Riesgos a los Sistemas SCADA, en empresas Colombianas.

Javier Eduardo Arias Torres

Universidad Piloto de Colombia, Bogotá, Colombia

ing.javierariast@gmail.com

Resumen – A medida que pasa el tiempo, se puede evidenciar los pasos agigantados con los que avanza la sociedad, la gente, las plataformas tecnológicas y hasta las organizaciones, con el fin de responder a un mercado evolutivo y lleno de nuevas tendencias, que buscan crear, solucionar y realizar labores diarias de forma más ágil y eficiente. Este boom evolutivo, no solo trae para las organizaciones mayores recompensas y destrezas, si no que también trae de la mano un sin número de retos y riesgos en el amplio campo de la Seguridad Informática.

Palabras Clave – SCADA, ICS, DCS, PLCs, Seguridad Informática, Disponibilidad, Autenticidad, Confidencialidad.

Abstract – As time passes, the giant can be evidenced with the steps that society advances, people, technology platforms and to the organizations, in order to respond to an evolving market and full of new trends, seeking to create, troubleshoot and perform daily work faster and more efficiently. This evolutionary boom, not only brings greater rewards for organizations and skills, but it also brings with it a number of challenges and risks in the broad field of Information Security.

Keywords – SCADA, ICS, DCS, PLCs, Computer Security, Availability, Authenticity, Confidentiality.

I. INTRODUCCIÓN

Las organizaciones en su gran mayoría, requieren tener controlados y conocer en tiempo real, toda la información crítica de sus procesos, maquinarias, líneas de producción, sistemas de refrigeración o hasta sistemas más complejos como una línea de distribución hidroeléctrica. Para determinar si su funcionamiento se encuentra dentro de los rangos de tolerancia establecidos, se requiere el uso de los sistemas de monitorización y control en tiempo real SCADA, los cuales otorgan la información necesaria para la toma de decisiones en caso de una avería o el mal funcionamiento de un dispositivo. [1]

A pesar de su gran funcionalidad, estos dispositivos SCADA son desconocidos por gran parte de la comunidad y mucho más, todas las herramientas que apoyan esta gestión de seguimiento en tiempo real a una o varias actividades de una organización. También existen diferentes clases de sistemas, como el de control industrial (ICS), el sistema de control distribuido (DCS) o los controladores lógicos programables (PLCs), que de forma estructurada dentro de una organización, facilitan y brindan el soporte y la información necesaria para llevar a cabo una operación, por más compleja que esta sea. Todo esto se logra gracias a la retroalimentación de información en tiempo real que puede ser recopilada por los operarios de una línea o por un líder de proceso. [1]

II. MARCO TEORICO

SCADA es un sistema automatizado que permite supervisar y controlar variables de algún proceso o cadena de procesos industriales a distancia, proporcionando comunicación con los dispositivos controladores (PLCs) y controlando el proceso de forma automática por medio de un software especializado. [11]

Es decir, se denomina sistema SCADA a aquel conjunto de redes, equipos y programas que monitorizan en tiempo real procedimientos industriales y tareas complejas, a partir de la información obtenida a través de sensores, estos se comunican con los dispositivos actuadores para transmitir información en tiempo real y adecuada, pudiendo controlar uno o varios procesos de forma automática, mediante un software especializado. La finalidad de esta continua comunicación es la de optimizar, vigilar y verificar los diversos cambios en el funcionamiento del sistema, también conocido como sistemas de monitorización y control en tiempo real. [1]

A. Componentes de un sistema SCADA

- ***Centro de control:*** Posiciones desde las que se opera, monitoriza y controla el sistema.
- ***Comunicaciones:*** Redes para la comunicación entre el centro de control y los componentes finales.

- ***Localizaciones finales:*** Son aquellos dispositivos que son monitorizados y controlados remotamente como sensores, válvulas, cámaras, climatización, etc.

B. Clasificaciones

- ***Industrial Control System* (ICS).** En general el término ICS se aplica a sistemas de monitorización y control orientados principalmente a usos industriales, por lo que en él se engloban los sistemas empleados en los sectores de electricidad, agua, petróleo, gas, química, etc. [1]

- ***Supervisory Control And Data Acquisition* (SCADA).** Los sistemas SCADA, o sistemas de control de supervisión y adquisición de datos, son un caso particular de ICS, cuya principal característica respecto a las otras dos categorías (DCS y sistemas basados en PLCs) es la gestión centralizada de todo el sistema. Hoy en día, el término SCADA ha alcanzado un significado más amplio, englobando a cualquier sistema que monitoriza y/o gestiona de forma centralizada y en tiempo real un conjunto de dispositivos finales. [1]

- ***Distributed Control System* (DCS).** Un DCS es en un comparativo, un conjunto de sistemas SCADA locales, que conforman un único sistema de monitorización sin ningún puesto de control central. [1]

- **Sistemas basados en *Programmable Logic Controllers* (PLCs).** Los sistemas de control basados en PLCs, son sistemas SCADA de tamaño y complejidad reducidos. Dado que los programas informáticos que monitorizan y controlan los actuadores residen en estos dispositivos, en los casos en los que el proceso no es muy complejo, estos dispositivos se usan como componentes principales del sistema. [1]

- ***Human Machine Interface (HMI).*** Si bien un sistema SCADA permite controlar uno o varios procesos, también debe existir una interfaz para el usuario final para controlar dicho sistema. Esta interfaz es llamada HMI y es el puente final entre el sistema y el operador. [11]

C. Estructura y Componentes

La estructura y componentes de un sistema SCADA típica son como en la Fig. 1. [1]

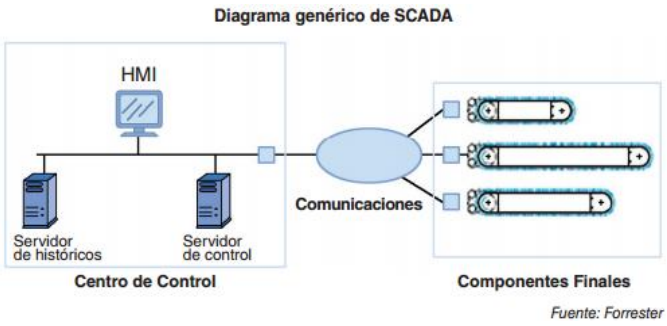

Fig. 1 Diagrama genérico de un sistema SCADA.

- ***Centro de control.*** Es el lugar donde se ubican los componentes centrales de un sistema SCADA como un equipo servidor de Históricos y un equipo servidor para Control.

- ***Comunicaciones***. Se trata de la interlocución entre el centro de control y los componentes finales. Estas comunicaciones pueden abarcar pequeñas o grandes distancias y utilizan una amplia gama de tecnologías, entre ellas las redes locales, redes telefónicas, conexiones vía satélite o radio, redes públicas, etc. La información transmitida en estas comunicaciones contiene datos de monitorización de los componentes finales, así como órdenes de control remoto.

- ***Componentes finales***. Son los sensores y actuadores que proporcionan los datos al sistema, incluyendo los dispositivos que son manipulados a través del sistema.

Los sistemas de monitorización y control en tiempo real SCADA, también tienen una denominación llamada, Infraestructura Critica y no por la complejidad o su estructura en sí, sino a la función o el servicio donde este sistema se desempeñe. La complejidad de una organización u otra, dará el calificativo de esencial, luego al estudio de las instalaciones, las redes y los procesos de trabajo por los que se desempeñe, se podrá determinar si una infraestructura cumple con las características para ser considerada crítica. En Europa a través de la Ley PIC, España establece una definición oficial para considerar una infraestructura como crítica: "Las infraestructuras estratégicas (es decir, aquellas que proporcionan servicios esenciales) cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales". [14]

Esto mismo se debe trabajar en Colombia, con el fin de indentificar cuales son sus infraestructuras esenciales y como trabajar con ellas a través de un solido marco regulatorio, para que sea trabajado a nivel región y no a nivel general, las pautas

han sido entregados por muchos paises como España, solo se debe aprovechar esta infraestrucutra para que sea planteada en el país, teniendo en cuenta que los sistemas SCADA se encuentran ligados a una variedad finita de sectores, por lo que es recomendable estudiar la legislación, regulación o normativa existente para cada sector específico en el que se vaya a operar.

D. Aplicaciones de los sistemas SCADA

Gracias a su versatilidad, durabilidad y estabilidad, los sistemas de monitorización y control en tiempo real, pueden ser usados en varios campos dentro de una organización sin importar su tamaño: [1]

- Monitorización y/o gestión de elementos geográficamente dispersos.
- Configuración de mecanismos de seguridad.
- Monitorización y gestión de un proceso industrial complejo.
- Almacenamiento histórico de información.
- Monitorización y gestión de servicios rutinarios e infraestructuras básicas.

III. DESARROLLO

Los sistemas de monitorización y control en tiempo real SCADA, hace unos años cumplían funciones como la verificación y control de válvulas, sensores, bombas, entre otros elementos mecánicos, donde trabajaban como sistemas aislados dentro de la organización, brindando información necesaria para los técnicos, jefes y/o directivos que la requirieran. Ahora su evolución, permite conectar estos sistemas a una red pública como Internet o permitir acceder de forma remota, por lo que el reto de las organizaciones está en que la autenticidad de su información no sea filtrada o en el peor de los casos, su disponibilidad. A continuación se muestra los riesgos para las organizaciones, estado actual frente a regulación y/o legislación en Colombia y los riesgos a los que se enfrenta una sociedad como la colombiana.

A. Costo de un ataque informático a una organización

Un reciente estudio realizado por el Instituto Ponemon en Estados Unidos, encontró que el costo promedio causado por ataques informáticos fue de 11,56 millones de dólares en el último año. Esto representa un incremento del 78% frente a las cifras del año pasado. Además del aumento en costo, también incrementó el tiempo necesario para solucionar los problemas generados por un ataque informático. En Estados Unidos, las organizaciones experimentaron 122 ataques exitosos a la semana. Eso es un incremento significativo frente al promedio de 102 que se registró el año pasado. Un ataque exitoso significa que hay una filtración de las redes centrales o de los sistemas de la empresa. [2]

B. Ataques informáticos en Colombia

Según informe de EL TIEMPO, seis millones de personas fueron víctimas de alguna modalidad de crimen digital en Colombia el año pasado, según la firma de seguridad digital Norton. La compañía calcula que el costo de los delitos informáticos en 2013 alcanzó 874 mil millones de pesos. [4]

Cuatro de cada 10 usuarios de Smartphone han sufrido de algún delito digital. La vulnerabilidad de los colombianos ante los ciber delincuentes quedó plasmada en su máxima expresión hace unos meses, cuando se descubrió que hasta las cuentas de correo del Presidente fueran hackeadas. [4]

La situación para las entidades públicas y privadas no es mejor, pues el más elemental diagnóstico sugiere que existe un alto reto en temas de ciberseguridad. Durante el 2013 se detectaron 1.551 DEFACES, una modalidad de ataque cibernético que cambia la página principal de un sitio de internet. En lo que va del 2014 se han reportado 801 de esos ataques: 507 a portales comerciales, 186 de sitios web educativos y 108 de sitios web de entidades. [4]

El análisis del Theat Intelligence Group, explora una campaña liderada por cibercriminales para tomar el control de routers en todo el planeta. Los dispositivos atacados, habrían sufrido alteraciones en su configuración DNS (Domain Name Server). Como resultado de los cambios en la configuración DNS se habría forzado a los routers a usar las direcciones IP 5.45.75.11 y 5.45.75.36. Se habrían identificado, por lo menos, unos 20.000 enrutadores (router) colombianos comprometidos en el ataque. [5]

De acuerdo con el más reciente reporte sobre 'Tendencias de Ciberseguridad en América Latina y el Caribe' publicado por la Organización de Estados Americanos (OEA) y la empresa de seguridad Symantec, Colombia se posiciona como el sexto país en generar una mayor actividad maliciosa en línea, según los datos registrados en 2013. [6]

C. Colombia y su preparación ante los delitos informáticos

El país se alista para implementar un nuevo modelo de ciberdefensa y de seguridad digital. Es por esto, que se conocerá la hoja de ruta que tanto a nivel oficial como privado se implementará desde el Gobierno para preparar a entidades, empresarios, sistema judicial, de Policía, fuerzas militares y entes de investigación para prevenir y combatir las amenazas de seguridad informática que puedan afectar a la ciudadanía y a los intereses de la Nación. Puntos del nuevo programa: [3]

- Dos sistemas de seguridad, una externa (ciberdefensa) y otro de políticas internas (ciberseguridad). Ambos con coordinación unificada y con enlace directo a Presidencia. [3]

- Refuerzo de personal. El pie de fuerza en seguridad digital crecerá. Se destinarán más recursos a los comandos y grupos de investigación de defensa y seguridad digitales. [3]

- Más tecnología. Según el ministro de Telecomunicaciones, el país cuenta con tecnología de punta para la lucha contra el cibercrimen. En este aspecto se aumentará el presupuesto y el trabajo con expertos privados. [3]

- Leyes fuertes. Judicializar a tiempo y de manera efectiva a los delincuentes digitales será punto clave. El marco legislativo actual requiere de revisión y endurecimiento. [3]

D. Marco regulatorio para sistemas de monitorización y control en tiempo real en Colombia

A la fecha, Colombia no cuenta con un marco regulatorio, estándar, guía y/o normativa para el uso de los sistemas de monitorización y control en tiempo real, no está de más, que en algún momento se contemple su regulación y propio modelo de funcionamiento, con un énfasis hacia la legislación y normatividad Colombiana, contemplando el modelo de trabajo y el tamaño de la organización.

Ahora, el hecho que Colombia no cuente con un esquema o regulación, no quiere decir que no existan guías regulatorias para algunos de estos sistemas, como las presentadas a continuación: [1]

- ***CCN (Centro Criptológico Nacional). Guía CCN-STIC-480 en materia de Seguridad en Sistemas SCADA.*** Cobra especial importancia en las industrias que trabajen con Infraestructuras Críticas y está orientada a cualquier organismo, institución, industria o empresa que cuente con sistemas SCADA. Uno de sus objetivos principales es el de presentar la problemática existente de los sistemas SCADA y sus vulnerabilidades, su impacto y la necesidad inmediata de controlar su seguridad, presentando algunas soluciones técnicas ante determinadas amenazas y referenciando algunos documentos donde se puede encontrar más información.

- ***IEEE (Institute of Electrical and Electronics Engineers) IEEE PC37.1™ Draft Standard for SCADA and Automation Systems.*** Estándar de referencia en materia de definición, especificación, análisis e implementación de sistemas SCADA y sistemas de automatización enfocado a las subestaciones eléctricas, dirigido para facilitar y mostrar las pautas necesarias para diseñar los sistemas SCADA y los sistemas de automatización en subestaciones eléctricas.

- ***ENISA (European Network and Information Security Agency) "Protecting Industrial Control Systems. Recommendations for Europe and Member States".*** Relacionada con los sistemas de monitorización y control en tiempo real, que incluye un exhaustivo informe anexo "ICS Security Related Standards, Guidelines and Policy Documents", en el que se exponen los diferentes estándares y normas de seguridad establecidas por diferentes organizaciones.

E. Leyes Colombianas contra los delitos informáticos

En Colombia solo se cuenta con una ley regulatoria para todo lo relacionado con los delitos informáticos, con penas de prisión, que van desde los 48 hasta los 96 meses. Así lo establece la ley 1273 de enero de 2009, por la que se modifica el Código Penal y se creó un nuevo bien jurídico denominado 'De la protección de la información y de los datos'. [7], [8]

Las penas de prisión serán impuestas a quienes, "con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes". Además tendrán multas de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya un delito sancionado con penas más graves. También se incluye a quien incurra en la modificación del sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP (Protocolo de Internet) diferente, en la creencia de que acceda a su banco o a otro sitio personal o de confianza. [7], [8]

Con esta nueva ley se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Sin dejar en el olvido quien atente contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

Las medidas legales son contra: [7], [8]

- Acceso abusivo a un sistema informático.

- Obstaculización ilegítima de sistema informático o red de telecomunicación.

- Interceptación de datos informáticos.

- Daño informático.

- Uso de software malicioso.

- Violación de datos personales.

- Suplantación de sitios web para capturar datos personales.
- Circunstancias de agravación punitiva.
- Hurto por medios informáticos y semejantes.
- Transferencia no consentida de activos.

Colombia avanza tanto en el tema de Seguridad Informática que el Juez segundo de control de garantías de Róvira (Tolima) Alexander Díaz García y especialista en nuevas tecnologías y protección de datos, asegura que "Colombia es el primer país en tener una legislación tan clara sobre este tipo de delitos". [9]

IV. RIESGOS Y AMENAZAS EN SISTEMAS SCADA

Un estudio de la empresa Positive Technologies hace algunas afirmaciones muy serias, las cuales indican que el 40% de los sistemas de monitorización y control en tiempo real SCADA disponibles en Internet, pueden ser hackeados fácilmente, la mitad de las vulnerabilidades encontradas permiten la ejecución de código arbitrario en los sistemas destino, un tercio de las vulnerabilidades son debido a malas configuraciones y el uso de contraseñas por defecto y una cuarta parte están relacionados con los administradores de sistema por no instalar actualizaciones de seguridad. [10]

Todo ejercicio en torno a la seguridad informática, debe iniciar por tener el riesgo al que se está expuesto, una definición útil consiste en expresar el riesgo en función de la probabilidad de que se produzca ese riesgo y el impacto que tendría lugar si ese riesgo se materializara. [12]

Al conocer las amenazas, se debe tratar de establecer sus motivaciones, para poder responder ante ellas. Dentro de una identificación de posibles amenazas, estarían: [12]

- Denegación de servicio
- Ataques dirigidos
- Ataques accidentales
- Accesos y controles no autorizados
- Código malicioso instalado en las máquinas (gusanos, virus, troyanos, spam, phishing, bots, etc.).

Las fuentes de las amenazas o de los atacantes potenciales para una organización, incluyen: [12]

- Hackers y delincuentes
- Malware de propagación automática
- Atacantes internos
- Personal descontento
- Personal realizando acciones no autorizadas
- Acciones accidentales
- Inteligencia corporativa
- Contratistas
- Servicios de inteligencia extranjeros
- Crimen organizado
- Terroristas
- Manifestantes y/o activistas medioambientales, políticos, etc.

Lo principal en un servicio SCADA es su información en tiempo real, por lo que no de sebe permitir la indisponibilidad del servicio, sea cual sea su criticidad. Ahora, si nos remontamos unos años atrás, recordemos que, los sistemas de control siempre han estado en riesgo, el riesgo principal era una intrusión física, pero a medida que han ido evolucionando los sistemas, el número de amenazas ha aumentado y no se limitan a riesgos físicos, sino lógicos. [11], [1]

V. ESTRATEGIAS PARA ASEGURAR UN SISTEMA SCADA SEGURO

A. Principios base. A lo largo del artículo, hemos venido identificando el objeto de trabajo de un sistema de monitorización y control en tiempo real, su aplicabilidad en el entorno económico Colombiano, sus riesgos y amenazas latentes, pero no hemos definido, cuales serían los tres principios base, para salvaguardar un sistema SCADA. Estos principios son los siguientes: [13]

- ***Proteger:*** Implementar medidas de protección concretas, para prevenir y desanimar un ataque electrónico en contra de los sistemas de control.
- ***Detectar:*** Establecer mecanismos para identificar rápidamente ataques informáticos.
- ***Responder:*** Adoptar medidas apropiadas en respuesta a incidentes de seguridad.

El diseño de un marco de seguridad para cualquier sistema de control, no se basa solamente en el despliegue de medidas de protección, también es importante ser capaz de detectar posibles ataques y responder de forma adecuada para minimizar su impacto. [13]

B. Medidas de reducción de riesgos. Factores a tener en cuenta como organización: [12]

- El coste
- La eficacia de las medidas
- El modelo de negocio
- La dificultad de implementación de una medida o estrategia
- Verificación de las soluciones existentes
- Grupo(s) de atención ante emergencias

C. Buenas Prácticas. [13]

- ***Estudiar el riesgo del negocio.*** Como guía de buenas prácticas, se debe comprender los sistemas con los que se va a trabajar, comprender las amenazas a las que se expone una organización dependiendo de su criticidad, comprender el impacto al llegar a materializarse un incidente sea cual sea, y comprender las vulnerabilidades a través de evaluaciones, auditorias y verificaciones a los diferentes sistemas, tanto físicos como lógicos.
- ***Realizar estudios continuos del riesgo del negocio.*** El riesgo del negocio es una función de las amenazas, los impactos y las vulnerabilidades. Debido a los constantes cambios de una organización, es necesario entregar un proceso continuo de gestión de riesgos para identificar cualquier cambio, reevaluar el riesgo y poner en marcha las mejoras de seguridad que se requieran.

D. Diseño e implementación de una arquitectura segura. Para una arquitectura segura dentro de una organización que requiera el uso de sistemas de monitorización y control en tiempo real, es requerido un diseño y una implementación acorde con el tamaño de la organización, los procesos y la criticidad de los mismos. Ítems a tener en cuenta: [13]

- Arquitectura de la red
- Sistemas Cortafuegos
- Acceso Remoto
- Software Anti Virus
- Correo electrónico
- Acceso a internet
- Fortalecimiento del sistema
- Fortalecimiento de la Plataforma Tecnológica
- Copias de seguridad y recuperación
- Seguridad Física
- Seguridad Lógica
- Monitoreo de los sistemas
- Monitoreo de la Plataforma Tecnológica
- Redes Alámbricas e Inalámbricas.
- Actualizaciones y/o parches de seguridad
- Verificación de antecedentes del personal con acceso y control a los sistemas SCADA.
- Contraseñas, cuentas y perfiles de usuario
- Control documental
- Infraestructura e instalaciones adecuadas
- Gestión de vulnerabilidades
- Rotación de personal
- Gestión del cambio
- Pruebas de seguridad
- Análisis de conectividad de nuevos dispositivos
- Capacitación de personal
- Verificación de Terceros
- Verificación de Proveedores

VI. CONCLUSIONES

A lo largo de este documento hemos identificado los riesgos, amenazas de un sistema SCADA, pero también una guía de buenas prácticas para implementar un sistema de monitorización y control SCADA seguro y robusto. Lo principal es que cada organización identifique cada criterio visto en este artículo, con el fin de llevar a cabo la correcta implementación de acciones, normativas y guías que controlen y mitiguen los riesgos de estos sistemas dentro de una organización.

Es de vital importancia que al diseñar, implementar y mantener un sistema SCADA dentro de una organización, se analicen factores como la correcta estimación de recursos, para que a la larga, estos no sean perjudiciales para el sistema y para la organización. Es muy importante buscar el apoyo de entidades públicas y privadas para desarrollar guías o estándares acordes con el modelo de trabajo y el tamaño de las organizaciones

Colombianas, de lo contrario se trabajaría con esquemas y modelos generales otorgados por otros países.

Es de recalcar que será una labor ardua de cada organización, que al comprar este tipo de sistemas de monitorización y control en tiempo real, se debe solicitar a los proveedores, productos que cumplan con requisitos mínimos de seguridad, mantenerse informados sobre las incidencias, vulnerabilidades y avisos de seguridad enviados por otras entidades o países, mantener y dar seguimiento al modelo de seguridad implementado y establecer dentro de su modelo documental, políticas de seguridad, con el fin de robustecer los sistemas de monitorización y control en tiempo real SCADA. [1]-[14]

VII. REFERENCIAS

[1] INTECO, GUÍA PARA EMPRESAS, MADRID, 2012.

[2] M. SANTOS, «REVISTA ENTER,» 01 NOVIEMBRE 2013. [En línea]. Available: http://www.enter.co/especiales/enterprise/el-costo-de-los-ataques-informaticos-supera-los-32-millones-de-dolares/. [Último acceso: 03 AGOSTO 2014].

[3] R. TECNOLOGÍA, «PERIODICO EL TIEMPO,» 07 ABRIL 2014. [En línea]. Available: http://www.eltiempo.com/archivo/documento/CMS-13797815. [Último acceso: 03 AGOSTO 2014].

[4] E. AMERICA, «ELECONOMISTA AMERICA.COM,» 11 JULIO 2014. [En línea]. Available: http://www.eleconomistaamerica.co/actualidad-eAm-colombia/noticias/5934325/07/14/Revista-de-Prensa-Colombia-el-pais-refuerza-proteccion-contra-ciberataques.html#.Kku8PjCP8NLKZ6j. [Último acceso: 03 AGOSTO 2014].

[5] E. L. MEDINA, «PERIODICO EL TIEMPO,» 06 MARZO 2014. [En línea]. Available: http://www.eltiempo.com/archivo/documento/CMS-13607575. [Último acceso: 03 AGOSTO 2014].

[6] R. TECNÓSFERA, «PERIODICO EL TIEMPO,» 10 JUNIO 2014. [En línea]. Available: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/colombia-el-sexto-pais-en-generar-mayor-actividad-maliciosa-en-linea/14087046. [Último acceso: 03 AGOSTO 2014].

[7] M. D. L. T. D. L. I. Y. L. COMUNICACIONES, LEY 1273 DEL 05 DE 2009, BOGOTÁ, 2009.

[8] AUTOR, «PERIODICO EL TIEMPO,» 08 ENERO 2009. [En línea]. Available: http://www.eltiempo.com/archivo/documento/CMS-4746916. [Último acceso: 03 AGOSTO 2014].

[9] A. D. GARCIA, «LINKEDIN,» [En línea]. Available: https://www.linkedin.com/in/alediaganet. [Último acceso: 03 AGOSTO 2014].

[10] V. MOTOS, «HACK PLAYERS,» 13 NOVIEMBRE 2012. [En línea]. Available: http://www.hackplayers.com/2012/11/informe-alerta-seguridad-scada.html. [Último acceso: 03 AGOSTO 2014].

[11] J. V. ROJAS, AUDITORÍA DE SEGURIDAD EN SISTEMAS SCADA, ISACA.

[12] E. Y. C. C. NACIONAL, GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-480) SEGURIDAD EN SISTEMAS SCADA, MADRID, 2010.

[13] E. Y. C. C. NACIONAL, GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-480A) SEGURIDAD EN EL CONTROL DE PROCESOS SCADA, MADRID, 2010.

[14] CNPIC, «CNPIC,» 2010. [En línea]. Available: http://www.cnpic-es.es/Preguntas_Frecuentes/Que_es_una_Infraestructura_Critica/index.html. [Último acceso: 03 AGOSTO 2014].