PLANTILLA OFICIAL PARA LA PRESENTACIÓN DE TRABAJOS
II CONVENCIÓN CIENTÍFICA INTERNACIONAL
"II CCI UCLV 2019"

DEL 23 AL 30 DE JUNIO DEL 2019.
CAYOS DE VILLA CLARA. CUBA.

II CONFERENCIA INTERNACIONAL DE PROCESAMIENTO DE LA INFORMACIÓN "CIPI2019"

Los certificados digitales como herramienta de seguridad sobre internet

Digital certificates as a tool of security on internet

MSc. Lic.: Sandra Blain Escalona[1]

1-Sandra Blain Escalona. Empresa de Telecomunicaciones de Cuba SA (ETECSA), Cuba. E-mail: sandra.blain@etecsa.cu

Resumen:

El empleo de Internet como herramienta de gestión del conocimiento, cada vez más va ganando terreno en el mundo entero. En Cuba, debido al proceso de informatización de la sociedad, el uso de internet para diversos fines ha escalado peldaños en varios sectores de la sociedad. Navegar con seguridad, hacer un uso consciente de esta herramienta y cómo realizar transacciones electrónicas seguras sobre internet es un reto que impone la necesidad de proveer, a los menos avezados en el tema, de algunos elementos o *tips* que le permitan identificar cuándo están navegando de forma segura en internet. Por tanto, el objetivo principal de este trabajo es analizar los elementos o técnicas que garantizan seguridad en las transacciones electrónicas y destacar la importancia de emplear certificados digitales para la navegación en internet. Para la realización de este trabajo se emplearon los métodos analítico-sintético e inductivo - deductivo que permitieron realizar un resumen de los aspectos más significativos a tener en cuenta unido con un conjunto de acciones preventivas a realizar por los usuarios.

Palabras Clave: Internet, Certificados, Firma digital, Informatización, Transacciones

Abstract:

The use of internet as a management knowledge tool, each more time it is going winning terrain in the whole world. In Cuba, due to the society computerization process, the use of internet has climbed rungs in many sectors of the Cuban society. Navigate with security, do conscious use of this tool and how make secure electronic transactions over internet is a challenge that impose the necessity to provide to those persons less connoisseurs in the theme, of some elements or tips that allow to identify when they are looking for on internet with security. Therefore, the principal objective of this article is to analyze the techniques that ensure the security on the electronics transactions and to emphasize in the importance that the digital certificates has on the sailing of internet. To carry out this work, the analytical-synthetic and inductive-deductive methods were used, which allowed a summary of the most significant aspects to be taken into account together with a set of preventive actions to be carried out by the users.

Key words: *Internet, Certificates, Digital Signature, Computerization, Transactions*

1. Introducción

La fuga de datos, como fenómeno amenazante del mundo digital, tiene un alto impacto negativo en el sector empresarial, pues ocasiona pérdidas financieras, daño a la marca, pérdida del prestigio de la empresa y pérdidas de clientes, acarrea responsabilidades legales e interrupción de la continuidad del negocio (ESET, 2016).

Según el ITRC[1] entre el 2015 y 2017 fueron expuestos más de 390 millones de registros personales por brechas de datos existentes. El 40% de las brechas de seguridad reportadas en el 2015, el 45.3% en el 2016 y el 55.1% en el 2017 han tenido protagonismo en el sector de los negocios, así lo evidencia la figura 1. Más de 390 millones de registros personales fueron comprometidos en este período (ITRC, 2016, 2018).

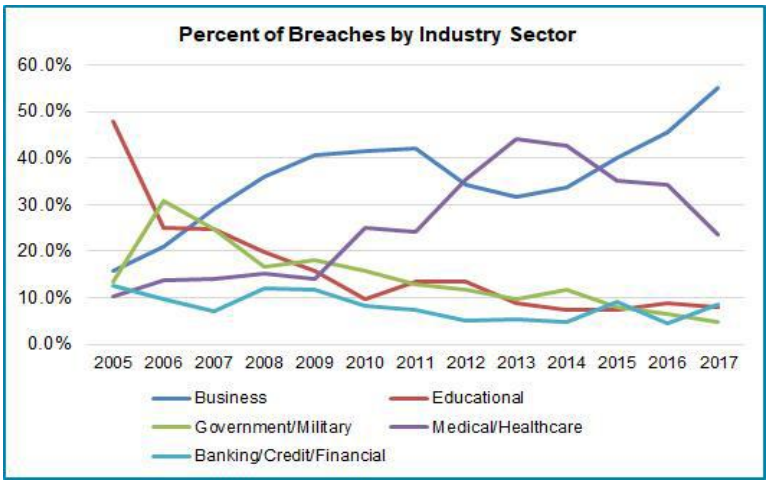

Figura 1. Fuente: ITRC End of Year Data Breach Report 2017

La figura 2 muestra una comparación entre el año 2017 y el 2018 en cuanto a las brechas de seguridad. A pesar de haber disminuido en un 23%, en el 2018, el total de las brechas de seguridad reportadas con relación al 2017 el número de registros expuestos registró un crecimiento del 126% con relación al año anterior, asumiendo el galardón el sector de

[1] Identity Theft Resource Center (por sus siglas en inglés) Centro de Recursos contra el Robo de Identidades es una organización sin fines de lucro establecida para ayudar a las víctimas del robo de identidad a resolver sus casos y para ampliar la educación pública y la concientización en la comprensión del robo de identidad, violaciones de datos, seguridad cibernética, estafas / fraudes y cuestiones de privacidad.

los negocios este año también, con casi el 46% de las brechas. Algunas de las más significativas brechas han sido las detectadas sobre la plataforma social Facebook y Google+ y la relacionada con el grupo hotelero Marriott International impactando estas a más de 480 millones de usuarios (ITRC, 2018) (Martínez, 2019).

DATA BREACH ANNUAL COMPARISON (2018 vs. 2017)				
	2018		2017	
Industry	# of Breaches	# of Records Exposed	# of Breaches	# of Records Exposed
Banking/Credit/Financial	135	1,709,013	134	3,230,308
Business	571	415,233,143	907	181,630,520
Education	76	1,408,670	128	1,418,455
Government/Military	99	18,236,710	79	6,030,619
Medical/Healthcare	363	9,927,798	384	5,302,846
Annual Totals	1,244	446,515,334	1,632	197,612,748

Figura 2. Fuente: ITRC End of Year Data Breach Report 2018

Como muestra la figura 3, aunque, según el reporte de brecha de datos del 2018 presentado por el ITRC, "el acceso no autorizado" disminuyó en un 20% con relación al 2017 este sigue ocupando el peldaño más alto como tipo de brecha detectada manifestándose a través del "hackeo" como forma más común de fuga de datos. De igual manera ocurrió en el 2017 (ITRC, 2018).

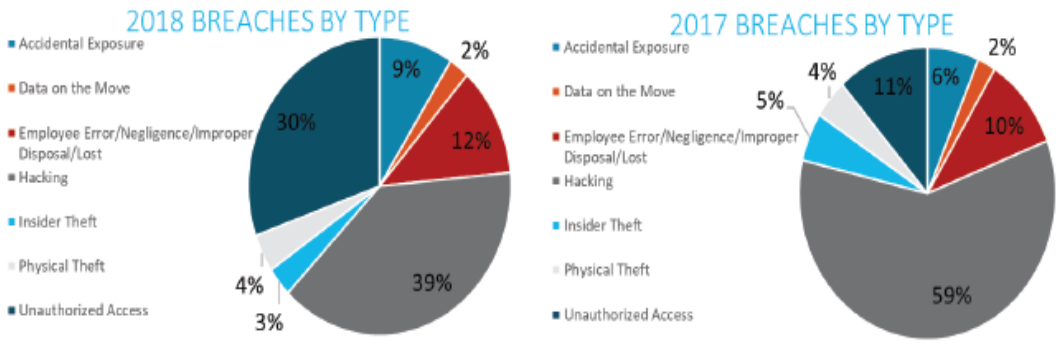

Figura 3. Fuente: ITRC End of Year Data Breach Report 2018

El hecho de que el mundo esté conectado hace que los incidentes tecnológicos afecten de forma global propiciada por la instantaneidad en que viaja la información con el empleo de las nuevas tecnologías. Las alteraciones de las páginas *web* que se visitan, las estafas asociadas al comercio electrónico y el repudio. Malas prácticas de seguridad, comportamientos humanos, La suplantación de identidades aparejado con técnicas de *phising* con gran impacto la ingeniería social. Las vulnerabilidades asociadas a los sistemas operativos y la desactualización de los parches concernientes a su seguridad son causales, entre otros, de este comportamiento.

Qué consecuencias puede conllevar revelar información confidencial?

Los *phisher* pueden realizar cargos a su cuenta. Pueden abrir nuevas cuentas y acordar contratos de prestaciones de servicios o alquiler en su nombre. Pueden utilizar una identidad falsa para vulnerar derechos utilizando sus datos personales. Todo esto también acarrea daños legales, pérdida de prestigio y desconfianza.

Cómo entonces, en los tiempos actuales donde comunicarse y realizar transacciones electrónicas, el uso de las redes sociales se hace cada vez más imperante y usual, se pueden garantizar niveles de seguridad adecuados que aminoren estas amenazas?

2. Metodología

Para el desarrollo de este trabajo así como para el arribo de las conclusiones del mismo se emplearon los métodos Analítico – Sintético para el estudio de técnicas de seguridad como criptografía asimétrica, firmas digitales, certificados digitales de llaves públicas e Infraestructuras de Llaves Públicas sustentado en el análisis de disímiles fuentes de información. También el método Inductivo – Deductivo para llegar a conclusiones sobre qué aspectos se deben tener en cuenta cuando se navega o realiza alguna transacción sobre internet.

3. Resultados y discusión

Centrando la atención en el empleo de Internet como medio fácil, rápido e inseguro sobre el cual se pueden realizar diversas consultas, trámites y acciones como compras on-line, pagos de facturas e impuestos on-line entre otras disimiles acciones; se destaca el uso de certificados digitales también llamados certificados digitales de llaves públicas o certificados X.509 para garantizar una navegación segura sobre la *web*.

Los certificados digitales de llaves públicas son tarjetas de identificación electrónica emitidas por terceras partes confiables llamadas Autoridades de Certificación (AC). En el proceso de emisión de certificados intervienen varias técnicas de seguridad que hacen con el uso de dichas tarjetas electrónicas la realización de transacciones confiables, seguras, legales, verificables, íntegras y confidenciales. Dichas técnicas son las firmas digitales, criptosistemas asimétricos y funciones hash o resúmenes interrelacionadas entre sí (Escalona, 2014; Guillermo E. Zanoletti García 2011; Simko, 2017).

Las firmas digitales no son más que datos binarios que se adicionan a un documento determinado y que vinculan al firmante con dicho documento. Estas se generan por la combinación del empleo de técnicas de encriptación asimétrica y funciones *hash* también llamada huella digital del documento. La encriptación asimétrica utiliza un par de llaves (una privada y otra pública) para el proceso de cifrado/descifrado de información, complementarias matemáticamente y que funcionan en simbiosis; es decir, lo que se cifra con una llave se descifra con la otra. La llave privada sólo conocida y celosamente guardada por el dueño y la pública es conocida por todos. La firma digital garantiza en el mundo digital la validez legal que la firma manuscrita en el mundo real. Es decir, que la persona que firma un documento no pueda negar que lo ha firmado una vez hecha esta acción, que se pueda probar que realmente fue esa persona y no otra y que el mensaje no ha sido alterado después de haberse firmado (Gallego, 2015)

Un mensaje que ha sido firmado digitalmente implica las acciones de cifrar y descifrar para lo cual se emplean el par de llaves donde la pública como ya se dijo es bien conocida por todos y, en un mundo abierto, como el mundo digital, donde se reciben mensajes de personas desconocidas y donde ocupar la personalidad de otra no es difícil, se impone la

necesidad de vincular ese secreto de la llave privada con una persona físicamente, con una entidad determinada. Es decir, hay que tener la certeza de que quien firmó el mensaje era en concreto la persona X que tenía ese secreto y no era Z y, que la llave pública es de quién dice ser que es. Esta es una incógnita que los certificados digitales vienen a resolver. Por tanto, los certificados digitales X.509 es un estándar definido por la UIT-T[2] para Infraestructura de Llaves Públicas identifican exclusivamente la identidad de una entidad (entiéndase una persona jurídica, una empresa, servidor, un sitio *web*, incluso, cualquier "cosa" conectada a internet"- *IoT*[3]) como propietario de su respectiva llave pública. Proporciona la confianza necesaria en el mundo digital o electrónico sobre quién es exactamente el emisor de un mensaje y que éste posee la correspondiente llave privada asociada a la pública que se avala en el certificado.

Las llaves o claves empleadas en los criptosistemas asimétricos son únicamente una secuencia de *bits* que permiten realizar cifrado y descifrado de información; sin embargo, dicho estándar especifica parámetros para probar, certificar o atestiguar la identidad del propietario de la llave pública asociada a la privada. En otras palabras, los certificados digitales validan el uso de las llaves públicas en el proceso de firma digital.

Existen varios tipos de certificados entre los que están los personales que sirven para realizar trámites administrativos, públicos y bancarios de forma *on-line*. Los de persona jurídica que representan a una empresa y facilita que se realicen diversos trámites *on-line* entre empresas. También se pueden hallar los de servidor seguro (*SSL*[4]) que demuestran

[2] UIT-T Unión Internacional de Telecomunicadores para las Telecomunicaciones o ITU (por sus siglas en inglés International Telecommunication Union). La UIT es el organismo especializado de las Naciones Unidas para las tecnologías de la información y la comunicación – TIC. Facilita la conectividad internacional de las redes de comunicaciones mediante la elaboración de normas técnicas.

[3] *Internet of Things* (por sus siglas en inglés). La *internet* de las cosas es un sistema de dispositivos de computación interrelacionados, máquinas mecánicas y digitales, objetos, animales o personas que tienen identificadores únicos y la capacidad de transferir datos a través de una red, sin requerir de interacciones humano a humano.

[4] SSL (Security Socker Layer por sus siglas en inglés) es un protocolo de seguridad el cual que hace que sus datos viajen de manera íntegra y segura, es decir, la transmisión de los datos entre un servidor y usuario *web*, y en retroalimentación, es totalmente cifrada o encriptada.

que una empresa es titular de un sitio *web* y garantizan que se realicen operaciones seguras sobre dicha *web* y es el centro de atención de este trabajo.

Los certificados digitales de llaves públicas han transitado por varias versiones. La versión 3 es una mejora de la versión 2 e incluye una serie de extensiones que permiten validar el uso de la llave pública sobre qué acciones son permitidas realizar con ella

En la figura 4 se observan los campos que conforman un certificado. De estos algunos, que a mi criterio, son considerados campos críticos (en rojo) los cuales deben ser de especial atención por quienes navegan en internet para evitar caer en sitios falsos y exponer o comprometer información personal y/o profesional.

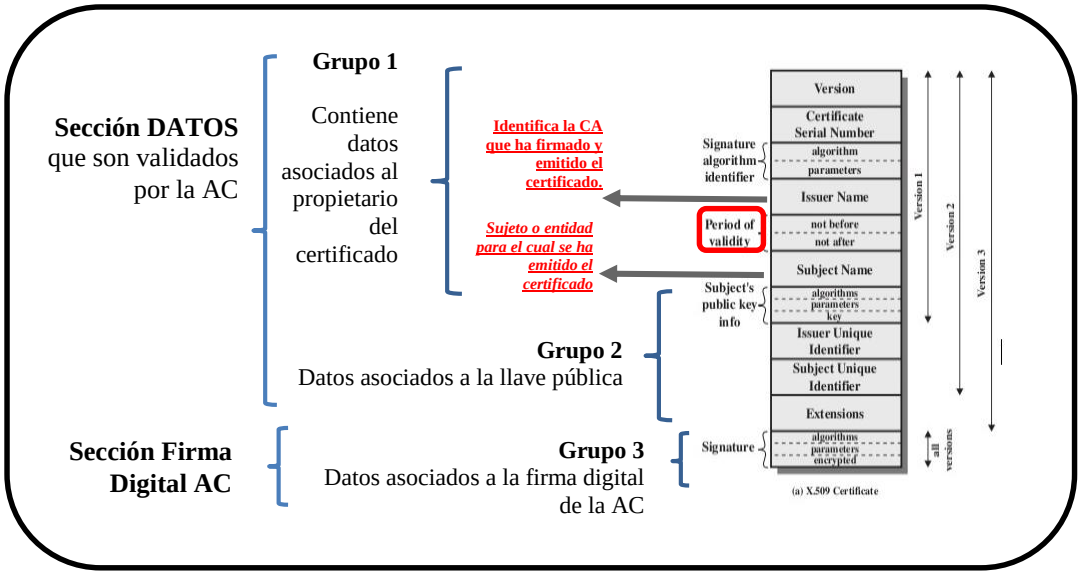

Figura 4. Campos de un certificado X.509 v3

Estos campos se dividen en tres grupos. En el primer grupo se encuentran tres campos críticos de especial atención en la navegación a sitios que funcionan bajo el protocolo *https*. El campo *Issuer Name* (Emitido por) corresponde a la Autoridad de Certificación (AC) que emitió el certificado y debe ser una AC válida y reconocida cuyo propio certificado debe estar incluido en el navegador en el almacén de certificados para Autoridades de Certificación. Un certificado firmado por una AC no reconocida no da

garantías de la identidad del sitio o titular de dicho sitio o página. Otro de los campos críticos es el *Period of validity* (Período de validez) en el cual se puede emplear el certificado para el propósito que fue emitido. El último campo es el *Subject Name* (Nombre del sujeto) que es para quien fue emitido el certificado, o sea, el titular del certificado. En el caso de una página *web* o sitio *web* el nombre o dominio que aparece en este campo debe coincidir con el servidor al cual se está accediendo en la *URL*[5] del navegador (algunos ejemplos más adelante).

El segundo grupo contiene todos los datos y parámetros asociados a la llave pública del titular del certificado. Estos son la propia llave pública y el algoritmo empleado para generarlo. Gracias a la inclusión de estos datos en el certificado, la verificación de la firma digital del titular se puede realizar en el tiempo, es decir, la firma digital pasa a ser longeva y verificable en el tiempo en caso que pasado unos años haya necesidad de verificar la integridad de alguna información mediante la verificación de la firma digital del titular y todos los parámetros asociados auto contenida en el certificado.

El tercer grupo está asociado a la validación de los campos anteriores (sección de datos) mediante la propia firma digital de la AC que emitió el certificado. La existencia de la firma digital de la AC en el certificado asegura, por parte de dicha AC que la firma, que la información de la identidad y la clave pública pertenecen al mismo usuario o entidad que posee la clave privada correspondiente.

La figura 5a es un ejemplo del certificado emitidos para el sitio *web* de la ITU. Dicho certificado esta emitido exactamente para el servidor al que se está accediendo a través del navegador. El propio certificado del sitio y el que pertenece a la AC que lo emitió y el de las otras AC que participan en la cadena de certificación están incorporados en el almacén de certificados de los navegadores. También pueden existir certificados que responden a un dominio y por tanto validan diferentes páginas bajo diferentes nombres alternativos de sujeto como muestra la figura 5b.

[5] Uniform Resource Locator (por sus siglas en inglés) Localizador Uniforme de Recusros. Se trata de la secuencia de caracteres que sigue un estándar y que permite denominar recursos dentro del entorno de Intrenet para que puedan ser localizados.

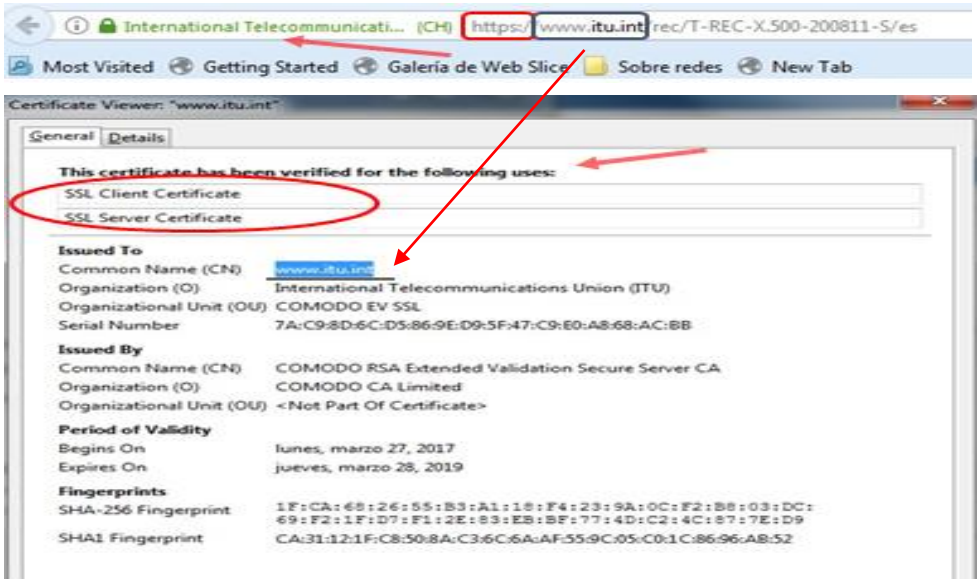

Figura 5a. Certificado para el sitio de la ITU

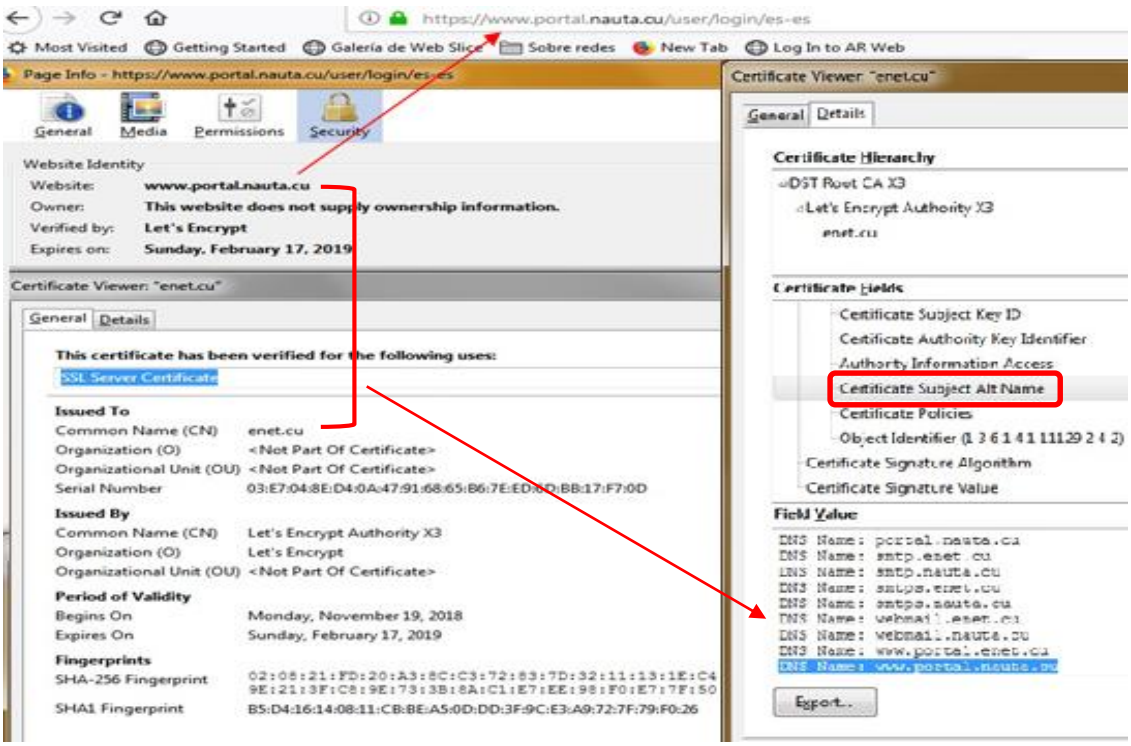

Figura 5b. Certificado para el dominio enet.cu con diferentes nombres alternativos de sujeto

Información de contacto
convencionuclv@uclv.cu
www.uclv.edu.cu

El empleo del protocolo *https* significa que entre el terminal del usuario y el servidor al que se está accediendo se genera un túnel temporal cifrado que está determinado por el empleo de los protocolos a nivel de transporte *SSL* y *TLS*[6] y, gracias a este cifrado la comunicación no podrá ser interceptada por alguien que aplicase un *sniffer* (analizador de protocolos). Esto es solamente seguro si el certificado en uso valida el 100% de la página *web*.

Es importante aclarar que existen condiciones que aunque se acceda a sitios o páginas *web* bajo el protocolo *https* no siempre se garantiza que los datos en tránsito estén protegidos bajo una conexión segura. Por ejemplo: cuando algunos componentes de la página como imágenes cuyo funcionamiento no soporta *https* o, se emplea un algoritmo de encriptación débil o, el certificado es auto firmado por una AC no reconocida o, el mismo ha sido expirado o revocado o, el dominio al que se accede desde la web no coincide con el rango definido en dicho certificado o, la longitud de la clave es menor de 2048 *bits* o, se emplea una versión obsoleta del protocolo *SSL* y *TLS*; el navegador invalida el certificado e informa que la página no es segura y por consiguiente no se establece una conexión cifrada y los datos en tránsito quedan sujetos a alteraciones. Así sucedió unos años atrás con algunos sitios como seguridad.unam.mx, twitter.com, sistrix.com y jd.com los que en la actualidad funcionan ya sin estos problemas (ver figura 6 a b).

Un sitio *web* con un certificado digital firmado por una AC reconocida garantiza que dicho sitio es de quien dice que es y por tanto la llave pública recibida le pertenece. En caso contrario no se considera un sitio seguro ya que no se tendría certeza de quien es realmente el titular de ese sitio.

[6] Transport Layer Security (por sus siglas en inglés). Seguridad de la Capa de Transporte es solo una versión actualizada y más segura de SSL.

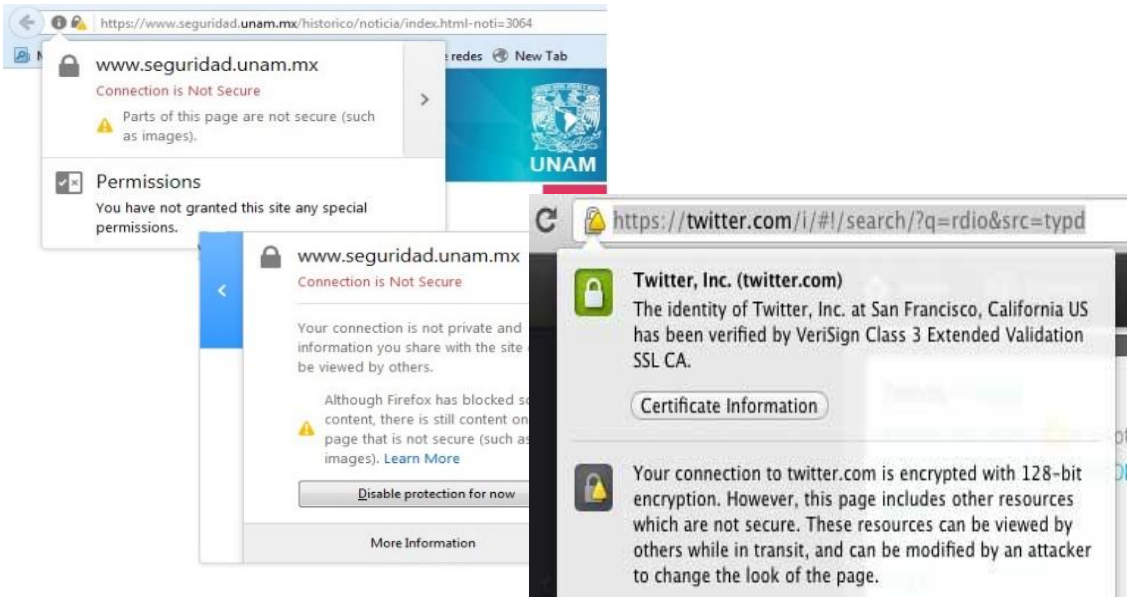

Figura 6a. Sitios no seguros completamente

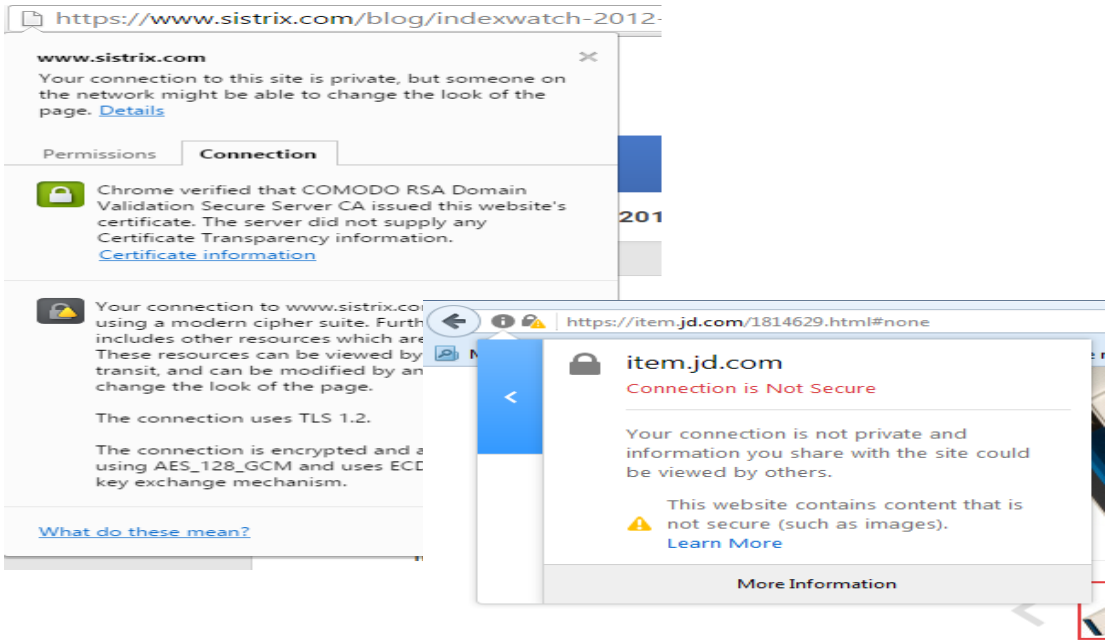

Figura 6b. Sitios no seguros completamente

Todas las acciones que intervienen en el ciclo de vida o etapas por las cuales transitan los certificados (emisión, revocación, expiración y suspensión) están determinadas por las

políticas de uso de dichos certificados. Los medios o vías de solicitud, la generación, publicación de los certificados y otras funciones relacionadas con el par de llaves asociadas a una entidad, así como las sanciones por incumplimiento de uso de los mismos están reguladas por las Infraestructuras de Llaves Públicas (PKI).

Una *PKI*, es una solución o tecnología bien posicionada basada en estándares que protege los dispositivos conectados a una red facilitando la seguridad en *IoT*. Está formada por un conjunto de elementos que se relacionan entre sí (*hardware*, *software*, bases de datos, redes, procedimientos de seguridad y obligaciones legales necesarias) para ofrecer servicios de seguridad basados en técnicas de encriptación con la finalidad de asegurar las comunicaciones y transacciones sobre las redes mediante el empleo de certificados digitales (Escalona, 2014; Simko, 2017).

Como componentes de esta solución están: las Entidades Finales (*End-Entity*) que son los titulares de los certificados, es decir para quien se han emitido los mismos. Las Autoridades de Registro (*Registration Authority*) median entre las Entidades Finales y las AC verificando toda la información presentada por dicha entidad, comprueban la relación o vínculo entre una clave pública y su propietario antes de que la AC la valide en un certificado.

Las AC constituyen la piedra angular en esta solución ya que son las que validan los certificados emitidos. Son entidades reconocidas por todos y en las que todos confían. Por tal razón, la base de las *PKI* es la confianza que hay en las AC cuya clave privada debe ser celosamente resguardada para evitar que sea comprometida y tener que revocar los certificados emitidos bajo su dominio. También como otro componente están los repositorios de certificados que contienen los certificados en uso y los revocados en una Lista de Certificados Revocados (*CRL*) y, como último componente están los propios certificados digitales o certificados X.509.

A modo de resumen se puede plantear que los criptosistemas asimétricos se emplean para el cifrado y descifrado de las comunicaciones a través del uso de dos llaves complementarias: una privada y otra pública. Las técnicas de encriptación asimétrica

intervienen, junto con las funciones *hash*, en la generación de la firma digital que garantiza de manera inequívoca y única la autenticación del emisor, el no repudio y la integridad en las transacciones electrónicas. Los certificados digitales validan la pertenecía de la llave pública con una entidad específica determinada que posee la llave privada correspondiente. El empleo de una Infraestructura de Llaves Públicas simplifica la gestión de los certificados e identidades digitales y permite establecer políticas para el empleo de los algoritmos de generación de claves, tamaño de la clave, modelo de confianza, tiempo de publicación de las *CRL* y los procedimientos de seguridad necesarios que permiten la ejecución con garantías de operaciones criptográficas como el cifrado/descifrado y firma digital de documentos electrónicos.

4. Conclusiones

La reparación de los daños causados por suplantación de identidad envuelve a las víctimas en un proceso convulsivo y extenso en el tiempo para acreditar su identidad y reclamar su patrimonio y derechos. Por esa razón se debe:

- Alertar a los usuarios de internet sobre practicar una navegación consciente no sólo para la realización de transacciones electrónicas seguras sino también para la consulta de información fidedigna.
- Enfatizar que los certificados digitales sólo son útiles cuando se va hacer uso de las claves públicas y si existe alguna AC que los valide.
- Verificar antes de exponer datos personales como tarjetas de crédito, etcétera si la *web* dispone de un certificado digital y cifra las comunicaciones (*https*) y si es así, asegurarse que el certificado valide el 100% de la página o sitio *web*.
- Comprobar la validez de los certificados mediante la revisión de los campos críticos.
- Mantener actualizados los navegadores permite, no sólo reducir los puntos vulnerables de éste que permitirían la ejecución de *software* malicioso relacionado con los fines que se ha hablado en este trabajo, sino que también da ciertas

garantías de reconocimiento de sitios *web* auténticos reduciendo los riesgos de seguridad.

- Leer las advertencias de los navegadores y prestar especial atención a aquellas páginas o sitios que al tratar de accederlos abren *pop-ups* o ventanas emergentes en primer plano ya que estas no disponen generalmente de una barra de direcciones que permita identificar los sitios *web* falseados y evitar acceder en los vínculos para evitar re direccionamientos de páginas o dominios.

5. Referencias bibliográficas

1. Escalona, S. B. (2014). *"Propuesta de Modelo de Negocio para la Implementación de una Infraestructura de Llaves Públicas en ETECSA".* (Licenciada Tesis para optar al titulo de Master en Ciencias Telematicas), Instituto Superior Politécnico Jose Antonio Echeverría

2. ESET. (2016). El impacto de la fuga de datos: 4 razones para tratar de evitarla. Retrieved from https://www.welivesecurity.com/la-es/2016/06/13/impacto-fuga-de-datos-razones-evitarla/

3. Gallego, G. (Producer). (2015). "¿Qué es y que necesidades jurídicas suple la firma electrónica?". *Píldoras de derecho de las TI y protección de datos.* Retrieved from https://www.youtube.com/watch?v=QVrXGg8Cfq8

4. Zanoletti, G. G. E. , H. D. P. y. Y. N. M. (2011). "Componentes de software para una Infraestructura de Llave Publicas", 1-2. Retrieved from informaticahabana website: www.informaticahabana.cu

5. ITRC. (2016). *"DATA BREACH REPORTS 2016 End of Year Report"*. Retrieved from https://www.idtheftcenter.org/images/breach/2016/DataBreachReport_2016.pdf

6. ITRC. (2018). *"2018 End of Year Data Breach Report"*. Retrieved from idtheftcenter.org: https://www.idtheftcenter.org

7. Martínez, M. B. (2019). "Hackers robaron casi 500 millones de registros personales en 2018". *PressDigital*. Retrieved from https://www.pressdigital.es/texto-diario/mostrar/1317960/hackers-robaron-casi-500-millones-registros-personales-2018

8. Simko, C. (2017, 20 Enero). "PKI: Las Buenas Prácticas en Seguridad Comienzan por la Identidad". Retrieved from https://www.globalsign.com/es/blog/globalsign-pki-seguridad-iot/