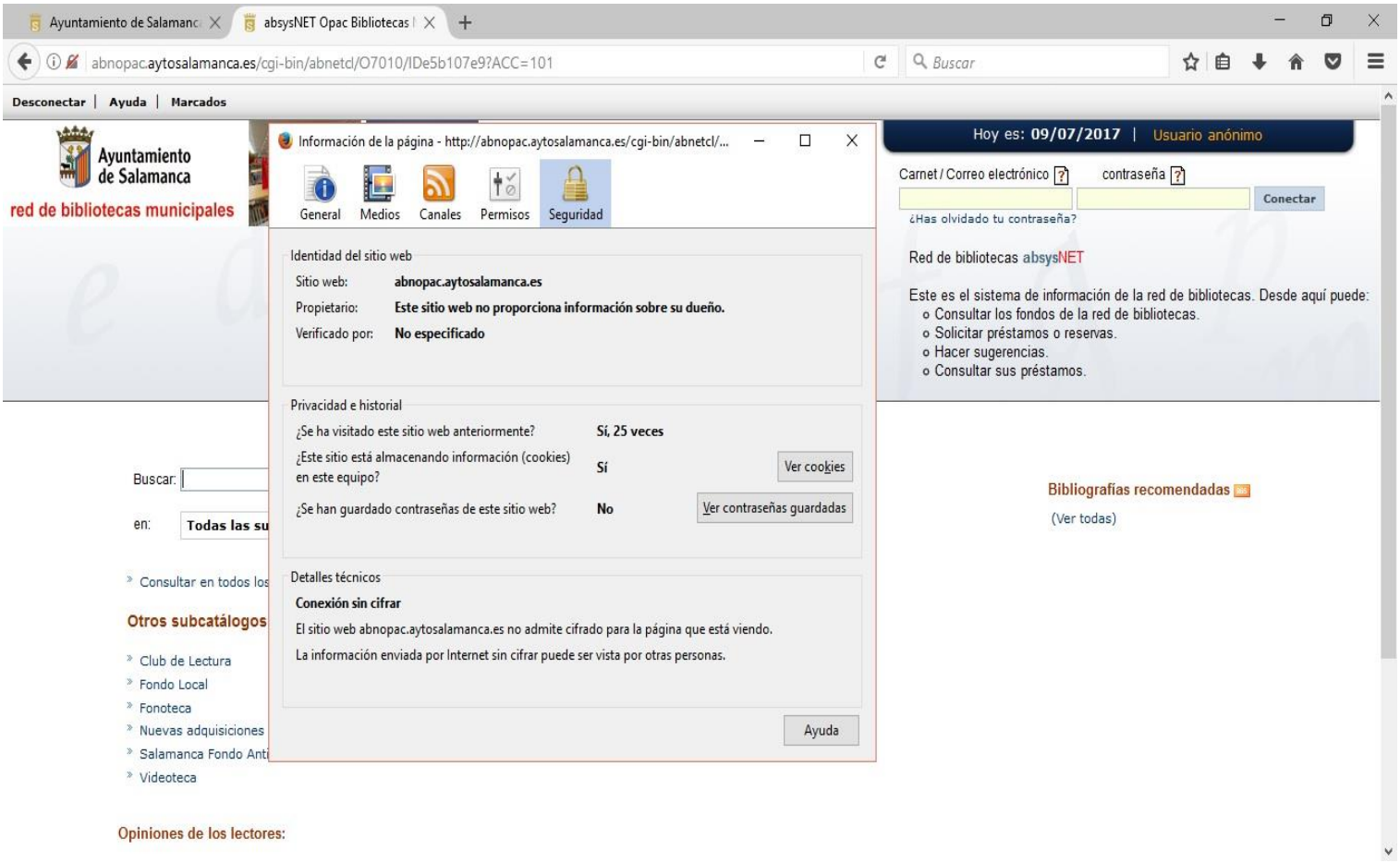


Ilustración 18 - Mozilla Firefox II

Conclusión

Ahora que se ha visto de forma práctica como los distintos navegadores muestran la configuración de los sitios web seguros y no seguros, se puede ver cómo todos los navegadores informan de ello, en el caso de los sitios web no seguros advirtiendo de que son sitios web más violales donde no se recomienda introducir datos importantes de carácter personal puesto que pueden ser interceptados por terceras partes; y en el caso de los sitios web seguros como muestran, aunque sea de forma básica, como los sitios web han sido cifrados para la seguridad del usuario.

De los navegadores vistos, los que muestran una información de forma similar son el navegador Internet Explorer y el navegador Google Chrome, aunque este último muestra más información, como es el algoritmo de cifrado, por ejemplo.

El navegador Opera, al igual que Google Chrome, muestra el protocolo, el algoritmo de cifrado y el de clave pública, pero no muestra el resto de detalles que los anteriores navegadores si muestran.

Respecto del navegador Mozilla Firefox, decir que es el que muestra la información más completa y mejor organizada de todos los probados para la práctica.
Dejando a un lado la presentación que cada navegador hace para mostrar la información de seguridad y fijando la atención y los protocolos y algoritmos, cabe reseñar que: en todos los protocolos son TLS (excepto Internet Explorer que no muestra el que utiliza), Google Chrome y Opera en la versión 1.2 y Mozilla Firefox en la versión 1.0; también en todos ellos el algoritmo de cifrado es el AES, pero en el caso de Google Chrome y Opera de 128 bit GCM y el en caso de Mozilla Firefox de 256 bit GCM (Internet Explorer que no muestra el que utiliza); el algoritmo de clave pública que todos utilizan el RSA, en el caso de Google Chrome e Internet Explorer se especifica que es de 2048 bits; y el algoritmo de firma hash de Internet Explorer, Google Chrome y Mozilla Firefox es SHA 256, Opera no especifica.

Certificados en el Sistema Operativo Android

Android es un Sistema Operativo basado en Linux. Fue diseñado, principalmente, para dispositivos móviles con pantalla táctil, como smartphones y tablets, y para Smartwhatch, SmartTV y automóviles.
Este S.O. trabaja con lo que se llama aplicaciones, que son similares a los programas informáticos. Para la realización de la práctica de con este S.O. se va a utilizar las aplicaciones Internet, instalada por defecto en el S.O., Google Chrome y Mozilla Firefox. Las páginas que se van a utilizar en este caso siguen siendo las mismas, la página de las bibliotecas de la USAL y en la página del catálogo de las bibliotecas del Ayuntamiento de Salamanca.

- **Internet**

Se comienza realizando la búsqueda del sitio web como en los navegadores y al cargar la web de las bibliotecas de la USAL, que se estudiará en primer lugar, se puede ver un candado gris a la izquierda de la dirección web del sitio. Si se toca encima de este candado se abre una nueva ventana en la que aparece la información sobre la página y en la parte inferior un enlace a "Ver certificado". Al tocar encima de este enlace se abre una nueva ventana con información sobre quien ha verificado el sitio web, en este caso TERENA con un protocolo SSL, también informa que ha sido cifrada con un algoritmo de 256 bits, que utiliza un protocolo TLS 1.0 y que la conexión ha sido encriptada con un algoritmo AES 256 CBC, con el algoritmo hash de firma SHA1 y con DHE-RSA como mecanismo para intercambio de claves.

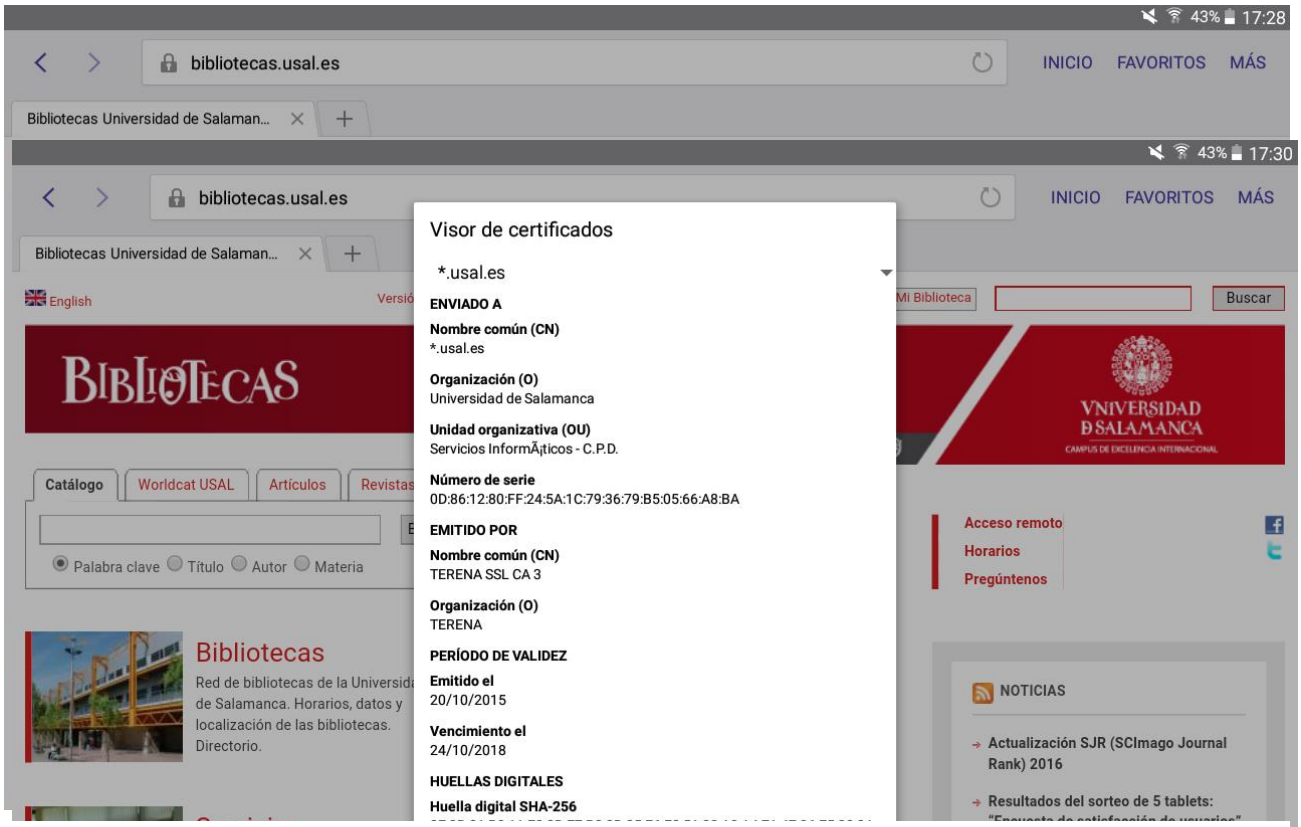


Ilustración 19 - Internet

Ilustración 20 – Internet II

Además de toda esta información tocando en "Datos del certificado" se puede ver la información del certificado con más detalle, como se puede ver en la imagen que aparece a continuación.

Al visitar el siguiente sitio web, no seguro, del catálogo de las bibliotecas del ayuntamiento, no aparece ningún símbolo del nivel de seguridad al lado de la dirección web ni tiene opción de mostrar la configuración de seguridad del sitio.

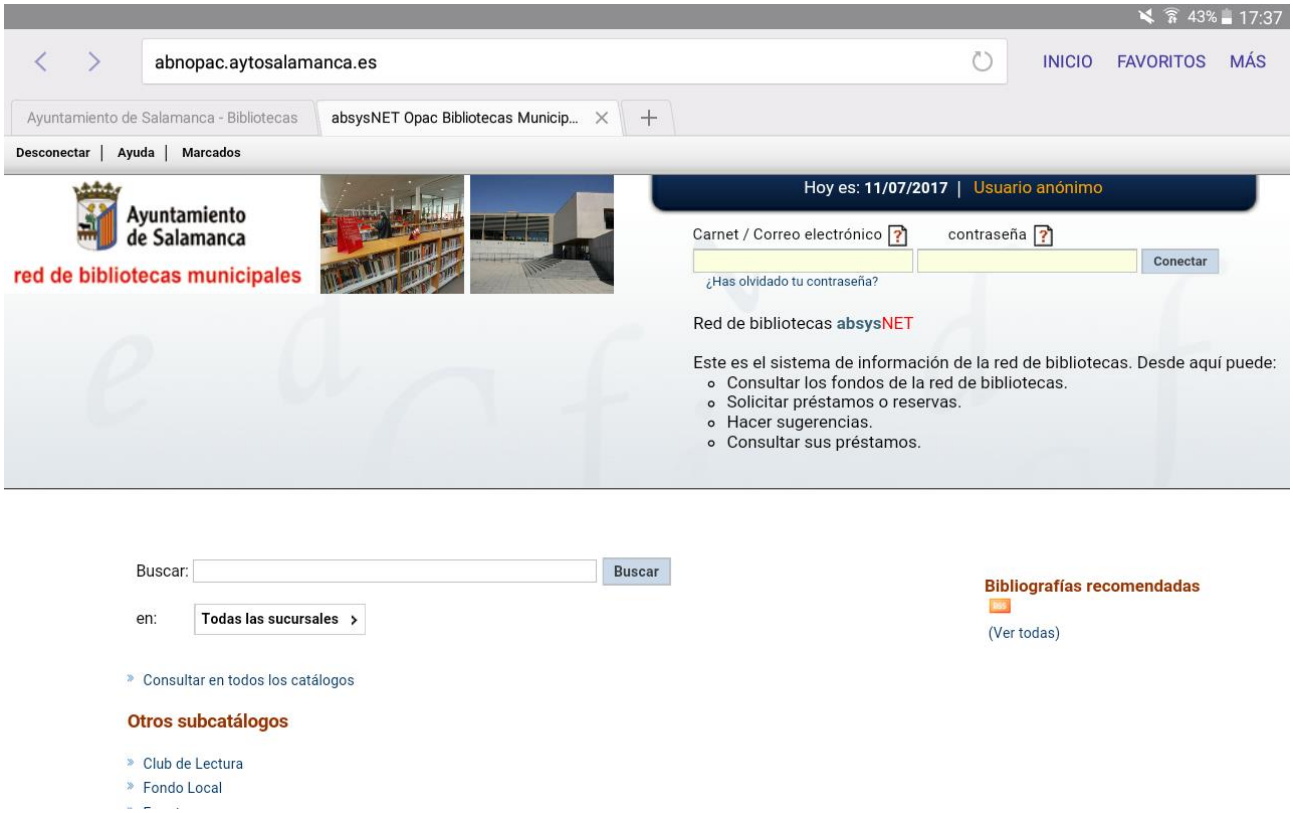


Ilustración 21 - Internet III

- **Google Chrome**

Al igual que en el caso anterior, esta práctica también se va a realizar con una aplicación, en este caso con la de Google Chrome para comprobar las diferencias que puede haber entre aplicación y programa informático, en este aspecto de seguridad en la web.

Al entrar en el primer sitio web, en de las bibliotecas de la USAL, aparece, al igual que en programa, el candado verde a la izquierda de la dirección web indicando que es un sitio seguro, al tocar encima de este aparece un mensaje que indica que "Tu conexión con este sitio es privada" y un enlace a los detalles, se toca encima del enlace y se abre una nueva ventana con la información de que el sitio web ha sido verificado por TERENA con un protocolo SSL CA 3, que la conexión utiliza un protocolo TLS 1.0, al igual que en el programa. También aparece el tipo de algoritmo de cifrado que es AES 256 CBC, en lo que difiere con el programa que utilizaba un algoritmo AES 128 GCM. Otro punto en el que difiere con respecto del programa es el algoritmo de firma hash, que en este caso es HMAC-SHA1, mientras que en el programa era SHA256; al igual que en el mecanismo de intercambio de claves que en la aplicación es DHE_RSA mientras que en el programa utiliza RSA de 2048 bits.

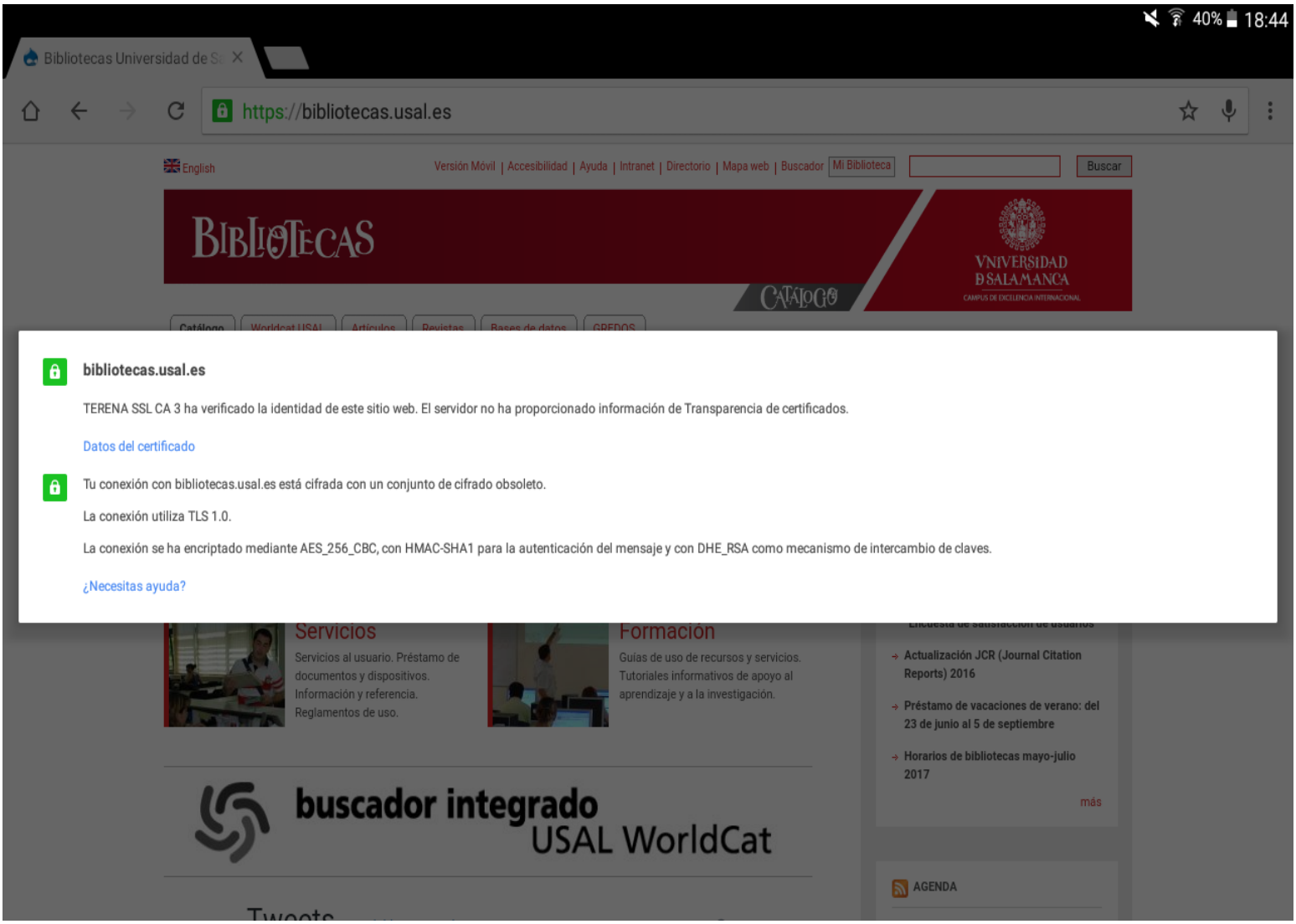


Ilustración 22 - Aplicación Google Chrome

En el segundo sitio web, el catálogo de las bibliotecas del ayuntamiento, al ser un sitio web no seguro, el candado ha sido sustituido por el icono de un folio y al tocar encima de este se abre una venta en la que se informa de que "Tu conexión con este sitio no es privada". En este caso no deja ver más configuración, pero hay un enlace hacia los "Ajustes del sitio" donde deja restablecer los ajustes para este sitio y borrar los datos utilizados en él.

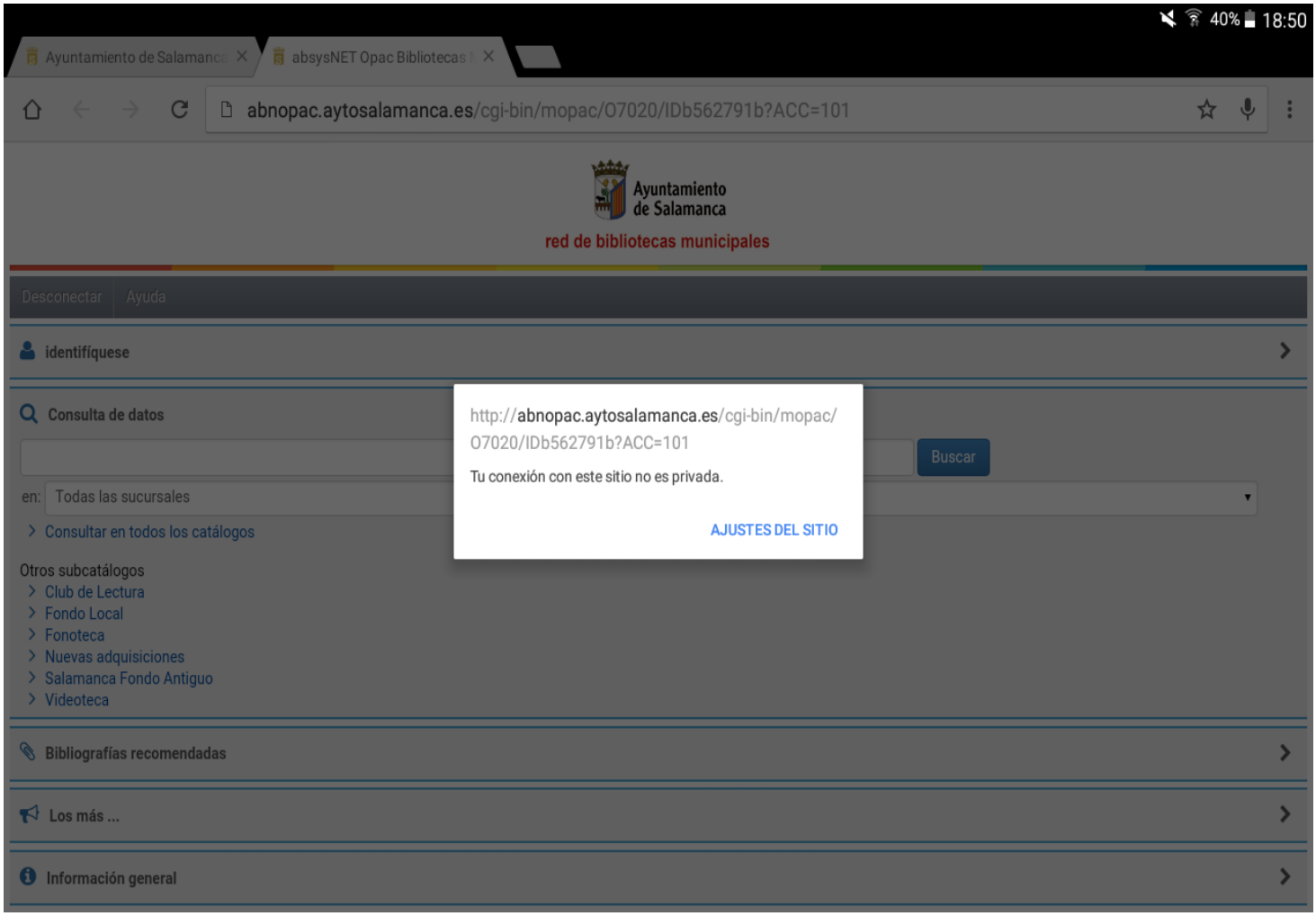


Ilustración 24 - Aplicación Google Chrome II

- **Mozilla Firefox**

Como en el caso anterior, el uso de la aplicación de Mozilla Firefox también es poder comparar las diferencias y similitudes en las configuraciones de seguridad de los sitios web entre aplicación y programa.

En la página de la biblioteca de la USAL, se puede ver, al igual que en el programa, que aparece un candado verde a la izquierda de la dirección web, al tocar encima de este se despliega una ventana en la que se informa de que en una conexión segura y que ha sido verificada por TERENA, pero no da opción a ver ninguna información más sobre la seguridad.

Teniendo en cuenta que, en comparación con el resto de los navegadores, Mozilla era el navegador que más información sobre la seguridad y los certificados aportaba, en el caso de la aplicación es la que no proporciona más que una pobre información sobre la

certificación de seguridad del sitio.

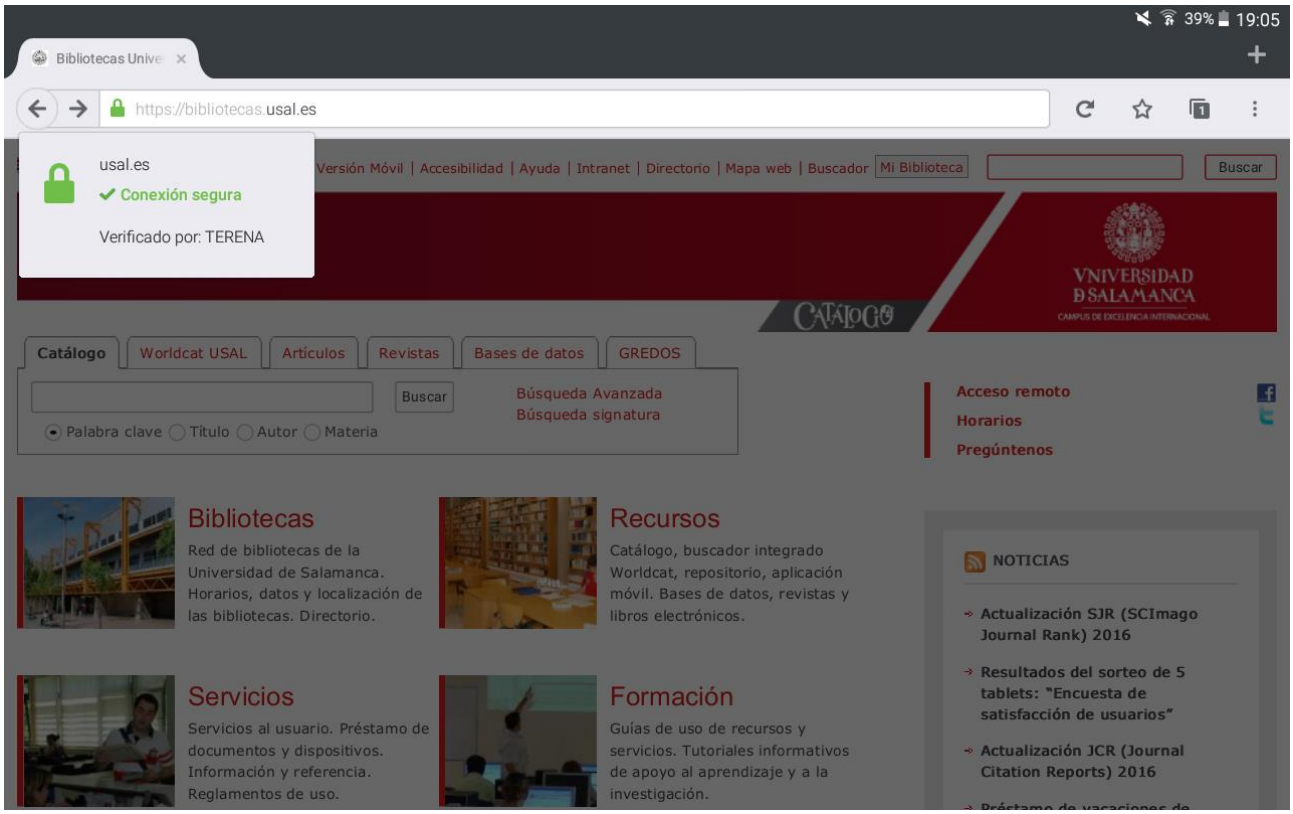


Ilustración 25 - Aplicación Mozilla

El siguiente y último sitio web, el del catálogo de las bibliotecas del ayuntamiento de Salamanca, tiene, al lado la dirección del sitio web una bola del mundo, lo que, indica que la conexión no es segura, al tocar encima de este icono, se despliega una venta

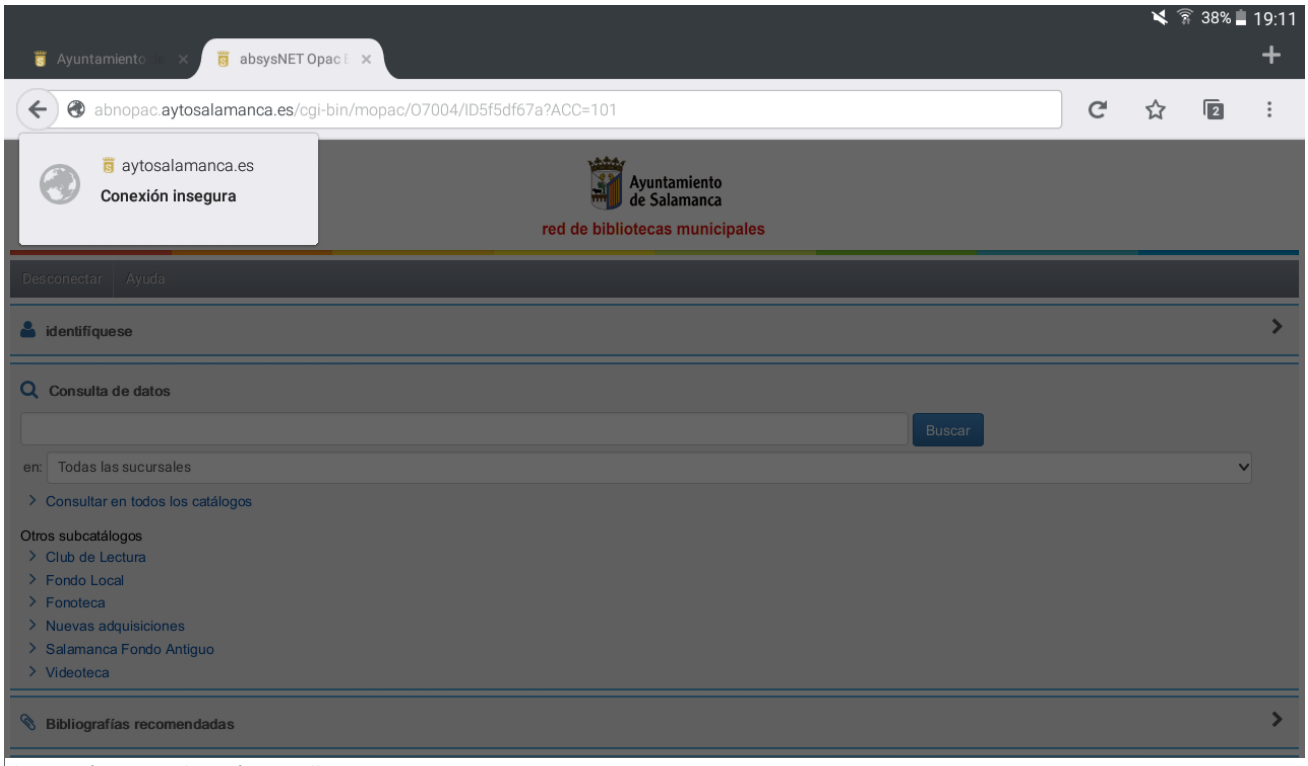


Ilustración 26 - Aplicación Mozilla II

nueva en la que se indica al usuario que la conexión es "insegura". No da opción a ver más configuración de seguridad, al igual que en el programa de Mozilla Firefox que tampoco daba lugar a más información.

Conclusiones

Como se ha podido comprobar a lo largo de toda la práctica con las aplicaciones del Sistema Operativo Android, la información facilitada no ha sido tan detallada como los fue con los programas en Windows, puede deberse, en primer lugar a que este Sistema Operativo lleva mucho menos tiempo comercializándose que el Windows, y en segundo lugar a que el sistema Windows es más utilizado en ordenadores y el sistema Android en Tablet y por ello, los usuarios que quieran consultar esta información lo hace más a menudo en los navegadores como programas utilizados en Windows que en los navegadores como aplicaciones utilizados en Android.

Para finalizar añadir, que en ninguna de las aplicaciones daba opción a ver el certificado del sitio web.

Certificados en el Sistema Operativo iOS

El Sistema Operativo iOS es el S.O. de Apple, cuyo navegador por defecto es el Safari y es con este con el que se va a realizar la práctica. Este sistema, al ser un sistema un poco "cerrado" no muestra demasiada información sobre la navegación y más aún porque se está utilizando en un dispositivo móvil como es un iPhone, además de que no tiene tantas compatibilidades con las aplicaciones como el sistema Android o el sistema Windows con los programas.

- **Safari**

Al acceder al primero de los sitios web, el de las bibliotecas de la USAL, aparece un candado negro a la izquierda de la dirección del sitio. Este navegador no da opción a ver ninguna configuración de seguridad, simplemente muestra el icono del candado para los sitios seguros.

Ilustración 27 - Safari

Al intentar acceder al siguiente sitio web del catálogo de las bibliotecas del ayuntamiento de Salamanca, el navegador no puede acceder al sitio, por lo que posiblemente el sitio web no esté habilitado para ser utilizado con el navegador.

CONCLUSIONES

Como se ha podido ver durante todo el trabajo, el cifrado de la información ha jugado un papel muy importante desde sus inicios, con los sistemas más básicos, hasta la actualidad, con completos métodos de cifrado y el uso conjunto, en ocasiones, de para las diferentes fases del intercambio de la información.

Dejando a un lado la visión teórica y centrando la atención en la parte práctica, se puede ver cómo están presentes en el día a día los sistemas de protección, pero pasan desapercibidos a los ojos de los usuarios cotidianos.

Observando los resultados obtenidos en el trabajo de campo, se puede ver como los sistemas de cifrado varían de un navegador a otro, como por ejemplo en el algoritmo de cifrado, o incluso de un mismo navegador con utilizando la versión de programa informático o la aplicación, en la misma página web.

Aunque, el uso de distintas metodologías dentro de los navegadores tiene la parte positiva de que dificulta la acción de los usuarios mal intencionados en los intentos de fraude.

Para finalizar añadir que, siempre que vaya a ser requerido por el sitio web introducir datos de autentificación, es importante fijarse en los símbolos que aparecen en la parte superior de las páginas indicando la seguridad del sitio web para navegar con una mayor seguridad.

BIBLIOGRAFÍA

New Direct in Cryptography. Diffie, Whitfield; Hellman, Martin E.

Guía de Seguridad de datos. Agencia Española de Protección de Datos.

El telegrama a México que definió la suerte de la Primera Guerra Mundial. Fajardo, Luis.

Una introducción a la Criptografía Clásica. Soler Fuensanta, José Ramón.
Conferencia sobre seguridad, privacidad y proteccion de datos. Agencia de Protección de Datos.

Algoritmo de cifrado simétrico AES. Aceleración de tiempo de cómputo sobre arquitecturas multicore. Pousa, Adrián

Protocolo de seguridad SSL. Ortega Martorell, Sandra; Canino Gutierrez, Liusbetty.

Privacidad y Seguridad en Internet. Agencia Española de Protección de Datos.

Guía de Protección de Datos para los responsables de ficheros. Agencia Española de Protección de Datos.

Protección de datos de carácter personal. Instituto Nacional de Tecnologías de Comunicación.