# Implementación de una API(Application Programming Interface) que facilite la implementación de autenticación de doble factor en sitios web.

Andrés Valencia Díaz

Esteban Moya Vargas

Universidad Icesi

Facultad de Ingeniería

Ingeniería Telemática

Cali

2017

# Implementación de una API(Application Programming Interface) que facilite la implementación de autenticación de doble factor en sitios web.

Andrés Valencia Díaz

Esteban Moya Vargas

Anteproyecto de grado

Juan Manuel Madrid Molina

Magister en Seguridad de la Información

Universidad Icesi

Facultad de Ingeniería

Ingeniería Telemática

Cali

2017

# Sobre el título del anteproyecto

* Debe reflejar el tema de investigación y su alcance, debe ser directo y preciso.
* Ofrece al lector una idea general del objetivo general, del tema de investigación o del problema de ingeniería que se quiere resolver, debe guardar relación con el proyecto.
* Es recomendable escribir varios títulos y jugar con las palabras, hasta que encuentre el que mejor exprese lo que pretende el proyecto.

**Recomendaciones de COLCIENCIAS sobre el título para proyectos de investigación**

COLCIENCIAS recomienda que el título permita identificar los siguientes elementos

1. PROCESO: ¿Qué se va a realizar, a desarrollar, a diseñar?
2. **OBJETO: ¿Sobre o para qué se va a ejecutar?**
3. UBICACIÓN: ¿Dónde se va a ejecutar?
4. Arquitectura de la red de comunicaciones **para una solución de medición inteligente orientada a la reducción de pérdidas no técnicas** **en el sector eléctrico colombiano**.
5. **Sistema de trazabilidad** de **documentos electrónicos** del **CEN Carvajal**
6. Sistema de monitoreo y control a distancia **para el Controlador Lógico Programable (PLC) y el Compresor de Aire** del Laboratorio de Ingeniería Industrial de la Universidad Icesi.
7. Sistema *open source* **para la detección de ataques** en páginas web desarrolladas en lenguaje PHP.
8. Diseño e implementación de prácticas de laboratorio **para la configuración y operación del protocolo IPv6**, utilizando el simulador ns-3.
9. **Sistema para la exploración de patrones de la incidencia del dengue, en las zonas del municipio de Buga.**

Tabla de contenido

[Título del anteproyecto i](#_Toc476070536)

[Título del anteproyecto ii](#_Toc476070537)

[Sobre el título del anteproyecto 2](#_Toc476070538)

[Lista de acrónimos 3](#_Toc476070539)

[Glosario de términos 4](#_Toc476070540)

[Motivación y antecedentes 6](#_Toc476070541)

[Contexto 6](#_Toc476070542)

[Antecedentes del problema 7](#_Toc476070543)

[Justificación 7](#_Toc476070544)

[Descripción del Problema 9](#_Toc476070545)

[Objetivos 10](#_Toc476070546)

[Objetivo general 10](#_Toc476070547)

[Objetivos específicos 10](#_Toc476070548)

[Anexos 11](#_Toc476070549)

[Referencias bibliográficas 12](#_Toc476070550)

## 

## Lista de acrónimos

UIT Unión Internacional de las Telecomunicaciones

MINTIC Ministerio de las Tecnologías de Información y Comunicación

CEO Chief Executive Officer

API Application Programming Interface

## Glosario de términos

**Hacker del Sombrero Negro:** También conocidos como crackers muestran sus habilidades en informática rompiendo sistemas de seguridad de computadoras, colapsando servidores, entrando a zonas restringidas, infectando redes o apoderándose de ellas, entre otras muchas cosas utilizando sus destrezas en métodos hacking. rompe la seguridad informática, buscando la forma de entrar a programas y obtener información o generar virus en el equipo o cuenta ingresada.

**Phishing:** Término informático que denomina un modelo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña, información detallada sobre tarjetas de crédito u otra información bancaria).

**Phisher:** Persona que intenta engañar a la gente para conseguir su información a través de Internet o por correo electrónico para que puedan sacar dinero de su cuenta bancaria.

**Encriptar:** Ocultar datos mediante una clave.

**Integridad:** Se refiere la correctitud y completitud de la información.

**Confidencialidad:** Capacidad del sistema para evitar que personas no autorizadas puedan acceder a la información almacenada en él.

**Disponibilidad:** Servicio que garantiza que los usuarios autorizados tengan acceso a la información y a otros activos de información asociados en el lugar, momento y forma en que es requerido.

**Autenticación:** Es el acto o proceso de confirmar que algo (o alguien) es quien dice ser.

**Autenticación de Doble Factor:** Se trata de una medida de seguridad extra que frecuentemente requiere de un código obtenido a partir de una aplicación, o un mensaje de SMS, además de una contraseña para acceder al servicio.

**API:** Es un conjunto de subrutinas, funciones y procedimientos (o métodos, en la programación orientada a objetos) que ofrece cierta biblioteca para ser utilizado por otro software como una capa de abstracción.

**Framework:** Es una estructura conceptual y tecnológica de soporte definido, normalmente, con artefactos o módulos concretos de software, que puede servir de base para la organización y desarrollo de software.

**Plataforma:** Es un sistema que sirve como base para hacer funcionar determinados módulos de hardware o de software con los que es compatible.

## Motivación y antecedentes

### Contexto

Según el informe “Medición de la Sociedad de la Información” de la Unión Internacional de las Telecomunicaciones (UIT), el 43,3% de la población mundial tiene acceso a internet [1]. En Colombia, el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) realizó una encuesta que evidenció que el 54% de los colombianos acceden a internet, de forma diaria, con un promedio de navegación de 2.6 horas [2].

Teniendo en cuenta las cifras mencionados anteriormente, se puede afirmar que diariamente se mueve un flujo de datos bastante amplio, el cual incluye información de cada uno de los usuarios que acceden a servicios en internet (redes sociales, correo, revistas, bancos, entre otros). Esto resulta atractivo para los hackers de sombrero negro, quienes identifican que la identidad e información son recursos valiosos para los usuarios, y fácilmente pueden llegar a realizar fraudes informáticos de tipo suplantación de identidad (phishing).

A nivel mundial existe el *Anti-Phishing Working Group,* un consorcio internacional líder de negocios, reguladores y agencias que se encargan de monitorizar los ataques de phishing de forma global y coordinar las respuestas a esos ataques. Este grupo revela que para los primeros cuatro meses del 2016, el número de sitios web para phishing incrementó en un 250% comparado con el mismo período en 2015 [3]. Adicionalmente, la comunidad PhishTank, el mayor centro de intercambio de internet acerca de estafas de phishing, indicó que, en el primer semestre del 2016, cerca de 102.573 denuncias de ataques sospechosos de phishing se verificaron como reales. [4].

Estos datos logran englobar a grandes rasgos que esta problemática y sus consecuencias van en aumento, generando la necesidad de crear grupos como los mencionados anteriormente con el fin de disminuir el impacto de esta problemática.

### Antecedentes del problema

En 2013, al menos 38 millones de cuentas de usuarios de Adobe fueron comprometida. Una firma de seguridad afirmó que los hackers obtuvieron datos de los usuarios que les permitieron averiguar fácilmente las contraseñas de los usuarios [5]. En 2014, al haber hackeado la cuenta de un empleado de eBay, los estafadores obtuvieron un número colosal de contraseñas encriptadas y otros datos de usuarios; aproximadamente 145 millones de datos de ingreso fueron robados. No hubo datos financieros robados, pero eBay quedó bajo investigación por al menos 4 estados (Florida, Connecticut, Illinois y California) y por la Cámara de Comercio Internacional del Reino Unido [6]. En 2016, El Banco Central de Bangladesh sufrió un gran robo en el que los ladrones se hicieron con 81 millones de dólares después de hackear el sistema de mensajería del banco. Lo más increíble del caso fue que el fallo fue causado por el simple robo de una contraseña. Incluso, hasta el mismo CEO de Facebook, Mark Zuckerberg sufrió un incidente similar, aunque menos costoso: los hackers robaron su contraseña para entrar en sus cuentas oficiales de Twitter y Pinterest. Una investigación encontró que las personas, incluso éste personaje, reúsan sus contraseñas el 31% de las veces [7].

### Justificación

La seguridad cibernética es una consideración necesaria para los individuos y las familias, así como en los negocios, gobiernos e instituciones de educación [8].

Lo que se espera con este proyecto es brindar una herramienta eficaz que permita adicionar una capa de seguridad, en bajo tiempo, para el proceso de autenticación que usan actualmente las empresas en sus portales web. Esto permitirá que la seguridad del sitio web sea mucho más robusta, generando una alta confiabilidad para los usuarios que consumen los servicios de la empresa a través de este medio. No bastará que el hacker de sombrero negro robe la contraseña de algún usuario, ya que se agregará una segunda clave de uso único la cual será generada cada minuto en una aplicación móvil, a la cual únicamente tendrá acceso el dueño de la cuenta.

Este proyecto nos permitirá conocer en mayor profundidad una de las áreas más importantes de la Ingeniería Telemática como lo es la Seguridad Informática. Esta se encarga principalmente de velar por la integridad, confidencialidad y disponibilidad de la información.

## Descripción del Problema

Actualmente existe un problema muy común en el ámbito de la seguridad informática: la suplantación de identidad en los sitios web. Se han detectado varios factores desencadenantes de este inconveniente: 1) Uso de contraseñas poco seguras, principalmente influenciado por la facilidad de los usuarios para recordarlas o también se podría inferir que existe un desconocimiento acerca de las buenas prácticas para crear una contraseña segura. 2) Existencia de deficiencias en el método de autenticación de un solo factor. 3) Gran cantidad de tiempo que se requiere para implementar mecanismos de seguridad adicionales. 4) Clonación de los sitios web. Todos estos factores no deseados posibilitan que la seguridad de la información e identidad de los usuarios puedan verse comprometidas, generando un bajo nivel de confiabilidad en las empresas que prestan sus servicios a través de un portal web e incluso pérdidas económicas para la misma.

Mediante el uso de una herramienta metodológica del tipo causa-efecto (árbol de problemas) se identificaron las causas y efectos que dan origen al problema formulado previamente. El árbol de objetivos hace referencia a las metas por cumplir mediante la ejecución del proyecto, identificando las causas a tratar para disminuir el impacto del problema (Anexos 1 y 2).

## Objetivos

### Objetivo general

Diseñar e implementar una API que permita la autenticación de doble factor en páginas web.

### Objetivos específicos

1. Seleccionar el framework o plataforma para el desarrollo del API.
2. Diseñar el API teniendo en cuenta el framework seleccionado
3. Implementar y validar el API.

## Anexos

En esta sección colocar todos aquellos anexos (tablas, figuras, gráficos, frameworks, códigos, etcétera) que el autor considera pueden ayudar a dar claridad a alguna idea o concepto expresado en el documento.

Colocar los anexos correspondientes a: análisis de participación, árbol de problemas, árbol de objetivos.

## Referencias bibliográficas

[1] U. I. de las Comunicaciones, “Informe sobre Medición de la Sociedad de la Información 2015 Resumen Ejecutivo.”

[2] M. de las TIC, “8 de cada 10 colombianos están usando Internet.”

[3] Anti-Phishing Working Group, “Phishing Activity Trends Report,” 2016.

[4] OpenDNS, “PhishTank &gt; Statistics about phishing activity and PhishTank usage,” 2016. [Online]. Available: https://www.phishtank.com/stats.php. [Accessed: 25-Feb-2017].

[5] KrebsonSecurity, “Adobe Breach Impacted At Least 38 Million Users — Krebs on Security,” 2013. [Online]. Available: https://krebsonsecurity.com/2013/10/adobe-breach-impacted-at-least-38-million-users/. [Accessed: 28-Feb-2017].

[6] Chicago Tribune, “EBay client information stolen in hacking attack - tribunedigital-chicagotribune,” 2014.

[7] R. Rijiv Gupta, “Mark Zuckerberg and the $80 million stolen password - Recode,” 2016. [Online]. Available: http://www.recode.net/2016/6/7/11868648/stolen-password-cybercrime-hackers-mark-zuckerberg-bangladesh-bank-security. [Accessed: 28-Feb-2017].

[8] CiscoSystems, “Cybersecurity: Everyone’s Responsibility,” 2010.