Luis Martinez 35083

Johana Alvarado

Jhonatan Crespo

Jesus Rea

Según: [Héctor Castillo](https://plus.google.com/102750700036006101435)

**Seguridad Fisica:**

La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático. Si bien algunos de los aspectos de seguridad física básicos se prevén, otros, como la detección de un atacante interno a la empresa que intenta acceder físicamente a una sala de cómputo de la misma, no. Esto puede derivar en que para un atacante sea más fácil lograr tomar y copiar una cinta de backup de la sala de cómputo, que intentar acceder vía lógica a la misma. Así, la Seguridad Física consiste en la “aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial”. Se refiere a los controles y mecanismos de seguridad dentro y alrededor del centro de cómputo, así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

**Seguridad Logica:**

La Seguridad Lógica consiste en la “aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo”. Existe un viejo dicho en la seguridad informática que dicta que “todo lo que no está permitido debe estar prohibido” y esto es lo que debe asegurar la Seguridad Lógica.

Según Eugenia Bahit:

**Seguridad básica en sistemas Web (PHP):**

Sin dudas, este es uno de los puntos fundamentales a tener en cuenta al momento de desarrollar nuestra aplicación. Frecuentemente los CMS, plataformas de eLearning e incluso de comercio electrónico -y me refiero a los más populares-, al momento de su instalación, nos piden asignar un directorio con permisos de escritura a fin de poder cargar archivos de imágenes (o cualquier otro contenido estático), mediante su plataforma de administración. Mayormente, es requisito que este directorio se encuentre servido dentro del DocumentRoot.

Un directorio Web con permisos de escritura, es una puerta sin llave ni cerrojo en un barrio lujoso: algo tentador para aquellas personas a quiénes les gusta ir de visita a casas ajenas, sin invitación y tomando como propios aquellos objetos de terceros (por si no se entendió, “ladrón”, solo que dicho en plan Neruda de supermercado).

El principal inconveniente que se le presenta a algunos programadores al momento de optar por no “servir” un directorio con permisos de escritura, es ¿cómo haré accesibles los archivos estáticos mediante el navegador si el directorio no se encuentra servido31? La respuesta a esta pregunta es simple: engañando al navegador.

La forma más eficiente, segura, genérica y reutilizable para lograrlo, es hacer que los archivos estáticos que se encuentran en un directorio no accesible mediante el navegador, se sirvan a través de un único archivo PHP encargado de leer y mostrar dichos archivos modificando previamente el Content-Type (tipo de contenido) en los encabezados HTTP. Desde la versión 5.3 de PHP se dispone del módulo fileinfo32, quien mediante sus funciones nos ayudará con este proceso. En versiones anteriores, puede utilizarse la función obsoleta mime\_content\_type(). Veamos un ejemplo con fileinfo.

Según [Logisman](http://www.custodia-documental.com/author/logisman/):

**ISO 27000:**

Proviene de la norma BS 7799 de British Standards Institution (organización británica equivalente a AENOR en España) creada en 1995 con el fin de facilitar a cualquier empresa un conjunto de buenas prácticas para la **gestión de la seguridad de la información.**

Esta familia de normas que tiene como objetivo definir requisitos para un **sistema de gestión de la seguridad de la información (SGSI)**, con el fin de garantizar la selección de **controles de seguridad** adecuados y proporcionales, protegiendo así la **información**, es recomendable para cualquier empresa grande o pequeña de cualquier parte del mundo y más especialmente para aquellos sectores que tengan **información crítica** o gestionen la información de otras empresas.

Según seguinfo:

**Firma digital:**

Cuando hablamos de firma digital en realidad nos estamos refiriendo a muchos conceptos relacionados, entre los cuales figuran documentos electrónicos, claves criptográficas, certificados digitales, funciones matemáticas, autoridades certificantes, infraestructuras de clave pública y muchos otros nombres que pueden resultarnos complicados o desconocidos.

Es una herramienta tecnológica que permite garantizar la autoría e integridad de los documentos digitales, posibilitando que éstos gocen de una característica que únicamente era propia de los documentos en papel.

**Certificado digital:**

Los certificados digitales son pequeños documentos digitales que dan fe de la vinculación entre una clave pública y un individuo o entidad. De este modo, permiten verificar que una clave pública específica pertenece, efectivamente, a un individuo determinado. Los certificados ayudan a prevenir que alguien utilice una clave para hacerse pasar por otra persona.

En algunos casos, puede ser necesario crear una cadena de certificados, cada uno certificando el previo, para que las partes involucradas confíen en la identidad en cuestión.

Según Yolanda Corral:

**Blockchains. Usos y aplicaciones**

Se habla de blockchain como de una tecnología disruptiva que puede hacer tambalear los cimientos de Internet para abrirnos un abanico de posibilidades impensables hasta el momento y cambiar muchas cosas en un futuro muy cercano dando pie a un nuevo Internet. **Se dice que puede dar un giro a la economía, a la forma de realizar contratos y gestionar bienes digitales, mejorar la seguridad del Internet de las cosas o ayudar a gestionar mejor nuestros datos e información en la red** con la consiguiente mejora de la privacidad y así, así un sinfín de cosas. Entonces llega la gran pregunta, ¿realmente qué es blockchain? ¿En serio que podemos hablar de algo que puede revolucionar Internet? Y sobre todo ¿estamos hablando de una tecnología segura?

Si nos atenemos a una definición técnica **blockchain es una cadena de bloques de transacciones una tecnología basada en un modelo descentralizado**y sobre esta base se sustenta el bitcoin, la primera de las criptomonedas que comenzó a funcionar allá por 2009. Pero como he dicho antes, en los últimos tiempos se está hablando cada vez más sobre el potencial que tiene aplicar esta tecnología en otros campos por la inalterabilidad, fiabilidad y seguridad de la información en esa cadena de bloques que se forma. Es por eso que en esta ocasión me he propuesto entrar de lleno en el mundo blockchain para conocer qué es y sobre todo la seguridad que ofrece y todos esas aplicaciones que se le podrían dar. Para ello contaré con la participación de **Yaiza Rubio, Pablo Fernández Burgueño, Alberto Gómez Toribio y Félix Brezo**cuatro profesionales de diversas áreas con un amplio conocimiento en la materia.

Según Omar Antonio Vega:

**Captcha. Tipos de capthca:**

Los CAPTCHA, las pruebas humanas interactivas más utilizadas, aparecen como un método de diferenciación entre usuarios humanos y máquinas para brindar seguridad a la información en internet y evitar el spam, especialmente. Por ello, se hace una presentación introductoria de las pruebas humanas interactivas, para luego profundizar en los CAPTCHA, donde se trata su evolución, su clasificación, especificando sus técnicas de generación, algunas de sus aplicaciones y los tipos de ataques a los que se ven sometidos. Después, se tratan algunas repercusiones que han tenido sobre la usabilidad/accesibilidad de servicios de internet para usuarios humanos, lo que lleva a plantearse la inquietud de si los CAPTCHA, más que una solución, se han convertido en un nuevo problema por resolver.

Los CAPTCHA, de acuerdo con Shirali-Shahreza y Shirali-Shahreza (2008), se clasifican fundamentalmente en métodos basados y no basados en OCR (Optical Character Recognition, por sus siglas en inglés) 4 . En los primeros, los más conocidos y usados en la actualidad, se presenta la imagen de una palabra con una distorsión de diversos efectos, la cual debe ser escrita por el usuario y, debido a los efectos pictóricos, no podrá ser reconocida por el equipo. Para su creación, se acostumbra llevar a cabo un procedimiento general (elegir una palabra de un diccionario predefinido, aplicar un formato a la palabra y convertirla en imagen y degradar la composición mediante distorsión), en el que se diferencian los métodos de generación por medio de los algoritmos de elección de palabras/diccionarios, el formato aplicado a los caracteres y las degradaciones realizadas sobre las imágenes.

Según Ivonne Munoz:

**Seguridad básica en Android**

Google sigue haciendo bien las cosas con Android y es que desde que lanzo la primera versión hace unos años ha ganado muchos seguidores, incluso dió un pequeño salto de los celulares a las tablets lo que aumenta su cuota de mercado. En la pasada Mobile World Congress 2011, [Eric Schmidt mencionó que diariamente se activan 350,000 equipos con Android](http://www.publico.es/ciencias/361561/la-demanda-crece-mas-rapido-que-la-capacidad).Este aumento en la popularidad de Android y sobre todo en ventas no sólo atrae a más desarrolladores y compañías a usarlo en sus equipos, también **aumenta la atención que los cyber delicuentes le dan**, lo cual es lógico ya que a más usuarios (de cualquier producto), más probabilidades de lograr alguna afectación existen.

Son los **troyanos** los principales programas que se utilizan para atacar Android, estos se instalan en el equipo y a partir de eso momento comienzan a robar la información de los usuarios junto con la ubicación del mismo y la envían a servidores que se encargan de recopilar esta información.

Hasta hace unos meses Android vivía tranquilo y sin este tipo de problemas hasta que llego [una aplicación que al instalarse enviaba mensajes a números de contenido premium](http://gizmovil.com/2010/08/primer-virus-para-android-descubierto)así como los datos del usuario, lo que terminaba con el saldo del teléfono.

**Niveles de usuarios**

Un usuario de información es aquel individuo que necesita información para desarrollar sus actividades. Según esto, todos los seres humanos somos usuarios de información, pues todos la necesitamos para realizar las actividades que llevamos a cabo diariamente. (Carmen MARTÍN MORENO, noviembre 2007)

Segun ***Noe Guadarrama Beltran (14/09/2015).*** Los niveles de usuarios están divididos por operacionales, supervisores y ejecutivos.

**Los usuarios operacionales**: son aquellos que tiene interacción directa a través del equipo de sistemas, son responsables de alimentar y acceder a la información para asegurar la toma de decisiones basada en datos exactos confiables y oportunos

Un ejemplo claro, podría ser un capturista de datos, ya que él es el que se encarga de recabar la información y asentarla en el sistema

**Usuarios Supervisores**

\* Pueden o no tener un panorama local

\* Generalmente están familiarizados con la operación

\* Lo rigen consideraciones presupuestales y a veces está más preocupados por incrementar el volumen de trabajo realizado disminuyendo a la vez el costo.

\* Actúa a menudo como intermediario entre los usuarios y los niveles superiores de la administración.

\* Es con quien el analista tendrá contacto directo. Es el que definirá los requerimientos y las políticas de la empresa que su sistema debe realizar.

En alguna grande empresa, son los analistas de nominas, por ejemplo, toda la información es pasada a ellos para que den el visto bueno y puedan ser pagadas estas papeletas sin ningun error antes de ser pasada al director general para que le de salida al dinero

**Usuarios Ejecutivos.**

Tiene un panorama global, Suelen no preocuparse por los detalles Provee de iniciativa para el proyecto

No tienen experiencia operacional directa, por lo tanto, no determina los requerimientos del sistema

Tiene preocupaciones estratégicas. Nuevos mercados, nuevos productos o la nueva ventaja competitiva que se pudiera obtener con el sistema

Estarán interesados por los modelos abstractos del sistema, no por los físicos. otro claro ejemplo de este tipo de usuarios son los gerentes o directivos de alguna empresa que solo se preocupan porque todo este bien dirigido y planeado

En general los sistemas de información, tienen diferentes usuarios de acuerdo a lo que cada uno tenga como responsabilidad en el uso de la información que proporciona el sistema

Criptografia

Según ***Kenny Barrera (12/05/2015)*** el objetivo de la criptografía es conseguir la confidencialidad de los mensajes. Para ello se diseñan sistemas de cifrado y códigos.

Los objetivos de **la criptografía** son: confidencialidad, integridad, vinculación y autenticación.

Existe una transformación diferente Ek para cada valor posible de la clave k y D es el conjunto de transformaciones de descifrado, análogo a E.

Criptosistemas asimétricos o de llave pública, que emplean una doble clave (kp, kP). kp se conoce como clave privada y kP se conoce como clave pública. Una de ellas sirve para la transformación E de cifrado y la otra para la transformación D de descifrado. En muchos casos son intercambiables, esto es, si empleamos una para cifrar la otra sirve para descifrar y viceversa. Estos criptosistemas deben cumplir además que el conocimiento de la clave pública kP no permita calcular la clave privada kp.

Cifrado por Sustitución: En un cifrado por sustitución, las letras (o grupos de letras) son sistemáticamente reemplazadas en el mensaje por otras letras (o grupos de letras).

Una sustitución muy conocida en el cifrado es la del Cifrado César. Para cifrar un mensaje mediante el Cifrado César, cada letra del mensaje es reemplazada por la letra ubicada tres posiciones después en el abecedario

Cifrado por trasposición: En un cifrado por trasposición, las letras no se cambian por otras sino que se cambia el orden de estas. El orden es alterado de acuerdo con un esquema bien definido. Muchos cifrados por trasposición se basan en un diseño geométrico. Un simple (y de nuevo fácil de decodificar) método de cifrado es el de escribir una palabra al revés (de atrás hacia delante)

Cifrados Modernos: Actualmente existen varios tipos de cifrados modernos, estos son conocidos como algoritmos simétricos, estos se basan en los conceptos de Confusión y Difusion. Dichos métodos consisten en ocultar la relación entre el texto plano, el texto cifrado y la clave (Confusión); y repartir la influencia de cada bit del mensaje original lo más posible entre el mensaje cifrado (Difusión)

Data Encryption Standard: DES utiliza bloques de 64 bits, los cuales codifica empleando claves de 56 bits y aplicando permutaciones a nivel de bit en diferentes momentos (mediante tablas de permutaciones y operaciones XOR). Es una red de Feistel de 16 rondas, más dos permutaciones, una que se aplica al principio y otra al final.

IDEA: El proceso de encriptación consiste ocho rondas de cifrado idéntico, excepto por las subclaves utilizadas (segmentos de 16 bits de los 128 de la clave), en donde se combinan diferentes operaciones matemáticas (XORs y Sumas Módulo 16) y una transformación final

**Criptosistema**

Definiremos un criptosistema como una quíntupla (M, C, K, E, D), donde M representa el conjunto de todos los mensajes sin cifrar que pueden ser enviados, C representa el conjunto de todos los posibles mensajes cifrados, o criptogramas, K representa el conjunto de claves que se pueden emplear en el criptosistema, E es el conjunto de transformaciones de cifrado o familia de funciones que se aplica a cada elemento de M para obtener un elemento de C.

Existen dos tipos de criptosistemas

Criptosistemas simétricos o de clave privada: Son aquellos que emplean la misma clave k tanto para cifrar como para descifrar. Presentan el inconveniente de que para ser empleados en canales de comunicación la clave k debe estar tanto en el emisor como en el receptor, lo cual nos lleva preguntarnos cómo transmitir la clave de forma segura.

Cifrado Clasico: Un cifrado es un medio para ocultar un mensaje, donde las letras del mensaje son sustituidas o traspuestas por otras letras, pares de letras y algunas veces por muchas letras. En criptografía, el cifrado clásico es un tipo de cifrado que fue usado históricamente pero que ahora ha caído, mayormente, en desuso. En general, los cifrados clásicos operan en un alfabeto de letras (como "A-Z"), a las cuales se les aplican métodos a mano o con aparatos mecánicos muy simples.

Criptología: Tradicionalmente se ha definido como el ámbito de la criptología el que se ocupa de las técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados.

**CRIPTOMONEDA**

Las criptomonedas o criptodivisas son monedas virtuales que utilizan un cifrado digital para sus operaciones, y con las que se pueden realizar transacciones económicas sin necesidad de intermediarios. Estas monedas digitales utilizan la criptografía para crear economías más seguras, con una mayor privacidad y que no responden al control de ningún país o institución, ya que se encuentran totalmente descentralizadas. ***(Walterhash 1/31/2014)***

**USO**

Tienen el mismo uso que cualquier tipo de moneda física, pero con la diferencia de que no lo podemos tocar. Con las monedas virtuales se pueden realizar pagos entre personas y, además, ya son varias las empresas que admiten este tipo de moneda, aunque es verdad que todavía no está muy extendido. Algunas empresas como Destinia, Dell o Microsoft ya permiten que se hagan compras a través de sus páginas web con bitcoins, la moneda digital más extendida en el mundo.

**TIPOS**

**Bitcoin**

El Bitcoin fue la primera moneda virtual y a través de la cual han surgido muchas más que han acabado formando el mercado de las criptodivisas. Es, sin duda, la moneda más conocida y ya la utilizan muchas personas en el mundo para realizar sus operaciones económicas. Además, ya son muchas las empresas que permiten el pago de sus productos con este moneda digital.

Esta moneda se preserva un límite total de 21 millones de Bitcoin, que nunca podrá superarse, ya que así lo estableció el mercado de esta criptodivisa. Cabe recordar que el mercado de esta moneda es que el siempre tiene el control, por lo que no puede eludirse.

El algoritmo de encriptación hace que esta criptodivisa sea muy dificil de falsificar o reproducir. Además, para la minería de Bitcoins hace falta potentes computadoras que le permitan introducir nuevos Bitcoins en el mercado y posee unos altos costes en energía eléctrica para conseguirlos.

**Ethereum**

Ethereum está considerada como la gran alternativa al Bitcoin en el mercado de las monedas virtuales y muchos expertos ya consideran que puede llegar a superarla en valor. Concretamente, la moneda se llama Éter, y Ethereum es la red o sistema que controla esta criptomoneda.

Ethereum posee una de las velocidades de transacción más altas que existen, ya que el tiempo de generación de bloques tan solo es de 15 segundos. Además, la técnica de encriptación da la posibilidad de extraer estas monedas con la GPU de computadoras normales, cosa muy complicada de conseguir con los Bitcoins. También cabe destacar, que las recompensas de la minería de Éter es la misma cada año y no se reduce como ocurre con el Bitcoin.

La red Ethereum introduce un nuevo concepto en el mundo del dinero virtual, los contratos inteligentes. Esto permite a dos usuarios o empresas firmar contratos desde cualquier parte del mundo, sin comisiones ni control por parte de ningún país, aunque no permitan criptomonedas, ya que solo están controlados por sistemas informáticos. De esta forma, dos partes acuerdan un contrato por el que alguien ofrece sus productos a cambio de X Éter y en el momento que el contrato reciba el dinero, el contrato dará el producto y el dinero a las partes correspondientes.

**Litecoin**

Está considerado como el hermano pequeño del Bitcoin, o como algunos expertos comparan "si el Bitcoin fuera el oro, el Litecoin sería la plata". Esto se debe a que tiene un funcionamiento igual que el Bitcoin, pero posee un límite de monedas mucho más alto, situado en los 84 millones de Litecoins.

El Litecoin es una moneda más utilizada por las personas que tienen menos experiencia en el mundo de las criptomonedas, debido a que su funcionamiento es más sencillo. Además, es menos exigente, ya que el tiempo de generación de bloques es de 2,5 minutos en lugar de los 10 minutos del Bitcoin, por lo que se puede gestionar con computadoras más sencillas y existe una mayor agilidad para realizar un gran número de transacciones.

**Ripple**

Ripple está considerada la moneda de los bancos. Aunque muchos piensen que las criptomonedas están creadas para desbancarlos, parece que este dinero virtual también puede tener grandes ventajas para las entidades bancarias. Esto se debe a que gracias a esta moneda, los bancos se saltan los controles fronterizos existentes y, además, pueden realizar sus operaciones sin ningún tipo de comisión nacional. De esta forma, les resulta más barato y aumentan la velocidad de transacciones, ya que se realizan casi de forma instantánea.

El objetivo de esta moneda es crear un sistema de gestión de crédito de forma descentralizado, para que los bancos puedan acceder a la financiación externa fácilmente sin el control de nadie. Muchos de los principales bancos mundiales del mundo ya utilizan estas criptodivisas para realizar algunas de sus operaciones.

**Dogecoin**

El Dogecoin es una moneda virtual que se ha postulado en varias ocasiones como la criptomoneda que mayor número de transacciones registra cada día. Esto no significa que sea la que más dinero mueva, ya que su cotización es muy baja. En esta caso, no existe un número limitado de Dogecins, como si ocurre en otras monedas, por lo que se pueden seguir generando de forma indefinida. Sin embargo, esto puede ser peligro por la inflación que puede provocar.

Las transacciones de esta moneda son muy rápidas ya que la generación de bloques en Dogecoin son de 1 minuto. Sin embargo, esta moneda no suele ser muy utilizada para comprar o vender, sino que se ofrece como recompensa a los proveedores de contenidos en la red, por lo que su valor es muy bajo.

**Dash**

Dash es una criptomoneda renombrada que antes se le conocía como Darkcoin. Una de las cualidades por las que se hizo famosa esta moneda virtual, fue la introducción del anonimato en las transacciones realizadas por los usuarios. Recordamos que las criptomonedas suelen ofrecer privacidad porque no se conocen los datos del usuario, pero todas sus transacciones quedan registradas y todo el mundo las puede ver. En este caso, Dash sí que ofrece este anonimato e intenta eliminar el origen de las transacciones realizadas.

Esta moneda digital está considerada como una forma de transacción mucho más segura que otras competidoras por su sistema de seguridad con 11 algoritmos que dificulta hackear la red Dash. Además, también es mucho más simple de utilizar para la minería de criptomonedas, ya que es más asequible para ordenadores normales que el Bitcoin.

**Monero**

A diferencia de otras criptomonedas, Monero se caracteriza por utilizar el protocolo CryptoNote y ofrece algunas mejores frente a la popular moneda, llamada Bitcoin. Este protocoloa permite el uso de la GPU y de la CPU del ordenador para minar monedas, cosa que es imposible de conseguir con el Bitcoin. Por lo que puedes llegar a minar Moneros con tu ordenador de sobremesa.

En este caso, la cadena de Bloques de Monero está oculta, por lo que esta criptomoneda también ofrece el anonimato en las transacciones realizadas por los usuarios. Además, estas transacciones también son mucho más rápidas que el Bitcoin, ya que el tipo de generación de bloques es de 2 minutos frente a los 10 del Bitcoin.

**Petro**

Aunque las monedas nacen como sistemas descentralizados para escapar del control del gobierno y organizaciones económicas internacionales, empiezan a surgir las primeras gubernamentales. Este es el caso del Petro, la primera criptomoneda lanzada por el Gobierno de Venezuela.

Esta criptomoneda se apoya en el petróleo para determinar su precio y se utiliza a modo de financiación para el desarrollo del país. Por si fuera poco, también se creará el Petro Oro, en este caso, una criptomoneda apoyada en el valor del oro.

**Bibliografia:**

* <http://seguridad-informatica-1-iutll.blogspot.com/2012/11/seguridad-fisica-y-logica.html>
* <http://46.101.4.154/Art%C3%ADculos%20t%C3%A9cnicos/Seguridad%20Inform%C3%A1tica/Seguridad%20b%C3%A1sica%20en%20desarrollos%20PHP.pdf>
* <http://www.custodia-documental.com/familia-iso-27000-seguridad-de-la-informacion/>
* <https://seguinfo.wordpress.com/2007/07/05/%C2%BFque-es-la-firma-digital-2/>
* <https://www.yolandacorral.com/que-es-blockchain-tecnologia-disruptiva/>
* [**http://www.redalyc.org/pdf/4768/476847246004.pdf**](http://www.redalyc.org/pdf/4768/476847246004.pdf)
* <http://blog.derecho-informatico.org/2011/02/27/seguridad-basica-en-android/>