



**Grado en Ingeniería del Software**

Curso Académico: 2013-2014

Seguridad en Sistemas de Información

Protección de Infraestructuras Críticas

(Basado en el trabajo “Critical Infrastructure Protection” de Antonio Guzmán Sacristán en Eleven Paths)

Autor: Francisco Javier Pulido Piñero

Tutor: Enrique Cabello

## Índice general

<b>1</b>	<b>Resumen .....</b>	<b>3</b>
<b>2</b>	<b>Introducción .....</b>	<b>4</b>
2.1	¿Por qué preocuparse?: Ataques intencionados.....	4
2.2	¿Por qué preocuparse?: Ataques NO intencionados .....	4
<b>3</b>	<b>Infraestructuras Críticas.....</b>	<b>5</b>
3.1	¿Qué es una infraestructura?.....	5
3.2	¿Qué es una infraestructura crítica? .....	5
3.3	¿Qué infraestructuras son consideradas críticas?.....	5
3.4	Esquema de la arquitectura de Infraestructuras Críticas .....	6
3.5	¿Por qué se consideran críticas? .....	7
3.6	Protección en Infraestructuras Críticas .....	7
<b>4</b>	<b>Los sistemas SCADA .....</b>	<b>8</b>
4.1	SCADA: OPC .....	8
4.2	Tipos de ataque que pueden sufrir los sistemas SCADA .....	9
<b>5</b>	<b>Sistemas MES.....</b>	<b>10</b>
<b>6</b>	<b>Sistemas ERP .....</b>	<b>10</b>
6.1	¿Cuál es el alcance de un ERP?.....	11
6.2	Hasta donde afecta la infección.....	11
<b>7</b>	<b>Curiosidad: Shodan .....</b>	<b>11</b>
<b>8</b>	<b>CIIP – ISO/EIC 27010 .....</b>	<b>12</b>
8.1	Control Systems Security Program (CSSP) – Certificación Estados Unidos .....	13
<b>9</b>	<b>Desafíos y futuro de la Seguridad en Infraestructuras Críticas.....</b>	<b>14</b>
<b>10</b>	<b>Referencias .....</b>	<b>16</b>

# 1 Resumen

Dentro del Máster de Ingeniería de Sistemas de Información en la asignatura de Seguridad en Sistemas de Información recibí formación sobre Protección de Infraestructuras Críticas, impartida por Antonio Guzmán Sacristán de la empresa Eleven Paths.

El presente documento tiene como intención exponer una visión global sobre este tipo de infraestructuras y los peligros activos y pasivos a los que se ven sometidas. Veremos qué es una infraestructura, los tipos y por qué podemos considerar si una infraestructura es crítica o no.

Hablaré sobre los sistemas SCADA, los sistemas MES, los ERP y distintos métodos de infección que sufren estos tipos de sistemas. Por otra parte mostraré el motor de búsqueda Shodan y lo sencillo que es encontrar un puerto asociado a una IP y acceder a los sistemas.

Veremos como se pueden proteger las Infraestructuras Críticas y la importancia de la Interdependencia entre Infraestructuras, así como los fallos en Cascada.

Analizaremos los tipos de certificación: CIIP-ISO (Critical Information Infrastructure Protection), algunas herramientas conocidas de CIIP y CSSP-US(Control System Security Program (CSSP).

Para finalizar hablaré sobre los futuros desafíos relacionados con las infraestructuras críticas.

## 2 Introducción

Antes de comenzar con la introducción debemos mostrar los antecedentes para poder comprender la importancia que tiene proteger sistemas que deben estar en perfecto funcionamiento, o si no podrían provocar desastres económicos, medioambientales o incluso acabar con vidas humanas.

### 2.1 ¿Por qué preocuparse?: Ataques intencionados

En Marzo de 1997 en Worcester Air Communications se realizaron ataques al sistema de comunicación de los aviones, provocando que decenas de ellos se quedaran sin comunicación y muchos otros tomaran decisiones incorrectas, poniendo en riesgo las vidas de miles de personas.

En Mayo de 2000 en Marooche Shire Sewage Spill, se detectaron ataques intencionados al sistema de seguridad su central nuclear, paralizando la producción y poniendo en riesgo el medioambiente y millones de vidas.

En Julio de 2010 el Stuxnet worm<sup>6</sup> infectó miles de computadoras alrededor del mundo, poniendo en jaque a toda los departamentos de inteligencia de todos los países del mundo.

### 2.2 ¿Por qué preocuparse?: Ataques NO intencionados

En Agosto de 2003:

- En el CSX Train Signaling System se infectó (con el virus SoBig) una computadora del cuartel general por abrir un email, tirando abajo las conexiones entre las centrales y los trenes, provocando retrasos e incluso la cancelación de decenas de líneas.

- La central nuclear de Davis-Besse mientras se encontraba parada por labores de mantenimiento, se introdujo al sistema por un camino secundario (email, pendrive..) un virus. Afortunadamente no ocurrió nada grave, simplemente se desinfectó el sistema.

- El Northeast Power Blackout estuvo inoperativo durante dos días a causa de una infección en el corazón de su sistema debido a un bug que tenía, dejando sin luz a los ciudadanos del área.

## 3 Infraestructuras Críticas

### 3.1 ¿Qué es una infraestructura?

Antes de ver el concepto de Infraestructura Crítica, debemos plantear el concepto de Infraestructura:

**Infraestructura:** redes de sistemas o procesos que operan colaborativamente y sinérgicamente para generar bienes o productos o asegurar su continua distribución.

Estos procesos serán:

- Independientes
- De Carácter privado
- Hechos por el hombre

Los tipos de infraestructuras que nos podemos encontrar son:

- Instalaciones civiles: como pueden ser los aeropuertos, las plantas refinadoras, los edificios, los parques solares, etc.
- Entornos fabriles: las cadenas de producción, el control de automatismos, etc.
- Defensa: Comunicaciones, radares, etc.

### 3.2 ¿Qué es una infraestructura crítica?






Podemos considerar que estas infraestructuras son críticas cuando:





**Son aquellas cuya incapacitación podría conducir a un serio debilitamiento en el sistema nacional de defensa, económico o bienestar social.**




Además, estas infraestructuras dependen de los sistemas IT para sus funcionalidades esenciales. Siendo fundamentales la fiabilidad y resistencia de estos sistemas que interconectan estas infraestructuras.

### 3.3 ¿Qué infraestructuras son consideradas críticas?

A continuación un listado de las categorías de infraestructuras que se pueden considerar como críticas:

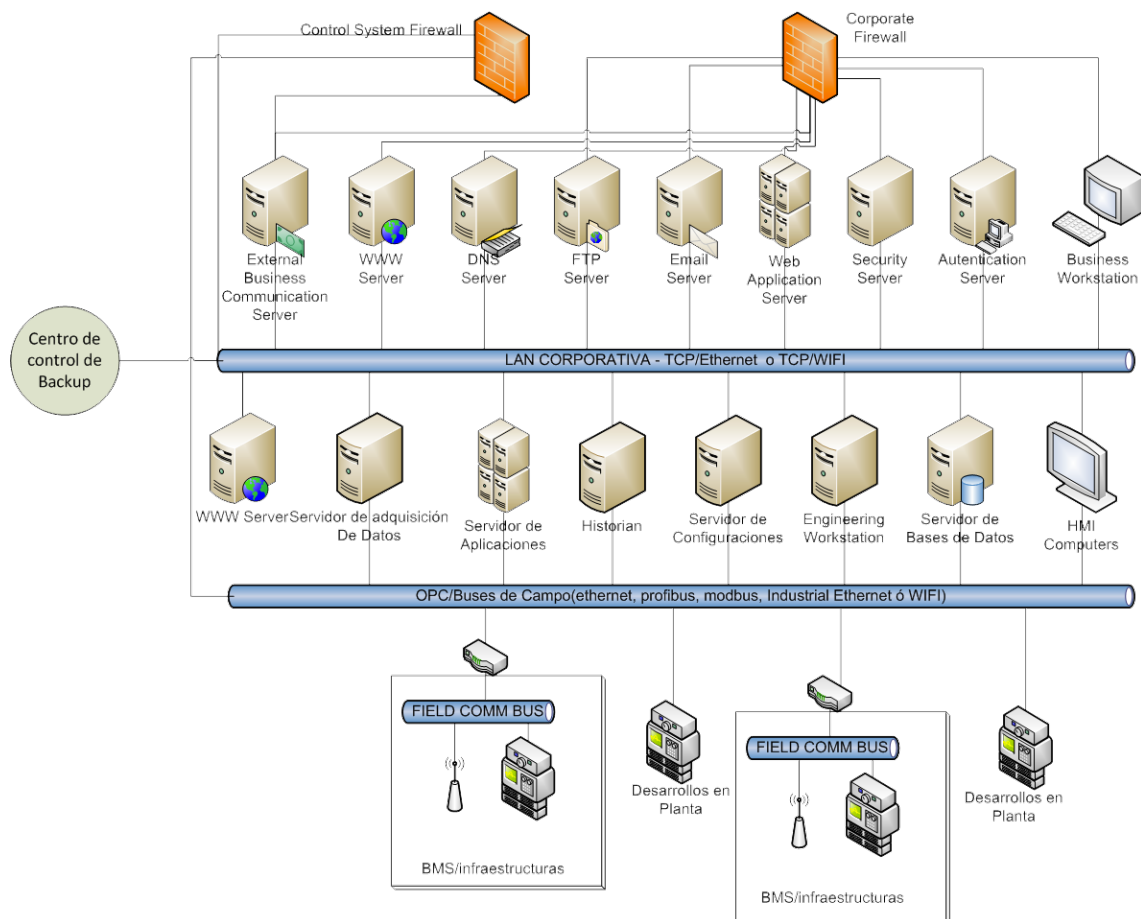
	Sistemas de telecomunicación		Los sistemas de emergencia, rescate y protección civil
	Sistemas de suministro eléctrico		Sistemas de suministro de alimentos (producción, almacenamiento y distribución)
	Sistemas de suministro de Gas Natural y Combustibles basados en hidrocarburos		Sistemas aeroespaciales

	Bancos y sistemas financieros
	Transporte
	Sistemas de suministro de agua y gestión de residuos
	Servicios gubernamentales y judiciales

	Productos estratégicos (Hierro, acero, aluminio y algunos productos manufacturados)
	Sistema sanitario
	Sistema educativo

### 3.4 Esquema de la arquitectura de Infraestructuras Críticas

Mediante el esquema que veremos a continuación entenderemos cómo se compone una Infraestructura Crítica:



Como podemos observar se divide en tres grupos (de arriba hacia abajo):

- Zona entre los Sistemas Firewall de Control/Corporativos y Lan Corporativa: aquí podemos encontrar servidores WWW, servidores FTP, Workstation, servidores de autenticación, etc.
- Zona Lan Corporativa y OCP/Buses de Campo(Ethernet, WIFI...): en esta zona se encuentran los servidores de configuración, los servidores de bases de datos, etc.

- Zona OCP/Buses de Campo(Ethernet, WIFI...): aquí están las infraestructuras, los desarrollos en planta, etc.

### 3.5 ¿Por qué se consideran críticas?








- Potencialmente pueden afectar a muchas personas y puede suponer enormes pérdidas económicas e incluso de vidas humanas.
- Pueden suponer la detención de los servicios de forma masiva.
- Pueden provocar la detención del servicio de otras infraestructuras al existir interdependencia entre ellas.
- En definitiva, porque trascienden el mundo digital y suponen que una vulnerabilidad en un sistema informático termina afectando no solo a nuestra información sino también a nuestro día a día.

### 3.6 Protección en Infraestructuras Críticas

En las infraestructuras críticas es preciso y altamente prioritario garantizar:

- Seguridad: deben tener un sistema de seguridad que evite infecciones en el sistema y que esté altamente estudiado para la arquitectura que se vaya a proveer.
- Continuidad: deben estar compartimentadas de manera que si una se cae no afecte al resto.
- Disponibilidad: debe existir un plan de emergencia que evite que el sistema esté caído a causa de una infección, ataque o explotación de alguna vulnerabilidad.

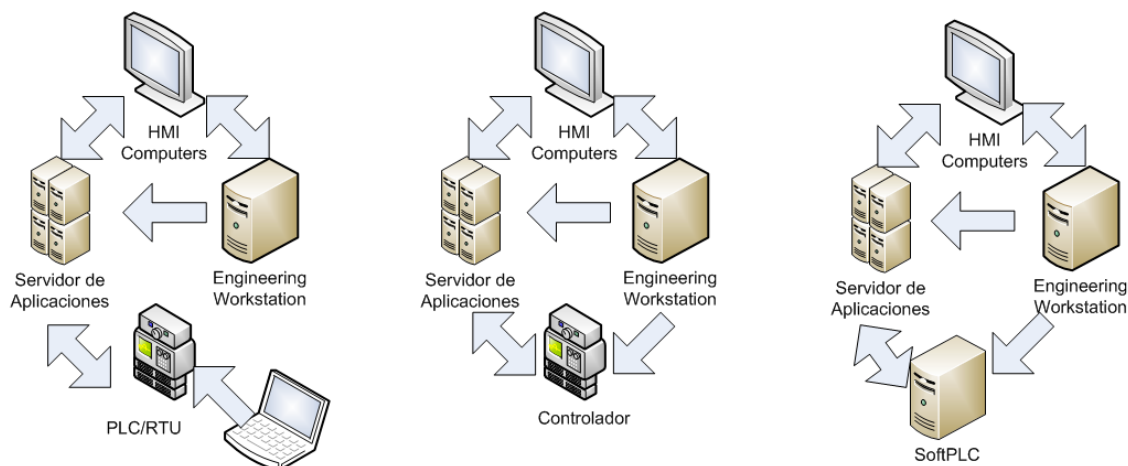
Pero proteger una infraestructura crítica conlleva una serie de desventajas asociadas a la propia arquitectura:

	Formación de los operarios de planta y servicios de mantenimiento demasiado especializada.
	Necesidad de Continuidad. Problemas a la hora de definir políticas de actualización, parcheo o pentesting.
	Necesidad de alto rendimiento. Dificil adopción de soluciones de seguridad clásicas (antivirus, antimalware, ... incluso métodos de autenticación).
	Falsa sensación de seguridad debido a la utilización de soluciones específicas.
	Coste de los daños provocados por un ataque exitoso.
	Información de carácter crítico y estratégico.
	Interdependencias entre infraestructuras.

# 4 Los sistemas SCADA

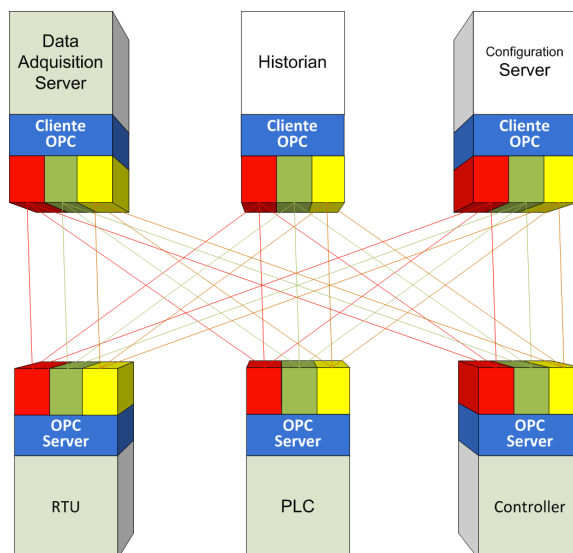
Los sistemas SCADA son muy complejos, tolerantes a fallos, sujetos a restricciones de tiempo real y que también se les suele denominar sistemas de automatización, sistemas de control distribuido o sistemas de control de procesos.

Algunas arquitecturas de ejemplo:



## 4.1 SCADA: OPC

El OPC (OLE. Object Linking and Embedding for Proceses Control) es un estándar de comunicación en el campo del control y supervisión de procesos:



De este modo se elimina la necesidad de que todos los dispositivos cuenten con drivers para dialogar con múltiples fuentes de datos. Basta con que tengan un Driver OPC.

En realidad OPC es un conjunto de protocolos entre los que podemos destacar los siguientes:

<b>OPC-DA</b> <i>(Acceso a Datos)</i> Para el intercambio de datos a tiempo real	<b>OPC-AE</b> <i>(Alarmas y eventos)</i>	<b>OPC-B</b> <i>(Batch)</i> Útil en procesos discontinuos	<b>OPC DX</b> <i>(Data eXchange)</i> Proporciona interoperabilidad entre
--	---	---	--



entre servidores y clientes			varios servidores.
<b>OPC-HDA</b> <i>(Acceso a datos históricos)</i> Acceso a datos históricos OPC.	<b>OPC-S</b> <i>(Seguridad)</i> Especificar cómo controlar el acceso de los clientes a los servidores	<b>OPC XML-DA</b> <i>(Acceso a datos XML)</i> Para el intercambio de datos como OPC-DA pero en vez de COM/DCOM utiliza mensajes SOAP (sobre http) con documentos en XML.	<b>OPC-CD</b> <i>(Datos complejos)</i> Permite a los servidores exponer y describir tipos de datos más complicados en forma de estructuras binarias y documentos XML.

## 4.2 Tipos de ataque que pueden sufrir los sistemas SCADA

A continuación tenemos un listado de los tipos de ataque que pueden sufrir los sistemas SCADA:

- **SQL Injection:** (inyección directa de comandos SQL o SQL injection) Técnica utilizada por personas maliciosas con el fin de alterar o atacar un sitio o servidor a través de comandos SQL. Las inyecciones utilizan información de entrada del usuario combinado con comandos SQL para construir una consulta SQL maliciosa. En otras palabras, se "inyecta" un código SQL malicioso para alterar el funcionamiento normal de las consultas SQL programadas por los diseñadores/webmasters. Al no haber seguridad, el código se ejecuta con consecuencias alarmantes. Con estas inyecciones se pueden obtener datos escondidos, eliminar o sobrescribir datos en la base de datos y hasta lograr ejecutar comandos peligrosos en la máquina donde está la base de datos. El hecho de que un servidor pueda verse afectado por las inyecciones SQL se debe a la falta de medidas de seguridad por parte de sus diseñadores/programadores, especialmente por una mala filtración de las entradas (por formularios, cookies o parámetros). En sistemas SCADA, se ven afectados los Servidores de adquisición de Datos, los Servidores de Aplicaciones, el Histórico, el Servidor de Base de datos y las computadoras HMI.
- **Ataque OPC/DCOM:** se basa en introducir software malicioso a través de los puertos físicos de las computadoras. Estos pueden afectar al Servidor de Adquisición de Datos, al Histórico y a las computadoras HMI.
- **Main in the Middle:** consiste en estar a la escucha de las comunicaciones entre dos interlocutores. Una vez en medio el software malicioso se puede hacer pasar tanto por el receptor como por el emisor, adquiriendo el control de las comunicaciones. En SCADA afecta al Servidor de Adquisición de Datos, al Histórico y a las computadoras HMI.
- **Acceso a puertas traseras a través de un punto de acceso:** consiste en encontrar un acceso oculto dentro del sistema de seguridad. Esto afecta al Servidor de Adquisición de Datos, al Histórico y a las computadoras HMI.
- **Acceso mediante puerta trasera a través de internet:** se consigue mediante la utilización de bugs en el sistema operativo o en la versión de los navegadores y sus

plugins, en internet o intranet y esto da acceso en sistemas SCADA a servidores de bases de datos y computadoras HMI.

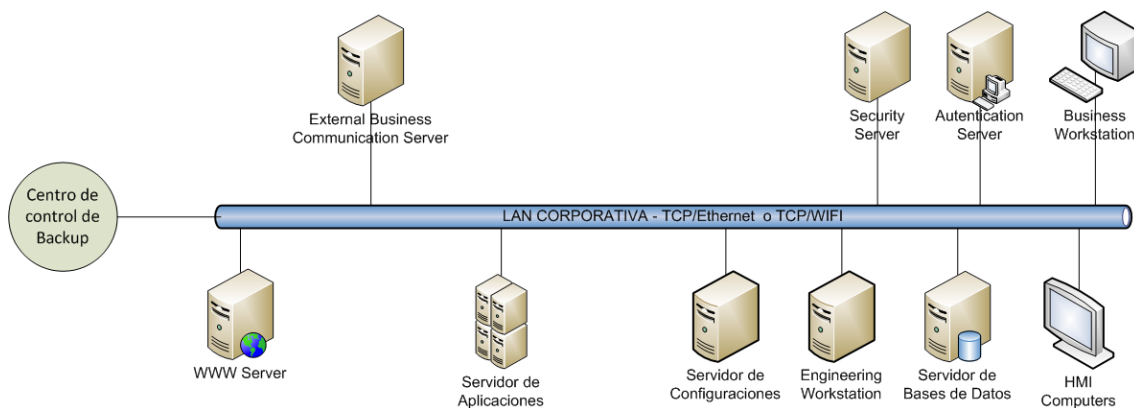
- XSS: XSS, del inglés Cross-site scripting es un tipo de inseguridad informática o agujero de seguridad típico de las aplicaciones Web, que permite a una tercera parte inyectar en páginas web vistas por el usuario código JavaScript o en otro lenguaje script similar (ej: VBScript), evitando medidas de control como la Política del mismo origen. Este tipo de vulnerabilidad se conoce en español con el nombre de Secuencias de comandos en sitios cruzados. En sistemas SCADA afecta a las Workstation de ingeniería y a las computadoras HMI.

## 5 Sistemas MES

Los sistemas MES (Manufacturing Execution System) son sistemas con consideraciones de tiempo real cuyos objetivos tienen que ver con:

- La producción: planificación, administración de recursos, medidas de rendimiento, gestión de órdenes, etc.
- El personal: control de presencia, control de accesos, etc.
- La calidad: TQM(Total Quality Management), SPC(Statistical Process Control), etc.

Se centran la zona LAN CORPORATIVA – TCP/Ethernet o TCP/Wifi:



## 6 Sistemas ERP

Una solución ERP, del inglés Enterprise Resource Planning, es lo que en español conocemos como Software de gestión integrada, y se define como un grupo de módulos conectados a una única base de datos.

El ERP es un paquete de software que permite administrar todos los procesos operativos de una empresa, integrando varias funciones de gestión en un único sistema; en otras palabras, representa la “columna vertebral” de una empresa.

El ERP se define según dos principios básicos:

- Aplicaciones informáticas como módulos independientes, pero perfectamente compatibles en una única base de datos común.

- El uso de un motor de flujos de trabajo debe permitir definir todas las tareas de un proceso y gestionar su aplicación en todos los módulos del sistema.

## 6.1 ¿Cuál es el alcance de un ERP?

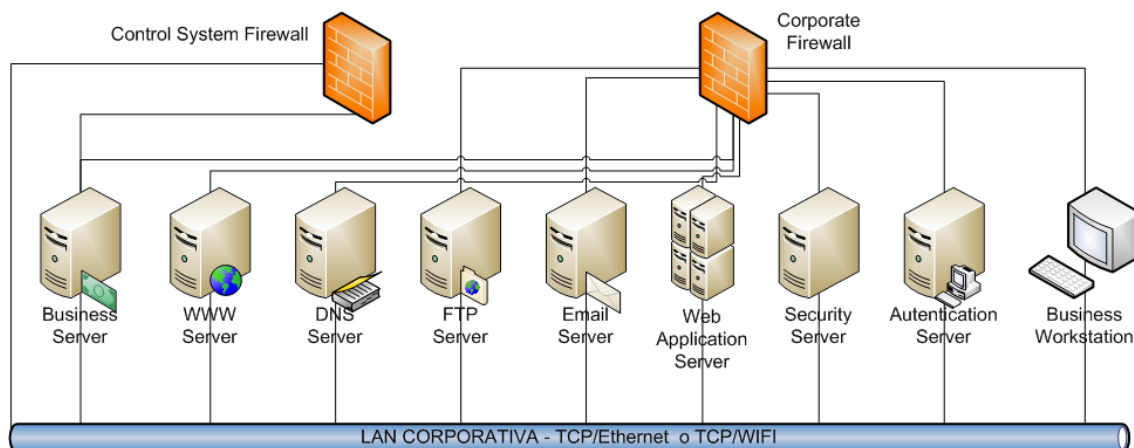
Un paquete de software de gestión integrada permite construir un sistema de información homogéneo sobre una base única. De este modo cubre un amplio ámbito de gestión:

- Gestión de compras
- Gestión de ventas
- Gestión contable: contabilidad de clientes, de proveedores, activos, personal..
- Control de gestión
- Gestión de la producción (planificación, etc.)
- Gestión de stocks (logística)

Así pues, un ERP se compone de varios módulos que corresponden a cada una de las áreas de gestión y garantiza la unicidad de la información que contiene, porque solo hay una única base de datos lógica.

## 6.2 Hasta donde afecta la infección

El siguiente gráfico muestra cuales son las principales partes que se pueden ver afectadas a través de ataques a sistemas SCADA:



# 7 Curiosidad: Shodan

A diferencia de Google que rastrea la Web en busca de sitios web, el buscador Shodan navega en los canales de Internet ocultos, los raros, los misteriosos. Es una especie de Google en busca de servidores distraídos y conectados sin seguridad a la web, cámaras web encendidas sin seguridad, impresoras, routers, etc.

Shodan recoge información en 500 millones de dispositivos conectados a la red y también en páginas web mal ocultas en tiempo real.



En realidad, Shodan recoge los banners que existen en las cabeceras de las web, que tienen un aspecto parecido al siguiente:

```
HTTP/1.0 301 Moved Permanently
Content-Type: text/html; charset=UTF-8
ETag: ""
Location: http://www.neoteo.com/
Server: Microsoft-IIS/7.5
Date: Sun, 07 Apr 2013 08:12:44 GMT
Content-Length: 145
```

Con estos datos podemos saber en ocasiones a que tipo de dispositivo nos estamos conectando y algunas veces hasta las versiones, pudiendo operar a través de los agujeros de seguridad conocidos para cada versión. Por ejemplo si hay algún sistema que no ha cambiado el password por defecto, podríamos introducirlo y hacernos con el control.

Los sistemas SCADA se ven afectados por ataques, que en muchas ocasiones utilizan herramientas como Shodan para interceptar los sistemas. A veces también la Ingeniería Social puede hacernos introducirnos en los sistemas SCADA, mediante uso de personal muy cualificado, actores, etc que logren introducirse hasta el centro del sistema.

## 8 CIIP – ISO/EIC 27010

En el contexto heterogéneo y multidimensional de las Infraestructuras Críticas, las infraestructuras de información críticas pueden verse amenazadas por catástrofes naturales, fallos técnicos, errores humanos, crimen internacional, etc. Por todo ello es necesaria una aproximación holística y colaborativa para su protección, centrándose en tres objetivos fundamentales:

- Prevenir los ataques informáticos contra las infraestructuras de información críticas.
- Reducir la vulnerabilidad nacional a los ciberataques.
- Reducir al mínimo los daños y el tiempo de recuperación cuando estos ataques se producen.

Por ello, existe un campo de investigación mucho más maduro, denominado Information Security Management (ISM) que mantiene una relación muy estrecha con CIIP.

Existen múltiples propuestas de estándares, taxonomías y recomendaciones globales que persiguen igualar a los diferentes estándares en el área de seguridad de la información (ISM-Information Security Management), que sí están reconocidos internacionalmente.

Desde 2012, se ha publicado la norma 27010, dentro de la familia ISO/EIC 27000 que proporciona una guía sobre seguridad de la información y las comunicaciones entre las industrias en los mismo sectores, en diferentes sectores industriales y con los gobiernos.

En concreto, la CIIP – ISO/EIC 27010 proporciona controles y orientaciones relativas específicamente a iniciar, implementar, mantener y mejorar la seguridad de la información en las comunicaciones inter-organizacionales e intersectoriales, es aplicable a todas las formas de intercambio y difusión de la información, tanto pública como privada, nacional e internacional, dentro de la misma industria o sector de mercado o entre sectores.

En particular, puede ser aplicable a los intercambios de información y el intercambio relaciones con el suministro, mantenimiento y protección de una organización o la infraestructura crítica del estado nación.

En el último año, ha habido grandes avances en CIIP, en concreto:

- Investigación de las dependencias y los efectos de cascada. Para estos estudios la teoría de sistemas complejos y la simulación han demostrado ser herramientas potentes y efectivas.
- Proposición de esquemas y procesos de colaboración que permitan compartir el conocimiento entre toda la comunidad de manera que la protección de una infraestructura se pueda hacer de manera mucho más eficiente aprovechando y reutilizando la información generada para otras infraestructuras similares en contextos parecidos.
- Investigación en la seguridad de los sistemas SCADA. Algunos ejemplos son las normativas ISA/IEC-62443.

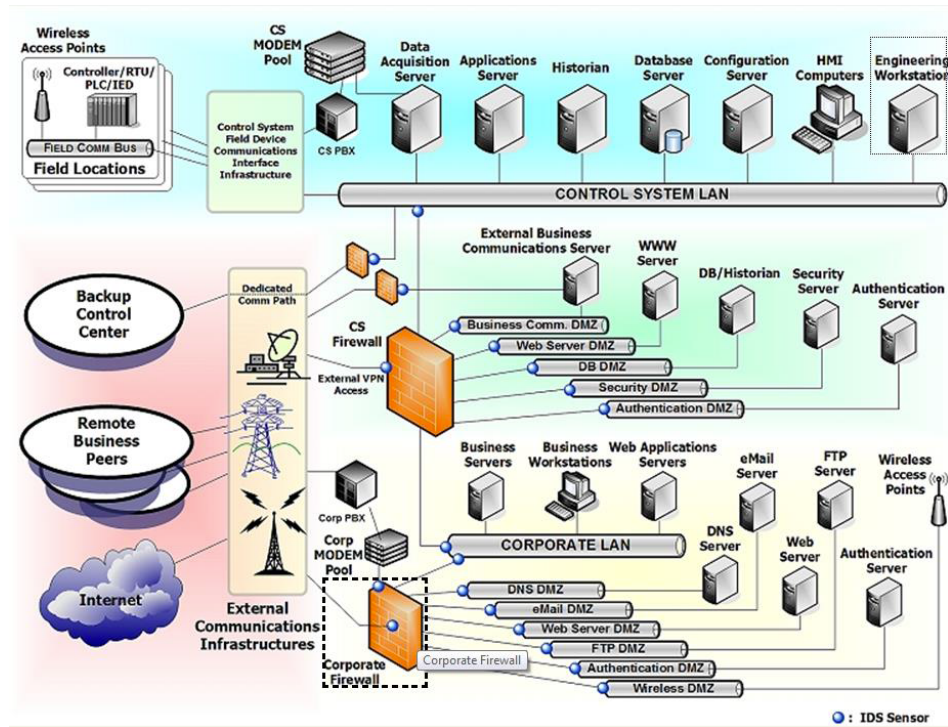
Por otra parte existen herramientas para CIIP relacionadas con ISM, bastante útiles para los problemas con infraestructuras críticas:

- Análisis de riesgos:
  - Hazard and operatbility study (HAZOP)
  - Fault Tree Analysis (FTA)
  - Failure Mode and Effect Analysis (FMEA)
  - Métodos basados en modelos de Markov y modelos ocultos de Markov
  - CCTA Risk Analysis
- Detección de ataques en tiempo real
  - Intelligent Event Proccesing (IEP)

## 8.1 Control Systems Security Program (CSSP) – Certificación Estados Unidos

En Estados Unidos llevan muchos años de ventaja respecto al mundo en cuanto a la seguridad y protección de infraestructuras críticas. Para ello utilizan la herramienta Cyber Security Evaluation Tool (CSET).

Prueba de ello es el diseño de arquitectura segura que tienen planteada en su documentación oficial:



## 9 Desafíos y futuro de la Seguridad en Infraestructuras Críticas

Aún quedan muchos retos que superar en la seguridad en infraestructuras críticas. De hecho, el avance depende en gran medida del “juego” entre hackers y sistemas, donde los sistemas van evolucionando a base de ser explotados en la mayor parte de los casos.

Si tuviéramos que realizar un listado del futuro de la seguridad en infraestructuras críticas pasaría por lo siguiente:

- Gestión de la propiedad de los servicios esenciales
- Control sobre la prestación de los servicios
- Intercambio de Información
- Trabajo en Equipo

El punto de Gestión de la propiedad de los servicios esenciales es el siguiente paso, que se podría desglosar en las siguientes características:

- Se debe legislar convocando a los sectores que serán impactados por la legislación.
- Quién controle debe garantizar el manejo ético e independiente de la información provista por quién opera los servicios.
- Para que el ciudadano participe, los distintos participantes (quien opera y quien controla) deben generar confianza y brindar transparencia.
- Es fundamental contar con un repositorio único de información en el cual se registren los activos, los incidentes, los cambios y todo dato que sea relevante al control.
- La protección de los servicios esenciales debe ser una política de estado.

# 10 Referencias

- [1] Charla de Antonio Guzmán Sacristán en Máster en Ingeniería de Sistemas de Información. Eleven Paths. [www.elevenpaths.com](http://www.elevenpaths.com) @ElevenPath

(Fecha: octubre 2013)