

**UNIVERSIDAD MARIANO GÁLVEZ DE GUATEMALA**  
**FACULTAD DE INGENIERÍA EN SISTEMAS DE INFORMACIÓN Y**  
**CIENCIAS DE LA COMPUTACIÓN**



**“IMPLEMENTACION DE PROTOCOLOS WEBAUTH Y OATUH2  
EN SISTEMA WEB DE INGENIO AZUCARERO”**

**NOMBRE: OSCAR DAVID TIZOL**

**CARNE: 2990-14-1638**

**GUATEMALA, FEBRERO DEL 2,019**

**UNIVERSIDAD MARIANO GÁLVEZ DE GUATEMALA**  
**FACULTAD DE INGENIERÍA EN SISTEMAS DE INFORMACIÓN Y**  
**CIENCIAS DE LA COMPUTACIÓN**

**IMPLEMENTACION DE PROTOCOLOS WEBAUTH Y OATUH2**  
**EN SISTEMA WEB DE INGENIO AZUCARERO**

**TESIS PRESENTADA**

**POR**

**OSCAR DAVID TIZOL**

**PREVIO A OPTAR EL GRADO ACADÉMICO DE LICENCIADO**  
**Y TITULO PROFESIONAL DE INGENIERO**  
**EN SISTEMAS DE INFORMACIÓN**  
**Y CIENCIAS DE LA COMPUTACIÓN**

**GUATEMALA, FEBRERO DEL 2,019**

## CONTENIDO

ANTECEDENTES.....	1
JUSTIFICACIÓN.....	3
PLANTEAMIENTO DEL PROBLEMA.....	5
PREGUNTAS.....	5
OBJETIVO GENERAL.....	6
OBJETIVOS ESPECÍFICOS.....	6
VIABILIDAD.....	7
MERCADO.....	7
SOPORTE.....	8
TÉCNICA.....	8
ADMINISTRATIVA.....	8

## ANTECEDENTES

Dentro del contexto de informática y/o tecnología, la autenticación o autentificación hace referencia al proceso que un dispositivo, por medio de su hardware y software, busca certificar o constatar la identidad de un remitente (un ser humano u alguna entidad tecnológica) que intenta establecer una comunicación y realizar una actividad o hacer uso de sus recursos.

La autorización por su parte, vela por la protección de los recursos de un sistema, ya sea de software o hardware, siendo los datos, funcionalidades o servicios, permitiendo el uso únicamente por un remitente previamente autenticado (un ser humano o alguna entidad tecnológica).

Aproximadamente en el año 1960 el doctor en física Fernando Corbato, quien vivió en la época de los primeros ordenadores, que eran grandes maquinas calculadoras, creó un sistema operativo llamado “Compatible Time-Sharing System” (CTSS), el cual solventaba la limitante del uso del ordenador por una única persona por un lapso limitado de tiempo. Este sistema dividía los recursos de procesamiento en segmentos y daba la capacidad de que varias personas hicieran uso de la misma. Al mismo tiempo, surgió un problema inherente, al compartir la maquina los archivos o documentos digitales eran accedidos por cualquier colaborador. Ante esta problemática ideó una fórmula matemática simple la cual denomino como “contraseña”.

Esta fórmula funcionaba como un mecanismo de acceso para que un colaborador solo pudiese acceder a su contenido personal, ofreciendo privacidad entre todos los usuarios del computador dando origen al primer método de autenticación en la historia. (


Años posteriores cuando entro en auge la Web, había mucha información sensible en todo el mundo.

“Expertos como el criptógrafo Robert Morris creo el concepto de “HASH”, proceso en el que una cadena de caracteres se transformaba en un código numérico que representaba de forma más segura, la contraseña original”. (<https://www.welivesecurity.com/la-es/2017/05/04/dia-de-la-contrasena-origen/>).

Sin embargo, en los años 80 surgieron los primeros ataques cibernéticos enfocados en el robo de credenciales e información de empresas y suplantación de identidad entre otros. Uno de los factores más relevantes, era el humano. Representaba y representa un riesgo inherente en los sistemas de información.


“El 41% de las personas tienen seis o más contraseñas y el 42% anota las contraseñas (...), el 23% siempre usa la misma contraseña y más del 60% de los adultos en línea usan al menos dos dispositivos cada día” (<https://www2.deloitte.com/co/es/pages/audit/articles/un-mundo-mas-alla-de-las-contrasenas.html>).

El proceso de otorgar o compartir las credenciales a una aplicación web imposibilitaba restringir el acceso a la información privada, proceso que era repetitivo cada vez que se visitaba una nueva página del sistema.

Para mitigación de este proceso, se utilizó el concepto de cookies. Pequeños archivos que se poblaban de información al ingresar a un sitio web correctamente, la información, como páginas visitadas, información de preferencias en páginas y otra información no sensible, es almacenada en el navegador. Información de sesión no sensible son guardados en la aplicación cliente, denominado cookies de sesión. Su finalidad es no estar iniciando sesión a cada momento (evitar compartir las credenciales por internet por cada visita).  están reguladas por estándares y tienen tiempo de vencimiento o de vida. La desventaja potencial es muy evidente, pueden ser seguidos

e incluso robados y ser perjudiciales dando pauta a robo de identidad o suplantación en servicios de correos, redes sociales y otros servicios.

El auge de las redes sociales, específicamente de Twitter en el siglo XIX surgió la necesidad de crear un método standard para la delegación de seguridad en sus aplicaciones. Oficialmente fue creado OAuth versión 1. Protocolo estándar el cual permite compartir una porción de la identidad del usuario sin comprometer la seguridad. La primera versión presento desventajas considerables como el no tener soporte para aplicación no basada en web y la larga duración de los tokens generados, entre otras.

Actualmente, el cibercrimen sigue creciendo e innovándose, creando la necesidad de poseer otros mecanismos de autenticación. 

En el contexto empresarial, el ingenio azucarero donde se originó la oportunidad de mejora, cuenta actualmente con procesos de negocio que utilizan sistemas basados web. Implementan procesos de seguridad dirigida al acceso y control de acceso a nivel local.

Sin embargo, en el área de suministros, estas aplicaciones no están concluidas y no poseen los métodos de autenticación y autorización, siendo vulnerables en ambientes internos e imposibilitan desplegarlos en ambientes externos.


### **Justificación**

Salvaguardar la identidad de cada usuario, proteger los recursos y tener acceso desde cualquier parte del mundo de forma segura a los sistemas de información es una prioridad al momento de crear sistemas y/o aplicaciones web. Los métodos de autenticación por medio de

credenciales (usuario y contraseña) ha dejado de ser seguros por poseer muchas deficiencias por mencionar que son creadas por los usuarios, las formas de robo, suplantación, estafas, el aprovechamiento de vulnerabilidades de los sistemas, software malicioso entre otros siguen creciendo y en constante cambio.

El estudio e implementación del protocolo de Autenticación Web Authentication (WebAuth) y el protocolo OAuth2 permitirá reforzar la seguridad en los proyectos empresariales, educativos, no lucrativos, etc.

Web Authentication ofrece reglas, políticas, buenas practica y métodos de seguridad informática para autenticación en plataformas web, basado en seguridad biométrica como recurso principal, evitando enviar credenciales cifradas por medio de la red interna o vía internet mitigando el riesgo del Hacking.


OAuth2 por su parte brinda flujos de autorización específicos para aplicaciones web, aplicaciones de escritorio, teléfonos móviles y dispositivos de sala de estar, protegiendo y administrado los recursos del sistema web 

Los protocolos WebAuthn y OAuth2 son adecuados para solventar las deficiencias en el sistema web de la empresa azucarera en el área de Suministros, donde se encontró vulnerabilidades de seguridad y deficiencias en el proceso. Se mejora la arquitectura para poder registrar usuarios, tener trazabilidad de la información y desplegar el sistema web por vía local e internet.

Aportará contenido de estudio para docentes, alumnos y personas interesadas en el tema. Por medio de la implementación los interesados podrán realizar comparativas con otros protocolos existentes.

## PLANTEAMIENTO DEL PROBLEMA

Actualmente la empresa azucarera posee sistemas y herramientas para toma de decisiones por cada área. Un módulo web que está en uso en el área de Suministros para toma de decisiones esta incompleto. No poseen mecanismos de autenticación, autorización y control de acceso por lo tanto no se puede registrar a ningún otro usuario en el sistema web, y no es accesible por el personal operativo del área de Suministros, quienes no pueden alimentar de información de forma directa al sistema web. Cada subjefe del área de Suministros descarga diariamente un archivo de tipo Excel de Microsoft Office, que contiene una plantilla para ser llenada por el personal operativo del área, posteriormente se unifica la información por el subjefe y es enviada por medio de correo electrónico al gerente del área de Suministro.

. La distribución de la información confidencial que contiene este archivo no puede ser controlada, y no puede ser protegida, representando un riesgo y generando vulnerabilidades de seguridad en el proceso. Además la información no es oportuna por ser ingresada y unificada de forma manual, no es confiable por no poseer procesos de validación y corrección de errores y, se considera poco confiable  integra la información por no tener trazabilidad de modificaciones o alteraciones. Las causas mencionadas anteriormente hacen imposible que el sistema pueda ser desplegado vía internet. La Gerencia General necesita corregir los puntos mencionados y aplicar una solución.


## PREGUNTAS DE INVESTIGACIÓN

- ¿Qué beneficios académicos aportará el estudio y la implementación de los protocolos propuestos?



- ¿Cuáles son las ventajas y desventajas de los protocolos OAuth2 y WebAuth que debe de conocer la empresa azucarera y otras personas interesadas?
- ¿Es seguro y confiable el sistema web del ingenio azucarero innovado con los protocolos OAuth2 y WebAuth?
- ¿La alta gerencia estará dispuesta considerar la aceptación del proyecto luego de evaluar las ventajas y desventajas del nuevo sistema con los protocolos en cuestión?
- ¿Es indispensable que la empresa azucarera cuente con dispositivos y equipos con tecnología biométrica para la realización del proyecto?
- ¿Es viable para la empresa azucarera, la adquisición de dispositivos o equipo de cómputo con tecnología biométrica?
- ¿El área de TI considerará implementar los protocolos propuestos en los sistemas web ya existentes?

### **OBJETIVO GENERAL**

Innovar la seguridad en la autenticación de usuarios y el control de accesos en sistemas o aplicaciones web existentes integrando los protocolos OAuth2 y el nuevo protocolo WebAuth para brindar nueva experiencia,  nimiento a los usuarios y beneficios a los procesos de la empresa azucarera.

### **OBJETIVOS ESPECÍFICOS**

- Brindar información académica actualizada, a personas interesadas sobre protocolos de seguridad WebAuth y OAuth2 con referencia a la autenticación de usuarios y control de acceso a recursos de un sistema web.

- Implementar e integrar exitosamente los protocolos OAuth2 y WebAuth en un sistema web empresarial ya existente.
- Comprobar los beneficios y las deficiencias que afirman las entidades creadoras de cada protocolo.
- Mitigar o disminuir el riesgo de robo de contraseñas, filtraciones de datos y robo de identidad.
- Beneficiar a la empresa azucarera con la entrega de un software web, confiable, seguro y de calidad.
- Incentivar a la empresa azucarera, a innovar los procesos, con tecnología actualizada en tema de seguridad.
- Adquirir conocimientos, habilidades, aptitudes, y mejorar la resiliencia por medio de proyecto propuesto.

## **VIABILIDAD**

### **MERCADO**

El protocolo OAuth2 es conocido en el país de Guatemala, muchas empresas lo implementan, ya sea por aplicaciones propias o de terceros. WebAuth por su parte es un protocolo lanzado en el 2019 el cual ha cobrado fuerza en la actualidad. Ambos son protocolos oficiales y estándares para la seguridad y por su adaptabilidad y funcionamiento puede ser implementado en cualquier sistema o aplicación web existente, además los beneficios que ofrecen la combinación de ambos protocolos hacen que sea atractivo para las empresas.

### **SOPORTE**

Los creadores de WebAuth y OAuth2 han innovado constantemente los protocolos haciéndolo más fáciles de implementar y de mantener los sistemas o aplicaciones que integran dicho protocolo. Por estar codificado en JavaScript, el cual es una tendencia en la actualidad, brinda una fácil comprensión del proceso y resultado de cada protocolo reduciendo el tiempo de aprendizaje.

## **TÉCNICO**

Será limitada inicialmente la implementación, WebAuth utiliza datos biométricos de los diferentes dispositivos o llaves de acceso externos como USB de acceso, dispositivos de confianza, etc. Por lo cual se necesitaría una inversión inicial para su correcto funcionamiento. Las computadoras del área de suministros, excepto la del gerente de suministros, son equipos de escritorio. Con la alternativa de utilizar Windows Hello por medio de PIN que viene integrado con Windows 8 y Windows 10, tomando medidas de seguridad alternas. El área de TI tiene por política interna, acceso remoto a los equipos suponiendo un riesgo medio a la seguridad.

## **ADMINISTRATIVA**

Se requiere autorización de alta gerencia administrativa para la implementación con datos reales y en tiempo real, lo que conlleva a un trámite formal entre el desarrollador del proyecto y la empresa, además del compromiso pactado por medio de un contrato de confidencialidad que lleva un tiempo prudencial el realizar el trámite con un riesgo inherente de no aprobación.