FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

ESTUDIO DE FACTIBILIDAD PARA LA MIGRACIÓN DE SISTEMAS DE CONTROL INDUSTRIAL DE EMPRESAS DE GENERACIÓN ELÉCTRICA AL CLOUD

AUTOR

Darwin Geovanny Molina Alvarez

AÑO

2019

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

ESTUDIO DE FACTIBILIDAD PARA LA MIGRACIÓN DE SISTEMAS DE CONTROL INDUSTRIAL DE EMPRESAS DE GENERACIÓN ELÉCTRICA AL CLOUD

Trabajo de Titulación presentado en conformidad con los requisitos

establecidos para optar por el título de Ingeniero en Redes y

Telecomunicaciones

Profesor Guía

Mg. Iván Patricio Ortiz Garcés

Autor

Darwin Geovanny Molina Alvarez

Año

2019

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido el trabajo, estudio de factibilidad para la migración de sistemas de control industrial de empresas de generación eléctrica al cloud, a través de reuniones periódicas con el estudiante, Darwin Geovanny Molina Alvarez, en el semestre 201920, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”.

Iván Patricio Ortiz Garcés
Magister en Redes de Comunicaciones
CI: 0602356776

DECLARACIÓN DEL PROFESOR CORRECTOR

"Declaro haber revisado este trabajo, estudio de factibilidad para la migración de sistemas de control industrial de empresas de generación eléctrica al cloud, de Darwin Geovanny Molina Alvarez, en el semestre 201920, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación".

Milton Neptalí Román Cañizares
Magister en Gerencia de Redes y Telecomunicaciones
CI: 0502163447

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que el presente trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes”.

_____

Darwin Geovanny Molina Alvarez

C.I.: 171434882

AGRADECIMIENTOS

Agradezco en primer lugar a Dios, por darme fuerzas para completar un escalón más en la vida; compañeros y maestros quienes estuvieron pendientes de la realización del presente trabajo.

DEDICATORIA

A mi familia: Estebitan y Estefanía, mis padres, mis hermanos y amigos cercanos por haberme dado ánimo, motivación y fuerza en todo momento para ver la vida desde una perspectiva distinta a la común. Por haberme enseñado lo importante de la vida, los valores que día a día deben ser demostrados e inculcados hacia nuestros hijos.

Gracias por todo mi linda familia.

Darwin Molina.

RESUMEN

En la actualidad es común hablar del término “Cloud”, el cual se refiere al manejo, control y administración de información, aplicaciones, servicios, etc., alojados en servidores en distintas ubicaciones geográficas y a los cuales se puede acceder desde cualquier lugar del mundo únicamente teniendo una conexión simple a Internet. Existen múltiples organizaciones dedicadas a ofrecer el servicio de Cloud Computing como negocio, por ejemplo: Microsoft, IBM, Amazon, etc.

Específicamente, la información que se genera en una central de generación eléctrica a través del sistema de adquisición de datos industriales SCADA (*Supervisory Control And Data Acquisition*), brinda información en tiempo real que permite a los controladores y/o operadores monitorear el normal funcionamiento de un equipo o sistema; pudiendo actuar de forma oportuna ante fallas críticas, y que, dicha información debe cumplir con aspectos de confidencialidad, seguridad y disponibilidad para personal autorizado.

El presente proyecto implica el estudio de información obtenida de una central de generación eléctrica “Gas Green” mediante el software especializado industrial SCADA y envío hacia un ambiente en la nube (Cloud).

Dicha información debe ser accesible hacia personal autorizado para monitoreo y control de normas de funcionalidad y en su defecto actuar de forma rápida ante posibles fallas en el sistema.

La identificación del tipo de datos, la forma de transportar dicha información hacia un ambiente en la Nube, protocolos de seguridad que debe cumplir la administración de información además de la veracidad, confidencialidad y disponibilidad contemplan el desarrollo del presente proyecto.

ABSTRACT

Currently it is common to speak of the term "Cloud", which refers to the management, control and administration of information, applications, services, etc., hosted on servers in different geographical locations and which can be accessed from anywhere in the world only having a simple connection to the Internet. There are multiple organizations dedicated to offering the Cloud Computing service as a business, for example: Microsoft, IBM, Amazon, etc.

Specifically, the information that is generated in a power generation plant through the industrial data acquisition system "SCADA" (Supervisory Control And Data Acquisition), provides information in real time that allows the controllers and / or operators to monitor the normal operation of a computer or system; being able to act in a timely manner in the face of critical failures, and that such information must comply with aspects of confidentiality, security and availability for authorized personnel.

The present project involves the study of information obtained to a power generation plant "Gas Green" through specialized industrial software SCADA and shipping to an environment in the cloud (Cloud).

This information must be accessible to authorized personnel for monitoring and control of functionality norms and failing to act quickly to possible failures in the system.

The identification of the type of data, the way of transporting said information to an environment in the Cloud, security protocols that must be fulfilled by the administration of information as well as the veracity, confidentiality and availability contemplate the development of the present project.

ÍNDICE

INDICE DE FIGURAS

INDICE DE TABLAS

Introducción

Antecedentes:

Cada día más servicios son migrados y monitoreados en un medio al cual se puede acceder en cualquier momento y desde cualquier lugar del mundo únicamente teniendo una conexión activa a Internet, así: el correo electrónico, almacenamiento de datos, ejecución de procesos, etc., son administrados en la nube (Cloud Computing).

Muchos de los servicios indicados son considerados de uso general y, como información pública requiere seguridad, confidencialidad y disponibilidad para lo cual se han desarrollado varias tecnologías que permiten asegurar, proteger y proveer respectivamente la información.

Sin embargo, existe cierto tipo de información que por su naturaleza requiere un tratamiento especial y por tanto es considerada como información sensible; así, los sistemas SCADA generan y procesan datos que se utilizan para monitorear niveles de presión, potencia, caudal, temperatura de motores - generadores, válvulas de presión, en general, datos industriales que son parte fundamental de una empresa generadora de electricidad.

Por tanto, dichas variables (información) es protegida y mostrada a determinado grupo social ya que están inmersos aspectos económicos, ambientales y legales.

El tratamiento y transporte de información industrial en nuestro país obtenida a partir del sistema SCADA no tiene un desarrollo notorio en cuanto a la migración y administración en un ambiente Cloud.

1) Alcance

El presente proyecto contempla el estudio de factibilidad para transportar señales industriales generadas en un sistema SCADA de una empresa generadora eléctrica hacia un ambiente diseñado en Cloud, empleando una

tecnología de telecomunicaciones actual y tomando en consideración aspectos de confidencialidad, seguridad y disponibilidad.

2) Justificación

Servicios considerados cotidianos (correo, almacenamiento, etc.) han ido migrando paulatinamente a ambientes controlados y administrados en la nube (Cloud); sin embargo, otro tipo de información obtenida en medios hostiles (industriales) obtenidos a partir de sistemas especializados como SCADA no han sido tomados muy en cuenta debido al carácter de confidencial, seguro y delicado respecto a magnitudes de monitoreo, administración y control.

Así, la información acorde a los distintos parámetros que arrojan turbinas, motores, generadores, bombas de presión, etc., utilizados en empresas de generación eléctrica son medidos, monitoreados, administrados y controlados por sistemas industriales especializados (SCADA) pero que únicamente personal acreditado tiene posibilidad de revisar en el propio lugar donde se genera la información, es decir, en la empresa generadora eléctrica.

La necesidad de enviar información “sensible” hacia un medio en el cual no sea necesario trasladarse físicamente al lugar en donde se genera; representa un cambio significativo respecto a ahorro de tiempo y costo.

De esta forma, utilizando tecnología de telecomunicaciones actual es posible migrar información, cualquiera que sea su naturaleza, a un entorno de acceso rápido, seguro y confiable.

Específicamente, albergar en Cloud información considerada delicada ofreciendo seguridad, disponibilidad, confidencialidad y confiabilidad.

3) Objetivo General

Realizar el estudio de factibilidad que permita determinar todos los aspectos necesarios para migrar información industrial obtenida del sistema SCADA (*Supervisory Control and Data Adquisition*) de una empresa de Generación Eléctrica y subirla a un entorno diseñado en Cloud, en el cual, se brinde

seguridad de información, administración de monitores, disponibilidad, acceso desde cualquier lugar y en cualquier momento.

4) Objetivos Específicos

Investigar los tipos de señales que genera el sistema de adquisición de datos industriales SCADA para control y monitoreo de equipos térmicos, mecánicos y eléctricos.

Determinar el ancho de banda necesario para procesar y transportar señales industriales hacia un entorno de Cloud e incluir la tecnología de transporte a utilizarse.

Diseñar un entorno de Cloud para transferir y albergar información generada por el sistema SCADA respetando protocolos empleados en ambientes industriales (protocolos de información SCADA). (DISEÑO DEL ENTORNO CLOUD PARA SISTEMAS INDUSTRIALES)

Brindar seguridad a la información almacenada en la nube además de confiabilidad y disponibilidad en tiempo real. (ASEGURAMIENTO DE INFORMACIÓN DE SISTEMAS INDUSTRIALES)

5) Metodología

La metodología que se empleará en el presente proyecto será Experimental y de Investigación.

La indagación que se realice a cada uno de los bloques que conforman una empresa generadora de electricidad, funcionalidad de cada parte, obtención de información, etc., validan que el proyecto a desarrollarse constituye un método experimental.

Metodología Investigativa involucra el análisis de los estudios realizados previamente para albergar temas relacionados a migración de datos en ambientes hostiles hacia un entorno de almacenamiento y control en la nube.

1. Capítulo I: Marco Teórico

1.1 Sistema SCADA

Un sistema de control industrial es un concepto que representa múltiples tipos de servicios de control y dispositivos relacionados para control de procesos industriales.

Tales sistemas comprenden desde simples controladores modulares en un panel y extenderse hasta llegar a ser un gran sistema de control interconectado con miles de conexiones de campo.

Todos estos sistemas reciben datos que provienen de sensores remotos, los cuáles miden variables específicas, los comparan con puntos de ajuste normales (predefinidos) y generan funciones de comando utilizados para controlar un proceso a través de dispositivos de control finales (válvulas de control).

Infraestructuras grandes se implementan mediante sistemas de control de supervisión y adquisición de datos (SCADA), o sistemas de control distribuido (DCS) y controladores lógicos programables (PLC).

Sistemas SCADA y PLC son aplicables a sistemas con pocos circuitos controlables. Estos sistemas son aplicados ampliamente en ambientes industriales de naturaleza variada: petróleo, procesamiento químico, fabricación de papel, procesamiento de gas, generación eléctrica, etc. (Corrales, 2007)

1.1.1. Definición

SCADA viene de las siglas "*Supervisory Control And Data Acquisition*", es decir, hace referencia a un sistema de adquisición de datos y control supervisor.

Tradicionalmente se define a un SCADA como un sistema que permite supervisar una planta o proceso por medio de una estación central que hace de Master (llamada también estación maestra o unidad terminal maestras, MTU) y una o varias unidades remotas (generalmente RTU´s) por medio de las cuales se hace el control / adquisición de datos hacia / desde el campo (Corrales, 2007).

Las topologías en las que se sustentan los sistemas SCADA se han adecuado a los protocolos y servicios de sistemas operativos actuales; sin embargo, las funciones de adquisición de datos y supervisión no han variado de forma notoria respecto a sus inicios.

Un sistema SCADA recolecta información proveniente de PLC´s ubicados en los distintos motores, generadores, válvulas, sensores, etc., pertenecientes a la planta y que se requieren medir y/o controlar.

Los datos son almacenados en una base de datos local o externa de acuerdo con las necesidades.

Un diagrama general del sistema se muestra en la Figura 1.

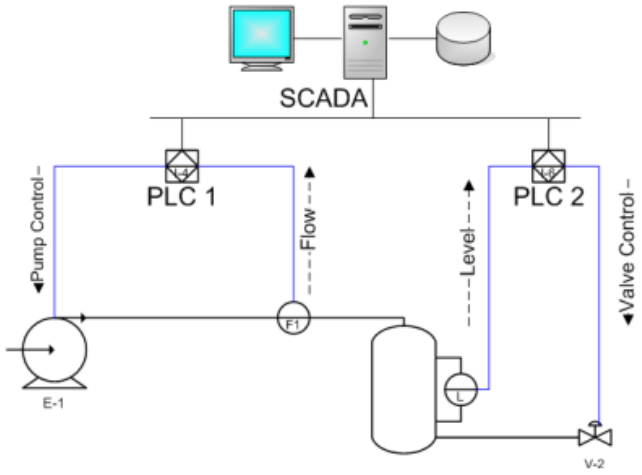


Figura 1. Diagrama General un sistema SCADA.
Tomado de (Paz, 2005)

Esquemáticamente, un sistema SCADA conectado a un proceso automatizado consta de las siguientes partes mostradas en la Figura 2.

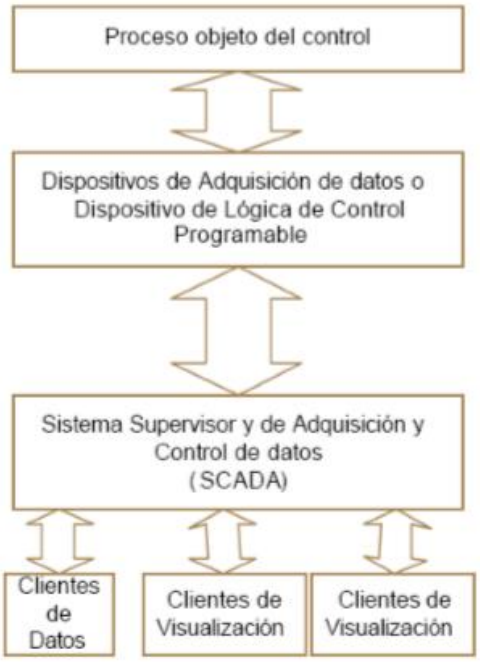


Figura 2. Representación esquemática de un sistema SCADA.
Tomado de *(Corrales, 2007)*

Proceso Objeto del control: Es el proceso que se desea supervisar. Es el origen de los datos que se requiere colectar y distribuir. En consecuencia, sensores instalados en cada generador y medidores de potencia.

Adquisición de Datos: Son un conjunto de instrumentos de medición dotados de alguna interface de comunicación que permita su interconexión. Corresponde entonces a los PLC´s los cuáles envían información digital / analógica al sistema.

SCADA: Combinación de hardware y software que permita la visualización y colección de los datos obtenidos de los instrumentos.

Clientes: Conjunto de aplicaciones que utilizan los datos obtenidos por el sistema SCADA. Hablamos entonces de las interfaces HMI con las cuáles se actúa en caso de ser necesario.

1.1.2. HMI o MMI

Interfaz Hombre – Máquina (Man-Machine Interface, MMI), es un mecanismo que posibilita a un operador humano interactuar con un proceso o máquina y

determinar el estado (apagado / prendido), magnitud de los dispositivos o variables físicas que tiene en ese momento en un proceso industrial o planta. Un ejemplo de interfaz HMI se muestra en la Figura 3.

Un HMI podrías ser tan simple como un interruptor para activar un motor o lámpara indicadora de estado, hasta una o múltiples pantallas desarrolladas en un computador en el cual se muestra representaciones esquemáticas de todo un proceso bajo supervisión, mostrando valores en tiempo real de variables monitoreadas de la planta.

Para “manejar” un sistema SCADA se recurre a un software especializado que es instalado en la computadora central, por medio del cual se desarrollan varios monitores que actúan como interfaces gráficas entre el operador y el proceso y/o máquina; permitiendo de esta forma supervisar o cambiar puntos de referencia ingresados previamente por el operador en la computadora (Corrales, 2007).

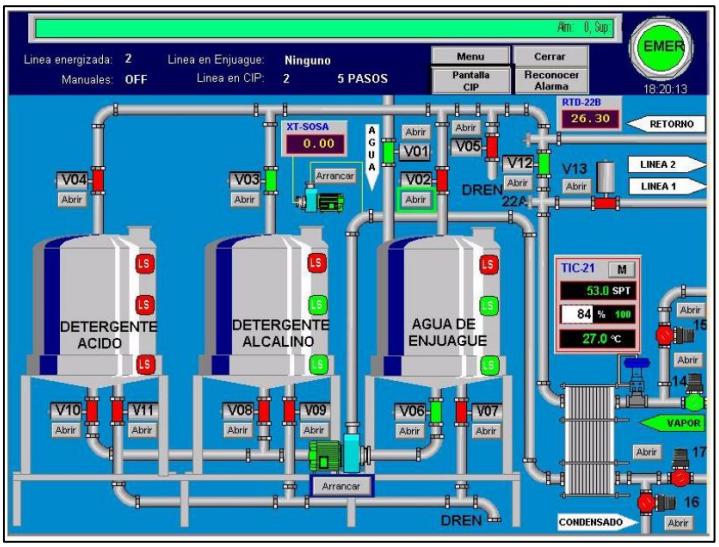


Figura 3. HMI en un sistema SCADA.
Tomado de (Chicúe, Automatización y Control Industrial, 2015)

Programas como *InTouch (*Wonderware*), Lookout* (National Instruments), constituyen plataformas abiertas de desarrollo que ayudan al diseño de las HMI en el computador.

Plataformas propietarias como RSView, WINCC (Siemens) garantizan solides de funcionalidad en relación con productos de monitoreo y control de sistemas SCADA.

En la actualidad los sistemas SCADA incluyen tecnologías de comunicación avanzadas, pero no empezaron de esa forma.

1.1.3. Unidad Remota de Telemetría (RTU)

Remote Telemetry Unit (RTU), es una parte importante de un sistema SCADA.

Es un equipo instalado en un sitio remoto que recopila información y la codifica en un formato que permita transmitirlos hacia una estación central (*Master Terminal Unit,* MTU) u otra RTU.

Una RTU además, recibe información desde la MTU, decodifica los datos y posibilita la ejecución de ordenes enviadas.

Una RTU está conformada por canales de entrada para medición y detección de variables en un proceso y de canales de salida para control y activación de alarmas y actuadores; además de puerto de comunicaciones.

Figura 4. RTU.
Tomado de (ZIV, 2011)

La CPU brinda inteligencia necesaria para procesar datos de entrada / salida de forma correcta.

Figura 5. CPU de una RTU.
Tomado de *(Corrales, 2007)*

La Figura 5 posee interfaces RS-485, RS 232 y puerto Ethernet. Además de una memoria volátil (RAM), memoria no volátil (generalmente Flash) en la cual se almacenan de forma permanente programas (protocolos de comunicación) y datos.

Determinadas RTUs incorporan capacidades de comunicación sea por pórtico serial o mediante un MODEM; está última que permite conexión a cualquier medio de comunicación ya sea radio RF, tecnología *Spread Spectrum* o Telefonía Celular (Corrales, 2007)

Figura 6. RTU con tecnología Celular.
Tomado de (Corrales, 2007)

1.1.4. Software de una RTU.

Las RTUs requieren software con las siguientes características:

- Sistema operativo en tiempo real (RTOS), o algún algoritmo que inicie un lazo de barrido en las entradas y, supervise pórticos de comunicaciones.

- Driver para sistema de comunicaciones, es decir, el programa que define el protocolo del enlace de comunicaciones hacia el módulo master del SCADA.

- Controladores para el sistema de entrada/salida, es decir, para los dispositivos del campo.

- Aplicación SCADA que controle el barrido de entradas, procesar / almacenar información, actuar ante solicitudes recibidas por el SCADA recibidas por el canal de comunicaciones.

- Métodos que ejecuten en las RTUs órdenes enviadas desde las aplicaciones del usuario HMI. Esta acción puede ser una acción simple como definir parámetros, habilitar / deshabilitar entradas o salidas e incluso modificar un programa completo de usuario.

- Finalmente, programas de autodiagnóstico.

1.1.5. Estándares

Las RTUs en su comienzo no tuvieron normalización suficiente en especial en aspectos de comunicación, además que los proveedores no tenían compatibilidad entre sus productos (RTUs).

Por estas razones, se han desarrollado estándares para normal el funcionamiento de las RTUs:

- DNP3 y IEC870 – Estándar para comunicaciones y

- Ec1131-3 para programación

1.1.6. Protocolos de Comunicación para RTUs

Un protocolo es un conjunto de reglas que definen cómo los dispositivos pueden comunicarse entre ellos.

Los datos que se recopilan en las RTUs previo a transmisión se encapsulan obedeciendo a protocolos DNP3 y IIEC870.

1.1.6.1. Protocolo DNP3

Desarrollado por GE Harris (Canadá) en 1990 y emitido en 1993. Hoy administrado por DNP

DNP3 es usado para comunicaciones seriales e IP, empleado principalmente para empresas de agua potable y eléctricas.

Fue diseñado para optimizar la transmisión de datos en el campo y comandos de control entre estaciones remotas y computadores maestras.

Usa el término "*outstation*" (estación externa) para hacer referencia a estaciones remotas ubicadas en el campo.

No es un protocolo de propósito general como los protocolos de Internet para transmitir hypertexto, peticiones SQL, email, multimedia, sino para aplicaciones SCADA (Corrales, 2007)

1.1.6.2. Protocolo IEC 870

Desarrollado por el Comité Técnico 57 para tele-operación, telecontrol y telecomunicaciones asociadas; para sistemas eléctricos de potencia.

El resultado son cinco especificaciones:

- IEC 870-5-1 El formato de la Trama de Transmisión
- IEC 870-5-2 Servicios de Transmisión de la Capa de Enlace
- IEC 870-5-3 Estructura General de los datos en la Capa Aplicación

- IEC 870-5-4 Definición y codificación de los elementos de Información.
- IEC 870-5-5 Funciones de Aplicación básicas.

En la terminología del protocolo se emplean términos como: Estación Controlada (*Controlled Station*) para referirse a la Estación Externa *(Outstation*), Estación Remota (*Remote Station*), Estación Esclava (*Slave Station*) y Unidad Terminal Remota (*Remote Terminal Unit)* comandadas o monitoreadas por una estación master (Corrales, 2007)

Se denomina Estación Controladora (*Controlling Station*) a la Estación Maestra (*Master Station*) en donde se realiza el telecontrol de las estaciones externas.

Los protocolos DNP3 e IEC870 obedecen a un esquema de capas.

1.1.7. Especificaciones en las RTUs

Para adquisición de RTUs, se deben especificar parámetros como: humedad relativa, polvo, vibración, protección contra neblina, sal, lluvia, rangos de temperatura, tamaño físico, consumo de energía, funcionalidad, protocolos de comunicación, entre otros (Corrales, 2007).

1.1.8. PLCs

Son controladores de propósito general, que pueden ser convertidos en controladores de propósito específico cambiando su configuración interna.

En principio, el control de procesos industriales se lo realizaba por medio de relees y contactores unidos por cables.

Cambios en los procesos conllevaba modificar físicamente gran parte de conexiones de los arreglos (montajes), para lo cual era necesario mano de obra técnica importante y por supuesto impacto económico.

Con la aparición del circuito integrado en 1959, se alcanza un notable avance en el desarrollo del primer PLC, integrándose a la industria en 1960 aproximadamente. La principal razón de esta mejora se da por la necesidad de

eliminar el costo elevado que implicaba reemplazar un sistema complejo de control basado en relees y contactores ya que para tal efecto, la planta debía cerrar por un tiempo considerable.

En este contexto, la mayor demanda de tiempo conllevaba rehacer y revisar el cableado de paneles de control y relees.

Para el año de 1968, ingenieros de Hydra-Matic (división de General Motors) desarrollan el primer PLC de uso comercial. Llamado MODICON 084.

Para 1970, el uso del PLC se hizo común en las industrias, en principio como reemplazo de aplicaciones gobernadas por relees. Por tanto, representó una solución al control de circuitos complejos de automatización.

A un PLC entonces, se conectan los captadores (pulsadores, sensores, etc.) por una parte, y los actuadores (lámparas, sirenas, receptores, bobinas, etc.) por otra.

En la actualidad, un PLC es la opción preferida en el ámbito industrial y su naturaleza es cada vez más compleja y creciente. De hecho, hoy en día un PLC es considerado un microcomputador que gestiona aplicaciones de control industrial y cuenta con funciones complejas que operan con arreglos de estructuras y variedad d formatos numéricos, así como gran cantidad de memoria y velocidades altas de ejecución.

De esta forma, el desarrollo de aplicaciones de control es vista como una tarea relativamente simple.

La potencia de un PLC está relacionada directamente con la velocidad de ejecución para manejar variables controladas. En el mercado, un PLC tarda 0,5 ms en responder a mil instrucciones, lo cual resulta muy bueno para el control automático de cualquier sistema

1.1.8.1. Partes de un PLC

En la Figura 7, se indica la estructura básica de un PLC típico

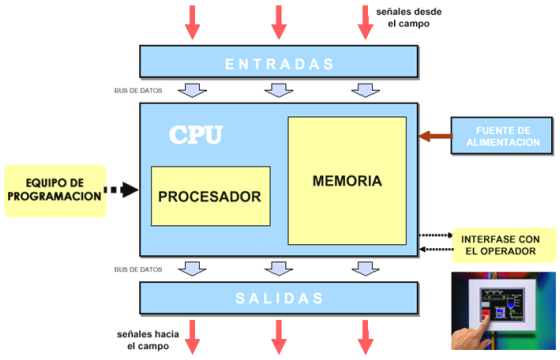


Figura 7. Estructura básica de un PLC.
Tomado de *(Calfi, 2011)*

Un PLC, consta de las siguientes partes:

- Fuente de alimentación
- CPU
- Memoria
- Módulos de salida
- Módulos de entrada
- Terminal de programación
- Periféricos
- Algoritmo de programación (scan)

En cuanto a la distribución externa, un PLC puede ser compacto o modular si las secciones están dentro de un mismo módulo o en diferentes módulos respectivamente.

1.1.9. Buses de Campo

Es un sistema de transmisión de datos (información) que facilita la operación e instalación de equipamientos industriales y maquinaria utilizados en procesos de producción.

1.1.9.1. Profibus.

Estándar de red de campo abierto independiente de proveedores, de origen alemán empleado en interconexión de equipamiento de campo en entrada / salida simples como PC´s y PLC´s.

Maneja 3 perfiles:

- Profibus DP (*Decentralized Periphery*): Orientado a sensores/actuadores interconectados a PLC's.
- Profibus PA (*Process Automation*): Para control de procesos y cumpliendo normas de seguridad especiales para industria química.
- Profibus FMS (*Fieldbus Message Specification*): Comunicación entre células de proceso o equipos de automatización.

Cada perfil dispone de su velocidad de transmisión máxima, además de la longitud de cable. La Tabla 1 detalla lo expuesto.

Tabla 1.
Velocidad de transmisión Profibus y Longitud del Cable.

Perfil Profibus	**Velocidad (máxima)**
FMS	1.5 Mbps
DP	12 Mbps
PA	31.2 kbps

Velocidad (Kbps)	9.6	19.2	93.75	187.5	500	1500	12000
Distancia/Segmento (m)	1200	1200	1200	100	400	200	100

Tomado de (Corrales, 2007).

1.1.10. Medios de comunicación para sistemas SCADA

La comunicación en los sistemas SCADA se logran mediante los siguientes métodos.

1.1.10.1. Cable.

Cables propietarios, rentadas y fibra óptica.

- Cables Propietarios: Se realiza inversión en tendido de redes de comunicación, lo que representa costos iniciales elevados. Además de contratar personal que mantenga operativo el entorno.

- Líneas Rentadas: Entidades estatales o privadas proveen una o varias líneas para la industria que requiere el servicio. Estas líneas pueden ser dedicadas o compartidas, evitando invertir en equipos e instalación, pero invirtiendo en tareas de mantenimiento.

- Fibra Óptica: Brinda seguridad y ancho de banda suficiente para cumplir necesidades, con la desventaja que es de acceso limitado geográficamente (Cornejo & Díaz, 2015).

1.1.10.2. Radio

Referido a enlaces de comunicación por medio de enlaces inalámbricos empleando desde RF hasta Microondas. Además de enlaces satelitales.

Los sistemas de RF pueden ser propios de la empresa, pero también es posible contratar el servicio ya que en el mercado existen radios en banda licenciada (150 y 450Mhz) para fines industriales (Cornejo & Díaz, 2015).

1.1.10.3. Líneas telefónicas (Dial – up)

Convenientes cuando las comunicaciones por cable o radio no son posibles debido a la distancia, terreno, etc.

Se recurre a PSTN (Andinatel, Paficitel, etc).

Un inconveniente obvio es que no exista servicio de telefonía en el lugar deseado.

De esta forma se obtiene servicios vía ADSL o ISDN.

1.1.11. Necesidad de un sistema SCADA

Para determinar si un sistema SCADA es necesario para un entorno industrial dado, el entorno a controlar debe cumplir las siguientes características.

- Número de variables a monitorear sea alto.
- El entorno debe tener actuadores y transmisores geográficamente distribuidos.
- Información requerida en tiempo real.
- Optimizar y facilitar operaciones de la planta.
- Los beneficios a ser obtenidos en el procedo de monitoreo y control justifiquen la inversión. Esto es, aumento de producción, confiabilidad, seguridad y disponibilidad.
- La complejidad del sistema requiere que la mayoría de las acciones de control sean iniciadas por un operador.

1.2. Cloud Computing

Computación en la nube es un término cotidiano hoy en día y cuyo concepto ha sido definido por organizaciones tecnológicas tales como NIST y la IEEE.

Según la NIST (Instituto Nacional de Estándares y Tecnología de EEUU) se define como: *“Cloud computing is a model for enabling ubiquitous, convenient, on-demand network Access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”.* Traducido a nuestro idioma: *“Un modelo que permite el*

acceso conveniente a una red bajo demanda que coparte un conjunto de recursos informáticos configurables (por ejemplo, redes, servidores, aplicaciones y servicios) que pueden ser rápidamente almacenados, provistos y lanzados con el mínimo esfuerzo de administración o interacción con el proveedor de servicios."

Según la IEE, define a Cloud Computing como: *"Cloud computing is an information-processing model in which centrally administered computing capabilities are delivered as services, on an as-needed basis, across the network to a variety of user-facing devices"*. Traducido a nuestro idioma: *"La computación en nube es un modelo de procesamiento de información en el que las capacidades de computación administrados centralmente son entregados como servicios, en una función de las necesidades, a través de la red a una variedad de dispositivos de cara al usuario"* (Cornejo & Díaz, 2015).

De acuerdo con las definiciones anteriores, "La Computación en la Nube es un modelo remoto de gestión de servicios que busca el manejo de información en una red bajo demanda, que puede brindar tanto servicios, como también infraestructura al cliente, minimizando el trabajo del mismo y facilitando la administración de las aplicaciones y recursos, a través de las tecnologías actuales y desde cualquier ubicación, sin restricción alguna de dispositivos o tiempo".

Cloud Computing busca aumentar el número de servicios que la red puede ofrecer, con rapidez y eficiencia suficiente, reduciendo gastos en clientes como en proveedores. Por tanto, se busca garantizar la disponibilidad, flexibilidad, integridad y escalabilidad de servicios como voz, video y datos reduciendo costos de implementación cumpliendo plenamente con la demanda de usuarios y servicios presentes en el mercado actual.

Podríamos indicar que el objetivo principal de la Computación en la Nube es resolver problemas computacionales de gran escala, mediante optimización de recursos distribuidos que combinados mejoran considerablemente el desempeño de la red.

La virtualización de recursos de hardware representa sin duda un aspecto importante relacionado con aspectos de negocio para proveedores de Cloud en el mercado ya que se aprovecha de mejor manera la infraestructura disponible.

Grandes empresas de TI como HP, IBM, Microsoft, Intel han invertido en la implementación de Cloud Computing, debido a la demanda creciente de servicios de software y hardware que la tecnología representa (Cornejo & Díaz, 2015)

1.2.1. Características de Cloud Computing

Según el NIST (*National Institute of Standards and Technology*), para considerar la implementación de *Cloud Computing*, se debe cumplir con los siguientes aspectos:

1.2.1.1. Autoservicio bajo demanda.

Cliente puede solicitar y recibir acceso al servicio ofrecido sin necesidad de recibir soporte de un administrador.

1.2.1.2. Acceso a la Red Extensa.

Se permite el acceso desde cualquier lugar del mundo a la red, en donde los usuarios deben contar con una conexión simple a Internet para conexión a servicios y aplicaciones (Cornejo & Díaz, 2015).

Hoy en día, es tan extenso el tema de acceso a la red que incluso se puede acceder desde un smartphone o Tablet.

1.2.1.3. Compartición de Recursos.

Reducción de costos y flexibilidad a usuarios para el acceso a recursos disponibles y gracias a la virtualización, hacer posible múltiples sesiones.

Un usuario puede acceder a los servicios contratados sin necesidad de conocer la ubicación física en donde se concentra su información y/o servicio (Cornejo & Díaz, 2015).

1.2.1.4. Aplicaciones son independientes del hardware.

La virtualización hace posible compartir recursos de hardware entre varios usuarios que acceden de forma simultánea, de esta forma, en un mismo equipo físico pueden correr aplicaciones de distinta naturaleza sin que el usuario lo note.

1.2.1.5. Rapidez y Elasticidad

Se refiere al crecimiento rápido de la red para satisfacer demandas, esto incluye recursos como: memoria, discos duros, CPU entre otros. El objetivo es cumplir con requerimientos de los usuarios en el menor tiempo.

1.2.1.6. Servicio Ponderado

Los servicios que ofrece Cloud son medibles en su implementación, gracias a ello se puede usar parámetros de análisis como: tiempo de uso, ancho de banda, uso de datos, etc.

1.2.2. Modelos de Servicio de *Cloud Computing*

Se refiere a la utilización de componentes accesibles desde internet, escalabilidad y compartición de recursos debido a la autonomía de hardware.

El cliente final es el encargado de elegir la opción que mejor se adapte a su negocio u organización, debido que en la implementación se requieren recursos físicos como monetarios y que van de acuerdo con los servicios que serán aplicados (Cornejo & Díaz, 2015)

De acuerdo con la NIST, se diferencias tres tipos de modelos, representados en la Figura 8.

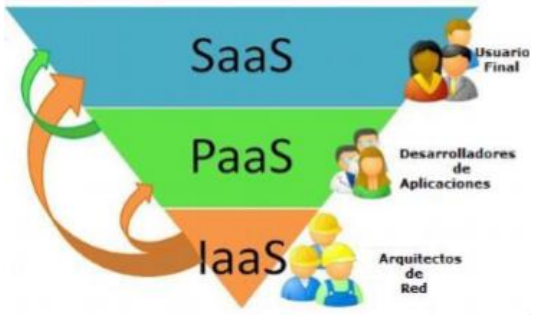


Figura 8. Modelos de servicio de la nube.
Tomado de *(Cornejo & Díaz, 2015)*

1.2.2.1. Servicios por Software (SaaS, *Software as a Service)*

Se refiere al modelo en el cual un proveedor ofrece software como servicio hacia una organización, para lo cual “vende” costos de licenciamiento para uso de software como servicio bajo demanda.

El cliente administra aplicaciones sin preocuparse de la infraestructura sobre la que se desarrolla el software, es decir, servidores o sistemas operativos.

Las aplicaciones pueden ser accedidas desde un navegador con conexión a Internet.

Aplicaciones SaaS brindan servicios a clientes empresariales debido a la reducción de costos tanto en instalación como en mantenimiento.

Ejemplos de aplicaciones SaaS: GoogleDrive, Gmail, en donde el acceso a las aplicaciones se da mediante navegadores web o enlaces que apuntan a los servidores donde están las aplicaciones listas para ser utilizadas por los usuarios (Cornejo & Díaz, 2015)

1.2.2.2. Servicios por Plataforma (Paas*, Platform as a Service*)

El modelo consiste en desarrollo de aplicaciones propias de la empresa u organización.

El cliente cuenta con recursos físicos de acceso a una plataforma en la cual desarrolla aplicaciones y administra servicios acorde a sus requerimientos sin necesidad de adquirir hardware.

La nube dispone de recursos suficientes para desarrollar aplicaciones sin contar con una infraestructura virtual o física, la cuál es ofrecida por el proveedor quien se encarga de administrar la plataforma y herramientas.

El cliente únicamente dispone de herramientas que el proveedor ofrece y con ello desarrolla aplicaciones o servicios y en donde puede utilizar plataformas como: NET, Python, PHP, Ajax, Java, Ruby, etc. (Cornejo & Díaz, 2015)

1.2.2.3. Servicios por Infraestructura (IaaS, *Infraestructure as a Service*)

El modelo, el proveedor provee al cliente la infraestructura para el uso de servicios.

El cliente se encarga únicamente de administrar el almacenamiento, procesamiento, recursos y equipos en los que se encuentras desplegados los servicios.

Este modelo es utilizado para reducir gastos que impliquen costos de tecnologías como son: servidores, switches, routers, equipos.

Los costos relacionados a este modelo se basan en el consumo de recursos que el cliente realice con la finalidad de reemplazar lo correspondiente a un Data Center.

Ejemplo de IaaS es: Amazon Web Services, en donde se permite administrar máquinas virtuales en la nube, es decir, dar características acorde a los requerimientos sin importar el hardware (Cornejo & Díaz, 2015)

1.2.3. Modelos de Despliegue de *Cloud Computing*.

Se caracterizan por la forma de cómo se brinda el acceso a un nodo privado o acceso a grandes cantidades de usuarios que desean acceder a información personal a través de enlaces directos o remotos (Cornejo & Díaz, 2015)

Se han definido 3 modelos.

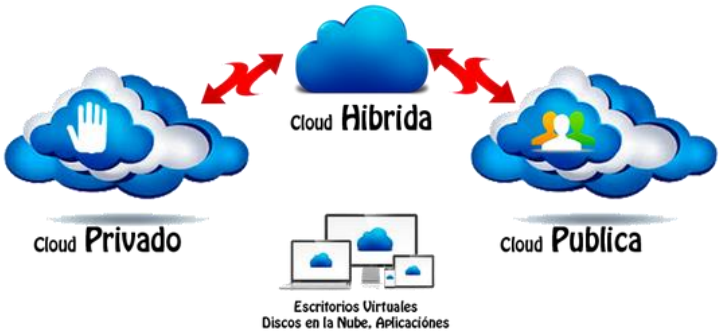


Figura 9. Métodos de despliegue en la nube.
Tomado de (Libygem, 2015)

1.2.3.1. Cloud Privada

Una nube privada es la infraestructura que solamente una empresa administra o maneja y que puede estar tanto dentro o fuera de ella. Su representación se muestra en la Figura 10.

Generalmente está ubicada dentro de las instalaciones de la empresa.

Una de sus mayores ventajas radica en que permite ofrecer únicamente servicios requeridos por la organización propietaria, además de contar con características de una nube pública.

Cuenta con el control completo de accesos, datos, aplicaciones y procesos que se despliegan en la nube.

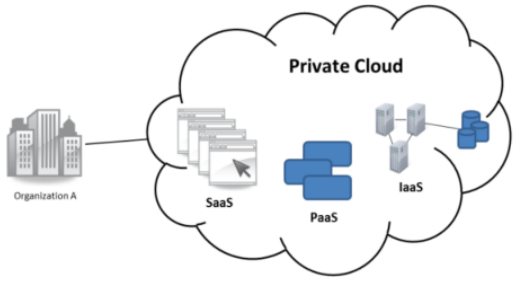


Figura 10. Nube Privada.
Tomado de *(Ahmad, 2017)*

La infraestructura, a diferencia de una nube pública, no debe ser compartida con ninguna empresa.

El despliegue es similar a un Datacenter ya que cuenta con infraestructura, equipos propios y su crecimiento está en base a la demanda.

Nubes privadas son diseñadas para concentración alta de recursos y sistemas tecnológicos. Por ejemplo: Administración pública, entidades bancarias, ambientes de desarrollo e investigación, etc (Cornejo & Díaz, 2015).

1.2.3.2. Cloud Pública

Es un modelo de implementación de uso general, en donde se busca que todos tengan acceso a aplicaciones e información. Su representación se muestra en la Figura 11y generalmente pertenece a una organización que brinda ese servicio.

Figura 11. Nube Pública.
Tomado de *(Hansen, 2017)*

La infraestructura es compartida con varios clientes a través de conexiones VPN o Internet y el pago se da por uso de infraestructura entre los clientes.

Las plataformas son propias y pueden crecer o disminuir acorde a necesidades del cliente, pagando únicamente los recursos utilizados y sin necesidad de redimensionar recursos (Cornejo & Díaz, 2015)

1.2.3.3. Cloud Híbrida

Consiste en una combinación de aplicaciones de nube privada con aplicaciones de nube pública, logrando mantener el control de sus aplicaciones Su representación se muestra en la Figura 12.

Este tipo de modalidad se aplica debido a la necesidad de clientes que, aun contando con su propia infraestructura, buscan aprovechar ventajas de un proveedor que también implementa ciertos servicios los cuáles serán ofrecidos a otras organizaciones o empresas (Cornejo & Díaz, 2015).

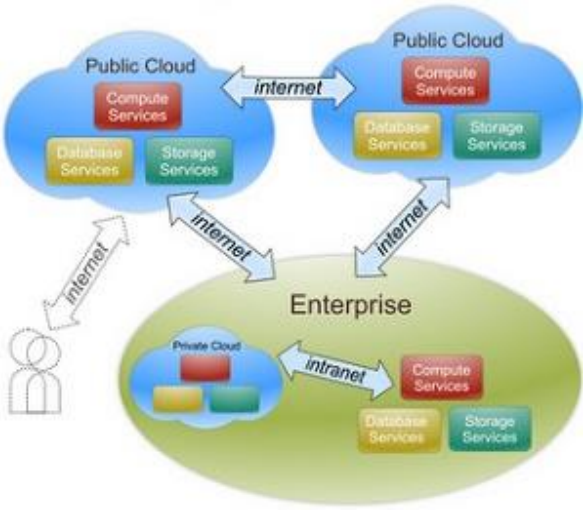


Figura 12. Nube Híbrida.
Tomado de *(Calfi, 2011)*

1.2.4. Arquitectura Básica de Cloud Computing

Distingue varias capas que se pueden implementar en nubes privadas, públicas e híbridas.

Se basa en la arquitectura de red, debido a que Cloud Computing emplea los mismos protocolos (Cornejo & Díaz, 2015).

Se caracterizan porque el despliegue en redes arrendadas como propias tiene una arquitectura genérica que cuenta con cinco capas principales mostradas en la Figura 13.

Figura 13. Capas básicas de Cloud Computing.
Tomado de *(Cornejo & Díaz, 2015)*

- **Recursos Físicos:** Compuesta por elementos físicos como servidores, almacenamiento y red, es decir, hardware que interviene en la nube.
    - **CPU, discos, memorias:** Se encargan del procesamiento de información lo que constituye la parte principal de Cloud Computing.
    - **Equipos de Enfriamiento:** Responsables de mantener a una temperatura adecuada los elementos que intervienen en la nube para evitar recalentamiento por uso y fallas.
    - **Redes**: Elementos para transporte hacia los medios de almacenamiento.
    - **Redundancia:** Se refiere a respaldos y recuperación ante desastres, fallas de energía, caídas de servidores o sobrecarga de datos.

- **Virtualización:** Se encarga de la infraestructura virtual como servicio, es decir, virtualizadores.
- **Infraestructura:** Encargada de administrar software de plataforma como servicio.
- **Plataforma:** En esta capa están los componentes de aplicación como servicio. En esta capa estarían los módulos o componentes en donde se despliegan las aplicaciones.
- **Aplicación:** En esta capa se incluyen servicios basados en software y web como servicio.

2. Capítulo II: Procesamiento de Señales a Cloud

El entorno en el que se desarrolla el presente proyecto es la Central de Generación Eléctrica “Gas Green” ubicada al Noreste de Quito.

Figura 14. Aspirador

La Figura 14 muestra el aspirador que absorbe el gas metano proveniente del relleno sanitario de Quito a través de conductos enterrados con longitud cercana a los 100 metros.

El gas obtenido es enfriado desde los 54°C hasta los 32°C y enviado a los generadores eléctricos.

El caudal de gas es controlado de acuerdo con las necesidades y horarios.

La presión que ejerce el gas en su transporte acorde al caudal establecido es medido y controlado efectivamente

La potencia que entrega cada generador bordea los 1,33 MWh y su funcionamiento se basa en tecnología de BioGas.

La Figura 15 muestra el identificativo de potencia máxima que entrega la planta.

Figura 15. Planta GasGreen Quito

El sistema SCADA recoge datos en tiempo real de las características indicadas anteriormente, esto es:

- Caudal.
- Temperatura.
- Presión y
- Potencia.

De esta forma la infraestructura que se extiende durante toda la planta tiene áreas específicas que reciben/envían información, transformación de datos, generación, transporte de fluidos, etc.

Se muestran en la Figura 16 los sensores que están presentes en la planta de generación además de el medidor de potencia ubicado en cada generador.

Figura 16. Sensores instalados en planta.

Se evidencia que los sensores utilizados para medir temperatura, caudal y presión corresponden a equipamiento del fabricante KOBOLD.

Estos sensores envían una señal de corriente continua (entre 4 y 20mA) hacia el PLC (Siemens S7-300) mediante el protocolo HART.

En la Figura 17, se observa la señal de corriente que es tomada como portadora y mediante modulación de frecuencia (FSK) se transmiten datos digitales representados por 1200Hz (1 lógico) y 2200Hz (0 lógico).

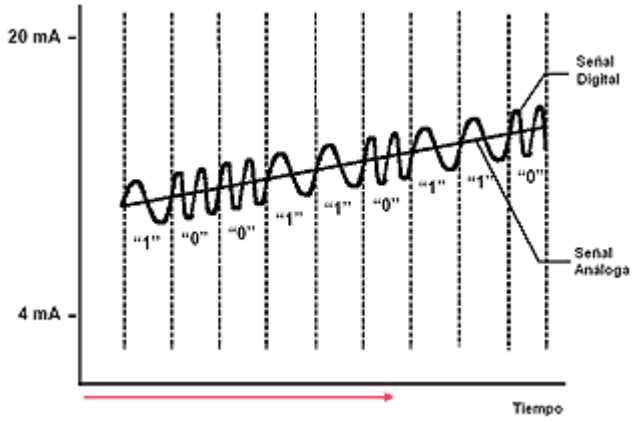


Figura 17. Protocolo HART.
Tomado de *(Meichsner, 2004)*

El protocolo HART constituye un medio de comunicación análoga / digital para trasmitir información desde el sensor hacia el controlador PLC.

Lo que recibe el PLC es una señal eléctrica modulada con información de estado real del sensor correspondiente.

Características del medio de transporte entre el sensor y el actuador están descritas en la Tabla 2.

Tabla 2.
Características de transporte protocolo HART.

	TOPOLOGÍA	MEDIO FÍSICO	VELOCIDAD	DISTANCIA SEGMENTO
HART	Bus lineal	Cable 2 hilos	1'2Kbps	3.000 m

Tomado de *(Meichsner, 2004)*

Los sensores envían información análoga que viaja mediante un conductor típicamente de cobre y llega hacia el tablero de concentración en donde se conecta al PLC correspondiente, tal como se muestra en la Figura 18.

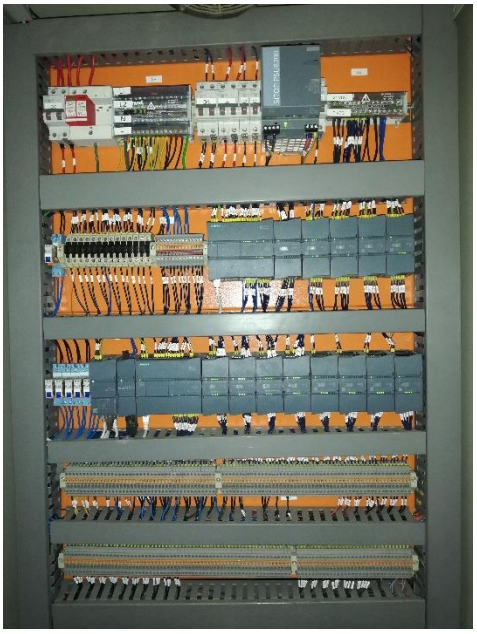


Figura 18. Tablero de Concentración.

Para nuestro interés, el análisis de transporte de información que se recibe desde los sensores es a través del procesamiento realizado en el actuador (PLC Siemens S7-300), del cual se envía información digital hacia el medio y hasta el software de control industrial SCADA.

Por tanto, las características técnicas del actuador SIEMENS S7-300 determina en gran medida el dimensionamiento del medio a utilizar en el diseño.

2.1. Análisis de variables en campo.

La central eléctrica cuenta con 5 generadores eléctricos los cuales operan de acuerdo con las indicaciones que recibe del Centro Nacional de Control de Energía (CENACE). Por tanto, el ancho de banda necesario debe ser calculado en base al tráfico de información de 5 estaciones generadoras trabajando a máxima capacidad.

Cada generador cuenta con un actuador (PLC) configurado en modo esclavo, el cuál recibe información en tiempo real proveniente de los sensores (caudal, presión y temperatura) y potencia.

Esta información es transmitida mediante Switches ubicados en cascada.

En campo se diferencian 2 conexiones separadas: Red de generadores y Red de Medidores de Potencia.

Red de generadores: Constituida por sensores conectados a PLC Siemens S7-300 y con salida Profinet conectadas en cascada con única salida hacia un Switch Xtratech para lectura en software SCADA y envío mediante proveedor Punto Net.

En esta red se localizan los distintos sensores (presión, temperatura y caudal).

Los datos relacionados a valores de potencia de cada generador son obtenidos mediante la red de medidores de potencia a través de un WatchGuard Switch XTM2.

Red de medidores de potencia: Constituida por instrumentos de medición Siemens Sentron y medidores ION.

La Figura 19 muestra el diagrama de conexión de los distintos elementos distribuidos en la planta.

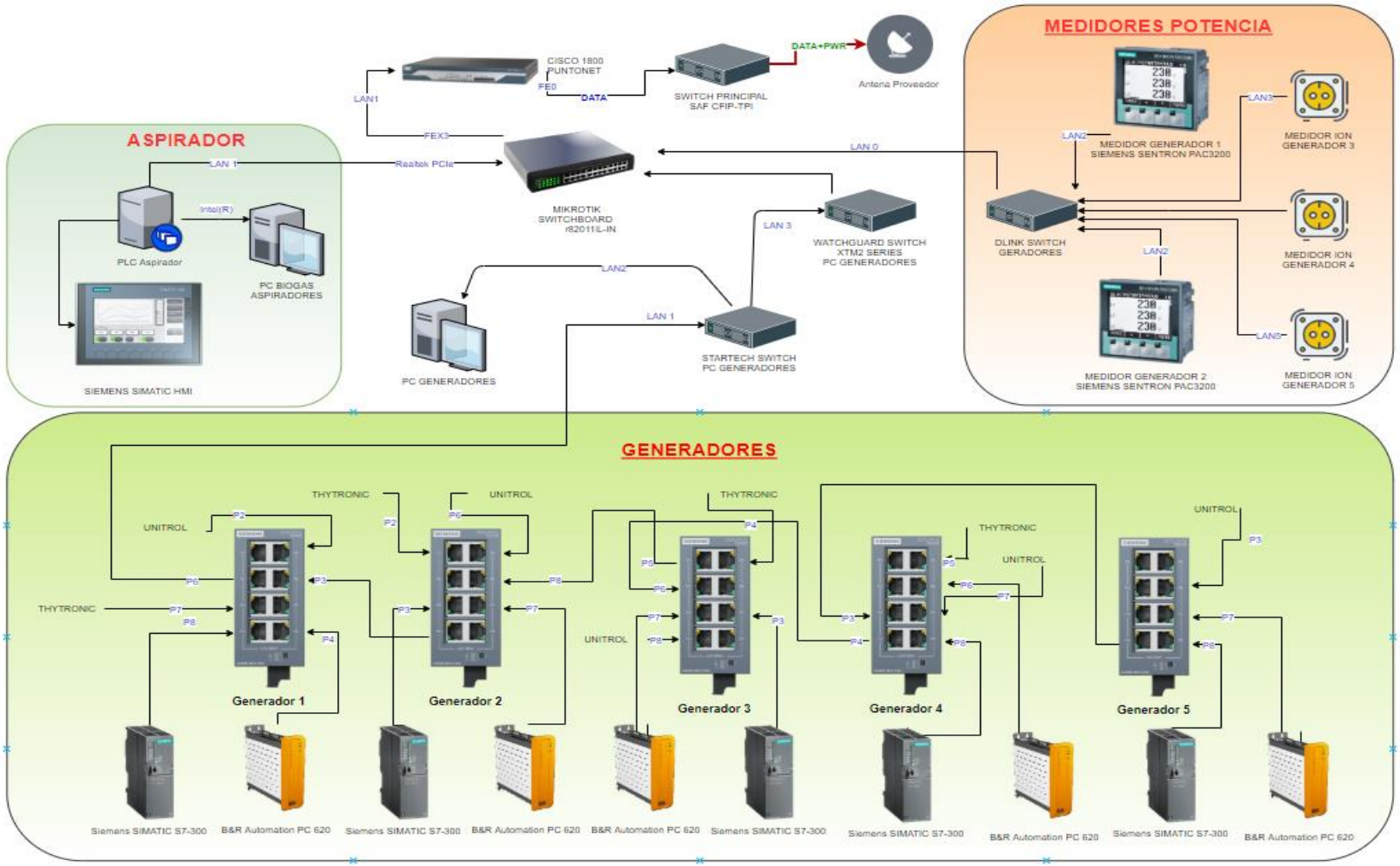


Figura 19. Diagrama de Conexión de Planta Gas Green

Para 2 generadores se utiliza medidores Siemens Sentron PAC3200 mientras que en los 3 generadores restantes se utiliza medidores ION.

La Figura 20 muestra el medidor de potencia ION para generadores Tipo4 instalados en campo, el mismo que poseen una interfaz ethernet para comunicación.

Figura 20. Medidor ION

Los datos de interés (sensores y potencia) son almacenados en una base de datos local y sincronizada cada hora con un servidor para registro y respaldo, mostrada en la Tabla 3.

Tabla 3.

Datos Obtenidos en Campo.

		GENERADOR 1			
FECHA	HORA	CAUDAL	PRESIÓN	TEMPERATURA	POTENCIA
dd/mm/aa	hh/mm/aa	m3/h	mBar	°C	Kw
7/5/2019	11:00:12 a. m.	899,99	300	58,00	637
8/5/2019	11:01:00 a. m.	899,99	300	59,00	641
9/5/2019	11:02:00 a. m.	899,99	300	58,00	640
10/5/2019	11:03:00 a. m.	899,99	300	58,00	637
11/5/2019	11:04:00 a. m.	899,99	300	58,00	640
12/5/2019	11:05:00 a. m.	899,99	300	58,00	639
13/5/2019	11:06:00 a. m.	899,99	300	59,00	639
14/5/2019	11:07:00 a. m.	899,99	300	59,00	644
15/5/2019	11:08:00 a. m.	899,99	300	59,00	642
16/5/2019	11:09:00 a. m.	899,99	300	59,00	637
17/5/2019	11:10:00 a. m.	899,99	300	58,00	641
18/5/2019	11:11:00 a. m.	899,99	300	58,00	642

19/5/2019	11:12:00 a. m.	899,99	300	58,00	637
20/5/2019	11:13:00 a. m.	899,99	300	58,00	638

Esta información es analizada y monitorizada por el centro de control para actuar en caso de emergencia o necesidad.

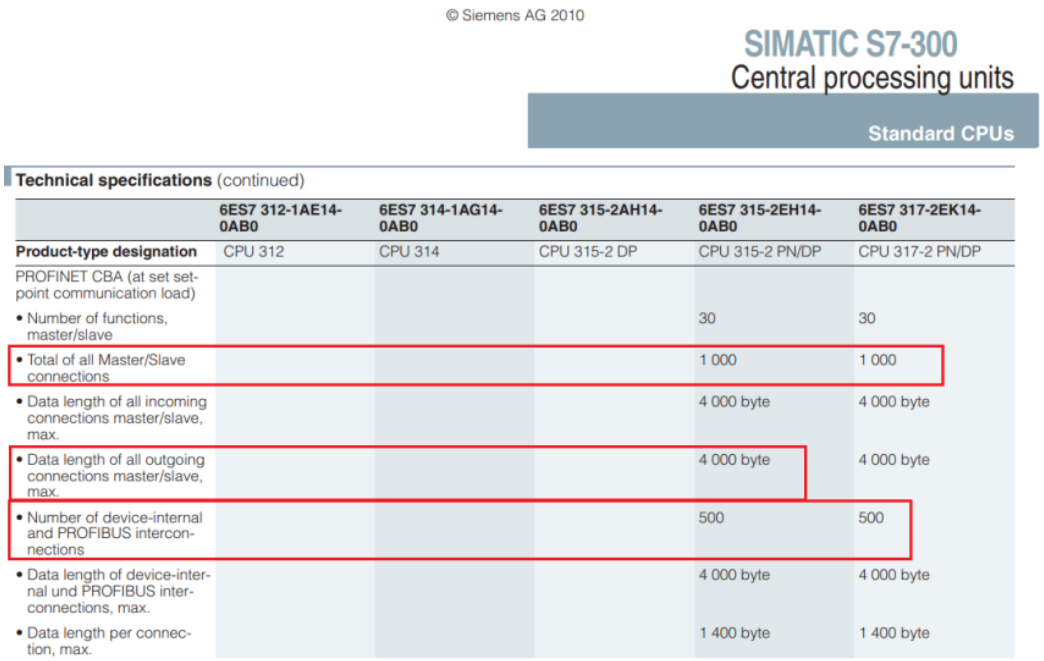
2.2. Determinación de Ancho de Banda.

Una vez determinados los elementos que intervienen en la obtención, intermediación y transmisión de datos hacia el software de recopilación de información (SCADA) como al centro de control de energía (CENACE), se analiza el canal de transmisión necesario para enviar los datos de interés por un enlace dedicado (exclusivo).

En primera instancia, se analiza el canal de datos necesario que requiere 1 generador para enviar información de 3 sensores y un controlador UPS conectados a un S7-3700 (PLC Siemens).

Tabla 4.

Datasheet S7-300.



© Siemens AG 2010

SIMATIC S7-300
Central processing units

Standard CPUs

Technical specifications (continued)

	6ES7 312-1AE14-0AB0	6ES7 314-1AG14-0AB0	6ES7 315-2AH14-0AB0	6ES7 315-2EH14-0AB0	6ES7 317-2EK14-0AB0
Product-type designation	CPU 312	CPU 314	CPU 315-2 DP	CPU 315-2 PN/DP	CPU 317-2 PN/DP
PROFINET CBA (at set set-point communication load)					
• Number of functions, master/slave				30	30
• Total of all Master/Slave connections				1 000	1 000
• Data length of all incoming connections master/slave, max.				4 000 byte	4 000 byte
• Data length of all outgoing connections master/slave, max.				4 000 byte	4 000 byte
• Number of device-internal and PROFIBUS interconnections				500	500
• Data length of device-internal und PROFIBUS interconnections, max.				4 000 byte	4 000 byte
• Data length per connection, max.				1 400 byte	1 400 byte

Tomado de (Siemens AG 2010, 2010)

La Tabla 4 muestra la característica relacionada a la interfaz LAN de comunicación (Profinet) respecto a 1 enlace *master/slave*, esto es, 4Kbyte como tamaño máximo.

Por tanto para el primer generador (AB_1) se tendrá:

$$AB_1 = \#conexiones\ x\ 4Kb$$

Luego:

$$AB_1 = (4\ conexiones\ maestro/esclavo\ + 2\ conexiones\ de\ control)\ x\ 4Kb$$

$$AB_1 = 6\ x\ 4Kb$$

$$AB_1 = 24Kb$$

Este ancho de banda es el que se conecta al switch en cascada hacia el segundo generador.

Para el segundo generador (AB_2), se tendrá una conexión de 16Kb sumado las 6 conexiones características del generador. Esto es:

$$AB_2 = AB_1 + (\#conexiones\ x\ 4Kb)$$

$$AB_2 = 24Kb + (6x4Kb)$$

$$AB_2 = 48Kb$$

De igual manera para el tercer generador (AB_3):

$$AB_3 = AB_2 + \ (\#conexiones\ x\ 4Kb)$$

$$AB_3 = \ 48Kb + (6\ x\ 4Kb)$$

$$AB_3 = 72Kb$$

Finalmente para el cuarto generador (AB_4):

$$AB_4 = \ AB_3 + (\#conexiones\ x\ 4Kb)$$

$$AB_4 = 72Kb + (6\ x\ 4Kb)$$

$$AB_4 = 96Kb$$

Por tanto para transporte de información relacionada a canales de control y sensores en la red de generadores es necesario un ancho de banda estaría dado por:

$$AB_{TG} = \ AB_4 + 20\%$$

SI:

$AB_{TG} = ancho\ de\ banda\ total\ generadores$

Luego:

$$AB_{TG} = 96Kb + \frac{(96Kb)x\ 20}{100}$$

$$AB_{TG} = 96Kb + 19{,}2Kb$$

Total ancho de banda necesario:

$$AB_{TG} = 115{,}2Kb$$

Los datos provenientes de los medidores de potencia, se emplea un PLC S7-1200 y su conexión es directa mediante red ethernet.

Por tanto se realiza el mismo análisis anterior tomando en cuenta que la tasa de transferencia en cada medidor de potencia es directamente enviada al switch de comunicación.

Al contar con 5 generadores, entonces se tiene 5 medidores de potencia.

Si:

$M = Medidor\ generador$

$AB_M = ancho\ de\ banda\ medidores\ de\ potencia$

Luego:

$$AB_M = payload + canal\ de\ control$$

$$AB_M = 4Kb + 4Kb$$

$$AB_M = 8Kb$$

Al tener 5 medidores con el mismo comportamiento, entonces el ancho de banda para cada medidor de potencia es el mismo.

Si:

$AB_{MT} = ancho\ de\ banda\ medidores\ de\ potencia$

$AB_{TM} = ancho\ de\ banda\ total$

$$AB_{MT} = 5\ X\ AB_M$$

$$AB_{MT} = 5\ X\ 8Kb$$

$$AB_{MT} = 40Kb$$

$$AB_{TM} = AB_{MT} + 20\%$$

$$AB_{TM} = 40Kb + \frac{(40Kb)x\ 20}{100}$$

$$AB_{TM} = 40Kb + 8Kb$$

Total ancho de banda necesario:

$$AB_{TM} = 48Kb$$

De esta manera determinamos que el ancho de banda total (AB_T) necesario para enviar información proveniente de sensores y medidores de potencia sería:

$$AB_T = AB_{TG} + AB_{TM}$$

$$AB_T = 115{,}2kB + 48\ Kb$$

$$AB_T = 163{,}2\ Kb$$

3. Capítulo III: Diseño de Entorno Cloud

En el capítulo 2, se describen los distintos equipamientos que dispone la central de generación para transporte, procesamiento, lectura y envío de información generada en sensores y medidores de potencia.

El presente capítulo tiene como finalidad validar la mejor alternativa de entorno en la nube tomando en cuenta los equipos y características necesarias para replicar la información de interés generada en la planta y que va a ser albergada en un entorno de acceso mediante Internet desde cualquier lugar del mundo.

La información migrada a la nube posee alta disponibilidad empleando un diseño de clúster en un entorno virtualizado además de un firewall para protección de información.

Debemos entonces analizar aspectos económicos, factibilidad, disponibilidad y alternativas de oferta en de proveedores en el mercado.

3.1. Elección de Modo Cloud

La central de generación eléctrica posee equipamiento propio y el cuál se encuentra distribuido geográficamente.

Bajo esta premisa, la información industrial que se obtiene en la planta y mostrada en el sistema SCADA local, debe ser replicada hacia la nube a través

de un enlace de datos definido y mostrada tal como si se estuviera en el lugar físico.

Figura 21. Entornos en la nube.
Tomado de *(Microsoft Azure, 2013)*

Tenemos 3 escenarios posibles para llevar nuestra información hacia la nube, de las cuáles debemos elegir la que más se acomode a nuestras necesidades.

Un entorno SaaS implicaría que el proveedor del servicio “alquilaría” todos los equipos requeridos para toma de información desde el origen de la información, es decir, desde la planta misma lo cual es innecesario ya que se cuenta con todos los elementos necesarios.

Un entorno PaaS en cambio ofrece servicios de administración de información (bases de datos), desarrollo y sistema operativo. Estas características pueden ser absorbidas por el administrador de la plataforma industrial ya que no constituye un campo complejo de implementar lo que reduce el costo.

En cambio un entorno IaaS ofrece una alternativa económica y que se ajusta a nuestras necesidades debido a que únicamente se “alquila” un equipo como infraestructura en el cual se establece el software de adquisición de datos SCADA, autenticación de usuarios, bases de datos local y seguridad de acceso.

Se requiere entonces de las siguientes características para replicar información de campo en la nube:

- Enlace dedicado.

- Características del equipo a ser virtualizado, esto es: CPU, Memoria RAM, Almacenamiento.

Se detalla a continuación en la Tabla 5 las características del ordenador obtenidas en sitio.

Tabla 5.

Características obtenidas del computador en sitio.

Información del sistema.	
Fecha y hora actuales:	lunes, 10 de junio de 2019, 10:33:52
Nombre del equipo:	GASGREEN
Sistema Operativo:	Windows 10 Pro 64 bits (10.0, compilación 17134)
Fabricante del sistema:	Dell Inc.
Modelo del sistema:	PowerEdge T30
BIOS:	BIOS Date: 11/14/16 02:49:04 Ver : 1.0.2
Procesador:	Intel(R) Xeon(R) CPU E3-1225 v5 @ 3,30 GHz (4CPUs), ≈ 6,3GHz
Memoria:	16384MB RAM
Archivo de paginación:	5376MB usados, 13305MB disponibles
Versión de DirectX:	DirectX 12

Se define de esta forma que el ambiente que más se acomoda a las necesidades es la de: Infraestructura en la nube (IaaS).

3.2. Alternativas en Mercado

Una vez definido el entorno a desarrollarse en la nube, se analiza las alternativas presentes en el mercado.

Se presentan 3 opciones verificadas en medio local. Estas son:

- CNT
- Claro Cloud
- Externa: AWS (Amazon)

3.2.1. Alternativa CNT

La empresa pública CNT ofrece el IaaS con la particularidad que, además del servicio de infraestructura en la nube, cuenta con servicio de Internet en sitio lo cuál es una ventaja sustancial para contratar tanto el enlace de comunicación como el de servicio de infraestructura en la nube.

La Tabla 6 muestra detalles del plan IaaS ofertado en el mercado y las características que ofrece:

- Procesamiento
- Almacenamiento
- Memoria

Tabla 6.

Costos IaaS ofertados por CNT

INFRAESTRUCTURA COMO SERVICIO (IaaS)

	SO	PROCESAMIENTO (GHz)	ALMACENAMIENTO (GB)	MEMORIA (GB)	TARIFA MENSUAL
CNT	Windows	1	20	2	$ 57.5
	Windows	2	40	4	$115
	Windows	4	80	8	$230
	Windows	8	120	16	$452,80

Adaptado de (CNT, 2019)

El plan más económico ($57,5) que corresponde a la primera opción, resulta suficiente para replicar la información proveniente de la planta hacia la nube, esto debido a que las características del computador en planta son utilizadas únicamente para visualizar y guardar la información proveniente de sensores y medidores de potencia.

No se requiere de procesamiento especial o consumo elevado de memoria en el medio virtual y/o físico ya que se trata de bajas velocidades de transferencia.

No se especifica el sistema operativo puntual para esta oferta, sin embargo, una versión profesional de Windows 7 será suficiente.

3.2.2. Alternativa Claro Cloud.

La empresa privada CONECEL ofrece servicios de Infraestructura en la nube cuyos planes están publicados en su página web de acuerdo con los servicios requeridos.

Tabla 7.

Planes IaaS Claro

INFRAESTRUCTURA COMO SERVICIO (IaaS)					
	SO	**PROCESAMIENTO (GHz)**	**ALMACENAMIENTO (GB)**	**MEMORIA (GB)**	**TARIFA MENSUAL**
CLARO	Windows 2008 R2 Enterprise	1	50	1	$ 59.36
	Windows 2008 SQL Web Edition	2	50	2	$ 104.16
	Windows 2008 R2 Standard, MS SQL Server Standard	1	50	2	$ 106.4

Adaptado de (CLARO, 2016)

La Tabla 7 muestra valores ofertados en el sitio web del proveedor y, al igual que con las ofertas del proveedor anterior, la primera opción será suficiente para el objetivo deseado ($59,36).

En la planta no se evidencia conexión cableada por parte de este proveedor para el servicio de Internet, por lo que el enlace entre la planta y el medio cloud que se oferta necesariamente debe ser de forma inalámbrica ya sea por antena satelital y/o telefonía celular.

Si bien el enlace y el servicio en la nube es posible con este proveedor, la diferencia radica fundamentalmente en el costo final.

Claro ofrece un sistema operativo en particular: Windows 2008 R2 Enterprise el cuál es suficiente para el propósito final.

3.2.3. Alternativa externa: AWS (Amazon).

Amazon tiene gran diversidad de servicios en la Nube.

Se debe tener en cuenta las características correctas y suficientes para que nuestro diseño tenga funcionalidad suficiente y evitar saturaciones y problemas de almacenamiento. Esto debido a que Amazon ofrece un pool de alternativas para elegir y de acuerdo a ello el costo mensual a facturar.

De igual manera que CNT, no se especifica el sistema operativo que oferta, pero ya se concluyó que no se requiere de un sistema operativo avanzado.

Detallamos a continuación en la Tabla 8, la selección realizada en el sitio oficial acorde a las necesidades requeridas y alternativas superiores con finalidad de validar costos con ofertas locales.

Tabla 8.

Opciones IaaS de proveedor externo AWS.

INFRAESTRUCTURA COMO SERVICIO (IaaS)					
	SO	**PROCESAMIENTO (GHz)**	**ALMACENAMIENTO (GB)**	**MEMORIA (GB)**	**TARIFA MENSUAL**
AWS	Windows	1	50	1	$ 57.8
	Windows	1	50	2	$ 94.4

	Windows	1	50	4	$ 167.6

Adaptado de (AWS, 2019)

3.2.4 Comparación de Alternativas.

Acorde a las características necesarias para migrar los datos a la nube indicadas en la Tabla 5, se afirma que el procesamiento, memoria y almacenamiento requeridos para diseñar el ambiente cloud, no amerita un tratamiento sofisticado o tasas altas de transferencia (<200Kbps).

La Tabla 9 recoge aspectos técnicos suficientes para el propósito requerido.

Tabla 9.

Comparativa para proveedores IaaS.

TABLA COMPARATIVA					
Alternativa	Memoria RAM (GB)	CPU (GHz)	Disco (GB)	Sistema Operativo	Costo Mensual (Dolares)
CNT	2	1	20	Windows (sin característica)	$57,50
CLARO	1	1	50	Windows 2008 R2 Enterprise	$59,36
AWS	1	1	50	Windows (sin característica)	$57,80

La opción del proveedor CNT es la opción más recomendable para nuestro efecto ya que a más de ofrecer el servicio de Infraestructura en la nube, provee del servicio de Internet al sitio remoto en la actualidad. Esto sumado a que su costo mensual es más bajo tomando en cuenta proveedores nacionales.

Las siguientes dos alternativas son opciones de diseño pero requieren de aspectos técnicos adicionales para brindar servicios en cloud, esto es, enlace de Internet y disponibilidad en sitio.

3.3. Clúster

Para obtener alta disponibilidad de información en la nube, es necesario implementar un diseño basado en clúster, esto es, tener 2 máquinas que comparten software industrial, almacenamiento, procesamiento y memoria similares.

El propósito de un diseño “clúster” es tener disponibilidad de información y recursos aun cuando 1 equipo falle por causas diversas.

En relación con el proyecto, se emplea un diseño basado en un ambiente virtualizado ya que únicamente se “alquila” un computador en modalidad IaaS.

Se requiere entonces software de virtualización para generar máquinas virtuales en la nube que compartan recursos físicos.

3.3.1. VMware

VMware, filial de EMC Corporation proporciona software de virtualización para ordenadores compatibles con X86.

Incluyen VMware Workstation, VMware Server y VMware Player que corren en procesadores Intel y funcionan en sistemas operativos Windows, Linux y Mac OS.

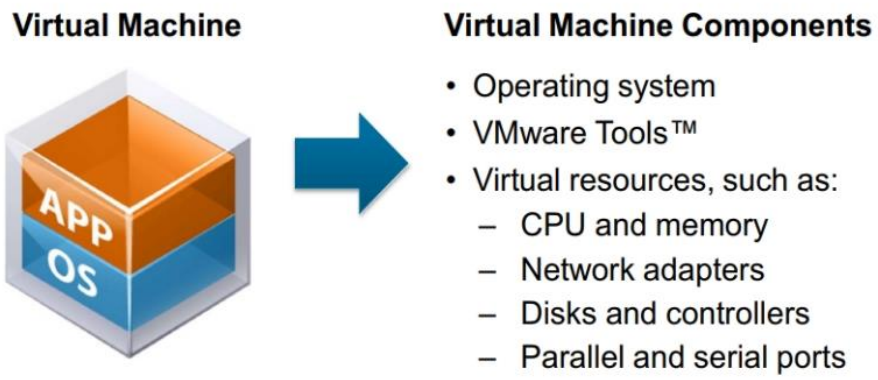


Figura 22. Máquina Virtual.
Tomado de *(eVantage, 2018)*

Una máquina virtual es la representación por software de un computador físico y todos sus componentes.

Un virtualizador por software permite ejecutar varios computadores (sistemas operativos) dentro de un mismo hardware de forma simultánea aprovechando al máximo los recursos físicos disponibles. Figura 23

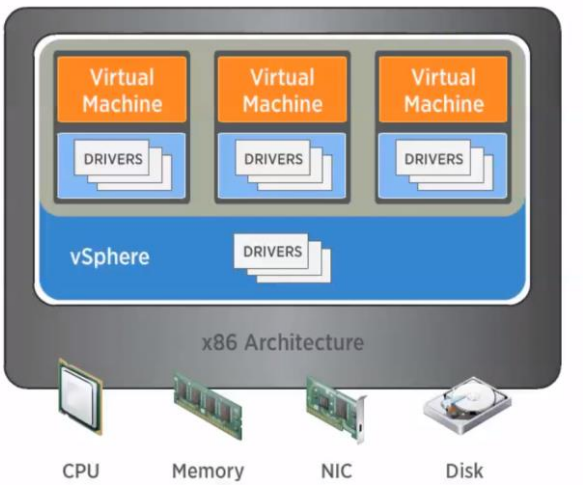


Figura 23. Virtualización.
Tomado de *(eVantage, 2018)*

El sistema de virtualización por software simula las características contratados en el proveedor IaaS de acuerdo con nuestras necesidades.

En este aspecto, dichas características deben distribuidas en dos equipos virtuales que van a trabajar en modo clúster para brindar alta disponibilidad a los datos industriales obtenidos desde la planta.

3.3.2. Crear clúster en VMware

Para el proceso de configuración de clúster se debe tener los siguientes elementos principales:

- Software de virtualización VMware vCenter Server: Es la plataforma instalada en el core del equipo físico el mismo que tiene administración de todas las funcionalidades que ofrece el entorno virtual.

  En esta plataforma se instalan (crean) los servidores virtuales, asignación recursos a los equipos, se brinda o limita conexión entre máquinas virtuales, etc.

- Conectividad de red con hosts que se unirán al clúster.

En primer lugar, se debe definir un “centro de datos”, para identificar los equipos que van a compartir recursos para dar alta disponibilidad a nuestro proyecto y se le asigna un nombre.

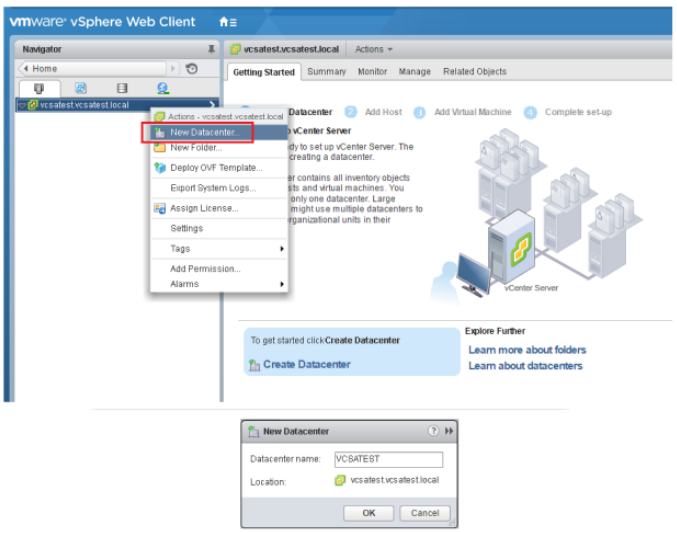


Figura 24. Creación del Centro de datos.
Tomado de (Lee, 2017)

Se crea el clúster y se le asigna un nombre.

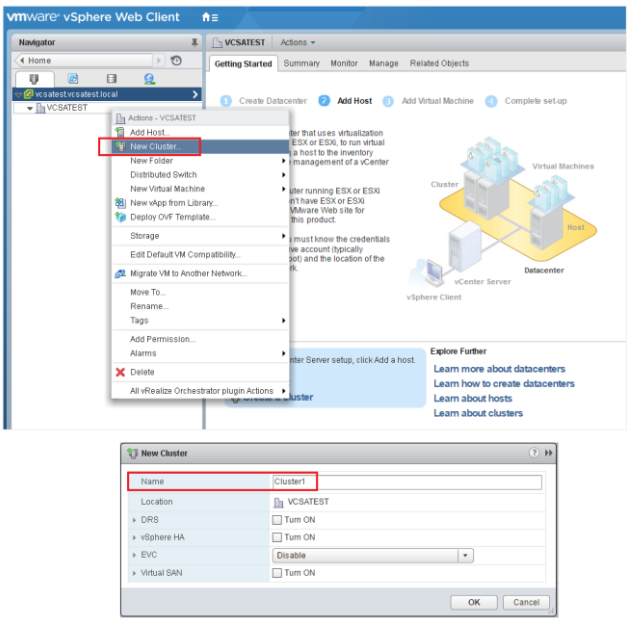


Figura 25. Creación de Clúster.
Tomado de *(Lee, 2017)*

Una vez definido el clúster, se procede a agregar los hosts que pertenecerán a dicho clúster.

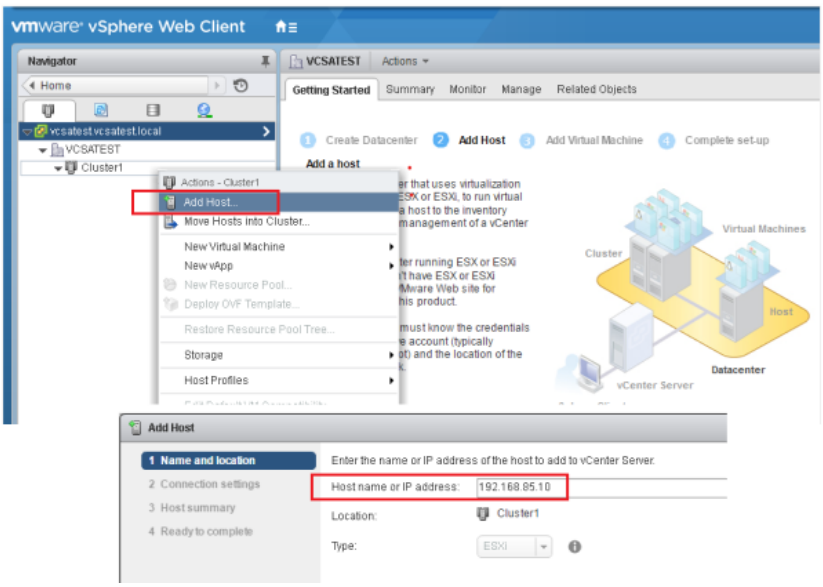


Figura 26. Agregación de Hosts al clúster.
Tomado de *(Lee, 2017)*

Posterior se proporciona credenciales para acceder a los hosts, certificados auto-firmados de forma predeterminada y licencias de evaluación.

La Figura 27 muestra el clúster creado y los hosts atados.

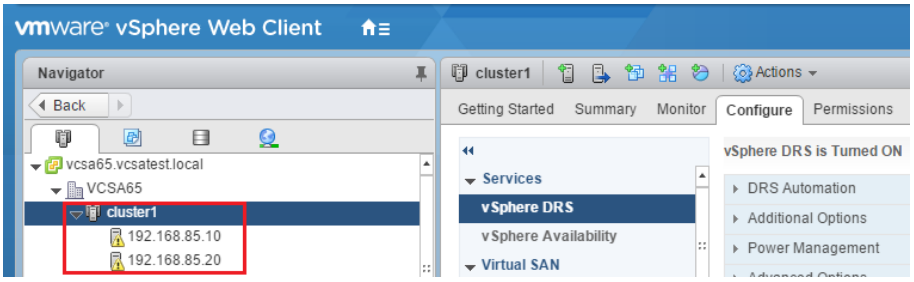


Figura 27. Clúster creado y hosts atados.
Tomado de *(Lee, 2017)*

La implementación de alta disponibilidad en el entorno contratado IaaS está dado por el software de virtualización, el cuál además de crear las máquinas virtuales como “hosts”, también configura el ambiente clúster que compartirá recursos entre los dos equipos virtuales de forma redundante.

Por tanto, las características contratadas al proveedor de servicio de Infraestructura en la nube que se elija (CNT, Claro, AWS), serán los valores que gestionar nuestras máquinas virtuales y clúster.

- Memoria RAM
- Disco
- Procesador

3.3.3. Seguridad en la nube

La seguridad es un punto muy importante en cualquier ámbito.

Independientemente del fabricante, la seguridad informática se refiere a un “firewall” instalado localmente en cada máquina virtual y que su función principal

es la de bloquear amenazas, ofrecer autenticación de usuario, evitar propagación de código desconocido, etc.

Específicamente para proteger información albergada en un servidor virtual hay varias opciones.

Alternativas como: Sophos, Fortinet, AWS Firewall son algunos productos que ofrecen seguridad para equipos perimetrales en una red física como en cloud.

3.3.3.1. Sophos

Inicialmente desarrollo productos antivirus y de cifrado.

La principal funcionalidad es mantener la seguridad TI de forma fiable a medida que aumenta la complejidad de redes TI.

Sophos brinda soluciones para proteger estaciones de trabajo de la red: portátiles, máquinas y servidores virtuales, servicios web, dispositivos móviles y correo electrónico.

Empresas tales como: Toshiba, Avis, Pixar, Xerox son algunas entidades que protegen sus redes con esta solución de seguridad.

3.3.3.2. Fortinet

Empresa Norteamericana dedicada a fabricación y diseño de componentes y dispositivos de seguridad en redes.

Constituyen una generación de equipos de seguridad de alto rendimiento que garantizan protección completa de sistemas en tiempo real.

Fortinet comercializa y desarrolla software y hardware enfocados en seguridad de redes informáticas.

Su nombre proviene de "*fortified networks"* (redes fortificadas) y constituye la cuarta empresa de seguridad de redes más grande a nivel mundial (iCORP, 2017).

Figura 28. Equipo FortiGate 200E para seguridad informática.
Tomado de *(FORTINET, 2019)*

Fortigate es el producto para Hardware y es una plataforma unificada de amenazas la cuál integra una gama completa de servicios y funciones de seguridad para proteger redes de sofisticadas amenazas.

Sus características son:

- Alta Disponibilidad
- Balanceo
- QoS
- Virtualización
- VPN
- Antivirus
- IDS/IPS
- Antispam

3.3.3.3. AWS Firewall

Es parte de Amazon.com y proporciona plataformas de computación en la nube bajo demanda de usuarios.

Es un servidor de seguridad de aplicaciones web de amenazas que pueden comprometer la seguridad o consumir recursos de la red.

El usuario es el encargado de crear reglas personalizadas diseñadas para bloquear patrones comunes de ataques tales como scripts entre sitios.

Dispone de una API con todas las funcionalidades que permite a usuarios automatizar la creación, implementación y mantenimiento de las reglas creadas.

Amazon cobra el servicio acorde a las reglas definidas y deseadas por los usuarios de acuerdo a las necesidades.

3.4. Recopilación de características obtenidas.

Determinadas las características del equipo a implementar en Cloud, la velocidad de transferencia requerida para transporte de información desde la planta, plan del proveedor seleccionado para el servicio IaaS en el mercado, necesidad de alta disponibilidad y seguridad de información en la nube; se plantea la siguiente alternativa plasmada en la Tabla 10.

Se detallan entonces los siguientes aspectos:

Tabla 10.
Resumen de Características.

	Característica	**Proveedor / Fabricante**	**Observación**
Enlace Dedicado	3Mbps	CNT	Disponible en planta. Transporte de Información, internet empresarial, correo.
Sistema Operativo	Windows 7, 8 Professional	Personal	Instalación de software industrial SCADA y programador PLC´s.

Clúster	Réplica a Máquina Virtual con similares características	VMware	Alta Disponibilidad
IaaS	$57,5 mensual	CNT	Enlace e IaaS con un solo proveedor.
Seguridad	Sophos	CNT	Soporte ofertado por CNT

4. Capítulo IV: Normativas de Seguridad Industrial

Una normativa industrial es una normalización que brinda garantía de que los sistemas y productos desarrollados presenten características deseadas en cuanto a eficacia, seguridad, fiabilidad y calidad.

En relación con sistemas de control, las normativas se centran principalmente en funcionamiento de dispositivos o a las especificaciones de los protocolos de comunicación.

El sector industrial demanda normativas de seguridad para proteger las instalaciones surgiendo así guías de seguridad y grupo de normas listadas a continuación.

4.1. ISA99

Engloba guías e informes técnicos de los que se publicaron las guías (ANSI/ISA-99.01.01-2007 y ANSI/ISA-99.02.01-2009) y el informe técnico SI/ISA-TR99.01.02-2007 (INCIBE, 2015).

La primera guía ANSI/ISA-99.01.01-2007 incluye términos, modelos y conceptos que han de usarse en componentes de la serie.

La guía ANSI/ISA-99.02.01-2009 describe elementos para implantación de sistemas de gestión de ciberseguridad y cómo conocer requerimientos de cada elemento.

El informe técnico SI/ISA-TR99.01.02-2007 recoge herramientas de seguridad, despliegue y modo de implantación en sistemas de control.

4.2. NIST SP 800-82

Realizada por Instituto Nacional de Estándares y Tecnología (NIST) y publicado en 2011, proporciona guías para seguridad de sistemas de control incluido SCADA (INCIBE, 2015).

Define topologías típicas de los sistemas industriales, proporciona contramedidas y recomendaciones para mitigar riesgos e identifica vulnerabilidades y amenazas.

4.3. NIST SP 800-53

De igual manera desarrollado por NIST, el propósito de esta guía es proporcionar guías de control de seguridad para sistemas de información que transmiten, almacenan y procesan información (INCIBE, 2015).

Una parte del documento recopila controles de seguridad diseñados para facilitar el cumplimiento con diversas leyes.

Fue publicada en 2013.

4.4. RG 5.71

Publicada para establecer controles para cumplimientos de regulaciones respecto a protección de ordenadores, comunicaciones y redes frente a ciberataques (INCIBE, 2015).

Describe una estrategia de defensa consistente mediante un conjunto de controles basados en NIST SP 800-82 como en NIST SP 800-53.

Los controles están diferenciados en 3 categorías:

- Gestión
- Técnicos y
- Operacionales

4.5. IEC 62443

Elaborada por el grupo TC65 de la IEC, es una evolución de la norma ISA99 con la finalidad de complementarla y ampliar capacidades de actuación (INCIBE, 2015).

Comprende un total de 13 documentos que se dividen en:

- 5 informes técnicos
- 1 especificación técnica y
- 7 guías

Estos documentos se agrupan en 4 bloques según el contenido y se muestran en la Figura 29.

- General
- Políticas y procedimientos
- Sistemas y
- Componentes

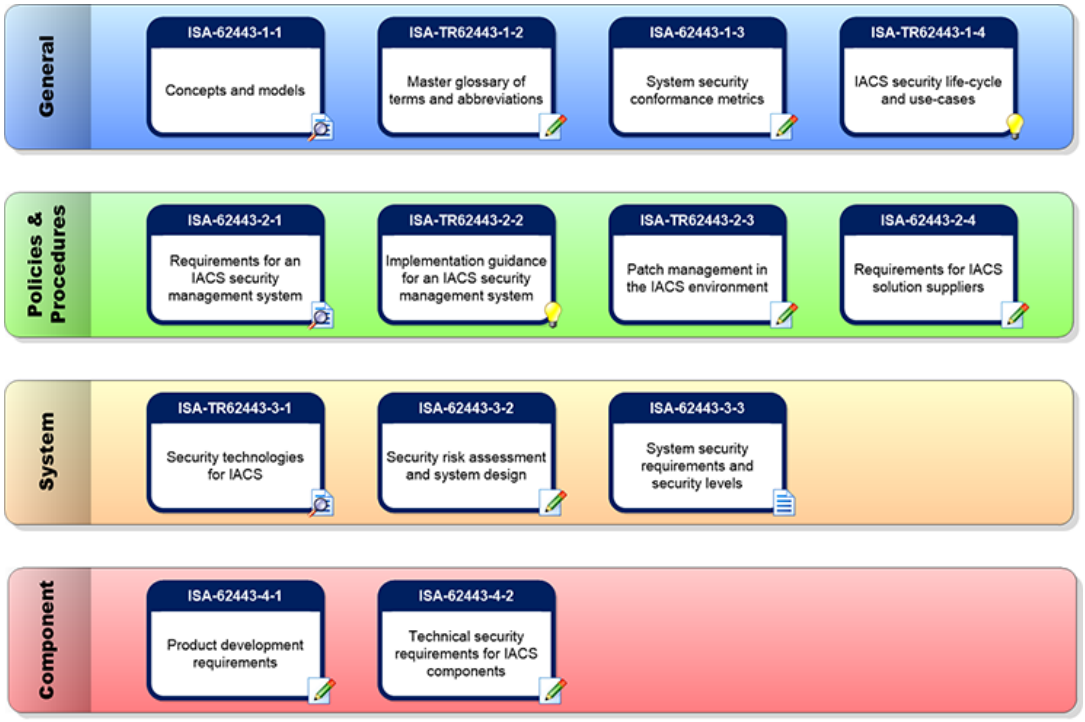


Figura 29. Documentos que conforman la norma IEC 62443.
Tomado de *(INCIBE, 2015)*

4.6. NERC CIP

NERC, organismo regulador de energía de EEUU, cuya finalidad es validar la seguridad de las instalaciones en general, creó guías con controles de cumplimiento obligado (INCIBE, 2015).

Inicialmente se crearon 9 guías de las cuáles, excepto una, se referían con ciberseguridad.

Posterior se ampliaron a 11 guías.

Ésta norma reconoce los roles distintos de cada entidad en operación del sistema eléctrico, vulnerabilidad de activos, criticidad y riesgos a los que están expuestos.

Demanda para gestión y mantenimiento de un sistema eléctrico cada vez más seguro por parte del negocio y la operación provoca que los ciberactivos

soporten cada vez más procesos y funciones clasificados como críticos para comunicarse entre ellos intercambiando servicios y datos.

5. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

El sistema de adquisición de datos SCADA es ampliamente utilizado en la industria; concretamente el sistema nacional de control de energía CENACE realiza el monitoreo de varias centrales de generación eléctrica a nivel nacional a través de esta herramienta.

PLC's de la gama Siemens S7-300 y S7-1200 son empleados en el campo industrial debido a que brindan un servicio confiable para controlar funcionalidad de bombas, motores, sensores, aspiradores, etc., instalados en entornos hostiles.

Cloud computing permite acceder a servicios albergados en un equipo físico o virtual mediante Internet desde cualquier lugar y en cualquier momento.

La velocidad de transmisión necesaria para transportar información del campo industrial al ambiente cloud no supera los 200Kbps, por lo que un enlace de 3Mbps es suficiente para obtener transporte de información, internet corporativo, además de correo.

La alternativa CNT es la elegida para el efecto ya que cuenta con enlace dedicado en sitio, IaaS y soporte para seguridad de información en nube mediante Sophos.

La información enviada al entorno cloud deberá ser protegida, para tal efecto se dispone de alternativas tanto en hardware como en software, en cuyo caso dependerá del presupuesto dispuesto para elegir la alternativa más efectiva.

Los costos ofertados por empresas nacionales en relación con servicios de Infraestructura como servicio IaaS son relativamente similares entre ellos y es nuestra decisión elegir el proveedor que más confianza refleja en el medio local.

Un proveedor externo oferta servicios IaaS, pero el enlace dedicado dependerá del medio local y si llega al sitio de interés por lo que no es una alternativa viable para el propósito deseado.

5.2 Recomendaciones

El diagrama eléctrico y de red de una instalación industrial debe ser cuidadosamente analizada para determinar correctamente todos los elementos que están involucrados en un proceso o función y así distinguir claramente parámetros de medición.

Si un servicio a contratar es más costoso, no necesariamente nos indica que es mejor que ante otra alternativa. En este aspecto se debe considerar confianza, soporte y reputación de determinada empresa.

Previamente se debe realizar un análisis de costo-beneficio y determinar la necesidad o no de migrar información hacia la nube.

La seguridad en la nube es importante y la administración de la misma debe ser responsabilidad de personal adecuado, por lo que es recomendable gestionar la seguridad de la nube a través del mismo proveedor de servicios IaaS.

REFERENCIAS

Ahmad, I. (2017). *Cloud Computing - A Comprehensive Definiton*. Recuperado el 11 de Junio de 2019, de https://www.researchgate.net/publication/314072571_Cloud_Computing_-_A_Comprehensive_Definiton

AIE. (2013). *PROTOCOLOS DE COMUNICACIONES INDUSTRIALES.* Obtenido de http://www.aie.cl/files/file/comites/ca/articulos/agosto-06.pdf

AWS. (2019). *SIMPLE MONTHLY CALCULATOR.* Recuperado el 27 de Febrero de 2019, de https://calculator.s3.amazonaws.com/index.html

Calfi, A. (2011). *APLICACIONES DEL PLC*. Recuperado el 20 de Mayo de 2019, de http://aplicacionesdeplc.blogspot.com/2011/03/estructura-de-un-plc.html

Chicúe, H. D. (2015). *Automatización y Control Industrial*. Recuperado el 10 de Enero de 2019, de http://hernandariogomezchicue.blogspot.com/p/acerca-del-administrador.html

Chicúe, H. D. (2015). *Automatización y Control Industrial [Figura del blog]*. Recuperado el 10 de Junio de 2019, de http://hernandariogomezchicue.blogspot.com/p/sistemas-scada.html

Christof. (2019). *Christof-strauch.de*. Recuperado el 07 de Abril de 2019, de https://www.christof-strauch.de/nosqldbs.pdf: https://www.christof-strauch.de/nosqldbs.pdf

CLARO. (2016). *Claro-cloud.* Recuperado el 29 de Junio de 2019, de https://www.clarocloud.com.ec/portal/ec/cld/infraestructura/servidores_virtuales/#info-02

CNT. (2019). *SOLUCIONES, COMUNICACIÓN MÓVIL, GOBIERNO.* Recuperado el 30 de Abril de 2019, de https://www.gobiernoelectronico.gob.ec/wp-content/uploads/downloads/2017/11/Presentaci%C3%B3n-Mintel-11-2017.pdf

Common, H. (2016). *Elentornodehadoop.wordpress.com. El entorno de Hadoop*. Recuperado el 19 de Marzo de 2019, de https://elentornodehadoop.wordpress.com/tag/hadoop-common/

Cook, J. D. (2009). *ACID versus BASE for database transactions*. Recuperado el 07 de Abril de 2019, de https://www.johndcook.com/blog/2009/07/06/brewer-cap-theorem-base/

Cornejo, A. M., & Díaz, C. F. (2015). *Análisis, Diseño e Implementación de Cloud Computing para una Red de Voz sobre IP (Tesis de Pregrado).* Universidad Politécnica Salesiana. Recuperado de https://dspace.ups.edu.ec/bitstream/123456789/7921/1/UPS-CT004762.pdf

Corrales, L. (2007). Interfaces de Comunicación Industrial. Recuperado el 17 de Junio de 2019

eVantage. (2018). *VMware vSphere: Install, Configure, Manage.* Recuperado el 15 de Mayo de 2019, de https://evantage.gilmoreglobal.com/#/

Fernández, E. (2017). *Big Data eje estratégico en la industria audivisual.* Barcelona: UOC. doi:78-84-9116-415-9

Forrester. (2019). *The Pragmatic Definition Of Big Data*. Recuperado el 31 de Marzo de 2019, de https://go.forrester.com/blogs/12-12-05-the_pragmatic_definition_of_big_data/

FORTINET. (11 de Enero de 2019). *FortiGate 200E Series.* Obtenido de https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_200E_Series.pdf

Gartnet. (2019). *Gartner IT Glossary*. Recuperado el 31 de Febrero de 2019, de What Is Big Data? - Gartner IT Glossary - Big Data: https://www.gartner.com/it-glossary/big-data

GEBNETA. (2019). *NoSQL: clasificación de las bases de datos según el teorema CAP*. Recuperado el 07 de Abril de 2019, de https://www.genbeta.com/desarrollo/nosql-clasificacion-de-las-bases-de-datos-segun-el-teorema-cap

Hansen, S. (2017). *Private Cloud vs Public Cloud Computing*. Recuperado el 12 de Mayo de 2019, de https://hackernoon.com/private-cloud-vs-public-cloud-computing-e2aeed6df46

IBM. (2013). *Almacenamiento de datos estructurados con Big Data*. Recuperado el 04 de Marzo de 2019, de https://www.ibm.com/developerworks/ssa/library/bd-almacenamiento-datos/index.html

iCORP. (2017). *Fortinet: la solución para proteger la infraestructura de TI*. Obtenido de http://www.icorp.com.mx/blog/fortinet/

Iglesias, A. (2014). *BEEVA Soluciones de tecnología e innovación para empresas. YARN, la solución de Hadoop para modelos de procesamiento*. Recuperado el 21 de Marzo de 2019, de https://www.beeva.com/beeva-view/tecnologia/yarn-la-solucion-de-hadoop-para-la-coexistencia-de-modelos-de-procesamiento/

INCIBE. (2015). *Normativas de seguridad en sistemas de control.* Obtenido de https://www.incibe-cert.es/blog/normativas-seguridad-sistemas-control

Lee, B. (2017). *NAKIVO*. Recuperado el 30 de Febrero de 2019, de Configuring a VMware ESXi Cluster [Artículo del blog]: https://www.nakivo.com/blog/configuring-vmware-esxi-cluster/

Libygem. (2015). *Tipos de Nube (Cloud Computing)*. Recuperado el 25 de Junio de 2019, de https://lanubedefher.wordpress.com/2015/11/05/tipos-de-nube-cloud-computing/

Manaure, A. (s.f.). *Señor CIO ¿Cómo será una empresa híbrida?* Recuperado el 15 de Abril de 2019, de http://www.cioal.com/2012/03/19/senor-cio-como-sera-una-empresa-hibrida/

Meichsner, K. (2004). *Electro Industria*. Recuperado el 25 de Junio de 2019, de Automatización: http://www.emb.cl/electroindustria/articulo.mvc?xid=95&edi=36&xit=el-protocolo-hart

Microsoft Azure. (2013). *Infraestructura como servicio*. Recuperado el 11 de Junio de 2019, de https://azure.microsoft.com/es-es/overview/what-is-iaas/

MongoDB. (2019). *NoSQL Databases Explained*. Recuperado el 07 de Enero de 2019, de https://www.mongodb.com/nosql-explained?lang=es-es

NIST. (2017). *NIST Big Data Working Group (NBD-WG)*. Recuperado el 31 de Febrero de 2019, de Bigdatawg.nist.gov: https://bigdatawg.nist.gov/

Paz, A. (2005). *Seguridad SCADA: Honeypots para simular redes SCADA III. [figura del blog]*. Recuperado el 01 de Julio de 2019, de https://www.gurudelainformatica.es/2016/08/seguridad-scada-honeypots-para-simular.html

Siemens AG 2010. (2010). *SIMATIC S7-300.* Recuperado el 12 de Abril de 2019, de https://www.paratrasnet.ro/pdf/automatizari-industriale/S7-300.pdf

Talend. (2019). *What is Data Processing? Definition and Stages - Talend Cloud Integration*. Recuperado el 31 de Enero de 2019, de Talend Real-Time Open Source Data Integration Software: https://www.talend.com/resources/what-is-data-processing/

TechTarget. (2019). *¿Qué es Análisis de “big data”? - Definición en WhatIs.com*. Recuperado el 22 de Enero de 2019, de SearchDataCenter en Español: https://searchdatacenter.techtarget.com/es/definicion/Analisis-de-big-data

ZIV. (2011). *USP 020 – Multifunction RTU for MV/LV switchgear applications*. Recuperado el 20 de Mayo de 2019, de https://www.zivautomation.com/distribution_automation/mv_automation/modular-rtu-for-mv-automation-usp-20/

ANEXOS

Anexo 1. Datasheet Siemens S7-300

Technical specifications (continued)

	6ES7 312-1AE14-0AB0	6ES7 314-1AG14-0AB0	6ES7 315-2AH14-0AB0	6ES7 315-2EH14-0AB0	6ES7 317-2EK14-0AB0
Product-type designation	CPU 312	CPU 314	CPU 315-2 DP	CPU 315-2 PN/DP	CPU 317-2 PN/DP
PROFINET CBA (at set set-point communication load)					
• Number of functions, master/slave				30	30
• Total of all Master/Slave connections				1 000	1 000
• Data length of all incoming connections master/slave, max.				4 000 byte	4 000 byte
• Data length of all outgoing connections master/slave, max.				4 000 byte	4 000 byte
• Number of device-internal and PROFIBUS interconnections				500	500
• Data length of device-internal und PROFIBUS interconnections, max.				4 000 byte	4 000 byte
• Data length per connection, max.				1 400 byte	1 400 byte
• Remote interconnections with acyclic transmission					
- Sampling frequency: Sampling time, min.				500 ms	500 ms
- Number of incoming interconnections				100	100
- Number of outgoing interconnections				100	100
- Data length of all incoming interconnections, max.				2 000 byte	2 000 byte
- Data length of all outgoing interconnections, max.				2 000 byte	2 000 byte
- Data length per connection, max.				1 400 byte	1 400 byte
• Remote interconnections with cyclic transmission					
- Transmission frequency: Transmission interval, min.				10 ms	10 ms
- Number of incoming interconnections				200	200
- Number of outgoing interconnections				200	200
- Data length of all incoming interconnections, max.				2 000 byte	2 000 byte
- Data length of all outgoing interconnections, max.				2 000 byte	2 000 byte
- Data length per connection, max.				450 byte	450 byte
• HMI variables via PROFINET (acyclic)					
- Number of stations that can log on for HMI variables (PN OPC/iMap)				3; 2x PN OPC/1x iMap	3; 2x PN OPC/1x iMap
- HMI variable updating				500 ms	500 ms
- Number of HMI variables				200	200
- Data length of all HMI variables, max.				2 000 byte	2 000 byte