**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**

**Antecedentes**

“En el año 2015, el costo promedio de una violación corporativa aumentó 7.6 por ciento (…), 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 (Deloitte & Touche y Arthur Andersen, Julio 2,016, Un mundo más allá de las contraseñas. Recuperado de <https://www2.deloitte.com/co/es/pages/audit/articles/un-mundo-mas-alla-de-las-contrasenas.html)>”.

La autenticación o autentificación ​ deriva de auténtico que significa “Acreditado como cierto y verdadero por los caracteres o requisitos que en ello concurren” (Diccionario de la Real Academia Española (s/f). Recuperado de <https://dle.rae.es/autentico>).

Autorización viene del adjetivo autorizar cuya definición es: “Dar o reconocer a alguien facultad o derecho para hacer algo (Diccionario de la Real Academia Española (s/f) Recuperado de https://dle.rae.es/Autorizar).

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 tecnología) 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. (Día de la Contraseña: una breve historia de su origen, mayo 4 del 2,017. Recuperado de <https://www.welivesecurity.com/la-es/2017/05/04/dia-de-la-contrasena-origen/>).

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. (Día de la Contraseña: una breve historia de su origen, mayo 4 del 2,017. Recuperado de <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. Actualmente, el cibercrimen sigue creciendo e innovándose, creando la necesidad de poseer otros mecanismos de autenticación

**Métodos De Autenticación Y Autorización Anteriores A WebAuth Y OAuth2**

**compartir usuario y contraseña**. Al otorgar las credenciales a una Api no es posible restringir el acceso a la información privada. “Imagina a día de hoy, donde infinidad de aplicaciones quieren llevar a cabo algunas acciones con tu perfil de Facebook, normalmente publicar en tu muro y obtener tu lista de amigos. Si utilizáramos este sistema le daríamos acceso a absolutamente todo, y podría recuperar conversaciones privadas, nuestras fotos, seguir a gente que no queremos, eliminar amigos que si queremos… ¿te haces una idea no?” (OAuth 2.0, OpenID Connect y JSON Web Tokens (JWT) ¿Qué es qué?, abril 14 del 2,019. Recuperado de [https://www.returngis.net/2019/04/oauth-2-0-openid-connect-y-json-web-tokens-jwt-que-es-que](https://www.returngis.net/2019/04/oauth-2-0-openid-connect-y-json-web-tokens-jwt-que-es-que/))

**cookies**. 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. Al igual, datos de sesión no sensibles son guardados para no estar iniciando sesión a cada momento y aunque estén reguladas por estándares y tengan tiempo de vencimiento, estos datos 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.

**api key**. Se considera un método seguro si esta conjuntamente con otro mecanismo de autenticación. Son usadas para autenticación de proyectos no de usuarios otorgando un acceso total a la aplicación, además son usadas desde el cliente y puede ser robadas con facilidad por su alta vulnerabilidad.

**oauth versión 1**. Protocolo estándar el cual permite compartir una porción de la identidad del usuario sin comprometer la seguridad. La primera versión posee desventajas considerables como el no tener soporte para aplicación no basadas en web y la larga duración de los tokens generados, entre otras.

**Justificación**

Salvaguardar la identidad de cada usuario, proteger los recursos en internet y tener acceso desde cualquier parte del mundo de forma segura es una prioridad al momento de crear sistemas y/o aplicaciones. 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) permitirá reforzar la seguridad en los proyectos empresariales, educativos, no lucrativos, etc.

Aportará contenido de estudio para docentes, alumnos y personas interesadas en el tema.

Y 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. Suministros es el área que posee proyectos por implementar e incompletos. Posee sistema web oficial que brinda información para toma de decisiones el cual está incompleto por ser considerado prioridad media en comparación a otros proyectos para la misma área. Es usado por el gerente de suministro quien procesa la información y presenta a su jefe inmediato de forma impresa. La alimentación del sistema la realiza el gerente de suministro. Cada jefe por departamento del área de suministros descarga la información del sistema oficial en un archivo de tipo Excel de Microsoft Office y la envían por medio de correo electrónico puesto que no tienen permiso, por parte del gerente, de utilizar la aplicación ya que no posee mecanismos de autenticación, autorización y control de acceso, aunque puede ser accedida por medio de una URL exponiendo información sensible al público interno. Además, por ser una empresa con políticas estrictas, información sensible, critica y confidencial, los métodos de acceso por medio de usuario y contraseña no se consideran viables para publicar un servicio en internet por lo cual todas las herramientas solo funcionan dentro de la red interna confiando la presentación de la información final de forma presencial o correo electrónico.

Preguntas de Investigación

¿Qué beneficios académicos aportara los protocolos propuestos a implementar?

¿Qué beneficios, a nivel empresarial, aportara los protocolos propuestos a implementar?

¿Qué desventajas, a nivel empresarial, presenta la implementación de los protocolos propuestos?

¿El sistema web integrado con los protocolos OAuth2 y WebAuth es confiable y seguro?

¿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?

¿Sera viable la adquisición de dispositivos o equipo de cómputo con tecnología biométrica?

¿El área de TI considerara implementar los protocolos 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 y por ende mitigar o disminuir el riesgo de robo de contraseñas, filtraciones de datos y robo de identidad ofreciendo una nueva experiencia y conocimiento a personas interesadas y brindar beneficios directos a los procesos implementados en la empresa azucarera

Objetivos Específicos

Brindar información académica 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 que ofrecen los protocolos según los creadores de cada protocolo.

Beneficiar a una empresa privada con la entrega de un software confiable y de calidad

Adquirir nuevas habilidades y aptitudes por medio de proyecto propuesto.

Viabilidad

*Mercado*

El protocolo OAuth2 es conocido en el país de Guatemala ya que muchas empresas lo implementan, ya sea por aplicaciones propias o de terceros. WebAuth por su parte es un protocolo lanzado en el 2,019 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 OAouth2 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 compresión del proceso y resultado de cada protocolo reduciendo el tiempo de aprendizaje

*Técnico*

Sera limitada inicialmente la implementación puesto que 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 ya que todas 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 ya que 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.

Alcance A

*Geográfico*

El proyecto se implementará en un Ingenio Azucarero dentro de los límites del municipio de Santa Lucia Cotzumalguapa, departamento de Escuintla en el país de Guatemala.

*Institucional*

El proyecto involucra a la alta gerencia por aprobación de utilización de información, gerencia del área de suministros quien dará el visto bueno del funcionamiento y el resultado deseado, el área de TI que evaluará la tecnología, la seguridad y los costos de implementación y demás gerencias de la empresa como candidatos a optar por la implementación en sus herramientas y sistemas existentes.

*Personal*

Se pretende la donación del software propuesto con la implementación de los protocolos en cuestión, y participación de los procesos administrativos y legales que conlleve la implementación del proyecto sin embargo queda fuera el soporte y mantenimiento después de la aceptación del producto ya lanzado en producción.

*Temporal*

El tiempo de implementación en sistema propuesto no excederá de 3 meses, se asumirá 15 días posteriores, para corrección de fallas y cambios no significativos. Se pactará 15 días como máximo la resolución de aprobación o desaprobación del resultado del proyecto dando como finalizado el proyecto en un máximo de 4 meses.

*Temático*

El presente proyecto estará dirigido al público en general con un rango de edad mínimo de 15 años en adelante por tema de búsqueda y comprensión de términos técnicos y madurez mental.