

REVISTA
CIENCIAS
SISTEMAS & TECNOLOGÍA

ABRIL 2020 - EDICIÓN XVI

ECYS

ESCUELA DE INGENIERÍA EN CIENCIAS Y SISTEMAS

SIMULACIÓN Y MODELACIÓN

LA IMPORTANCIA EN LA ACTUALIDAD

INTELIGENCIA ARTIFICIAL

EL PRÓXIMO COMPETIDOR EN LA OFERTA LABORAL

DESARROLLO FRONT END

CON VueJS

SERVERLESS

INTRODUCCIÓN A SU ARQUITECTURA

IOT

EN LA ACTUALIDAD



FACULTAD DE INGENIERÍA



EDITORIAL

CIENCIAS, SISTEMAS & TECNOLOGÍA

El área de tecnología se hace cada vez más presente en cada una de las disciplinas de la ciencia y en la cotidianidad de la vida, su presencia ha permitido distintos avances en múltiples áreas. Es así como hoy en día se plantean nuevos retos para los profesionales en las áreas de tecnología, los cuales requieren mantener una gama mucho más amplia de conocimiento y de aplicación. Lo cual demanda su versatilidad y capacidad para entender "el negocio" con una mayor agilidad a la vez de tener la capacidad de innovar en éste.

Es así como cada vez se abre paso a un ritmo mucho más vertiginoso disciplinas como el internet de las Cosas IoT, o inteligencia artificial. La primera permite tener una presencia casi omnipresente, relacionando múltiples elementos y tecnologías con el fin de crear soluciones que cada vez se masifican más.

Por otro lado, el desarrollo en el campo de la inteligencia artificial, ha permitido aumentar la capacidad de procesamiento y respuesta, cambiando la lógica del trabajo y ocupación humana, en la cual no es la excepción el área de tecnología, que también se ha visto remplazada en la realización de sus propias tareas, principiendo por las de carácter más mecánico. Pero a la vez ha aperturando nuevos nichos. Haciendo cada vez más accesible tecnología y herramientas, las cuales permitirán el desarrollo e irradiación de la presencia de profesionales de sistemas.

Pero el reto no solo va en función del conocimiento, también demanda un balance ético en su proceder, así como una claridad de dirección, toda vez que parte de su perfil demandará características de liderazgo cada vez más.

MSc. Ing. Carlos Gustavo Alonso
Director de la Escuela de Ciencias y Sistemas
Facultad de Ingeniería
Universidad de San Carlos de Guatemala

Director General

MSc. Ing. Carlos Gustavo Alonso

Coordinación Editorial

Ing. Álvaro Giovanni Longo Morales

Colaboración Especial

Ing. Miguel Marín de León

Portada, edición, diseño y diagramación

Celma Evelyn Pérez Pérez

Links Disponibles:

- Revista Ciencias, Sistemas y Tecnología
- Escuela de Ingeniería en Ciencias y Sistemas
- Revista Ciencias, Sistemas y Tecnología - Issuu.com

Contactenos:

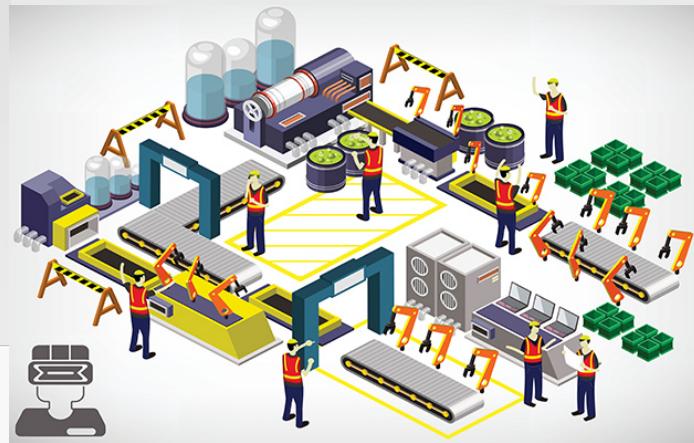
revista.ecys@gmail.com



ECYS

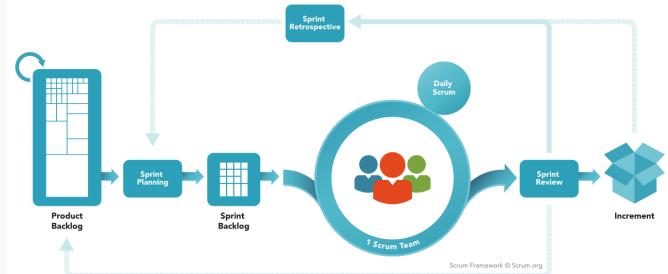
CONTENIDO

CIENCIAS, SISTEMAS & TECNOLOGÍA



01	Introduciendo a arquitecturas serverless	
04	Inteligencia Artificial, el próximo competidor en la oferta laboral	
06	IoT en la actualidad	
08	La importancia de la simulación y modelación en la actualidad	
11	Desarrollo Frontend con VueJS	
13	Adaptándose a Scrum	
15	Docker y Herramientas de Orquestación	
18	Ruta de aprendizaje, para ser un mejor profesional	
21	Firma electrónica avanzada, el futuro de la autenticidad de documentos	
24	Introducción a Hyperledger Composer	
26	Analista de Datos	
29	Google Search como herramienta para Hacking	
32	Progressive Web Apps y el futuro del desarrollo web	
35	Criptografía: El arte de ocultar mensajes	

SCRUM FRAMEWORK



Scrum.org



Introduciendo a arquitecturas serverless

Ronald Neftali Berdúo Morales
ronaldnef1996@gmail.com

Estudiante de Ingeniería en Ciencias y Sistemas - USAC

Palabras Clave:

Servicio, función, proveedor, servidor

Aunque el término Serverless traducido al español es "sin servidor", en realidad una arquitectura Serverless se refiere específicamente a lo que es olvidarse de la gestión de servidores al momento de desplegar aplicaciones y servicios.[1]

¿Qué es Serverless? Es un término que se refiere a otros dos términos a la vez los cuales son Backend as a Service (BaaS) y Function as a Service (FaaS).[2]

Backend as a Service Es un término que lleva ya bastante tiempo de existir; el primer proveedor en lanzar este tipo de servicio fue Amazon con Amazon S3 lanzado en el año 2006 el cual provee un alojamiento de archivos en la nube. BaaS es muy similar a Software as a Service (SaaS) en donde los proveedores proporcionan servidores que son conectados a nuestras aplicaciones mediante una API, en general nos ofrecen componentes genéricos como almacenamiento, autenticación de usuarios, servicios de base de datos, entre otros. Generalmente estos servicios son utilizados para construir otros servicios más específicos, esto tiene una gran ventaja ya que como desarrollador puedo decir que no se pierde lo que es tiempo en construir aplicaciones o servicios que ya existen y sin preocuparse por mantenerlas. Hay muchas empresas que nos ofrecen este tipo de servicios entre ellas tenemos a Amazon con DynamoDB y Firebase de Google.

Function as a Service FaaS, nació en 2014 con la llegada de Amazon Lambda [3] ha sido el término que ha hecho popular a Serverless y lograr que aparezca. FaaS no es más que una nueva forma de ejecutar y diseñar aplicaciones con la cual se pueden reducir inversiones en infraestructura ya que solo se generan costes cuando se utiliza el servicio, algunos ejemplos de proveedores de FaaS son Amazon Lambda, Google Functions y Azure Functions [4].

¿Cuándo usar Serverless? Antes de entrar a detalle de cuando es correcto usar Serverless, veamos los siguientes beneficios [5]:

Beneficios - Como sé a dicho anteriormente una ventaja es no administrar los servidores.

- No hay administración de infraestructura, el desarrollador no tiene ningún control sobre las instancias y contenedores, ya que los proveedores FaaS o BaaS se encargan de mantenerlos.
- La escalabilidad automática, la capacidad aumenta y se distribuye automáticamente según se necesita esto es así para todos los servicios Serverless; los proveedores siempre tienen algún contrato donde exponen cual es la máxima capacidad que ellos proveen, aunque se puede llegar a dar el caso en donde se comunique con el proveedor para solicitar un aumento en las capacidades de nuestros servicios.
- Arquitectura orientada a eventos, como por ejemplo responder a peticiones Http, a cambios en una base de datos, modificación de archivos, en la creación de un nuevo usuario en el sistema, o cualquier tipo de evento valido para que se disparen nuestras funciones.
- No hay costos de contratación, ya que simplemente se paga por lo que se usa, si una función no se está ejecutando, esta función no llega a generar un costo.

Con los beneficios que nos otorga Serverless se puede decir que es conveniente usarlo cuando se tiene los siguientes casos:

- Cuando necesitamos que una tarea corta se deba ejecutar con una frecuencia fija.
- Si necesitamos trabajar con un modelo de integración y despliegue continuo.

- Poder realizar microservicios ya que no necesitamos gestionar instancias.
- Aplicaciones web que no requieran realizar procesos rigurosos.

¿Cuándo no usar Serverless? - Cuando no queremos depender de un proveedor, ya que estamos usando servicios sin haberlos creados nosotros mismos, esto limita a empresas que no quieren migrar a un servicio a la nube, para esto es recomendable realizar un análisis de riesgos para estar completamente convencidos si vale la pena o no utilizar estos servicios.

- Cuando tenemos ejecuciones largas que no se pueden cortar o no se pueden paralelar, ya que servicios como Amazon Lambda solo nos provee un máximo de 5 minutos de tiempo de espera por cada función.
- Para operaciones complejas, existen operaciones que necesitan infraestructura dedicada, muy específica para poder resolver ciertas tareas en un tiempo razonable ya que la infraestructura que nos provee la plataforma de la nube es muy genérica y no se puede realmente modificarla.

Un ejemplo sencillo Supongamos que tenemos una aplicación web en la cual podemos subir imágenes y poder visualizarlas, también se tiene que administrar usuarios, y por último se tiene que interactuar con un servicio RESTful para poder obtener las imágenes y poder guardarlas. Para esto se describirán los servicios a utilizar para implementar esta aplicación en Amazon Web Services (AWS). La aplicación hará uso de AWS Lambda, Amazon API Gateway, Amazon S3, Amazon DynamoDB y Amazon Cognito, como se muestra en la imagen 1.[6]

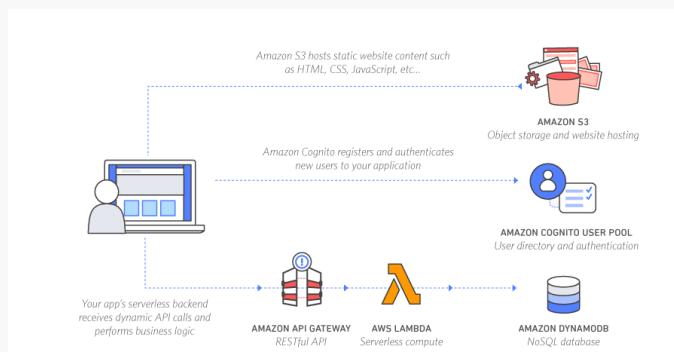


Imagen 1: Ejemplo de una arquitectura sin servidor en AWS

S3 Como primer punto tenemos lo que es Amazon S3 que es un servicio de almacenamiento para internet, es decir es donde nosotros alojaremos nuestros archivos estáticos como HTML, CSS, JavaScript, imágenes o cualquier tipo de archivos que se puedan cargar en algún tipo de navegador.

Cognito Este servicio es muy útil ya que nos facilita en gran medida lo que es la autenticación, autorización y administración de usuarios para nuestras aplicaciones móviles y web.

DynamoDB Es un servicio de base de datos NoSQL en la cual para este ejemplo se guardará la información necesaria para guardar una imagen como por ejemplo el nombre del archivo y la ruta de S3 en donde se localizará la imagen.

Lambda En lambda se crean una función para almacenar una imagen en S3 y guardar la información en una tabla de DynamoDB, también se creará una función para obtener toda la información de las imágenes que se guardaron en DynamoDB.

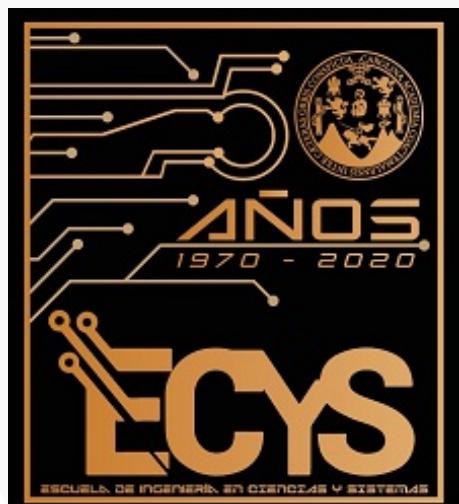
API Gateway Y por último tenemos a quien dispare los eventos Http para poder invocar a las funciones creadas en Lambda para guardar una imagen y poder obtenerlas.

Conclusiones

- Las arquitecturas Serverless han logrado evolucionar hasta ser una herramienta de gran utilidad para el despliegue de alguna funcionalidad a un ambiente de producción sin invertir en la infraestructura y pagando solamente cuando se ejecute.
- Al utilizar Serverless se reducen los costos, se reduce el tiempo de desarrollo, se aumenta la seguridad y se incrementa la fiabilidad.
- Serverless no es el enfoque correcto para cada problema, así que siempre se tiene que realizar un análisis antes de pasarse a trabajar con este tipo de arquitectura.

Referencias

- [1] Amazon. (5 de noviembre 2018). Amazon: **Creación de aplicaciones con arquitecturas sin servidor.** Recuperado de: <https://go.aws/33BuWx0>. [Último acceso: 10 de octubre de 2019].
- [2] Hernando, C. (Abril 2017). Chernando: **¿Qué es Serverless?**. Recuperado de: <https://bit.ly/39aX3Ei>. [Último acceso: 11 de octubre de 2019].
- [3] L. Gracia (22 de junio 2016). Unpocodejava: **¿Qué es una Arquitectura Serverless (y AWS Lambda)?**. Recuperado de: <https://bit.ly/2Wwy6At>. [Último acceso: 12 de octubre de 2019].
- [4] Rucinque, P. (04 de enero 2017). Medium: **¿Qué es eso de serverless?**, Recuperado de: <https://bit.ly/2QBbwD7>, [Último acceso: 10 de octubre de 2019].
- [5] Borillo, R. (01 de abril 2019) Genbeta: **Qué es serverless y por qué adoptarlo en el desarrollo de tu próxima aplicación** Recuperado de: <https://bit.ly/3a3MT9T>. [Último acceso: 08 de octubre de 2019].
- [6] Amazon. (05 de noviembre 2018). Amazon: **Aplicación web sin servidor.** Recuperado de: <https://go.aws/33BMAkf>. [Último acceso: 10 de octubre de 2019].



Ahora trabajamos todos en

UUSAC - SICOIN

Sistema de Contabilidad Integrada
SICOIN / Descentralizadas(PROD-SRV1)

<https://sicoindes.minfin.gob.gt/>



USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala



GOBIERNO de
GUATEMALA

MINISTERIO DE
FINANZAS PÚBLICAS



SIAF-SAG





Inteligencia Artificial, el próximo competidor en la oferta laboral

Noé Alfonso Ruiz Rivera
noetux7@gmail.com

Estudiante de Ingeniería en Ciencias y Sistemas - USAC

Palabras Clave:
Inteligencia Artificial, trabajo, competencia

Como civilización hemos avanzado en muchos aspectos tecnológicos, nuestro conocimiento es cada vez más amplio y nuestro estilo de vida exige cada vez más de ciencia, esto por su puesto es algo que va en conjunto con los tipos de trabajo que realizamos.

Podemos ver a lo largo de la historia que el ser humano ha mejorado su entorno y se ha facilitado muchos trabajos, la idea principal de crear nuevas herramientas es esa: hacer más fácil una tarea que anteriormente demandaba mucho esfuerzo, un ejemplo de esto puede ser el automóvil, con su ayuda es más fácil desplazarnos grandes distancias, más cómodos y con menos esfuerzo. De forma similar en la agricultura ahora se utiliza maquinaria que se encarga de tratar la tierra, regar las plantaciones y automatizar las cosechas. Todo este trabajo era algo que anteriormente hacían las personas, pero ahora es realizado por máquinas. Podemos ver que actualmente algo parecido está sucediendo, pero con trabajos en los cuales creímos que solamente eran capaces los humanos de realizar. La inteligencia artificial cada vez se asemeja más a la humana y en ámbitos específicos es capaz de retar a los mejores.

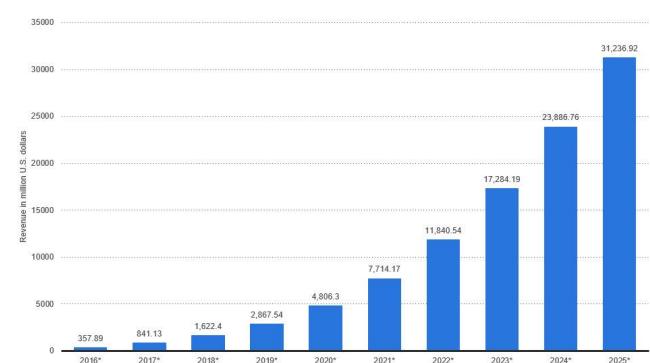
Los trabajos que empieza a realizar la inteligencia artificial ya no son físicos sino intelectuales. Entonces ¿qué sucede en un mundo donde las máquinas son capaces de hacer prácticamente todo lo que pueden hacer los humanos?, ¿qué pasa con esos empleos?, ¿de qué vivirán las personas?

Los avances en la IA son muy impactantes, sin embargo, aún hay mucho camino por recorrer. La IA que tenemos actualmente está especializada para un tipo específico de problema, la IA de propósito general aún se encuentra en una etapa temprana. Actualmente la IA en muchos de los negocios aún requiere de supervisión humana. Los trabajos que la IA está comenzando a tomar son aquellos que son repetitivos y en los cuales la toma de decisiones

es básica, así que este tipo de trabajos también son los más aburridos. Pero conforme la IA avanza sus capacidades le permitirán tomar empleos más complejos, esto puede ser preocupante para muchos y nos lleva a la pregunta ¿está mi empleo en riesgo?

Los trabajos que puede tomar la IA son los más básicos, se espera que hasta mediados de los 2030s se tenga un aproximado de 30% de empleos tomados por la IA. Y esto va a ir en aumento. Pero entonces cómo podemos los seres humanos hacerle frente a un competidor que nunca se cansa, trabaja todo el día y no cobra como nosotros, la respuesta puede ser en un cambio total de paradigma que debe hacer la sociedad, surgirán nuevos empleos en los cuales las personas supervisen el trabajo que realice la IA, sin embargo, esto requiere de especialización ya que no cualquiera puede crear o mantener una IA sin previa educación del tema.

Enterprise artificial intelligence market revenue worldwide 2016-2025
Revenues from the artificial intelligence for enterprise applications market worldwide, from 2016 to 2025 (in million U.S. dollars)



statista

Imagen 1: Ingresos de la Inteligencia Artificial para aplicaciones empresariales a nivel mundial.

Un consuelo es que los empleos no van a ser arrebatados por completo por la IA, lo que en realidad se espera que suceda es que en los puestos de trabajo

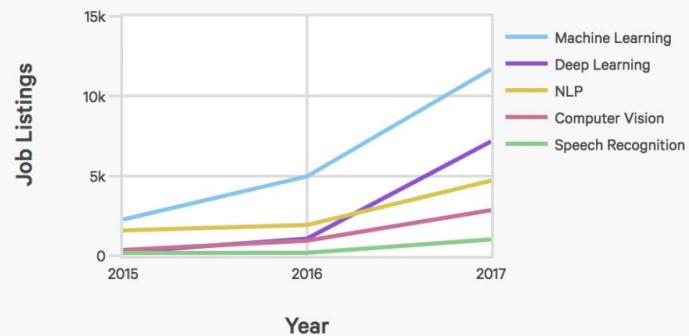
se especialicen para trabajar en conjunto con la IA. Por ejemplo, en el servicio al cliente se pueden mejorar los procesos y la velocidad de respuesta, en el sector de la salud los médicos se van a apoyar de herramientas de IA para obtener diagnósticos más precisos. Podemos ver esto como una evolución de nuestra civilización, donde la única opción es adaptarnos.

Durante la revolución industrial los empleos comenzaron a cambiar drásticamente, las fábricas comenzaron a mejorar sus procesos usando maquinaria que reemplazaba a las personas que hacían ciertas tareas. Esto fue necesario ya que la demanda de productos crecía cada vez más y se requería de otros métodos para satisfacerla. De forma parecida podemos ver ahora esta evolución que está comenzando a darse en la industria. Podemos verlo como algo que traerá otras oportunidades, otro tipo de empleos que posiblemente no tenemos ni idea de que existirán, no como algo que nos perjudicará.

Para no ser reemplazados por la IA lo que tiene que hacer la sociedad es prepararse, especializar a las personas y brindarles los conocimientos necesarios para trabajar de forma conjunta con la IA. Solo perderá quien no esté dispuesto a el cambio, como es en todo.

No todos los empleos van a verse afectados directamente por la IA. Empleos en los cuales se requiere de creatividad, capacidad de expresión humana, arte, etc., van a estar por mucho tiempo más como algo exclusivamente humano. Es probable que entonces nuestra industria nos lleve a las personas a trabajar más en cosas que solo nosotros como humanos seríamos capaces de hacer y apreciar y dejar el trabajo aburrido a las máquinas. Todo esto aún está por descubrirse, no se sabe con certeza cómo evolucionará nuestra sociedad y que tan rápido nos adaptaremos a estos cambios, pero si sabemos que debemos prepararnos y aprovechar las oportunidades ya que los empleos van a evolucionar y se crearan otros nuevos.

Job Openings, Skills Breakdown (Monster.com)



Source: Monster.com

AIINDEX.ORG

Imagen 2: Nuevos empleos, desglose de habilidades.

Conclusiones

- La Inteligencia Artificial aún se encuentra en una etapa temprana y la mayoría de trabajos que puede realizar son los más repetitivos con supervisión humana.
- Es cierto que la IA está avanzando y cada vez podrá realizar trabajos más complejos con menor supervisión. Por lo tanto, se dará un cambio en la industria y es necesario que las personas se comiencen a capacitar en habilidades de IA como su creación, mantenimiento y control.
- El avance de la IA también trae oportunidades, existirán cada vez más empleos en este campo. Lo importante es estar preparados para el cambio. Así como sucedió en la revolución industrial y muchas personas cambiaron de trabajos así también nos esperan cambios en la industria.

Referencias

- [1] Marria, V. (11 de enero 2019). Forbes: **The Future of Artificial Intelligence in The Workplace**. Recuperado de: <https://bit.ly/3a9MJ0C>. [Último acceso: 11 de enero de 2019].
- [2] Minevich, M. (28 de enero 2019). Observer: **A.I. and Automation Are NOT the Death of the American Workforce**. Recuperado de: <https://bit.ly/3deyZ6O>. [Último acceso: 28 de enero de 2019].



IoT en la actualidad

Diana Maribel Jimenez Alonzo
dianajimalon@gmail.com

Estudiante de Ingeniería en Ciencias y Sistemas - USAC

Palabras Clave:

Voto electrónico, *blockchain*, votación, seguridad, política, elecciones, democracia.

En la actualidad podemos ver diversos objetos de uso diario que se conectan a la red, por ejemplo un reloj con capacidad para contar distancias recorridas, el sistema eléctrico de una casa manipulado desde un teléfono celular, sistemas de vigilancia para mascotas, automatización de electrodomésticos de una casa y muchos otros.

Con el avance de la tecnología se están generando grandes cantidades de datos de diferentes dispositivos electrónicos. Todos estos datos recolectados son utilizados por las diferentes empresas para ser analizados y generar las acciones correspondientes dependiendo del tipo de servicio que brinden.

IoT es la abreviación del inglés Internet of Things (Internet de las Cosas). La internet de las cosas es un sistema de dispositivos de computación interrelacionados, máquinas mecánicas y digitales, objetos, animales o personas que tienen identificadores únicos y la capacidad de transferir datos a través de una red[1].

Miles de objetos están siendo utilizados por IoT en todo el mundo. Todo esto ha sido posible con la evolución de la tecnología a lo largo del tiempo. Cada vez es más la demanda de estos objetos debido a que las personas buscan optimizar y facilitar la realización de sus actividades lo que los lleva a buscar diversas soluciones que satisfagan sus necesidades. Estos objetos están siendo utilizados en diversos lugares como lo puede ser hogares, negocios, empresas y en diversas áreas como por ejemplo los deportes y agricultura.

Además, las empresas relacionadas con la creación de software se están aliando con empresas de creación de objetos cotidianos, con el fin de crear productos novedosos que incluyan lo último en tecnología y conectividad a la red.

En la actualidad se pueden ver una amplia gama

de objetos que han incluido IoT, a continuación se mencionaran algunos.

No es muy común en la sociedad y sobre todo en Guatemala, pero ya existe la ropa que incluye IoT con la capacidad de realizar acciones de regularización de temperatura, controlar un dispositivo móvil, recepción de impulsos de sonido y vibración.

Zapatos inteligentes ya es una realidad, tal es el caso de la empresa Nike que lanzó unas zapatillas de baloncesto las cuales se ajustan al tamaño y adaptan los cordones de forma manual o través de una aplicación móvil y un sistema indicador con luces led [2]. Nike también tiene una línea llamada Nike Connected Jersey diseñada para la NBA las cuales están conectadas con la aplicación NikeConnect por medio de un chip para obtener información de los juegos, presentar contenido durante está ocurriendo el juego y contenido interactivo del equipo al que pertenece la camiseta, esta tecnología también la aplican en camisolas del Chelsea FC.



Imagen 1: Zapatos Nike Adapt

También podemos encontrar una chaqueta inteligente diseñada en colaboración de Levis's y Google, esta chaqueta permite gestionar música y obtener direcciones de Google Maps. Esta chaqueta se conecta mediante una pulsera electrónica a una serie de hilos de tecnología inalámbrica incrustados en la chaqueta y en la etiqueta[3].

Los relojes que integran IoT son objetos que están siendo bastante populares. Algunas ventas de teléfonos celulares los incluyen en la compra de un Smartphone, estos relojes nos proporcionan diversos beneficios, van desde contar el número de pasos, estimar frecuencias cardíacas, mostrar información relacionada con el clima local, brindar servicios de ubicación, mostrar notificaciones del teléfono celular e incluso algunos pueden realizar llamadas.

En Guatemala son muy pocas las empresas que se dedican tanto a la realización de proyectos con IoT y a la prestación de estos servicios.

Flatbox es una empresa guatemalteca que ofrece servicios de IoT, cuenta con servicios que gestionan el número de personas que entran a los negocios o empresas, un servicio para gestionar el consumo eléctrico, también ofrecen un servicio para controlar la temperatura sobre algún lugar deseado y por último tiene un servicio para medir el consumo de agua y generar históricos. Flatbox se ocupa de mantener una base de datos con todas las lecturas de todos tus dispositivos, proporciona análisis y comentarios valiosos[4].

Aerobots es otra empresa guatemalteca que aplica sus servicios de IoT en la agricultura. Ofrece los servicios de fotografía RGB e infrarroja, medición de índices de vegetación, generación de modelos de elevación digital, detección de líneas de surco, detección de maleza, análisis de rebrote en caña de azúcar, automatización de bombas de riego, detección de fuego por medio de radares y video 360 para supervisar las diversas áreas.



Imagen 2: . Aerobots digitalizando la agricultura

Aerobots se dedica al desarrollo de tecnologías de recolección y análisis de datos para generar información ejecutable[5].

Conclusiones

- IoT es algo que en Guatemala aún no es tan popular debido a que no hay tantas empresas que provean estos servicios, pero conforme el tiempo esto se volverá una tendencia.
- IoT busca agilizar de manera eficiente las actividades de los seres humanos.
- La mayoría de objetos que conocemos pueden ser automatizados, tal es el caso de los artículos de vestir, que aunque actualmente son pocos los que existen, en el futuro esto va a ser bastante común verlo.

Referencias

- [1] Rouse, M. (31 de enero 2017). Searchdatacenter: **Internet de las cosas (IoT)**. Recuperado de: <https://bit.ly/2WtH95n>. [Último acceso: 05 octubre 2019].
- [2] Frías, G. (16 de enero 2019). CNN: **Nike lanza zapatos deportivos inteligentes** . Recuperado de: <https://cnn.it/2Qyd6Ws>, [Último acceso: 05 octubre 2019].
- [3] Fernández, M. (25 de septiembre 2017). El Androide Libre: **La primera chaqueta inteligente es de Google y Levi's**. Recuperado de: <https://bit.ly/3didDpi>. [Último acceso: 05 octubre 2019].
- [4] Flatbox. (2016). Flatbox: **Haga crecer su negocio**. Recuperado de: <https://flatbox.com>. [Último acceso: 05 octubre 2019].
- [5] Aerobots. (2019). Aerobots: **Digitalizando la agricultura**. Recuperado de: <https://www.aerobots.gt/>. [Último acceso: 05 octubre 2019].



La importancia de la simulación y modelación en la actualidad

Dénilson Eduardo Argueta Higueros

deahtom123@gmail.com

Estudiante de Ingeniería en Ciencias y Sistemas - USAC

Palabras Clave:

Simulación, Modelación, procesos, transporte.

La modelación y simulación es algo realmente importante ya que nos permite experimentar y visualizar cómo se comporta un sistema y en qué área se pueden realizar mejoras en el funcionamiento del sistema basándonos en resultados obtenidos en la simulación [1]. Antes de empezar cualquier tipo de proyecto se debe de entender bien como es que funciona el sistema y cuáles son las variables involucradas para poder modelar el sistema y que sea muy parecido al sistema en la realidad. La manera más sencilla de que podamos determinar que el modelo sea válido es determinar que las salidas del modelo están muy cerca de la realidad del sistema.

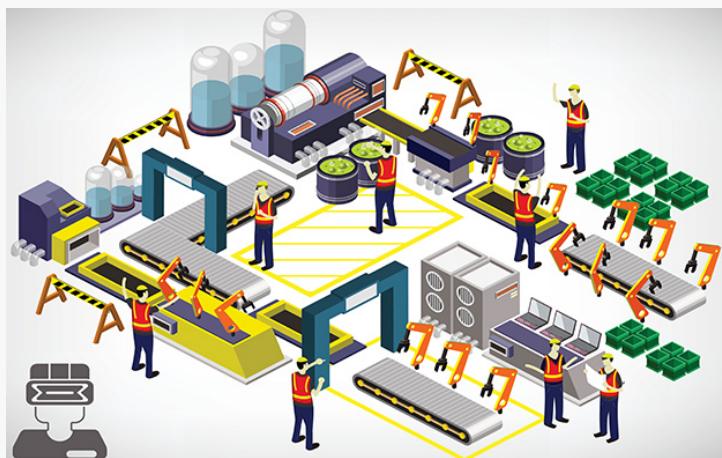


Imagen 1: Dibujo de una fábrica en donde se encuentra empleados cada uno en un área.

La modelación y simulación puede ser aplicada en diversos campos como la industria, entrenamiento militar, elaboración de automotores, supermercados, proyectos de reducción de costos[2], etc. Uno de los ejemplos más sencillos para entender cómo funciona la modelación y simulación es imaginarse el funcionamiento de un banco. Cada día llegan a los bancos un número de personas, pero no se puede saber con exactitud la cantidad de personas que llegarán a un banco en un día X, pero basándose en información histórica se puede determinar con

algún tipo de probabilidad la cantidad de personas que pueden llegar y los inérvulos de tiempo en donde llegará más gente. Por ejemplo, se sabe que finales de mes y en quincena es cuando más gente acude al banco ya que son los días de pago y por lo regular la gente acude al banco después de las 4:00 pm ya que a esa hora comienzan a salir de su trabajo.

Basándonos en esta información histórica y determinando como es el sistema, se puede realizar un tipo de animación en algún programa, para poder determinar con la llegada de estas personas cuántos servidores(empleados) se necesitan en ciertos días y horas para que cuando llegue la gente no se sature en banco y así la gente no tengan molestias ni se produzca alguna pérdida para el banco. Al momento de que una persona espera mucho tiempo es una pérdida tanto para el cliente como para la empresa ya que el cliente estará perdiendo tiempo y eso le ocasionara una molestia ya que es pérdida de tiempo. Y bien se sabe que un cliente molesto es una pérdida para las empresas ya que puede significar la pérdida del cliente o que cuente su mala experiencia a otros clientes potenciales de la empresa.

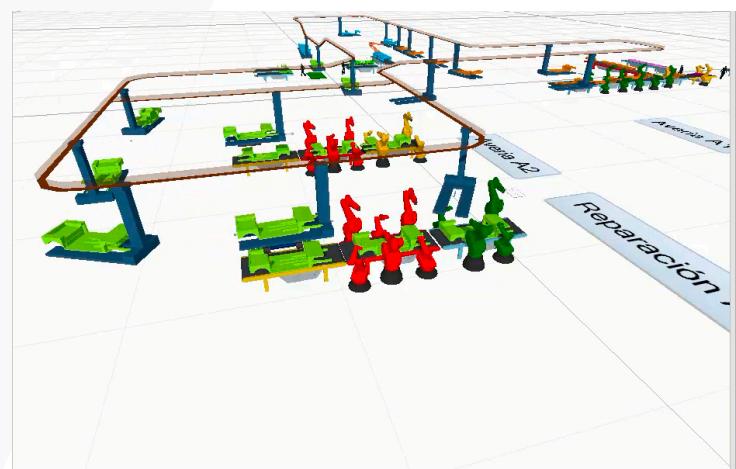


Imagen 2: Ejemplo de un modelo de simulación.

Otro ejemplo de simulación y modelación sería el planeamiento y modelación de tráfico. Este tema es muy importante ya que actualmente el problema que se presenta en el tráfico en la ciudad de Guatemala a las horas pico afecta a todos las personas que transitan en las vías congestionadas. Y es por la mala planeación que se ha tenido desde un principio en la construcción de las principales vías en la ciudad y en todo el territorio guatemalteco. Y es que las autoridades realizan construcciones como puentes, pasos a desnivel, etc. hasta el momento que se dan cuenta que se están generando problemas de tránsito.

Lo ideal sería presentar una simulación del tráfico en horas pico en el sector y posterior a esto un análisis para ver si es necesario la construcción de algún tipo de estructura que ayude con el tránsito, luego determinar en cuánto tiempo sería adecuado la construcción y por último el impacto que tendrá la construcción en el sector. Un ejemplo en Guatemala es el departamento de Sacatepéquez, específicamente en San Lucas. En ese sector se encuentra por lo regular muy congestionado ya que hay un cruce en donde paran el tráfico por un par de minutos una vía muy circulada y si no paran el tráfico es prácticamente imposible poder cruzar en ese sector. Y ahora que se quiere realizar una construcción en ese sector será algo que afectará aún más el tránsito en ese lugar.

Para este y muchos casos más sería de gran ayuda la simulación ya que nos permitiría conocer más las zonas más circuladas en el país y si en base a los resultados obtenidos tomar decisiones para la construcción de algún tipo de estructura para mejorar el tráfico, algún semáforo, o en los sectores que existan semáforos cuánto tiempo debería de dar a cada vía para que el tráfico sea más fluido en las principales arterias del país.

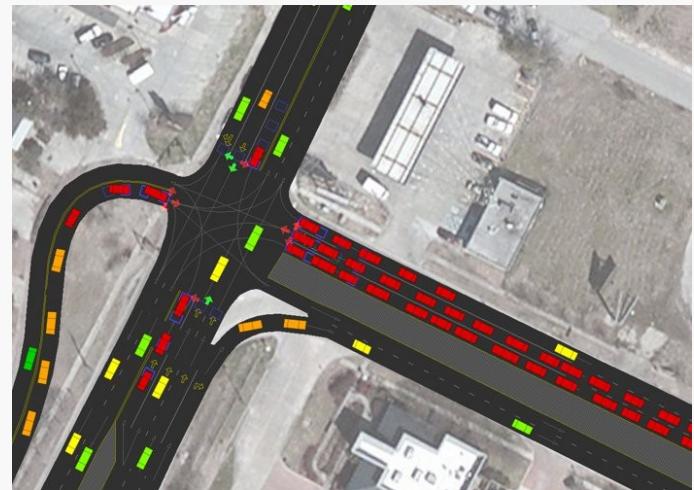


Imagen 3: Simulación de planeamiento y modelación de tráfico en 2 dimensiones

Existe programas especializados para la simulación de planeamiento y modelación de tráfico. Es común que estos programas permitan realizar simulaciones en 2 dimensiones y 3 dimensiones, esto para que sea más fácil para el usuario entender el modelo y que pueda verificar si está funcionando adecuadamente el modelo. Este tipo de programas son bien completos ya que es posible simular semáforos, cruces, señales de tránsito, carriles, transporte público, etc.

Existen muchas herramientas hoy en día que cada vez nos hacen la vida más fácil y nos ayudan a la toma de decisiones. ¿Seguirá cambiando la modelación y simulación la forma que miramos al mundo?



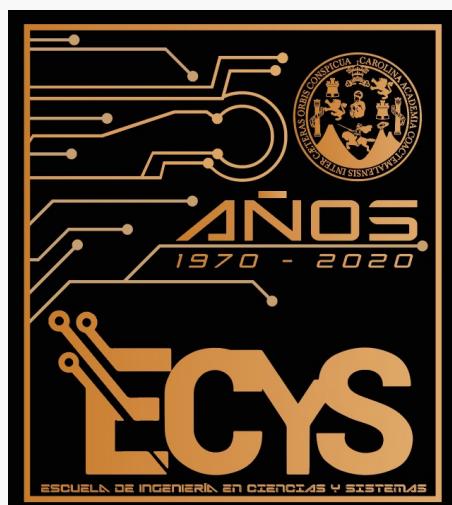
Imagen 4: Simulación de planeamiento y modelación de tráfico en 3 dimensiones

Conclusiones

- Es de suma importancia conocer la modelación y simulación para entender un sistema y tomar decisiones con los resultados de este.
- Existen diversos programas y cada uno está especializado en un área por ejemplo modelación de tráfico, transporte, industrias, etc.
- Es posible realizar un ambiente sintético por medio de un programa para simular una situación de la vida real.
- Es posible predecir el comportamiento en el futuro de un sistema mediante la simulación.

Referencias

- [1] Desconocido. Caliper: **TransModeler Introducción**. Recuperado de: <https://bit.ly/2Wz1jL5>. [Último acceso: 29 de octubre de 2019].
- [2] Soto, J. (30 de abril 2012). lisdiur: **Simulación y Modelación**. Recuperado de: <https://bit.ly/2J4BtGZ>. [Último acceso: 29 octubre 2019].
- [3] Desconocido. (21 de marzo 2017). Two Reality: **La simulación virtual como método de formación de personal**. Recuperado de: <https://bit.ly/3akbuHP>. [Último acceso: 29 octubre 2019].



BIOTOPO CERRO CAHUI

Ubicado en el Departamento de Petén.

Cuenta con acceso a la playa del Lago Petén Itzá, senderos, miradores, área para acampar, salón de reuniones, observación de animales

Horario de lunes a domingo de 7:00 a 17:00 horas
Costo de entrada: Nacionales Q.10.00; Extranjeros Q.40.00;
Colegios, Estudiantes y Trabajadores de la USAC Q.5.00;
Escuelas públicas Q.1.00

[/areasprotegidasuniversitarias.cecon/](#)

Fotografía: David Creswell



Desarrollo Frontend con VueJS

Diego Antonio Momotic Montesdeoca

diegomomotic@gmail.com

Estudiante de Ingeniería en Ciencias y Sistemas - USAC

Palabras Clave:

Desarrollo web, Front-end, Vue, Cliente, Servidor, JavaScript, Framework.

Vue es un framework JavaScript de código abierto, enfocado completamente al desarrollo de interfaces, creado por el ex empleado de Google Evan You y lanzado en el año 2014[1].

Una de las principales razones que me motivaron incursionar en Vue luego de interesarme en el desarrollo web frontend, fue la impresionante cantidad de artículos y tutoriales que existen en internet sobre Vue, esto me llevo a investigar un poco más y a realizar comparaciones de Vue con el framework Angular y con la librería React, los 2 gigantes para el diseño de interfaces. Mi sorpresa fue grande al notar que, en muchos artículos con relación al tema, posicionan a Vue entre los mejores en cuanto a su rendimiento y curva de aprendizaje donde claramente destaca sobre Angular y React.



Imagen 1: Logotipo de VueJS,

¿Qué debo saber antes de utilizar Vue?

Lo único que necesitas, es tener conocimientos en HTML y JavaScript. Adicionalmente es un “plus” conoces sobre CSS, sin embargo, no es del todo necesario ya que existen algunas herramientas que facilitan el proceso de estilización en nuestras aplicaciones hechas con Vue de una manera sencilla, sobre estas herramientas hablaremos un poco más adelante.

¿Qué beneficios obtengo al utilizar Vue?

A continuación, detallaré el conjunto de Característica que me han convertido en un gran fan de este poderoso y magnífico framework.

- **Debemos preocuparnos únicamente por los datos y no por la renderización.** Nosotros necesitamos enfocarnos específicamente en la lógica de procesamiento de datos y será Vue, el encargado de renderizar la información en pantalla cada vez que detecte un cambio
- **Integración sencilla.** Desde mi primer proyecto con Vue (el típico “Hola mundo”), fue grande mi sorpresa al notar lo extremadamente fácil que es integrarlo a nuestros proyectos, ya que, basta con añadir el CDN a nuestra página y ya estaremos listos para iniciar a trabajar con el framework. Otras herramientas requieren mucho más esfuerzo para su integración.



```
<script src="https://cdn.jsdelivr.net/npm/vue/dist/vue.js"></script>
```

Imagen 2: Adición de Vue a nuestro proyecto,

- **No necesitas aprender ningún lenguaje adicional.** Como lo mencioné anteriormente, solo debemos tener buenas bases en HTML y JavaScript, estos lenguajes son los que, por lo general, todos necesitamos aprender antes de incursionar en el maravilloso mundo del desarrollo web. Esta es una de mis características favoritas ya que otros frameworks requieren un lenguaje adicional para poder aprovechar sus características al máximo.
- **El código completo de un componente puede colocarse en un solo archivo.** Vue nos permite agregar todo el código HTML, JavaScript y CSS

que conforman un componente, en un mismo archivo con extensión vue, lo que facilita la lectura y compresión del componente como tal.

- **El framework es modularizado.** Esta característica nos da una versatilidad impresionante conforme nuestro proyecto va creciendo, ya que nos permite integrar funcionalidades a nuestro proyecto, hasta que la necesitamos y todas estas características se encuentran divididas en una serie de librerías las cuales han sido diseñadas por el mismo equipo de desarrollo de Vue.
- **Soporta diseños para páginas webs complejas.** Actualmente Vue cuenta con su propia consola llamada vue-cli, la cual también incluye una interfaz gráfica. Esta herramienta está un poco más enfocada al desarrollo de aplicaciones avanzadas con Vue, gracias a la integración de las distintas librerías de este framework como vue-router, vuex o vue-server-rendering.
- **Existen herramientas que facilitan estilizar nuestros componentes.** Estas son de gran ayuda para quienes no dominamos CSS en su totalidad y nos apoyan a lograr diseños amigables y atractivos a la vista de los usuarios. Dentro de estas herramientas podemos destacar BootstrapVue y Vuetify las cuales podemos utilizar de forma gratuita y son un complemento que agilizarán un poco más nuestro desarrollo.
- **Permite la creación de SPA (Single Page Application).** Estas aplicaciones son construidas una única vez por el servidor y la interacción del usuario junto con el poder de Vue, permiten la renderización de los cambios de una manera sumamente rápida y solo cuando es necesario, haciendo que las peticiones al servidor sean de un tamaño menor y logrando aplicaciones mucho más rápidas que las tradicionales.

Seguramente existe un sinfín de características adicionales las cuales han hecho de Vue uno de los frameworks más populares y queridos por la comunidad en estos últimos años. Ha demostrado estar a la altura de los gigantes y en ciertos aspectos ha salido como ganador al comparar este framework con los demás. El objetivo de este artículo no es demostrar que el resto de frameworks son peores o malos “porque no lo son”, sin embargo, personalmente he encontrado en Vue la elegancia, potencia y sencillez, que me ha llevado a elegir este framework como mi favorito.

Si te encuentras interesado en el desarrollo web frontent te extiendo una cordial invitación, para que puedas conocer un poco más sobre esta magnífica herramienta y seguramente quedarás igual de impresionado que yo.

Conclusiones

- El desarrollo web en la actualidad es sumamente complejo y debemos dominar las tecnologías y herramientas que se utilizan para su construcción.
- Todos los frameworks son sin duda de gran ayuda, no existe ninguno mejor que otro.
- Puede hacerse una carrera muy completa en el desarrollo frontend con Vue.
- Debemos tener criterio personal para elegir las herramientas a utilizar en el desarrollo de cualquier proyecto.

Referencias

- [1] Garcia, E. (01 de abril 2019). Código Facilito: **¿Qué es Vue.js?**. Recuperado de: <https://bit.ly/2J9UlnT>. [Último acceso: 25 septiembre 2019].



Adaptándose a Scrum

José Amilcar Batz Itzol
amilbat@gmail.com

Estudiante de Ingeniería en Ciencias y Sistemas - USAC

Palabras Clave:

Red, automatización, Internet, Datos, Tecnología

Hoy en día hemos escuchado bastante sobre las metodologías Ágiles, sobre como ayuda a las empresas a hacer mejores entregas, pero realmente sabemos el costo o el impacto que tendrá adaptarse a una metodología Ágil, y qué método o estrategia utilizar para llevarlo a cabo. De este concepto nace lo siguiente en términos de experiencia e investigación.

Primero, ¿qué es Scrum? según la guía "su visión general lo define como un marco de trabajo por el cual las personas pueden abordar problemas complejos adaptativos, a la vez que entregan productos del máximo valor posible, productiva y creativamente [1]", entonces a partir de ello, ¿cuál es la definición de Scrum?, es un conjunto estandarizado de conceptos, prácticas y criterios para enfocar un tipo de problemática particular que sirve como referencia, para enfrentar y resolver nuevos problemas de índole similar.



Imagen 1: Logo Scrum

A partir de los conceptos mencionados arriba podemos agregar que Scrum es como un modelo de trabajo, donde la idea principal es seguir estándares para lograr un entregable funcional, ahora bien la pregunta es, ¿cuál es la mejor manera de adaptarse a Scrum?, en mi experiencia, estuve gestionando proyectos por 5 años de los cuales todos fueron manejados con metodologías tradicionales, la más conocida es el método Cascada, fueron buenos años, hasta que llegó el cambio, cambio que toda empresa que quieren seguir a la vanguardia tecnológica debe implementar, lo cual fue innovar con algo nuevo o migrar a nuevas tendencias, en nuestro caso fue la implementación de Scrum, al inicio lo vi como un "se ve interesante, pero no va a poder ser aplicado

por los tipos de proyectos que llevaba" me resistía al cambio, pero como no soy el dueño de la empresa, entonces tuve que hacerme a las políticas de la empresa, aprender y migrar a Ágil.

¿Qué paso en este proceso? pues lo que debe pasar en todo nuevo reto, lo primero fue que no deseaba cambiar, no le veía mucho futuro, pero por las disposiciones de la compañía, tuve que hacerme a la idea que debía adaptarme costaría lo que costara, mi primera experiencia fue tratar de hacer un mix de cascada y Scrum, algo totalmente mal, pero era yo vs el cambio, como era lo esperado no funcionó, y como dice la guía de Scrum o "lo aplicamos todo o no es Scrum[2]". El proceso de adaptación en los primeros meses fue difícil ya que no era el único que se resistía al cambio.

Los Daily inicialmente era difíciles de realizar, no todos sabíamos cuál era el propósito, se decidió iniciar con capacitaciones brindados por personal certificado a los desarrolladores, con el objetivo de iniciar y crear una célula inmadura hasta llegar y evolucionar a una célula madura, pero que tenía ciertas implicaciones llegar a esta adaptación, primero iniciar con la autodidacta de investigar, leer y empaparse del tema, seguido de los talleres o capacitaciones que se obtuvieron de parte de la empresa para poder implementar bien este marco de trabajo, el segundo paso fué utilizar el Framework de Scrum y aplicarlo, y ¿cuál fue el resultado de aplicarlo en los primeros Sprint?, como era de esperarse, al no ser una célula madura y no tener la experiencia caímos en los errores básicos, al no dar seguimiento a lo hablado en los Daily, otro problema que encontramos en la adaptación fue que al ser un equipo de desarrollo de casi 50 desarrolladores realizar un sprint planning con este equipo era complicado escuchar a todos, algo que no era funcional tanto a la empresa como al equipo, esto fue algo que se tuvo que cambiar, se platicó

y se revisó quienes tenían más conocimiento en Scrum y el negocio, para crear células con equipos más pequeños, y crear diferentes backlog's y no perder tiempo en los sprint planning. Como lo indicaba anteriormente, solamente haciendo el uso del Framework de Scrum se puede pasar de ser una célula inmadura a madura, ya que acá es donde se identifican los problemas como tal y si realmente se está siguiendo los manifiestos de Scrum.

SCRUM FRAMEWORK

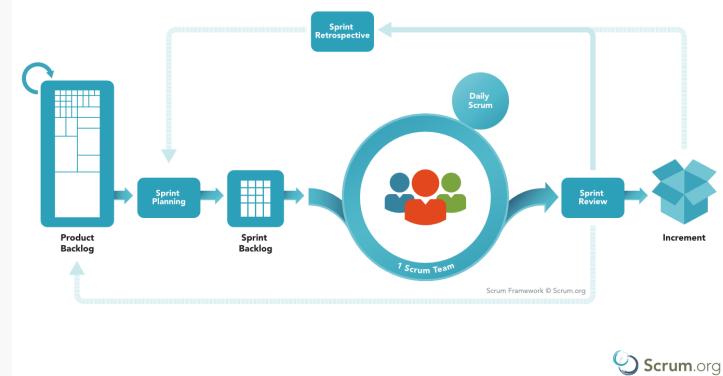


Imagen 2: Scrum Framework

Entonces, ¿es difícil adaptarse? “NO” ¿que se necesita? lo primero es leer e investigar, aprender los conceptos, recibir talleres si fuera posible certificarse. Con una persona que esté certificada en una célula,

esta puede hacer que la célula pueda madurar a tal punto que los resultados serán más que obvios en la finalización de cada sprint.

Conclusiones

- Scrum recomienda transparencia en todos sus procesos, por difícil que sea se necesita que todos los integrantes puedan hablar sobre posibles bloqueos o inconvenientes que puedan salir de imprevistos durante el sprint, esto para realizar leves ajustes [1] para tener un buen entregable al final del sprint.
- Scrum al ser Ágil ayuda a tener claro el futuro de una aplicación al realizar entregables funcionales seguidos.
- Certificarse en Scrum hoy en día es un gran plus para cualquier empresa.

Referencias

- [1] [2] Sutherland, J. Schwaber, K. Scrum Guides: The Scrum Guides. Recuperado de: <https://www.scrumguides.org/>. [Último acceso: 08 octubre 2019].

USAC FORTALECIENDO LA TRANSPARENCIA

<https://siges.minfin.gob.gt/>



MINISTERIO DE
FINANZAS PÚBLICAS





Docker y Herramientas de Orquestación

Ricardo Antonio Cutz Hernández

ricardcutzh@gmail.com

Estudiante de Ingeniería en Ciencias y Sistemas - USAC

Palabras Clave:

Docker, Devops, Cloud, Microservicios, Desarrollo, Programación, Orquestadores.

En la actualidad en el contexto de desarrollo de aplicaciones, Docker es una herramienta que se utiliza por las ventajas que ofrece y la variedad de herramientas que se pueden utilizar para el despliegue y orquestación de contenedores. El uso de contenedores se ha convertido en una práctica común en los equipos de trabajo porque permiten un ambiente uniforme en las diferentes etapas de desarrollo, pruebas y despliegue de servicios. Uno de los problemas frecuentes a los que un desarrollador se enfrenta son las dependencias y librerías utilizadas para el despliegue de una aplicación, esto incluyendo el sistema operativo y el ambiente de desarrollo que se ha preparado para un proyecto en curso, aquí es donde Docker entra en contexto como una solución viable. Para poder entender la importancia que Docker tiene se debe de responder a la pregunta: ¿Qué es Docker?

Docker es una plataforma de contenerización que permite empaquetar una aplicación junto con sus dependencias que asegura que la aplicación funcione en cualquier ambiente. En el contexto de transporte de mercancías en barcos, un contenedor es una unidad estándar para realizar esta tarea, esta misma idea aplica para los contenedores de Docker convirtiéndose en una medida estándar para empaquetar una aplicación.

La utilización de Docker ha crecido durante los últimos años y el manejo de contenedores se ha popularizado, la necesidad de poder administrar estos mismos ha incrementado, por ello existen diferentes herramientas llamadas "orquestadores de contenedores" que han surgido para suplir esta necesidad. Una herramienta de orquestación de contenedores tiene como propósito el manejo del ciclo de vida de los contenedores, principalmente en ambientes de producción dinámicos, son utilizados para el manejo de diferentes tareas.

Por ejemplo:

- Monitorear la salud de los contenedores activos
- Provisionar redundancia
- Provisionar alta disponibilidad
- Balanceo de carga y descubrimiento de servicios
- Repartición de recursos y otras tareas

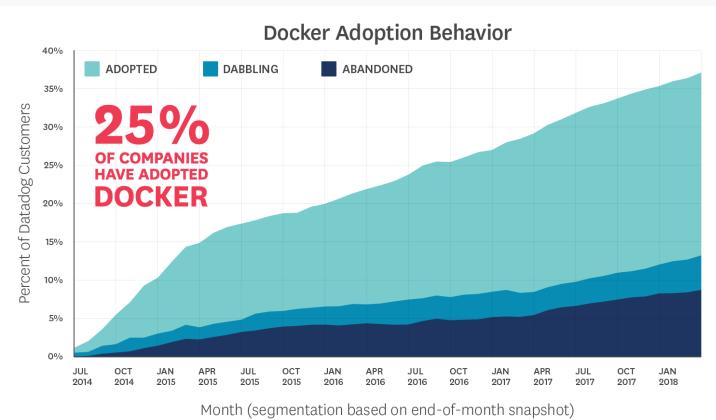


Imagen 1: Estadísticas de Adopción de Docker

El utilizar una herramienta de orquestación implica que la configuración del ambiente de despliegue se describe en uno o varios archivos de configuración, estas configuraciones incluyen las imágenes de los contenedores a utilizar, volúmenes de almacenamiento, conexión de red entre los diferentes servicios entre otras configuraciones. El poder utilizar este tipo de archivos (YML o JSON) permite que se pueda llevar un control de las versiones de las configuraciones y controlar el despliegue en diferentes ambientes, puede ser un ambiente de pruebas o un ambiente de producción, esto debido a que todo se maneja como código. La herramienta permite desplegar los contenedores en clústers, manejar los recursos necesarios para cada uno de los servicios y agregar o quitar contenedores de ser necesario. Actualmente existen diferentes herramientas disponibles para lograr todo

lo anteriormente mencionado, a continuación, se mencionan algunas de ellas.

Kubernetes

Es una herramienta de código abierto bastante popular para la orquestación de contenedores, permite desplegar y manejar aplicaciones que están conformadas por múltiples contenedores, ayuda a administrar la aplicación contenerizada de diferentes tipos, física, virtual y ambientes de nube [1]. Kubernetes es usualmente utilizada con Docker, pero puede trabajar con cualquier sistema de contenedores que se apegue a los estándares de imágenes de contenedores. Sus beneficios son los siguientes:

- Correr en nubes privadas y públicas (Google Cloud, Azure, AWS, etc.)
- Asegurar que los contenedores corren en todo momento y ayuda a administrar los recursos.
- Permitir que las aplicaciones contenerizadas puedan ser liberadas y actualizadas sin tiempo de caída.

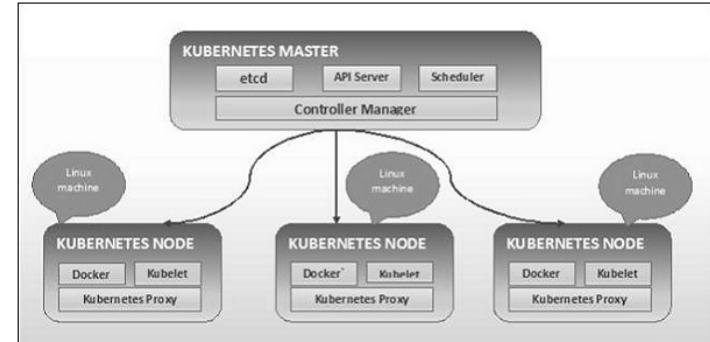


Imagen 2: Arquitectura de Kubernetes

Docker Swarm

Es la herramienta de orquestación de contenedores en clústeres que proporciona Docker, permite desplegar y orquestar contenedores en número grande de anfitriones que corren el motor de Docker. Se hace referencia a esta herramienta que proporciona Docker como el modo Swarm. Esta herramienta es importante mencionarla por la relevancia que tiene Docker, aunque cabe mencionar que no es muy utilizada, ya que existen otros tipos de orquestadores que permiten mayor funcionalidad y compatibilidad con contenedores que no son de

Docker. Docker Swarm permite:

- Escalar, declarando tareas que pueden correr para cada servicio a desplegar
- Manejar la red de los servicios que se despliegan.
- Descubrimiento de servicios
- Balanceo de carga.

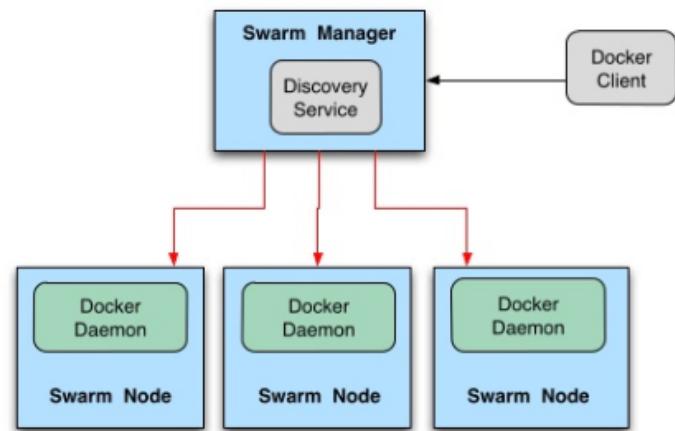


Imagen 3: Arquitectura de Docker Swarm

AWS ECS

Llamada "Amazon Elastic Container Service"[3], una herramienta para el manejo de contenedores altamente escalable y rápida, es provista por Amazon para correr contenedores en clúster de máquinas virtuales (Amazon EC2) que tienen el motor de Docker preinstalado. ECS maneja la instalación, monitoreo y el control de las instancias del clúster por medio de la API de AWS o de la consola de manejo. La idea de esta herramienta es ver el clúster de EC2 como una fuente de recursos de CPU y memoria, permite también que se interactúe con los demás servicios de AWS como Cloudwatch configurando alarmas, permitiendo así escalar cuando sea necesario. Dentro de los conceptos que se manejan en el servicio de ECS podemos mencionar:

- Task: es una definición de las propiedades de un contenedor, como por ejemplo la imagen a utilizar, la cantidad de CPU y memoria que puede utilizar, el ambiente y los puertos.
- Service: Es la definición del máximo o mínimo de "tasks" que pueden correr.

Es importante mencionar es que ECS puede trabajar con EC2 (Servicio de instancias de AWS) o con Fargate, siendo esta última un motor que permite que se ejecuten contenedores sin servidores, lo cual elimina la necesidad de velar por la plataforma en donde se ejecutan los contenedores, prácticamente permite enfocarse directa y solamente en el manejo de contenedores.

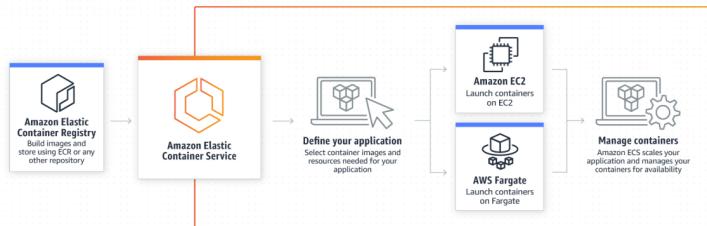


Imagen 4: Como trabaja ECS

Conclusiones

- Docker es una herramienta de contenedores que se ha vuelto tendencia en el medio de desarrollo de aplicaciones
- Las herramientas de orquestación permiten manejar y gestionar los contenedores y recursos en aplicaciones y servicios
- Dependiendo de la plataforma de contenedores que se utiliza existen herramientas de orquestación que ofrecen o no compatibilidad.

- Las herramientas de orquestación están enfocadas a manejar escalabilidad y monitoreo de los contenedores que conforman una aplicación.

Referencias

- [1] Yegulalp, S. (03 de abril 2019). InfoWorld: What is Kubernetes? Your next application platform. Recuperado de: <https://bit.ly/2WwHPqt>. [Último acceso: 3 de septiembre de 2019].
- [2] Campus MVP. (07 de agosto 2018). Campus MVP: Las 10 herramientas más importantes para la orquestación de Contenedores en Docker. Recuperado de: <https://bit.ly/2J5vBgM>. [Último acceso: 3 de septiembre de 2019].
- [3] Amazon Web Services. (03 de diciembre 2019). AWS Amazon: AmazDocker Docs: Swarm mode overview. Recuperado de: <https://dockr.ly/2wrG9E3>. [Último acceso: 03 julio 2019].
- [4] Docker. (20 de junio 2016). on Elastic Container Service:. Recuperado de: <https://aws.amazon.com/ecs/>. [Último acceso: 03 julio 2019].
- [5] Kubernetes. (10 de octubre 2019). Kubernetes: ¿Qué es Kubernetes?. Recuperado de: <https://bit.ly/2QAax63>. [Último acceso: 03 julio 2019].





Ruta de aprendizaje, para ser un mejor profesional

Carlos Gabriel Peralta Cambrán
carlospecam@gmail.com

Estudiante de Ingeniería en Ciencias y Sistemas - USAC

Palabras Clave:

Tecnología, desarrollo, cloud, herramientas, servicios, containers, kubernetes, infraestructura, certificación

¿La universidad te enseña lo necesario? Esta es una pregunta sencilla que cualquier persona se hace, pero ¿Cuál es la respuesta? Es necesario adentrarnos un poco a nivel de grados académicos. Desde el inicio de nuestra educación superior, hemos sido inculcados, por nuestros padres, que al tener un título universitario podremos ser mejores profesionales. Pero, al obtener la tan anhelada titulación académica, descubrimos que no tenemos el conocimiento necesario de las herramientas, tendencias, tecnologías y disciplinas que el entorno laboral requiere de nosotros.

¿Te sientes identificado? ¿Deseas ser mejor profesional? ¿Leíste lo anterior con voz de anuncio comercial? Probablemente no seas la única persona con estos sentimientos. Ahora bien, volviendo a nuestra pregunta inicial. La formación profesional es responsabilidad de cada uno, la universidad te instruye en conocimientos básicos e intermedios de los saberes procedimentales y actitudinales que necesitas. Sin embargo, el conocimiento no se detiene, la tecnología avanza a pasos agigantados, el futuro es hoy, no en el año 2045. Por esta razón, es necesario dedicarle tiempo e inversión económica a la persona más importante, tú mismo

Tecnologías de mayor tendencia a nivel global
En el ámbito empresarial, relacionado con la ingeniería en sistemas y operaciones, han surgido varias tendencias a las cuales se les ha puesto un mayor interés.

- AIOps:** Inteligencia Artificial para Operaciones de TI, consisten en automatizar y mejorar las operaciones de TI, mediante el uso de análisis y aprendizaje automático para analizar grandes volúmenes de datos recopilados de diversas herramientas y dispositivos de operaciones de TI, con el fin de detectar y reaccionar automáticamente a problemas en tiempo real.[1]

• Serverless: es un modelo de ejecución en el que el proveedor en la nube (AWS, Azure o Google Cloud) es responsable de ejecutar un fragmento de código mediante la asignación dinámica de los recursos.[2]

• Cloud-native infrastructure: Las tecnologías “nativas en la nube” aprovechan la nube para crear y ejecutar aplicaciones. Estas tecnologías se caracterizan por el uso de contenedores, microservicios, funciones sin servidor, carteras de desarrollo e infraestructura basada en código.[3]

• Kubernetes: Es una plataforma, portátil, extensible, open-source para el manejo de cargas de trabajo contenerizadas y servicios. La cual facilita la configuración, despliegue y automatización.[4]

• Containers: Ofrecen un modo estándar de empaquetar el código, las configuraciones y las dependencias de su aplicación en un único objeto.[5]

¿Identificas algunas de las tecnologías de tendencia mundial? Probablemente tengas la noción de una o de varias. Sin duda alguna, es sorprendente el vasto camino de conocimiento que hay por adquirir. Para ti, una persona apasionada por la informática, la programación, la solución de problemas y sobre todo el pensamiento lógico es de suma importancia que fijes un rumbo y decidas en que deseas ahondar para realizarte como profesional.

Tener las habilidades correctas en un nivel alto, es pieza fundamental para adquirir un trabajo en el sector tecnológico. Los saberes conceptuales deben ir de la mano con las habilidades prácticas. Es decir, yo no puedo llegar a una finca canadiense a cultivar y cosechar coliflor si nunca en mi vida he aprendido sobre hortalizas, mucho menos si no he trabajado en el campo.

De forma homologa, en el ámbito tecnológico, si nunca me he documentado y trabajado con un lenguaje de programación o una tecnología no sabré la manera correcta de hacerlo.

Entonces... ¿Qué debo saber? La respuesta no es tan sencilla, si bien es cierto las tendencias indican por donde se está dirigiendo el mercado laboral. El pilar más importante, en el ámbito informático, es tener conceptos de ciencias de la computación, algoritmos, estructuras de datos. Además de conocer varios lenguajes de programación, aplicar correctamente unit testing y experiencia de usuario. Pero... ¡Eso es lo que me enseñan en la universidad! efectivamente. Que se encuentre dentro del pensum de estudios, no garantiza que tu adquieras por completo estos conocimientos y habilidades al cien por ciento.

El gigante de internet, por supuesto Google, sugiere una ruta de aprendizaje [6], no importa si eres un profesional, estudiante, apasionado por la informática o un experto programador. Sin duda, será de utilidad para incrementar tus conocimientos y reafirmar algunos que perdemos con el transcurrir del tiempo.

1. Foundations of Programming, consiste en reforzar habilidades de ingeniería de software.
2. Advanced Programming, consiste en afinar habilidades y el uso de herramientas para programadores experimentados.
3. Machine Learning, consiste en masterizar las habilidades con machine learning.
4. Cloud Computing, consiste en construir tus habilidades con todo lo relacionado a conceptos en la nube.

Si puedes observar, cada uno de los ítems enumerados corresponden a los conocimientos básicos de cada una de las tendencias tecnológicas a nivel mundial. Es de suma importancia construir tu conocimiento, adquirir todo lo bueno que proporciona internet e invertir en conocimiento. Porque el conocimiento te hará un mejor profesional, te dará la capacidad de considerar múltiples escenarios para solucionar un problema y lo más importante serás capaz de demostrar a ti que necesitas aprender continuamente.



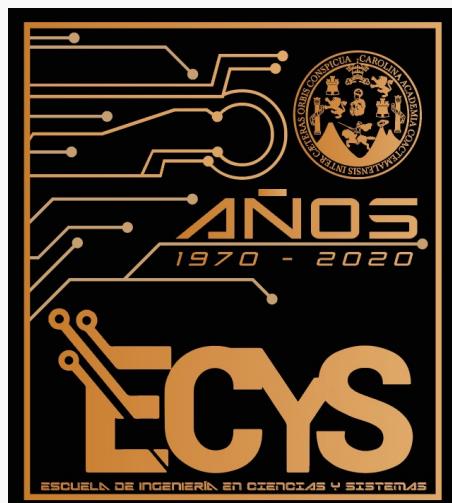
Imagen 1: Deep Learning Networks Can't Generalize – But they are learning from the brain

Conclusiones

- En la actualidad debe mantenerse un perfil competitivo tanto técnico como individual, las habilidades blandas como toda habilidad, requieren práctica por lo que es importante involucrarse en grupos sociales, decir '**Sí**' a nuevas oportunidades y si no estamos preparados completamente, ser capaces de adaptarse fácilmente, aunque la adaptación a ambientes y personas desconocidas pueda ser a veces complicado, es más fácil adaptarse si como individuo se trabaja por tener una actitud abierta y pasión por crecer.
- Las habilidades blandas y duras no son mutuamente excluyentes, de hecho, el trabajar en una puede automáticamente repercutir positivamente sobre la otra. Por ejemplo, si hay dedicación hacia cierta área de trabajo y se tiene conocimiento sobre ella, esto aumenta la seguridad y la autoconfianza o bien, si se mantiene un hábito de lectura sobre cualquier tema, esto puede mejorar la capacidad comunicativa y al mismo tiempo, aumentar el conocimiento.

Referencias

- [1] **Desconocido.** (30 de noviembre 2017). Insitech: ¿Qué es AIOps?. Recuperado de: <https://bit.ly/2WwHPqt>. [Último acceso: 11 de octubre de 2019].
- [2] **Desconocido.** (30 de diciembre 2018). Serverless Stack: ¿Qué es serverless?. Recuperado de: <https://bit.ly/3dleZPM>. [Último acceso: 11 de octubre de 2019].
- [3] **Desconocido.** (26 de abril 2017). Oracle Cloud Platform: ¿Qué significa “nativo en la nube”??. Recuperado de: <https://bit.ly/33BDbt5>. [Último acceso: 11 de octubre de 2019].
- [4] **Desconocido.** (25 de febrero 2019). Kubernetes: What is kubernetes?. Recuperado de: <https://bit.ly/2J6CyOK>. [Último acceso: 11 de octubre de 2019].
- [5] **Desconocido.** (16 de noviembre de 2018). Amazon Web Services: ¿Qué es un contenedor?. Recuperado de: <https://go.aws/2J3ytKX>. [Último acceso: 11 de octubre de 2019].
- [6] Desconocido. (24 de agosto 2017). Tech Dev Guide: Grow Your Technical Skills with Google. Recuperado de: <https://techdevguide.withgoogle.com/>. [Último acceso: 11 de octubre de 2019].



**USAC FORTALECIENDO LA
TRANSPARENCIA**

<https://siges.minfin.gob.gt/>





Firma electrónica avanzada, el futuro de la autenticidad de documentos

David Alejandro Asencio Sagastume
dasensag@gmail.com

Estudiante de Ingeniería en Ciencias y Sistemas - USAC

Palabras Clave:
Criptografía, tecnología, encriptación, servicios, gobierno.

Entorno de la firma electrónica avanzada en Guatemala

En el día a día, para realizar cualquier tipo de operación, se requiere la verificación de la identidad de las personas, principalmente en procesos legales o bancarios. Por lo general, estos procesos implican la presencia de la persona como tal y que esta, presente su documento de identificación. Dependiendo del proceso, se generan documentos que avalan la transacción y son firmados por las partes involucradas para asegurar la autenticidad del documento, toda esta logística consume el tiempo de las partes involucradas, principalmente porque se requiere que se presenten físicamente en un mismo lugar a realizar la firma.

Gracias al reconocimiento de la firma electrónica avanzada por parte del gobierno, como una forma de autentificación legal, las instituciones bancarias y los procesos legales empezaron a utilizar y aceptar su uso [1], disminuyendo enormemente los tiempos que se requieren para realizar este tipo de procesos.



Imagen 1: 5B Digital Summit 2018, panel sobre la firma digital y su aprobación por parte de las instituciones bancarias

¿Qué es la firma electrónica avanzada?

Lo primero es entender a que nos referimos con una firma electrónica avanzada, al escuchar este término podemos pensar que se habla de la firma manuscrita que se realiza comúnmente, que ha sido digitalizada y colocada en un documento digital. Sin embargo, esto no es a lo que se refiere como firma electrónica avanzada, esta se refiere a la generación de un certificado único, que representa a una persona individual, jurídica o una institución [2]. Este certificado garantiza la autenticidad de las personas que firmaron el documento y por lo tanto la autenticidad del documento en cuestión.

La tecnología y funcionamiento detrás de la firma electrónica avanzada no es algo nuevo, es algo que existe desde hace varios años y es utilizado, de cierta forma, en el día a día. Utiliza la encriptación asimétrica, también conocida como Infraestructura de Llave Pública (PKI por sus siglas en inglés).

Se basa en el uso de algoritmos matemáticos para generar una serie de números, a los cuales se les denomina "llave". Se requiere de dos llaves, una pública y una privada. La llave privada debe ser resguardada y solo el dueño debe tener acceso a esta, mientras que la llave pública, como su nombre lo indica, debe ser pública y ser accesible para todo el mundo.

El flujo de la encriptación asimétrica es el siguiente: cuando una persona firma un documento, por medio de un algoritmo se genera un hash, luego este es encriptado por la llave privada. El hash encriptado es utilizado como firma y se adjunta al documento, incluyendo la fecha en la que se agregó la firma. Si el documento cambia después de la fecha en que se firmó, la firma queda invalidada.

El documento viaja a través de la red, cuando alguien recibe el documento ocurren dos operaciones.

Se utiliza el mismo algoritmo para generar el hash del documento recibido, y se utiliza la llave pública para desencriptar y generar otro hash. Se comparan los valores hash y si ambos son iguales quiere decir que la firma es válida. En caso de que no sean iguales en la comparación, o la llave pública no sea capaz de desencriptar la firma, quiere decir que la firma no pertenece a la persona que envió el documento, o este fue modificada en el camino.[3]

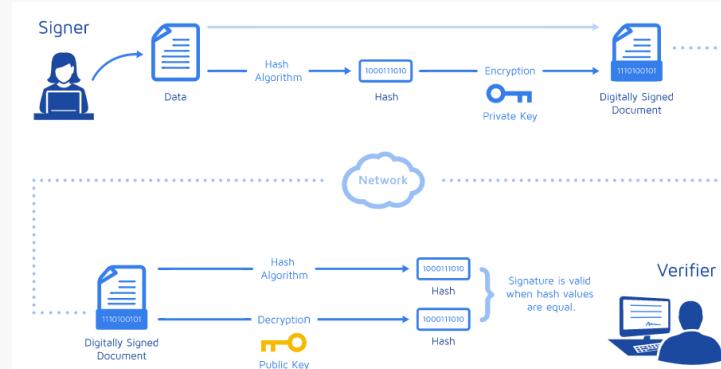


Imagen 2: Flujo de funcionamiento de la encriptación asimétrica

La firma electrónica avanzada comparte los tres atributos clave de la encriptación asimétrica [4], que hacen que este proceso sea totalmente transparente para su uso legal.

- **Autenticidad:** Garantiza la identidad de la persona que envía el documento, al ser firmado con la llave privada de esa persona se puede tener la seguridad de que la persona es quien dice ser.
- **Integridad:** Garantiza que los datos del documento no fueron alterados, ya que hacerlo deja sin validez la firma.
- **No repudio:** Quien envía el documento no puede negar el conocimiento de los datos y los compromisos adquiridos con este. Debido a que el documento fue firmado con su llave privada, la cual es única para esa persona.

Como todo proceso tecnológico existen riesgos en su uso, los cuales radican en una mala administración de la pareja de llaves, si no se resguarda cuidadosamente la llave privada, puede generar suplantación de identidad por parte de un tercero, al utilizar la llave privada sin el consentimiento del dueño. Para garantizar la integridad de este flujo, la pareja de llaves debe ser

creada, distribuida y almacenada de forma segura, para esto existen múltiples proveedores certificados a nivel nacional e internacional que se encargan de realizar esta tarea.

¿Por qué es tan importante? Como se mencionó anteriormente, el flujo de la encriptación asimétrica es algo que utilizamos de cierto modo todos los días. Ya que el mismo concepto se utiliza para generar los certificados que utilizan las páginas web para mantener seguro el transporte de datos. Si esto es algo tan común entonces ¿por qué es tan importante la firma electrónica digital?

La razón radica en las tendencias actuales, la firma electrónica avanzada existe desde hace varios años, pero está tomando fuerza actualmente en Guatemala debido a dos factores. El primero es debido a la tendencia de disminuir el uso del papel. Y el segundo es que el gobierno reconoce su uso legalmente. En otros países se busca impulsar un gobierno y comercio electrónico, Guatemala ahora se une a esta causa.[5]

¿Cómo nos afecta? La transición al uso de la firma electrónica digital es algo que afecta a todas las personas para bien, debido a que, muchos de los procesos como se conocen actualmente irán cambiando con el paso del tiempo. Ya no será necesario que las personas asistan a un banco a firmar una solicitud de crédito, ya que, pueden enviar el documento firmado electrónicamente, disminuyendo así los tiempos en el traslado al banco y la espera para ser atendido.

Actualmente varias instituciones se han empezado a adaptar al uso de la firma electrónica avanzada, la SAT, por ejemplo, redujo los tiempos para los trámites de títulos de propiedad de los vehículos al firmarlos electrónicamente. La SAT también empezó a impulsar el uso de facturas electrónicas, dando fechas límites para los diferentes grupos de empresas para abandonar el uso del papel.

Con el paso del tiempo surgirán más procesos que se adapten, disminuyendo el tiempo que requieren para ser completados, pero los tiempos no es lo único que se verá afectado por el uso de la firma electrónica. Su uso abre las puertas a múltiples oportunidades de negocio, empresas como GuateFacturas vieron la fuerza que tomaba el uso de facturas electrónicas en

otros países y decidieron empezar desde hace años con sus operaciones, ganando terreno en el mercado actual para el manejo de facturación electrónica.

Como adquirir una firma electrónica

La llave privada es un archivo con extensión PFX, CRT o PEM o similar y puede ser manejado en dos modalidades. Por medio de un token físico, como una USB, siendo este el modo menos seguro. O por medio de un API (Application Programming Interface) o un HSM (Hardware Security Module), conectándose a estos para solicitar la firma, reduciendo el riesgo de robo de la llave privada.

Para conseguir una firma se puede solicitar a distintos proveedores, en Guatemala se reconocen los certificados de firma electrónica emitidos por 5B, la Cámara de comercio o Infile. [6] Cualquier persona individual, jurídica o empresa puede solicitar su firma electrónica a una de estas tres entidades y empezarla a utilizar, ya que es totalmente reconocida por la ley.

Conclusiones

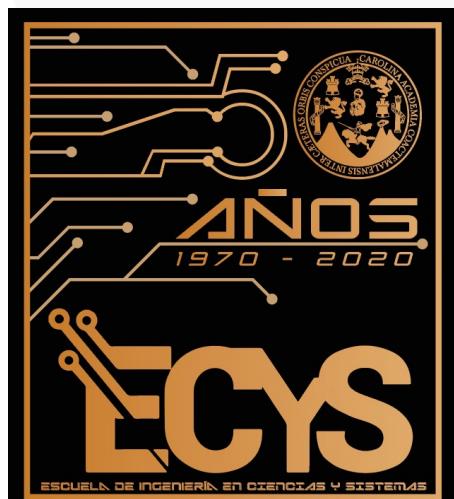
- Con el paso del tiempo la firma electrónica digital avanzada se convertirá en el único medio reconocido por las instituciones, por lo que es importante adaptarse al cambio.
- El uso de la firma electrónica abre las puertas a una variedad de oportunidades de negocio, si se aprovechan se puede ganar terreno en nuevos

mercados.

- Al optar por el uso de una firma electrónica se debe manejar con alta seguridad, ya que, al descuidar la llave privada se puede sufrir de suplantación de identidad y puede generar una gran variedad de problemas legales.

Referencias

- [1] Alvarado, V. (24 de agosto 2018). El Siglo: Bancos de Guatemala implementarán la firma electrónica. Recuperado de <https://bit.ly/2wtD4Ds>. [Último acceso: 3 de octubre de 2019].
- [2] [6] Desconocido. (06 de septiembre 2019). Firma-e: Firma Electrónica Avanzada. Recuperado de https://www.firma-e.com.gt/?page_id=1647 .[Último acceso: 3 de octubre de 2019].
- [3] Desconocido. (20 de octubre 2015) DocuSign: Understanding digital signatures. Recuperado de <https://bit.ly/2WuT8zs>. [Último acceso: 3 de octubre de 2019].
- [4] De Luz, S. (16 de noviembre 2010). RedesZone: Criptografía: Algoritmos de cifrado de clave asimétrica. Recuperado de <https://bit.ly/2Wz2biP>. [Último acceso: 3 de octubre de 2019].
- [5] Jiguan, B.. (24 de agosto 2018). Diario de Centro América: Firma avanzada se expandirá a bancos. Recuperado de <https://bit.ly/2J6s7KO>. [Último acceso: 3 de octubre de 2019].





Introducción a Hyperledger Composer

Fernando Antonio Hernández Gramajo

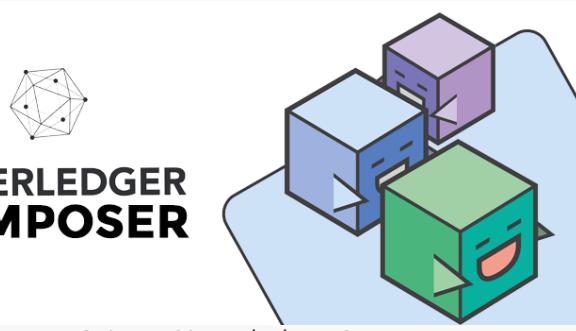
hernandezfernando18982012@gmail.com

transacciones, almacenamiento, desarrollo, consenso, herramientas

Palabras Clave:

Procrastinar, aplazar, posponer, holgazanería.

Como conocimiento previo, blockchain como tal, es una red de miembros donde cada uno de ellos tiene la misma base de datos en sus máquinas o misma cadena de bloques (distribuido), en contraste con un entorno centralizado en el cual todos son clientes los cuales se conectan a un único servidor donde aquí si se encuentra la base de datos. También cabe resaltar que no es una base de datos normal, este tipo de almacenamiento tiene una característica muy importante y es que es immutable [1], lo que significa que no puede modificar el registro que ya se ha guardado en él. Solo puede agregarlo o leer entradas, pero no las puede actualizar. Teniendo en claro que blockchain es una manera de almacenar y procesar criptomonedas, hay que separar los términos los cuales se van a tratar, dado que hyperledger no es otra criptomoneda más, sino una tecnología de software libre que nos ayuda a desarrollar aplicaciones de este tipo con la ayuda de estándares, lineamientos y protocolos los cuales ya se establecen en blockchain tradicional, pero acá se trasladan a servicios y consensos los cuales se tienen que cumplir para que el blockchain que desarrollemos en esta herramienta sea tan bueno como si fuera hecha en otras más conocidas. (Imagen 1).



**HYPERLEDGER
COMPOSER**

Imagen 1: Logo Hyperledger Composer

Ahora sí, ¿qué es hyperledger composer?, como tal hyperledger compone una colección de varias herramientas de desarrollo en la cual se encuentra composer, el gran propósito y meta de este

software es tener disponible una plataforma la cual desarrolle blockchain listas para ser implementadas en ambientes de producción de grandes empresas formando así una comunidad de desarrollo de blockchain unido y comprometido a seguir mejorando este software dado que es código abierto muchas más empresas se suman a este proyecto con el pasar del tiempo.

Con hyperledger composer se necesitan tener 4 aspectos claros para el desarrollo de blockchain, los cuales son:

- **Participantes:** Son las personas o entidades las cuales va a participar en la red de nodos se acostumbra a que si hay una característica por pequeña que sea se agregue otro tipo de participante para contemplar todas las posibilidades que se pueden dar en este apartado.
- **Modelos:** Son en sí las transacciones las cuales manejan los nodos para conformar un bloque en blockchain, se acostumbra que contengan un participante origen, un participante destino y el bien o servicio el cual se va a intercambiar, la fecha y hora bien puedo o no ir en este tipo de objetos, pero queda a discreción de quien está diseñando esta red el incluirlo o no.
- **Lógica de Negocio:** son las acciones para llevar a cabo las transacciones, estas son escritas en un lenguaje propio de hyperledger composer pero se asocian a promesas asíncronas en javascript, dado a varias similitudes entre ambas sintaxis.
- **Reglas de Acceso:** Si bien las reglas de acceso solo dicen quién puede interactuar con ciertos participantes y quien no, es aquí donde se origina la petición de un participante a otro, en donde por un lado se tiene el paquete a enviar y que es lo que se espera como respuesta (Imagen 2).

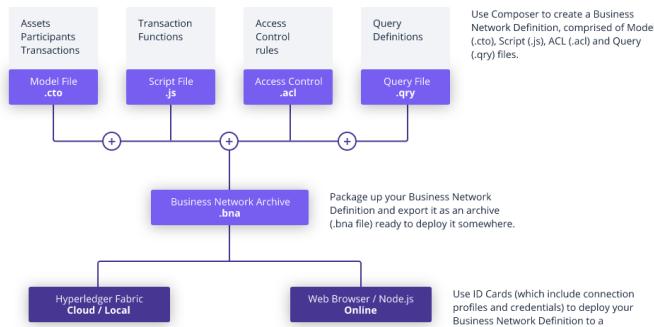
Conclusiones

- Las redes de nodos generadas con la herramienta hyperledger composer pueden servir para testeos rápidos los cuales agilizan la toma de decisiones.
- La aplicación de redes de nodos no solo se limita a criptomonedas, sino que va más allá que cualquier objeto o servicio puede llegar a ser una transacción almacenable dando así un alto nivel de abstracción a nuestros blockchain.
- El software libre ha hecho mucho por las comunidades de desarrolladores durante mucho tiempo y este es un claro ejemplo de cuando se tienen una buena idea en mente puede llegar convertirse en verdaderos mega proyectos [4].

Imagen 2: Componentes de diseño para una red de nodos.

Luego de definir todos estos componentes, queda generar la red de nodos, por lo cual hyperledger se apoya en uno de sus lenguajes disponibles y compatibles con la herramienta composer como lo es Angular en su versión 5, dado a su alta demanda generar aplicaciones provenientes de node js es muy sencillo montar un ambiente de pruebas para verificar si todo se encuentra funcionando como debe y luego enviar al ambiente de producción, todo en cuestión de minutos se cuenta con un equipo de desarrollo ágil, ahora los temas de seguridad y cuestiones de compatibilidad pasan a ser desplazados a un segundo plano ya que la herramienta genera todo desde cero.

También cabe mencionar que composer cuenta con un ambiente de pruebas en línea, el cual lleva por nombre: hyperledger composer playground,[2]: en donde en cuestión de minutos y unas cuantas configuraciones podemos probar como funcionarían blockchains desde las más sencillas hasta las más elaboradas transacciones, por lo que se considera también como una herramienta muy completa para propósitos de prueba. Esta es solo una alternativa de muchas existentes pero que da mucha facilidad a su desarrollo[3] y así este tipo de generadores de blockchain se convierte en uno de los más completos y rápidos hasta el día hoy.



Referencias

- [1] Krzywiec, W. (14 de junio 2019). Medium: Your first blockchain in a matter of minutes using Hyperledger Composer. [En línea]. Disponible en: <https://bit.ly/3a7ZBVf>. [Último acceso: 01 de octubre de 2019].
- [2] Hyperledger composer community. (01 de septiembre 2017). Hyperledger: Welcome to Hyperledger Composer. [En línea]. Disponible en: <https://bit.ly/2y06p9j>. [Último acceso: 30 de septiembre de 2019].
- [3] Rodriguez, N. (19 de marzo de 2019). 101blockchains: Hyperledger: La Blockchain Empresarial. [En línea]. Disponible en: <https://bit.ly/2J6vG3P>. [Último acceso: 30 de septiembre de 2019].
- [4] Aprendeblockchain. (12 de mayo 2018). Aprendeblockchain: Hyperledger. [En línea]. Disponible en: <https://bit.ly/3dhCERb>. [Último acceso: 30 de septiembre de 2019].



Analista de Datos

Glen Abra-ham Calel Robledo

g13ncal3l@gmail.com

Estudiante de Ingeniería en Ciencias y Sistemas - USAC

Palabras Clave:

Dato, información, analista, R, Datacamp.

¿Cuál es la diferencia entre dato e información?

Como es de costumbre, en algún momento de la carrera nos han preguntado si existe la diferencia entre dato e información, probablemente al inicio de la carrera no hemos determinado la diferencia entre estos dos conceptos tan distintos e importantes. Dato se define como "Cifra, letra o palabra que se suministra a la computadora como entrada y la máquina almacena en un determinado formato" [1] en otras palabras un dato es un conjunto de caracteres almacenados. Información se define como "el conjunto de datos organizados y procesados que constituyen mensajes, instrucciones, operaciones, funciones y cualquier tipo de actividad que tenga lugar en relación con un ordenador" [2] en otras palabras es un conjunto de datos que tienen un sentido o un significado.

Luego de esta breve introducción como cultura general "en 1963, se introdujo el término base de datos en un simposio llamado Development and Management of a Computer-Centered Data Base" [3] si analizamos las definiciones previas, ¿Por qué se llaman bases de datos y no bases de información? Si el lector tiene la oportunidad de leer el libro Modelos de Bases de Datos del ingeniero Luis Espino, en el capítulo 2 encontraran la respuesta.

¿Qué significa analista de datos? Al entender la diferencia entre un dato e información se puede abarcar el tema principal, el cual consiste en definir qué significa un analista de datos. El término fue creado por William Cleveland, él definió un analista de datos como una persona que tiene un título de ingeniería de software o ingeniería en sistemas, que tiene como objetivo principal programar software para el análisis de datos. Puede sonar algo redundante el nombre con relación a su término, pero si le damos mayor profundidad al término hoy en día se le conoce como el profesional

que "se encarga de recolectar, procesar y ejecutar análisis estadísticos de datos" [4]. Cabe destacar otra definición que identifica a un analista de datos el encargado de participar en la recopilación de datos, que además estructuran bases de datos, creando y ejecutando modelos para realizar el análisis y determinar patrones en los datos que hayan obtenido, con el fin de presentar resultados para la toma de decisiones.

Esta profesión nace debido a la cantidad enorme de datos que se procesan diariamente en cualquier tipo de ámbito, podemos hacer mención de los siguientes casos: la cantidad de nacimientos o decesos que se dan en un determinado tiempo, o la cantidad de carros que ingresan a un parqueo en ciertas temporadas, o la cantidad de transacciones que realiza una empresa en un determinado tiempo. En general podemos observar que en situaciones básicas donde no interviene la tecnología o en áreas donde es de vital importancia la tecnología, podemos recopilar enormes cantidades de datos, almacenarlos en grandes volúmenes y además podemos agregar condiciones a cada situación donde se puede obtener múltiples resultados, es ahí donde el analista de datos aplica los términos de extracción, limpieza, análisis y visualización, utilizando una de las ramas esenciales de la ciencia, como lo es la estadística, donde este puede realizar predicciones basándose en el historial de todos los datos procesados o puede identificar patrones en un determinado conjunto de datos. Un analista de datos "es un perfil profesional que gracias a la interpretación de los datos puede establecer estrategias dentro de una empresa" [5].

Un analista de datos debe determinar cómo se deben usar los datos con el fin de responder preguntas y resolver problemas, recordemos que los analistas de datos trabajan con volúmenes grandes de datos almacenados que no tienen ninguna interpretación o sentido hasta que él ejecuta una

serie de acciones hasta tener un resultado. Un analista de datos aplica y ejerce su profesión en una amplia y extensa variedad de áreas. Previamente definido este término, podemos destacar ciertas funciones y características que un analista de datos debe aplicar, como:

- Debe poseer y aplicar conocimientos en bases de datos y lenguajes de programación.
- Debe poseer técnicas en diseño de bases de datos.
- Debe manejar y aplicar conocimientos sobre Hadoop & MapReduce.
- Debe aplicar técnicas para visualizar datos (Reportes).
- Se encarga de realizar el proceso de extracción, procesamiento y agrupación de datos.
- Identifica patrones o tendencias en un conjunto de datos.
- Analiza los patrones o agrupaciones de datos utilizando herramientas y técnicas estadísticas.
- Puede generar resultados utilizando distintas técnicas (utilizando estadística).
- Generan resultados utilizando un formato de tipo informe.
- Es esencial al momento de la toma de decisiones o para establecer estrategias.
- Identifican nuevas soluciones para la mejora de procesos.
- Pueden diseñar, crear y dar mantenimiento a los sistemas de bases datos.

¿Qué herramientas usa un analista de datos? Un analista de datos emplea y aplica cálculos utilizando sistemas informáticos, debido a la extensa variedad de áreas en la que un analista de datos puede ejercer su profesión, se podría recomendar en general el uso de las siguientes herramientas, conceptos y lenguajes de programación, como:

- **Software:** IBM SPSS, Statistical Analysis System (SAS), Herramientas de Business Intelligence(SSDT, SAP BI, Oracle BI, Tableau, etc.), Bases de Datos SQL, Hadoop, Apache Spar.

• **Lenguajes de programación:** Python, R, C/C++, Java, Javascript.

¿Dónde puedo especializarme? A este punto de la lectura es necesario entender que se debe tener una carrera universitaria enfocada a la informática, como una licenciatura en informática, ingeniería de software, ingeniería en sistemas e inclusive una licenciatura en estadística. Si deseas obtener una certificación en análisis de datos puedes ingresar en las siguientes plataformas: Datacamp, IEBSchool, Coursera, Ubiquum, Acamica, Florida Business School, Digitalhouse, UniSA Online, Western Sydney University, UNSW Sydney.

Si el lector desea explorar sobre el análisis de datos, la plataforma DataCamp ofrece una lista amplia de cursos gratuitos, así como también cursos de categoría Premium, estos se pueden acceder por un costo cómodo en comparación a las demás plataformas.



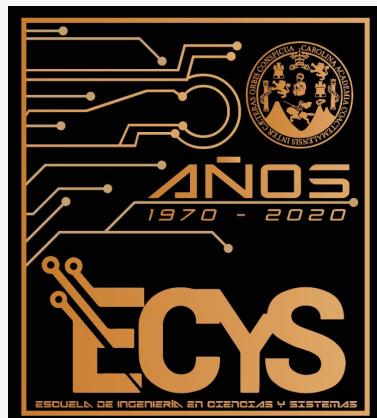
Imagen 1: Data Analyst with R.

Conclusiones

- Un dato es un conjunto de caracteres almacenados, mientras que información es un conjunto de datos que tienen un sentido o un significado.
- Un analista de datos es la persona encargada de extraer, analizar, procesar y visualizar un conjunto de datos aplicando métodos y técnicas estadísticas.
- Un analista de datos es fundamental en la toma de decisiones o en la gestión de sugerencias dentro de una organización o empresa.
- Un analista de datos debe manejar los conceptos de business intelligence, bases de datos, Hadoop, lenguajes de programación como R, Python, Javascript, C/C++ entre otros.
- DataCamp es una plataforma que brinda de un catálogo extenso de cursos (algunos gratuitos) con el fin de formar especialistas en el área de la ciencia de los datos.

Referencias

- [1] **Desconocido.** (11 de julio 2019). Lexico: Definition of dato in Spanish. Recuperado de: <https://bit.ly/3bqq0hl>. [Último acceso: 07 de octubre de 2019].
- [2] **Bembibre, V.** (febrero 2009). DefiniciónABC: Definición de Información. Recuperado de: <https://bit.ly/2Wwt9I3>. [Último acceso: 05 de octubre de 2019].
- [3] Espino, L.(febrero 2016). Amazon: Modelos de Bases de Datos (Spanish Edition)Recuperado de: <https://amzn.to/2U9iUHS>. [Último acceso: 06 de octubre de 2019].
- [4] Hipodec. (13 de noviembre 2018). HIPODEC: La industria del Data Science. Recuperado de: <https://bit.ly/2J6sk0y>. [Último acceso: 05 de octubre de 2019].
- [5] Estaún, M. (11 de noviembre 2019). IEBSchool: ¿Qué es y qué hace un Analista de Datos o Big Data Analyst?. Recuperado de: <https://bit.ly/3abjktp>. [Último acceso: 15 de Noviembre de 2019]



Se ofrecen recorridos guiados con previa cita. Reservar al correo educacion.jardinbotanico@gmail.com o a nuestra fan page [f/jardinbotanicousac](https://www.facebook.com/jardinbotanicousac)

De lunes a viernes de 8:30 a 15:00 horas
Nacionales Q.3.00, Extranjeros Q.10.00
Entrada por Calle Mariscal Cruz 1-56, z.10
Teléfonos: 2334-6064 y 2361-5450
jardinbotanicousac@gmail.com



Google Search como herramienta para Hacking

Marvin José Calderón García
marvin93.0@gmail.com

Estudiante de Ingeniería en Ciencias y Sistemas - USAC

Palabras Clave:

Motor de búsqueda, Google, Hacking, Vulnerabilidades, Sitios Web.

La fuente de alimentación del hacker es la información y Google indexa millones de datos día con día a toda hora. Es por ello que esta información es la fuente inagotable de material necesario para que los hackers puedan acceder a información que de otra forma podría resultar difícil de conseguir. Utilizar Google Search como una herramienta de estudio de vulnerabilidades en sitios web implica el conocer diferentes técnicas que, a medida que se van perfeccionando, ayudan a determinar imperfecciones de seguridad tanto en la configuración de los servidores que alojan las aplicaciones, así como también en el código que los sitios web implementan. A partir de este punto, es necesario explicar algunos conceptos importantes que conlleva el realizar hacking utilizando esta herramienta.

The screenshot shows a Google search results page for the query "access denied for user" "using password" "general error" "-inurl:phpbb". The results list several examples of SQL injection vulnerabilities found in various websites. One result from "FindAGround.com" shows a specific exploit for a MySQL database. Another result from "eternal-wowl.com" discusses a general error in MySQL. Other results mention "My SQL Error? [RESOLVED]" and "General Error" from different forums. The sidebar on the left shows navigation links like "Búsqueda", "Todo", "Imagenes", "Maps", "Videos", "Noticias", "Shopping", "Más", "Madrid", and "La Web".

Imagen 1: Visualización de uno de los trucos utilizados en Google Hacking para conseguir nombres de usuario y contraseñas de alguna base de datos.

El utilizar el motor de búsqueda de Google para hacer hacking tiene un nombre: Google Hacking.[1] Este término hace referencia a la técnica que conlleva el utilizar las avanzadas herramientas de Google Search para la búsqueda de información de carácter sensible como lo son las credenciales, datos

personales, contraseñas, imágenes, archivos, etc. Los atacantes o "hackers" pueden buscar cualquier tipo de archivo, incluso con extensión específica, que esté siendo indexado por los motores de Google y que los encargados del sitio hayan olvidado mencionarle, entre los archivos de configuración que solicita Google, que no tome en cuenta dichos archivos para mostrarlos como resultado en sus búsquedas.

Por ejemplo, si se desea que los resultados de búsqueda muestren todos los archivos SQL (extensión: SQL) que Google ha indexado de los sitios web y que además esté habilitada en la lista de directorios del sitio[2] (los cuales Google necesita para saber que archivos indexar para búsquedas y cuales no), se realiza como se muestra en la imagen 2. Así como puede hacerse búsqueda de archivos con algún tipo de extensión, también se puede hacer mejor la búsqueda restringiendo a buscar en un solo sitio en específico, así como también definir una lista de sitios web que pueden contener la información que se desea buscar. Para adentrarse más sobre todos los posibles "hacks" que se pueden realizar utilizando el motor de búsqueda de Google, es necesario detallar todos y cada uno de los comandos disponibles para realizar estas acciones.

The screenshot shows a Google search results page for the query "intitle:index of filetype:sql". The results list numerous websites that have their directory structures indexed by Google, making them vulnerable to directory traversal attacks. Many of the results contain the word "sql" highlighted in yellow, indicating the presence of SQL files or code. The sidebar on the left shows navigation links like "Búsqueda", "Todo", "Images", "Videos", "Books", "News", "More", "Settings", and "Tools".

Imagen 2: Ejemplo de comando de Google Hacking que muestra en los resultados de búsqueda todos los sitios

web que contienen la indexación de archivos con extensión SQL.

Los diferentes comandos que se pueden utilizar para realizar hacking por medio del motor de búsqueda de Google conllevan una serie de operadores los cuales están segmentados en dos categorías: operadores lógicos y operadores avanzados de búsqueda [5]. El primero hace referencia a todos los operadores lógicos que usa Google, como por ejemplo AND, OR, NOT, etc., y que pueden ser aprovechados por los hackers para facilitar sus búsquedas (ver tabla 1).

Operador Lógico	Descripción	Ejemplo
AND o +	Se utiliza para indicar que todas las palabras deben de ser encontradas.	• motor AND aplicación AND fuente • motor + aplicación + fuente
NOT o -	Se utiliza para especificar que no se incluya la palabra después del operador.	• motor aplicación NOT fuente
OR o	Se utiliza para indicar que por lo menos una de todas las palabras debe ser encontrada.	• motor aplicación OR fuente • motor aplicación fuente
Tilde (~)	Se utiliza para incluir sinónimos o palabras parecidas en la búsqueda.	• motor aplicación ~ fuente
Comillas dobles ("")	Se utiliza para hacer un match exacto con la palabra proporcionada.	• "motor aplicación fuente"
Punto (.)	Se utiliza para incluir una porción de caracteres como comodín.	• .tor aplicación fuente (todas las palabras que terminen en ".tor").
Asterisco (*)	Se utiliza para incluir comodines entre palabras.	• Motor * fuente (cualquier cosa que venga entre esas dos palabras).
Paréntesis [()]	Se utiliza para agrupar expresiones de búsqueda.	• ("motor aplicación" motor-aplicación).

Tabla 1: Lista de todos los operadores lógicos manejados por Google y que están disponibles para utilizar en las búsquedas..

La segunda hace énfasis en los diferentes tipos de operadores disponibles para hacer referencia a sitios, tipos de archivo, links, etc. Estos tienen una sintaxis un poco diferente, la cual está dividida en 3 partes: el operador, el símbolo de dos puntos (:) y la palabra clave a buscar[6]. Lo que hace Google con esto es restringir la búsqueda de tal forma que se haga énfasis únicamente en la palabra a encontrar. En el ejemplo de la imagen 2, Google busca en el título del sitio (operador: intitle) la palabra clave "index of". Esta palabra clave es la que muestran como título todos los sitios alojados en un servidor de Apache Server en la que se listan todos los archivos disponibles en determinado directorio. Adicional a esa búsqueda se le agrega el buscar el tipo de archivo (operador: filetype) con la palabra clave "SQL". Esta instrucción complementa a la anterior indicando que se restrinja la búsqueda a solo archivos con extensión SQL.

Existe una lista pequeña de los diferentes operadores avanzados que se pueden utilizar en las búsquedas de tal forma que sean explícitas para no obtener información no deseada de la búsqueda y así poder obtener lo que se busca de una forma rápida y

efectiva (ver tabla 2).

Operador Avanzado	Descripción	Ejemplo
site:	Se encarga de delimitar la búsqueda a un único dominio o sitio web en específico.	• site: misitioweb.com
filetype:	Se encarga de restringir que la búsqueda se realice únicamente sobre un archivo de extensión específica.	• HelloWorld filetype:txt
link:	Se encarga de restringir la búsqueda a un sitio web en específico.	• link:www.misitioweb.com
cache:	Se encarga de buscar y desplegar la última versión de la página que Google indexó.	• cache: misitioweb.com
intitle:	Se encarga de buscar el texto proporcionado en el título del sitio.	• intitle: "texto_del_título"
inurl:	Se encarga de buscar el texto proporcionado dentro del URL del sitio.	• inurl: robots.txt

Tabla 2: . Lista de todos los operadores avanzados manejados por Google y que están disponibles para utilizar en las búsquedas..

En la actualidad existen un sinfín de información que puede ser encontrada utilizando los motores de búsqueda de Google para hacer hacking. Entre las cosas más curiosas que han encontrado los usuarios se destacan elementos como elementos de hardware que están conectados a internet (o como se le conoce hoy en día: Internet de las cosas). Estos dispositivos comparten información a través de la red los cuales, por lo regular, son configurados por usuarios promedio que no tienen un concepto claro sobre la seguridad de la información y dejan vulnerables accesos y contraseñas dentro de estos dispositivos [3]. Otro caso curioso es el de tener acceso a las cámaras de seguridad de diferentes sitios. Estas son fáciles de acceder ya que la mayoría de dispositivos encargados de alojar el sistema DVR de las cámaras utilizan los mismos nombres de archivos y puertos que se configuran por defecto. Todo esto puede ser posible utilizando de forma inteligente los operadores definidos anteriormente.

¿Cómo puedo prevenir estos ataques? Si bien se explicaron las maneras en las que es posible realizar hacking a sitios web desde Google Search, también debería de existir una forma de detenerlo. La solución es simple: contemplar la seguridad en el diseño de un sistema. Todo sistema, así como tiene un apartado en el diseño para su construcción y funcionamiento, también debe tener un área que se encargue de contemplar la seguridad y el control de vulnerabilidades. Si el sitio web va a estar a disposibilidad de todo público, todo dueño del sitio web va a querer que el sitio aparezca dentro de los primeros resultados de búsqueda del motor de Google. Para ello, se debe de tener altos conocimientos en técnicas de indexación como SEO, optimización de código fuente del sitio, no publicar

información que muestre a detalle las diferentes tecnologías utilizadas en el servidor que aloja el sitio, establecer un archivo de robots.txt el cual se encarga de indicarle a los robots de Google que directorios debe de indexar y cuáles no.

Al tomar en cuenta todas estas características al momento de permitir que Google indexe el sitio web, se debe tener por seguro que una gran parte de la seguridad del sitio ha sido cubierta. El poder que se le otorga a Google no depende de nadie más que de uno mismo. En la actualidad el tema de Google Hacking es un poco controversial ya que, dependiendo de la situación, el realizarlo hacia un sitio web en específico puede implicar términos legales. Si se hace con la autorización del dueño del sitio con fines de identificar vulnerabilidades se puede decir que se está haciendo de la forma legal, de lo contrario puede implicar ciertos problemas y es donde el hacking pasa de ser bueno y positivo, a ser algo con malas intenciones.

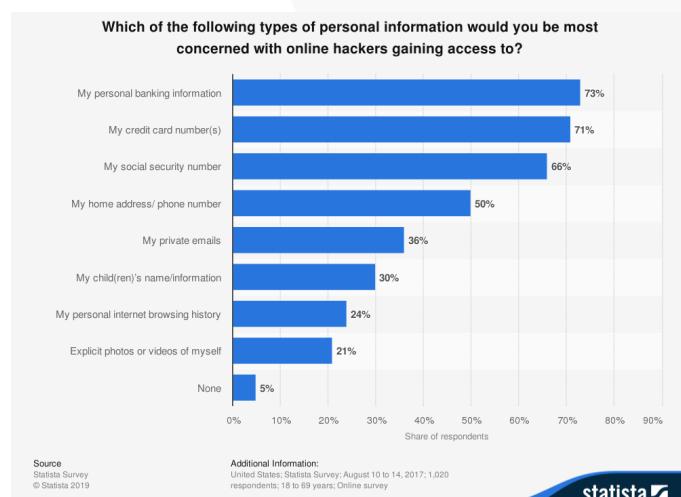


Imagen 3 Encuesta realizada en Estados Unidos sobre qué información personal se vería más comprometida de que los hackers tuvieran acceso.

Conclusiones

- Se descubrió que el hacking realizado desde el motor de búsqueda de Google no siempre significa que va a ser realizado con buenas intenciones. Existen muchos "hackers" por todo el mundo que ven estos comandos y herramientas como una oportunidad para aprender y crecer en

sus habilidades informáticas, pero así también existen algunos que solo ven la oportunidad de dañar sistemas que en la actualidad ya luchan por un puesto entre las indexaciones de Google.

- Se determinó que las diferentes combinaciones de los operadores lógicos y de búsqueda avanzada pueden llegar a ser comandos con mucho poder, que, si es usado de buena manera, se pueden llegar a detectar grandes vulnerabilidades de seguridad en los sitios web sobre los que se estén trabajando.
- Se determinó que la única forma de evitar el hacking desde esta herramienta de Google es invertir una buena cantidad de trabajo en lo que a la seguridad del sitio respecta. Si el sitio web es público en la red y se desea que aparezca entre las búsquedas de Google, se debe de hacer un correcto trabajo de SEO y configuración de la seguridad del sitio para indicarle a los indexadores de Google que contenido debe indexar y que no. Al final, todo el poder recae sobre la persona que administra el sitio y él es el único responsable.

Referencias

- [1] Natividad, R. (14 de abril de 2018) Roger Natividad. Introducción a Google Hacking. Recuperado de: <https://bit.ly/3dlg0ay>. [Último acceso: 09 de octubre de 2019].
- [2] [5] [6] **Desconocido.** Acunetix: Google Hacking: What is a Google Hack?. Recuperado de: <https://bit.ly/2Ww6lZ1>. [Último acceso: 09 de octubre de 2019].
- [3] **Desconocido.** (19 de septiembre 2018). WiFiBit: Todo sobre Google hacking - 30 Comandos de Ejemplo. Recuperado de: <https://wifibit.com/google-hacking/>. [Último acceso: 09 de octubre de 2019].
- [4] Kunst, A. (3 de septiembre 2019). Statista: Most sensitive private information online 2017. Recuperado de: <https://bit.ly/2WDL3Zg>. [Último acceso: 09 de octubre de 2019].



Progressive Web Apps y el futuro del desarrollo web.

Fernando Andrés Mérida Antón
fer.merida94@gmail.com

Estudiante de Ingeniería en Ciencias y Sistemas - USAC
Palabras Clave:

Tecnología, Web, Tendencia, Aplicación

Introducción a PWA Si alguna vez has desarrollado una aplicación web seguramente te has enterado de este importante cambio que el desarrollo de aplicaciones ha tenido en los últimos tiempos. Las aplicaciones web progresivas han sido ampliamente comentadas y es considerada una de las tendencias en cuanto a innovación tecnológica junto a IOT o Inteligencia artificial. Pero, ¿Por qué las aplicaciones web progresivas son tan importantes? ¿Qué cambio suponen para el desarrollo convencional?

Lo primero que haremos es definir qué constituye una aplicación web progresiva o PWA. Actualmente la línea que separa las aplicaciones web y las aplicaciones nativas es muy clara. Las aplicaciones web son utilizadas en una página web dentro de un navegador y no es necesario instalar esta aplicación, solamente tener acceso a internet para utilizarla. En cambio, las aplicaciones nativas son específicamente desarrolladas para el sistema operativo en el que corren y funciona de una manera más fluida dentro de este contexto. Acá es donde empieza a tomar relevancia las PWA, estas son aplicaciones híbridas entre ambas tecnologías. En otras palabras, es lo mejor de dos mundos combinados en una sola app.

PWA ha logrado ser una evolución de las aplicaciones web tradicionales con las que hemos tratado normalmente atendiendo las principales deficiencias de estas y dándoles un acercamiento más eficiente, pudiendo realizar acciones que previamente solo podrían haber sido posibles para aplicaciones nativas. Esto ha provocado que esta división clara entre ambos tipos de aplicaciones disminuya. Este cambio se debe a la utilización de Service Workers, un script que el navegador ejecuta en segundo plano separado de la página. Los cambios que los Service Workers han generado en las aplicaciones web son considerables. Un caso de estudio realizado por Google en el 2017 para determinar el impacto de las PWA en los indicadores

de negocio muestra un cambio considerable, como lo demuestra la siguiente imagen.



Imagen 1: Estadísticas de ventajas utilizando PWA sobre aplicaciones web normales

Presente y futuro del desarrollo web

El mercado móvil ha crecido considerablemente en los últimos años, siendo la primera opción de muchas compañías que desean dar a conocer sus servicios y facilitar su interacción con los usuarios. Todos conocemos varias páginas web o compañías que tienen sus propias aplicaciones móviles disponibles para que sus usuarios las descarguen, pero siendo francos ¿Cuántas aplicaciones de compañías has decidido instalar cuando te da la opción su página web? Si lo hiciste, voluntariamente o porque no tenías opción ¿Cuánto tiempo duro en tu smartphone esa aplicación antes de que decidieras eliminarla? Acá es donde resalta la importancia de las PWA.

Ciertamente frente a aplicaciones web tiene bastantes ventajas técnicas, pero frente a las aplicaciones nativas sus ventajas están más orientadas a lógica de negocio. PWA trata de eliminar ese proceso molesto de tener que instalar una aplicación para poder utilizar sus funciones. Los pasos para llevar lo contenido en la página web a tu pantalla de inicio disminuyen y esto provoca que clientes potenciales

no se pierdan en ese proceso. Actualmente el ejemplo más claro sobre esto es Twitter Light, que es una implementación semi exitosa de aplicaciones progresivas para lograr que su aplicación web no se sienta como una aplicación web.

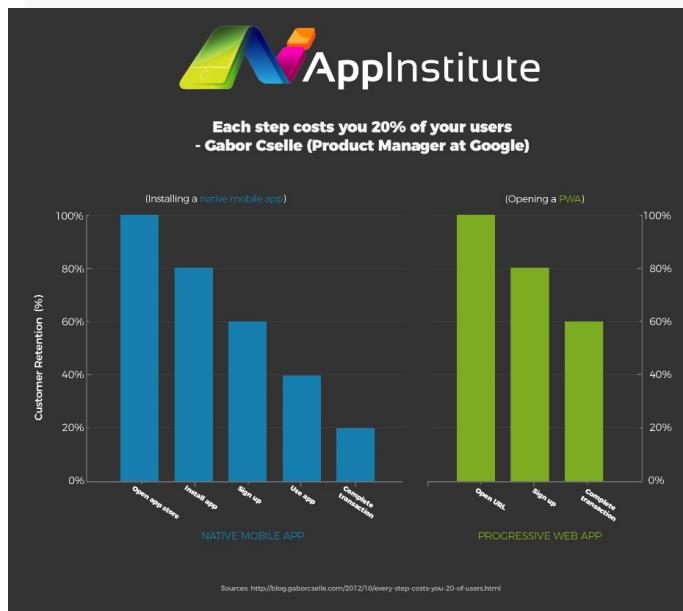


Imagen 2: Retención de clientes por cada paso, Aplicaciones Nativas vs PWA

Tomando todo esto en cuenta una de las principales preguntas que surgen es ¿Cuál es el futuro de las aplicaciones progresivas? Algunas personas sugieren que las aplicaciones nativas disminuirán en los próximos años, a medida que los desarrolladores se den cuenta de los beneficios de las aplicaciones progresivas. Siendo otra de sus ventajas que son mucho más baratas de implementar que una aplicación nativa. Otros autores creen que las PWA no remplazarán a las aplicaciones nativas y que simplemente serán una opción más en el mercado, porque hay cierto tipo de implementaciones que están destinados a ser nativos. Además de la cultura general que se ha creado a la hora de instalar y el efecto de seguridad que provoca en el usuario manejar sus credenciales en una app nativa.

Aún con todos los puntos a favor aún hay problemas que son necesarios tomar en cuenta, esto será el foco para esta tecnología en los próximos años. Uno de ellos es que, aunque las aplicaciones no dependan del entorno físico si lo harán del navegador. Tanto Chrome, Opera y el navegador de Samsung son los únicos que soportan PWA en este momento. Además de estas limitantes, se añade la

falta de soporte para hardware que no es soportado por HTML5 y la falta de comunicación con otras aplicaciones para procesos de autenticación.

Introducción al desarrollo de PWA en Guatemala

Ahora que conocemos esta nueva tendencia en el desarrollo web y que es una de las tecnologías que veremos en los próximos años nos queda la interrogante de ¿Qué haremos para contribuir y adaptarnos a ella? Actualmente la introducción a PWA, especialmente para los novatos en desarrollo web, supone una implementación con bastante código que podría ser intimidante y compleja. Con esto en cuenta, estar a la vanguardia en desarrollo de software siempre lo es. La tecnología está en constante cambio y estar enterado de las nuevas tendencias supone un valor agregado para nosotros que estamos en este campo.

Personalmente, creo que estas tendencias de tecnología actuales están llegando a nosotros en la universidad de manera progresiva y a un ritmo pausado. Si queremos que nuestro conocimiento y habilidades tecnológicas estén actualizadas no debemos esperar a que el conocimiento venga a nosotros, sino ser nosotros quienes estemos en constante búsqueda de este. Siempre investigando y probando estas tendencias para tener una postura clara del ámbito nacional y mundial tecnológico.

En conclusión Es imposible predecir que tanto auge tomarán las PWA en los próximos años. Ciertamente parecen ser una evolución y un paso hacia adelante para las aplicaciones web, pero se encuentra aún en etapas tempranas donde todavía hay mucho que resolver. No se puede decir tampoco que tomará el lugar de las aplicaciones nativas, pero si existe un interés creciente en este tipo de aplicaciones. Lo que se puede decir con certeza es que las aplicaciones web pueden no volver a ser las mismas y queda en nosotros como contribuir o aprender sobre el tema. Podemos esperar a que sea una realidad o podemos ser parte del proceso desde etapas tempranas y aportar nuestro conocimiento, aprender por nuestra cuenta y crecer como profesionales. Si quieras empezar a aprender a hacer una PWA puedes comenzar en esta página.

Conclusiones

- Uno de los principales atractivos de las aplicaciones web progresivas es su bajo costo de implementación y la oportunidad de eliminar los tiempos de instalación excesivos para los usuarios.
- Los service workers son el alma de las PWA gracias a su manejo en segundo plano, su almacenamiento de cache confiable e inteligente y la posibilidad de notificaciones automáticas.
- Las aplicaciones web progresivas son aplicaciones web con comportamiento de aplicaciones nativas que proveen un cambio innovador en la visión y forma de desarrollo de aplicaciones móviles y aplicaciones web.

Referencias

- [1] **Bapna, A.** (17 de mayo 2017). Developers Google: MakeMyTrip.com's new PWA delivers 3X improvement in conversión. Recuperado de: <https://bit.ly/2xdRask>. [Último acceso: 27 de febrero de 2020].
- [2] LePage, P. (16 de mayo 2019). Developers Google: Your First Progressive Web App. Recuperado de: <https://bit.ly/394Dk9j>. [Último acceso: 10 de octubre de 2019].
- [3] S Nath, D. (24 de marzo 2017). Medium: 4 important points to know about Progressive Web Apps. Recuperado de: <https://bit.ly/399ZPd3>. [Último acceso: 10 de octubre de 2019].
- [4] Scacca, S. (28 de diciembre 2018). Smashing Magazine: Will PWAs Replace Native Mobile Apps?. Recuperado de: <https://bit.ly/2wtYuR5>. [Último acceso: 10 de octubre de 2019].

Ahora trabajamos todos en

USAC - SICOIN

Sistema de Contabilidad Integrada
SICOIN / Descentralizadas(PROD-SRV1)

<https://sicoindes.minfin.gob.gt/>



MINISTERIO DE
FINANZAS PÚBLICAS



Farmacia Universitaria

Venta de Medicamentos y Suplementos Vitamínicos

De Lunes a Viernes de 8:00 a 19:00 horas.
Sábados de 8:00 a 12:30 horas.

PBX: 2418-8000
Exts.: 83240 / 9662



2418-9662
2418-7722

Edificio de Recursos Educativos, 2do Nivel Farmacia Universitaria, zona 12 (Biblioteca Central).

E-mail: farmaciauniversitaria@usac.edu.gt



Criptografía: El arte de ocultar mensajes

Elmer Orlando Real Ixcayau

elmerreal98@gmail.com

Estudiante de Ingeniería en Ciencias y Sistemas - USAC

Palabras Clave:

Comunicación, llave pública, llave privada, clave, seguridad.

La comunicación es una necesidad de todos los seres humanos, es la única manera que se pueden expresar ideas propias a otros individuos. El proceso de la comunicación permite que dos individuos o más intercambien información a través de un canal siguiendo un mismo código y contexto para darse a entender entre si.

La necesidad de ocultar y transmitir mensajes a coexistido desde el inicio de la humanidad. El ser humano con el fin de ocultar mensajes a desarrollado técnicas para codificar los mensajes, denominada criptografía, así como técnicas disuasorias para ocultar la existencia misma del mensaje a esto se le denomina: esteganografía.

Esteganografía

La esteganografía es la aplicación de ingenio para ocultar la existencia de un mensaje. En la antigüedad era de interés de la élite política o militar el intercambio de mensajes de manera que el enemigo no se entere.

El griego Herodoto en su Libro III [4] de su magna Historia expone como el tirano Mileto ordenó a un hombre raparse la cabeza, a continuación, escribió en el cráneo del sujeto el mensaje que deseaba transmitir y esperó a que volviera a crecerle el cabello para enviarlo a su destinatario (Demarato).

Demarato, rey espartano exiliado en Persia, luego de recibir el mensaje escribió un nuevo mensaje en una tabla y posteriormente cubrió la misma con cera derretida de manera que aparentaba ser una tabla en blanco para enviársela a los Lacedemonios advirtiéndoles del proyecto de invasión del rey persa, Jerjes.

Pareciera que la esteganografía es la solución al ocultamiento de información, sin embargo, el principal problema de este es que al ser interceptada deja expuesta de manera transparente el mensaje por

lo que es recomendado utilizar de manera conjunta la esteganografía y la criptografía.

Criptografía Es la aplicación de técnicas que permiten cambiar el mensaje por un equivalente codificado según una clave específica lo cual permite que solo aquellos que conozcan dicha clave puedan descifrar el mensaje de manera correcta. Los métodos criptográficos han evolucionado conforme transcurre la historia. Algunas de sus evoluciones son:

La criptografía por transposición

Este método de criptografía consistió en la escritura de mensajes en tiras largas de papel con los símbolos del mensaje y se agregan símbolos aleatorios de manera que al enrollarlos en el bastón que tuviera las dimensiones (longitud y grosor) pudieran mostrar el mensaje correcto [3]. En este método de criptografía el bastón realizó la función de clave del sistema porque si no se poseía el bastón con las dimensiones correctas no se podía leer el mensaje correctamente.

Sin embargo, el principal problema de este método es que mediante prueba y error se puede encontrar la clave y se puede leer sin problemas el mensaje que se deseaba ocultar.

Cifrado Cesar o cifrado por sustitución

Este tipo de cifrado se le atribuye su uso a Julio Cesar. Consiste en desplazar cada carácter n veces en el abecedario [5]. Siendo el valor n la clave ya que dependiendo este valor se cambiaba por la letra n veces más adelante.

El método Cesar puede ser fácilmente burlado intentando todos los desplazamientos posibles hasta que el texto tuviera sentido, mediante aritmética modular o utilizando análisis de frecuencias donde se calcula la aparición de los caracteres y dependiendo de la frecuencia que se obtiene se sustituyen los que poseen mayor frecuencia con caracteres que

comúnmente aparecen con alta frecuencia de uso hasta encontrar la clave del cifrado Cesar.

El cifrado poli alfabético

Para burlar el análisis de frecuencias con la que se podía encontrar la clave del cifrado cesar se diseñó un nuevo cifrado llamado cifrado poli alfabético que tal como lo sugiere su nombre se trata de un cifrado donde utiliza varios alfabetos cifrados[6].

Un ejemplo de cifrado poli alfabético es el cuadrado De Vigenere el cual consiste en n alfabetos cifrados, cada uno de ellos desplazados una letra a la izquierda la cual permite que para codificar un mensaje se utilice cualquiera de los símbolos equivalentes de los alfabetos cifrados, lo cual lo hace inmune al análisis de frecuencias porque un símbolo puede ser representado por n opciones según los alfabetos cifrados.

Pareciera que el cifrado poli alfabético soluciona una vez por todas el problema del análisis de frecuencias, pero como podemos darnos cuenta la longitud de la cadena sugiere la cantidad de lenguajes utilizados y como un cuadrado De Vigenere utiliza n lenguajes con cifrado Cesar los cuales son susceptibles a criptoanálisis. A prueba y error es posible descifrar el mensaje debido a esta cualidad del cuadrado De Vigenere.

Los métodos descritos anteriormente pertenecen a la criptografía simétrica, debido a que se basa en una sola clave privada y se genera solo una llave que tiene que ser compartida entre las partes interesadas para poder cifrar y descifrar un mensaje.

La seguridad de los métodos criptográficos simétricos recae en la clave, por lo que al compartir la clave se vulnera el cifrado. El principal problema de este tipo de métodos es como compartir la clave sin quedar vulnerables al hacerlo. Un claro ejemplo de dicha vulnerabilidad fue la máquina enigma utilizada por el gobierno alemán utilizada durante la segunda guerra mundial que era una máquina de cifrada electromecánica que generaba abecedarios según las posiciones de unos rodillos que podría tener distintas órdenes y posiciones pero su mayor vulnerabilidad era que dependía de una clave la cual la mayoría de días los ingleses conseguían.

La distribución de clave sugiere un problema serio porque todos los canales posibles para compartirlos son canales comprometidos y vulnerables a ser interceptados por lo que para garantizar la seguridad del criptosistema es necesario implementar una clave pública para todo aquel interesado y una clave privada propia de cada parte interesada en el intercambio del mensaje. A esto se le conoce como criptografía asimétrica. La cual se basa en el uso de dos claves: Una pública que se difunde y una privada que nunca debe revelarse.

En 1976 dos jóvenes científicos estadounidense, Whitfield Diffie y Monte Hellman [7], dieron con un modo de que dos individuos intercambiaran mensajes cifrados sin tener que intercambiar previamente alguna clave. Este método se apoya de la aritmética modular y así como las propiedades de los números primos.

El algoritmo de Diffie-Hellman mostro que teóricamente existe la posibilidad de crear un método criptográfico sin necesidad de intercambiar claves más que la clave pública con la que se calculan las demás claves. En agosto de 1977 el estadounidense Martin Gardner publicó en la revista Scientific America un artículo titulado "Un nuevo tipo de cifrado que costaría millones de años descifrar"[1], donde presento un algoritmo conocido como RSA, acrónimo de los apellidos Rivest, Shamir y Adelman. La cual es la primera implementación práctica del modelo de clave pública planteada por Diffie y Hellman"[9].

Un ejemplo de cifrado poli alfabético es el cuadrado De Vigenere el cual consiste en n alfabetos cifrados, cada uno de ellos desplazados una letra a la izquierda la cual permite que para codificar un mensaje se utilice cualquiera de los símbolos equivalentes de los alfabetos cifrados, lo cual lo hace inmune al análisis de frecuencias porque un símbolo puede ser representado por n opciones según los alfabetos cifrados.

Pareciera que el cifrado poli alfabético soluciona una vez por todas el problema del análisis de frecuencias, pero como podemos darnos cuenta la longitud de la cadena sugiere la cantidad de lenguajes utilizados y como un cuadrado De Vigenere utiliza n lenguajes con cifrado Cesar los cuales son susceptibles a criptoanálisis. A prueba y error es

posible descifrar el mensaje debido a esta cualidad del cuadrado De Vigenere.

Los métodos descritos anteriormente pertenecen a la criptografía simétrica, debido a que se basa en una sola clave privada y se genera solo una llave que tiene que ser compartida entre las partes interesadas para poder cifrar y descifrar un mensaje.

La seguridad de los métodos criptográficos simétricos recae en la clave, por lo que al compartir la clave se vulnera el cifrado. El principal problema de este tipo de métodos es como compartir la clave sin quedar vulnerables al hacerlo. Un claro ejemplo de dicha vulnerabilidad fue la maquina enigma utilizada por el gobierno alemán utilizada durante la segunda guerra mundial que era una máquina de cifrada electromecánica que generaba abecedarios según las posiciones de unos rodillos que podría tener distintas órdenes y posiciones pero su mayor vulnerabilidad era que dependía de una clave la cual la mayoría de días los ingleses conseguían.

La distribución de clave sugiere un problema serio porque todos los canales posibles para compartirlos son canales comprometidos y vulnerables a ser interceptados por lo que para garantizar la seguridad del criptosistema es necesario implementar una clave publica para todo aquel interesado y una clave privada propia de cada parte interesada en el intercambio del mensaje. A esto se le conoce como criptografía asimétrica. La cual se basa en el uso de dos claves: Una publica que se difunde y una privada que nunca debe revelarse.

En 1976 dos jóvenes científicos estadounidense, Whitfield Diffie y Monte Hellman[8], dieron con un modo de que dos individuos intercambiaran mensajes cifrados sin tener que intercambiar previamente alguna clave. Este método se apoya de la aritmética modular y así como las propiedades de los números primos.

El algoritmo de Diffie-Hellman mostro que teóricamente existe la posibilidad de crear un método criptográfico sin necesidad de intercambiar claves más que la clave publica con la que se calculan las demás claves. En agosto de 1977 el estadounidense Martin Gardner publicó en la revista Scientific America un artículo titulado "Un nuevo tipo de cifrado que costaría millones de años descifrar"[10], donde

presento un algoritmo conocido como RSA, acrónimo de los apellidos Rivest, Shamir y Adelman. La cual es la primera implementación práctica del modelo de clave publica planteada por Diffi y Hellman[11].

El método RSA es el que emplean la mayoría de los sistemas computacionales porque a pesar de que se ha comprobado que este método no es infalible del todo, el romper el cifrado requiere demasiado poder de procesamiento gracias a las propiedades de los números primos y la aritmética popular. El algoritmo RSA es seguro, en cierta manera, y funcional, pero está en peligro. Con la inminente llegada de la computación cuántica el nivel de procesamiento que requiere romper dicho cifrado dejará de ser un problema y se convertirá en algo que se puede realizar en cuestión de segundos.

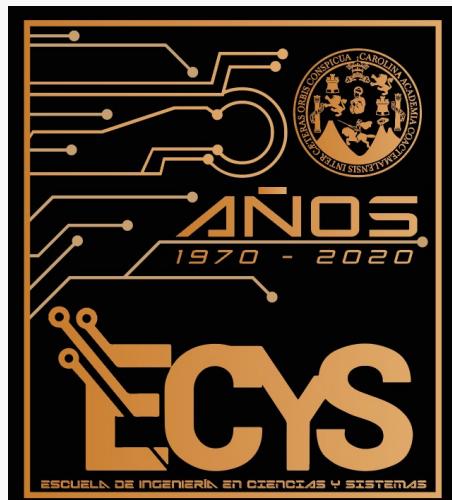
A través del tiempo el ser humano ha buscado la manera de ocultar sus mensajes. Para alcanzar dicho cometido ha diseñado múltiples tipos de cifrado, ninguno infalible hasta el momento. ¿Existirá algún método que sea imposible de vulnerar?, ¿La computación cuántica abrirá un nuevo horizonte en el desarrollo de métodos criptográficos al derribar la barrera del procesamiento limitado y costoso?

Conclusiones

- La criptografía no es una tecnología, es el arte y técnica de ocultar mensajes.
- Los medios y canales de comunicación son inseguros por naturaleza lo cual compromete el proceso de comunicación.
- La criptografía simétrica es la que depende de una sola clave.
- La criptografía asimétrica depende de una clave privada y una pública.
- Los números primos y la aritmética modular van de la mano con el desarrollo de métodos criptográficos por el costo de procesamiento que se necesita para realizarles ingeniería inversa y descifrarlos.
- La computación cuántica promete expandir el horizonte de la criptografía.

Referencias

- [1] [9] [10] [11] Gutiérrez, P. (25 de agosto 2017). Genbeta: Tipos de criptografía: simétrica, asimétrica e hibrida, (03/01/2013). Recuperado de: <https://bit.ly/2xcrpcj>. [Último acceso: 10 de octubre de 2019].
- [2] **Granados, G.** (10 de julio 2006). Revista UNAM: Introducción a la Criptografía. Recuperado de: <https://bit.ly/2QBfbAK>. [Último acceso: 10 de octubre de 2019].
- [3] [5] [6] [7] [8] Gómez, J. (1 de octubre 2010). *Matemáticos, espías y piratas informáticos: Codificación y criptografía*. España. Editorial RBA.
- [4] De Halicarnaso, H. (Año 2000). *Los nueve libros de la Historia*. Argentina. Editorial Claleph.



RADIO 92.1 FM Universidad

web radiou.usac.edu.gt
f [/universidad921](#)
t [@universidad921](#)
w 5478-1217
n PBX: 2207-9090
n Cabina: 2207-9017 y 18

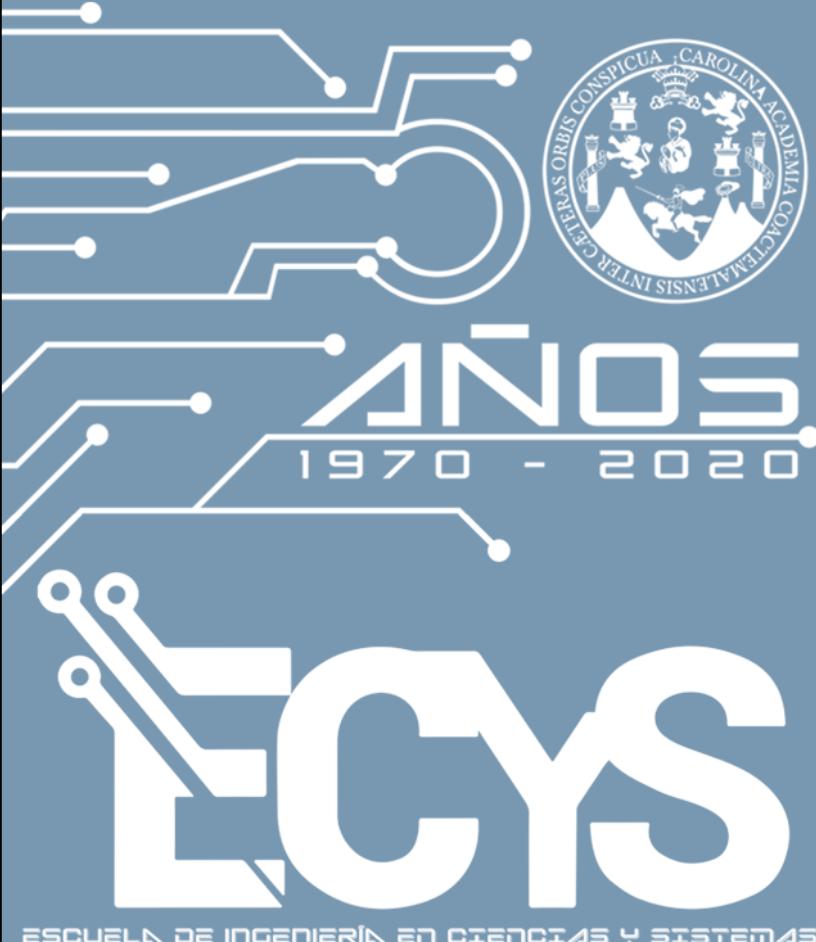
JARDÍN BOTÁNICO
CECON-USAC

De lunes a viernes de 8:30 a 15:00 horas
Nacionales Q.3.00, Extranjeros Q.10.00
Entrada por Calle Mariscal Cruz 1-56, z.100
Teléfonos: 2334-6064 y 2361-5450
jardinbotanicousac@gmail.com

Se ofrecen recorridos guiados con previa cita. Reservar al correo educacion.jardinbotanico@gmail.com o a nuestra fan page [f/jardinbotanicousac](#)

**CIENCIAS
SISTEMAS
& TECNOLOGÍA**

ABRIL 2020 - EDICIÓN XVI



FACULTAD DE INGENIERÍA