

## **RIESGOS Y BENEFICIOS DE LA INTEGRACIÓN DE UN SISTEMA SCADA CLOUD**

### **RISKS AND BENEFITS OF THE INTEGRATION CLOUD SCADA SYSTEM.**

**Rene Ardila Navarro.\* Johan Sebastian Zapata Acero.\*\***

#### **Resumen:**

El presente artículo identifica y busca hacer una revisión sobre los riesgos y beneficios que conlleva la integración de un sistema de supervisión y adquisición de datos (SCADA) en un entorno Cloud, haciendo énfasis en las capacidades, oportunidades, riesgos y alternativas de la gestión integral y dinámica de la información, en un proceso industrial automatizado y en la nube. El internet permite una disponibilidad remota y continúa para monitorear el rendimiento de un proceso industrial en cualquier lugar y en cualquier momento, brindando la posibilidad de tomar decisiones en tiempo real, sin la necesidad de presentarse personalmente en el lugar específico, de allí la importancia en la implementación de protocolos seguridad y protección para este tipo de sistemas SCADA Cloud, que recogen información de gran importancia.

---

\* Tecnólogo en Electrónica, Universidad Distrital Francisco José de Caldas, Colombia.  
[johanszapataa@gmail.com](mailto:johanszapataa@gmail.com).

\*\* Tecnólogo en Electrónica, Universidad Distrital Francisco José de Caldas, Colombia.  
[ardila\\_rene@yahoo.com](mailto:ardila_rene@yahoo.com).

**Palabras clave:** Sistema de supervisión y adquisición de datos (SCADA), Nube, HMI, seguridad cibernética

**Abstract:** This article identifies and seeks to make a review of the risks and benefits of the integration of a Supervisory Control And Data Acquisition (SCADA) on a Cloud environment, emphasizing the capabilities, opportunities, risks and alternatives of integrated management and dynamic information, in an automated industrial process on the cloud. The Internet allows remote availability and continues to monitor the performance of an industrial process, at anywhere and at any time, providing the ability to make decisions in real time, without the need to appear in person at the specific place, hence the importance in the implementation of security protocols and safety for this type of Cloud SCADA systems, which collect information of great importance.

**Key Words:** Supervisory Control and Data Acquisition system (SCADA), Cloud, HMI, Cyber Security.

## **1. Introducción**

En la industria, la ventaja competitiva por lo general es adquirida por las empresas que hacen uso de la tecnología para automatizar sus líneas de producción, la tendencia a recopilar grandes cantidades de información de todos los niveles de la organización, ha empujado a

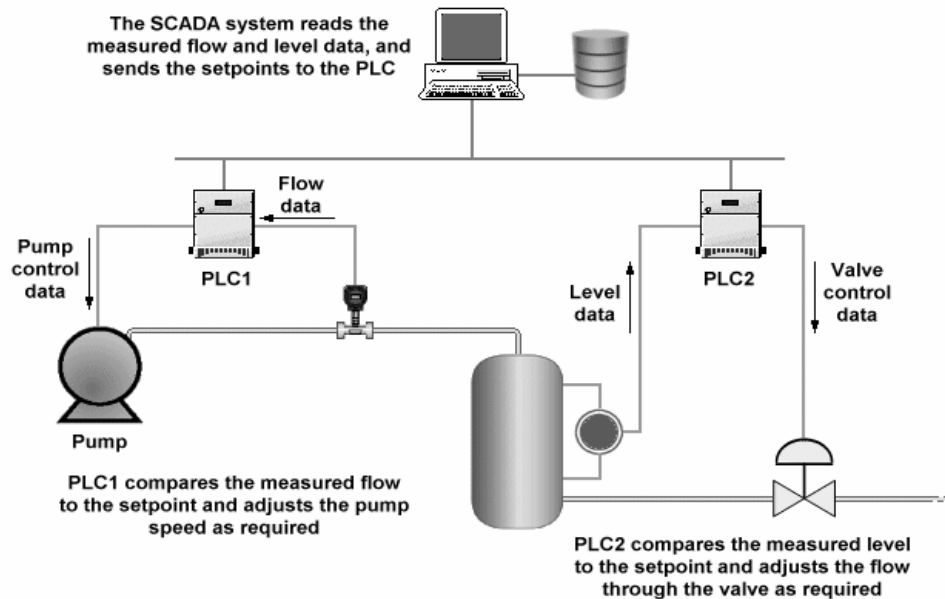
los sistemas SCADA como componentes de gran importancia en un proceso industrial automatizado [1]. La integración de sistemas SCADA en la nube (Cloud) no solamente es una alternativa para almacenar información de forma económica y obtener una gran capacidad de computación, también es una herramienta que puede facilitar una gestión de producción en un entorno industrial, gracias a la flexibilidad, la disponibilidad y la movilidad que permite la Internet [2].

## **2. SCADA (*Control de Supervisión y Adquisición de Datos*)**

SCADA comprende todas aquellas soluciones de aplicación para referirse a la captura de información de un proceso o planta industrial automatizada, SCADA hace referencia a un sistema central de monitoreo y control, que recopila información específica de un proceso y es capaz de realizar análisis, identificar y visualizar características del proceso y rendimiento del mismo [3].

El flujo de la información en los sistemas SCADA inicia con la variable que se desea medir, que depende del proceso, por ejemplo la presión, la temperatura, el flujo, la intensidad de corriente, el voltaje, etc. [11]. Este fenómeno debe traducirse a una variable inteligible para el sistema SCADA, y para ello se utilizan los sensores o transductores que convierten las variaciones del fenómeno físico en variaciones eléctricas proporcionales. Una vez acondicionada la señal, esta misma se convierte en un valor digital, equivalente a una conversión de datos [4]. Toda esta información es almacenada y se utiliza para su

correspondiente análisis y para la toma de decisiones. En la Figura 1 se puede observar el esquema básico de un sistema SCADA/HMI.

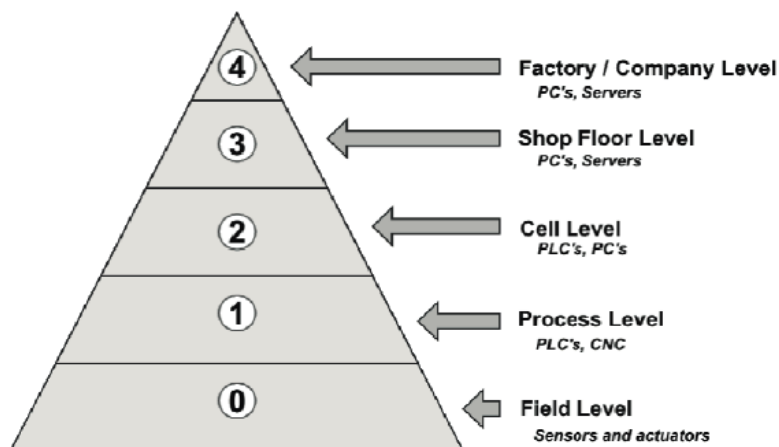


**Figura 1. Esquema básico sistema SCADA/HMI. Fuente: SCADA system**

**design: a proposal for optimizing a production line, IEEE.**

### 3. La Pirámide CMI

Los sistemas de control y supervisión se crean basándose en un modelo propuesto por el ingeniero francés Jean Baptiste Walder, que se llama *Computer Integrated Manufacturing* (CIM), que es esencial en la identificación de la estructura jerárquica y funcional de un sistema de producción en fábrica. En la Figura 2 se puede observar la pirámide CIM.



**Figura 2. Pirámide CIM. Fuente: SCADA system**

**design: a proposal for optimizing a production line, IEEE.**

La pirámide CIM de la Figura 2 pone de relieve cuatro niveles presentes en la mayoría de los sistemas de fabricación [1]:

**Nivel 0:** Incluye dispositivos (sensores y actuadores) que recogen los datos de las variables físicas y los envían al plano de trabajo.

**Nivel 1:** Incluye dispositivos como PLC (Controladores lógicos programables) o DCSs, RTU, los PAC y PC que recopilan información de las variables físicas medidas y analizan los datos de proceso, y luego la envían.

**Nivel 2:** El coordinador, que está a cargo de la supervisión y control de los procesos (Supervisión y adquisición de datos - SCADA), y de la generación y la trazabilidad de información relevante, para la gestión del proceso en los niveles superiores.

**Nivel 3:** Está a cargo de la planificación y la fabricación de los productos MES (Manufacturing Enterprise System) y MRP (Material Requirement Planning).

**Nivel 4:** Toma la información de los procesos, para analizar en los sistemas de información de la empresa. ERP (Enterprise Resources Planning).

#### **4. Cloud Computing**

Un modelo que permite la ubicuidad, el acceso a la red bajo demanda para compartir un conjunto de recursos informáticos configurables. Por ejemplo las redes, servidores, almacenamiento, aplicaciones y servicios. Que pueden ser rápidamente compartidos con el mínimo esfuerzo de gestión o interacción con el proveedor [6].

El “*Cloud computing*” permite la separación de las aplicaciones, de la plataforma sobre la que se ejecutan (incluyendo servidores, redes y almacenamiento). Mientras que la “*virtualización*” separa el sistema operativo de su hardware [13].

NIST (The National Institute of Standards and Technology) describe cinco características esenciales de la computación en la nube [7]:

*On-demand self-service*, Un consumidor puede acceder a las capacidades de prestación de computación de manera unilateral, como a servidores de red y almacenamiento.

*Broad network access*, Las capacidades están disponibles en la red y se puede acceder a través de mecanismos estándar que promuevan el uso de plataformas de cliente delgado (por ejemplo, teléfonos móviles, tabletas, ordenadores portátiles y estaciones de trabajo).

*Resource pooling*, Los recursos informáticos del proveedor se combinaron para servir a múltiples consumidores, mediante un modelo de múltiples usuarios, con diferentes recursos físicos y virtuales, asignados dinámicamente y reasignados de acuerdo con la demanda de los consumidores.

*Rapid elasticity*, Las capacidades pueden ser elásticamente aprovisionadas y liberadas, en algunos casos de forma automática, las capacidades disponibles para la provisión menudo parecen ser ilimitadas y pueden ser apropiados en cualquier cantidad en cualquier momento.

*Measured service*, sistemas CLOUD controlan automáticamente y optimizan el uso de recursos mediante funciones de medición en un cierto nivel de abstracción apropiado para el tipo de servicio (por ejemplo, cuentas, almacenamiento, procesamiento, ancho de banda, y cuentas de usuario activas).

#### **4.1. Modelos de servicio Cloud**

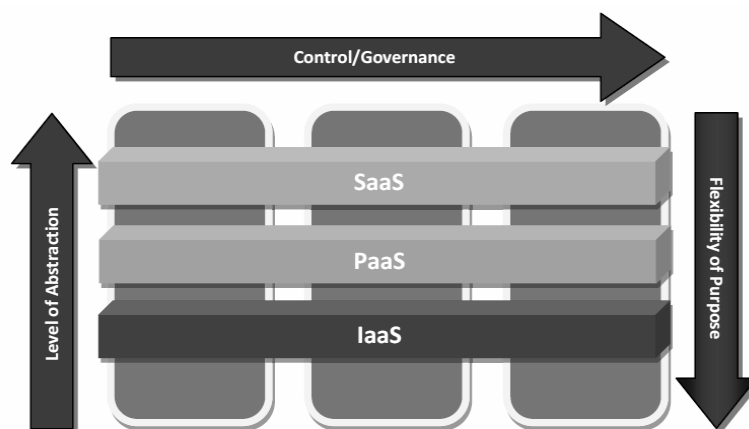
La computación en nube se puede describir en tres modelos de servicio [7]:

*Software as a Service (SaaS)*, ofrece aplicaciones de usuario final a través de Internet como un servicio completo sobre la demanda. El consumidor puede tener en la nube, elección de preferencia limitada y ajustes, y no tiene control de la infraestructura de la nube. El consumidor puede tener limitaciones en las preferencias de selección y ajustes y no tiene control sobre la infraestructura de la nube.

*Platform as a Service (PaaS)*, proporciona una combinación de plataformas, servicios y herramientas de desarrollo de aplicaciones bajo demanda. El consumidor cloud tiene control sobre las aplicaciones y la configuración de la plataforma.

*Infrastructure as a Service (IaaS)*, ofrece la infraestructura informática subyacente; servidores, redes y software bajo demanda. Estos se utilizan a continuación para la plataforma con la que el consumidor cloud desarrolla y aloja aplicaciones. Este tipo de servicio puede dar a los usuarios, la libertad de elegir los sistemas operativos y el entorno de desarrollo [12]. Aparte de la infraestructura física, la seguridad se lleva a cabo por parte del consumidor cloud.

La Figura 3 muestra los modelos de servicio SCADA/HMI Cloud mencionados.



**Figura 3. Modelos de servicio SCADA/HMI Cloud. Fuente: Securing Scada In The Cloud: Managing The Risks To Avoid The Perfect Storm, IEEE.**



## **4.2 Modelos de implementación Cloud**

Existen diferentes modelos de implementación para la computación Cloud, éstos describen la gestión, la propiedad y la naturaleza de los recursos que se utilizan para los servicios que se entregan a los usuarios. Los modelos de implementación también se diferencian del tipo de cliente [7].

- Cloud Publica, una nube pública, como su nombre indica, en donde los recursos informáticos y de infraestructura, están disponibles para el público.
- Cloud Privada, Una nube privada es operada exclusivamente por una organización específica, o su gestión puede ser delegada a terceros. Las nubes privadas ofrecen a las organizaciones un control sobre la infraestructura y los recursos en la nube.
- Comunidad Cloud, una nube comunitaria combina características tanto privadas como públicas, y es el resultado de colaboración entre las organizaciones con necesidades comunes, como la regulación, la seguridad y la privacidad;
- Cloud Híbrida, una nube híbrida puede ser una combinación de dos o más tipos de nube, ya sea pública, privada o comunitaria. Las nubes híbridas vinculan a las organizaciones mediante el uso de tecnología común que proporciona aplicaciones en la nube o la tecnología subyacente de apoyo a la movilidad de datos.

## **5. Beneficios de implementación de un sistema SCADA Cloud**

La mayoría de los procesos industriales que tienen sistemas SCADA están centralizados en la planta de manufactura [12]. En la actualidad, muchos de estos procesos se migran hacia la nube debido a que los riesgos se han ido mitigando y los beneficios son más grandes y flexibles. Algunos de los beneficios a grandes rasgos se pueden ver a continuación:

### **5.1. Pague sólo por lo que use**

Muchos procesos centralizados de automatización y monitoreo industrial son costosos, necesitan de personal especializado para operación y mantenimiento, requieren de equipo (hardware) y software especializado el cual aumenta los costos operativos del proceso. En un sistema Cloud se puede acceder a los recursos necesarios para una operación específica, un tercero se encargaría de suministrar los recursos, servidores, seguridad, mantenimiento, etc. y garantiza la estabilidad y recursos en la plataforma cloud donde se aloja el sistema de monitoreo cloud [8].

### **5.2. Posibilidad de expandir los recursos a medida que crece la empresa**

Cuando una empresa crece, en el sistema tradicional de monitoreo necesita más servidores, espacio de almacenamiento y recursos. En un sistema Cloud a medida que aumenta el tamaño y procesos de una empresa, solo se adquieren los recursos necesarios para suplir las necesidades inmediatas sin tener que hacer grandes inversiones en infraestructura.



*Preparación de Artículos revista VISIÓN ELECTRÓNICA: algo más que un estado sólido*

*Fecha de envío:*

*Fecha de recepción:*

*Fecha de aceptación:*

### **5.3 Los costos de TI se tercerizan**

En un sistema Cloud los gastos correspondientes personal correspondientes mantenimiento y soporte interno de la plataforma desaparecen, estos gastos ahora son asumidos por un tercero que debe garantizar la operatividad y disponibilidad de la plataforma. La empresa como tal debe dedicar su tiempo y recursos a escoger entre todos los oferentes un buen servicio de acuerdo a necesidades específicas [8].

### **5.4. Acceder a los datos es más fácil**

Este es uno de los mayores beneficios que trae con si la implementación de sistemas de monitoreo SCADA/HMI Cloud, en especial para los gerentes y administradores de empresas ya que desde cualquier parte del mundo pueden acceder a la información, reportes y datos cruciales para la toma de decisiones, en definitiva es posible acceder a la información administrativa y también se puede tener acceso a la parte operativa [12]. El acceso a los datos depende solo de los privilegios otorgados a los miembros de la organización, los cuales son suministrados por el personal administrativo.

### **5.5. Mayor colaboración**

Al estar descentralizado, el esquema permite que varios miembros de la organización de distintos niveles del proceso accedan a la información y procedan a hacer su trabajo de

forma colaborativa en proyectos o solución de problemas sin importar el lugar de ubicación, lo cual aumenta la productividad de la empresa.

## **5.6 Facilidad de actualización y reparación**

Este es otro aspecto atractivo del uso de este tipo de sistemas SCADA/HMI. Debido a su naturaleza on-line, las actualizaciones e instalación de nuevos aplicativos son accesibles casi de inmediato y se pueden usar por el personal de la empresa sin importar la ubicación geográfica de cada uno de los miembros del equipo [8].

## **6. Riesgos de implementación de un sistema SCADA-HMI Cloud**

Aunque para muchas organizaciones los sistemas Cloud son atractivos por su relación costo beneficio, existen ciertos riesgos que se corren al momento de implementar un sistema SCADA/HMI de este tipo. Básicamente son tres los grandes riesgos que se deben sortear en el momento de pensar en implementar un sistema de monitoreo Cloud: Seguridad, rendimiento y fiabilidad.

### **6.1. Seguridad.**

Es un factor crítico en el momento de pensar implementar un sistema SCADA/HMI en una empresa. Por ejemplo en una empresa de manufactura la seguridad juega un factor crítico ya



*Preparación de Artículos revista VISIÓN ELECTRÓNICA: algo más que un estado sólido*

*Fecha de envío:*

*Fecha de recepción:*

*Fecha de aceptación:*

que si alguno de sus procesos deja de ser privado, se corren grandes riesgos con los competidores [5].

Uno de los grandes dilemas es si la información es pública o no y depende de la empresa catalogar la información que aloja en servidores externos. Cada organización debe dar prioridad al manejo de sus datos críticos ya que en el momento de tercerizar el almacenamiento de datos por ejemplo ya se está perdiendo de cierta forma la potestad de esta y puede estar comprometida cierta información sensible como derechos de patentes, fórmulas, procesos, etc. El método más saludable de abordar este tema es preguntarse de forma objetiva ¿me importa si esta información la ve un tercero? y decidir qué datos pueden ser almacenados por un tercero y cuáles es mejor almacenarlos en servidores físicos de propiedad de la empresa [9].

Otro de los riesgos latentes con respecto a la seguridad de la información son los ataques informáticos de “piratas” debido a que esta información viaja por una red pública y otras personas con otro tipo de intenciones pueden acceder de una u otra forma a datos sensibles de la empresa. En los últimos años se han visto ejemplos de cómo empresas grandes como Sony o Citigroup han perdido información sensible debido a ataques informáticos de terceros lo cual es un claro ejemplo de la latencia del problema de seguridad de estas plataformas.

Otro de los posibles riesgos referentes a la seguridad se puede observar en el punto de que un servicio de almacenamiento Cloud puede albergar datos de más de una empresa, por lo tanto un solo ataque informático centralizado a hacer daños o intrusiones de uno o varios

servidores de una empresa que suministre alojamiento e infraestructura Cloud para SCADA/HMI puede no solo hacer daños focalizados (solo una empresa), sino, que puede hacer un daños de mayor escala al involucrar datos de más organizaciones.

La legislación vigente también juega un papel importante en la evaluación de riesgos de seguridad, por ejemplo en Estados Unidos, después de los ataques del 11 de septiembre, el gobierno tiene autoridad legal de hacer copias a cualquier información que esté almacenada en la nube [14].

## **6.2. Rendimiento.**

Para tener un rendimiento aceptable en un sistema SCADA/HMI Cloud se deben contemplar dos parámetros cruciales para su óptima operación: al ancho de banda y a la latencia de la conexión de internet. Si hay sobrecarga del ancho de banda, el sistema no puede responder a las peticiones externas lo cual hace que el problema esté fuera de control interno de la empresa y se esté a merced del proveedor de internet. Si los tiempos de respuesta o latencia son muy grandes se pierde una de las características fundamentales de los sistemas SCADA/HMI que es el de monitoreo de datos en tiempo real. Cuando alguno de estos dos problemas aparece en un sistema SCADA/HMI Cloud la experiencia del usuario final puede llegar a ser desastrosa e insatisfactoria [15].

El rendimiento inconsistente en un sistema SCADA/HMI Cloud puede causar problemas en la línea de producción, por ejemplo, mientras en un sistema cableado al presionar el botón de



*Preparación de Artículos revista VISIÓN ELECTRÓNICA: algo más que un estado sólido*

*Fecha de envío:*

*Fecha de recepción:*

*Fecha de aceptación:*

arranque, la máquina se pone en marcha inmediatamente, es tolerable un retraso de milisegundos o un segundo, si en un sistema Cloud tarda más de este tiempo la percepción del operario es que algo anda mal y que la maquina no está funcionando adecuadamente. En definitiva, si la latencia es relativamente corta o aceptable, el operario puede acostumbrarse al retardo ya que puede ser insignificante, si el retraso es prolongado puede causar errores y volver lento el proceso productivo.

Algunas de las aplicaciones industriales, como la lectura de medidas en tiempo real a través de arquitecturas como la definida en IEC\_61499 o los sistemas de gestión de procesos en tiempo real, para utilizar servicios distribuidos de la nube deben minimizar el tiempo de latencia y por ello debe haber algún nodo en las proximidades del punto de control. Hay que tener en cuenta que determinadas medidas de seguridad como el cifrado de datos perjudican la latencia [5].

### **6.3. Confiabilidad.**

Este es uno de los factores más importantes en el momento de implementar un sistema SCADA/HMI Cloud. Aquí es donde se evalúa la relación entre accesibilidad y prestaciones enmarcadas en la confiabilidad del servicio. Antes de decidir migrar hacia la nube se debe evaluar primero la posibilidad de enfrentar problemas que en un sistema tradicional SCADA/HMI son de baja probabilidad de ocurrencia. Aspectos como confiar en el prestador

de servicios de internet, accesibilidad a la información, privacidad y confianza hacia el servicio contratado en la nube son de suma importancia y deben ser tratados minuciosamente para no tener una mala experiencia. Problemas como el fallo en la conexión de internet, el ataque de piratas informáticos, fallas en el sistema de alojamiento Cloud hace que la empresa pierda, filtre o quede desconectada de los datos y variables de sus procesos productivos [15].

Existen numerosos trabajos de investigación en la línea de sistematizar la solicitud de garantías de seguridad y privacidad a los proveedores de Cloud, no sólo en los contratos o SLA (Service Level Agreements) (p.ej. algunos proyectos de investigación financiados por Europa, la CCM (Cloud Control Matrix) y el PLA (Privacy Level Agreement) de la Cloud Security Alliance), sino también en los protocolos de transparencia de los métodos de seguridad que emplean (p.ej. el CTP (Cloud Trust Protocol) de la Cloud Security Alliance) [10].

## **7. Conclusiones**

- ❖ El uso de recursos Cloud permite monitorizar, controlar e informar datos y variables, proporcionando transparencia, tanto para el proveedor, como para el consumidor del servicio utilizado a un costo menor que el sistema tradicional SCADA/HMI de forma descentralizada.



- ❖ Aún con las ventajas que aporta esta tecnología, expertos del sector son reacios a su uso por el hecho de que hay ciertos sistemas que usan tecnologías antiguas y los dispositivos tienen ciclos de vida muy largos. Por ejemplo, en algunos sistemas de control aún se siguen utilizando sistemas operativos como Windows 95 - XP y aplicaciones software que sólo son capaces de operar en esos sistemas operativos antiguos. Su virtualización puede ser en algunos casos compleja y la confianza en que funcione de forma correcta no es elevada.
- ❖ Al ser una tecnología relativamente nueva presenta ciertos niveles de vulnerabilidad respecto a la seguridad. El hecho de tercerizar el servicio no garantiza que los datos sensibles de una organización no sean filtrados o accedidos por personas externas a la organización.
- ❖ Antes de pensar en migrar a un sistema SCADA/HMI Cloud se debe evaluar los tres riesgos fundamentales. La empresa como tal debe decidir sus prioridades y escoger cuáles datos puede almacenar y tratar en un sistema Cloud y cuales debe mantener en servidores e infraestructura. Además en el momento de migrar a un SCADA/HMI.

#### **4. Referencias**

[1] J. A. Ruiz, J. C. Muñoz y J. L. García “SCADA system design: a proposal for optimizing a production line”, IEEE, 2016 International Conference on Electronics, Communications and Computers (CONIELECOMP), pp. 192-197. Enero 2016.

- [2] M. Geberslassie y B. Bitzer “Future SCADA Systems for Decentralized Distribution Systems”. IEEE, Universities Power Engineering Conference (UPEC), pp. 3 - 4, Septiembre 2010.
- [3] D. Kang y J. Lee, “Analysis on Cyber Threats to SCADA systems”. IEEE, Transmission & Distribution Conference & Exposition: Asia and Pacific, pp. 1 - 2, Octubre 2009.
- [4] A. Giani y G. Karsai “A Testbed for Secure and Robust SCADA Systems”. IEEE, Intelligent Information Hiding and Multimedia Signal Processing, pp. 1 - 5, Octubre 2013.
- [5] J. Ruiz y J. Muñoz “SCADA system security: Complexity, history and new developments”. IEEE, 6th IEEE International Conference on Industrial Informatics, pp. 560 - 561, Julio 2008.
- [6] A. Kelgere y M. Agarwal “Low power interactive operative system and SCADA Based universal wireless gateway for automation using cloud technology”. IEEE, 2nd International Conference on Information Science and Control Engineering, pp. 791 - 792, Febrero 2015.
- [7] R. Piggin “Securing Scada In The Cloud: Managing The Risks To Avoid The Perfect Storm”. IEEE, Instrumentation Symposium, IET & ISA 60th International, pp. 1 - 2, Junio 2014.
- [8] Inductive Automation “Cloud-Based SCADA Systems:The Benefits & Risks”. Is Moving Your SCADA System to the Cloud Right For Your Company, pp. 1 - 12, Junio 2011.
- [9] M. McQueen y F. Boyer “Quantitative Cyber Risk Reduction Estimation Methodology for a Small SCADA Control System”. IEEE, Proceedings of the 39th Hawaii International Conference on System Sciences, pp. 1 - 11, Septiembre 2006.
- [10] P. Chopade y S. Karago “Novel Smart Grid and SCADA System Interdependency Networks for Future’s Clean, Sustainable and Green Energy”. IEEE, Emerging Technologies for a Smarter World (CEWIT), pp. 2 - 6, Octubre 2013.
- [11] A. Sallam y Om P. Malik, "Scada Systems and Smart Grid Vision", Wiley-IEEE, Electric Distribution Systems , pp. 469-493, Octubre 2011.
- [12] H. Huth y A. Houyou “Resource-aware Virtualization for Industrial Networks”. IEEE, Data Communication Networking (DCNET), pp. 1 - 2, Julio 2013.



**VISIÓN ELECTRÓNICA**

*Preparación de Artículos revista VISIÓN ELECTRÓNICA: algo más que un estado sólido*

*Fecha de envío:*

*Fecha de recepción:*

*Fecha de aceptación:*

[13] S. Hong, T. N. Phuong and M. Lee, "Development of Smart Devices for Secure Communication in the SCADA System", IEEE, Computational Science and Its Applications (ICCSA), 2011 International Conference, Santander, pp. 176-180, 2011.

[14] J. A. Bertolín, "Mejora de la protección de la seguridad de los sistemas SCADA utilizados en el control de procesos industriales", REE, Seguridad en redes industriales, pp. 60-70, Enero 2012.

[15] D. Sutic and B. Atagic, "Requirement bottlenecks in a cloud based SCADA system", IEEE, Information & Communication Technology Electronics & Microelectronics (MIPRO), 36th International Convention, Opatija, pp. 857-862, 2013.