7 CONCLUSIONES

7.1 OBJETIVOS ALCANZADOS

En el desarrollo de este proyecto he alcanzado varios de los objetivos que inicialmente se determinaron:

- Desarrollar una metodología donde se describa paso a paso que tipo de información y como se debe buscarse durante una auditoria. Considero que el procedimiento desarrollado, sin llegar a tener mucho nivel de detalle, es correcto y fácilmente aplicable en cualquier empresa que cuente con un sistema industrial, ya que puede aplicarse de igual manera para auditar un sistema MES, SCADA o de cualquier otro tipo.
- Establecer un calendario y los cálculos o fórmulas[16] para planificar y determinar el coste aproximado de una auditoría, en función del número de sistemas industriales.
- Recopilar información sobre el estado del arte, es decir, he accedido a prácticamente todo el material existente al día de hoy en materia de seguridad en entornos industriales. Sin embargo no he podido revisarlo todo con el mismo nivel de detalle, pero sí he revisado todas las metodologías de auditoría y todos los mecanismos de protección de libre acceso.
- Probar a fondo las herramientas de auditoría de vulnerabilidades de código abierto más conocidas, como son Nmap y Nessus con muchas de sus opciones contra varios dispositivos industriales y servidores que los controlan.
- Aplicar el marco de auditoría del sistema MES en una empresa de gran tamaño del sector alimenticio. Se ha podido aplicar la metodología aunque por las restricciones de tiempo se ha tenido que limitar a unos pocos sistemas.

Verificación de las hipótesis formuladas inicialmente:

---

[16] Ver apartados 7.2 y 7.3

- La primera hipótesis se cumplió parcialmente ya que en el transcurso de este proyecto apareció la herramienta "OPC Security Tester", sin embargo no existen otras herramientas de código abierto especializadas en la auditoría de sistemas industriales aunque sí existen herramientas comerciales.
- Durante las pruebas he demostrado la segunda hipótesis, que es posible bloquear estos dispositivos con un simple escaneo.

7.2 PLANIFICACIÓN Y COSTES INICIALES Y REALES

7.2.1 PLANIFICACIÓN REAL

Inicialmente se hizo una estimación del tiempo necesario en que se incurriría al realizar cada una de las tareas en las que se divide este proyecto y se planificaron las fechas de inicio y fin de cada una de ellas, en este apartado veremos como se han ejecutado las tareas en la realidad, que diferencias ha habido en las fechas de realización y sus causas.

El gran cambio que ha modificado la planificación inicial del proyecto ha sido el hecho de que la empresa a la que se le haría la auditoría, tardo más tiempo del previsto en aceptar la propuesta de este proyecto, por lo que se redujo considerablemente el tiempo para implantar el marco de auditoría y dedicara más tiempo en ampliar el capítulo de estado del arte e investigara más a fondo las tecnologías existentes.

Lo que implicó que la fase de estado del arte se prolongara en siete días y por tanto las siguientes fases de metodología e implantación en laboratorio se retrasaron. Adicionalmente, aún cuando ya contaba con la aprobación de la empresa, tenía que ponerme de acuerdo con sus técnicos para realizar la presentación y para que me asignaran un coordinador, por lo que decidí adelantar la fase de documentación y comenzar a escribir todas las pruebas y resultados obtenidos en laboratorio, así como la fase de refinación de la metodología de acuerdo con los resultados alcanzados en el laboratorio.

Tarea	Diferencia	Días	Horas	Inicio	Fin	Rol
Planificación	**0**	**4**	**32**	**8-feb**	**13-feb**	**G**
Búsqueda de documentación	**0**	**8**	**64**	**14-feb**	**23-feb**	**C**
Lectura	**0**	**15**	**120**	**26-feb**	**16-mar**	**C**
Estado del arte	**+7**	**12**	**96**	**19-mar**	**3-abr**	**-**
Elaboración	+7	11	84	19-mar	2-abr	C
Revisión	0	1	8	3-abr	3-abr	G
Metodología	**0**	**23**	**184**	**4-abr**	**9-may**	**-**
Elaboración	0	20	160	4-abr	4-may	C
Revisión	0	3	24	7-may	9-may	G
Implantación	**-7**	**12**	**152**	**10-may 29-may**	**15-may 8-jun**	**-**
En laboratorio	0	4	32	10-may	15-may	C
En empresa	-7	8	64	29-may	8-jun	C
Refinar metodología	**0**	**5**	**40**	**23-may 11-jun**	**28-may 11-jun**	**C**
Documentar resultados	**0**	**12**	**96**	**16-may**	**20-jun**	**-**
Elaboración	0	10	80	16-may 12-jun	22-may 18-jun	C
Revisión	0	6	48	19-jun	26-jun	G
Presentación	**0**	**4**	**32**	**27-jun**	**2-jul**	**-**
Preparación	0	4	24	27-jun	29-jun	C
Revisión	0	½	4	2-jul	2-jul	G
Empresa	0	¼	2	[17]		G
UPC	0	¼	2	5-jul	5-jul	G
Total Consultor		**84**	**672**	-	-	-
Total Gerente		**15**	**120**	-	-	-
TOTAL		**99**	**792**	-	-	-

Debido a que cada vez quedaba menos tiempo para la finalización del proyecto, tuve que reducir la implantación del marco de auditoría en la empresa a siete días, lo que implicó que tuviera que ser muy práctico en la aplicación de todas las pruebas realizadas y no empleara tiempo en aplicar pruebas que pudieran tener escaso valor en una auditoría del sistema MES, por lo que se limitó la auditoría de la capa de control del MES a solo dos sistemas en dos plantas distintas.

---

[17] La fecha de presentación de los resultados en la empresa será en la primera semana de julio.

Todos estos cambios e imprevistos hicieron que el enfoque del proyecto cambiara, volviéndose más teórico y menos práctico, sin embargo se incurrieron las mismas horas/hombre a las previstas originalmente.

7.2.2 COSTE REAL

El coste total en la finalización del proyecto es de 63.920 euros que incluye los siguientes conceptos:

Concepto	Coste
Personal	77.760 €
Software	0 €
Hardware	0 €
Adicionales	560 €
Total	**78.320 €**

7.3 ESTIMACIÓN DE COSTES EN LA APLICACIÓN DE LA METODOLOGÍA

7.3.1 DURACIÓN DE LA AUDITORÍA

En el caso de aplicarse esta metodología en una empresa no sería necesario volver a realizar todas las fases del proyecto, sino tan solo aplicarla, lo que reduciría significativamente la duración del proyecto.

Es importante mencionar que el tiempo que hay que invertir en auditar una empresa no es proporcional al número de sistemas, ya que el tiempo en el que se auditó una empresa con dos sistemas industriales sería el mismo en otra con cinco, ya que en los dos casos hay que estudiar los procesos de negocio y (muy probablemente) un solo conjunto de aplicaciones MES (de las que dependen todos los sistemas industriales) de la empresa y la única diferencia sería que para la segunda empresa hay que invertir un extra de tiempo para auditar más sistemas industriales o más plantas.

A continuación, se presenta una estimación de la duración que tendría el aplicar esta metodología en una empresa de tamaño medio/grande pero limitando el estudio sobre 5 sistemas industriales y sus dependencias:

Descripción tareas	Estimación		Fecha		Rol
	Días	Horas	Inicio	Fin	
Planificación	**1**	**8**	**-**	**-**	**G**
Implantación	**10**	**80**	**-**	**-**	**-**
Sistema Industrial	1d x 5	8h x 5	-	-	C
Sistema en general	5	40	-	-	C
Documentar resultados	**5**	**40**	**-**	**-**	**-**
Elaboración fija	4	32	-	-	C
Elaboración por Sistema Industrial	1 d x 5	8h x 5	-	-	C
Revisión	1	8	-	-	G
Presentación	**2**	**14**	**-**	**-**	**-**
Preparación	1	8	-	-	C
Revisión	½	4	-	-	G
Empresa	¼	2	-	-	G
Total Consultor	**20**	**160**	**-**	**-**	**-**
Total Gerente	**3**	**22**	**-**	**-**	**-**
TOTAL	**23**	**182**	**-**	**-**	**-**

7.3.2 COSTE DE LA AUDITORÍA

Si asumimos los mismos costes de software, hardware y conceptos adicionales, y volvemos a calcular el coste por personal, sería el siguiente:

Concepto	Horas	Precio Hora	Coste
Consultor	160	80 €	12.800 €
Gerente	22	200 €	4.400 €
Subtotal	**182**	**95 €**	**17.200 €**

El coste total en la finalización del proyecto es de 17.760 euros e incluye los siguientes conceptos:

Concepto	Coste
Personal	17.200 €
Software	0 €
Hardware	0 €
Adicionales	560 €
Total	**17.760 €**

Estos costes se podrían resumir en la siguiente fórmula:

CT = CA + CF + CF*(+/- 30%) + #SI * 16h

Donde:

- CA (Costes Adicionales): en función de la empresa será necesario realizar más o menos desplazamientos.
- CF (Costes Fijos): es una cantidad que varía poco (más menos 30%) en función del tamaño de la empresa y de los sistemas a auditar.
- #SI (Número de Sistemas Industriales): es el número de sistemas a auditar por el coste de 16 horas/hombre que se emplean al auditar cada uno (8 horas de implantación + 8 horas de documentación).

De acuerdo con esta fórmula, en el caso anterior sería:

CT= (560 €) + (22h gerente * 200 € + 80h consultor * 80 €) + (5 sistemas * 16h * 80 €) = 560 + 10.800 + 6400 = 17.760 €

El resultado de la aplicación de esta fórmula coincide con el cálculo y resultado anterior. Por lo que con esta sencilla formula, es posible calcular rápidamente el presupuesto de costes a incurrir en un marco de auditoría para cualquier tipo de empresa, con tan solo saber el número de sistemas industriales.

7.4 VALORACIÓN PERSONAL

Durante el desarrollo de este proyecto he tenido la sensación de estar aprendiendo cada día algo nuevo. Ha sido un proyecto sencillo en cuanto a que no hay cuenta con grandes dificultades técnicas, pero ha sido difícil desde el punto de vista de la elección y orden de tareas a realizar dentro de las muchas opciones, la gestión de todos los resultados obtenidos y la aplicación de los resultados en un entorno real, todo esto sin interrumpir los procesos del negocio de la empresa.

En cuanto a la aplicación del marco de auditoría de un sistema MES en un entorno real, estoy contento de los resultados obtenidos al nivel de ejecución hasta donde me permitieron realizar tantas pruebas como quise. Sin embargo en el nivel de planificación, me hubiera gustado realizar más pruebas pero no fue posible debido al riesgo que existía de bloquear el sistema ERP y porque los técnicos de la empresa no consiguieron hacer funcionar el antiguo sistema.

Asimismo, al nivel de control pude hacer tantas pruebas como quise contra la interfaz Ethernet (red local) pero no contra la interfaz Profibus, ya que la empresa no disponía de la tarjeta de red especial, igualmente me hubiera gustado realizar pruebas contra más sistemas industriales, pero no fue posible ya que las plantas estaban produciendo.

Otro aspecto que ha limitado la aplicación del marco en la empresa ha sido la limitación de tiempo, ya que la autorización necesaria para comenzar a realizarla se otorgó casi en el momento estimado a la finalización del proyecto, con lo que el tiempo disponible era menor del que se planificó en un principio.

Del mismo modo, un aspecto que me ha dejado insatisfecho con este proyecto, es el no haber dispuesto de los recursos económicos para comprar los plugins de Nessus y haberlos podido usar en la aplicación del marco de la auditoría, lo que la hubiera hecho mucho más completa. No obstante, entiendo que era complicado buscar patrocinadores para financiar su coste y que la empresa no iba a pagarlos hasta que no viera claramente sus ventajas, lo cual no pasaría hasta un tiempo después en el que reciban los resultados de la auditoría.

Considero que las formulas para planificar y presupuestar la auditoría obtienen una estimación bastante realista y fácil de emplear para calcular cuánto podría facturarse en cada proyecto, esto puede resultar muy útil a las personas que busquen ofrecer este tipo de servicios.

De acuerdo a todo lo que he aprendido durante este proyecto, considero que el aplicar un marco de auditoría a sistemas industriales, puede ayudar a muchas empresas a prevenir incidentes informáticos y a mejorar su gestión del riesgo.

Asimismo, me gustaría poder ayudar a la empresa auditada a solucionar las vulnerabilidades encontradas, porque considero que estoy en una posición aventajada para hacerlo ya que conozco el mundo de la seguridad en entornos industriales y ahora también conozco el funcionamiento de la empresa.

Finalmente, en los próximos meses me gustaría desarrollar varias herramientas de código abierto que ayuden a mejorar la seguridad de los entornos industriales y a automatizar la presente metodología.

7.5 FUTURO DE LA SEGURIDAD EN ENTORNOS INDUSTRIALES

En la actualidad el mercado de seguridad en entornos industriales es muy pequeño, pero está creciendo muy rápidamente, ya que por ejemplo, existen muy pocas herramientas para auditar los sistemas industriales, los estándares están en borrador o recién aprobados y prácticamente nadie en el sector las conoce.

No obstante, gracias a la labor de los medios de comunicación, el público en general y los administradores de sistemas en particular se están preocupando cada vez más por la seguridad, por lo que llegará el punto en que busquen la mejor manera de verificar la seguridad de los entornos industriales. Es precisamente por esto que considero que el número de nuevas herramientas especializadas y la aplicación/adaptación de herramientas genéricas irá en aumento.

En función de las necesidades detectadas en el desarrollo de este proyecto estimo que aparecerán (o me gustaría que aparecieran) estándares, técnicas y herramientas para:

- Medir el retraso introducido por los sistemas criptográficos y recursos de hardware ocupados como memoria, CPU, etc.
- Automatizar los análisis de riesgos y generación de informes.
- Incluir un gran número de plugins para los scanners de vulnerabilidades.
- Estandarizar y diseñar herramientas para verificar la resistencia ante ataques de las propias herramientas, ya que algunas instalan servidores y podrían servir también para atacar a los sistemas.
- Verificar el correcto funcionamiento de las herramientas de protección de sistemas y para demostrar que no hay interacciones perjudiciales para los sistemas donde se integran.

7.6 TRABAJO FUTURO

A continuación describo brevemente las tareas o las futuras líneas de investigación que se concluyen después de la realización del presente proyecto:

- Realizar pruebas técnicas contra más dispositivos industriales y de diferentes marcas.
- Realizar pruebas con herramientas de auditoría comerciales y con los plugins/firmas comerciales de Nessus y Snort.
- Implantar un IDS como Snort en una red industrial y estudiar el número de falsos positivos que más suelen producirse en este tipo de entornos.
- Ampliar y mejorar este marco de auditoría en función de los resultados obtenidos al aplicarlo en otras empresas, tales como nuevas herramientas, estándares y técnicas.
- Investigar vulnerabilidades en protocolos y aplicaciones, especialmente Modbus y ICCP.
- Desarrollar herramientas para la automatización del marco de auditoría.

8 ANEXOS

8.1 PUERTOS ABIERTOS

Listado de puertos abiertos por protocolo

Nombre	Tipo	Puertos	Servicio
Modbus	Protocolo comunicación	502 TCP	
Profibus/ Profinet	Protocolo comunicación	34962 TCP/UDP 34963 TCP/UDP 34964 TCP/UDP	Profinet unicast Profinet multicast Profinet server
Foundation Fieldbus	Protocolo comunicación	1089 TCP/UDP 1090 TCP/UDP 1091 TCP/UDP	FF Annunciation FF Fieldbus Message Specification FF System Management
DNP3	Protocolo comunicación	20000 TCP/UDP	
ICCP	Protocolo comunicación	102 TCP	

Puertos abiertos en algunos PLC disponibles en el mercado

Nombre	Modelo	Puertos	Servicio
Wago	¿	21 TCP 23 TCP 80 TCP 502 TCP ¿	FTP Telnet WWW Modbus
Siemens	S7-400	102 TCP 1010 TCP	

8.2 HERRAMIENTAS UTILIZADAS

Estas han sido las herramientas utilizadas en el proyecto:

Nombre	Descripción	Coste
Nmap	Escáner de puertos más usado. Sirve para detectar: Máquinas disponibles en la red, Puertos de comunicación abiertos Servicio que se ejecuta en cada puerto, sistema Operativo	Licencia GPL
Nessus	Escáner de vulnerabilidades. Permite: Máquinas disponibles en la red, Puertos de comunicación abiertos Servicio que se ejecuta en cada puerto, Vulnerabilidades en cada servicio, Sistema Operativo, Vulnerabilidades del sistema operativo	V2 GPL V3 Freeware Los plug-ins para detectar vulnerabilidades SCADA tienen un coste de $1200
Aircrack-ng Aircrack-ptw	Conjunto de herramientas para capturar, inyectar y descifrar tráfico encriptado con los algoritmos WEP de 64 y 128 bits	Licencia GPL
Bases de datos de vulnerabilidades	Se han utilizado las siguientes bases de datos de vulnerabilidades: • Altair • Secunia • CVE-Mitre • ISS X-Force	Gratuito

OPC Security Tester	Pequeña aplicación que prueba diversas operaciones para detectar vulnerabilidades en servidores OPC	Gratuita

8.3 EFECTOS SECUNDARIOS ESCANEOS DE DISPOSITIVOS DE CAMPO

En las siguientes tablas se muestra los efectos secundarios de escanear varios sistemas industriales y dispositivos de campo con distintas opciones de los escáneres Nmap y Nessus.

Dispositivo	Lantronix-Pantalla	Wago
Ping	OK	OK
nmap -sS -T5	OK	OK
nmap -sS -T5 -O	OK	OK
nmap -sS -sV -T5	Para lo que había, reinicia la pantalla y añade un * en la pantalla	OK
nmap -sS -sV -O -T5	Para lo que había, reinicia la pantalla y añade un * en la pantalla	OK
nmap -sS -sV -sR -O -T5	Para lo que había, reinicia la pantalla y añade un * en la pantalla	OK
nmap -sS -sR -T5	Para lo que había, reinicia la pantalla y añade una serie de caracteres sin sentido en la pantalla	OK
nmap -sU -T5	OK	Bloquea el servidor FTP y WEB
Nessus con DoS	Modifica pantalla: **GET / HTTP/1.0HELP	OK
Nessus sin DoS	OK	OK
Nessus DoS sin SafeChecks	Modifica pantalla: **GET / HTTP/1.0HELP y luego are you dead?	Bloquea el PLC por competo (luces rojas) a nivel de red pero I/O y Arena OK. Nessus: ataque Nestea CVE-1999-02

Tabla 2. Efectos secundarios escaneo sistemas laboratorio ESAII

Dispositivo	S7-400	OPC Almacen	SGAP Almacen	SGT Almacen	SGTP Almacen
Ping	OK	OK	OK	OK	OK
nmap -sS -T5	OK	OK	OK	OK	OK
nmap -sS -T5 -O	OK	OK	OK	OK	OK
nmap -sS -sV -T5	OK	OK	OK	OK	Se reinicia SQL Server
nmap -sS -sV -O -T5	OK	OK	OK	OK	Se reinicia SQL Server
nmap -sS -sV -sR -O -T5	OK	OK	OK	OK	Se reinicia SQL Server
nmap -sS -sR -T5	OK	OK	OK	OK	OK
nmap -sU -T5	OK	OK	OK	OK	OK
Nessus con DoS	OK	OK	Se reinicia SQL Server y crash svchost.exe	OK	Se reinicia SQL Server y crash svchost.exe
Nessus sin DoS	OK	OK	Se reinicia SQL Server	OK	Se reinicia SQL Server
Nessus DoS sin SafeChecks	OK	OK	Se reinicia SQL Server y crash svchost.exe	OK	Se reinicia SQL Server y crash svchost.exe

Tabla 3. Efectos secundarios escaneo sistemas empresa

8.4 DOCUMENTO ACEPTACIÓN AUDITORIA

PROYECTO DE AUDITORIA SISTEMAS INDUSTRIALES

A continuación se detallan las fases del proyecto de auditoría de los sistemas industriales de la empresa _____. Básicamente consiste en una primera fase de revisión de documentación existente y una segunda de revisión técnica. De esta manera se comprobará que las medidas de seguridad adoptadas son adecuadas para garantizar confidencialidad, integridad y disponibilidad de los sistemas de información y de fabricación para así garantizar que la producción de las fábricas no se verá afectada por un incidente de seguridad.

Objetivos de la auditoría:

- Estudio de la información proporcionada por la empresa
  - Listado de activos
  - Esquemas de red
  - Estadísticas de incidencias
  - Planes de contingencia
  - Políticas de seguridad
- Captura de información del sistema
  - Verificación del esquema de la red incluidas redes inalámbricas
  - Servicios que se ofrecen en los nodos
  - Vulnerabilidades de los servicios
  - Verificación de contraseñas

El responsable de la empresa ____ autoriza a ___ con DNI _____ a acceder a la documentación relevante para la realización del proyecto, a realizar las siguientes pruebas y asume el riesgo que conllevan y exime de este al auditor:

Marcar con una X las que apliquen: Documentación ☐ Activa ☐ Pasiva ☐

Fdo. A fecha: Sello:

8.5 GLOSARIO

Backup: copia de seguridad de los datos de un sistema de información para que en caso de pérdida se puedan recuperar de forma rápida.

Customer Relationship Management (CRM): software para la gestión de clientes y relación con estos muy utilizados en medianas y grandes empresas.

Denegación de servicio: ataque que afecta a la disponibilidad de un sistema.

Distributed Control Systems (DCS): son sistemas de control donde los elementos de control (I/O) están situados a una cierta distancia de la CPU principal que es la que controla los sucesos.

Enterprise Resource Planning (ERP): conjunto de aplicaciones software para gestionar el control de una empresa.

Exploit: código que se suele utilizar para demostrar la existencia de una vulnerabilidad mediante el ataque activo de esta aunque también se suelen utilizar por personas con fines maliciosos por lo que existe un amplio mercado negro.

Gusano: código malicioso que ataca vulnerabilidades en los sistemas informáticos que utiliza a su vez para propagarse y causar un efecto dañino. Suelen ser peligrosos tanto por su capacidad destructiva como por el colapso que provocan en las redes.

Hash: algoritmo criptográfico del que a partir de un texto o documento se obtiene un valor que lo identifica y del que es imposible obtener el valor original. El hash debe ser suficiente largo (número de bits) para garantizar que dos documentos distintos no generan el mismo hash. Algunos algoritmos son MD5, SHA1, Tiger-160.

Human Machine Interface (HMI): interfaces, normalmente gráficas, para que un operador pueda operar de forma fácil un sistema industrial.

MES (Manufacturing Execution System): es un conjunto de soluciones hardware y software que tienen como finalidad el hacer más eficientes los procesos de fabricación ya que mejoran la

comunicación entre los diferentes niveles del negocio y ofrecen información antes no disponible.

Material Requirements Planning (MRP): software para la planificación de requisitos en gestión de almacén.

Manufacturing Resource Planning (MRP II): software para la planificación de recursos en la industria.

Parche: actualización del software para corregir un defecto, algunos de ellos son de seguridad.

Programmable Logic Controller (PLC): ordenadores industriales que controlan procesos como la fabricación y que son capaces de operar en condiciones ambientales adversas. Su sistema operativo es capaz de realizar las operaciones asignadas en tiempo real.

Remote Terminal Units (RTU): terminales remotos formados por CPU y I/O situados a mucha distancia del centro de control. Generalmente la conexión con estos sistemas es mediante MODEM.

Router: dispositivo que interconecta y dirige el tráfico entre redes.

Salvaguarda: medida de seguridad para reducir o eliminar un riesgo en el sistema.

Sniffer: herramienta que captura datos de una red informática.

Supervisory Control And Data Acquisition (SCADA): aplicación para la supervisión de procesos en tiempo real.

Tablas Rainbow: listado de hashes de contraseñas que se utilizan para realizar ataques de diccionario y fuerza bruta más rápidamente.

Transmission Control Protocol (TCP): protocolo de comunicación orientado a conexión y fiable del nivel de transporte (capa 4 ISO).

User Datagram Protocol (UDP): protocolo mínimo de nivel de transporte orientado a mensajes.

Virus: programa o código malicioso que suele venir dentro de otro medio como correo electrónico, fichero, programa y que tiene la capacidad de replicarse automáticamente. Generalmente es necesaria la interacción del usuario para que realice su efecto dañino.

Vulnerabilidad: fallo de seguridad que puede permitir a un atacante local o remoto romper la confidencialidad, integridad y/o disponibilidad de un sistema.

9 BIBLIOGRAFÍA

Achilles [En línea] / aut. Technology British Columbia Institute of. - 2005. - http://www.bcit.ca/appliedresearch/security/projects/achilles.

appcluster05 [En línea] / aut. Singer Bryan L.. - Octubre de 2005. - http://www.appcluster05.com/images/375/Speakers/SP99%20-%20Singer.pdf..

Asociación de la industria Eléctrica - Electrónica [En línea] / aut. AIE. - 30 de Abril de 2007. - 30 de Abril de 2007. - http://www.aie.cl/comites/automat/articulos/agosto-06.pdf.

CIAG Research Projects [En línea] / aut. Pothamsetty Venkat // Honeynet for SCADA Environments. - 2005. - http://www.cisco.com/web/about/security/security_services/ciag/research/CRP_honeynet_for_scada_environments.html.

CIAG Research Projects [En línea] / aut. Wright Andrew // Secure Administrative Access in SCADA Networks. - 2005. - http://www.cisco.com/web/about/security/security_services/ciag/research/CRP_secure_administrative_access.html.

CIAG Research Projects [En línea] / aut. Wright Andrew // SCADA Serial Link Protection. - 2004. - http://www.cisco.com/web/about/security/security_services/ciag/research/CRP_scada_serial_link_protection.html.

Cisco CIAG Research Projects [En línea] / aut. Pothamsetty Venkat // ModBus Netfilter Extesion. - 2003. - http://www.cisco.com/web/about/security/security_services/ciag/research/CRP_netfilter_extensions.html.

Cisco Systems [En línea] / aut. Franz Matt // Scadasec.net. - Octubre de 2003. - http://www.scadasec.net/oldio/papers/franz-isa-device-testing-oct03.pdf.

Computerworld [En línea] / aut. Crawford Michael // Utility hack led to security overhaul. - 16 de Febrero de 2006. - http://www.computerworld.com.au/index.php?id=885750551.

Control System Security [En línea] / aut. ABB // Antivirus Guidelines. - 15 de Enero de 2006. - http://library.abb.com/GLOBAL/SCOT/SCOT296.nsf/VerityDisplay/61BC171DDC184AD1C12570FC00744ACD/$File/3BUR002683_C_en_CONTROL__SYSTEMS_SECURITY_-_ANTI_VIRUS_GUIDLINES.pdf.

Critical Infrastructure: Control Systems and the terrorist threat [Conferencia] / aut. Shea Dana A. // Report for Congress. - Washington : FAS, 2003.

Digital Bond [En línea] / aut. Peterson Dale // SCADA and Zotob Worm. - 2005. - http://www.digitalbond.com/index.php/2005/08/21/scada-and-zotob-worm/.

Digitalbond [En línea] / aut. Franz Matt // Livedata ICCP Heap-based buffer overflow. - 16 de Mayo de 2006. - http://www.digitalbond.com/wiki/index.php/LiveData_ICCP_Server_heap_buffer_overflow_vulnerability.

Digitalbond [En línea] / aut. Franz Matt. - 16 de Mayo de 2006. - http://www.digitalbond.com/index.php/2006/05/16/us-cert-livedata-iccp-vulnerability-note/ .

DigitalBond [En línea] / aut. Peterson Dale. - 2006. - http://www.digitalbond.com/wp-content/uploads/2006/11/scada_honeynets.pdf.

DNP.org [En línea] / aut. DNP. - 2006. - http://www.dnp.org/About/Default.aspx.

Electrónica Unicrom [En línea] / aut. López Luis González // Funcionamiento de un autómata. - 27 de Febrero de 2005. - http://www.unicrom.com/tut_PLC8.asp.

Evaluation of Symantec Security Products in an Areva T&D-Implemented SCADA Environment using ICCP Comunication Servers [En línea] / aut. S. Katipamula M.D. Hadley, T.P. McKenna. - Mayo de 2004. - http://enterprisesecurity.symantec.com/Content/displaypdf.cfm?PDFID=804.

GTI Services [En línea] / aut. American Gas Association. - Mayo de 2007. - http://www.gtiservices.org/security/.

Illinois Security Lab - Overview of DNP3 [En línea] / aut. LeMay Michael. - 2007. - http://seclab.uiuc.edu/docs/dnp-intro.pdf.

Illinois Security Lab - Overview of TASE.2/ICCP [En línea] / aut. LeMay Michael. - 2007. - http://seclab.uiuc.edu/docs/iccp-intro.pdf.

Industrial Information System Security - Part 1 [En línea] / aut. ABB. - Febrero de 2005. - http://library.abb.com/GLOBAL/SCOT/scot271.nsf/VerityDisplay/449A3AA6AD2B0997C125701A004C862A/$File/66-70%202M535%20ENG-72dpi.pdf.

Industrial Information System Security - Part 2 [En línea] / aut. ABB. - Marzo de 2005. - http://library.abb.com/GLOBAL/SCOT/SCOT296.nsf/VerityDisplay/811EC16CC4CC76B2C12571350078E048/$File/3BUS094320_en_ABB_Review_Security_2005_2.pdf.

Industrial Information System Security - Part 3 [En línea] / aut. ABB. - Abril de 2005. - http://library.abb.com/GLOBAL/SCOT/SCOT296.nsf/VerityDisplay/379EE9E980EE6A4FC12571350078E3C3/$File/3BUS094321_en_ABB_Review_Security_2005_3.pdf.

Industrial Security [En línea] / aut. Siemens. - 2007. - http://www.automation.siemens.com/download/internet/cache/3/1430001/pub/en/E20001-A410-P820-V1-X-7600.pdf.

Industrial security incident database subscriptions [En línea] / aut. BCIT. - 2007. - http://www.bcit.ca/appliedresearch/security/services.shtml.

Literature [En línea] / aut. Automation Rockwell // News & Events. - Mayo de 2005. - http://literature.rockwellautomation.com/idc/groups/literature/documents/td/rsas-td001_-en-p.pdf.

Malware Impact on Network Devices [En línea] / aut. CIAG Cisco. - 2005. - http://www.cisco.com/web/about/security/security_services/ciag/research/CRP_malware_impact.html.

Microsoft Compatibility Table for Various ABB OCS Products [En línea] / aut. ABB. - 10 de Mayo de 2006. - http://library.abb.com/GLOBAL/SCOT/SCOT296.nsf/VerityDisplay/B89F0AD90DF90E9CC125716A007398DB/$File/3BUA000061D1_N_en_Microsoft_Compatibility_Table_for_OCS_Products.pdf .

Microsoft Security Update Policy [En línea] / aut. ABB. - 2007. - http://www.abb.com/product/ap/seitp334/b98ec312595ea7a7c1256fd8005268eb.aspx.

Nettedautomation [En línea] / aut. Falk Herbert. - 2003. - http://www.nettedautomation.com/download/MMS-Analyzer-user-guide.pdf.

Network Security Infrastructure Testing [En línea] / aut. Laboratories Ray Parks - Sandia National. - 12 de Octubre de 2005. - http://www.sandia.gov/scada/documents/NSTB_NSIT_V1_2.pdf.

Neutralbit [En línea] / aut. Mora Lluís. - 16 de Febrero de 2007. - http://www.neutralbit.com/es/press/news/19/.

Neutralbit [En línea] / aut. Mora Lluís // SCADA Security Scientific Symposium. - Enero de 2007. - http://www.neutralbit.com/downloads/NB-NB-001-EXT-OPC%20Security%20Testing.pdf.

NISCC Good Practice on Firewall Deployment for SCADA and Process Control Networks [En línea] / aut. BCIT. - 15 de Febrero de 2005. - http://www.bcit.ca/files/appliedresearch/pdf/security/230205.pdf.

NIST - CSRC [En línea] / aut. Stouffer Keith, Falco Joe y Kent Karent // 800-82 - Guide to Supervisory Control And Data Acquisition (SCADA) and Industrial Control Systems Security. - 26 de Septiembre de 2006. - http://csrc.nist.gov/publications/drafts/800-82/Draft-SP800-82.pdf.

NIST Special Publication 1058: Using Host-Based Antivirus Software on Industrial Control Systems [En línea] / aut. Falco Joe. - 18 de Septiembre de 2006. - http://www.isd.mel.nist.gov/projects/processcontrol/NIST_SP1058.pdf.

OptiView Protocol Expert [En línea] / aut. Networks Fluke // OptiView Protocol Expert v. 8.0 Users Manual. - 2006. - http://www.flukenetworks.com/fnet/en-us/products/OptiView+Protocol+Expert/Manuals.htm?categorycode=LANS.

OSSTMM 2.2 [Libro] / aut. Herzog Pete. - Barcelona : ISECOM, 2006.

Plantdata Technologies, Inc. [En línea] / aut. Pollet Jonathan. - 2005. - http://www.controlglobal.com/whitepapers/wp_001_SCADApollet.pdf.

Rockwell automation [En línea] / aut. Automation Rockwell. - Mayo de 2006. - http://literature.rockwellautomation.com/idc/groups/literature/documents/pp/gmsn10-pp005_-en-e.pdf.

Rockwell Automation [En línea] / aut. Automation Rockwell. - 2006. - http://www.rockwellautomation.com/rockwellsoftware/assetmgmt/rsmacc/.

Rockwell Automation [En línea] / aut. Automation Rockwell // Allen-Bradley PLC-5. - Febrero de 2004. - http://literature.rockwellautomation.com/idc/groups/literature/documents/rn/1785-rn003_-en-p.pdf#xml=http://127.0.0.1/texis/search/pdfhi.txt?query=vulnerability&pr=literature.rockwellautomation.com&prox=page&rorder=500&rprox=750&rdfreq=0&rwfreq=0&rlead=25.

Sandia [En línea] / aut. Doggan David P. // Penetration Testing of Industrial Control Systems. - Marzo de 2005. - www.sandia.gov/scada/documents/sand_2005_2846p.pdf.

SCADA IDS Signatures [En línea] / aut. DigitalBond. - 25 de Abril de 2007. - http://www.digitalbond.com/wiki/index.php/SCADA_IDS_Signatures.

SCADA Security and Terrorism: we're not crying wolf [En línea] / aut. ISS-IBM // Blackhat Federal 2006. - 2006. - https://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf.

SCADA Security and Terrorism: We're not crying wolf [Conferencia] / aut. ISS. - Las Vegas : [s.n.], 2006. - Vols. http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf.

SCADA SYSTEMS AND THE TERRORIST THREAT: PROTECTING THE NATION'S CRITICAL CONTROL SYSTEMS [En línea] / aut. Representatives US House of. - 18 de Octubre de 2005. - http://www.fas.org/irp/congress/2005_hr/scada.pdf.

scadasec [En línea] / aut. Franz Matthew. - 30 de Enero de 2006. - 30 de Abril de 2007. - http://www.scadasec.net/secwiki/Protocols.

Securing SCADA Systems [Book] / auth. Krutz L.. - 2005.

Securing SCADA Systems [Libro] / aut. Krutz Ronald L.. - Indianapolis : Wiley Publishing Inc., 2006.

SecurityFocus [En línea] / aut. Lemos Robert // "Data storm" blamed for nuclear-plant shutdown. - 18 de Mayo de 2007. - http://www.securityfocus.com/news/11465/1.

SecurityFocus [En línea] / aut. Poulsen Kevil. - 2003. - http://www.securityfocus.com/news/6767.

Selinc [En línea] / aut. Paul W. Oman Allen D. Risley, Jeff Roberts, and Edmund O. Schweitzer, III. - 2006. - http://www.selinc.com/techpprs/6132.pdf.

Shared Physical SCADA Honeypots [En línea] / aut. Peterson Dale. - DigitalBond, 30 de Agosto de 2006. - http://www.digitalbond.com/index.php/2006/08/30/shared-physical-scada-honeypots/.

SIMATIC HMI [En línea] / aut. Siemens. - 2004. - https://www.click4business-supplies.siemens.de/images_artikel/e20001-a200-p810-v1-7800.pdf.

Simatic Net - Industrial Communications for Automation [En línea] / aut. Siemens. - Abril de 2007. - http://www.automation.siemens.com/download/internet/cache/3/1430628/pub/en/k_schrift_en_0407.pdf.

Simatic Net - Scalance W [En línea] / aut. Siemens. - 2005. - http://www.sea.siemens.com/scalance/docs/Scalance-W-Brochure.pdf.

Simatic PCS 7 [En línea] / aut. Siemens. - 2003. - https://www.click4business-supplies.siemens.de/images_artikel/e20001-a160-p280-x-7800.pdf.

Simatic Production Suite [En línea] / aut. Siemens. - 2005. - https://mes-simaticit.siemens.com/product_production_suite.asp?main=product.

Sisconet [En línea] / aut. Sistems Integration Specialists Company Inc.. - 25 de Febrero de 2005. - http://www.sisconet.com/downloads/NESSUS_Vulnerability_Announcement.pdf.

Soluciones de automatización para la indústria del cemento [En línea] / aut. Siemens. - 2007. - http://www.click4business-supplies.de/images_artikel/e20001-a490-p200-x-7800.pdf.

SRI [En línea] / aut. Cheung Steven [y otros] // Using Model-based Intrusion Detection for SCADA Networks. - 7 de Diciembre de 2006. - http://www.csl.sri.com/papers/scadaIDS07/SCADA-IDS-S4-2007.pdf.

Standard 1200 - Cyber Security [En línea] / aut. NERC. - 13 de Agosto de 2003. - ftp://www.nerc.com/pub/sys/all_updl/standards/rs/Urgent_Action_Standard_1200_Cyber_Security.pdf.

Symantec Solution for the Oil and Gas Industry [En línea] / aut. Symantec. - 2005. - http://eval.symantec.com/mktginfo/enterprise/fact_sheets/ent-factsheet_oil_and_gas_industry_solution_12-2005.en-us.pdf.

The Route to a Factory Information System [En línea] / aut. Systems Lighthouse. - 2006. - http://www.lighthousesystems.com/Home/content/File/Route%20to%20a%20Factory%20Information%20System%20new%20PDF.pdf.

Toorcon [En línea] / aut. MGrimes. - 2005. - www.toorcon.org/2005/slides/mgrimes/mgrimes-scadaexposed.pdf.

Transparent Modbus/TCP Filtering with Linux [En línea] / aut. Franz Matt. - 2003. - http://modbusfw.sourceforge.net/.

University of Louisville [En línea] / aut. Hieb Jeffery y Graham James H.. - Diciembre de 2004. - http://louisville.edu/speed/cecs/facilities/ISLab/tech%20papers/ISRL_04_03.pdf.

Using McAfee VirusScan Enterprise With System 800xA [En línea] / aut. ABB. - 18 de Abril de 2007. - http://library.abb.com/GLOBAL/SCOT/scot313.nsf/VerityDisplay/2A91238D48AFABC6C12572C10076DFD3/$File/3BSE048631_A_en_Using_McAfee_VirusScan_Enterprise_with_System_800xA.pdf.

vsantivirus [En línea] / aut. VSA. - 5 de Septiembre de 2003. - 30 de Abril de 2007. - http://www.vsantivirus.com/ev-blaster-apagon.htm.

Washington Post [En línea] / aut. Krebs Brian // Microsoft's Achilles' Heel: Office. - 5 de Enero de 2007. - http://blog.washingtonpost.com/securityfix/2007/01/microsofts_achilles_heel_offic_1.html.

Wikilearning [En línea] / aut. Wikilearning. - 2007. - http://www.wikilearning.com/historia_del_surgimiento_de_los_sistemas_erp-wkccp-11812-2.htm.

Wikipedia [En línea] / aut. Wikf. - 2007. - http://en.wikipedia.org/wiki/White_box_testing.

Wikipedia Devicenet [En línea] / aut. Wikc. - 2007. - http://en.wikipedia.org/wiki/Devicenet.

Wikipedia DNP3 [En línea] / aut. Wike. - 2007. - http://en.wikipedia.org/wiki/DNP3.

Wikipedia FF [En línea] / aut. Wikb. - 2007. - 30 de Abril de 2007. - http://en.wikipedia.org/wiki/FOUNDATION_fieldbus.

Wikipedia Fieldbus [En línea] / aut. Wikd. - 2007. - http://en.wikipedia.org/wiki/Profibus.

Wikipedia Modbus [En línea] / aut. Wik. - 2007. - 30 de Abril de 2007. - http://en.wikipedia.org/wiki/Modbus.

Wildpackets [En línea] / aut. Wildpackets // Etherpeek Decodes. - 2007. - http://www.wildpackets.com/support/product_support/etherpeek/decodes#others.

WinCC 6.2 [En línea] / aut. Siemens. - Marzo de 2007. - http://www.automation.siemens.com/salesmaterial-as/productbrief/es/kb_wincc_62_news_es.pdf.

wirelessdefence [En línea] / aut. COWPATTY. - 2006. - http://www.wirelessdefence.org/Contents/coWPAttyMain.htm.

wirelessdefence [En línea] / aut. wirelessdefence. - 2006. - http://www.wirelessdefence.org/Contents/Wireless%20Pen%20Test%20Framework.pdf.