ANÁLISIS PARA EL DESARROLLO DE UN SISTEMA DE INFORMACIÓN DEL SISTEMA ELÉCTRICO DE POTENCIA DE UNA ZONA DE OPERACIÓN DE TRANSMISIÓN UTILIZANDO TECNOLOGÍAS WEB (SISEPW)

1st José Rafael Plancarte Oliva
División de Posgrado e Investigación
Tecnológico Nacional de México
Campus Acapulco
Acapulco, México
mm20320013@acapulco.tecnm.mx

2nd Eduardo de la Cruz Gámez
División de Posgrado e Investigación
Tecnológico Nacional de México
Campus Acapulco
Acapulco, México
eduardo.dg@acapulco.tecnm.mx

3rd Francisco J. Gutiérrez Mata
División de Posgrado e Investigación
Tecnológico Nacional de México
Campus Acapulco
Acapulco, México
francisco.gm@acapulco.tecnm.mx

4th Rafael Hernández Reyna
División de Posgrado e Investigación
Tecnológico Nacional de México
Campus Acapulco
Acapulco, México
rafael.hr@acapulco.tecnm.mx

5th Eduardo Viveros Capote
Zona de Operación de Transmisión Guerrero Morelos
CFE Transmisión
Acapulco, México
eduardo.viveros@dt.cfe.mx

6th Jorge Ortiz García
Zona de Operación de Transmisión Guerrero Morelos
CFE Transmisión
Acapulco, México
jorge.ortizga@dt.cfe.mx

***Resumen*— Desarrollar un Sistema de Información Web que recopile los datos generados en tiempo real por el Sistema Eléctrico de Potencia (SEP) perteneciente al Sistema Eléctrico Nacional (SEN) de la Comisión Federal de Electricidad (CFE), el cual es monitoreado permanentemente por la Zona de Operación de Transmisión.**

Palabras claves— Sistema Eléctrico de Potencia (SEP), sistema de Información Web, adquisición de datos, SCADA, seguridad informática.

***Abstract*— Develop a Web Information System that collects the data generated in real time by the Electric Power System (EPS) belonging to the National Electric System (NES) of the Comisión Federal de Electricidad (English: Federal Electricity Commission) (CFE), which is permanently monitored by the Zone of Transmission Operation.**

***Keywords*— Electric Power System (SEP), Web Information system, data acquisition, SCADA, Informatic security.**

I. INTRODUCCIÓN

El presente artículo tiene como finalidad desarrollar una propuesta de solución que permita realizar un Sistema de Información Web que facilite a los ingenieros operadores de una Zona de Operación de Transmisión la obtención de información en tiempo real del Sistema Eléctrico de Potencia sin tener que estar dentro de la sala de Operación y así poder tomar decisiones concerniente a los eventos ocurridos en el Sistema Eléctrico de Potencia (SEP).

Con la propuesta de este trabajo se busca reducir los tiempos de reacción ante los imprevistos ocurridos, lo cual permitirá reducir los gastos de combustibles de los vehículos utilitarios así como los tiempos de traslado a la sala de operación.

A. Sistemas web

Se denomina sistema web a aquellas aplicaciones de software que puede utilizarse accediendo a un servidor web a través de Internet o de una intranet mediante un navegador [1].

Las aplicaciones web pueden ser usadas por varios usuarios al mismo tiempo. Al estar toda la información centralizada no se tendrá que compartir pantallas o enviar emails con documentos adjuntos. Varios usuarios pueden ver y editar el mismo documento de manera conjunta.

Además son accesibles desde cualquier lugar. Se puede trabajar desde una PC, un portátil, un móvil o una tablet, desde la oficina, un parque o un aeropuerto.

Existe solo una versión de la aplicación web en el servidor, por lo que no hay que distribuirla entre las demás computadoras. El proceso de actualización es rápido y limpio [1].

B. Sistema de información

Un sistema de información es un conjunto de datos que interactúan entre sí con un fin común [2].

En informática, los sistemas de información ayudan a administrar, recolectar, recuperar, procesar, almacenar y distribuir información relevante para los procesos fundamentales y las particularidades de cada organización [2].

La importancia de un sistema de información radica en la eficiencia en la correlación de una gran cantidad de datos ingresados a través de procesos diseñados para cada área con el objetivo de producir información válida para la posterior toma de decisiones [2].

C. SCADA

Acrónimo de Supervisory Control And Data Acquisition, el sistema SCADA es una herramienta de automatización y control industrial utilizada en los procesos productivos que puede controlar, supervisar, recopilar datos, analizar datos y generar informes a distancia mediante una aplicación informática. Su principal función es la de evaluar los datos con el propósito de subsanar posibles errores [3].

Los elementos que conforman un Sistemas SCADA se representan gráficamente en la Fig.1, mismos que se describen textualmente a continuación:

HMI: Es la interfaz que conecta al hombre con la maquina presentando los datos del proceso ante el operario mediante un sistema de monitoreo. Además, controla la acción a desarrollar a través de una pantalla, en la actualidad táctil.

Sistema de supervisión o MTU (Ordenador/Computadora): Tiene la función de recopilar los datos del proceso y enviar las instrucciones mediante una línea de comandos.

Unidades Terminales Remotas (RTU): Son microprocesadores (Ordenadores Remotos) que obtienen señales independientes de una acción para enviar la información obtenida remotamente para que se procese. Se conectan a sensores que convierten las señales recibidas en datos digitales que lo envían al ordenador o sistema de supervisión (MTU)

PLC: Denominados comúnmente autómatas programables, estos son utilizados en el sistema como dispositivos de campo debido a que son más económicos, versátiles, flexibles y configurables que las RTU comentadas anteriormente.

Red o sistema de comunicación: Se encarga de establecer la conectividad del ordenador (MTU) a las RTU y los PLC. Para ello utiliza conexiones vía modem, Ethernet, Wifi o fibra óptica.

Sensores: Son dispositivos que actúan como detectores de magnitudes físicas o químicas, denominadas variables de instrumentación, y las convierten en variables o señales eléctricas.

Actuador: Es un dispositivo mecánico que se utiliza para actuar u ofrecer movimiento sobre otro dispositivo mecánico [3].

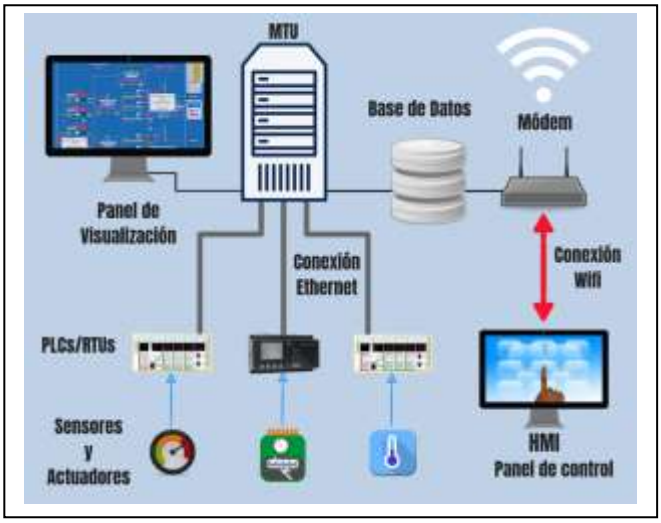

Fig. 1. Diagrama básico de un Sistema SCADA.

D. Seguridad Informatica

La Seguridad Informática (SI) es el área que se enfoca en "la protección de la infraestructura computacional y todo lo relacionado con esta, especialmente, la información contenida o circulante" [18].

La SI llega a ser un área de vital importancia dentro de la Ingeniería de Software (IS), ya que trata de minimizar los riesgos asociados al acceso y utilización de determinado sistema de forma no autorizada y en general malintencionada.

La SI tiene el objetivo de minimizar los riesgos asociados al acceso y utilización de determinado sistema de forma no autorizada y en general malintencionada [19].

Para afrontar el establecimiento de un sistema de seguridad es necesario conocer [20]:

Cuáles son los elementos que componen el sistema: esta información se obtiene mediante entrevistas con los responsables o directivos de la organización, para lo que previamente hay que realizar un estudio de los riesgos que puedan presentar.

Cuáles son los peligros que afectan al sistema, accidentalmente o provocados: estos datos se deducen de los aportados tanto por la organización como por el estudio y prueba del propio sistema.

Cuáles son las medidas que deberían adoptarse para conocer, prevenir, impedir, reducir y controlar los riesgos potenciales, definiendo los servicios y mecanismos necesarios para minimizarlos.

La Seguridad Informática consta de 5 principales fundamentos [19, 20]:

Integridad: garantiza que los datos no sean modificados desde su creación sin autorización y que ningún intruso pueda capturar y modificar los datos en tránsito.

Confidencialidad: garantiza que la información, almacenada en el sistema informático o transmitida por la red,

solamente va a estar disponible para aquellas personas autorizadas a accederla.

Disponibilidad: garantiza el correcto funcionamiento de los sistemas de información y su disponibilidad en todo momento para los usuarios autorizados.

No repudio: garantiza la participación de las partes en una comunicación. El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no puede negar dicha acción.

Autenticación o Autenticidad: asegura que sólo los individuos autorizados tengan acceso a los recursos.

E. Seguridad en base de datos

La seguridad en una base de datos contiene las mismas dificultades a las que se enfrenta la información, esta es el garantizar la integridad, la disponibilidad y la confidencialidad. Un Sistema Gestor de Base de Datos (SGBD) debe suministrar mecanismos que ayuden en esta tarea [17].

Algunos de los mecanismos que ayudan en la seguridad de datos son los siguientes:

1) Control de Acceso

El administrador de la base de datos (DBA) es el responsable superior de declarar las reglas dentro del SGBD. Este es el responsable de conceder o eliminar privilegios, crear o excluir usuarios, y atribuir de un nivel de seguridad a los usuarios del sistema, de acuerdo con la política de la empresa.

2) Control de Inferencias

Es un mecanismo de seguridad para base de datos estadísticas que trabaja protegiendo informaciones estadísticas de un individuo o de un grupo.

La base de datos puede contener informaciones confidenciales sobre individuos. Los usuarios tienen permiso sólo para recuperar informaciones estadísticas sobre poblaciones y no para recuperar datos individuales.

3) Control de Flujo

Es un mecanismo que previene que las informaciones fluyan por canales secretos y violen la política de seguridad al alcanzar usuarios no autorizados. Este regula la distribución o flujo de información entre objetos accesibles.

Los controles de flujo tienen la finalidad de verificar si las informaciones contenidas en algunos objetos de menor protección.

4) Criptografía de Datos

Es una medida de control final, utilizada para proteger datos sigilosos que se transmiten por medio de algún tipo de red de comunicación.

Esta también se puede usar para ofrecer protección adicional para que partes confidenciales de una base de datos no sean accedidas por usuarios no autorizados. Para eso, los datos están codificados a través de la utilización de algún algoritmo de codificación.

La criptografía permite disfrazar el mensaje para que, aún con el desvío de la transmisión, el mensaje no sea revelado.

5) Usuarios

Comprende a los usuarios y al esquema de la base de datos donde cada base de datos tiene una lista de nombres de usuario. Para acceder a una base de datos, un usuario debe usar una aplicación de este tipo e intentar una conexión con un nombre de usuario valido.

Cada nombre tiene una contraseña asociada para evitar el uso sin autorización. Deben estar implementados diferentes perfiles de usuario para diferentes tareas en la base de datos, con el enfoque de que cada aplicación/usuario tiene su necesidad de acceso.

6) Dominio de seguridad

Donde cada usuario tiene el dominio de seguridad, un conjunto de propiedades que determinan cosas como acciones (privilegios y roles) disponibles para el usuario; cotiza los tablespaces (espacio disponible en el disco) del usuario; limita los recursos de sistema del usuario. Las tablas (tablespaces) del sistema, como system, deben estar protegidas de accesos de usuarios diferentes de los usuarios del sistema.

7) Autoridad.

Las autoridades suministran un método para agrupar privilegios y controlar el nivel de acceso de los administradores y operadores de la base de datos en relación al mantenimiento y operación de permitidas. Las especificaciones de la base de datos están almacenadas en catálogos de la propia base de datos.

Las autoridades del sistema están asociadas a miembros de grupos y están almacenados en el archivo de configuración administrativa de la base de datos. Este archivo define las concesiones de acceso y lo que podrá ser ejecutado de acuerdo con cada grupo

8) Privilegios

Los privilegios son únicos dados a cada usuario o grupo estos definen permisos para los tipos de autorización. Con los privilegios es posible autorizar al usuario a modificar o alcanzar un determinado recurso de la base de datos. Los privilegios también son almacenados en catálogos de la propia base de datos, visto que los grupos autoridad ya tienen grupos predefinidos de privilegio conceden implícitamente privilegios a sus miembros.

a) Discrecionales

El SGBD debe ofrecer acceso selectivo para cada relación de la base de datos basándose en cuentas específicas. Las operaciones también pueden ser controladas; deben tener una cuenta no necesariamente habilitada del poseedor de todas las funcionalidades ofrecidas por el SGBD.

Informalmente existen dos niveles para la atribución de privilegios para el uso del sistema de base de datos:

- El nivel de cuenta: En ese nivel, el DBA establece los privilegios específicos que cada cuenta tiene, independientemente de las relaciones en la base de datos.
- El nivel de relación (o tabla): En ese nivel, el DBA puede controlar el privilegio para acceder a

cada relación o vista individual en la base de datos.

b) Revocación

En algunos casos, interesa conceder un privilegio temporal a un usuario. Por eso, es necesario un mecanismo para la revocación de privilegios.

En SQL el modo REVOKE se introducen con el intento de cancelar privilegios.

9) Controles de acceso

a) Obligatorio y seguridad para multi-nivel

En este método, el usuario no tiene un término medio, o tiene o no tiene privilegios, siendo utilizado normalmente en BD que clasifican datos de usuarios, dónde es necesario un nivel de seguridad más alto. Normalmente se utilizan en sistemas gubernamentales, militares o de inteligencia, así como industriales y corporativas.

Las clases de seguridad típicas son altamente sigilosas (top secret, TS), secreta (secret, S), confidenciales (confidential, C) y no clasificada (unclassified, U), en el que TS es el nivel más alto y U el más bajo. De una forma general, los mecanismos de control de acceso obligatorio imponen seguridad multinivel, ya que exigen la clasificación de usuarios y de valores de datos en clases de seguridad e imponen las reglas que prohíben el flujo de información a partir de los niveles de seguridad más altos hacia los más bajos.

b) Basado en roles

Es un enfoque para restringir el acceso a usuarios autorizados y una alternativa a los sistemas de controles de acceso del tipo MAC y DAC.

La idea central del RBAC es que los permisos de acceso están asociados a roles, y estos roles están asociados a usuarios. Los roles son creados de acuerdo con diferentes cargos en una organización, y los usuarios están asociados a roles de acuerdo a su responsabilidades y cualificaciones. Se pueden designar varios individuos a un mismo rol. Los privilegios de seguridad comunes a un rol se conceden al nombre de este, y cualquier individuo designado para ese rol automáticamente tendrá esos privilegios concedidos.

El uso del modelo RBAC es un objeto altamente deseado para seleccionar los principales requisitos de seguridad de las aplicaciones basadas en web.

c) Utilizando Triggers.

Con la utilización de los Triggers es posible crear mecanismos de seguridad más complejos que pueden ser disparados cada vez que se llama una acción. Si el comando ejecutado por el usuario no es validado por los Triggers, salta un error en el cuerpo del propio Trigger para impedir que la tabla sea modificada indebidamente.

d) Utilizando Views.

Las views constituyen otro método de control de acceso, normalmente son utilizadas para restringir el acceso directo a los datos. Con la view es posible permitir el acceso de un usuario concediendo privilegios, ocultar líneas y columnas de informaciones confidenciales o restringir a los residentes en la tabla original de las indicaciones del SQL. Los privilegios y concesiones están definidos solamente en la view, y no afectan a la tabla base, estando el acceso de los usuarios delimitado por la view, la cual se genera creando un subconjunto de datos en la tabla referenciada. La opción With Verification provee mayor seguridad porque no permite al usuario modificar las líneas de la tabla sin tener los privilegios de lectura dentro de la view [17].

II. ANTECEDENTES

Considerada como la primera Zona de Operación de Transmisión (antes Sub-área de Control) en el territorio Nacional, la Zona de Operación de Transmisión Guerrero Morelos se ubica en la ciudad de Acapulco, Guerrero. Fue creada a partir de la interconexión del Sistema Colotlipa-Acapulco en Mayo de 1973 al Sistema Interconectado Nacional.

Se tiene conocimiento que la Zona de Operación de Transmisión surge en el tablero de la subestación “El Quemado” ubicada en el poblado con el mismo nombre, junto al operador de la misma. Las primeras relatorías de los que se tiene referencia datan de Abril de 1974.

Se hace oficial su existencia el 20 de Septiembre de 1976 atreves del convenio CFE-SUTERM No. 127-76, en donde se constituye de manera oficial el Despacho Nacional de Carga, así como los Despachos de Carga Occidental, Peninsular, Noroeste, Noreste, Norte, Mexicali y el Despacho de Carga Acapulco (hoy Zona de Operación de Transmisión Guerrero Morelos) [4].

La Zona de Operación ejerce su ámbito de influencia sobre las redes de 230 y 115 Kv´s en una extensión geográfica de 53,550 Km2 que corresponden con los estados de Guerrero y Morelos y una pequeña parte del estado de Oaxaca.

Mantiene relaciones de carácter técnico administrativo con la División de distribución Centro Sur; La Gerencia Regional de Transmisión Central, las Gerencias Regionales: Hidroeléctrica Ixtapantongo y Termoeléctrica Central, la Residencia de Obras Zona Centro Sur.

III. PLANTEAMIENTO DEL PROBLEMA

La principal problemática es la falta de un sistema de visualización remota de la información en tiempo real que facilite de manera segura y confiable la información necesaria fuera de la sala de operación para una toma de decisión adecuada ante los imprevistos ocurridos en el Sistema Eléctrico de Potencia (SEP) para el personal de la Comisión Federal de Electricidad (CFE) Transmisión.

Una necesidad de la CFE Transmisión es el acceso remoto a la información generada en tiempo real por el sistema SCADA y trasmitida a la sala de operación.

La actualización de la información solo puede ser visualizada dentro del lugar de trabajo en la sala de operación, la cual cuenta con una red local pero sin conexión externa, esto no permite que se monitoree y visualice la información fuera de dicha sala, con la introducción de la propuesta del Sistema

de Información Web y su aplicación, se contempla mejorar el desempeño del servicio del Sistema Eléctrico de Potencia (SEP).

Por otra parte, la propuesta del Sistema de Información Web podrá mostrar en tiempo real los indicadores técnicos de los elementos en servicio y el estado en que se encuentran, de esta forma el operador tomará decisiones oportunas ante los eventos que se puedan presentar.

IV. Objetivo general

Analizar la propuesta de desarrollo del Sistema de Información Web para consulta de información de las condiciones del Sistema Eléctrico de Potencia (SEP) en tiempo real.

V. Objetivos específicos

Analizar una propuesta de desarrollo de un Sistema de Información Web para la visualización de eventos del sistema SCADA que auxilie a los ingenieros de la Zona de Operación de Transmisión Guerrero Morelos en la operación en tiempo real del Sistema Eléctrico de Potencia a su cargo.

Analizar las especificaciones de los equipos para realizar la correcta operación de los mismos.

Contrastar la funcionalidad del Sistema de Información Web en el proceso de generación, transmisión, distribución y operación del Sistema Eléctrico de Potencia.

Analizar el sistema de recolección de datos para diseñar la propuesta de Telecomunicaciones y el Sistema de Información Web.

VI. Metodología

Un modelo de proceso de software es una representación simplificada de este proceso. Un modelo de actividad del proceso muestra las actividades y su secuencia, pero quizá sin presentar los roles de las personas que intervienen en esas actividades.

En este caso se pretende utilizar el modelo de cascada (waterfall), el cual toma las actividades fundamentales del proceso de especificación, desarrollo, validación y evolución, para después representarlos como fases separadas del proceso, representadas en la Fig. 2, tal como especificación de requerimientos, diseño de software, implementación, pruebas, etcétera.

A. Análisis y definición de requerimientos

Los servicios, las restricciones y las metas del sistema se establecen mediante consulta a los usuarios del sistema. Luego, se definen con detalle y sirven como una especificación del sistema.

B. Diseño del sistema y del software

El proceso de diseño de sistemas asigna los requerimientos, para sistemas de hardware o de software, al establecer una arquitectura de sistema global. El diseño del software implica identificar y describir las abstracciones fundamentales del sistema de software y sus relaciones.

C. Implementación y prueba de unidad

Durante esta etapa, el diseño de software se rea liza como un conjunto de programas o unidades del programa. La prueba de unidad consiste en verificar que cada unidad cumpla con su especificación.

D. Integración y prueba de sistema

Las unidades del programa o los programas individuales se integran y prueban como un sistema completo para asegurarse de que se cumplan los requerimientos de software. Después de probarlo, se libera el sistema de software al cliente.

E. Operación y mantenimiento

Por lo general (aunque no necesariamente), ésta es la fase más larga del ciclo de vida, donde el sistema se instala y se pone en práctica. El mantenimiento incluye corregir los errores que no se detectaron en etapas anteriores del ciclo de vida, mejorar la implementación de las unidades del sistema e incrementar los servicios del sistema conforme se descubren nuevos requerimientos.

Esta metodología ha sido elegida porque nos lleva paso a paso durante el desarrollo de nuestro software, estableciendo en primera instancia los requisitos de los usuarios, que en este caso son los ingenieros encargados de la Zona de Operación de Transmisión [5].

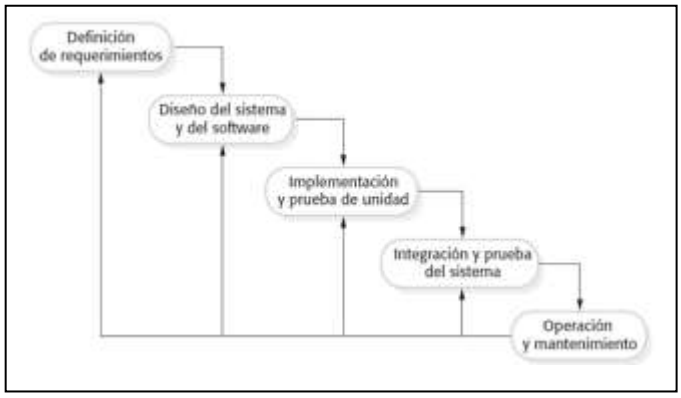

Fig. 2. El modelo de cascada.

VII. Análisis de requerimientos

A. Requerimientos de usuario

La falta de un sistema de visualización remota de la información en tiempo real que brinde de manera segura y confiable la información necesaria para una adecuada toma de decisiones en situaciones de eventos en la Sistema Eléctrico de Potencia para el personal de la Zona de Operación de Transmisión.

B. Requerimientos del sistema

1. Acceso a información actualizada generada en tiempo real por el sistema SCADA (Supervisión, Control y

Adquisición de Datos) y transmitida a las instalaciones de la ZOT.

2. La actualización de la información se podrá ver fuera del lugar de trabajo en la sala de operación que tiene una red local pero no una conexión externa.

3. Permitir el seguimiento y visualización de información fuera de la sala de operación.

4. Un Sistema de Información Web y una aplicación que tiene como objetivo mejorar el desempeño del servicio del Sistema Eléctrico de Potencia (SEP).

VIII. PROPUESTA SOLUCIÓN

Con el propósito de presentar una propuesta de solución se revisará en conjunto con el personal del Centro de Control todos los requerimientos y necesidades sobre el problema a resolver, en este caso para implementar un Sistema de Información Web que permita visualizar los datos del sistema SCADA en tiempo real de manera remota para agilizar la toma de decisiones de los ingenieros operadores.

La solución propuesta se basa en una herramienta informática que se pueda utilizar accediendo a un servidor web, ya que son programas diseñados para ser ejecutados en teléfonos, tabletas y otros dispositivos móviles, que permiten al usuario realizar actividades profesionales, acceder a servicios, mantenerse informado, entre otro universo de posibilidades.

Para el entorno de desarrollo se pretende utilizar tecnologías web como HTML, CSS y JavaScript, con la capacidad de trabajar en iOS y Android como una aplicación nativa. No necesariamente se tiene que instalar la aplicación en el teléfono inteligente ya que permitirá acceder a través de un navegador.

A. Elementos de la interfaz

Se propone que en primera instancia se encuentre el nombre de la aplicación, con el color verde que caracteriza a la Comisión Federal de Electricidad.

En seguida se observaría que se encuentra un área para ingresar el usuario, el cual aún no se decide si será el nombre del trabajador, matricula, número de plaza o contrato.

Como tercer elemento se encontraría el área para ingresar la calve de acceso o contraseña.

El cuarto elemento será un botón de inicio de sesión, el cual validará si los datos de usuario y contraseña son correctos o no, si son correctos dará acceso a la visualización de la información, de lo contrario negara el acceso.

Dentro de esta pantalla principal también encontraremos el logotipo de CFE, el cual nos redireccionará a la página oficial de la Comisión Federal de Electricidad.

Y por último en la parte inferior de la pantalla se encontrarían las redes sociales oficiales de la CFE.

IX. CONCLUSIONES

El artículo propone el desarrollo de una herramienta informática de implementación web que sea de gran utilidad para el sector energético en Zona de Operación de Transmisión Guerrero Morelos, empleando un método de visualización remoto del sistema SCADA.

La herramienta mencionada en este trabajo se encuentra en un estatus de propuesta, es por este motivo que aun no se han obtenido resultados, por lo cual no se conoce el nivel de efectividad y practicidad que se pueda obtener.

Los beneficios establecidos no son solo en los aspectos técnicos, sino que se contribuye plenamente a las ventajas económicas en términos de reducción de costos operativos y de actualización.

En el futuro se tiene la intención de continuar con el desarrollo del sistema propuesto y realizar estudios sobre la seguridad, vulnerabilidades y rendimiento del sistema.

REFERENCIAS

[1] Ltda., A. (s. f.). Ventajas de los sistemas web. Diseño web y páginas web | Marketing Digital | aeurus. Recuperado 15 de mayo de 2021.

[2] Chen, C. Significado de Sistema de información. Significados. 21 Mayo, 2019.

[3] A. (2021, 11 mayo). Qué es un sistema SCADA, para qué sirve y cómo funciona. aula21 | Formación para la Industria.

[4] Comisión Federal de Electricidad. Reglas de Despacho y Operación del Sistema Eléctrico Nacional. Noviembre 2005.

[5] Sommerville, I. Software Engineering (Ninth Edition). Pearson Education. 2011.

[6] Ozdemir, E., Karacor, M. Mobile phone based SCADA for industrial automation, ISA Transactions, Volume 45, Issue 1, 2006.

[7] Chen, Q., Ghenniwa, H., Shen, W. Architecture of a Web-Based Power SCADA System Using J2EE TechnologyInformation Technology for Balanced Manufacturing SystemsWeiming Shen, Editor, Springer series in Computer Science, NY, 2006.

[8] Gligor, A., Turc, T. Development of a Service Oriented SCADA System, Procedia Economics and Finance, Volume 3, 2012

[9] Gustavsson, R. Ensuring Dependability In Service Oriented Computing, in Proc. of The 2006 International Conference Securuty and ManagementHamid R. Arabnia and Selim Aissi, Editor, CSREA Press, Las Vegas, Nevada, USA, 2006.

[10] Gligor, A., Dumitru, C.-D. Agents-Based Distributed Processes Control Systems , in Proc. of “The 5th Edition of the Interdisciplinarity in Engineering International Conference, Tirgu Mures, Rumania, 2011", Petru Maior University Press, 2011.

[11] Robles, R. J., Choi, M.-k. Assessment of the Vulnerabilities of SCADA, Control Systems and Critical Infrastructure Systems, in Int. Journal of Grid and Distributed Computing, vol. 2, No. 2, Osvaldo Gervasi, Editor, SERSC, Republic of Korea, 2009.

[12] Otani T., Kobayashi H. and Koda Y. "Performance evaluation of SCADA system isolating fault section in a demand area power system", Inst. Elect. Eng. Jpn. Trans. Power Energy, vol. 126-B, no. 10.

[13] Paxson V. and Allman M., Computing TCP's retransmission timer, 2000.

[14] Lange D. and Oshima M., "Seven good reasons for mobile agents", Commun. ACM, vol. 42, no. 3, 1999.

[15] Rojas, H., Cadena, E., Hernández, J. M. “Desarrollo de prototipo SCADA para control de nivel de agua en dos contenedores para uso en la Comisión de Agua Potable y Alcantarillado del Municipio de Acapulco (capama), Acapulco, Guerrero, México, 2019.

[16] Ramírez, R., Gutiérrez, F.J., De Jesús A. D. “Desarrollo de un sistema de información web para el seguimiento y control del mantenimiento de infraestructura y equipo”, Acapulco, Guerrero, México, 2020.

[17] Gallardo, G. Seguridad en Base de Datos y Aplicaciones Web.

[18] CDI Centro de Delitos Informáticos. 2017.

[19] Garfinkel, S. Seguridad y Comercio en la Web: McGraw Hill/Interamericana de España. 1999.

[20] Aguilera López, P. (2010). Seguridad informática. México.