FEPOL
Fondo
Editorial

CERTIFICACIÓN DIGITAL CON QR </>

Gianmarco Garcia Curo

bnp biblioteca nacional del perú

CERTIFICACIÓN DIGITAL CON QR

Gianmarco Garcia Curo

Lima - 2022

CERTIFICACIÓN DIGITAL CON QR

© Gianmarco Garcia Curo
Dirección: Jr. La Mar N° 127, Huancayo – Junín, Perú
gianmarco.garcia.c@gmail.com
Tel. de contacto: +51 925 622 439

Editada por:

© Professionals On Line SAC. (FEPOL) - Fondo Editorial.
Dirección: Av. La Marina Nro: 2900, San Miguel – Lima, Perú
professionalsonline.net@gmail.com
Teléf. móvil: +51 999 140 920
Web: https://professionalsonline.net/

Coeditor
Biblioteca Nacional del Perú
Dirección: Av. De La Poesía 160, 15034 San Borja - Lima, Perú

Primera edición digital: Agosto 2022
Libro digital disponible en: https://editorialfondo.com/

Hecho el Depósito Legal en la Biblioteca Nacional del Perú N° 2022-08157
ISBN: 978-612-48981-4-3
DOI: https://doi.org/10.47422/fepol.6

Corrección de estilo: Luis Pablo Diaz Tito
luisp.diaz@upsjb.edu.pe / Tel. de contacto: +51 955 129 801

Diseño y Diagramación: Gráfica “imagen”
Manuel Enrique Sampen Antonio
sampen25@gmail.com / Tel. de contacto: +51 990 064 589

Libro resultado de Investigación y con revisión por pares doble ciego.
Sello editorial: Fondo Editorial (978-612-48981)

COTENIDO

Gianmarco Garcia Curo

Universidad Nacional de Huancavelica

AGRADECIMIENTO

Agradezco a Dios y a mi madre, por permitirme seguir publicando continuamente y contribuir a los lectores apasionados en general.

Gianmarco Garcia Curo

RESUMEN

La certificación le atribuye a un usuario haber cumplido una designación, curso o haber culminado satisfactoriamente una determinada actividad; sin embargo, a lo largo de los años su versión física está siendo desplazada por los certificados digitales, posicionándose una excelente alternativa. La certificación digital por sí misma debe contar con identificadores que permitan verificar su originalidad; sin embargo, incrustarle la verificación QR le da un valor agregado, el acceso con este tipo de identificador simplifica el proceso de verificación de originalidad, ya que se puede acceder desde cualquier equipo con lectora QR. El sistema de emisión de certificados digitales es un sistema web, dadas sus características de accesibilidad, para su desarrollo son necesarias un conjunto de herramientas y la aplicación de una metodología para garantizar el cumplimiento de requerimientos que una entidad establezca para su propio sistema de emisión de certificados. Regular la emisión de certificados es importante, la gran cantidad de entes proveedores permite una tasa mayor de falsificaciones, por ello en el Perú se promulgó

la Ley y Reglamento de Firmas y Certificados Digitales que tiene por objetivo garantizar la autenticación y a su vez la integridad de los certificados digitales.

Palabras clave: Certificados digitales, Código QR, Accesibilidad, Sistema de certificación.

INTRODUCCIÓN

El presente manuscrito da a conocer información general sobre los certificados digitales con incrustación de códigos QR. La relevancia y masificación de este tipo de certificados se inició a partir de la aparición del COVID 19. La versatilidad que poseen en sus diversas presentaciones ha permitido a instituciones estatales y privadas facilitar su proceso de certificación en Perú y el mundo, validando a los usuarios que son participes en sus diferentes eventos o actividades.

Los certificados físicos, eran susceptibles a falsificaciones continuamente, y el proceso para verificar la originalidad a su vez complejo de realizar; sin embargo, los certificados digitales contienen identificadores en la web, permitiendo que el proceso de verificación de originalidad sea simplificado y rápido.

La incrustación del código QR ha permitido la accesibilidad a los certificados digitales desde diversos dispositivos facilitando la disponibilidad de verificación de originalidad.

El manuscrito se despliega en 5 capítulos, los cuales se detallan a continuación:

Capítulo I: Se presentan generalidades de los certificados digitales, conceptos, clasificación e información detallada del tema.

Capítulo II: Se presentan generalidades de los códigos QR, relacionados a la investigación detallando aspectos relevantes.

Capítulo III: Se presentan los recursos para el desarrollo del sistema de certificación digital.

Capítulo IV: Se presentan información de la accesibilidad a los certificados digitales y como son validados.

Capítulo V: Se presentan aspectos legales que permiten la validez de los certificados digitales en el Perú.

CAPÍTULO I

Contexto de la deficiencia visual entorno al aprendizaje

Definición de certificados digitales

Según la ley N° 27269, ley de firmas y certificados digitales, define al certificado digital como "el documento electrónico generado y firmado digitalmente por una entidad de certificación, la cual vincula un par de claves con una persona confirmando su identidad" (p.187). Emplea las tecnologías de información y comunicación con los niveles de información que tienen los funcionarios para la implementación del certificado digital y permita la reducción de las barreras burocráticas.

Tipos de certificados

a. Certificados de autoridad: Las entidades emisoras de certificados raíz tienen la capacidad de asignar certificados a certificados de autoridad. Corresponden a entidades que certifican. Los certificados raíz son los únicos auto-firmados.
b. Certificados de servidor: Certifica que un servidor es de la empresa que dice ser y que el identificador del servidor es correcto. Los certificados de servidor identifican a servidores que participan en comunicaciones seguras con otros equipos mediante la utilización de protocolos de

comunicaciones. Estos certificados permiten al servidor probar su identidad ante los clientes.

c. Certificados personales: Los certificados personales aseguran que una dirección de correo y clave pública corresponden a una persona. Estos certificados identifican a personas y se pueden utilizar para autenticar usuarios con un servidor.
d. Certificados de productores de software: Se utilizan para "firmar" el software y asegurar que no ha sido modificado. Esto no implica que se pueda ejecutar con seguridad, pero informa al usuario que el fabricante de software participa en la infraestructura de compañías y entidades emisoras de certificados de confianza. Estos certificados se utilizan para firmar el software que se distribuye por Internet.

Componentes de un certificado

a. Versión: Contiene el número de versión del certificado codificado.
b. Número de serie: Es un entero asignado por la autoridad certificadora. Cada certificado emitido por una CA debe tener un número de serie único.
c. Identificador de algoritmo de firmado: Identifica el algoritmo empleado para firmar el certificado.

d. Nombre del emisor: Identifica la CA que ha firmado y emitido el certificado.
e. Periodo de validez: Indica el periodo de tiempo durante el cual el certificado es válido. Nombre del sujeto. Identifica el nombre del usuario para el que se emite el certificado.
f. Nombre del sujeto: Indica el nombre del usuario para el cual se emite el certificado.
g. Información de clave pública del sujeto
h. Identificador único del emisor: Información de la clave pública del usuario para el que se emite el certificado (nombre, algoritmo, etc.).
i. Identificador único del sujeto: Es un campo opcional que permite reutilizar nombres de sujeto.
j. Extensiones: Otros campos específicos de cada protocolo que están sujetos a sus propias regulaciones.

Propiedades de los certificados

a. Autenticación

   Para el receptor de un documento, la autentificación implica asegurar que los datos recibidos han sido enviados por quien declara ser poseedor de la identidad contenida en la firma digital. La autentificación de claves asimétricas permite que

un mensaje cifrado con una clave privada sólo pueda haber sido enviado por el propietario de la misma.

b. Confidencialidad

La confidencialidad implica asegurar que la información enviada no podrá ser interceptada por terceros. Para lograr la confidencialidad, el remitente (emisor) de un mensaje debe cifrarlo con la clave pública del destinatario (receptor), que puede obtenerse de su Certificado Digital. De esta forma el emisor se asegura que el mensaje sólo podrá ser descifrado con la clave privada del receptor, es decir, sólo podrá ser leído por el destinatario.

c. Integridad

La integridad de los documentos implica tanto para el remitente como para el destinatario asegurar que la información enviada no será modificada por terceros. Para garantizar la integridad, el remitente antes de enviar un mensaje aplica un algoritmo hash. De esta forma, al enviar un mensaje, el emisor envía el resultado del hashing cifrado junto con el mensaje original. Cuando el destinatario recibe el mensaje, recalcula el hashing del mensaje y lo compara si es igual al hashing recibido, para comprobar si el mensaje no ha sido modificado.

d. Privacidad

   La privacidad de los mensajes implica que los datos sólo podrán ser leídos por el destinatario por contener elementos cifrados.

e. No repudio

   El no repudio implica para el receptor de un mensaje asegurar que el emisor no negará haber enviado la información recibida. También como consecuencia directa del concepto de firma digital, la sola existencia del mensaje "firmado" por su clave privada, una vez comprobada su integridad, impide al emisor el repudio del mensaje, ya que el mismo no podría haberse generado por otra vía. El receptor conserva el documento firmado como comprobante de la operación.

CAPÍTULO II

Códigos QR

Código QR

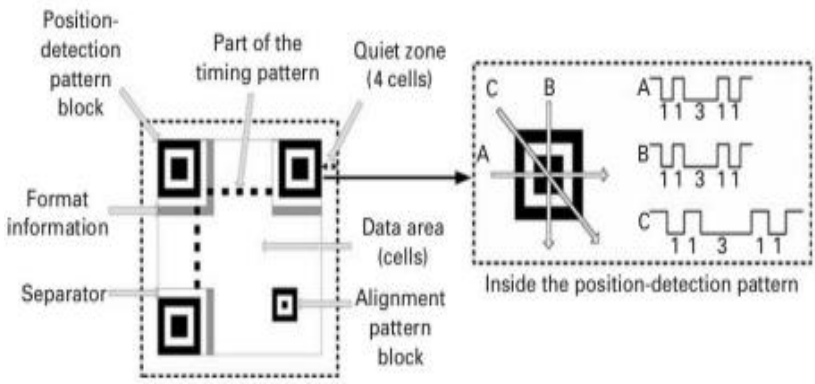
Es el acrónimo de Quick Response (respuesta rápida). Un código QR es código de barras de dos dimensiones cuya lectura se debe hacer por lectores de código QR (como las cámaras de celulares). Son similares a los códigos de barras usados en inventarios y en productos vendidos al por menor, con la excepción que pueden contener más información. De hecho, los códigos QR pueden contener miles de caracteres alfanuméricos (hasta 4000 caracteres en un solo código) haciéndolos muy útiles para cualquier organización. Generalmente, consisten en cuadrados de color negro organizados en un fondo blanco. Sin embargo, los cuadros pueden ser de colores diferentes al negro, y el fondo no debe ser necesariamente blanco.

Estructura

El código QR consiste en siete elementos conocidos como: patrón de búsqueda, patrón de tiempo, patrón de alineamiento, zona reservada, información de formato, área de información y separador.

Figura 1

Estructura del código QR



a. Patrón de búsqueda

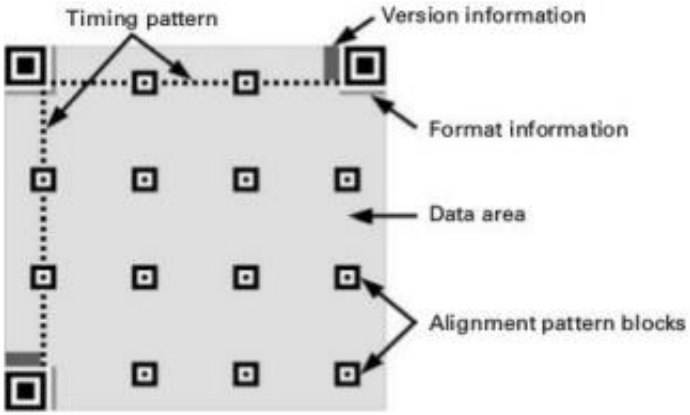
   Está localizado en tres esquinas (Ilustración 2). Cuando el código es escaneado, estos patrones son los primeros en ser localizados por el lector (cámara de dispositivo móvil), que localiza la posición del código muy rápidamente. Los radios de los espacios en blanco y negro en una línea que atraviesa el centro del patrón son 1 : 1 : 3 : 1 : 1, en cualquier ángulo. Este conjunto de radios permite la rápida detección de los tres patrones de búsqueda. Una vez la posición del código es encontrada, el tamaño L, el ángulo y la orientación son calculados a partir de la posición de los tres patrones de búsqueda. Esto permite que el código QR sea leído en cualquier dirección.

b. Patrón de tiempo

Consiste en un par de bordes (horizontal y vertical) ubicados entre los patrones de búsqueda (Ilustración 3). Dichos bordes se usan para calcular el centroide de cada celda y modificarlo cuando se encuentren distorsiones en el código QR o cambios en el campo de la celda.

Figura 2

Patrón de tiempo



c. Patrón de alineamiento

Permite la corrección de cualquier distorsión. Esto es posible determinando las coordenadas centrales de cada patrón de alineamiento y ajustando los centroides de las celdas. La celda negra aislada dentro de cada patrón de alineamiento permite calcular rápidamente la coordenada central del patrón.

d. Información de formato

   Indica la versión de código QR, el nivel de corrección de error y la máscara usada para el código QR. Además, esta área es la primera en ser leída en el proceso de decodificación.

e. Área de información

   Aquí es donde la información original y el código Reed-Solomon son codificados. El código Reed-Solomon es método matemático de corrección de errores desarrollado inicialmente para sondas planetarias y satélites artificiales como una medida para mitigar el ruido en las comunicaciones. Tiene la capacidad de hacer corrección a nivel de byte.

f. Zona reservada

   El código QR requiere una zona reservada o margen. Esta zona permite que el código sea distinguido de su color de fondo, lo cual produce una lectura precisa de forma rápida.

Corrección de error

El código QR tiene la capacidad de corrección del error, restaurando la información original si el código está sucio o dañado. Hasta el 30% del código puede ser restaurado incluso si el código QR está dañado.

Figura 3

Corrección del error QR

La corrección de errores se realiza mediante la implementación del código Reed Solomon a la información original. Hay cuatro niveles de corrección de error:

- L, aproximadamente el 7%
- M, aproximadamente el 15%
- Q, aproximadamente el 25%
- H, aproximadamente el 30%

El usuario puede seleccionar esta opción de acuerdo a sus necesidades. Entre más alta sea la corrección de error más incrementa la cantidad de información a ser codificada, lo cual implica un código QR más grande. La opción M es la más usada. El nivel de corrección de error debe ser escogido de acuerdo a la cantidad de información que lo necesita. Por ejemplo, por cada 50 de 100 palabras (en código) que necesitan corrección, se requieren 100 palabras del código Reed

Solomon. Por lo tanto, el número total de palabras es de 200. Quiere decir que 50 palabras (en código) de 200 pueden ser corregidas. Esto es una tasa del 25% de corrección de error en relación con el total de palabras, que corresponde al nivel de corrección de error Q.

Decodificación

El proceso de decodificación se compone de cuatro pasos:

a. Se localizan los patrones de búsqueda, y se calcula el centro de cada uno.

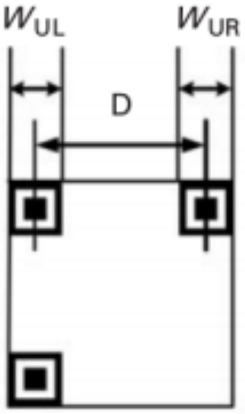
Figura 4

Localización de los patrones de búsqueda

b. Se determina el tamaño del módulo del símbolo mediante la medición de Wul y Wur; y se determina el tamaño del símbolo mediante el cálculo del tamaño de D.

Figura 5

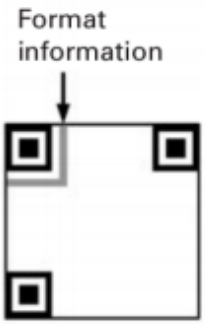
Cálculo de tamaño del módulo



c. La información de formato es decodificada y se definen el nivel de corrección de error y el patrón de enmascaramiento a usar.

Figura 6

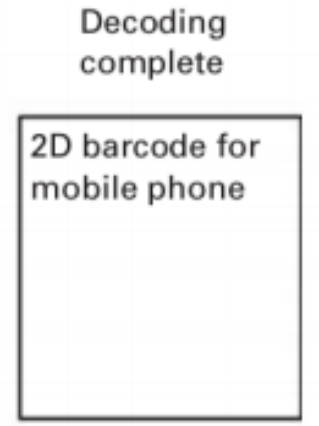
Información de formato



d. Se detecta el bloque de información y las palabras usadas para la corrección de error son removidas. La información no procesada es decodificada de acuerdo al nivel de corrección de error y al patrón de enmascaramiento definidos. Como resultado, se obtiene el texto en plano.

Figura 7

Decodificación QR



Encriptación

Es el proceso por el cual se puede transformar un mensaje en texto normal o plaintext en texto encriptado o codificado, lo que asegura que dicho texto no puede ser leído sin utilizar un proceso contrario denominado desencriptación que da lugar a la conversión del texto encriptado en texto normal. Para realizar estos procesos es requerido un algoritmo de

encriptación (función matemática), llaves de encriptación (contraseña de encriptación) y la longitud de la llave. Esto, debería usarse para conseguir cosas como: protección de datos que se transmiten a través de redes de comunicaciones, para que éstos no puedan ser interceptados, leídos o manipulados; detectar alteraciones que se puedan producir en los datos; verificar la autenticidad de una transacción, documento o mensaje; entre otras.

CAPÍTULO III

Recursos para el desarrollo del software de generación de certificados digitales

El sistema de certificación digital es un sistema web dadas sus características de accesibilidad, para su desarrollo se requieren algunas herramientas básicas, para ello es necesario considerar el lenguaje de programación, la base de datos a utilizar para almacenar los registros, en conjunto permitirán el desarrollo del sistema.

Otro aspecto importante para llevar a cabo el desarrollo adecuadamente es hacer uso de una metodología de desarrollo de software, que facilitará el proceso organizando tareas y agilizando al desarrollo, puesto que se incurrirá en menos errores al seguir una guía.

Metodología

Son conjunto de técnicas y métodos que aplicados en conjunto se aplican para el diseño de soluciones de software, actualmente existen dos grandes grupos de metodologías, las de desarrollo tradicional y las ágiles.

Metodología tradicional: Su principal característica es su proceso rígido, que específica na línea de desarrollo poco flexible, la cual no permite incluir cambios durante el proceso de desarrollo. Algunas de estas metodologías son:

- Cascada
- Espiral

Metodología ágil: Son metodologías altamente flexibles y ágiles, es incremental permitiendo en cada ciclo ir agregando funcionalidades extra que el usuario requiera incorporar. Algunas metodologías son:

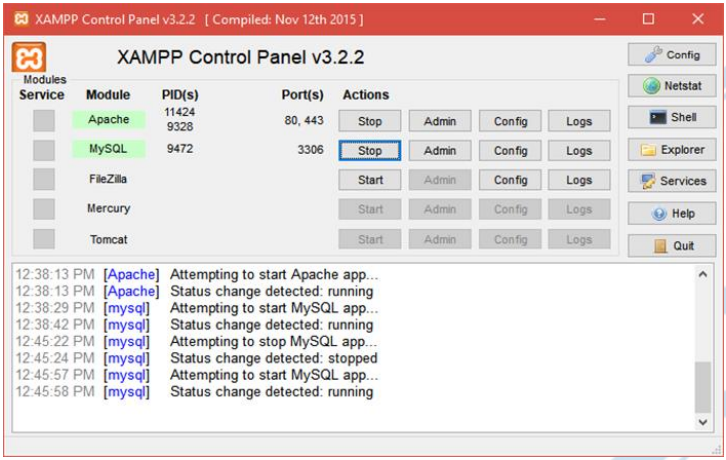
- Kanban
- Scrum
- Lean

XAMPP

XAMPP es un servidor independiente de plataforma, software libre, que consiste principalmente en el sistema de gestión de base de datos MYSQL, el servidor web Apache y los intérpretes para lenguajes de script: PHP y Perl.

Figura 8

XAMPP

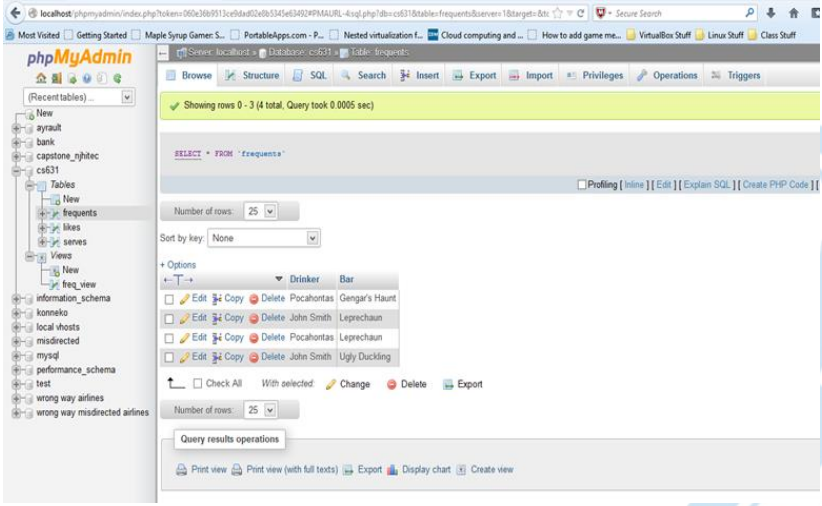


MySQL

MYSQL es un sistema de administración de bases de datos (Database Management System, DBMS) para bases de datos relacionales así, MYSQL no es más que una aplicación que permite gestionar archivos llamados de bases de datos, como base de datos relacional, utiliza *múltiples* tablas para almacenar y organizar la información. MYSQL fue escrito en C y C++ y destaca por su gran adaptación a diferentes entornos de desarrollo, permitiendo su interactuación con los lenguajes de programación más utilizados como PHP, Perl y Java y su integración en distintos sistemas operativos.

Figura 9

PhpMyAdmin



ISO 25010

Se interpreta como el grado en que dicho producto satisface los requisitos de sus usuarios, aportando de esta manera un valor (IS025010, 2019).

Para determinar la calidad, se determinaron 8 características:

1. Adecuación funcional
2. Eficiencia de desempeño
3. Compatibilidad
4. Usabilidad
5. Fiabilidad
6. Seguridad
7. Mantenibilidad
8. Portabilidad

Para propósitos de la investigación, solo se utilizaron algunas características de entre las 8 las cuales son funcionalidad, usabilidad y compatibilidad.

Compatibilidad

Capacidad del sistema de intercambiar información con otros sistemas o entre sus propios componentes cuando comparte un mismo entorno hardware y software. Esta característica está dividida en dos:

- Coexistencia. Capacidad de coexistencia con otro software diferente en un mismo entorno, compartiendo recursos.
- Interoperabilidad. Capacidad de realizar intercambio de información entre sistemas y hacer uso de la información intercambiada.

Usabilidad

Capacidad del software para ser comprendido, utilizado y resultar atractivo al usuario al ser utilizada en determinadas condiciones. Esta subdividida en otras características:

- Capacidad para reconocer su adecuación. Capacidad que permite reconocer si el producto es adecuado para el tipo de usuario y sus necesidades.
- Capacidad de aprendizaje. Capacidad que permite al usuario aprender a utilizarlo.
- Capacidad para ser usado. Capacidad del producto que permite al usuario manipularlo y utilizarlo con facilidad.
- Protección contra errores del usuario. Capacidad que protege al usuario de cometer errores.
- Estética de la interfaz de usuario. Capacidad de agradar y satisfacer una adecuada interacción con el usuario.
- Accesibilidad. Capacidad que permite que el producto sea utilizado por usuarios con características específicas.

Fiabilidad

Capacidad del producto para desempeñar su función al ser puesto en uso. Esta característica esta subdividida en 4 características:

- Madurez. Capacidad de satisfacer con fiabilidad en condiciones normales.
- Disponibilidad. Capacidad el sistema de estar operativo y a disposición para su uso cuando sea requerido.
- Tolerancia a fallos. Capacidad del sistema de seguir en marcha en presencia de fallos hardware o software.
- Capacidad de recuperación. Capacidad de recuperar y reestablecer el estado del sistema en caso de interrupción o fallo.

Lenguajes de programación web

Definición

Son aquellos lenguajes que son asimilados directamente por el navegador y no necesitan pre tratamiento. Los lenguajes de programación Web han ido surgiendo según las necesidades de las plataformas, intentando facilitar el trabajo a los desarrolladores de aplicaciones. Se clasifican en lenguajes del lado cliente y lenguajes del lado servidor.

PHP

PHP es un acrónimo recursivo para "PHP: Hypertext Preprocessor", originalmente Personal Home Page, es un lenguaje interpretado libre, usado originalmente solamente para el desarrollo de aplicaciones presentes y que actuaran en el lado del servidor, capaces de generar contenido dinámico en la World Wide Web. Figura entre los primeros lenguajes posibles para la inserción en documentos HTML, dispensando en muchos casos el uso de archivos externos para eventuales procesamientos de datos.

El código es interpretado por el lado del servidor por el módulo PHP, que también que genera la página web para ser visualizada en el lado del cliente. El lenguaje evolucionó, pasó a ofrecer funcionalidades en la línea de comandos, y además, ganó características adicionales, que posibilitaron usos adicionales del PHP.

HTML

Desde el surgimiento de internet se han publicado sitios web gracias al lenguaje HTML. Es un lenguaje estático para el desarrollo de sitios web (acrónimo en inglés de HyperText Markup Language, en español Lenguaje de Marcas Hipertextuales). Desarrollado por el World Wide Web

Consortium (W3C). Los archivos pueden tener las extensiones (htm, html).

Javascript

Este es un lenguaje interpretado, no requiere compilación. Fue creado por Brendan Eich en la empresa Netscape Communications. Utilizado principalmente en páginas web. Es similar a Java, aunque no es un lenguaje orientado a objetos, el mismo no dispone de herencias. La mayoría de los navegadores en sus últimas versiones interpretan código Javascript.

El código Javascript puede ser integrado dentro de nuestras páginas web. Para evitar incompatibilidades el World Wide Web Consortium (W3C) diseño un estándar denominado DOM (en inglés Document Object Model, en su traducción al español Modelo de Objetos del Documento).

Ajax

De siglas en inglés "Asynchronous JavaScrip and XML". Es un conjunto de técnicas nuevas, que envuelven diversas tecnologías antiguas como JavaScript, XML, Document Object Model (DOM), que permite al cliente comunicarse con el servidor a través de este request, que es realizado en segundo plano, sin recargar la página, uniendo de manera efectiva y

eficiente la tecnología client- side con la tecnología server-side y potencializando la comunicación.

CSS

Sus siglas en ingles vienen de Cascading Style Sheets(CSS), son bloques de código en lenguaje XML o XHTML que se encargan de separar dentro del documento HTML el estilo lógico del estilo físico, siendo l estilo lógico la estructura del documento y el estilo físico su aspecto final. Las hojas de estilo permiten redefinir las reglas para presentar una página web.

Términos sobre los certificados digitales con QR

La definición de términos permitirá clarificar términos clave presentados.

Certificado digital: El Certificado Digital es un documento digital que garantiza y permite identificar a las personas en Internet.

Código QR: Combinación de barras y cuadros que acompaña a un producto o unidad de consumo para que pueda ser leído y descifrado mediante un lector óptico que transmite los datos a una máquina o una computadora.

Verificación de originalidad: Es el acto de confirmar que un documento o creación sea original.

Metodología: Conjunto de procedimientos racionales utilizados para alcanzar el objetivo o la gama de objetivos que rige una investigación científica.

CAPÍTULO IV

Recursos para el desarrollo del software de generación de certificados digitales

Accesibilidad

La accesibilidad a los certificados digitales es una de las características que le dan un valor añadido, permitiendo tanto a usuarios como proveedores de los certificados acceder a estos en tiempo real, asimismo poder adquirirlos una y otra vez, ya que el documento original se almacena en internet. Para acceder a estos en tiempo real es necesario:

Celular, computador o punto de acceso: Debe contar con la que cuente con la tecnología para acceder a internet.

Sistema de Intermediación Electrónico. - Es el sistema WEB que permite la transmisión y almacenamiento de información, garantizando el no repudio, confidencialidad e integridad de las transacciones a través del uso de componentes de firma electrónica, autenticación y canales seguros.

Sistema WEB ("World Wide Web"): Sistema de documentos electrónicos enlazados y accesibles a través de Internet. Mediante un navegador Web, un usuario visualiza páginas Web que pueden contener texto, imágenes, vídeos u otros contenidos multimedia, y navega a través de ellas usando hiperenlaces.

Verificación

Si bien el certificado en sin mismo ya sea en su formato digital o físico permite verificar ciertos datos y credenciales, a primera vista pueden ser falsificados con fines maliciosos, corrompiendo su integridad. Para poder verificar la originalidad se consideran:

Número de serie: Es el entero asignado por la autoridad certificadora. Cada certificado posee un número único e irrepetible para el tipo de certificado que brinda el proveedor.

Código QR: Posee un identificador único que en la web direcciona a la ubicación del certificado digital, en la que se deben ver las mismas características del certificado que se verifica, en caso no coincida la información, sería una falsificación del mismo.

CAPÍTULO V

Sustento legal en el Perú

La certificación digital ha pasado de ser una tendencia a convertirse en un documento ampliamente aceptado tanto en entidades estatales como en entidades privadas. Los certificados emitidos son únicos para cada usuario; sin embargo, la emisión masiva de estos, permite a facinerosos llevar a cabo la falsificación con fines de negocio o personales, este es un grave problema que debe afrontarse.

La regularización es necesaria para evitar fraudes y a su vez dar validez a este tipo de certificados, el Estado Peruano ha promulgado la Ley Nº 27269 de Firmas de Certificados Digitales y el Reglamento de la Ley de Firmas y Certificados digitales (2008) que establecen parámetros claros que se deben considerar para que un certificado sea reconocido como original.

Los actores en este proceso no son únicamente las organizaciones que brindan la certificación, el usuario receptor tiene que ceñirse a aspectos de la ley.

Algunos aspectos relevantes según la Ley Nº 27269 de Firmas de Certificados Digitales y el Reglamento de la Ley de Firmas y Certificados digitales (2008) son:

Finalidad de la ley de firmas y certificados digitales

La finalidad de la ley es regular el uso de la firma digital que tiene la misma validez y eficacia que una firma manuscrita, si se adjunta este a cualquier documento electrónico ya hay un vínculo con el firmante, por ende, se debe garantizar la autenticación entidad de estos documentos.

Firma digital

Artículo 3.- Firma digital La firma digital es aquella firma electrónica que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada.

Del titular de la firma

Artículo 4.- Titular de la firma digital El titular de la firma digital es la persona a la que se le atribuye de manera exclusiva un certificado digital que contiene una firma digital, identificándolo objetivamente en relación con el mensaje de datos.

Artículo 5.- Obligaciones del titular de la firma digital El titular de la firma digital tiene la obligación de brindar a las entidades de certificación y a los terceros con quienes se

relacione a través de la utilización de la firma digital, declaraciones o manifestaciones materiales exactas y completas.

De los certificados digitales

Artículo 6.- Certificado digital El certificado digital es el documento electrónico generado y firmado digitalmente por una entidad de certificación, la cual vincula un par de claves con una persona determinada confirmando su identidad.

Artículo 7.- Contenido del certificado digital Los certificados digitales emitidos por las entidades de certificación deben contener al menos:

1. Datos que identifiquen indubitablemente al suscriptor.
2. Datos que identifiquen a la Entidad de Certificación.
3. La clave pública.
4. La metodología para verificar la firma digital del suscriptor impuesta a un mensaje de datos.
5. Número de serie del certificado.
6. Vigencia del certificado.
7. Firma digital de la Entidad de Certificación.

Artículo 8.- Confidencialidad de la información La entidad de registro recabará los datos personales del solicitante de la firma digital directamente de éste y para los fines señalados en la

presente ley. Asimismo, la información relativa a las claves privadas y datos que no sean materia de certificación se mantiene bajo la reserva correspondiente. Sólo puede ser levantada por orden judicial o pedido expreso del suscriptor de la firma digital.

Artículo 9.- Cancelación del certificado digital La cancelación del certificado digital puede darse:

1. A solicitud del titular de la firma digital.
2. Por revocatoria de la entidad certificante.
3. Por expiración del plazo de vigencia.
4. Por cese de operaciones de la Entidad de Certificación.

Artículo 10.- Revocación del certificado digital La Entidad de Certificación revocará el certificado digital en los siguientes casos:

1. Se determine que la información contenida en el certificado digital es inexacta o ha sido modificada.
2. Por muerte del titular de la firma digital.
3. Por incumplimiento derivado de la relación contractual con la Entidad de Certificación.

Artículo 11.- Los Certificados de Firmas Digitales emitidos por Entidades Extranjeras tendrán la misma validez y eficacia jurídica reconocidas en la presente Ley, siempre y cuando tales

certificados sean reconocidos por la autoridad administrativa competente.

Entidad certificadora

Artículo 12.- Entidad de Certificación La Entidad de Certificación cumple con la función de emitir o cancelar certificados digitales, así como brindar otros servicios inherentes al propio certificado o aquellos que brinden seguridad al sistema de certificados en particular o del comercio electrónico en general. Las Entidades de Certificación podrán igualmente asumir las funciones de Entidades de Registro o Verificación.

Artículo 13.- Entidad de Registro o Verificación La Entidad de Registro o Verificación cumple con la función de levantamiento de datos y comprobación de la información de un solicitante de certificado digital; identificación y autenticación del suscriptor de firma digital; aceptación y autorización de solicitudes de emisión de certificados digitales; aceptación y autorización de las solicitudes de cancelación de certificados digitales.

Artículo 14.- Depósito de los Certificados Digitales Cada Entidad de Certificación debe contar con un Registro disponible en forma permanente, que servirá para constatar la

clave pública de determinado certificado y no podrá ser usado para fines distintos a los estipulados en la presente ley. El Registro contará con una sección referida a los certificados digitales que hayan sido emitidos y figurarán las circunstancias que afecten la cancelación o vigencia de los mismos, debiendo constar la fecha y hora de inicio y fecha y hora de finalización. A dicho Registro podrá accederse por medios telemáticos y su contenido estará a disposición de las personas que lo soliciten. **Artículo 15.-** Inscripción de Entidades de Certificación y de Registro o Verificación El Poder Ejecutivo, por Decreto Supremo, determinará la autoridad administrativa competente y señalará sus funciones y facultades. La autoridad competente se encargará del Registro de Entidades de Certificación y Entidades de Registro o Verificación, las mismas que deberán cumplir con los estándares técnicos internacionales. Los datos que contendrá el referido Registro deben cumplir principalmente con la función de identificar a las Entidades de Certificación y Entidades de Registro o Verificación. "Artículo 15-A.- Régimen de Infracciones y Sanciones La autoridad administrativa competente tiene la facultad de tipificar las infracciones por incumplimiento de lo establecido en la Ley 27269, Ley de Firmas y Certificados Digitales, su Reglamento

y las Guías de Acreditación de la Autoridad Administrativa Competente. La autoridad competente podrá imponer las siguientes sanciones:

1. Multa, hasta un monto máximo de cincuenta (50) UIT.
2. Suspensión temporal de la acreditación.
3. Cancelación de la acreditación.

Las infracciones serán establecidas como leves, graves y muy graves; y la determinación de la sanción se establecerá teniendo en cuenta criterios de proporcionalidad. Cuando se trate de infracciones muy graves, la autoridad competente adicionalmente podrá disponer la inhabilitación hasta por diez (10) años para solicitar nuevamente la acreditación como entidad de certificación, de registro o verificación de datos, prestadora de servicios de valor añadido o como entidad de software de firma digital. La autoridad competente aprobará el correspondiente reglamento de infracciones y sanciones que comprenda la tipificación de las infracciones administrativas, el procedimiento administrativo sancionador y la escala de sanciones correspondiente.”

Reglamento de la ley de firmas y certificados digitales

Artículo 12.- De los requisitos Para la obtención de un certificado digital, el solicitante deberá acreditar lo siguiente:

a) Tratándose de personas naturales, tener plena capacidad de ejercicio de sus derechos civiles.
b) Tratándose de personas jurídicas, acreditar la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva, debiendo contar con un representante debidamente acreditado para tales efectos.

Artículo 13.- De las especificaciones adicionales para ser titular Para ser titular de un certificado digital adicionalmente se deberá cumplir con entregar la información solicitada por la Entidad de Registro o Verificación, de acuerdo a lo estipulado por la Entidad de Certificación correspondiente, asumiendo el titular la responsabilidad por la veracidad y exactitud de la información proporcionada, sin perjuicio de la respectiva comprobación. En el caso de personas naturales, la solicitud del certificado digital y el registro o verificación de su identidad son estrictamente personales. La persona natural solicitante se constituirá en titular y suscriptor del certificado digital.

Artículo 15.- De las obligaciones del titular Las obligaciones del titular son:

a) Entregar información veraz durante la solicitud de emisión de certificados y demás procesos de certificación (cancelación, suspensión, re-emisión y modificación).
b) Actualizar la información provista tanto a la Entidad de Certificación como a la Entidad de Registro o Verificación, asumiendo responsabilidad por la veracidad y exactitud de ésta.
c) Solicitar la cancelación de su certificado digital en caso de que la reserva sobre la clave privada se haya visto comprometida, bajo responsabilidad.
d) Cumplir permanentemente las condiciones establecidas por la Entidad de Certificación para la utilización del certificado.

Artículo 16.- Del contenido y vigencia Los certificados emitidos dentro de la Infraestructura Oficial de Firma Electrónica deberán contener como mínimo, además de lo establecido en el artículo 7 de la Ley, lo siguiente:

a) Para personas naturales:

* Nombres completos
* Número de documento oficial de identidad
* Tipo de documento

b) Para personas jurídicas:

* Razón social
* Número del Registro Único de Contribuyentes (RUC)
* Nombres completos del suscriptor
* Número de documento oficial de identidad del suscriptor
* Tipo de documento del suscriptor

La Entidad de Certificación podrá incluir indistintamente, a pedido del solicitante del certificado, la dirección oficial de correo electrónico del suscriptor, la dirección oficial de correo electrónico de la persona jurídica o el domicilio electrónico del solicitante. Asimismo, podrá incluir información adicional siempre y cuando la Entidad de Registro o Verificación compruebe de manera fehaciente la veracidad de ésta. El período de vigencia de los certificados digitales comienza y finaliza en las fechas indicadas en él, salvo en los supuestos de cancelación conforme a lo establecido en el artículo 17 del presente Reglamento.”

Conclusiones

Los certificados digitales, son una alternativa viable para cualquier entidad que requiera proveerlos a sus usuarios; de forma tradicional estos requieren un proceso extenso para su expedición y poseen una tendencia a ser falsificados, dada sus características y tediosa forma de verificar la originalidad. La alternativa digital es una opción que sustituye a la tradicional certificación física, brindando accesibilidad continua y facilitando la forma de verificar la originalidad

Recomendaciones

Se recomienda sustituir de forma progresiva la certificación tradicional y migrar a la certificación digital, la digitalización provee de beneficios tanto a usuarios como proveedores, permitiendo simplificar procesos y automatizarlos.

Es necesario tener conocimiento de algunas normas que permitan reglamentar el proceso de certificación, así como definir la estructura que se manejará a nivel organizacional, logrando la diferenciación y reconocimiento de la organización.

Es recomendable tener un respaldo de los certificados digitales, dado su almacenamiento en la web, contar con un respaldo permitirá no perder los archivos y evitar futuros problemas de accesibilidad.

Referencias

Diario Oficial del Bicentenario El Peruano. (2008). El Peruano. Obtenido de https://diariooficial.elperuano.pe/pdf/0030/ley-27269.pdf

Bravo Carranza , L. A., & Aguilar Arboleda, G. H. (2019). Módulo de emisión de certificado con código QR y depuración del sistemas web de seguimiento de actividades de los pasantes del Consultorio Jurídico De La Facultad De Jurisprudencia De La Universidad De Guayaquil. Repositorio Institucional de la Universidad de Guayaquil. Obtenido de http://repositorio.ug.edu.ec/handle/redug/39743

Date C, C. (s.f.). Introducción a los sistemas de dases de datos. Ed. Pearson.

Espino Canelo, J. A. (2018). Aplicación web para la mejora de la gestión del almacén de suministros en San Fernando S.A.C. Tesis, Universidad Inca Garcilzo de la Vega. Obtenido de http://repositorio.uigv.edu.pe/bitstream/handle/20.500.11818/3320/TESIS-JESUS%20ALBERTO%20ESPINO%20CANELO.pdf?sequence=2&isAllowed=y

Gabaldón, L. G., & Pereira, W. (2008). Usurpación de identidad y certificación digital: propuestas para el control del fraude electrónico. Sociologías, 20. doi:https://doi.org/10.1590/S1517-45222008000200008

Gamboa Cruzado, J., Comun Manrique, U., & Bruno Luciani, I. (2016). Desarrollo de un sistema de informacion, basado en la metodologia RUP, para mejorar el proceso de matricula en el colegio Von Humboldt del Sur. Universidad Autónoma del Perú. Universidad Autónoma del Perú. Obtenido de http://repositorio.autonoma.edu.pe/handle/AUTONOMA/149

Jayo Cusipoma, H. (2019). Sistema de ifnormación web para optimizar la gesión de certificados de inspección de hermiticidad de la empresa Hertig, Lima - 2019. Universidad Científica del Sur. Obtenido de https://repositorio.cientifica.edu.pe/bitstream/handle/20.500.12805/852/TB-Herica%20J%28Restringido%29.pdf?sequence=1&isAllowed=y

Munevar Bejarano, F. A., & Chavarro Muñoz , J. K. (2018). Sistema de validación web de documentos mediante escaneo de códigos QR haciendo uso de dispositivos móviles. Universidad Distrital Francisco José de Caldas. Obtenido de https://repository.udistrital.edu.co/bitstream/handle/11349/14

196/ChavarroMu%c3%b1ozJohnKenedy2018.pdf?sequence=1&isAllowed=y

Rivas Lara, A. E. (s.f.). Influencia del uso del certificado digital en el proceso de formalización de negocios en la Municipalidad Distrital de Pítipo - Ferreñafe en el 2020. Universidad de Lambayeque. Obtenido de https://repositorio.udl.edu.pe/bitstream/UDL/408/1/RivasLara_Tesis%20IC.pdf

Sandoval Medrano, H. A., & Sandoval Medrano, G. B. (2015). Análisis y diseño de un Framework JavaScript basado en los estándares de la W3C para la implementación en Front-End de Juliaca.com. Universidad Andina Néstor Caceres Velásquez. Universidad Andina Néstor Caceres Velásquez. Obtenido de http://repositorio.uancv.edu.pe/bitstream/handle/UANCV/747/TESIS%2041440198%20%26%2002549288.pdf?sequence=3&isAllowed=y

CERTIFICACIÓN DIGITAL CON QR

Gianmarco Garcia Curo

Scopus Author ID: 57290570700
Web of Science Researcher ID: 3514656
Dialnet Autor ID: 5436347
Código Renacyt: P0224148

FEPOL
Fondo Editorial

CERTIFICACIÓN DIGITAL CON QR

bnp biblioteca nacional del perú

Gianmarco Garcia Curo