CONCEPTUALIZACIÓN DEL RESUMEN DE MENSAJES Y CERTIFICADO DIGITAL

CONCEPTUALIZATION OF THE SUMMARY OF MESSAGES AND DIGITAL CERTIFICATE

AUTORES: Navira Gissela Angulo Murillo[1]

Francisco Bolaños Burgos[2]

Gabriel García Murillo[3]

Alex Gregorio Mendoza[4]

DIRECCIÓN PARA CORRESPONDENCIA: Universidad de Especialidades Espíritu Santo, Guayaquil, Ecuador, nangulo@uees.edu.ec

Fecha de recepción: 04-06-2017

Fecha de aceptación: 10-07-2017

RESUMEN

En la actualidad las tecnologías de la información y comunicación constituyen uno de los factores de innovación en los negocios, cada vez hay más compradores online que requieren productos y servicios como elemento clave para el comercio electrónico. En este artículo se realiza la revisión de varios conceptos y definiciones sobre el resumen de mensajes y certificado digital, con el propósito extraer y analizar elementos de base para su conceptualización. Se aplicó la metodología cualitativa, que consistió en la recopilación de definiciones, selección de elementos claves para para la medición de los objetos de estudio, se analizaron, cuantificaron los resultados y finalmente se conceptualizan los términos: resumen de mensajes y certificado digital. Se concluye con la exposición detallada y organizada de los conceptos relacionados al resumen de mensajes y certificado digital, los mismos que servirán de plataforma para futuras investigaciones, relacionadas con el marco legislativo del certificado digital en las transacciones comerciales. Como limitante del estudio, se establece la cantidad de fuentes empleadas y

[1] Universidad de Especialidades Espíritu Santo, Guayaquil, Ecuador. Ingeniera en Sistemas y magíster en Dirección Estratégica de las Tecnologías de la Información y Comunicación en la universidad Nacional de Piura – Ecuador, en proceso de elaboración de tesis para obtener el título de magíster en Auditoría de las Tecnologías de la Información y Comunicación, Universidad de Especialidades Espíritu Santo de Guayaquil. Se desempeña como Coordinadora de Planificación Estratégica y Operativa en la Universidad Laica Eloy Alfaro de Manabí, Ecuador.

[2] Universidad Espíritu Santo – Ecuador, Samborondón, Guayas, Ecuador. Ingeniero en Computación y magíster en seguridad informática aplicada de la Escuela Superior Politécnica del Litoral (ESPOL) en Guayaquil, Ecuador. Se desempeña como director de la Maestría en Auditoría de Tecnologías de la Información (MATI). Enseña criptografía, hackeo ético y seguridad de la información en la Facultad de Postgrados en UEES. Sus líneas de investigación son: seguridad de la información y herramientas de evaluación (rubrics y scripts). Email: fcobolanos@uees.edu.ec

[3] Magíster. Profesor a tiempo completo. Vice-Decano de la Facultad de Filosofía, Letras y Ciencias de la Educación de la Universidad Técnica de Manabí. Portoviejo, Ecuador. E-mail: grgarcia@utm.edu.ec

[4] Universidad de Especialidades Espíritu Santo, Guayaquil, Ecuador. Ingeniera en Sistemas y magíster en Dirección Estratégica de las Tecnologías de la Información y Comunicación en la universidad Nacional de Piura – Ecuador, en proceso de elaboración de tesis para obtener el título de magíster en Auditoría de las Tecnologías de la Información y Comunicación, Universidad de Especialidades Espíritu Santo de Guayaquil. Email: alexmendoza@uees.edu.ec

términos extraídos de las definiciones, en virtud de la variedad de documentos publicados y otros que apenas empiezan su desarrollo.

PALABRAS CLAVE: Conceptualización; resumen de mensajes; certificado digital; autoridad certificadora.

ABSTRACT

Today information and communication technologies are one of the factors of innovation in business; there are more and more online shoppers who require products and services as a key element for electronic commerce. In this article we review several concepts and definitions about message digest and digital certificate, with the purpose of extracting and analyzing basic elements for its conceptualization. The qualitative methodology was applied, which consisted in the collection of definitions, selection of key elements for the measurement of the objects of study, analyzed, quantified the results and finally conceptualized the terms: message summary and digital certificate. It concludes with a detailed and organized presentation of the concepts related to message digest and digital certificate, which will serve as a platform for future research, related to the legislative framework of the digital certificate in commercial transactions. As a limitation of the study, it establishes the number of sources used and terms extracted from the definitions, by virtue of the variety of published documents and others that are just beginning their development.

KEYWORDS: Conceptualization; message summary; digital certificate; certification authority.

INTRODUCCIÓN

Según Giménez (2014), la criptografía es la ciencia que estudia las técnicas para escribir en clave o de un modo enigmático, con la finalidad de garantizar la comunicación secreta entre dos personas o entidades. No obstante, la criptografía ha evolucionado en las últimas décadas, con importantes investigaciones que plantean el uso de operaciones matemáticas, que cimentaron las bases de la teoría de la información (Shannon, 1949) y la clave pública o criptografía asimétrica (Diffie y Hellman, 1976).

Un empuje decisivo de la ciencia es la aplicación de los algoritmos criptográficos, es así, que 1978 se propone el hasta hoy más usado método de firma digital denominado RSA, (Rivest, Shamir, y Adleman, 1978). También se realizaron otros estudios investigativos, que se basan en el problema matemático del logaritmo discreto, adoptado actualmente para generar firmas digitales (El Gamal, 1985).

Cabe recalcar, que en el año de 1991 el Instituto Nacional de Normas y Tecnología de los Estados Unidos propone el algoritmo para uso del Estándar Digital (DSS), que se utiliza para firmar y cifrar información. Posteriormente, en 1995 se crea la primera ley en materia digital denominada “Utah Digital Signature Act”, cuyo objetivo fue facilitar mediante mensajes electrónicos y firmas digitales las transacciones (Iriarte, 1999).

Con la aparición de la criptografía moderna, se dio paso a nuevos conceptos importantes como la criptografía asimétrica o de clave pública (Diffie y Hellman, 1976), la cual abrió el abanico en la aplicación de la firma digital, que se define como un conjunto de datos adjuntos a un mensaje electrónico, que utiliza un método de encriptación asimétrico (Contreras, 2011). Al respecto, González y Quintero (2006), mencionan que el certificado digital es el único medio que permite garantizar técnica y legalmente la identidad de una persona en internet.

Dentro del marco descriptivo de este estudio, es importante abordar aspectos epistemológicos de la Criptología, tal como establece Guyot (2005), quien relata acerca de la relación entre el conocimiento teórico y práctico, de igual modo se considera la teoría de Braga (1994, p.78) que expone desde este enfoque "la relación teórica – práctica es una relación unidireccional, que se manifiesta en la capacidad del conocimiento para controlar la práctica […]"; desde este punto de vista, se justifica la importancia de la conceptualización de la firma digital y certificado electrónico, porque en ocasiones se puede cuestionar la inadecuada interpretación de conceptos en las aplicaciones prácticas.

En conexión con el objeto de estudio, así mismo, en este artículo se fundamentan teoóricamente otros conceptos importantes de la criptografía; que sirven de apoyo para la comprensión de la firma digital, certificado digital y autoridad certificadora, elementos fundamentales para el desarrollo del comercio electrónico (De Miguel, 2004)

Por otra parte, Gutiérrez (2009), refiere acerca de la importancia que desempeñan las entidades de certificación de firmas digitales, por lo que es primordial conocer mecanismos de seguridad en todas las aristas del comercio electrónico. El incremento de actividades electrónicas a través de internet, requiere la necesidad urgente de conocer y comprender la definición de la firma electrónica y el certificado digital, para que el usuario tenga conocimiento de cómo intercambiar información de forma segura a través de la red, puesto que a lo largo de la historia se mantiene latente la necesidad de proteger la información y generar ambientes de confianza en los sistemas (Stallings, 2004).

El presente trabajo tiene como objetivo principal analizar varias definiciones relacionadas al resumen de mensajes y certificado digital, con la finalidad de obtener una base consistente que permita conceptualizar los elementos estudiados.

DESARROLLO

Criptología

Según la interpretación de Granados (2006), la criptografía proviene de una rama de las matemáticas descubierta por Claude Elwood Shannon en 1948 denominada teoría de la información, ésta a su vez se subdivide en teoría de códigos y criptología, finalmente se deriva en criptoanális y criptografía.

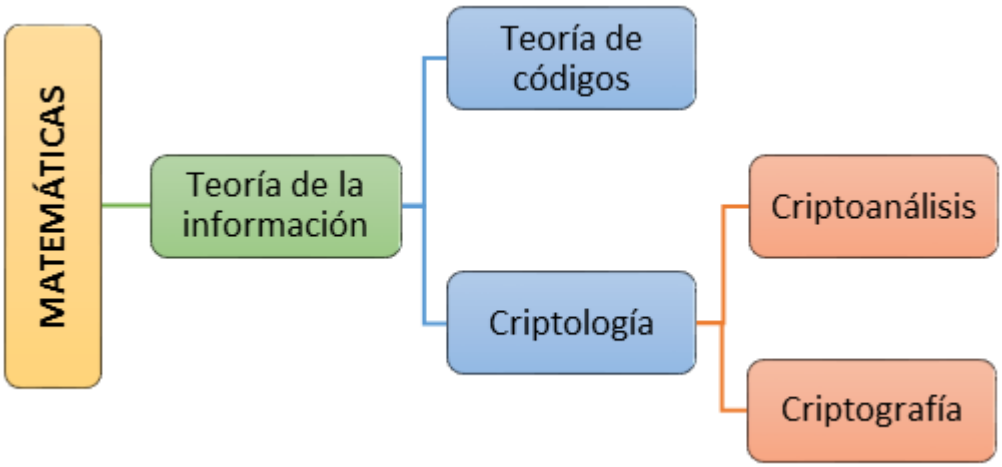

Figura 1: Origen de la Criptología. Fuente: (Granados, 2006)

Por su parte, Gallardo (1992) sostiene que la criptología es una disciplina matemática que estudia las técnicas para ocultar información y garantizar su confidencialidad y autenticidad. De igual manera, Calabuig (1999) indica que es una ciencia que trata los problemas relacionados con la seguridad de los mensajes en clave entre un emisor, receptor y el canal de comunicaciones.

Solis y Galdeno (2015), afirman que esta ciencia comprende dos ramas: criptografía y criptoanálisis, que son técnicas empleadas para encontrar debilidades en los sistemas criptográficos.

En la figura 2 se muestra la clasificación de la Criptología:

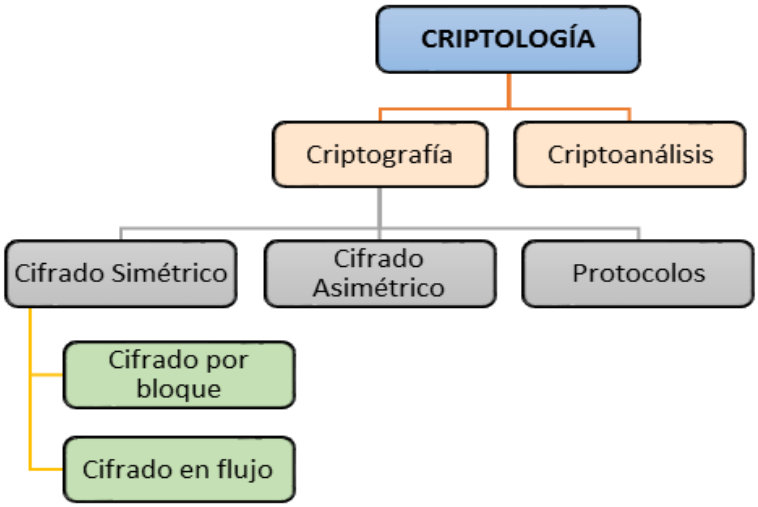

Figura 2: Clasificación de la Criptología. Fuente: (Paar y Pelzl, 2010)

Criptografía

Galende (1995) define la criptografía como la ciencia que estudia la escritura oculta o el arte para escribir mediante el uso de claves; por su parte Mario y Sancho (2003) señalan que es una disciplina relacionada con el envío de mensajes secretos a través de un sistema.

Marrero (2003), menciona que la criptografía es una rama de las matemáticas que proporciona las herramientas necesarias para solucionar problemas relacionados con la autenticidad y la confiabilidad. Del mismo modo, Ángel (2000) argumenta que la criptografía resuelve los principales inconvenientes de seguridad como: la privacidad, la integridad, la autenticación y el no rechazo. Porolli (2013), agrega que el cifrado de los datos es indispensable no sólo en las comunicaciones, sino también en la protección de información sensible en las organizaciones.

Como complemento, Rubí, Santana, Díaz, y Almanza (2011), señalan que el objetivo principal de la criptografía es proteger información sensible y evitar el acceso no autorizado de usuarios, además controlar la integridad de los mensajes para que no sean modificados en su trayectoria.

Criptosistemas

Gutiérrez y Tena (2003), indican que un criptosistema consta de cinco componentes: M, C, K, E y D) donde: M es el conjunto de los mensajes en claro; C es el conjunto de los mensajes cifrados; K es el espacio de claves que pueden ser empleados en el criptosistema; E es el conjunto de los métodos de cifrado, representado por $E=\{Ek|k \in K\}$, que es una familia de funciones $Ek:P \rightarrow C$

que utiliza para el cifrado y D es el conjunto de los métodos de descifrado, representado por $D=\{Dk|k \in K\}$ es una familia de funciones $Dk:C \rightarrow P$ que es utilizado para el proceso de descifrado.

Al respecto, Lucena (2010) considera que todo criptosistema debe cumplir con la condición de que todo mensaje p, se lo cifra empleando una clave k y luego se descifra aplicando la misma clave k y se obtiene nuevamente el mensaje original p.

Criptoanálisis

Tortosa (2000) afirma que el criptoanálisis estudia métodos y principios para transformar un mensaje ininteligible en un mensaje inteligible sin conocer la clave utilizada. Del mismo modo, Itzcoatl (2013) declara que el criptoanálisis busca recuperar información, sin necesidad de un código o clave. Una vez que se rompe una técnica criptográfica, ésta necesitará aumentar su complejidad.

Criptografía simétrica

De acuerdo a Zhao, Ran, Yuan, Chi, y Ma (2016) la criptografía simétrica o de clave privada, emplea una misma llave para cifrar y decifrar el mensaje, la cual es intercambiada entre el emisor y receptor a través de un canal inseguro. Sin embargo, Shannon (1949), demostró que la información se puede transmitir sobre un canal con ruido, si la magnitud de la fuente no excede la capacidad de transmisión del canal que la conduce.

Visto desde la perspectiva de Fúster, Hernández, Martín, Montoya, y Muñoz, (2012), la criptografía simétrica o de clave privada es más eficiente que la criptografía de clave pública al momento de cifrar y descifrar, puesto que utiliza una sola clave. En cuanto a las ventajas de este tipo de algoritmos, manifiestan Díaz, Mur, Sancristóbal, Alonso, y Piere (2012), que son más rápidos que los cifrados de clave pública y son aún utilizados como base para los sistemas criptográficos basados en hardware.

Entre los algoritmos más utilizados hoy en día se encuentran: Data Encryption Standard (DES), Triple DES, Advanced Encryption Standard (AES), Blowfish (Vargas y Velasco, 2006); también se encuentran otros algoritmos estándares como el IDEA y RC4 (Agé, y otros, 2015).

En la figura 3 se muestra el proceso del cifrado simétrico.

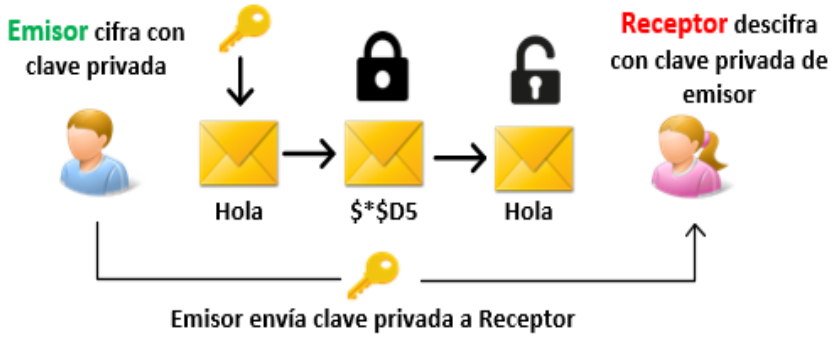

Figura 3: Proceso de cifrado simétrico. Fuente: (Stallings, 2004)

De acuerdo a lo señalado por Hernández (2007), se usan dos tipos básicos de cifrado: en flujo y en bloque. El cifrado en flujo cifra carácter por carácter, combinado con una sucesión obtenida a

través de un proceso pseudoaleatorio; mientras que el cifrado en bloque trabaja con bloques de texto en claro y texto cifrado de longitud 64, 128 o 256 bits.

Criptografía asimétrica

Rivest, Shamir, y Adleman (1978), introdujeron un sistema criptográfico que basa su seguridad en la factorización de un entero denominado RSA, el cual implementa un criptosistema de clave pública y firmas digitales, motivado por los trabajos publicados de Diffie y Hellman.

Carvajal (2007) expone que la criptografía asimétrica es la más moderna y es considerada el futuro del comercio electrónico; los criptosistemas más conocidos son: RSA y ECC. Por su parte, Lenstra y Verheul (2001) distinguen tres tipos de criptosistemas: Clásicos (RSA), Logaritmos discretos (Diffie-Hellman, ElGamal, DSA) y Curva elíptica.

Tal como expresan Medina y Miranda (2015), la criptografía asimétrica utiliza dos claves: la pública que se utiliza para el cifrado y la clave privada usada para el descifrado. La clave pública y la privada se relacionan entre sí por cualquier medio matemático. Es decir, los datos cifrados por una clave pública pueden ser encriptados sólo por su clave privada correspondiente. El proceso de cifrado y descifrado se muestra en la figura 4.

Firma digital

Según Zanuy (2000), la firma digital es un mensaje codificado que contiene información de un producto determinado, realiza una verificación de la autenticidad del emisor a través de algoritmos públicos. Del mismo modo Rojas, Suárez, y Meneses (2011), definen la firma digital como el equivalente de la firma manuscrita, que incorpora elementos de seguridad como: autenticidad, confidencialidad, integridad y no repudio. Añade Lucena (2010), que la firma digital es la transformación de un mensaje a una secuencia de bits a través de un criptosistema asimétrico y la llave privada de una persona.

Por su parte, Reyes y Quintero (2006) señalan que la firma digital debe cumplir con las siguientes características para que ésta sea válida: Vigencia: creada en un período de vigencia del certificado digital.

Verificación: Verificar los datos que son detallados en el certificado.

Emisión: Certificado reconocido por un certificador licenciado.

Cabe señalar, que existen algoritmos (hash) que permiten garantizar que un mensaje no ha sido alterado, asegurando la integridad del mensaje transferido, entre ellos están: MD5 (128 bits message digest) y SHA (160 bits message digest) (Agé, et al. 2015). La figura 5 muestra el funcionamiento de la firma digital.

Para finalizar Rocha, Castello, y Bollo (2014), describen el funcionamiento de la firma digital, en primera instancia el firmante genera mediante una función matemática, una huella digital del mensaje, la cual se cifra con la clave privada. El resultado (firma digital) se enviará adjunto al mensaje original; para la verificación del mensaje el receptor generará la huella digital del mensaje recibido, se descifrará la firma digital del mensaje, utilizando la clave pública del firmante y obtendrá de esa forma la huella digital del mensaje original.

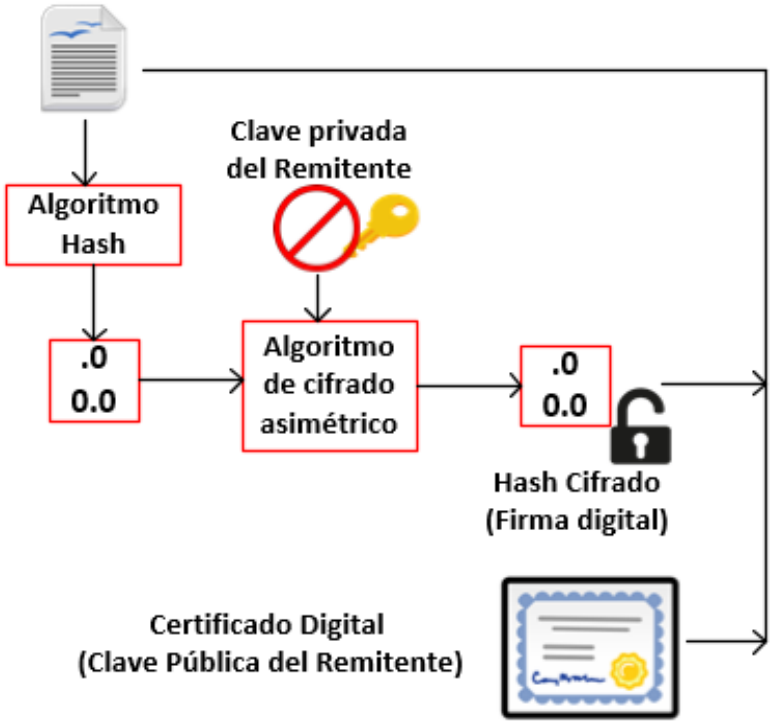

Figura 5: Funcionamiento de la firma digital. Fuente: (Vicent y Gómez, 2007)

Autoridad Certificadora

Quintanilla y López (2016), indican que la Autoridad Certificadora (AC) es la entidad de confianza que certifica la relación de un usuario con su llave pública. En los esquemas de llave pública, la llave privada es inversa a la llave pública y viceersa, la vinculación de una entidad con su llave pública involucra de igual manera la vinculación con su llave privada. Del mismo modo, Castro, Díaz, Alzórriz, y Sancristóbal (2014), adicionan que la Autoridad de Certificación, es la entidad que emite, controla y gestiona los certificados digitales.

Igualmente declaran Buch y Jordán (2001), que la Autoridad Certificadora (CA), emite certificados que se genera en formato x.500, y la firma digital permitirá que un tercero pueda verificar su autenticidad utilizando la clave pública de la CA. Del mismo modo Vigil, Sánchez y Cruz (2003) declaran, que la Autoridad Certificadora mantiene una lista actualizada con las claves privadas, con el objetivo de invalidar los certificados digitales que no tienen validez, los motivos de la invalidación podrían ser: clave privada comprometida, contexto del certificado, entre otros.

Metodología

Para el desarrollo de ésta investigación, se aplicó el método de investigación pura, el cual permite acrecentar los conocimientos teóricos para el progreso de una determinada ciencia, es más formal y persigue propósitos teóricos en el sentido de aumentar el acervo de conocimientos de una determinada teoría (Egg, 1995).

Se inició el estudio, con la revisión de varias fuentes bibliográficas (libros, artículos, tesis doctorales, documentos de internet, ponencias en congresos, entre otros), a fin de extraer las definiciones o conceptos relacionados al resumen de mensajes y certificado digital.

Posteriormente, se seleccionaron las definiciones aportadas por los autores más relevantes en la temática de estudio, y a partir de sus análisis, se extrajo los términos más destacados de cada concepto, lo que permitió extraer elementos comunes a estas definiciones. Finalmente, se llevó a cabo una cuantificación de los elementos/conceptos, para conceptualizar los términos resumen de mensajes y certificado digital.

Definiciones de conceptos relacionados con el objeto de estudio

A continuación se realiza la exposición de cada uno de los conceptos y definiciones que fueron analizados en este estudio, a fin de definir el concepto del resumen de mensajes y certificado digital.

Concepto de resumen de mensajes o función hash

Calabuig (1999) manifiesta que "Una función hash (H) es una transformación que toma un mensaje de entrada (m) o preimagen, y devuelve una cadena de tamaño fijo (h), llamada valor hash o digest". (p. 16)

Bermúdez, y otros (2007) definen el resumen de mensajes como una función que comprime una cadena arbitraria de bits a una cadena de bits de longitud fija.

Para Rocha, Castello, y Bollo (2014), una función de hash H se denomina también función resumen, la cual opera sobre un mensaje M de longitud arbitraria y produce una salida h de longitud fija. h = H(M).

Por su parte Mogollon (2007), afirma que el resumen de mensajes o función hash se utiliza para demostrar que los datos transmitidos no se han alterado. Esta función toma un mensaje de entrada (variable) y lo transforma una función del mensaje (cadena de tamaño fijo).

Desde el punto de vista de Castillo, Santana, Díaz, Almanza, y Castillo (2011), el resumen de mensajes es una función que asigna al mensaje a una longitud fija hash, el tamaño de la función hash tiene similar longitud en bits del hash.

Considera Varela (2006), que las función de resumen de mensaje o función hash, son operaciones que se aplican al mensaje para extraer una parte de él, si cambia el mensaje, cambia el resultado de la operación.

De acuerdo a la interpretación de Vicent y Gómez (2007), matemáticamente se define la función de resumen de mensaje (hash), como proyecciones de un conjunto elevado de elementos sobre un conjunto de tamaño fijo y más pequeño que el anterior.

Concepto de certificado digital

De acuerdo con la opinión de Lucena (2010), un certificado digital es una clave pública y un identificador, firmado por una autoridad certificadora; con el propósito de demostrar que una clave pública pertenece a un usuario concreto.

Carvajal (2007), manifiesta que el certificado digital es un mecanismo basado en la criptografía asimétrica de clave pública para conseguir comunicaciones seguras entre el emisor y receptor, utilizando medios de comunicación insegura (internet), además, que un tercero de confianza denominado Autoridad Certificadora (AC) que garantiza la confidencialidad y el no repudio de la comunicación.

Ramos (2000), afirma que los certificados digitales son registros electrónicos que atestiguan que una clave pública pertenece a un determinado individuo o entidad.

De acuerdo a la interpretación de Ramos (2015), el certificado digital es un documento firmado digitalmente por una persona o entidad denominada Autoridad Certificadora (AC), mediante el cual se atestigua que una clave pública pertenece a un determinado individuo o entidad.

Del mismo modo Aguilera (2010), expresa que el certificado digital es un documento en el que una autoridad certificadora, se encarga de emitir y renovar los certificados digitales y certificados de firmas electrónicas, garantizando que la clave pública y una persona están realmente asociados.

Para Castaño y Jurado (2016), el certificado digital es necesario cuando se envía una firma digital reconocida, porque la información del certificado digital, es reconocida por una entidad (Autoridad Certificadora), asegurando que la persona o entidad que usa el certificado es quien dice ser.

Confirman Vivas, Huerta, Zambrano, Clotet, y Satizábal (2007), que el certificado digital es un documento electrónico que contiene: los datos de identificación de una persona o entidad (empresa, servidor web, etc.) y la clave pública, siendo la Autoridad Certificadora la responsable de la autenticidad de los datos que figuran en éste archivo.

Análisis de los resultados

Se muestra en las tablas 1 y 2 los resultados obtenidos del análisis individual de los conceptos que abordan el objeto de estudio (resumen de mensajes y certificado digital), de forma que la primera columna incluye los autores seleccionados para la conceptualización del objeto de estudio, en las otras columnas se detallan los elementos/conceptos comunes en cada una de las definiciones descritas por los autores, se escogieron siete autores por cada análisis.

Tabla 1: Elementos/conceptos del resumen de mensajes

Autor(es)	Elementos/Conceptos Resumen de mensajes				
	Transformación del mensaje	Cadena de tamaño fijo	Comprime cadena	Datos no alterados	Operaciones
Calabuig (1999)	X	X			
Bermúdez, y otros (2007)		X	X		
Rocha, Castello, y Bollo (2014)		X			
Mogollon (2007)		X		X	
Castillo, Santana, Díaz, Almanza, y Castillo (2011)		X			
Varela (2006)					X
Vicent y Gómez (2007)		X			
TOTAL	1	6	1	1	1

Tabla 2: Elementos/conceptos del Certificado digital

Autor(es)	Elementos/Conceptos Certificado digital				
	Clave pública de remitente	Autoridad Certificadora	Comunicación segura	Confidencialidad y no repudio	Autenticidad de datos
Lucena (2010)	X	X			X
Carvajal (2007)	X	X	X	X	
Ramos (2000)	X				X
Ramos (2015)	X	X			X
Aguilera (2010)	X	X			X
Castaño y Jurado (2016)		X			X
Vivas, Huerta, Zambrano, Clotet, y Satizábal (2007)	X	X	X		X
TOTAL	6	6	2	1	6

En la tabla 1 se observa que el elemento que los elementos con mayor frecuencia son: canal de tamaño fijo, seguido de: transformación del mensaje, comprime cadena datos no alterados y operaciones.

En la tabla 2 se aprecia que los elementos con mayor frecuencia son: clave pública, Autoridad Certificadora, autenticidad de datos y comunicación segura. Estos resultados permiten definir a los objetos de estudio: resumen de mensajes y certificado digital.

CONCLUSIONES

La conceptualización del resumen de mensajes y certificado digital, se fundamenta principalmente de: libros, Journals académicos, publicaciones periódicas, memorias de congresos, tesis doctorales, entre otros; base fundamental para la conceptualización del objeto de trabajo, la definición propuesta se detalla a continuación:

- Resumen de mensajes: Función matemática que transforma el mensaje de entrada (bits) en una cadena binaria de longitud fija, se utiliza para garantizar que la firma digital es auténtica.
- Certificado digital: Documento electrónico emitido por una Autoridad Certificadora (AC), que contiene la firma electrónica y la clave pública de una persona o entidad, con la finalidad de garantizar su identidad digital.

Una de las limitaciones encontradas en el estudio fue la cantidad de conceptos analizados, por la existencia de otros documentos en constructo respecto a ésta temática. Así mismo, la cantidad de elementos/conceptos aplicados para calcular la frecuencia de términos relacionados a: resumen de mensajes y certificado digital no fue el suficiente, por lo que se podría ampliar el número de definiciones y elementos.

En la actualidad las tecnologías de la información y comunicación han revolucionado el mundo de los negocios, siendo el uso de los certificados digitales cada vez más frecuente en las empresas; por ello en futuras investigaciones se pueden explorar otros ambientes relacionados con el marco legal de la firma electrónica en el Ecuador.

REFERENCIAS

Agé, M., Ebel, F., Rault, R., Crocfer, R., Dumas, D., Schalkwijk, L., Fortunato, G. (2015). Seguridad informática. Hacking Ético. Barcelona: Eni.

Aguilera, P. (2010). Seguridad informática. Madrid: Editex.

Ángel, J. d. (2000). Criptografía para principiantes. Red Mundial, 5.

Banco Central del Ecuador. (mayo de 2016). Certificación Electrónica. Quito, Ecuador. Recuperado el 27 de diciembre de 2016, de https://www.eci.bce.ec/web/guest/noticias1

Bermúdez, A., Carrillo, S., Cortés, J., Guinea, F., López, J., Martínez, F.,Villamayor, O. (2007). Las Matemáticas en la Comunidad de Madrid. Computación e interacción I+D+i. Madrid: Imdea.

Braga, G. (1994). La naturaleza del conocimiento didáctico: el debate epistemológico. Documento inédito.

Bush, J., y Jordan, F. (2001). La seguridad de las transacciones bancarias en internet. Informe SEIS. Recuperado el 30 de diciembre de 2016, de http://www.conganat.org/Seis/informes/2001/PDF/6BuchTarrats.pdf

Calabuig, V. (1999). Elementos de la Criptología (Vol. 572). España: Fundación Universitaria San Pablo CEU Valencia. Obtenido de http://dspace.ceu.es/bitstream/10637/2031/1/Calabuig,Vicente99-00.pdf

Carvajal, A. (noviembre de 2007). PKI y firmas digitales: aplicaciones reales. Inventum (3). doi:ISSN 1909-2520

Castaño, J. J., y Jurado, S. (2016). Mercado digital: compraventa online (comercio electrónico). España: Editex.

Castillo, M. A., Santana, N., Díaz, A., Almanza, G., y Castillo, F. (17 de junio de 2011). Teoría de número en criptografía y su debilidad ante la posible era de las computadoras cuánticas. Ergo Sum, 18(3), 264-273.

Castro, M., Díaz, G., Alzórriz, I., y Sancristóbal, E. (2014). Proceso y herramientas para la seguridad de Redes. Madrid: UNED.

Contreras, I. (2011). La firma electrónica y la función notarial de Jalisco. México: CUCSH-UDG.

De Miguel, P. (2004). Regulación de la firma electrónica: Balance y perspectivas. Associacao Portuguesa de Direito Intelectual., 115-143.

Díaz, G., Mur, F., Sancristóbal, E., Alonso, M., y Piere, J. (2012). Seguridad en las comunicaciones y en la información. Madrid: UNED. Obtenido de https://books.google.com.ec/books?id=AEmYX1u9kQkC&printsec=frontcover#v=onepage&q&f=false

Diffie, W., y Hellman, M. (1976). New Directions in Cryptography. IEEE Transactions on Information Theory., 644-654.

Egg, A. (1995). Técnicas de investigación social. Buenos Aires: Lumen.

El Gamal, T. (1985). A public Key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans Information Theory, 31(4), 469 - 472.

Fúster, A., Hernández, L., Martín, A., Montoya, F., y Muñoz, J. (2012). Criptografía, protección de datos y aplicaciones. (Primera ed.). México DF.: Alfaomega. doi:ISBN 978-607-707-469-4.

Galende, J. C. (1995). Criptografía: historia de la escritura cifrada (Primera ed.). Madrid, España: Complutense.

Gallardo Ortíz, M. (1992). Criptología; Seguridad Informática y Derecho Leyes del Ciberespacio. Criptología; Seguridad Informática y Derecho Leyes del Ciberespacio. Madrid: UNED. Obtenido de http://www.egov.ufsc.br/portal/sites/default/files/46.pdf

Giménez, J. F. (2014). Seguridad en equipos informáticos. IFCT0510. Málaga, España: IC editorial.

González, E., y Quintero, J. (2006). Firma digital basada en redes (Lattice). Revista Científica, 8, 53-64.

Granados, G. (10 de julio de 2006). Introducción a la criptografía. Revista Digital Universitaria, 7(7), 17. Obtenido de www.revista.unam.mx/vol.7/num7/art55/jul_art55.pdf

Gutiérrez, J., y Tena, J. G. (2003). Protocolos criptográficos y seguridad en redes. España: Universidad de Cantabria.

Gutiérrez, M. (2009). El papel de las entidades de certificación y la seguridad de la información y los derechos personales en el comercio electrónico. Colombia: ABC.

Guyot, V. (2005). Epistemolog;ia y prácticas del conocimiento. Ciencia, Docencia y Tecnología., 16(30), 9-24.

Hernández, A. (2007). Las Matemáticas en la Comunidad de Madrid. Matemáticas y Criptografía (págs. 97-104). Madrid: instituto madrileño de estudios avanzados.

Iriarte, E. (1999). Firma digital y certificado digital. Sistema Argentino de Información Jurídica, 4. Recuperado el 14 de noviembre de 2016, de http://www.saij.gob.ar/doctrina/dacf000081-iriarte_ahon-firma_digital_certificado_digital.htm?bsrc=ci

Itzcoatl, J. (2 de mayo de 2013). seguridad. Obtenido de http://revista.seguridad.unam.mx/numero-17/criptograf%C3%AD-y-criptoan%C3%A1lisis-la-dial%C3%A9ctica-de-la-seguridad

Lenstra, A., y Verheul, E. (2001). Selecting Cryptographic Key Sizes. Journal of cryptology, 14(4), 255-293.

Lucena, M. J. (2010). Criptografía y seguridad en computadores. España.

Mario, P., y Sancho, F. (2003). Máquinas moleculares basadas en ADN. Sevilla, España: Divulgación Científica. Obtenido de https://books.google.com.ec/books?id=O4RehPJl2CkC&printsec=frontcover#v=onepage&q&f=false

Marrero, Y. (2003). La criptografía como elemento de la seguridad informática. ACIMED, 1-8. Recuperado el 18 de diciembre de 2016, de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352003000600012

Medina, Y., y Miranda, H. (2015). Comparación de Algoritmos Basados en la criptografía Simétrica DES, AES y 3DES. Mundo Fesc(9), 14-21.

Mogollon, M. (2007). Cryptography and Security Services. Dallas, USA: Cybertech Publishing.

Paar, C., y Pelzl, J. (2010). Understanding Cryptography - A Textbook for Students and Practitioners. Germany: Springer.

Piaget, J. (1969). La epistemología y sus variedades. Paris: Gallimard. Recuperado el 12 de noviembre de 2016

Porolli, M. (30 de julio de 2013). welivesecurity. Recuperado el 19 de diciembre de 2016, de http://www.welivesecurity.com/la-es/2013/07/30/por-que-deberia-cifrar-mis-datos/

Quintanilla, K., y López, M. (9 de junio de 2016). Generación de certificados de registro basados en firmas agregadas. Programación matemática y software, 17-24.

Ramos Suárez, F. (2000). Eficacia jurídica de una transacción electrónica. La figura de no repudio. Revista electrónica de Derecho e Informático. Obtenido de www.mct.pt/novo/legislacao/despachos/txtab.html

Ramos, J. (septiembre de 2015). Historia clínica computarizada y firma digital: su implementación práctica. Consejo Argentino de Oftalmología, 8. doi:ISSN 1851-2658

Reyes, E., y Quintero, J. G. (2006). Firma digital basada en redes (Lattice). Ingeniería y Tecnología. Recuperado el 17 de diciembre de 2016

Rivest, R., Shamir, A., y Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Comm ACM, 21, 120-126.

Rocha, M., Castello, R., y Bollo, D. (2014). Criptografía y firma electrónica/digital en el aula. IX Jornadas de docentes universitarios de sistemas y tecnología de la información, DUTI. Argentina: Científica Universitaria.

Rojas, M., Suárez, D., y Meneses, C. (2011). Firma digital: instrumento de transmisión de información a entidades financieras. Avances en Sistemas e Informática, 8(1), 7-14. Recuperado el 18 de diciembre de 2016, de http://www.revistas.unal.edu.co/index.php/avances/article/view/26709/27006

Rubí, M., Santana, N., Díaz, A., y Almanza, G. C. (17 de junio de 2001). Teoría de números en criptografía y su debilidad ante la posible era de las computadoras cuánticas. Ciencia Ergo Sum, 10. Recuperado el 21 de diciembre de 2016, de http://cienciaergosum.uaemex.mx/index.php/ergosum/article/view/867/620

Shannon, C. (1949). A Mathematical theory of communication. The Bell System Technical Journal,, 27, 656-715.

Solis, C., y Oviedo, H. (2015). Transmisión segura mediante el uso de algoritmo criptográfico basado en cuaterniones y fracciones de Farey. 15vo Congreso Nacional de Ingeniería Electromecánica y de Sistemas (CNIES 2015), (pág. 6). México. Recuperado el 13 de diciembre de 2016, de http://www.sepi.esimez.ipn.mx/cnies/memorias/TEL18.pdf

Stallings, W. (2004). Fundamentos de seguridad en redes: aplicaciones y estándares (Segunda ed.). España: Pearson Prentice Hall.

Tortosa, L. (2000). Mensajes secretos y códigos con TI-83. España: Club Universitario.

Varela, R. (10 de julio de 2006). Criptografía una necesidad moderna. Revista Digital Universitaria, 7(7), 9.

Vargas, E., y Velasco, J. (2006). Desarrollo de una Aplicación para Control de Acceso Usando Smart Cards. Grupo de Bio-nanoelectrónica. Recuperado el 28 de diciembre de 2016

Vicent, J., y Gómez, A. (2007). Propuesta y análisis de criptosistemas de clave pública basados en matrices triangulares superiores por bloques. España, España: Taller Digital. Obtenido de www.eltallerdigital.com

Vigil, j. L., Sánchez, N., y Cruz, G. (2003). Infraestructuras de claves públicas en redes corporativas. Ingeniería Electrónica, Automática y Comunicaciones., 24(3), 90-95. Recuperado el 4 de enero de 2016

Vivas, T., Huerta, M., Zambrano, A., Clotet, R., y Satizábal, C. (2007). Aplicación de mecanismos de seguridad en una Red de Telemedicina basados en Certificados digitales. Springer Berlin Heidelberg, 971-974.

Zanuy, M. (2000). Tratamiento digital de voz e imagen y aplicación a la multimedia. Barcelona: marcombo.

Zhao, T., Ran, Q., Yuan, L., Chi, Y., y Ma, J. (agosto de 2016). Information verification cryptosystem using one-time keys based on double random phase encoding and public-key cryptography. Optics and Lasers in Engineering, 83, 48-58. doi:10.1016/j.optlaseng.2016.03.001