Protección en Infraestructuras Críticas. Análisis de seguridad de los sistemas de control industrial.

Autor: Sergio Díaz Marco.

Tutor: Jorge Chinea López.

Profesor: Helena Rifà Pous.

Master Universitario en Seguridad de las TIC.

Seguridad en la Internet de las Cosas.

Créditos/Copyright

FICHA DEL TRABAJO FINAL

Título del trabajo:	Protección en infraestructuras críticas. Análisis de seguridad de los sistemas de control industrial.
Nombre del autor:	Sergio Díaz Marco.
Nombre del colaborador/a docente :	Jorge Chinea López.
Nombre del PRA:	Helena Rifà Pous.
Fecha de entrega (mm/aaaa):	12/2019
Titulación o programa:	Master en Seguridad de las TIC.
Área del Trabajo Final:	Seguridad en la Internet de las Cosas.
Idioma del trabajo:	Español.
Palabras clave	Ciberseguridad – Infraestructuras Críticas - Industrial

Resumen del Trabajo :

En los últimos años se han repetido ataques a sistemas críticos y sistemas de control industrial de lo más diverso, desde una red eléctrica a plantas potabilizadoras de agua, y año tras año el número de incidentes se incrementa. La evolución de los sistemas de control ha pasado de sistemas monolíticos muy sencillos a sistemas con múltiples usuarios y ubicaciones, además de contener el activo más valioso de la actualidad: la información. Esto ha favorecido que desde delincuentes a Estados soberanos hayan planificado y perpetrado estos ataques, con el objetivo de obtener algún rédito estratégico o monetario. Pese a todos estos ataques, la seguridad de los sistemas hoy en día, sigue sin ser una prioridad para muchas empresas.

El objeto de este documento es analizar las infraestructuras críticas (IC) y sistemas de control industrial (SCI) y las causas más comunes que han facilitado el ataque a estos sistemas en los últimos años. Con esa información, se pretende elaborar una serie de pautas para la protección de estos sistemas. Se revisaran las arquitecturas con DMZ y los mecanismos de seguridad como IDS o IPS que se implementan en la actualidad.

Partiendo de la base de que nunca es posible obtener una protección total de un sistema, es cierto que tener en cuenta y llevar a cabo pequeñas pautas como rutina, permitirían reducir el número de incidentes en ciberseguridad. Las infraestructuras críticas son sistemas básicos para el mantenimiento de la sociedad que no deberían fallar, y por tanto es fundamental prestar la atención que necesitan para protegerlos de agentes externos.

Protección en infraestructuras críticas. Análisis de seguridad en los sistemas de control industrial.

Abstract (in English, 250 words or less):

In recent years several attacks on critical systems and industrial control systems have been taking place with an increasing level of difficulty. From a power grid to water treatment plants, the number of incidents increases every year. The evolution of controlling systems has changed from very simple monolithic systems to multiple users and locations systems. Nowadays we can say that information is one of the most valuable tools for corporations. This results that criminals and sovereign States have carried out these attacks. However, the security of these systems is not a priority for the majority of the companies.

The purpose of this document is to analyze the critical infrastructure (IC) and industrial control systems (SCI) and the most common causes that have allowed the attack on these systems in recent years. With these information, I´m going to create a guideline to increase the protection of these systems. The architectures with DMZ and the security mechanisms such as IDS or IPS that are currently implemented will be reviewed as well.

Although small guidelines would reduce the number of incidents greatly, it´s never possible to reach full protection in a system. However, critical infrastructures are basic systems for the maintenance of society that should not fail. These infrastructures are companies most vulnerable security value and they should make every effort possible to protect it.

Agradecimientos

A mi mujer y mis hijos por animarme a seguir adelante.

A mis padres por ayudarnos a todos en los momentos más necesarios.

Resumen

En los últimos años se han repetido ataques a sistemas críticos y sistemas de control industrial de lo más diverso, desde una red eléctrica a plantas potabilizadoras de agua, y año tras año el número de incidentes se incrementa. La evolución de los sistemas de control ha pasado de sistemas monolíticos muy sencillos a sistemas con múltiples usuarios y ubicaciones, además de contener el activo más valioso de la actualidad: la información. Esto ha favorecido que desde delincuentes a Estados soberanos hayan planificado y perpetrado estos ataques, con el objetivo de obtener algún rédito estratégico o monetario. Pese a todos estos ataques, la seguridad de los sistemas hoy en día, sigue sin ser una prioridad para muchas empresas.

El objeto de este documento es analizar las infraestructuras críticas (IC) y sistemas de control industrial (SCI) y las causas más comunes que han facilitado el ataque a estos sistemas en los últimos años. Con esa información, se pretende elaborar una serie de pautas para la protección de estos sistemas. Se revisaran las arquitecturas con DMZ y los mecanismos de seguridad como IDS o IPS que se implementan en la actualidad.

Partiendo de la base de que nunca es posible obtener una protección total de un sistema, es cierto que tener en cuenta y llevar a cabo pequeñas pautas como rutina, permitirían reducir el número de incidentes en ciberseguridad. Las infraestructuras críticas son sistemas básicos para el mantenimiento de la sociedad que no deberían fallar, y por tanto es fundamental prestar la atención que necesitan para protegerlos de agentes externos.

Palabras clave

Sistema Control Industrial, Infraestructuras Criticas, Ciberseguridad, Ciberataques.

Índice

Figuras y tablas

Índice de figuras

Índice de tablas

1.Introducción.

Los sistemas de control industrial (en adelante SCI) están implantados en la sociedad actual en todas las tareas que se desarrollan diariamente. Detrás de tener electricidad o agua potable en casa, hay un SCI que lleva a cabo un control automático para realizar esa tarea de la forma más automatizada posible.

Dentro de los SCI hay unos más importantes que otros: por ejemplo, los sistemas que están en un hospital o que ayudan a la gestión de la red eléctrica son más críticos que aquellos que manejan una pequeña industria. Debido al perjuicio para la sociedad que supondría un fallo de estos sistemas, se consideran sistemas críticos o infraestructuras críticas (en adelante IC).

Los SCI de hace unas décadas, se instalaban y permanecían aislados de redes y sistemas informáticos. La comunicación entre operario y SCI era mediante sinópticos que estaban compuestos por pilotos e interruptores. En algunos casos se podía incluir alguna pantalla táctil (HMI) o incluso un ordenador. En este ordenador se instalaba el programa necesario para comunicarse con el sistema y durante toda la vida del ciclo no se actualizaba ni la maquina ni el sistema operativo y la única comunicación del ordenador era con el automatismo del SCI.

Los últimos avances en la industria conectada han propiciado un gran desarrollo de la gestión y optimización de estos sistemas. Ahora esos sistemas están altamente relacionados con sistemas propios de las TI, como bases de datos o programas de gestión corporativa, lo que facilita una mejor gestión. Por el contrario, han traído otros problemas asociados, derivados de que son más accesibles que nunca. Esto ha propiciado ataques a SCI e IC nunca vistos hasta ahora.

El punto de inflexión, pese a no ser el primer caso, fue el gusano STUXNET que consiguió el paro del programa nuclear iraní en el año 2010. La complejidad del mismo, su orientación a atacar a un sistema en concreto de la marca Siemens, así como la posterior propagación del mismo se podría considerar como la primera ciberarma que atacaba a SCI e IC.

1.1. Descripción.

Se pretende realizar un estudio sobre el estado de los SCI e IC en la actualidad y analizar a qué amenazas se enfrentan. Para ello se va a partir de un análisis histórico de cómo han evolucionado estas amenazas y cómo afectan en la actualidad a los SCI, que tienen más en común con las Tecnologías de la Información (en adelante TI) que con los primeros SCI, aislados de cualquier red y con sistemas y protocolos cerrados.

Protección en infraestructuras críticas. Análisis de seguridad en los sistemas de control industrial.

Sin lugar a dudas es un tema importante que tiene gran impacto en la sociedad. Continuamente aparecen noticias de ataques que afectan a una IC o a una empresa. El número de este tipo de ataques crece año tras año, tanto en cantidad como en sofisticación.

Además del enfoque teórico, que contextualizará los sistemas usados en la actualidad y las amenazas a las que se enfrenta, se pretende aportar una visión de cómo se pueden fortalecer estos sistemas para hacerlos más resistentes a estos ataques. También es importante tener en cuenta que no solo los sistemas son vulnerables, sino que los operadores y usuarios también pueden ser parte del problema o de la solución, tanto desde el diseño como desde la operación.

1.2. Objetivos generales

El objetivo general de este TFM es analizar las diferentes amenazas que sufren los SCI, principalmente orientado a las IC, para después desarrollar una serie de medidas para minimizar los daños y proteger así estas infraestructuras frente a posibles ataques.

1.2.1. Objetivos principales

Estudiar los SCI:

- Recopilar información sobre los SCI existentes: Autómatas y SCADAs.
- Analizar información sobre protocolos de comunicación en SCI.
- Analizar Información sobre los elementos de campo usados en SCI.

Analizar las IC:

- IC en España.
- Datos estadísticos sobre ataques a IC.

Analizar las amenazas existentes en SCI e IC:

- Elaborar un histórico de los ataques más importantes.
- Recopilar la información relevante sobre ataques reales.
- Analizar de contagio y propagación (vectores de ataque).

Desarrollar medidas de fortalecimiento en SCI e IC:

- Elaborar medidas a aplicar para la protección de SCI.
- Desarrollar pautas para el diseño de sistemas.
- Analizar las limitaciones en el diseño.

1.3. Metodología y proceso de trabajo

El proceso de trabajo a desarrollar va a ser el siguiente:

- Recopilación de información. Para ello se usarán fuentes como INCIBE (Instituto Nacional de Ciberseguridad) o CNPIC (Centro Nacional de Protección de Infraestructuras Críticas), además de usar documentación de carácter privado de empresas de seguridad como Karspesky o ESET.
- Análisis y clasificación de la información, separando como temas principales: SCI, IC, Amenazas y Fortalecimiento de SCI.
- Análisis de casos reales, teniendo muy en cuenta tanto lo que ha pasado, y qué es lo que ha fallado para que suceda un incidente de ciberseguridad.
- Conclusiones y medidas a tomar. Fortalecimiento de SCI.

La parte más importante consistirá en la recopilación de información. Para ello se acudirá a fuentes de garantía, quedando fuera en la medida de lo posible noticias del ámbito del periodismo y apostando por instituciones del ámbito público o empresas de seguridad que proporcionaran rigor y conocimientos técnicos.

Una vez recogida toda la información se procederá a clasificarla, facilitando así el análisis y comprensión de los datos. A partir del análisis de la información clasificada se procederá a elaborar las medidas más adecuadas para la fortificación. Es importante para ello partir del análisis de casos reales y averiguar qué ha pasado y porqué, si por ejemplo se ha producido un incidente por un mail malicioso, una vulnerabilidad 0-day o una actualización no instalada. Teniendo la visión de otros ataques, se analizarán las medidas que se pueden tomar para asegurar los SCI.

Todos estos pasos se reflejan en el siguiente diagrama de flujo (ver ilustración 1).

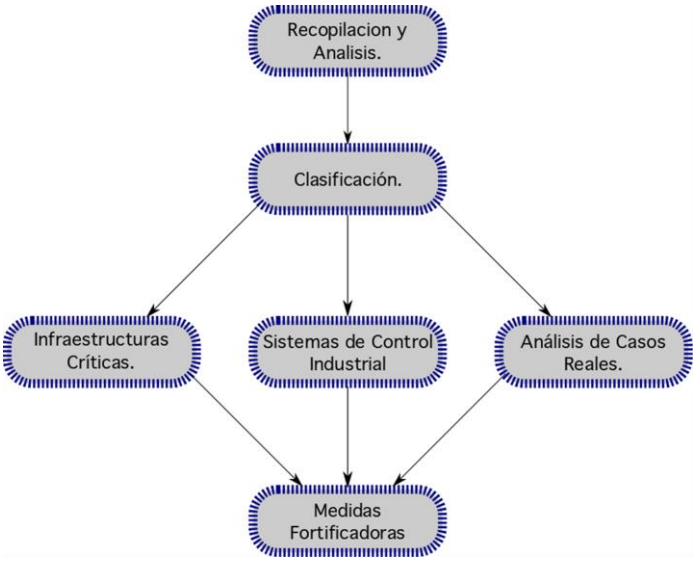


Ilustración 1 : Metodología de trabajo.

1.4. Planificación

En la Tabla 1 se describen las tareas a llevar a cabo y el tiempo previsto de realización de cada una de ellas. Por su parte, en la Ilustración 2, se ha diseñado un diagrama de Gantt para plasmar visualmente la cronología del trabajo a desarrollar, con el objetivo de ajustarse después a los plazos marcados.

Tabla 1 : Planificación de tareas

PLANIFICACIÓN.	DIAS	Fecha Inicio	Fecha Fin.
1.Elaboración del Plan de trabajo.	13	18/09/19	01/10/19
2.Recopilación de documentación	11	24/09/19	05/10/19
3.Lectura y Análisis	24	05/10/19	29/10/19
4.Analizar la IC	20	10/10/19	29/10/19
4.1 IC en España	10	10/10/19	19/10/19
4.2 Analizar datos estadísticos sobre ataques a IC	10	10/10/19	19/10/19
5. Estudio de los SCI existentes.	20	10/10/19	29/10/19
5.1 Información ISA 95	7	10/10/19	16/10/19
5.2 Protocolos de comunicaciones	7	17/10/19	23/10/19
5.3 Elementos de campo.	6	24/10/19	29/10/19
6. Analizar las amenazas existentes en SCI e IC.	20	10/10/19	29/10/19
6.1 Elaborar histórico de las amenazas mas importantes.	7	10/10/19	16/10/19
6.2 Recopilación de información relevante de los ataques	7	17/10/19	23/10/19
6.3 Vectores de ataque.	6	24/10/19	29/10/19
7 Fortalecimiento SCI e IC	20	10/10/19	29/10/19
7.1 Elaborar medidas a aplicar en la protección de SCI	7	10/10/19	16/10/19
7.2 Desarrollar pautas para el diseño de sistemas	7	17/10/19	23/10/19
7.3 Analizar de limitaciones en el diseño.	6	24/10/19	29/10/19
8. Clasificación de la información para el desarrollo del TFM	28	29/10/19	26/11/19
9. Elaboración de la memoria principal.	34	27/11/19	31/12/19
10. Elaboración del video de defensa del TFM.	13	01/01/20	07/01/20
11. Preparación de la defensa del TFM.	4	13/01/20	17/01/20

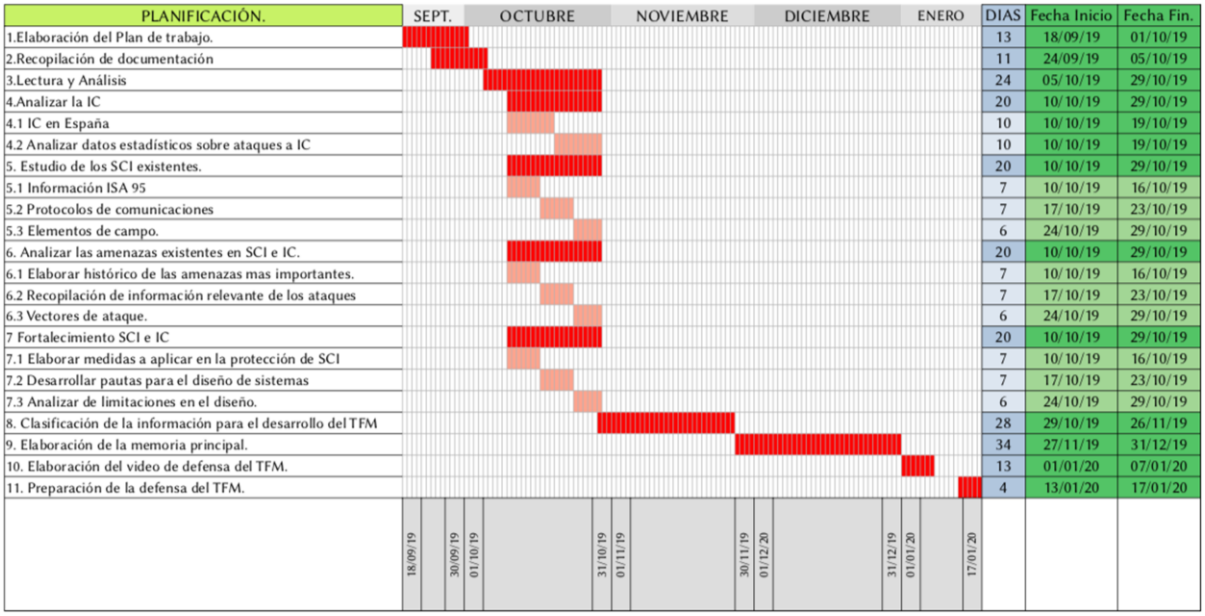


Ilustración 2 : Planificación del TFM. Diagrama de GANTT

1.4.1. Descripción de Tareas.

A continuación se van a describir las tareas a llevar a cabo:

- Elaboración del plan de trabajo. La realización de este documento es de vital importancia, ya que este documento supone el punto de partida de todo el desarrollo del TFM.
- Recopilación de documentación. Realizar una labor de investigación sobre todos los temas a tratar, utilizando para ello diversas fuentes tanto nacionales como internacionales, noticias de prensa, guías y documentos técnicos.
- Lectura y Análisis. Análisis crítico de toda la información recopilada para hacer un cribado de la información más relevante.
- Investigación sobre IC. De toda la información válida, analizar la que trata sobre Infraestructuras Críticas.
    - Analizar las IC en España.
    - Analizar datos estadísticos sobre ataques a IC.
- Investigación sobre SCI. De toda la información valida, analizar la que trata sobre Sistemas de Control Industrial.
    - Recopilar información sobre la ISA95 y las diferentes capas de un SCI.
    - Analizar la información sobre protocolos de comunicación.
    - Analizar la información sobre los elementos de campo.
- Investigación sobre ciberarmas y ciberataques. De toda la información valida, analizar la que trata sobre ciberataques o ciberarmas.
    - Elaborar un histórico sobre los ataques más importantes.

    - Recopilar información sobre ataques reales.
    - Analizar vectores de ataque.

- Investigación sobre securización de sistemas. De acuerdo a la información recogida en los apartados anteriores, se desarrollarán medidas para la securización de sistemas. Esta será la parte más importante del TFM.
    - Medidas a aplicar en la protección de SCI.
    - Desarrollo de pautas en el diseño de sistemas.
    - Analizar de las limitaciones de diseño.
- Clasificación de la información para el desarrollo del TFM. Reordenación y elaboración del guion sobre el que se va a redactar el TFM. Organización en capítulos, apartados y anexos.
- Elaboración de la memoria principal. Redacción de la memoria de acuerdo a todas las tareas anteriores.
- Elaboración del video defensa del TFM.
- Preparación de la defensa del TFM.

1.5. Estado del arte.

En la actualidad continuamente se informa en medios de comunicación y web especializadas de ataques a SCI e IC. Muchos de estos ataques se realizan a infraestructuras cotidianas como hospitales o servicios de distribución de aguas, que son la base de cualquier Estado del Bienestar.

Muchos de estos sistemas se pusieron en marcha en el siglo pasado (parece que suene raro, pero estos sistemas tienen una vida que supera los 20 años siguen hoy en día funcionando). Vienen de una época en la que no existían tantas amenazas, y mucho menos estas infraestructuras requerían una conexión a Internet. Muchas de estas instalaciones no se actualizaban nunca mientras estuvieran funcionando, (ni el firmware de PLC, ni las versiones de SCADA). La evolución de Internet arrastró a todas estas instalaciones por inercia a conectarse también, lo que supuso un gran avance porque permitía monitorizar, trabajar o incluso realizar tareas de mantenimiento remotamente en las instalaciones. Pero por el contrario abrió una puerta que permanecía cerrada. Las instalaciones estaban ahora conectadas a la red, con los riesgos que esto suponía (sobre todo en equipos con una cierta edad y que no se había actualizado lo más mínimo). Estas instalaciones tenían como prioridad básica de funcionamiento la disponibilidad y rapidez. Tenían que estar el mayor número de horas funcionando sin problemas y además lo más rápidamente posible. Sin embargo en su diseño no se contempló su seguridad. Eran sistemas basados en la confianza, y por lo tanto, no se dudaba de cualquier acción que se llevara a cabo sobre las mismas.

Sin embargo desde hace unos años nos encontramos un panorama diferente. Cada año el número de ataques a sistemas de control aumenta y continuamente se encuentran vulnerabilidades en estos sistemas. Los ataques que antes realizaban jóvenes sin ayuda, los realizan ahora todo tipo de ciberterroristas e incluso Estados soberanos los llevan a cabo como forma de alcanzar posiciones estratégicas de control sobre otros países. En 2010 se marcó un antes y un después con Stuxnet, una ciberarma que consiguió para el programa nuclear Iraní, lo que antes hubiera supuesto un ataque militar. El ataque consistió en diseñar un malware que consiguió detener el programa nuclear iraní mediante el ataque a las centrifugadoras de uranio. Crear Stuxnet, según muchos expertos, requirió de un número elevado de programadores y recursos.

Durante muchos años, los técnicos que programan y desarrollan estos sistemas de control industrial han provenido del mundo de las Tecnologías de la Operación (TO en adelante) donde el panorama de seguridad es muy diferente. Conceptos como usuarios, perfiles y permisos son conceptos que en las TI se usan desde los tiempos UNIX, pero que en TO se seguía ignorando en el desarrollo de cualquier sistema. Solamente el creciente número de incidentes ha hecho cambiar esta perspectiva.

En los próximos años se va a convertir en un tema de gran importancia, dado que las IC son la base de cualquier país, y además, los SCI están en los tejidos productivos de cualquier nación. Poco a poco las empresas se están empezando a concienciar de la importancia de la seguridad, tanto por costes que puede repercutir un ataque como las consecuencias sobre su imagen corporativa de un posible ataque.

En España se han creado diversas instituciones gubernamentales cuyo objetivo es fomentar las buenas prácticas y la formación para la prevención de ciberataques. Podríamos destacar:

- INCIBE (Instituto Nacional de Seguridad).
- CNPIC (Centro Nacional de Protección de Infraestructuras Críticas).
- CCN (Centro Criptológico Nacional).

El resultado del presente TFM pretende analizar el funcionamiento de los SCI y cómo se han transformado los SCI de las TO a las TI, pasando de sistemas monolíticos a sistemas que se pueden encontrar en múltiples ordenadores, siendo éstos, accesibles desde diferentes ubicaciones. Se llevará a cabo una investigación de los incidentes de seguridad en España en 2018. También se realizará un análisis de los ataques más mediáticos ocurridos en los últimos años.

Con toda esta información se procederá a recoger y exponer medidas fortificadoras en SCI. Estas medidas estarán orientadas desde la fortificación del sistema en sí, hasta los servicios que se encuentran asociados y que trabajan conjuntamente.

2. Estructura de un Sistema de Control Industrial.

En esta parte se van a mostrar los elementos de cualquier sistema de control industrial. Queda claro que no todos los sistemas de control industrial van a tener todos los elementos, pero también es cierto que para que exista un sistema de control, deben existir los dos niveles más bajos según el modelo ISA95 que son: Nivel 1 elementos de campo, sensores y actuadores que permiten interactuar con el mundo real y Nivel 2 control de Procesos, donde está la lógica de control que hacer en cada situación. Es un tema muy importante a tener en cuenta porque debajo de cada IC siempre existe un SCI que controla todo o parte de un proceso. (Ver ilustración 3).

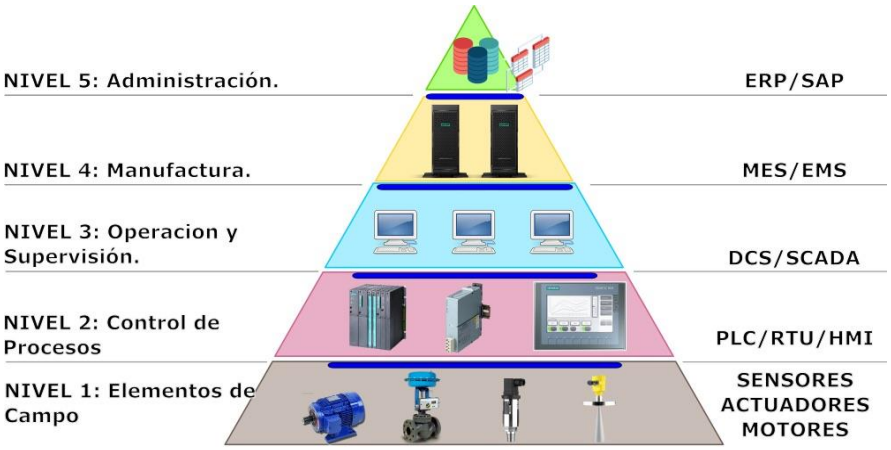


Ilustración 3 : Modelo ISA 95.

2.1. Modelo ISA 95.

Para esta parte se usa como referencia el Modelo ANSI/ISA 95, que es un estándar internacional desarrollador por ISA (International Society of Automation) para el desarrollo de sistemas de control e integración con los elementos de la organización.

Hoy en día no se entiende ninguna industria en la que los procesos productivos estén separados de cualquier otro proceso (administrativo, stock, etc.) pero sí es cierto que hasta hace no mucho eso sí era así. En la actualidad cualquier proceso productivo es controlado, en un intento de buscar optimizaciones de cualquier tipo (desde reducir un coste, mejorar una instalación que se avería o reducir un tiempo productivo). Todos los elementos por dispares que sean se recogen y se analizan conjuntamente y ahí es donde entran las capas superiores y las tecnologías de la información.

La idea de ISA95 es la integración, desde el sensor de campo hasta el ERP (Enterprise Resource Planning). El ERP es un elemento que interactúa con todos los recursos de la empresa compartiendo

esa información entre departamentos. El más conocido de estos sistemas es SAP, de la compañía alemana SAP SE.

2.2. Capa 1. Elementos de Campo.

Los elementos de campo pueden dividirse en dos grandes grupos:

- Accionadores: Elementos que mediante una orden de origen eléctrico ejercen un trabajo mecánico en el mundo real. Puede ser una válvula que permita abrir o cerrar el paso a un fluido, un motor que permita mover una materia prima o un relé para arrancar una máquina de cualquier tipo. Interactúan con el mundo real.
- Sensores: Recogen información en forma de magnitudes físicas del mundo real. Ejemplos de sensores pueden ser aquellos que midan un nivel de un depósito, una temperatura o un caudal de fluido. Esta información es enviada a la siguiente capa para que, de acuerdo a esta información, adopte la decisión programada previamente.

Tanto accionadores como sensores tienen que comunicarse de alguna manera con la capa superior, en este caso los autómatas o dispositivos similares en sus múltiples variantes. Para ello los PLCs (Programmable Logic Controller o Controlador Lógico Programable) disponen de entradas y salidas con el mundo real. Hay varios tipos de PLCs, según lo que estemos conectando (se comentara más en profundidad en la siguiente capa), pero en resumen hay entradas y salidas, que pueden ser analógicas (valor cuantitativo) o digitales (valor SI o NO). Normalmente los accionadores van en las salidas y los sensores en las entradas de los PLCs. Estas entradas y salidas funcionan mediante señales eléctricas.

Los 4 tipos de e/s más usados para el control de procesos son:

Tipo	Descripción.	Interface	Uso
AI Analog Input	Entrada Analógica. Hace referencia al PLC, es decir que el sensor es una salida analógica. Generalmente se usan señales eléctricas para enviar la información analógica. En la actualidad se usan más señales de corriente 4..20mA o 0..20mA por inmunidad al ruido y preferiblemente 4..20mA por su capacidad de detección de rotura de cable.	0-10V 2-10V 4..20mA 0..20mA PT100 (T) PT1000 (T)	Presión Temperatura Humedad Caudal ...
AO Analog Output	Salida Analógica. Hace referencia al PLC. Se usan para controlar elementos que no son todo o nada, como válvulas proporcionales o velocidad de motores. Preferiblemente se utilizan señales por corriente.	0-10V 2-10V 0..20mA 4..20mA	Velocidad Apertura ...

DI Digital Input	Entrada Digital. Hace referencia al PLC. Se usan en la detección de estados o informaciones binarias, ej: un depósito en el máximo nivel, un interruptor de caudal. Como peculiaridad, las entradas digitales de los PLC están aisladas galvánicamente. Mediante un opto acoplador se separan los circuitos de campo, de la electrónica del PLC.	Nivel 0-5V	Max Min Interruptor de Flujo Final de Carrera ...
DO Digital Output	Salida Digital. Hace referencia al PLC. Se usan en el mando de órdenes a elementos de campo. Lo elementos que se controlan son todo o nada, arranque o paro de un bomba o elemento, apertura o cierre de una válvula.	0-5V Salida Relé Salida Transistor	Marcha/Paro elementos

También hay elementos de campo que usan un protocolo específico de comunicación para enviar esa información al PLC, y que a su vez pueden ser “accionados”. Es decir, se tienen las entradas y salidas pero mediante unos protocolos de comunicación entre equipos.

Los protocolos más usados en SCI son: Modbus, Profibus, Profinet o HART. Generalmente este método de integrar se usa en elementos que incorporan ya su lógica de funcionamiento con un PLC y sólo se permite su actuación (arranque/paro de la máquina, y consignas de proceso). Estas máquinas son en sí mismas un SCI. Un ejemplo podría ser un grupo electrógeno (mediante ordenes arrancamos o paramos), pero dentro lleva un sistema que controla todos los parámetros de funcionamiento, y nosotros mediante este protocolo de comunicación se transmiten ordenes de arranque y paro.

2.3. Capa 2. Control de Procesos.

El control de procesos se realiza mediante PLC. Existen diferentes equipos asociados al control de elementos:

- PLC: es el que dota a los procesos de capacidad de decisión. Es un controlador en el que secuencialmente se introducen las decisiones que tiene que tomar en cada punto de un proceso.
- Periferia Descentralizada: son terminales “tontos”, es decir, no aportan ninguna capacidad de toma de decisiones en un proceso. Simplemente repiten las señales que vienen
- RTU (Remote Terminal Unit): es muy parecido a la periferia descentralizada no tiene lógica de control, la mayor diferencia es que está pensada para comunicarse con el controlador principal mediante GSM/GPRS o señales de RF. Destacan entre sus características bajo consumo, capacidad de almacenar datos localmente y un amplio rango de temperaturas de trabajo.

- PAC (Programmable Automation Controllers): una variante más avanzada que los PLC pero con su misma filosofía, la diferencia radica en que incluyen características avanzadas como control de servomotores, comunicaciones avanzadas o incluso interactuar con bases de datos mediante SQL.

Existen múltiples variantes posibles en las arquitecturas que se pueden disponer para el control de procesos, dependiendo del caso concreto. A continuación se exponen las más usadas:

- Maestro/Esclavo: se basa en un PLC que actúa de maestro en decisiones que afectan al conjunto de los esclavos y unos equipos esclavos que controlar una pequeña parte de todo el proceso. Se opta por esta arquitectura cuando la parte que tiene que controlar cada esclavo, o es una maquina única, o es importante no perder todo el proceso en caso de un fallo. El maestro comunica con el SCADA.
- PLC con periferia descentralizada: se utilizan cuando un proceso no es extremadamente crítico, pero espacialmente es una instalación en la que hay mucha distancia o incluso zonas de diferentes peligrosidad como ATEX (abreviaturas de Atmósfera Explosiva). Ahorra costes en cableado al usar esta periferia descentralizada como interface de entrada/salida con el mundo real, que se conectará con el PLC mediante una comunicación.
- Maestros Redundantes: pueden ser usados en múltiples arquitecturas, en procesos críticos. En cuanto a ejecución o en peligrosidad se suelen usar para que, en caso de que caiga un PLC, el otro continúe con los procesos de planta, evitando de este modo una parada de un proceso o una situación que desencadene algún peligro. Se puede usar con periferia descentralizada o en arquitecturas maestro/esclavo.

La programación de un PLC se realiza mediante un listado de secuencias lógicas ordenadas en las que al final se toma una decisión, tal y como se muestra en la ilustración 4.

```
SI NivelDeposito > 240cm ENTONCES
    Bomba=OFF;
SI NivelDeposito < 100cm ENTONCES
    Bomba=ON;
FSI
```

Ilustración 4 : Seudocódigo.

También puede realizarse en el caso de una toma de decisiones más refinada de máquinas de estados, en el que a cada estado de una máquina se llega mediante una serie de condiciones y avanza mediante otras. En cada uno de los estados se ejecuta una parte del proceso (ver ilustración 5).

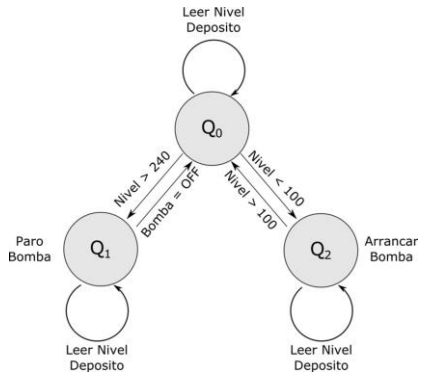


Ilustración 5 : Maquina de estados. Control de una bomba.

Para transcribir estos diseños, ya sea mediante seudocódigo o mediante una máquina de estados, se desarrollan para la programación de PLC diversos lenguajes basados en el estándar internacional IEC 61131-3. Publicada por primera vez en diciembre de 1993 por la IEC (International Electrotechnical Commission) y actualizada en 2013. Bajo este estándar se describen los lenguajes de programación de PLC compuestos por tres lenguajes gráficos (LD, FBD y SFC) y dos textuales (IL y ST). Los equipos del fabricante alemán Siemens también usan estos lenguajes de programación, si bien su denominación está basada en las siglas en alemán y no en las inglesas como en el resto de fabricantes de PLC. Los diferentes lenguajes de programación son:

-Lenguaje ST Structured Text. (**SCL** Structured Control Language en Siemens).

Es lo más parecido al seudocódigo y en los últimos años se ha adoptado principalmente por su parecido con lenguajes estructurados usados en TI. Un ejemplo de programa podría ser este (ver ilustración 6).

```
IF (NIVEL < 100) THEN
        BOMBA:=TRUE;
ELSIF (NIVEL > 240) THEN
        BOMBA:=FALSE;
END_IF;
```

Ilustración 6 : Código en Lenguaje ST.

Es muy parecido a Pascal. Permite el uso de operaciones aritméticas, iteraciones y ejecución de condicionantes. Permite el uso de estructuras de datos complejas más allá de las entradas y salidas que poseen los autómatas. Usa un fuerte tipado de datos, lo que implica detectar errores en la implementación. En el caso del ejemplo no podríamos comparar con 100 la variable NIVEL si esta fuera un BOOL.

-Lenguaje IL Instruction List. (**AWL** *Anweisungsliste* en Siemens).

Es un lenguaje muy parecido al ensamblador, con instrucciones minimalistas. Todo está basado en el uso de registros y realización de operaciones de comparación, aritméticas y lógicas (ver ilustración 7)

```
LD    NIVEL
GT    240
R     BOMBA

LD    NIVEL
LT    100
S     BOMBA
```

Ilustración 7 : Código en Lenguaje IL.

-Lenguaje LD Ladder. (**KOP** *Kontaktplan* en Siemens).

Es un lenguaje de programación muy parecido a la lógica cableada usada en sistemas de control antes de la aparición de PLC. La particularidad de este lenguaje es que la conexión de los elementos se hace de forma similar a como se cablean los elementos en un cuadro eléctrico (ver ilustración 8).

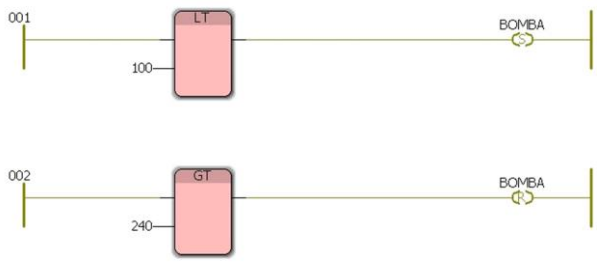


Ilustración 8 : Programación en lenguaje LD.

Para secuencias y maniobras sencillas es rápido, intuitivo y potente. Pese a que hoy en día se pueden integrar los diagramas de contactos con bloques más potentes de función, en el momento que se complica el algoritmo es más dificultoso de implementar que con otros lenguajes. La principal ventaja es la similitud con los esquemas eléctricos, lo que facilita mucho el trabajo de programación para ingenieros o técnicos eléctricos.

-Lenguaje FBD Function Block Diagram. (FUP *Funktionsplan en Siemens).*

Es muy parecido a la programación LD. La mayor diferencia con éste es que no es necesario crear malla a derecha e izquierda de los contactos, que simulan positivo y negativo de un esquema eléctrico (ver ilustración 9).

Protección en infraestructuras críticas. Análisis de seguridad en los sistemas de control industrial.

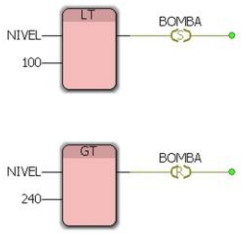


Ilustración 9 : Programación en lenguaje FBD.

-Lenguaje SFC (Sequential Function Chart).

Es el más parecido a una máquina de estados. La programación se divide en Transiciones y Acciones. Una transición es una condición que se debe cumplir para pasar al siguiente estado. Y una Acción es una modificación de una variable (ver ilustración 10).

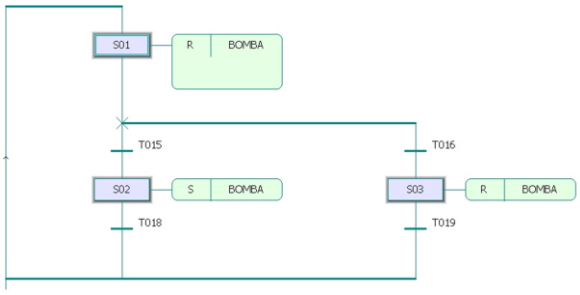


Ilustración 10 : Programación en lenguaje SFC.

2.4. Capa 3. Operación y Supervisión.

De alguna forma el PLC recoge señales del mundo real y de acuerdo a estas señales actúa. Por otro lado el operador del sistema debe poder interactuar con el sistema, bien sea eligiendo qué secuencia se ejecuta de forma automática, ajustando una receta o parámetros de un proceso. Para esta interacción hay diversos elementos, que se describen a continuación.

2.4.1. HMI (Human Machine Interface).

Son pantallas táctiles que permiten capacidad de control, activación y desactivación de secuencias y procesos. Hasta hace unos años en esta catalogación solo estaban las pantallas táctiles, que ofrecían a pie de máquina o planta una posibilidad de ajuste de parámetros en campo, más cerca del proceso.

Hoy en día, gracias a la industria conectada, podríamos catalogar como HMI pantallas táctiles, clientes de SCADA con funciones reducidas, terminales portátiles de campo (Mobile Panels), PC industrial

táctil o con teclado integrado. El objetivo básico de todos ellos es el mismo: transmitir órdenes a un proceso y recibir información básica del estado del mismo (ver ilustración 11).

Ilustración 11 : Ejemplo de un HMI. Pantalla táctil de 6,5"

2.4.2. Scada (Supervision Control And Data Adquisition).

Es un entorno amigable que permite realizar todas las operaciones en un SCI, aunque con el tiempo han ido implementando cada vez más funciones, dependerá un poco de la arquitectura del sistema. Por ejemplo sistemas pequeños disponen de SCADA Stand-Alone (Dispositivo único), en los que elementos de capas superiores como HISTORIAN o BATCH están integrados en el mismo SCADA. Desde este SCADA se extraen informes para la gestión de la empresa.

Los SCADA han ido evolucionando con el resto de sistemas de control desde sistemas monolíticos a sistemas en múltiples ordenadores. La decisión de uso se correspondería más a la complejidad del proyecto que a una evolución temporal, Podemos diferenciar 4 tipos:

- Stand Alone (Dispositivo Único), también conocidos como SCADA monolítico. Son sistemas SCADA de complejidad baja en los que existe un único cliente, sin capacidad de redundancia y con las comunicaciones básicas. Generalmente recogen un nivel de información muy bajo. Todo lo que se tiene que integrar está en el mismo equipo. Las comunicaciones están centralizadas en este equipo. Puede usar protocolos propietarios.
- Distribuidos: Existen múltiples estaciones repartidas, lo que permite diferentes posibilidades como separar el SCADA en diferentes equipos, separar cliente SCADA y servidor SCADA o incluso disponer de múltiples clientes en diferentes ubicaciones y un único servidor o servidores redundantes. Es el primer tipo de SCADA donde se empezaron a usar y desarrollar las comunicaciones LAN.
- Networked (En red): Muy parecidos a los anteriores. Se intenta mediante comunicaciones mejorar la integración con los diferentes equipos o servicios, incluso elementos que geográficamente están distribuidos mediante redes. Se pueden separar también las diferentes partes del SCADA en diferentes equipos dispuestos en red. Permite múltiples arquitecturas, como en el caso anterior.

- Web-based (Basados en red): Integración de los SCADA con la web. Permite un acceso deslocalizado basado en clientes web, la conversión de los sistemas SCADA a páginas web y el acceso desde cualquier dispositivo móvil, tablet, teléfono u ordenador portátil. Se simplifica el lado del cliente remoto. En estos sistemas se empiezan a integrar mecanismos de seguridad más sofisticados, ya que el acceso muchas veces es desde ubicaciones externas.

Pese a ser los más antiguos en aparición, en muchas instalaciones se siguen usando SCADA monolíticos, o evolución de HMI, capaces de integrar muchos de los elementos de un SCADA. Esto supone una reducción de costes, puesto que estamos hablando de sistemas que gestionan un número muy reducido de variables y elementos.

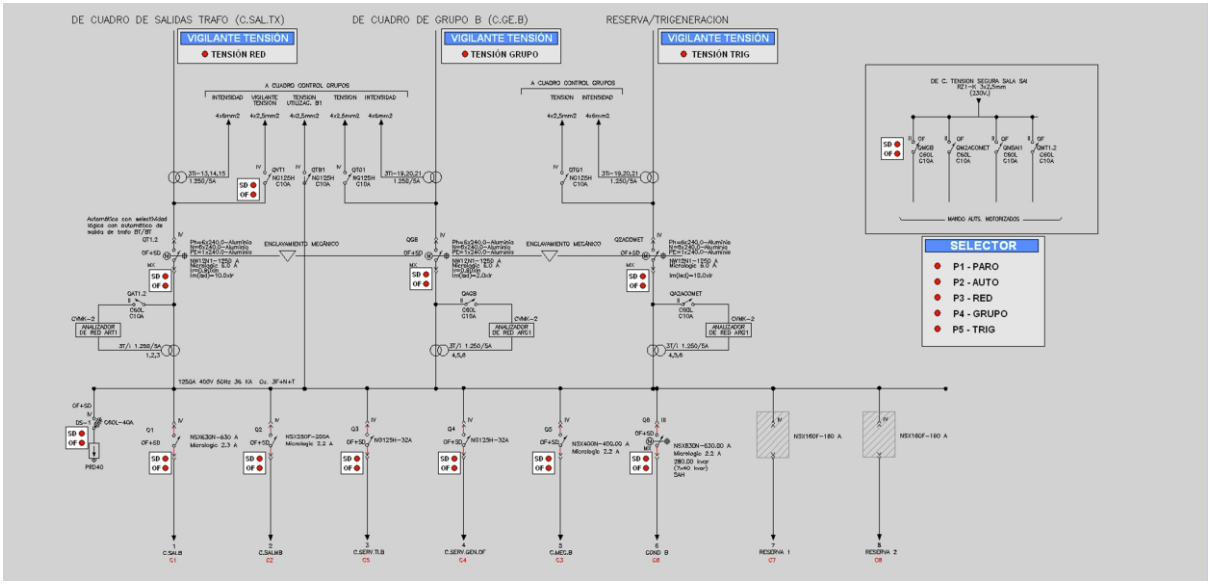
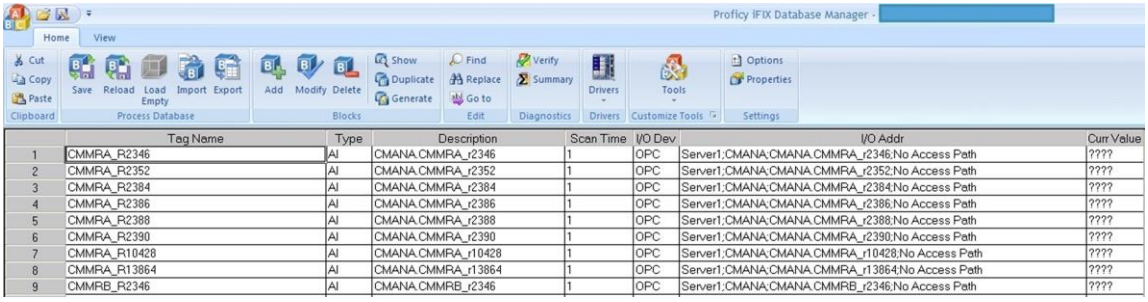


Ilustración 12 : Ejemplo SCADA.

Un sistema SCADA se compone en la mayoría de los casos de estos 4 elementos básicos:

- Servidor de E/S. Aquí se definen las variables que usamos en nuestro SCADA, ya sea como un valor a visualizar, como estado que leer o como SP que enviar al proceso. Todos los parámetros que se quieren visualizar o enviar al PLC deben estar aquí. Se deben tener en cuenta los tipos de datos que cambian de un SCADA a otro los tipos más comunes son BOOL, INT, REAL, etc. Se debe definir de que equipo se lee y que método se usa en la comunicación. Generalmente una dirección y un protocolo. Es un proceso que va haciendo lecturas y escrituras de valores continuamente. En la siguiente ilustración se pueden ver la configuración de un servidor de e/s donde se declaran las variables “Tag Name”, el tipo “AI” (Analog Input), cada cuanto se escanean “Scan Time”, el dispositivo “IO Dev” y la dirección “I/O Addr”. Es un servidor E/S del SCADA de GE Ifix (ver ilustración 13).



	Tag Name	Type	Description	Scan Time	I/O Dev	I/O Addr	Curr Value
1	CMMRA_R2346	AI	CMANA.CMMRA_r2346	1	OPC	Server1;CMANA;CMANA.CMMRA_r2346;No Access Path	????
2	CMMRA_R2352	AI	CMANA.CMMRA_r2352	1	OPC	Server1;CMANA;CMANA.CMMRA_r2352;No Access Path	????
3	CMMRA_R2384	AI	CMANA.CMMRA_r2384	1	OPC	Server1;CMANA;CMANA.CMMRA_r2384;No Access Path	????
4	CMMRA_R2386	AI	CMANA.CMMRA_r2386	1	OPC	Server1;CMANA;CMANA.CMMRA_r2386;No Access Path	????
5	CMMRA_R2388	AI	CMANA.CMMRA_r2388	1	OPC	Server1;CMANA;CMANA.CMMRA_r2388;No Access Path	????
6	CMMRA_R2390	AI	CMANA.CMMRA_r2390	1	OPC	Server1;CMANA;CMANA.CMMRA_r2390;No Access Path	????
7	CMMRA_R10428	AI	CMANA.CMMRA_r10428	1	OPC	Server1;CMANA;CMANA.CMMRA_r10428;No Access Path	????
8	CMMRA_R13864	AI	CMANA.CMMRA_r13864	1	OPC	Server1;CMANA;CMANA.CMMRA_r13864;No Access Path	????
9	CMMRB_R2346	AI	CMANA.CMMRB_r2346	1	OPC	Server1;CMANA;CMANA.CMMRB_r2346;No Access Path	????

Ilustración 13 : Servidor E/S.

- Servidor de Alarmas. Una vez definidas las variables, se definen qué parámetros son críticos y, en caso de que este parámetro exceda de unos límites, mostrar una alarma. Estas alarmas se muestran en el “alarmero”: zona de la pantalla que continuamente muestra los avisos que durante la operación van apareciendo. Además, es posible configurar alarmas sonoras o señalización visual sobre el elemento que está fuera de rango. Toda la información que proporciona el alarmero es importante a la hora de identificar qué ha pasado. En la ilustración 14 se muestra una imagen de un alarmero del SCADA de GE Ifix.

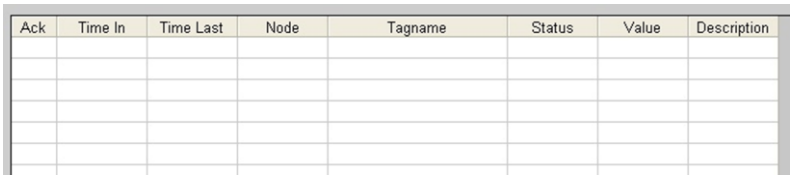


Ilustración 14 : Gestor Alarmas.

- Pantallas. Es un interface gráfico amigable y usable para el usuario donde aparece la información. Para ello se suele dibujar usando símbolos las diferentes partes del SCADA y mediante botones facilitamos la navegación por el entorno gráfico (ver ilustración 15).

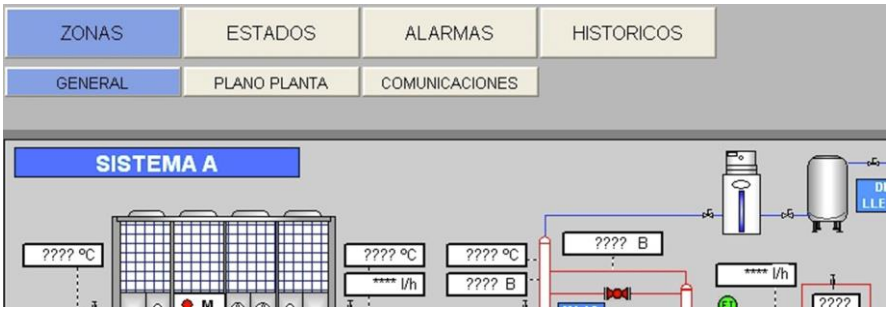


Ilustración 15 : Control de navegación.

- Servidor de Seguridad: Se gestiona qué privilegios tiene cada usuario y a qué pantallas puede acceder o no. Incluso qué consignas de proceso puede cambiar o no. En general como mala

práctica profesional se crean pocos perfiles y con muchos privilegios para simplificar el desarrollo general del SCADA.

2.5. Capa 4. Manufactura.

2.5.1. MES.

El MES (Manufacturing Execution System), es un sistema que mejora la trazabilidad al proporcionar información de materias primas y productos terminados. En el MES se almacenan datos de la producción como el consumo de una materia prima, el personal de producción, etc. Al tener integrada toda esta información ayuda a tomar decisiones que permiten mejorar y optimizar la producción de una planta. Ayuda en la planificación de producción facilitando detectar cuellos de botella en procesos productivos, analizar tiempos de paradas por cambios de producto, etc.

Opera en múltiples áreas de un proceso productivo entre ellas:

- Programación de recursos.
- Ejecución y envió de pedidos.
- Análisis de la producción.
- Administración de tiempos para mejorar la efectividad.
- Calidad de un producto.
- Seguimiento de materiales.
- Ciclo de vida de un producto.

Para todo ello recoge información de los procesos productivos.

2.5.2. BATCH.

El BATCH hace referencia al trabajo por lotes, es decir, responde a la necesidad de una industria de atender a un proceso en el que influyen múltiples partes de la planta. Por ejemplo, en la industria química el BATCH está muy asociado a las “recetas” de producción. Son procesos en los que se determina como se fabricara un producto, el proceso se realizara en diferentes partes de la planta o plantas, que posteriormente se unen, ensamblan o mezclan para formar el producto final.

La ventaja del trabajo por lotes es que una vez ajustada esa receta, el proceso es fácilmente repetible para la creación de productos iguales.

Protección en infraestructuras críticas. Análisis de seguridad en los sistemas de control industrial.

2.5.3. Historian.

Los historian o historiadores se encargan de almacenar los datos que van tomando las magnitudes físicas durante el proceso. Para ello en el diseño de un SCI se decide qué valores que se denominaran PV (Process Value) se tienen que almacenar, cada cuanto tiempo se tomara una muestra (tiempo de muestreo), si se tomara conjuntamente o desplazada respecto a otras señales (offset).

Los primeros historian estaban basados en ficheros de texto plano y cada muestra de un parámetro se almacenaba en una línea contigua en el tiempo. En la actualidad los historian usan bases de datos para agilizar cualquier tipo de consulta, con mayor potencia que permite consultas en múltiples tablas y con múltiples parámetros en busca de correlaciones. Es una forma de registrar todos los parámetros de un proceso productivo. La tendencia es el uso de Historian en la nube.

2.6. Capa 5. Administración.

2.6.1. ERP

Los denominados Enterprise Resource Planning (Planificadores de recursos empresariales).Este software se encargan de la gestión de una gran cantidad de procesos dentro de una empresa, como pueden ser:

- Gestión de proveedores.
- Ciclo de vida de un proyecto.
- Gestión del departamento de RRHH.
- Gestión del departamento Financiero.
- Gestión de manufactura o producción.
- Gestión de almacenamiento y logística.

Es un sistema modular, de modo que cada empresa usa los módulos que necesita para automatizar lo más posible sus procesos. Una opción es el uso de ERP SaaS (Software As Service), es decir ERP ubicados en la nube en donde se alquila el software según el uso, módulos instalados, etc.

De cara a la ciberseguridad, en un sistema ERP se encuentra mucha información de la empresa y además de sectores muy críticos como el financiero, de ahí el interés por parte de los ciberdelincuentes en los datos contenidos en esos sistemas. Los ERM forman parte de las TI mucho más que de las TO.

2.6.2. CRM

La herramienta CRM (Customer relationship management) o gestión de relación con los clientes, es un enfoque orientado a gestionar todas las relaciones con los clientes y potenciales clientes. Puede contener las siguientes funcionalidades.

- Automatización de promoción y ventas.
- Almacenamiento de información transaccional.
- Análisis de claves de negocio.
- Seguimientos de campañas de marketing y gestión de oportunidades de negocio.
- Capacidad predictivas y proyección de ventas.

Esta relación intenta conseguir una mejora en la relaciones comerciales basada en la retención de los clientes actuales, intentando obtener un impuso de las ventas hacia los clientes.

El CRM puede ser parte integral del ERP para obtener información completa, desde la venta, hasta con qué recursos se ha fabricado. Como el caso anterior es un sistema basado en las TI, aunque tiene o puede tener como fuente de información las TO. En relación a la ciberseguridad, se repite el caso del ERP: en los sistemas CRM se incluye información importante susceptible de ser robada.

2.7. Comunicaciones industriales.

Los protocolos de comunicación industrial han estado desde el principio de los SCI. El problema de que estos protocolos lleven tanto tiempo en el sector de los SCI es su diseño. Su diseño inicial iba orientado a la principal característica de las comunicaciones que gestionaban CPU, que implicaba una capacidad de proceso limitada, por lo que se primó la sencillez ante la seguridad. Es cierto que hace muchos años nadie temía por un SCI puesto que eran sistemas totalmente aislados sin ninguna conexión con el exterior y cualquier tipo de información que se tuviera que extraer se obtenía mediante informes o se consultaba directamente en el ordenador que hacía de SCADA.

Por ese motivo muchos de los protocolos que se presentan a continuación carecen de seguridad, siendo su prioridad el envío de la forma más ágil de tramas para su lectura. En la mayoría de estos protocolos mediante un splitter (derivador), es posible ver los mensajes que se intercambian los equipos sin ningún tipo de impedimento.

2.7.1. Modbus.

Es uno de los protocolos de comunicación más antiguos que se usan en la actualidad en SCI, diseñado para favorecer la comunicación entre PLCs, periferias y actuadores. Fue creado en 1979 por la

empresa Modicon (lo que actualmente se conoce como Schneider-Electric). Es uno de los protocolos más usados en el mundo debido a su facilidad de integración.

En la actualidad hay tres implementaciones: Protocolo Serial, TCP/IP y UDP. Su forma de comunicación está basada en la generación por parte del maestro de peticiones, pasando a esperar una respuesta. Siempre el maestro es el que inicia las comunicaciones. Normalmente este maestro es un SCADA, autómata principal o HMI. Y los esclavos sensores, controladores menores o accionadores (Variadores de Frecuencia).

El protocolo original usa comunicación serie y no estaba dividido en capas. La variante Modbus TCP usa datagramas TCP o UDP y usa separación de capas. El puerto por defecto del protocolo Modbus TCP es el 502.

El modelo de datos es el siguiente:

	Tipo Dato	Acceso Maestro	Acceso Esclavo	Dirección Asociada.	Ejemplos Registro 1.
Bobina	Bool	Lectura/Escritura	Lectura/Escritura	0XXX 0XXXX 0XXXXX	0001 00001 000001
Entrada Discreta	Bool	Solo Lectura	Lectura/Escritura	1XXX 1XXXX 1XXXXX	1001 10001 1000001
Registro de Retención	Palabra sin signo	Lectura/Escritura	Lectura/Escritura	4XXX 4XXXX 4XXXXX	4001 40001 400001
Registro de Entrada.	Palabra sin singo	Solo Lectura	Lectura/Escritura	3XXX 3XXXX 3XXXXX	3001 30001 300001

Una vez expuestos estos datos, cada sistema tiene múltiples configuraciones posibles, 4,5 o 6 dígitos. Alternancias en el orden que se envían los bytes de cada tipos 4-3-2-1, 3-4-1-2, etc. Cada dispositivo usa su propia configuración.

Las tramas usadas son:

Para el modbus serie.

Address Field	Function Code	Data	CRC

Address Field – Dirección del esclavo.

Function Code – Que función se va a usar, lectura, escritura o múltiples registros.

Data – Los datos que se envían.

CRC – Comprobación de la adecuación de lo enviado.

Para el modbus TCP.

Paquete de capa aplicación (4)

MBAP	Function Code	Data

En la capa transporte (3) se añade la cabecera TCP. *TCP Header.*

En la capa Internet (2) se añade la cabecera IP. *IP Header.*

En la capa red (1) se añade la cabecera Ethernet. *Ethernet Header.*

Seguridad:

Este protocolo generalmente no ofrece ninguna seguridad contra órdenes no autorizadas o contra pinchazos en el cable. Un splitter ubicado entre el maestro y la red de esclavos vería todos los valores y ordenes que se enviaran.

El diseño de modbus (aún en la versión TCP), se ideó para entornos controlados, con lo que no hay ningún mecanismo de seguridad: no hay autenticación ni permite cifrado.

2.7.2. Profibus

Estándar de comunicación serie sobre cableado RS-485, MBP (Manchester coding and Bus Powering) o fibra óptica. Desarrollado en 1989 por el departamento alemán de educación e investigación, usado principalmente por fabricantes alemanes como Siemens o Phoenix Contact. Es un protocolo que no tiene un único fabricante y está certificado. Es abierto en el sentido de que cualquier fabricante que se adapte a sus especificaciones puede usarlo. Se basa en una red con maestro/esclavo aplicando un token ring (paso de testigo en anillo), aunque su conexión física sea de bus.

Requiere terminado de bus, resistencias que se colocan al final del bus y que evitan que las señales reboten o vuelvan a ser recibidas y leídas por una estación. Generalmente esta terminación está incluida en el conector profibus. (Ver ilustración 16).

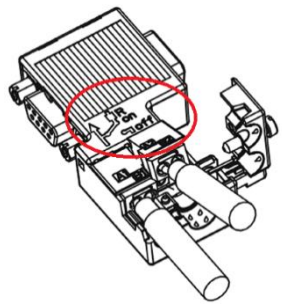


Ilustración 16 : Resistencia terminación bus.

Profibus usa 3 capas del modelo OSI.
Capa 7: Aplicación usando FMS,DP-V0,DP-V1 y DP-V2.
Capa 2: Enlace usando FDL
Capa 1: Física usando comunicación por RS-485, Fibra óptica o MBP.
Existen 3 variantes:

- Profibus DP (Decentralized Periphery - Periferia Descentralizada) en la operación de actuadores como control descentralizado. Es plug&play y económico.
- Profibus PA (Process Automation - Automatización de Procesos) generalmente usada en la lectura de medidas en sistemas de control de proceso. Dispone de Seguridad intrínseca y opcionalmente la alimentación por bus.
- Profibus FMS (Fieldbus Message Specification – Especificación mensajes bus de campo): Automatización de propósito general. Permite la comunicación multimaestro en gran variedad de aplicaciones.

Además existen tres versiones.
DP-V0: Funcionalidades básicas, transferencia cíclica de datos, diagnostico de estaciones, módulos y canales. Soporte para interrupciones.
DP-V1: Transferencia cíclica de datos. Esta transferencia está orientada a parámetros de operación y visualización.
DP-V2: Comunicación entre esclavos.
Las arquitecturas permitidas son monomaestro y multimaestro

Seguridad.
En este protocolo no existe autenticación y ni cifrado de los mensajes. No tiene ninguna seguridad.

2.7.3. Profinet.

Es un estándar basado en profibus, pero usando como medio de transmisión cable Ethernet. El sistema de transmisión es el paso de testigo (token). La transmisión es funcionalidad completa en TCP/IP.

Existen varios protocolo profinet dependiendo del uso:

- Profinet/CBA: (Component Based Automation) Asociado a aplicaciones de automatización distribuida.
- Profinet/DCP: (Discover and Configuration Protocol) Descubrimiento y configuración básica. Usado en aplicaciones medianas y pequeñas que no existe DHCP.
- Profinet/IO: (Input Output) también conocido como Profinet-RT (RealTime) utilizado en comunicación con periferias descentralizadas.

- Profinet/MRP: (Media Redundancy Protocol) Protocolo de Redundancia de medios. Usado en la reestructuración de redes en caso de un fallo de red en topología de anillo.
- Profinet/MRRT: (Media Redundancy for RealTime) Soluciones para la redundancia de medios en profinet/RT.
- Profinet/PTCP: (Precision Time Control Protocol) Basado en capa enlace, sincroniza señales de reloj y tiempo entre varios PLC.
- Profinet/RT: (Real Time) Para la transferencia de datos en Tiempo real.
- Profinet/IRT: (Isochronous Real Time) Transferencia en tiempo real de forma isócrona.

Seguridad.

Este protocolo carece de funciones de seguridad propias, no existe ningún tipo de autenticación o cifrado de comunicaciones. Sus características están orientadas a la fiabilidad y disponibilidad, no a la seguridad. Al ser un protocolo que usa Ethernet, aumenta su exposición a amenazas. Además, cualquier dispositivo Profinet, a parte de la respuesta a mensajes de Profinet, también responde a otros protocolos como ARP, LLDP o SNMP.

2.7.4. OPC

(OLE Process Control) es un mecanismo que permite la interconexión entre diferentes fabricantes. Basado en la arquitectura cliente-servidor. El cliente periódicamente solicita una información y el servidor responde.

Es una implementación que permite usar protocolos de comunicación de los sistemas de control, dentro de las tecnologías Microsoft. Según la tecnología que se usa se puede denominar OPC Clásico, (basado en tecnologías COM de Microsoft), o OPC-Xi (eXpress Interface) basado en tecnologías .NET de Microsoft. Esta tecnología usa casi siempre el protocolo TCP/IP.

Un cliente OPC de un SCADA o de un DCS se puede comunicar con uno o varios servidores OPC. De esta forma se obtiene acceso a datos de diferentes fabricantes desde la misma interface. Según el servicio que presten podemos tener varios tipos diferentes:

- OPC-DA (Servidor de Acceso a Datos): El servidor mantiene todos los datos unificados dentro de un grupo.
- OPC-AE (Servidor de Alarmas, Condiciones y Eventos): Provee de la interface para que los clientes OPC sean notificados de sucesos como alarmas o eventos.
- OPC-HDA (Servidor de Acceso a Datos Históricos): Se facilita el acceso a datos. Es una arquitectura abierta y eficaz que se concentra en el acceso y no en el tipado. Favorece la creación de aplicaciones que usen estos datos, y se integra con aplicaciones de terceros tipo Office.

- OPC-DX (OPC de intercambio de datos). Permite a servidores OPC-DA intercambiar datos sin necesidad de clientes, comunicaciones server-to-server. No requiere un cliente.
- OPC XML DA (OPC de Acceso de Datos XML). Método de intercambio usado en aplicaciones de empresa, ofrece la interface SOAP (Simple Object Application Protocol) para objetos OPC DA 2.0/3.0. Permite aplicaciones clientes en múltiples lenguajes de programación java,pert,python,etc. Es una plataforma más estándar que las tecnologías DCOM de Microsoft, sin embargo no puede considerarse en tiempo real.
- OPC UA (OPC de Arquitectura Unificada). Basado en las tecnologías .NET de Microsoft, una versión más moderna que soporta el transporte mediante SOAP y HTTP.

Seguridad.

Debido al enorme número de tecnologías de Microsoft diferentes que usa (RPC,DCOM,.NET y OLE) es susceptible a vulnerabilidades de cualquiera de estas tecnologías. El problema es que aunque existen parches para vulnerabilidades en estas tecnologías, algunos pueden no ser aplicables por la dificultad de aplicar parches al software usado en SCI.

Como recomendación usar (siempre que se pueda elegir) OPC – UA basado en .NET

2.7.5. CIP (Common Industrial Protocol)

Protocolo creado para la automatización de procesos industriales, se integra con Ethernet y Internet. Cuenta con diferentes versiones que ofrecen diferentes integraciones, estas son:

- Ethernet/IP: Adaptación de CIP a TCP/IP.
- ControlNET: Integración CIP con tecnologías CTDMA (Concurrent Time Domain Multiple Access)
- DeviceNet: Adaptación CIP con CAN, Controller Area Network.
- CompoNet: Adaptación TDMA (Time División Multiple Access).

Es un modelo de comunicación basado en objetos, en los que cada objeto tiene propiedades o atributos (datos), interacciona mediante métodos (servicios o comandos), está conectado con el mundo real (conexiones o entradas y salida de datos) y se comporta de alguna manera. Los métodos hacen algo.

La idea de CIP es disponer de una gran variedad de objetos para cubrir casi todas las necesidades. Los objetos del mismo perfil se comunican de la misma manera. La comunicación CIP sigue un modelo productor-consumidor, basado en multicast, es decir, que el productor envía el mensaje y todos los consumidores lo reciben. Posteriormente son ellos los que determinan si el mensaje es para ellos y si es así lo procesan.

En caso de no ser para ellos el proceso se deja pasar. De ahí podemos clasificar los mensajes en dos categorías.

- Mensajes Implícitos. Disponen de un identificador, el consumidor determina si es para ello o no.

Identificador	Datos	CRC

- Mensajes Explícitos. Disponen de información de origen y destino, e información sobre una acción concreta.

Origen	Destino	Datos	CRC

Protocolo Ethernet/IP: es el más usado de los protocolos CIP. Tiene dos métodos para realizar su conexión mediante TCP/IP, una es mediante TCP para envió de mensajes explícitos, y UDP en el envío de mensajes implícitos.

Para el mensaje explícito se usa el protocolo TCP en el puerto 44818. Son los mensajes entre PLC, HMI, transferencia de ficheros o diagnóstico. Estos mensajes siguen el paradigma productor-consumidor.

Para el mensaje implícito se usa el protocolo UDP en el puerto 2222. Son los mensajes en tiempo real, por lo que se transmiten datos en multicast para mejorar la velocidad. Para múltiples entregas sólo se envía una vez el mensaje.

Seguridad por tipos de CIP.

DeviceNET	bus CAN	No dispone de ninguna medida de seguridad. Es posible la manipulación de dispositivos mediante objetos modificados.
ControlNET	coaxial RG-6	No dispone de ninguna medida de seguridad. Es posible la manipulación de dispositivos mediante objetos modificados.
CompoNET	cables redondos	No dispone de ninguna medida de seguridad. Es posible la manipulación de dispositivos mediante objetos modificados.
Ethernet/IP	UTP	Todas las vulnerabilidades de Ethernet, phishing, mitm, inyección de trafico malicioso en UDP

3. Infraestructuras críticas.

3.1. Qué es una infraestructura crítica.

El termino infraestructura crítica es referido por los Estados para definir aquellas instalaciones y sistemas esenciales para el funcionamiento de la Nación y para la que no hay un sistema alternativo. Son esenciales para la seguridad nacional o la economía de un país.

Estas infraestructuras críticas (en adelante IC) son clasificadas por sectores estratégicos. Estos son tan variados como: defensa, energía, aeroespacial, nuclear, administración o financiero.

La protección de estas IC surge como necesidad a proteger este complejo sistema que da soporte a un país y posibilita el buen funcionamiento en general de los sectores productivos y del bienestar de la sociedad. Esta creciente amenaza surge con fuerza en los últimos años debido a la gran repercusión que diversos incidentes han tenido sobre estos sistemas críticos. Detrás de estos incidentes pueden encontrase desde otros países a terroristas, pero el objetivo suele ser el mismo: debilitar un país.

3.2. IC en España.

En España la Ley 8/2011 del 28 de abril de título “Medidas para la protección de infraestructuras críticas” se encarga de establecer las medidas de protección. Asociado a esto mediante el Real Decreto 704/2011 del 20 de Mayo, de título “Reglamento de protección de las infraestructuras críticas” se desarrolla su reglamento. Esta Ley define qué sectores son necesarios para el mantenimiento de los servicios básicos de una sociedad como pueden ser seguridad, salud, bienestar y el normal funcionamiento de las estructuras del Estado. En España el conjunto de IC está dividido en 12 sectores que se consideran estratégicos:

- Administración.
- Espacio.
- Industria Nuclear.
- Industria Química.
- Instalaciones de investigación.
- Agua.
- Energía.
- Salud.
- TI y las comunicaciones.
- Transporte.
- Alimentación.
- Sistema financiero y tributario.

Partiendo de estos 12 sectores se aplica una metodología “top-down” de arriba abajo. Para ello se elige un sector, y desde el nivel más alto se va desglosando en los elementos que facilitan la provisión de ese servicio. De cada uno de estos elementos vitales para la provisión del servicio se analiza que impacto tiene en el conjunto del sector si hubiera un fallo. Como criterios que se tienen en cuenta en la evaluación de un fallo de dicho elemento se pueden destacar:

- Número de vidas humanas que se ponen en riesgo.
- Impacto económico.
- Impacto en el servicio.

De acuerdo a los resultados obtenidos podemos catalogar en:

- Infraestructura Estratégica. Elemento sobre el que descansa el funcionamiento de un servicio esencial. Puede ser una instalación, una red, un sistema, un equipo físico, …,
- Infraestructura Esencial. El servicio que se vería afectado sobremanera si se produce un fallo de la Infraestructura Esencial.
- Infraestructuras Complementarias. Es una infraestructura estratégica que afecta levemente al conjunto del servicio.

Además en 2018 se desarrollaron varias iniciativas legales, bien desde instituciones Europeas o nacionales.

- **Estrategia de Ciberseguridad Nacional**, se empezó la actualización de la Estrategia de Ciberseguridad Nacional (la actual data del año 2013). Se publicó en 2019 en el BOE del 20 de Abril de 2019.
- Real Decreto-Ley 12/2018 de 7 de Setiembre sobre seguridad de las redes y sistemas de la información, en cumplimiento de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, con fecha 6 de Julio de 2016. Esta Ley establece al CCN-CERT como equipo de referencia de respuesta a incidentes dentro del sector público, y como coordinador superior en emergencias a nivel nacional que requieran de una respuesta técnica dada su gravedad.
- Resolución del 13 de Abril de 2018, de la Secretaria de Estado de Función Pública, para la aprobación de la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad, que establece los criterios para la notificación de incidentes de seguridad al CCN desde el sector público.

A nivel nacional el organigrama de las agencias que se encargan de los incidentes es el siguiente (ver ilustración 17):

Este modelo de gobernanza está recogido en el nuevo Real Decreto y queda sustentado por el esquema de competencias que se detalla a continuación.

- Consejo de Seguridad Nacional. Es el punto de contacto de España con el resto de la UE.

- Consejo Nacional de Ciberseguridad. Su función es apoyar al Consejo de Seguridad Nacional. Su presidencia la ostenta el director del CNI.
- Autoridades Competentes. Esta clasificación queda desglosada por sectores, según indica RD-Ley 12/2018 los tres ministerios como autoridades competentes son: Ministerio de Defensa, Ministerio de Interior y Ministerio de Economía y Empresa.
- CSIRT de referencia. Según sea el ámbito público, privado o militar se tiene un CSIRT de referencia, aunque trabajen en cooperación. Por ejemplo, las entidades públicas dependen del CCN-CERT, las entidades privadas del INCIBE-CERT y las autoridades militares del ESPCERTDEF. En los supuestos de máxima gravedad el CCN-CERT tiene la misión de coordinador a nivel nacional.

Ilustración 17 : Organigrama RD-Ley 12/2018

3.3. Ciberseguridad en IC.

La ciberseguridad industrial es un término que no se usa mucha pero que recoge unos criterios para la protección de IC. Las principales actividades de la ciberseguridad en IC son:

- Prevención de ataques.
- Monitorización de sistemas.
- Preparación de IC ante ataques.
- Gestión de las consecuencias.

De alguna forma el objetivo que busca perseguir la ciberseguridad en IC es proteger los procesos productivos.

Los principales errores que hacen que no se invierta en ciberseguridad son:

- Es una inversión que no repercute positivamente en el negocio.
- Implantación de medidas de seguridad limitadas que no integran el conjunto de elementos del sistema.

3.4. Incidencias en IC y SCI en 2018 en España. *(Fuente: Informe Anual Ciberamenazas y Tendencias. Edición 2019).*

Según el informe anual *Ciberamenazas y Tendecias. Edicion 2019,* el CCN-CERT gestionó más de 38000 incidentes, en el mismo periodo del año pasado se produjeron 26.472 incidentes lo que supone un incremento de casi el 47%. Esta cifra crece año tras año. Si bien es cierto de que solamente el 2,7% de estos incidentes tuvieron la consideración de “Crítica” o “Muy Alta”. Estas cifras suponen un total de unos 1000 incidentes en todo el año, casi tres incidentes al día.

Tabla 2 : Numero Incidentes/Año. Incremento Porcentual.

Año	Incidentes Totales	Incremento Incidentes	%
2012	4003	0	0,00
2013	7259	3256	81,34
2014	12916	5657	77,93
2015	18232	5316	41,16
2016	20807	2575	14,12
2017	26472	5665	27,23
2018	38029	11557	43,66

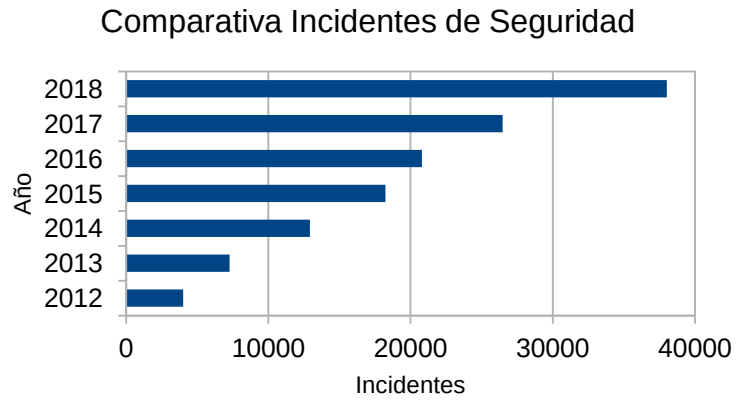


Ilustración 18 : Comparativa número de incidentes.

Como se ve en las gráficas de las páginas anteriores, el año que menos han subido los incidentes fue entre 2015 y 2016, en los que apenas se incrementó algo más de 10%. Como se observa en la Ilustración 19 hubo una serie de tendencias a la baja entre 2014 y 2016. Pero desde 2016 crece otra vez.

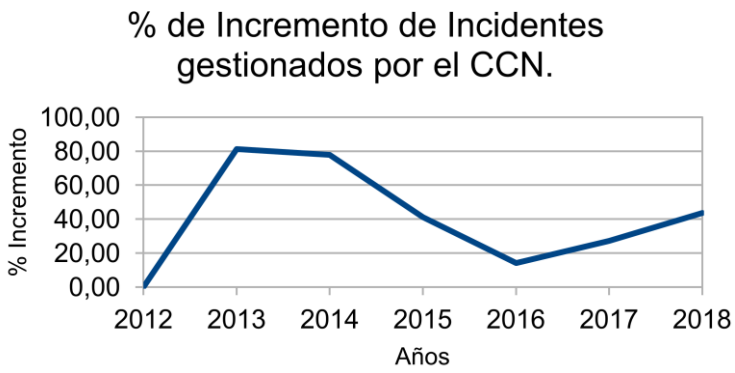


Ilustración 19 : Evolución número de incidentes.

La gravedad de los incidentes en 2018 se distribuye de la siguiente manera.

Tabla 3 : Distribución por gravedad.

Peligrosidad	% Incidentes
Bajo	6,92
Medio	29,46
Alto	60,88
Muy Alto	2,65
Crítico	0,09

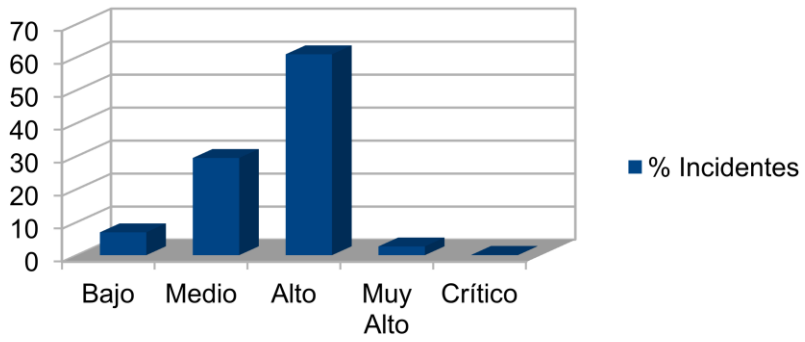


Ilustración 20 : Distribución por gravedad.

Protección en infraestructuras críticas. Análisis de seguridad en los sistemas de control industrial.

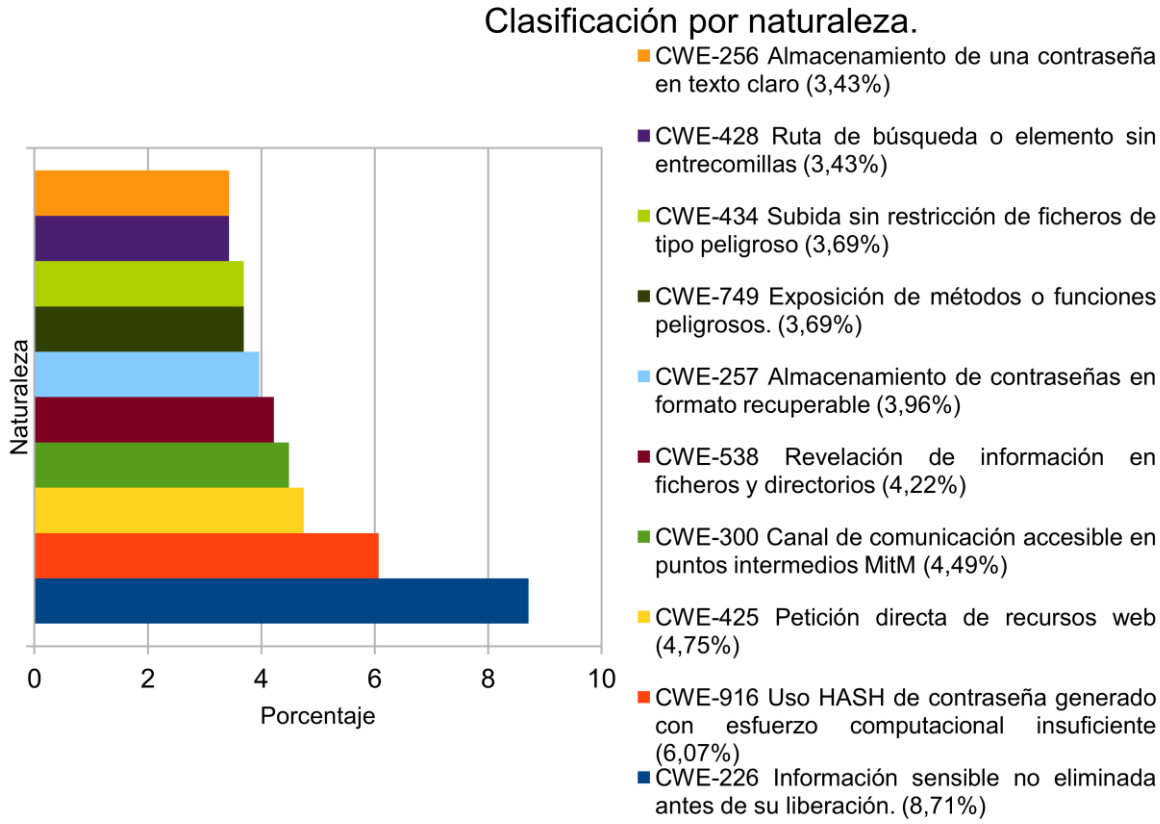
La tipología de los incidentes también la podemos calificar según el tipo de ataques. Aquí se hará referencia a los que más afectan a IC, que son: Código Dañino, Disponibilidad, Información comprometida, Recogida de información e intrusiones.

Estos datos exponen un análisis general de todos los sistemas. Se ha decidido comentarlos, debido a que muchos incidentes que puedan surgir en un entorno industrial, pueden comenzar desde un entorno más próximo a las TI que a las TO. Como el tema que nos ocupa son las IC y los SCI, usamos para concretar aún más los datos Incibe-Cert, analizando datos relacionados con la seguridad industrial. Los datos corresponden a 2018.

En 2018 se notificaron un total de 228 avisos, comparados con los 199 de 2017. Lo que supone un 14% más de avisos en comparación con 2018.

3.4.1. Vulnerabilidades más encontradas en SCI e IC según Incibe-Cert.

Cabe destacar en el grafico anterior que estas son las vulnerabilidades que en mayor porcentaje se han encontrado en los avisos. Si analizamos los datos, nos daremos cuenta de que no se corresponden a vulnerabilidades originadas por grandes ataques realizados por grupos de expertos. Por ejemplo, la vulnerabilidad más detectada 8,71% corresponde a “información sensible no eliminada de un dispositivo” o hay con más de un 3% dos vulnerabilidades referentes a “contraseñas en texto plano” o “contraseña almacenada en formato recuperable”.



En la clasificación de estas vulnerabilidades se ha usado el código CWE (Common Weakness Enumeration), es un catálogo de debilidades en el software que está dirigida a desarrolladores o profesionales de la seguridad. El objetivo es unificar la vulnerabilidad con arquitectura, diseño y código. Se suele ver como un catálogo de debilidades que se suelen cometer programando.

3.4.2. Incidencias por fabricantes. Top 10.

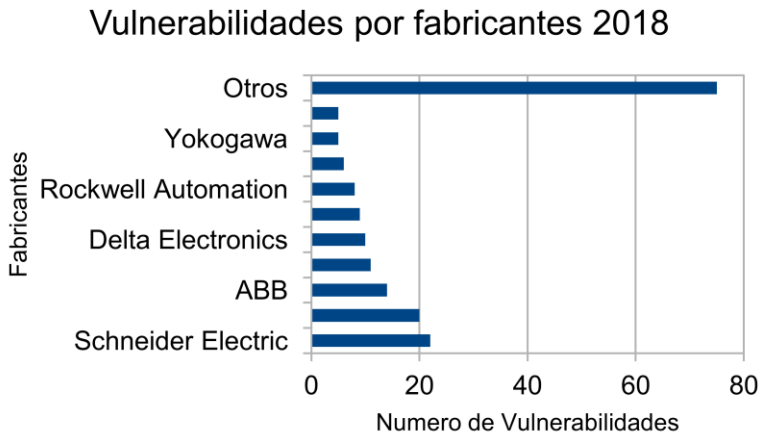


Ilustración 21 : Vulnerabilidades por fabricante.

Los fabricantes que aparecen en las 2 primeras posiciones repiten posición respecto a 2017. Si bien es cierto que el número de vulnerabilidades se ha reducido algo.

Como nota a tener en cuenta es importante mencionar que estos avisos en gran parte los proporciona el fabricante, en un esfuerzo por detectar vulnerabilidades de seguridad en sus equipos. Con lo cual, un fabricante que no aparece en la lista no quiere decir que no tenga vulnerabilidades. Cabe la posibilidad de que no se busquen estas debilidades o que una vez detectadas no se publiquen las vulnerabilidades.

Para establecer una comparación se muestran el Top 15 de empresas de automatización por facturación del mundo.

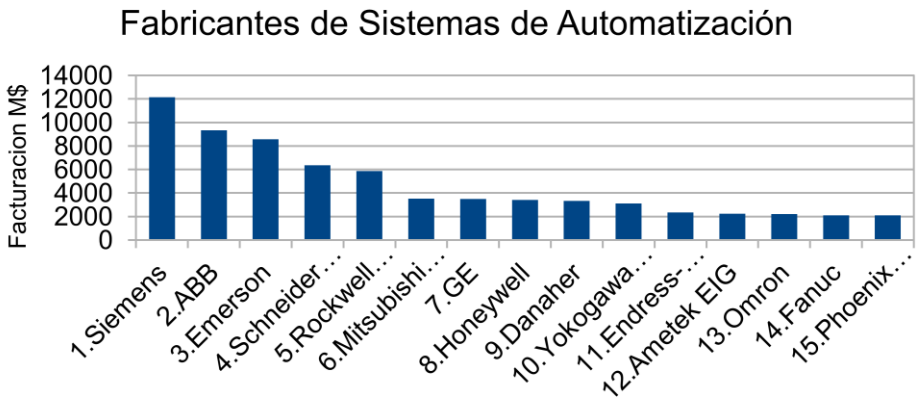


Ilustración 22 : TOP 15. Fabricantes de hardware automatización.

Llama la atención que grandes empresas de automatización que aparecen dentro de las 10 que facturan anualmente no tengan vulnerabilidades un poco más acorde al número de equipos que venden, lo que hace pensar que muchas empresas no investigan o documentan sus vulnerabilidades.

3.5. Incidencias IC y SCI en 2018 en el Mundo.

Según World Economic Forum (en adelante WEF) en 2018 los ciberataques son el quinto riesgo global que existe para personas, gobiernos y empresas. Teniendo en cuenta en esta clasificación cosas como el cambio climático, catástrofes naturales o armas de destrucción masiva.

En 2018 no se detectó ninguna nueva oleada de ramsonware que añadir al que actuó en 2017 como petya/not petya. Pese a todo existen en la actualidad 800 millones de códigos dañinos en cualquiera de sus variantes que pueden afectar a IC.

Protección en infraestructuras críticas. Análisis de seguridad en los sistemas de control industrial.

Según estimaciones de McAfee, los ciberdelitos suponen 600.000 Millones de dólares, o lo que es lo mismo, el 0,8% del PIB mundial.

Las IC en 2018 han recibido a nivel global los siguientes incidentes

Tabla 4 : Actores implicados.

Estados extranjeros o grupos de apoyo.	Delincuentes	Terroristas	Hacktivistas	Cibervandalos Script Kiddies	Insiders (Personal interno).
Sabotaje Interrupción de Servicios. Espionaje	Manipulación de sistemas Interrupción de servicios.	Sabotaje	Interrupción de servicios. Manipulación de información.	Interrupción de servicios. Robo de información.	Robo de información. Interrupción de servicios.

3.5.1. Actores implicados.

Estados Extranjeros o grupos de apoyo.

Los Estados Soberanos han pasado a ser una de las principales amenazas contra la ciberseguridad de IC, el objetivo que busca cualquier nación es la mejora de su posición estratégica, política o económica.

Muchas de las herramientas usadas para perpetrar estos ataques contra naciones extranjeras han pasado a formar parte de un arsenal. Al igual que en periodos anteriores formaban parte de estos arsenales aviones, carros de combate o cualquier tipo de arma.

Este tipo de armas en muchos casos tienen en objetivo de obtener información sobre el estado de la seguridad de una IC, con el objetivo de lanzar un posterior ataque. Se analizan el nivel de implantación de medidas de seguridad, actualizaciones de hardware y software, etc. Es el tipo de ataque que más se ha detectado en Europa, contra IC en territorio Europeo.

Delincuentes.

Los ciberdelincuentes generaron en 2018 más del 80% de actividad dañina, con un impacto del 0,85% de PIB mundial.

Protección en infraestructuras críticas. Análisis de seguridad en los sistemas de control industrial.

El método usado es el correo electrónico: se estima que el 60% de los correos que viajan por el ciberespacio contienen código dañino. Mediante este 60% consiguen ejecutar el 90% de los ataques.

Estos correos electrónicos en su mayoría persiguen recolectar información de sesiones mediante el phishing, es decir mediante la suplantación de identidad. Hacerse pasar por un banco, entidad o gobierno con el fin de obtener los usuarios y contraseñas de un determinado servicio con el objeto de explotarlo.

Ciberterroristas – Ciberyihadistas.

En 2018 la actividad de estos grupos ha sido baja. Se ha usado la red como medio de obtener financiación, de reclutamiento de efectivos y como forma de influencia en redes sociales.

Hacktivistas.

La actividad se ha mantenido en niveles comparables a años anteriores. Con ataque con el principal objetivo de obtener visibilidad en medios de comunicación. Basándose principalmente en ataques DDoS y desfiguración de páginas web. Su motivación no es económica.

Insiders.

En 2018 el 25% de los incidentes en una empresa estuvieron provocados por el personal interno. En este porcentaje se incluyen desde actos deliberados a negligencias. Es una de las amenazas más importantes que se está teniendo en cuenta en las organizaciones. Se puede buscar un beneficio económico, pero en la mayoría de los casos se debe más a un problema de negligencia o falta de formación por parte del personal.

3.5.2. Vectores de Ataque en 2018.

Los SCI han sido víctimas de ataques no dirigidos, siendo los principales elementos infectados los puestos de operador y algún componente del sistema de control. Como principales vectores de infección se encuentran los correos maliciosos, los dispositivos de almacenamiento extraíbles y sistemas de mantenimiento remoto configurados incorrectamente.

Vamos a comentar algunas de las maneras en que se consigue atacar a los sistemas.

- Ataque a la cadena de suministro: Consiste en manipular o secuestrar el instalable de aplicaciones de uso legítimo. Este método se ha llevado a cabo por ejemplo con el famoso programa “CCleaner” que fue atacado en su desarrollo, lo que permitió modificar el código para contener un troyano que se instalaba con el programa. Otra variante es el secuestro de actualizaciones o incluso controladores, que además permite que superen en el caso de los controladores de Windows el firmado de los mismos por parte de Microsoft.

- Correos electrónicos: El correo electrónico, como antes se ha mencionado, es uno de los elementos más usados como vector de ataque. Sus principales usos son la inyección de código dañino, mediante enlaces a sitios phishing para obtener todo tipo de datos de inicio de sesión, credenciales, etc. Es el método más usado en las fases iniciales de cualquier ataque.

- Exploits drive-by: Método que usa como infección el aprovechamiento de vulnerabilidades de los sistemas operativos o navegadores web. Este exploits es activado en el momento que se navega por el sitio malicioso o se abre la publicidad que contiene. En muchos casos no es necesaria la interacción del usuario.

- Exploits-kits: Fragmento de código o secuencia de comandos que explotan vulnerabilidades en un producto.

- Vulnerabilidades de RAT: Aprovechan vulnerabilidades en las herramientas de acceso remoto que se usan en infinidad de sistemas para tareas de mantenimiento, para poder acceder a un sistema.

- Contraseñas débiles: Aprovechamiento de contraseñas por defecto o débiles para realizar el ataque. En muchos casos no es necesario más que conocer la marca y modelo del equipo para localizar por Internet el manual de usuario, en el que aparecen las contraseñas por defecto. Otro aprovechamiento es la prueba de contraseñas débiles tipo admin/admin, root/root , etc.

- Spam: Se denomina Spam al envio masificado de correos electrónicos no solicitados. Podríamos distinguir entre el S*pam convencional,* que generalmente trata de anuncios de productos y el *Malware Spam*, usado de la misma manera pero con un contenido de código malicioso con la intención de infectar al destinatario.

- Phishing: Es una suplantación de identidad con la intención de hacer creer a la víctima que es otra persona la que solicita esa información y así obtener desde credenciales o datos de inicio de sesión. Se han hecho famosas las peticiones de las contraseñas. En los últimos años se ha desarrollado otra forma de Phishing, conocida popularmente como “La estafa del CEO”, en la que mediante una llamada telefónica del CEO de la empresa se solicitaba una transferencia bancaria u otro tipo de actuación. Queda demostrado que el phishing es la forma preferida de comprometer una organización. El 75% de los Estados Miembros de la UE revelaron casos de phishing. El 90% de infecciones con código dañino y 72% de violaciones de datos en organizaciones tuvieron como vector de ataque el phishing. Como dato se adjunta la siguiente figura (ver ilustración 24).

- Spear-Phishing: Es otra modificación del phishing, pero esta vez no se envía publicidad de ninguna entidad, sino que este correo va dirigido a personas, organizaciones o empresas concretas. Su objetivo es la infección o robo de datos con fines maliciosos. El siguiente paso, una vez recibido el correo, es intentar direccionar a un sitio donde infectar su equipo con malware.

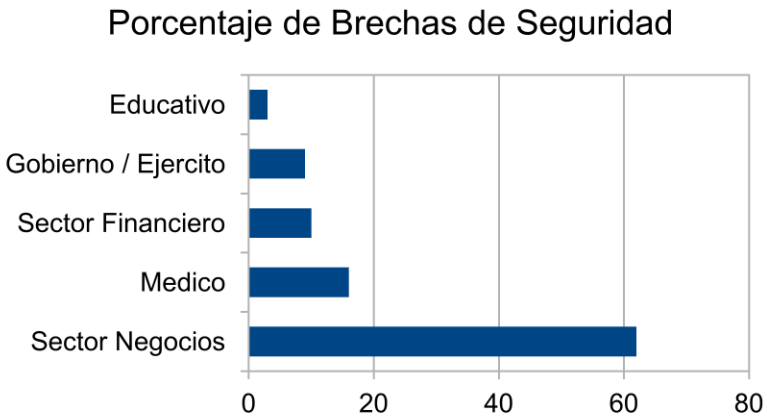


Ilustración 23 : Porcentaje de brechas de seguridad por sector.

- Sim Swapping: Una variante de phishing que consiste en atacar al doble factor de autenticación usado en transacciones bancarias, cuentas de correo electrónico, etc. Consiste en hacerse pasar por la víctima y conseguir un duplicado de su tarjeta SIM, lo que permite que los SMS del doble factor de autenticación sean accesibles para atacantes y permitan desde hacer transferencias bancarias, a cambio de contraseñas de cualquier cuenta.

Tanto por correo electrónico o mediante un fichero adjunto en un dispositivo de almacenamiento por USB, el objetivo último ha sido inyectar un malware, sea en forma de fichero MS Office en que se solicita encarecidamente activar las macros, o mediante otro tipo de fichero.

Los tipos de ataque realizados con este método independientemente del vector de ataque usado son:

- Ransonware: Es un tipo específico de código dañino que tiene por finalidad el bloqueo y cifrado de un ordenador con el fin de obligar a los usuarios a pagar un rescate por la recuperación de los datos. Destacan campañas que en 2017 causaron estragos como WannaCry o NotPetya/ExPetr.

- Código Dañino: Se entiende por código dañino cualquier programa que realiza funciones dañinas o malintencionadas. Entran en esta categoría: troyanos, virus, gusanos, spyware,etc.

Generalmente es una parte integral de cualquier ataque. Al conjunto de todos estos elementos se le puede clasificar como Malware.

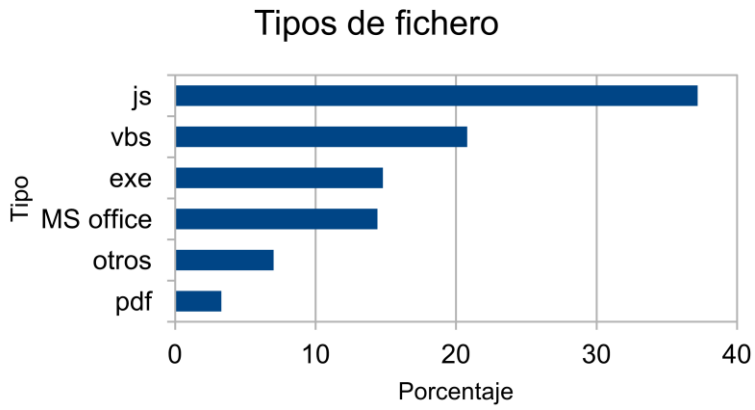


Ilustración 24 : Tipos de ficheros.

3.5.3. Tipologías de los ataques.

Las tipologías más usadas y que pueden afectar a IC son:

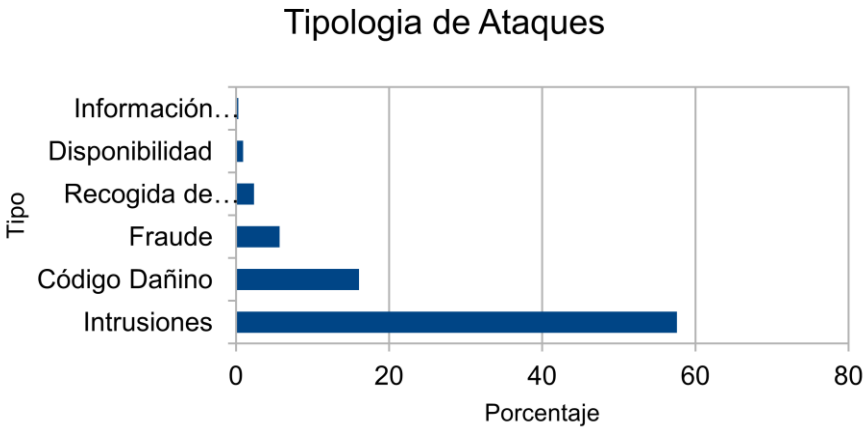


Ilustración 25 : Tipologías de ataque.

No se ha comentado el criptojacking pese a que pueden verse afectadas máquinas de IC. El principal objetivo de estos ataques es robar recursos de un sistema, básicamente capacidad de computación, para minar criptomonedas y obtener un beneficio económico, lo que implica, más que un ataque, la incapacidad de usar toda la potencia de la máquina.

3.5.4. Vulnerabilidades en 2018

El número de vulnerabilidades en software se ha incrementado en este año 2018. Vamos a analizarlas como parte fundamental de cualquier IC y SCI, los sistemas operativos y los navegadores web. En la Ilustración 27 vemos que los sistemas operativos tienen un número significativo de vulnerabilidades críticas.

VULNERABILIDADES SOFTWARE.

En el caso del Kernel de ***Linux*** casi 200, y los sistemas operativos ***Windows*** de Microsoft o ***Mac Os X*** de Apple aproximadamente unas 100 cada uno. Se refieren a vulnerabilidades críticas. Esto implica en muchos casos conseguir el control del equipo e incluso no requerir contacto físico para explotar la vulnerabilidad. Cabe exponer que el Kernel de Linux es el que se encuentra en los teléfonos con sistema operativo Android. En muchos casos las actualizaciones para solucionar estas vulnerabilidades no se ha desarrollado un parche o no se ha creado con la suficiente rapidez.

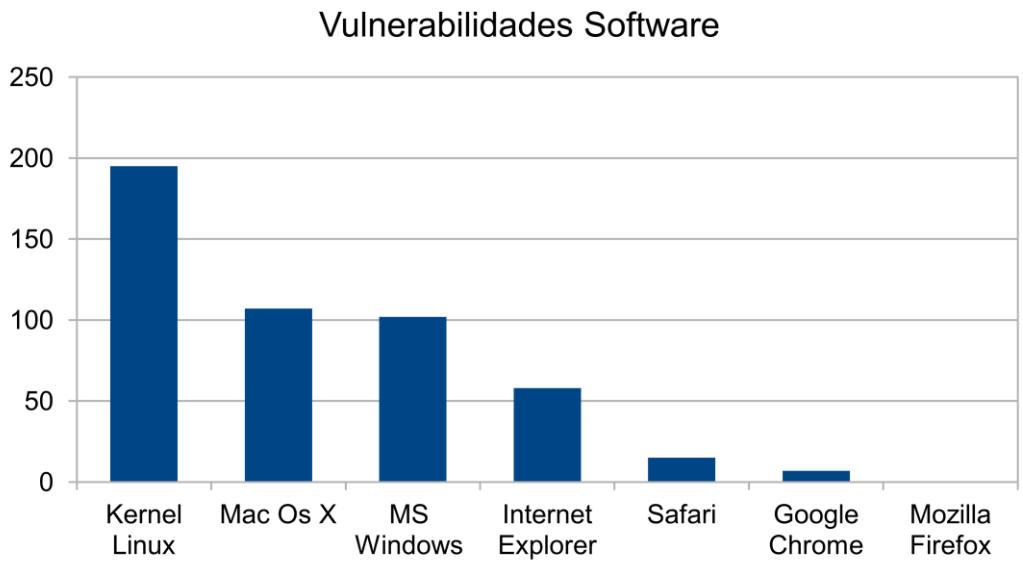


Ilustración 26 : Vulnerabilidades por software.

Cabe destacar el bajo número de vulnerabilidades de Google Chrome y Mozilla Firefox. Desde hace un par de años, ambas empresas no mantienen entradas en la base de datos MITRE de CVE, se referencian en sus publicaciones y no se describen las vulnerabilidades, así que no hay ninguna evaluación o puntuación base.

Vulnerabilidades en la implementación ***OpenPGP*** y *S/MIME*. Esta vulnerabilidad permite manipular correos electrónicos cifrados para que se reenvíen como texto plano, después de la recepción por

parte del destinatario. Muchos proveedores de correo electrónico han implantado medidas que evitan el aprovechamiento de esta vulnerabilidad.

Vulnerabilidad de ***Cisco Smart Install***, es una forma de configuración automática de switch de Cisco. El problema es que esta configuración automática no provee de ningún tipo de control de acceso, lo que ha permitido ataques en casi todo el mundo a equipos Cisco así configurados.

Vulnerabilidad ***Krack***, ciertas técnicas que hacían vulnerables a dispositivos WI-FI, que usaban el cifrado WPA y WPA2. Esta vulnerabilidad es difícil de usar de manera eficiente y requiere estar cerca de la víctima.

VULNERABILIDADES HARDWARE.

Además de las vulnerabilidades software, en 2018 se descubrieron vulnerabilidades en arquitecturas hardware, concretamente ***Meltdown*** y ***Spectre***. Es una vulnerabilidad que afecta a los fabricantes de arquitecturas x86 (Intel y AMD) y a la arquitectura ARM, más usada en smartphones y tablets.
Estas vulnerabilidades permiten leer áreas de memoria protegida, el fallo se viene arrastrando desde los años 90 por la incorporación de características que mejoraran el rendimiento de los procesadores. El problema de las vulnerabilidades hardware está en el parcheo, ya que supone la corrección un rediseño del procesador y en los equipos en funcionamiento un parche software que afecta al rendimiento. Además, en muchos casos, para analizar la seguridad de un software se dispone del código fuente, aunque en el caso de los microprocesadores la arquitectura es secreta y los fabricantes no comparten información sobre ella.

Vulnerabilidad ***AMDflaws*** compuesta por vulnerabilidades graves y 13 puertas traseras. Para poder explotar estas vulnerabilidades el sistema tiene que estar comprometido y haber alcanzado privilegios de administrador.

Vulnerabilidad ***Glitch***, es una nueva forma de perpetrar ataques, estos ataques se denominas ***Rowhammer***, es usar el procesador gráfico para cometer ataques.

3.6. Ataques en 2018.

Enero 2018 – Una brecha de seguridad de la Health South East RHF Noruega, la mayor autoridad noruega de salud, permitió el robo de los datos de salud de 2,9 Millones de Noruegos.

Febrero 2018 – El gobierno Alemán anuncio que había sido atacado e infectado durante aproximadamente un año. Se había atacado a las redes y servidores del Ministerio del Interior. El ataque se detectó en diciembre de ese mismo año.

Marzo 2018 - Ramsonware SamSam, vulnerabilidad a través de componentes de servidores web y aprovechamiento de contraseñas débiles, paralizo importantes servicios de la ciudad de Atlanta (Georgia).

Marzo 2018 – Ciberataques Carbanak-Cobalt contra el sector financiero. Se atacó mediante vulnerabilidades no parcheadas y en 2 semanas se alcanzó un control total del sistema. No se usó ninguna nueva herramienta. Se usaron herramientas de disponibilidad pública como Powershell y Cobalt Strike.

Abril 2018 – Ministerio de la Energía de Ucrania. La página web del ministerio de energía cayó y fue cifrado todo su contenido, parece ser una vulnerabilidad de Drupal 7.

Abril 2018 – El grupo Emissary Panda robaron 200Gb de información a empresas del sector aeroespacial. Para ello se aprovecharon de servidores abandonados y no actualizados en la zona DMZ. Tampoco se usó un nuevo malware. Se logró mediante Webshells (China Chopper).

Abril 2018 – Orangeworm, es una APT orientada al sector médico. Mediante el troyano Kwampirs se abrió en los ordenadores una puerta trasera que permitió robar información médica y confidencial. Afectó principalmente a los ordenadores que controlaban rayos X, resonancia magnética nuclear RMN y equipos donde los pacientes completaban los formularios de consentimientos informados. Se detectaron en sedes de Europa, Asia y Estados Unidos.

Noviembre 2018 – Ataque a aproximadamente 3000 víctimas relacionadas con el sector público. El responsable fue el grupo APT29, y para ello usó una funcionalidad del sistema operativo para instalar y ejecutar código dañino.

4. ANALISIS DE ATAQUES EN INFRAESTRUCTURAS CRÍTICAS.

Vamos a analizar los ataques a IC desde sus orígenes, el objetivo es analizar cuáles han sido las formas usadas con anterioridad que nos proporcionara una perspectiva importante, para en conjunto con la primera y segunda parte elaborar medidas para securización de SCI e IC.
Empecemos con una línea temporal de los ataques (ver ilustración 28).

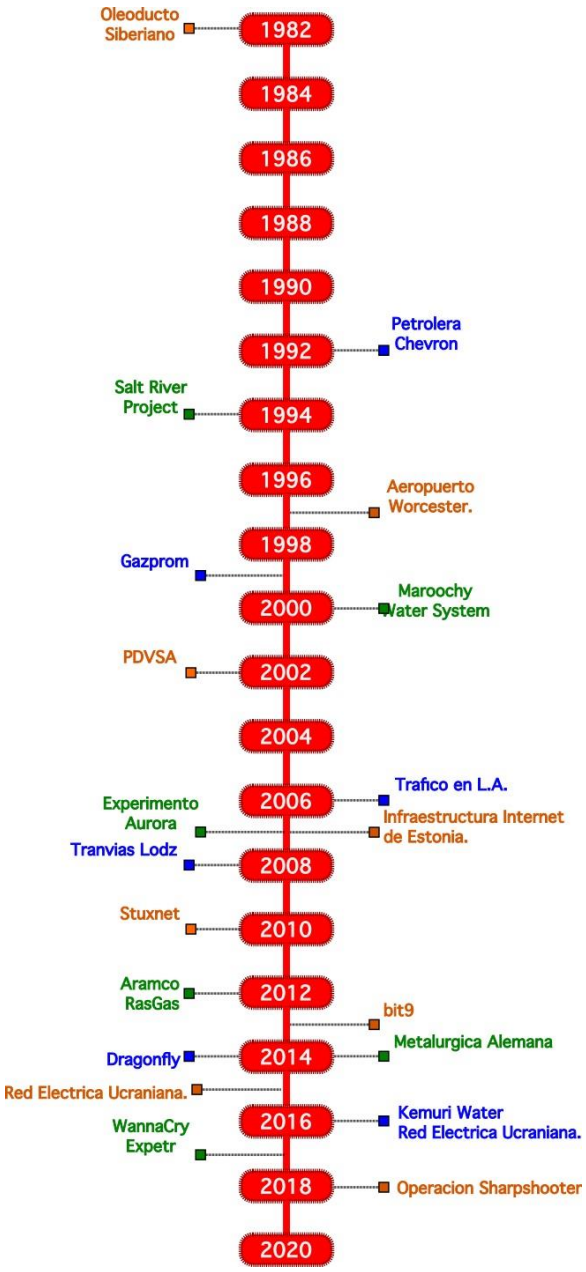


Ilustración 27 : Timeline Ataques a IC.

4.1. Ataque Oleoducto Siberiano (1982)

Todo comenzó en 1982 con el primer ataque a una infraestructura crítica. Estamos hablado de los años de la guerra fría. En esos años empezó una apertura comercial de Estados Unidos hacia la URSS. En aquel momento el gobierno soviético se interesó por la compra de sistemas de abastecimiento de gas y petróleo para sus explotaciones siberianas, a lo que el gobierno de EEUU no accedió. La forma que encontraron los soviéticos de hacerse con ese material fue comprarlos a través de una empresa canadiense. En los equipos vendidos a la URSS se encontraba instalado un troyano, su objetivo, someter a válvulas, bombas y turbinas del sistema a más presión de la que podían soportar. Estos desemboco en una gran explosión.

Vector de ataque: Troyano instalado en los equipos informáticos del SCI. (Código Dañino)

4.2. Petrolera Chevron (1992)

La empresa Petrolera Chevron, sufrió un hackeo de sus ordenadores en las sedes de California y San José, concretamente eran los equipos que controlaban todos los sistemas de alerta, este hackeo los deshabilito. El ataque se descubrió cuando se produjo un incidente que libero una sustancia nociva sin que se enviara la alerta pertinente. El ataque coincidió con el despido de un trabajador de la compañía.

Vector de Ataque: Sabotaje, coincidiendo con el despido de un trabajador. (INSIDER)

4.3. Salt River Project (1994)

Mediante un modem en el año 1994 se consiguió acceder a la información completa de la compañía que suministra agua y electricidad por el estado de Arizona (EEUU). Se pudo acceder a los ficheros de los sistemas de suministro de agua y electricidad, a la información del personal y a la información financiera de clientes y trabajadores.

Vector de Ataque: Línea modem abierta, con poca protección, sistemas sin contraseñas, contraseñas por defecto o débil.

4.4. Aeropuerto de Worcester (1997)

Un ciberdelincuente se introdujo en los sistemas de comunicaciones de tráfico aéreo del aeropuerto de Worcester en el estado de Massachussetts (EEUU), dejando inutilizados los sistemas de telefonía de torre de control, departamento de bomberos, servicio meteorológico y las líneas telefónicas de las compañías aéreas. El sistema estuvo interrumpido 6h.

Vector de Ataque: Seguridad débil o sistema abierto sin contraseña, contraseña por defecto o débil.

4.5. Gazprom (1999)

Una de las empresas más grandes del mundo en el sector de la energía, cuenta con más de 400.000 empleados en todo el mundo y el 15% de las reservas mundiales de gas. En el año 1999 se consiguió

instalar un troyano en los sistemas SCADA, en el sistema que controla los flujos de gas por las tuberías. En principio se saldó sin incidentes, pero la compañía rusa perdió el control unas horas.

Vector de Ataque: Troyano, con la ayuda de un trabajador de la compañía. (INSIDER y código dañino)

4.6. Maroochy Water System.

En el año 2000 se hackeo, con material robado de la empresa, el sistema de control de aguas que provoco un vertido de aguas residuales en un rio cercano. Detrás del incidente se encontraba un ex empleado de la compañía.

Vector de Ataque: Sabotaje de un ex-empleado, material sustraído a la empresa. (INSIDER)

4.7. PSVSA(2002)

En el año 2002 se produjo un incidente de seguridad que bajo la producción de petróleo de la compañía Petróleos de Venezuela SA en más de 2 millones de barriles al día. El hackeo se produjo en días en que lo empleados estaban realizando huelga. Se hackearon varios ordenadores.

Vector de Ataque: Sabotaje de un empleado o ex-empleado. Sistemas de seguridad sin supervisión o caídos. (INSIDER)

4.8. Tráfico en la ciudad Los Ángeles (2006)

En el año 2006 se produjo grandes atascos en la ciudad, se escogieron minuciosamente semáforos en zonas de mucho tráfico y se aumentó el tiempo en que el semáforo permaneció en rojo. Dos ingenieros de tráfico de la ciudad hackearon los semáforos durante una protesta laborar.

Vector de Ataque: Sabotaje de un empleado o ex-empleado.

4.9. Experimento Aurora (2007)

El experimento Aurora se realizó en el Laboratorio Nacional de Idaho, con el objetivo de averiguar si se podía dañar una máquina de la red eléctrica, en este caso un generador diésel, usando simplemente una comunicación industrial. Podríamos decir que fue el primer caso de intento de daño a un equipo físico mediante software.

Se usó un generador diésel con comunicación modbus, mediante órdenes se conectaba y desconectaba la orden de ajuste de velocidad para obligar al sistema de frenado a entrar continuamente en regulación hasta que se los frenos se sobrecalentaron. El experimento consiguió su objetivo.

Vector de Ataque: Al usar un protocolo sin ningún tipo de autenticación cualquiera pudo dar órdenes al generador, además la programación del mismo permitía realizar cualquier tipo de maniobra.

4.10. Infraestructura de Internet de Estonia (2007)

El primer ciberataque a la infraestructura de Internet se produjo en Estonia, en 2007 varios ataques contra la infraestructura de Internet provoco que cayeran las páginas del parlamento, ministerios, bancos, periódicos, etc. El ataque además ataco a direcciones no públicas de IC, con lo que cayeron también las telecomunicaciones del país y todas las transacciones financieras.

Vector de Ataque: Sin información del vector de ataque. Se sospecha que se produjo un ataque coordinado de otra nación soberana.

4.11. Tranvías de Lodz (2008)

En la ciudad polaca de Lodz se hackeo la red de tranvías, como consecuencia 4 tranvías descarrilaron. El autor un estudiante de 14 años construyo un dispositivo que transmitía señales de infrarrojos a los controles de los cruces de vías y cambiaba el estado sin ningún tipo de control.

Vector de Ataque: Sistema de autenticación nulo, ninguna protección en gestión de cruces de vías.

4.12. Stuxnet (2010)

El gran cambio en la protección de SCI empezó con Stuxnet, era el primer malware diseñado exclusivamente para un ataque, en este caso para un controlador de la marca Siemens S7-315, que controlaba las centrifugadoras de uranio de la planta nuclear de Natanz en Irán. Se aprovechaba de varias vulnerabilidades de día 0. Pese a ser un sistema aislado, no estaba conectado a Internet, se consiguió que una persona instalara el malware.

Vector de Ataque: Vulnerabilidades de día 0, infección de un agente infiltrado que inserto un pendrive USB con el malware. (INSIDER – código dañino)

4.13. Aramcon - RasGas (2012)

En 2012 se consiguió el acceso a 30.000 ordenadores de la compañía petrolera más grande del mundo Saudí Samco. Se consiguió acceso a un ordenador y después el ataque se fue extendiendo hasta afectar a los 30.000 ordenadores. Una vez conseguido esto, simultáneamente se borró el contenido de todos los equipos a la vez que aparecía una bandera de EEUU en llamas en las pantallas.
Pocos días después, la empresa catarí RasGas sufría un ataque similar con el mismo malware.

Vector de Ataque: Infección de un equipo individual, contraseña débil o sin contraseña. Ninguna protección en capas, permitió que se extendiera a todos los equipos. (código dañino)

4.14. bit9 (2013)

Basándose en un paradigma diferente al resto de los sistemas de seguridad, las herramientas de seguridad de bit9 se basan en listas blancas, es decir, los sitios de la whitelist son totalmente confiables. La empresa sufrió un ataque en el que se comprometieron sus certificados digitales y con

ello crearon malware pre autorizado por bit9. El resultado fue la infección de malware por parte de sus clientes.

Vector de Ataque: Robo de certificados digitales para firmar malware. (código dañino)

4.15. DragonFly (2014)

Siguiendo a Stuxnet, este grupo de ciberespionaje especializado en SCI e IC, se enfocó en Norteamérica y Europa, con objetivo del control remoto de equipos Basado en troyanos su objetivo es infectar equipos mediante campañas de spam o ataques watering hole para lograr su objetivo.

Vector de Ataque: Spam, troyanos, Watering Hole (Estrategia basada en la localización de páginas web de la organización que se pretende atacar e intentar infectarlos para poder obtener acceso). (Código malicioso)

4.16. Metalurgia Alemana (2014)

Unos atacantes consiguieron acceder al ordenador de un empleado, mediante ingeniera social, desde allí a la red donde se encontraba el sistema de control. Como consecuencia un alto horno se quedó encendido y se generaron cuantiosos daños en las instalaciones.

Vector de Ataque: Ingeniería social, poca o ninguna separación por capas de las diferentes partes de la planta. (Ingeniería social)

4.17. Red Eléctrica Ucraniana (2015-2016)

Un ciberataque a la red eléctrica dejo sin energía a más de 600.000 personas en 2015, ataque similares se repitieron en 2016. BlackEnergy es un malware que se utiliza para instalar otros componentes KillDisk, que aparte de impedir que la computadora arranque, actúa sobre los sistemas industriales encargados del control de la red eléctrica. El vector de ataque es una vulnerabilidad sobre archivos de Office concretamente de Powerpoint en el que se tienen que aceptar la habilitación de macros. Una vez habilitada el equipo ya se ha infectado con BlackEnergy.

Vector de Ataque: Fichero PowerPoint con macros enviado por mail, vulnerabilidad día 0. (Código dañino)

4.18. Kemuri Water (2016)

Un grupo accedió al SCADA de una planta depuradora del Reino Unido, para ello uso como forma de entrar el portal de pago de clientes que no se encontraba adecuadamente protegido, una vez vulnerado el portal de pago, se accedió al SCADA y se cambió incluso la composición del agua. A su vez se obtuvieron los datos de millones de consumidores.

Vector de Ataque: Portal de pagos sin parchear, no se separaron por capas TI y TO.

4.19. WannaCry Expetr (2017)

Wannacry es un ramsonware que cifra los datos de los ordenadores y solicita un rescate para la liberación de la información. Afecta al sistema operativo Windows, en 2017 infecto a 230.000 computadoras en 150 países. El ataque se inicia cuando se abre un correo de phishing, una vez hecho esto mediante un exploit llamado EthernalBlue se propaga por la red local o anfitriones remotos.

Vector de Ataque: Mail phishing con el ramsonware, vulnerabilidad día 0.

4.20. Operación Sharpshooter (2018)

Es una campaña a nivel mundial de ciberespionaje a IC, para ello se usó el malware Rising Sun, que es una puerta trasera encargada del reconocimiento de una red con el objetivo de obtener información. En 2018 se introdujo en 87 organizaciones, de sectores como el militar, eléctrico, financiero y nuclear. Para introducir el malware se usó spear-phishing con la tapadera de una oferta de trabajo, una vez se ha descargado un fichero Word, ya se ejecuta sharpshooter.

Vector de Ataque: Spear-Phishing para buscar víctimas, código malicioso en fichero Word.

5. SECURIZACIÓN DE SISTEMAS DE CONTROL.

Los SCI tradicionalmente han sido sistemas cerrados, se diseñaban y se ponían en marcha para una funcionalidad y durante todo el ciclo de vida del equipo se hacían pequeñas modificaciones. Pero generalmente el PLC sobre el que corría el programa o el sistema SCADA de monitorización permanecía inmutable durante años. Los principios de diseño eran la funcionalidad, la fiabilidad y la velocidad (se primaba en muchos casos la lectura de datos lo más rápidamente o el almacenamiento de históricos).

Hasta hace pocos años estos mantenimientos tan limitados, además se hacían in situ, en las instalaciones del cliente. No se realizaba ningún tipo de mantenimiento en "remoto". Posteriormente, con la llegada de sistemas interconectados a redes, se permitió, sin desplazarse a una instalación, que un sistema pudiera estar mantenido a distancia, lo que abarató los costes e introdujo la posibilidad de continuas mejoras. Como contrapartida, esta apertura propició nuevos riesgos para los sistemas.
Hoy en día un sistema TO comparte sistemas de las Tecnologías de la Información, como bases de datos, redes o sistemas operativos multiusuarios dentro de redes corporativas.

5.1. Principios.

Para proteger cualquier sistema se puede usar como guía los siguientes principios rectores.

- Proteger: Es imprescindible implementar medidas de protección que de alguna manera previenen cualquier tipo de ataque. Si bien unas medidas de protección que protejan contra el 100% de los ataques no es posible, se intentara disuadir o dificultar en la medida de lo posible un ataque.
- Detectar: Hay que tener capacidad para identificar cualquier ataque. Para ello existen diversos elementos que permiten una detección temprana lo que posibilita tomar medidas.
- Responder: Tener una capacidad de respuesta al incidente, una vez iniciado o detectado.

5.1.1. Instalación de medidas técnicas.

En principio la instalación de medidas es una buena idea, pero conlleva en sí mismo una responsabilidad. Instalar un cortafuegos sin una configuración adecuada o una supervisión de posibles incidentes no va a servir como medida de protección. La instalación de cualquier medida debe ser un proceso continuo. Se debe instalar, supervisar su funcionamiento, ser puesta a prueba y adaptar a nuevas exigencias del sistema. Esto implica un uso de recursos técnicos y humanos en continua evolución. Normalmente los SCI trabajan 24h al día, durante los 365 días del año.

Hace unos años se instalaba un SCI y una vez superadas las pruebas de la puesta en marcha no se hacía nada en todo el ciclo de vida. En la actualidad se ha demostrado que no es viable, puesto que afecta a su seguridad.

5.1.2. Análisis de riesgo de negocio.

Una de las partes más importante es saber a qué se enfrenta un sistema. Para ello es importante realizar un análisis de riesgo del negocio. Los criterios que se evaluarán para ello son:

- Comprender los sistemas. Evaluación del sistema de control y saber la composición completa de la instalación.
  - Listado completo de los sistemas que forman el SCI.
  - De cada equipo o sistema que papel en el conjunto del SCI tiene, que tarea cumple, que puntos débiles puede tener y que consecuencias tendría un fallo del mismo.
  - Quien es propietario del sistema, quien lo gestiona y quien le da soporte.
  - Un sistema de control de cambios, para controlar modificaciones.
  - Un inventario de los sistemas, la pérdida o sustracción de un equipo podría servir para la extracción de información muy importante del sistema a un atacante.

- Comprender las amenazas. Hacer un listado de las amenazas que puedan afectar al SCI, se relacionara con el sistema que pueda ser afectado. No todos los sistemas o equipos tienen las mismas amenazas. Las más comunes son :
  - Ataques de Denegación de Servicio
  - Ataque dirigido
  - Control o accesos no autorizados.
  - Infecciones de malware.
  - Incidentes o Accidentes.

- Comprender el impacto. Se analizará el impacto, tanto interno como externo, como el impacto en un sistema mayor del que tiene la incidencia. Por ejemplo, si hablamos de una central eléctrica, dentro del sistema eléctrico de un país se deberá analizar qué consecuencias tendrá un incidente en la propia central y también en el conjunto del sistema eléctrico. Como impactos más genéricos podemos enumerar:
  - Pérdida de reputación de la empresa.
  - Incumplimiento de una normativa vigente: Medioambiental, Laboral, Protección de datos, etc.
  - Incapacidad de cumplir con un compromiso adquirido, con sus costes financieros asociados.

- Comprender las vulnerabilidades. Realizar un estudio de las vulnerabilidades conocidas que pueden afectar al SCI. En el estudio se analizarán:
  - La infraestructura del SCI.
  - El Software que incluirá: Sistemas operativos, aplicaciones instaladas y el propio software del SCI, se tendrá especial cuidado si se trata de una estación de ingeniería, ya que en ella recae el peso del mantenimiento de la instalación.
  - Arquitectura de red, conexiones, equipos de red y conectividades de acceso remoto.
  - Procesos y procedimientos, que puedan contener instrucciones que generen una amenaza.

5.1.3. Riesgos de terceros.

Otros riesgos son los provocados desde terceras partes. En este grupo podemos encontrar cualquier proveedor, organización de soporte o empresas que forman parte de una cadena de suministro. Así que una parte de las medidas que se aplican en los sistemas de control es importante que se exija a las empresas que forman parte del entorno. Por tanto es importante identificar todas estas empresas del entorno y de alguna forma colaborar en mejorar la seguridad. Las medidas a tomar se detallan a continuación:

- Exigencias a proveedores.
  - En todos los contratos que se firmen se deben recoger las cláusulas de seguridad.
  - El compromiso de ante cualquier vulnerabilidad descubierta en el proveedor y que pueda afectar a la empresa cliente sea notificada y corregida. (Ejemplo. Vulnerabilidad detectada en un web Server que provee un tercero)
  - Compromiso de seguridad en sus sistemas. (Ejemplo. Control de usuarios y permisos en equipos de un SCI)
  - Integración de sistemas de seguridad en equipos. Siempre que esto sea posible. (Ejemplo. software antivirus, firewall, etc...)
  - Gestión de parches y actualizaciones.
  - Identificación de todas las tecnologías usadas en un desarrollo. (Ejemplo. Bases de datos, arquitecturas de red,…)
  - Inspecciones y revisiones periódicas.
- Exigencias a empresas de soporte.
  - Impedir el acceso a empresas de soporte que no cumplan unos determinados requisitos. Es importante que quede formalizado en un contrato el compromiso de cumplir estas exigencias. (Ejemplos de prohibición: ordenadores con sistemas operativos obsoletos, ordenadores sin ningún software antivirus).
  - Compromiso de informar en caso de detección de fallo o vulnerabilidad del SCI. Tanto propios como sistemas asociados (Ejemplo: proveedor de servicios de red que detecte una vulnerabilidad grave en sus router)

    - Especificar unos procedimientos de actuación ante los sistemas de control. (Ejemplo: acordar horas en las que se instalarán actualizaciones, o en caso de equipos redundantes el proceso de instalación para que no caiga el sistema).
- Exigencias a la cadena de suministro.
    - Garantías de un soporte ante riesgos de seguridad.

5.2. Aspectos en diseño.

Una vez un sistema entra en producción es muy complicado la instalación de medidas, por eso es importante a la hora de empezar un proyecto, tener claro que se trabaja para conseguir un resultado que sea funcional pero también seguro. A la vez que se hace la puesta en marcha del sistema, una parte a revisar son las medidas de seguridad implementadas. Todas las amenazas identificadas en las fases más tempranas permitirán implementar una solución o contramedida en los diseños finales, siendo más complicado conforme se avanza en el desarrollo del proyecto.
Como regla de oro en el diseño de cualquier SCI, sobre todo si va a ser usado en una IC, es:
“Cualquier sistema que tenga vulnerabilidades conocidas y no vayan a ser solucionadas, no es un sistema que se pueda integrar”.

5.2.1. Problemática de los SCI.

A la hora de realizar un diseño o el posterior mantenimiento de un SCI en general se encuentran las siguientes limitaciones:

- Comunicaciones abiertas: Los datos de los SCI deben llegar rápido, refrescarse en las pantallas de operador lo más rápido posible. Los protocolos transmiten sin implementar ningún mecanismo de cifrado. Protocolos que se han comentado anteriormente como modbus transmiten la información en texto claro.
- Falta de verificación de identidades: En un SCI ningún equipo de una red duda de la identidad de los otros, es decir no se exige ningún tipo de autenticación antes de establecer comunicación para confirmar que las partes que quieren comunicarse son quienes dicen ser. Un equipo de la red puede enviar comandos falsos o incorrectos.
- Accesos remotos: Puede ser necesario implementar accesos remotos para facilitar tareas de mantenimiento y reparación. Se deberán analizar cuidadosamente estos accesos.
- Áreas de alcance grandes: Muchas de estas infraestructuras tienen equipos dispersados en áreas muy grandes e incluso muchas posiciones están desatendidas.
- Software específico y obsoleto: El ritmo de actualización del software usado en SCI muchas veces no avanza al mismo ritmo que el software de las TI, es muy normal encontrar la última versión de un software SCADA que no es compatible con las últimas versiones de sistemas operativos o las últimas actualizaciones.

- Uso de contraseñas débiles: Se tienen contraseñas genéricas que usan todos los operadores, que no cumplen con los criterios de seguridad (longitud, minúsculas y mayúsculas, números y símbolos). En la mayoría de los casos ante la rotación de operadores están apuntadas cerca de los dispositivos correspondientes.
- Ninguna política de control de usuarios: Otra consecuencia de la rotación de personal, para simplificar accesos se limita mucho el número de perfiles diferentes o directamente en el software de SCI todos los usuarios usan el mismo perfil con nivel elevado de privilegios.
- Ordenadores con múltiples funciones: Por economizar equipos se usan los mismos para tareas administrativas y cliente SCADA.
- Nulo mantenimiento de ordenadores: No se instalan actualizaciones o se hacen de forma manual y con períodos muy largos entre actualizaciones. No se tiene en cuenta estas tareas.
- Configuración funcional antes que segura: Se intentar agilizar cualquier tarea se prioriza la funcionalidad de cualquier sistema, antes que la seguridad.
- Gestión de usuarios inexistente. No se controla el software que se instala, las páginas web a las que se accede o el uso de dispositivos personales en equipos del SCI.
- No se registran eventos de aplicaciones ni del sistema operativo.
- Durabilidad muy elevada. Generalmente los equipos de campo, tienen una duración muy elevada. No es raro encontrar equipos como PLC o equipos electrónicos con una longevidad de 20 años, muy superior a los ordenadores de control y supervisión. Además, estos PLC tienen un coste muy elevado. Lo que supone que aunque se renueven los ordenadores se instala el mismo software obsoleto, incluso buscando instalar los mismos sistemas operativos que se descatalogaron hace tiempo.

Todos estos inconvenientes hay que tenerlos presentes a la hora del diseño de un SCI. En muchos casos no se realiza un nuevo diseño, sino una mera actualización o ampliación de una planta existente. Esto conlleva que se suelen heredar defectos de diseños obsoletos.

Un problema más que surge dentro de los sistemas TO es la dificultad de realizar un análisis forense ante un incidente. Si bien es cierto que para realizar análisis forenses se usan herramientas que se aplican a los sistemas TI, es cierto que esa falta de herramientas específicas se dificulta más cuando se utilizan sistemas de un fabricante, que son cerrados. Por lo tanto, sin su colaboración es imposible llevar a cabo un análisis forense. Un análisis forense nos permitirá aprender de lo que ha sucedido y recopilar pruebas para un proceso judicial. Si bien en según qué casos la prioridad es el restablecimiento del sistema lo antes posible.

5.2.2. Seguridad en diseño.

Una vez se han expuesto los problemas que se presentan a la hora de implementar un SCI, es importante mencionar unas pautas que ayuden a mejorar la seguridad de un SCI. Pese a todo muchas de estas medidas no se podrán tomar, por la complejidad de los sistemas. Están clasificadas por apartados.

Arquitectura de la red.

- Se debe realizar un esquema y anotar todas las conexiones existentes dentro de un sistema. Es importante además anotar el hardware, dirección MAC, dirección IP e incluso versión del firmware. No es raro la instalación de equipos comprados a la vez y con firmwares diferentes. También ayuda tener un diagrama del conexionado completo de equipos.
- Reducir al mínimo el número de conexiones y simplificar en lo posible las mismas.
- Siempre que sea posible, las redes y equipos de un SCI debe estar separada de otras redes corporativas, o en caso de que tenga que haber un flujo constante de información entre ambas, separarlas como mínimo con un cortafuegos.
- Se eliminarán siempre que sea posible las conexiones TCP/IP en procesos críticos. Un apagado de emergencia es mejor que no se envíe mediante comunicación TCP/IP.
- Siempre que sea posible se usarán redes redundantes o arquitecturas mediante anillos de F.O.
- Se garantizará una gestión de cambios para el hardware de red.

Cortafuegos.

- Para aislar en la medida de lo posible redes TI de redes TO se protegerán adecuadamente. Una posible solución es un área DMZ o el uso de cortafuegos entre zonas.
- Las reglas de un cortafuegos deben "denegar" por defecto. El inconveniente es que esto requiere de una configuración más delicada. Se crearan reglas que "permitirán" el paso.
- Se debe establecer una política de supervisión y configuración de reglas de firewall, además de un adecuado control de cambios en las modificaciones que se realicen.
- Se debe establecer una política de gestión y supervisión del estado de los cortafuegos. De nada sirve instalar un firewall si no se comprueba su funcionamiento y se comprueba que es realmente eficaz.
- Es recomendable la instalación de sistemas de seguridad como IDS o SIEM. Es una supervisión 24/7 aunque según la envergadura del proyecto esto no será viable. Es importante un mínimo de supervisión.

Acceso Remoto.

- Es necesario realizar un inventario de conexiones remotas. Como información se deberá incluir: Usuario, empresa, fecha de validez y medio de conexión usado. Es recomendable el uso de un log con las horas de conexión.
- Se reducirán al mínimo el número de conexiones remotas.
- La conexiones requerirán autenticaciones fuertes, como ejemplo:
  - Contraseñas de autenticación de un solo uso.
  - Autenticación basada en certificados.
  - Matrices de tokens
  - Dobles factores de autenticación. Contraseña + Código a un móvil.
- Implementar mecanismos de habilitación y deshabilitación de accesos remotos, que sean rápidos y eficaces. Es importante mencionar que por defecto el acceso remoto siempre debe estar deshabilitado.
- Es importante exigir al prestador del servicio, revisiones de seguridad o la instalación de software antimalware. (ver exigencias a empresas de soporte).
- Muchas veces una solución eficaz y barata es disponer para acceso remoto de una línea de acceso exclusivo para acceso remoto. En el momento que no se use, el operador apagará el router y la conexión quedara totalmente inutilizada.

Antivirus.

- Siempre que sea posible se instalará software antivirus en los puestos de operador y servidores.
- En caso de no poder ser desplegado un software antivirus, se intentará buscar una solución que no requiera de instalación.
- La diversidad de software en SCI hace que la instalación de un antivirus afecte al funcionamiento general del sistema. Se procederá a realizar la consulta al fabricante antes del despliegue.

Correo Electrónico y acceso a Internet.

- En la medida que sea posible no se usara ni un servidor, ni un puesto de operador para trabajar con herramientas ofimáticas, correo electrónico o acceso a Internet.
- Como alternativa, es más seguro el uso de equipos independientes, como el puesto de operador por un lado y equipos administrativos con correo, Internet y ofimática por otro.

Securización de sistemas.

- Se deberá analizar los servicios de servidores y ordenadores de puestos de operador para limitar el número de puertos abiertos. Se cerrarán todos los puertos innecesarios, se

desinstalarán las aplicaciones innecesarias. Más aplicaciones implica más posibilidades de vulnerabilidad.

- Todos los sistemas tendrán que tener habilitadas todas las medidas de seguridad posibles. Por ejemplo: antivirus, firewall,
- Se restringirá al máximo el uso de CD's, DVD's o unidades extraíbles. Si es necesario se debe garantizar que no contienen malware. En muchos casos se dispondrá de un único pendrive USB que se garantice su limpieza y sea el único que se use para el intercambio de información entre equipos.

Ubicación Física.

- Se debe garantizar la seguridad física de los equipos más críticos. Por ejemplo una sala de servidores con llave o control de accesos.
- De forma disuasoria se puede instalar sistemas de circuito cerrado de TV.
- En el acceso a zonas seguras se priorizará el acceso mediante tarjetas de accesos, en los que quedará registrada la hora de acceso y el usuario. Normalmente a la vez se instalá una cámara para visualizar el acceso.
- El equipamiento crítico debe estar en zonas con temperatura y humedad controladas, se tendrán en cuenta elementos como sistema de extinción de incendios y control de fugas de agua.

Hardware Sistemas de Control

- En sistemas de control en algunos casos los autómatas se puede configurar como solo lectura mediante una llave, esa llave como mínimo no estará en posición programación. Es caso de máxima seguridad, permanecerá quitada del autómata.
- Los cuadros eléctricos de sistemas críticos pueden estar cerrados bajo llave.
- Se llevará un control físico de la ubicación de cada equipo, y se debe asegurar que están en una ubicación segura.
- En cuadros críticos o instalaciones remotas se instalarán sensores de puerta abierta, para detectar que se ha realizado una apertura de cuadro. Este evento llevará asociado el envío de una alarma.
- Se garantizará una gestión de cambios para el hardware del SCI.
- Siempre que sea posible cualquier modificación se realizará en un entorno de pruebas.
- Cualquier sistema que disponga de algún tipo de redundancia de software o hardware debe ser debidamente puesto a prueba.

Monitorización de sistemas.

- Se deben realizar una supervisión de los sistemas TI (detectando un tráfico superior al habitual en segmentos de red o equipos) como a nivel de sistemas TO (maniobras extrañas, paro de secuencias sin aparente explicación)
- Si es posible se instalará un IDS (Sistema de detección de intrusos) que analice la actividad de red. Es importante recordar que se deben adaptar estos sistemas a las peculiaridades de los SCI.
- Analizar en conjunto los LOG de IDS y firewall de forma periódica. Realizar copias de los mismos en máquinas externas.

Redes Inalámbricas (WI-FI).

- Debido a los riesgos que implica la introducción de sistemas inalámbricos se procederá a su instalación en casos en que sea la única alternativa.
- Se priorizará el uso de conexiones de red cableadas.
- Una alternativa al uso de terminales portátiles con WIFI, es la instalación estratégica de terminales HMI táctiles que se encuentren ubicados en campo.
- Se ajustará en la medida de lo posible el área de cobertura de la WIFI, la idea es protección por ocultación, no tener posibilidad de detectar las WIFI fuera del recinto que eviten accesos lejanos.
- El uso de puntos de acceso WIFI para uso personal dentro de empresas no puede estar de ninguna manera relacionado con las redes de SCI o corporativas.

Actualizaciones y parches.

- Se debe procedimentar la instalación de parches y actualizaciones. Es importante el trabajo conjunto de departamentos TI y TO para concretar la manera en que se debe realizar y adaptar a las peculiaridades del SCI.
- Se auditará el correcto desplegado de la actualización o parche.
- Siempre que sea posible se solicitará al proveedor garantía de la aplicación del parche. Tanto a nivel de sistema operativo, como del software de control del SCI.
- Antes de la instalación de la actualización o parche hay que asegurarse de tener un punto de restauración en estado de funcionamiento para poder restaurar a ese punto en caso de que algo falle.
- Como caso ideal se dispondrá de una máquina de pruebas para realizar instalaciones que permita que no afecten a maquinas en producción sin comprobar antes su funcionamiento. Es cierto que esto en muy pocas instalaciones es posible.
- Se implementarán también procedimientos para hacer frente a vulnerabilidades que aparezcan durante el ciclo de vida de la instalación.
- Se garantizará un control de cambios para software.

Contraseñas y cuentas de usuario.

- Se debe establecer una política de contraseñas para todos los equipos del SCI.
- Se usarán contraseñas fuertes, con números, símbolos, letras mayúsculas y minúsculas de como mínimo una longitud de 8 caracteres.
- Se cambiarán periódicamente.
- Se gestionará el alta, baja y modificación de usuarios, y las consiguientes cuentas con sus permisos asociados.
- No se usará ninguna contraseña por defecto.
- Se elegirán los niveles apropiados de permisos para el desempeño de funciones. Se tiene que evitar en la medida de lo posible usar las cuentas de administrador en todos los equipos.
- Se revisarán los privilegios de usuarios periódicamente.
- No se apuntarán las contraseñas en los mismos equipos que se tienen que proteger (Parece obvio pero pasa muy a menudo, incluso escritas en el mismo teclado).
- Como excepción, si se considera que hay un determinado perfil de visualización que no es crítico en el funcionamiento, este perfil puede estar sin contraseña.

Documentación.

- Se realizará un inventario de todos los equipos del SCI, con números de serie, modelo y firmware. Resultará útil para labores de mantenimiento también.
- Se documentaran también medidas de seguridad instaladas, las amenazas y planes establecidos. Esta información solo será accesible para personal autorizado.
- Se guardará toda la documentación del proyecto y se comprobara que se ajusta lo proyectado con lo instalado. Se confirmará con los planos "as build" (como construidos, planos en los que incluyen las últimas modificaciones.

5.2.3. Análisis del impacto de una parada.

Un SCI es un sistema complejo en el que existe una infinidad de sistemas interconectados. La diversidad de equipos y de zonas que se suelen encontrar hacer que haya mucha diferencia entre la parada de una parte de la instalación u otra.

Es recomendable analizar el impacto de una parada, para ello es recomendable analizar todos los equipos instalados dentro del SCI, y determinar que función tienen en el conjunto del SCI y que impacto tendría. Los equipos que se analizarían son:

- Equipos PLC de automatización: Es importante analizar qué procedimientos se ejecutan, de qué elementos o zonas de campo leen información o envían órdenes. En este análisis se analizarán varios supuestos:

  - Equipo inutilizado: Qué pasaría si ese equipo quede bloqueado o apagado. Qué procedimientos dejarían de ejecutarse y con qué consecuencia para el sistema.
  - Equipo aislado: Qué pasaría si ese equipo pierde comunicación con el resto del sistema, podría seguir ejecutando su programa o qué funciones se podrían perder.
  - Las redundancias de equipos si funcionan correctamente.

- Equipos de la arquitectura de red del SCI: Los equipos de arquitectura de red, pese a formar parte de la infraestructura de red, en muchos casos se gestionan en el entorno de las TO más que de las TI. Se debe analizar las consecuencias de fallo de un equipo de red, qué equipos dejaría aislados si se está usando un anillo de fibra óptica, cómo actuaria la redundancia y a qué zonas de planta afectaría.

- Equipos de control de operador: En estos equipos incluimos equipos de operación, pantallas táctiles de campo. En este caso más que un fallo que incapacite el equipo, preocupa más el uso que se pueda hacer de estos equipos, ya que normalmente se dispone de más de un ordenador o en caso de un solo ordenador de operación, se dispone de un HMI táctil en campo para realizar las operaciones en caso de avería. Es más importante analizar en caso de que el equipo se vea comprometido qué posibilidades tiene un atacante de poner en marcha o parar elementos, qué perfiles se han creado y qué limitaciones tienen.

- Elementos externos: Se analizara la consecuencia que puede tener que caiga un equipo externo controlado desde el sistema de control para el proceso.

Con todo esto se realizará un análisis completo que determinará cómo un fallo en una parte del sistema afectará al conjunto del SCI. Se localizarán equipos más sensibles que otros y se podrá analizar qué consecuencias tendrá para el conjunto y para la organización una parada de este tipo.

5.3. Securización del puesto de operador.

Siempre que se habla de securizar un sistema, se tienen en cuenta multitud de factores, pero pocas veces se tiene en cuenta al operador o usuario de un SCI. En muchos casos los operadores se enfrentan a situaciones para las que no se les ha preparado o formado. Tienen un amplio conocimiento de su proceso productivo pero poca formación ante las amenazas que externamente pueden afectarle.

5.3.1. Principales amenazas del puesto de operador.

Las amenazas más comunes son:

- APTs (Advanced Persistent threat), amenazas muy sofisticadas, de gran complejidad técnica y que tienen una cierta persistencia. Un ejemplo es Stuxnet. En muchos casos su objetivo principal es a largo plazo y no es un objetivo económico.

- Ingeniería Social. El objetivo es convencer al operador para que realice despreocupadamente acciones que puedan perjudicarle a él o a la empresa para la que trabaje. Se intenta aprovechar mediante manipulación de las personas. El Spear Phishing (Envió de correos personalizados con adjuntos maliciosos con el objeto de afectar al equipo objetivo). Una variante muy usada de la ingeniería social es lo que se conoce popularmente como "La estafa del CEO", una llamada a un trabajador por parte del supuesto jefe que le ordena que haga una transferencia urgentemente.

- Dispositivos Físicos. Tanto profesionales como personales que infectan un sistema. Un ejemplo es el tipo USB que alguien se deja olvidado.

- Vulnerabilidades 0-day. No catalogadas, que no existe parche o que aunque hay parche no se ha instalado. En los SCI es complicado seguir el ritmo de las actualizaciones.

5.3.2. Dispositivos extraíbles.

En los últimos años ha pasado a ser un artículo muy necesario en muchos sistemas, por su sencillez de uso y gran capacidad. Es importante contar con una política interna de uso que establezca límites. En muchos casos no se dispone de esta política, pero por lo menos hay que cumplir unas premisas básicas:

- Usar siempre y solamente USB proporcionados por la empresa. Solo se insertaran en ordenadores de la empresa y nunca en ordenadores personales.
- Deben estar debidamente identificados e inventariados.
- En caso de necesidad de extraer información a un USB ajeno a la empresa se deberá: formatear, hacer un borrado seguro y escaneo con software antimalware.
- Se analizaran con cierta periodicidad los dispositivos.
- Nunca se usaran dispositivos que aparecen en las zonas de trabajo.
- Posibilidad en casos extremos de uso de herramientas como kioscos o simplemente ordenadores de prueba. Los kioscos son dispositivos que aseguran que los USB no contengan ninguna amenaza.

5.3.3. Dispositivos móviles.

En la actualidad es común el uso de dispositivos móviles para el acceso remoto a plantas o como terminal de mantenimiento. En algún caso el software SCADA han desarrollado capacidad de acceso

mediante equipos móviles para realizar pequeñas tareas de operación y consulta. Dentro de estos dispositivos encontramos teléfonos móviles, tablets y ordenadores portátiles. Su naturaleza portátil hace que se expongan a riesgos diferentes que otros sistemas. Las precauciones a tener en cuenta para cualquier sistema que se conecte a un SCI son:

- El dispositivo debe está protegido con contraseña, datos cifrados y si es posible garantizar el borrado remoto.
- Si es posible no memorizar en el equipo la contraseña ni usuario de acceso remoto.
- En caso de pérdida o extravió, notificar inmediatamente a los responsables de seguridad para proceder a dar de baja ese acceso remoto y si es de la empresa bloquear remotamente el terminal.
- Las conexiones se deberán establecer mediante conexiones cifradas o VPN. En ningún caso desde conexiones públicas.
- Como en otros casos se llevara un control o inventario de los equipos móviles que pueden acceder al sistema de control, propietario, versiones de software, etc...

5.3.4. Uso del WIFI en entornos industriales.

En muchos casos la introducción de redes inalámbricas introduce en el SCI una serie de riesgos importantes que solamente se pueden justificar en caso de que aporte algún beneficio. Es importante tener muy claro el uso al que va destinado, porque en muchos casos plantearse un uso para todo no genera más que riesgos innecesarios. Las precauciones a tomar son:

- Se debe usar como mínimo un WPA2, siempre prestando atención a elementos como la contraseña, segura y de continua actualización. Siempre estar atento a posibles vulnerabilidades en el protocolo de autenticación, continuamente aparecen vulnerabilidades.
- La comodidad de no conectar un cable de red en un portátil, en muchos casos expone toda la red corporativa. Minimizar el uso de redes inalámbricas siempre que sea posible y si es inevitable, crear redes separadas para el uso de teléfonos móviles personales y la red corporativa.
- Limitar el alcance, es arriesgado usar equipos y repetidores para aumentar la cobertura mucho más allá del perímetro de la instalación, implica dar cobertura a un posible ataque.
- Uso de listas negras o listas blancas siempre que sea posible con equipos de confianza.

5.3.5. Instalación de software antimalware.

Se debe instalar en los equipos alguna solución malware, lo ideal es que este certificado el software para evitar incidencias o fallos de funcionamiento. En caso de no tener ninguna garantía del correcto funcionamiento o en caso de tener 2 o más ordenadores de operación iguales, se instalará en uno y comprobará su correcto funcionamiento. Si sólo hay un equipo hay que asegurarse de tener un punto de restauración para volver en caso de que el equipo no funcione bien después de la instalación.

Un problema que surge es que el acto de instalar un antivirus en sí mismo no protege, es responsabilidad del operador realizar análisis periódicos y asegurarse de que los archivos de firmas están convenientemente actualizados.

5.3.6. Concienciación y habilidades

Los controles de seguridad básicos a aplicar en un puesto de operador son:

- Eliminar cuentas innecesarias. Lo cual no implica usar únicamente la de administrador.
- Desactivar servicios que no se usan. Si no se va a usar el RDP (Remote Desktop Protocol), el escritorio remoto de Microsoft no tiene sentido tenerlo, el día que se descubra una vulnerabilidad se estará expuesto por un servicio que no se ha usado nunca.
- Limitación de la ejecución de programas tanto manualmente como automáticamente. Muy parecido al punto anterior. Tener instalado un programa que no se usa puede abrir una puerta para posibles incidentes en un futuro.
- Tener muy claro las políticas de actualizaciones y parches. Es importante tener en cuenta no sólo a los sistemas operativos, también las aplicaciones y los firmware.
- Hay que asegurarse de que todas las comunicaciones, tareas de administración remota, etc. usen canales seguros HTTPS, SSL, IPSEC.
- Crear imágenes de los sistemas y almacenar fuera del entorno que podría resultar dañado. Es una forma rápida de recuperar un sistema.

5.4. Arquitectura en SCI.

En los últimos años las arquitecturas de los SCI ha sufrido grandes variaciones, desde los primeros sistemas monolíticos en que no existía seguridad, hasta las arquitecturas más modernas que han heredado muchos de los sistemas y sensores de las TI.

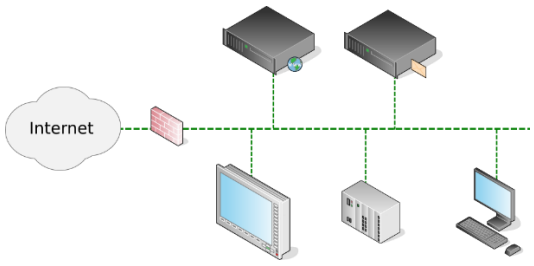


Ilustración 28 : Arquitectura primeros SCI

En esta arquitectura no existe ninguna medida de seguridad, estas arquitecturas se usaban a finales de los 90. Internet se conectaba al switch y todos los equipos. Además estas arquitecturas tenían la

problemática de que se generaba un gran tráfico por parte de los SCI que se compartía con el tráfico generado en oficinas. No eran muy seguras, ni eficientes. Una evolución posterior consistió en añadir entre el acceso a Internet y la red, por lo menos un cortafuegos (Ilustración 29). En estos sistemas no se monitorizaba nada, así que se podían vulnerar las políticas de seguridad del cortafuegos o de algún equipo de la red, sin que se detectara.

Las nuevas arquitecturas sectorizan y están pensadas para realizar una defensa por capas. No existe nunca un sistema 100% seguro, pero la defensa por capas ha demostrado ser más eficaz, separando zonas mediante cortafuegos.

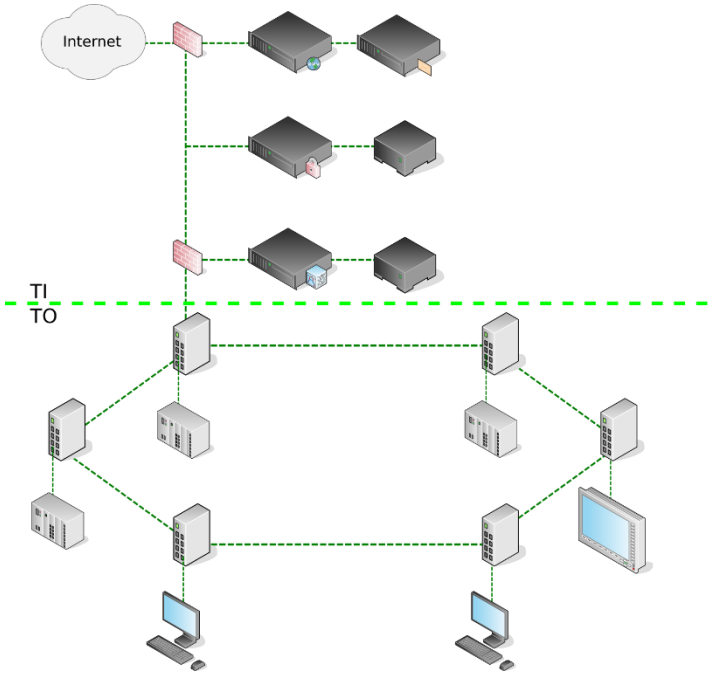


Ilustración 29: Arquitectura avanzada SCI. Fuente “Diseño y configuración de IPS,IDS y Siem en SCI”. Incibe.

Al estar sectorizado es más fácil la integración de sensores para IDS/IPS o SIEM. La idea principal es ir añadiendo barreras para dificultar el ataque, muchas veces además de su función defensiva tiene una función disuasoria, dado que para ir superando todos los obstáculos el coste de tiempo y recursos se incrementa, con lo que el coste del ataque aumenta. Usando la defensa por capas:

- Se dificulta el reconocimiento de redes y sistemas de las capas más profundas.
- Se añade un coste económico y temporal al ataque.
- Mejora la ubicación de sensores en diferentes capas que alertaran de anomalías.

La configuración de los equipos es diferente. Por un lado conforme en esta arquitectura los equipos tienen menos capas hasta Internet, por ejemplo la parte más próxima que sólo dispone de un cortafuegos, debe disponer de un bastionado mayor. Los equipos más profundos, que son los equipos del SCI que suelen ser equipos más difíciles de bastionar aprovechan esta profundidad como

protección, se deberán pasar por más medidas de seguridad para llegar a ellos. Estos equipos, como hemos comentado con anterioridad, reciben parches de seguridad más tarde, son equipos más antiguos, etc.

5.4.1. Defensa en profundidad.

La defensa de los SCI necesita garantizar la disponibilidad, mucho más que la confidencialidad de la información como sucede en los TI. Pese a todo cada vez más los entornos TO requieres y usan servicios de TI. Como principios básicos independientemente de los comentados en el apartado 5.2.2 serian:

- Usar cifrados y firmas digitales siempre que sea posible.
- Segregar redes y dispositivos.
- Implementar algún sistema IDS, IPS o SIEM.
- Realizar labores de pentesting.
- Implementar medidas de seguridad física.

Una estrategia de defensa en profundidad incluirá la creación de DMZ, algún sistema de detección de intrusos y sobretodo mecanismos de monitorización y alerta. Recordemos que no sirve de nada la instalación más protegida si nadie se entera cuando sucede una alerta.

Las capas en una estrategia de defensa en profundidad son:

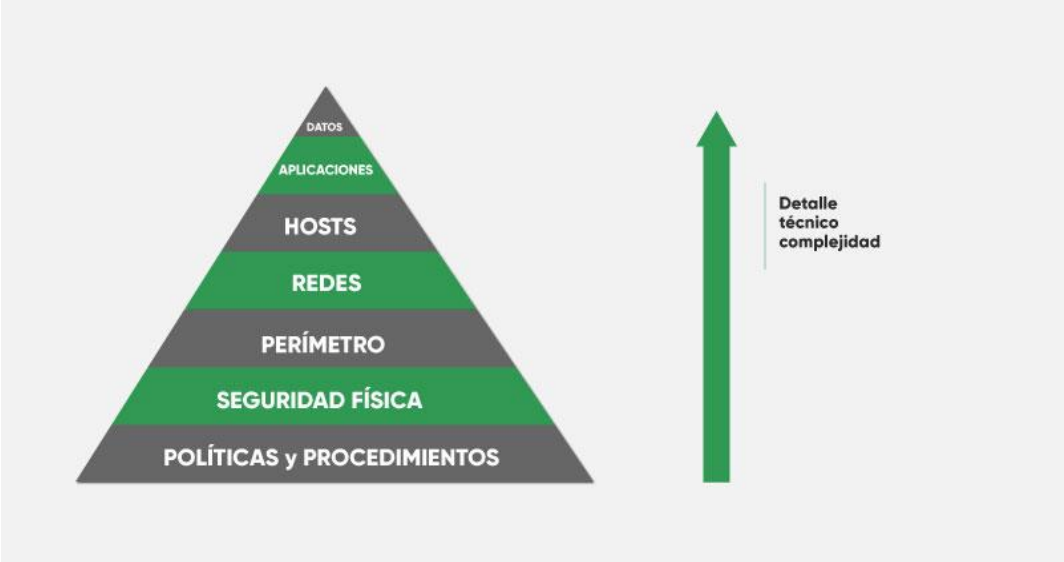


Ilustración 30 : Capas defensa en profundidad. Fuente Logitek.

- Políticas y procedimientos: Reglas que se establecerán para el funcionamiento del SCI.
- Seguridad física: Barreras para evitar el acceso físico a sistemas sin la debida autorización.
- Perímetro: Aseguramiento del acceso desde el exterior al SCI.

Protección en infraestructuras críticas. Análisis de seguridad en los sistemas de control industrial.

- Redes: Implementación de sistemas de detección de intrusos y detectar lo antes posible su acceso.
- Hosts: Implementación de las medidas para fortificación y bastionado de equipos.
- Aplicaciones: Uso de mecanismos de autenticación para el acceso a equipos con aplicaciones y perfiles dentro de la aplicación.
- Datos: Si se han conseguido superar todas las capas un sistema de cifrado evitara que los datos sean fácilmente accesibles.

Como complemento a la arquitectura los factores a tener en cuenta en la fortificación del perímetro y redes son:

- Control de todo el tráfico entrante y saliente.
- Control de todos los accesos VPN, lo ideal es doble factor de autenticación.
- Control de todas las aplicaciones y registro de la navegación web.
- Uso de sistemas IDS o IPS y de detección de malware.
- Gestión centralizada.

5.4.2. Sistemas IDS

Es el encargado de detectar y monitorizar los que sucede dentro de la red. Con esta información, además, previene ataques y analiza cómo se ha producido un ataque. Los IDS usan cuatro informaciones para realizar esto: Histórico de eventos de la red, configuración actual del sistema, procesos activos y reglas. Para recoger estos datos se usan sensores. Lo sensores no son más que puntos de una red donde se escucha el tráfico en busca de comportamientos extraños o patrones. Estos comportamientos anómalos generalmente al igual que las firmas de los antivirus se pueden generar o descargar. Por ejemplo, el IDS Snort es un sistema escalable en el que se puede insertar reglas nuevas que se ajusten a la arquitectura de sistema o para amenazas nuevas detectadas.
La misión principal que tendrán será:

- Prevención: Detectando patrones y comportamientos anómalos. Incluso ataques para los que no se ha creado reglas, pueden ser detectados por su comportamiento.
- Reacción: Se avisa al detectar estos comportamientos extraños.

El principal problema es que los avisos no siempre son 100% reales, se pueden encontrar falsos positivos e incluso ataques que no saltan ninguna alarma. Los IDS se clasifican por enfoque, origen de datos, estructura y comportamiento.

Por su enfoque:

Detección de anomalías: Basado en el aprendizaje de lo que es normal en el sistema, detecta comportamientos fuera de esa normalidad. Depende de cómo se haga ese aprendizaje será más eficaz o menos. Esas anomalías las detecta mediante:

- Sistemas basados en conocimiento: Detecta los ataques mediante las reglas introducidas. Nada que no esté en una regla será considerado ataque. No detecta ataques nuevos, salvo los que están basados en ataques viejos.
- Sistemas basados en métodos estadísticos: Analiza el comportamiento de los usuarios en entornos como sistemas y redes para crear unas métricas que usarán en la detección de patrones anómalos.
- Sistemas basados en aprendizaje automático. Analiza los comportamientos pero va, a su vez, aprendiendo de situaciones nuevas. Genera firmas nuevas de los acontecimientos.

Detección de usos: Hace un análisis del uso de recursos para, mediante reglas, detectar actividades que coincidan con una actividad maliciosa. Pueden ser:

- Sistemas expertos: Conjunto de condiciones que llevan asociada una acción.
- Detección de firmas: Comparación con conjuntos de acciones. Este conjunto de acciones que han producido una actividad maliciosa son las firmas.
- Análisis de transición de estados: Representación de la actividad maliciosa como una máquina de estados. Dificultad de decisión en caso de que la actividad no se desarrolle en el mismo orden.

Híbridos. Mezcla de ambos. Opera como los dos tipos de detecciones por anomalías y por usos.

Origen de datos:

- NIDS (Netword Intrusion Detection System): sistema que trabajara en modo promiscuo para escuchar todas las comunicaciones de su segmento de red, analizando el tráfico en tiempo real. Según en qué segmento se realice el ataque puede no detectarlo.
- HIDS (Host Intrusion Detection System): estos sistemas operan solamente en máquinas. Por lo tanto, trabaja en las actividades de servicios y usuarios dentro de una máquina determinada para la detección de actividades maliciosas.
- Híbridos: Mezcla de ambos. Se encarga de recoger datos de red y del sistema, para una mejor detección de actividades maliciosas.

Estructura:

- Centralizados. Se instalan sensores por la infraestructura en pocos nodos que envían los datos a un equipo central que realiza el control. Se da una visión más local al no alcanzar la totalidad de la infraestructura.
- Distribuidos. Dispone de diversos sensores distribuidos por la infraestructura. Estos envían información a un sistema que recoge toda la información, ofreciendo así una visión global de un ataque.

Protección en infraestructuras críticas. Análisis de seguridad en los sistemas de control industrial.

Comportamiento:

- Activos: Escucha el tráfico de red en búsqueda de actividades maliciosas pero también puede hacer funciones de cortafuegos, bloqueando determinados paquetes. Un IDS de comportamiento activo es un IPS.
- Pasivos: Uso del modo promiscuo para permanecer a la escucha sin generar ningún tráfico. Sólo generan alertas en caso de detección de actividad maliciosa.

5.4.3. Sistemas IPS.

Se podría hacer el símil de que un IPS es la mezcla de un IDS y un cortafuegos. Tiene la capacidad de detectar tramas de actividades maliciosas y además bloquear esas tramas para que no lleguen a su destino. Los IPS tienen capacidad de analizar el contenido del paquete. Las características que tienen son:

- Capacidad de acción en base al contenido de la trama.
- Bloqueo de ataques en tiempo real.
- Reduce las falsas alarma al hacer un análisis más exhaustivo.
- Capacidad de actualización con nuevas reglas.

Los IPS los podemos clasificar como:

- HIPS, Host IPS: solamente actúan a nivel de un host. Sólo protegen ese equipo.
- NIPS, Network IPS: trabajan en toda la red para analizar el tráfico y buscar comportamientos sospechosos.
- WIPS, Wireless IPS: monitorizan las redes inalámbricas para analizar el tráfico y buscar comportamientos sospechosos.
- NBA, Network Behavior Analisys: analizan el tráfico para detectar amenazas que generan un tráfico inusual.

La elección del IPS a utilizar dependerá del alcance de la monitorización. Un HIPS no sirve para detectar amenazas en la red, pero sí detecta amenazas en un host, incluso cifradas. Sin embargo, un NIDS detecta amenazas en diferentes partes de una red, pero es más lento en su detección y transmisión de sus hallazgos.

5.4.4. Sistemas SIEM (Security Information and Event Management – Gestor de eventos e información de seguridad.)

Conocidos también como SEM (Security Event Management) o SIM (Security Information Management), los SIEM son una combinación de ambos. Sus principales capacidades son la recopilación de información de diversas fuentes, el análisis de la misma y la presentación de esa

información de la forma más comprensible posible a la hora de tener que tomar una decisión. Las fuentes de información pueden ser:

- Aplicaciones de gestión de identidades, accesos o servicios de directorio.
- Gestores de vulnerabilidades.
- Eventos de sistemas operativos.
- Eventos de bases de datos.
- Datos de amenazas externas.
- Logs.
- Instrumentos de políticas de cumplimiento.

Deben tener la capacidad de recopilar y analizar en tiempo real la información. A la hora de implantar un SIEM en un entorno industrial hay que tener en cuenta que es un proceso largo, que requiere de una gran planificación y conocimiento del sistema sobre el que se va a integrar. Por lo tanto, hay varios factores a tener en cuenta a la hora de integrarlo en un SCI.

- Conocer la red y todos los protocolos de comunicación que se vayan a usar.
- Es más fácil la integración separando el SIEM en un SEM, que tendrá la capacidad de detección de eventos en tiempo real y un SIM el que va a recopilar los datos proporcionados por las diversas fuentes.
- Detectar qué elementos hay que proteger. Identificar los activos.
- Hay que normalizar la información desde las distintas fuentes y configurar qué se hace con las fuentes de información, cómo se almacenarán los datos y qué será considerado un incidente.

5.4.5. Arquitectura con sensores IDS/IPS/SIEM.

Una vez se ha establecido la política de seguridad por capas y se ha diseñado una arquitectura, se debe elegir qué sistemas de detección o prevención de intrusos se integrarán. De acuerdo a esta elección se colocarán determinados sensores. Los sensores no son más que fuentes de información que notifican actividades sospechosas y generan alertas.
Un ejemplo de arquitectura con 2 cortafuegos y sensores para IDS/IPS/SIEM puede ser la de siguiente ilustración.

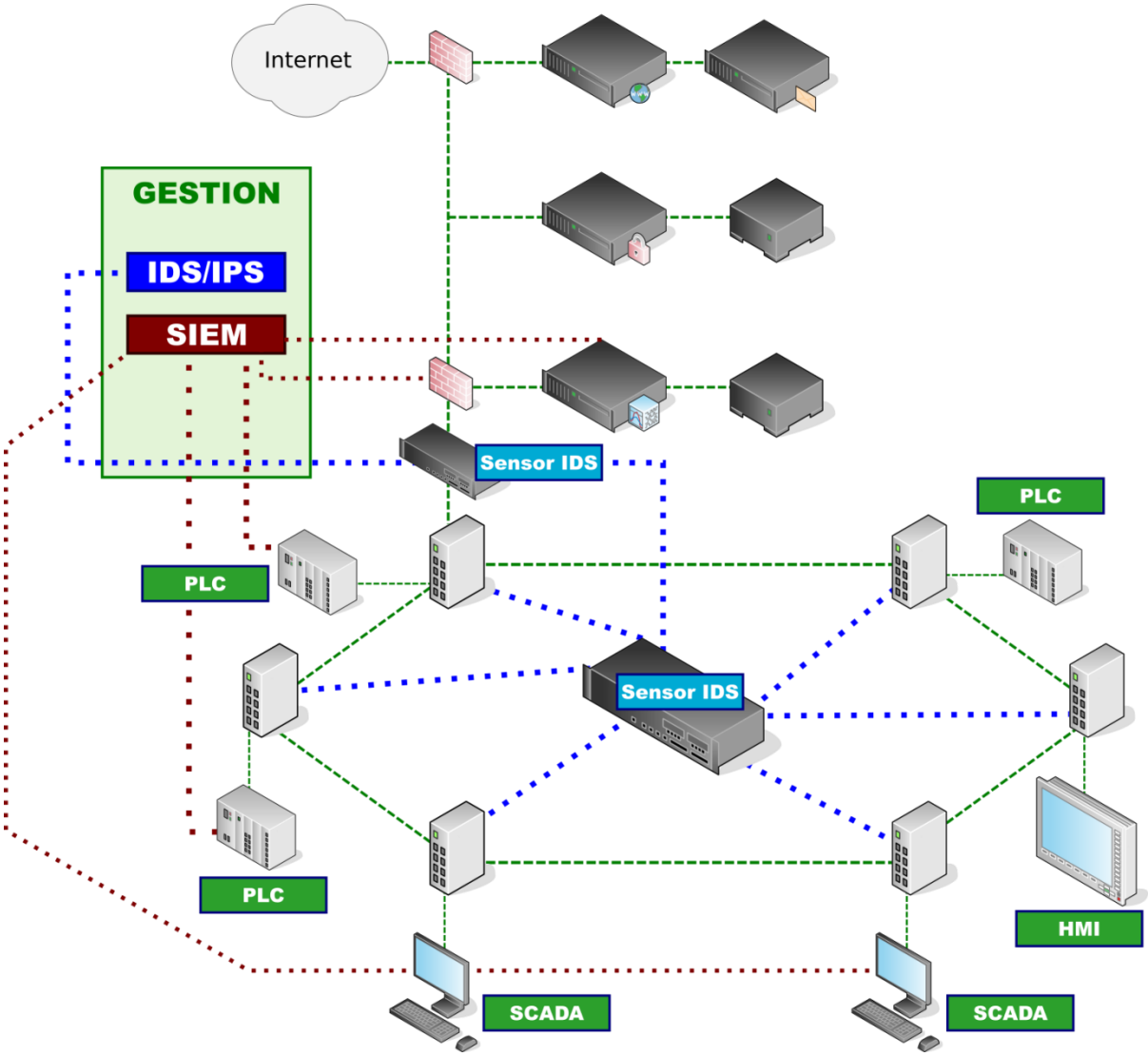


Ilustración 31 : Ejemplo Arquitectura con sensores IDS/IPS/SIEM. Fuente “Diseño y configuración de IPS,IDS y Siem en SCI”. Incibe.

De forma conjunta recogeremos la información de IDS/IPS/SIEM, se instalarán sensores IPS en el anillo de FO del SCI y en la entrada al SCI después del cortafuegos, con el objetivo de monitorizar comportamientos maliciosos que se pudieran saltar reglas del cortafuegos. Se recogerán en SIEM datos de PLC, HMI y SCADA, aparte de los historian si los hubiese. Toda esta información se recogerá para tomar acciones en caso de que el sistema se viera comprometido.

5.5. Restablecimiento de actividad.

Es imposible tener controlados el 100% de los riesgos, aun así cualquier tipo de incidencia puede suceder. Se puede tener un sistema muy robusto a nivel de ciberseguridad, pero sufrir un incendio o un fallo en un disco duro. Por lo tanto, una de las partes dentro de la securización de un SCI es planificar que puede pasar lo inevitable y prepararse para ello. Es importante que se establezca una política de

copias de seguridad o restablecimiento de sistemas. En los SCI nos encontraremos con dos posibles escenarios: equipos que hacen la función de HMI y que una vez en marcha no almacenan ningún tipo de información, haciendo de interface con planta, y equipos en los que se guarda algún dato del proceso. La política de copias de seguridad es diferente para ambos. Mientras en el primer caso será suficiente con realizar una imagen de disco que habrá que renovar en el momento en que se instale un parche o actualización, sin requerir continuamente un backup, en el segundo caso se tiene que determinar el período entre copias de seguridad y realizar backup tanto del sistema como de los datos. Como regla general aplicaremos varios principios a la hora de la elaboración de copias de seguridad o imágenes.

- Se deben garantizar que los procedimientos de copia de seguridad y restauración funcionan adecuadamente. Se dan muchos casos en los que a la hora de restaurar una copia de seguridad, ésta no funciona.
- Se comprobará regularmente el estado de las mismas. Lo ideal es realizar una restauración completa.
- Se usarán diferentes ubicaciones para guardar las copias de seguridad. Preferiblemente alguna en una segunda ubicación para, en caso de incidente grave, poder recuperarla.
- Siempre que sea posible el transporte a estas ubicaciones se realizará de forma segura o por valija.

5.5.1. Política de copias de seguridad.

A la hora de elegir las políticas de copias de seguridad habrá que elegir entre:

- Total. Copia todos los datos marcados para hacer backup, dentro del disco y particiones. Tiene un elevado coste temporal y de espacio, lo que implica que no se puede hacer con una frecuencia elevada.
- Diferencial. Es una copia incremental en el que el nivel de actualización se basa en la anterior copia de seguridad. Todo lo que haya cambiado desde el último backup se vuelve a almacenar.
- Incremental. Basada en diferentes niveles en los que aplicamos cuánto tiempo pasa desde la última copia. Por ejemplo, un nivel 1 sería un backup diferencial, un nivel 2 sería una copia de seguridad respecto a lo que cambió hace 2 días.

Como regla general, para equipos en los que se genere un volumen de datos considerable, una recomendación seria:

- Copia total una vez a la semana. Preferiblemente en horarios donde la carga de trabajo sea menor.

- Copia diferencial cada noche. Lo que reducirá considerablemente el volumen de información esas noches. El inconveniente es que la recuperación implicará recuperar primero la copia total y posteriormente las copias diferenciales de cada día.

Se debe planificar también:

- Medios usados para las copias: discos externos, DVD, cintas backup.
- Horarios para realizarlas.
- Tiempo que se almacenarán las copias. Ejemplo: un mes de backup, cuatro juegos de cintas backup de 7 cintas cada una: 1 total + 6 incrementales. Lo que hace un total de 28 cintas.

Como se ha comentado con anterioridad, es importante comprobar que los backup realizados funcionan, pero además de comprobar que se hace bien, también se tendrá en cuenta el tiempo de recuperación de un sistema, sobre todo cuando se trata de infraestructuras críticas que se tengan que recuperar rápidamente.

Otra alternativa podría ser la creación de imágenes. En este proceso el principal problema es que el equipo tiene que estar parado para poder realizarlo. Por contra realiza un clonado sector a sector del disco duro. Por lo tanto, es solo recomendable en sistemas que no registren datos como cliente SCADA. Pero ante cualquier actualización de sistema operativo (parcheo o actualización drivers) implicaría tener que volver a repetir el proceso.

6. CONCLUSIONES.

En los últimos años, la evolución en materia de ataques informáticos ha sido muy considerable. Hemos pasado de ataques realizados por jóvenes utilizando pocos recursos, al uso de sofisticadas herramientas de ataque, preparadas para un objetivo concreto. Un ejemplo de ello es el de Stuxnet, que conllevó un coste elevado y que fue desarrollado por un servicio de inteligencia. En muchos de estos ataques el objetivo era claro y para tal fin se trabajó durante mucho tiempo en la recopilación de información para su preparación.

El hecho de que estos ataques sean tan elaborados, ha obligado a tomar medidas ya desde las fases de diseño de cualquier infraestructura o sistema de control. Es por eso que en este documento se recogen medidas de securización, tanto desde las fases del diseño, ciclo de vida y restablecimiento del sistema.

Además, se han definido unas pautas que son básicas en la implantación de la seguridad en un SCI, que, aunque puedan parecer de sentido común, hoy en día continúan sin aplicarse en la mayoría de los casos. Se ha expuesto un ejemplo de cómo debería ser una arquitectura segura, en la que se integren todas las capas del modelo ISA95, desde las que formen parte de las TO, a las que formen parte de las TI, ya que cada vez se parecen más los SCI a sistemas de las TI. El objetivo de exponerlo así ha sido porque, en muchos casos, los SCI son diseñados y programados por ingenieros del mundo de las TO, con menos experiencia en estos tipos de arquitecturas. En la arquitectura segura, además, se han añadido los sensores para sistemas como IDS, IPS o SIEM, que aportan la capacidad de detectar comportamientos sospechosos.

Pese a todo, es imposible dotar a cualquier sistema de una protección 100% fiable ante posibles ataques. Por eso mismo, en la última parte del documento se han detallado las formas de restablecimiento de un sistema, con el objetivo de recuperar los sistemas dañados en el menor tiempo posible.

Como conclusión final, después de analizar los casos de ataques más relevantes de los últimos años, podemos decir que un porcentaje elevado de incidentes se podrían haber evitado si se hubieran tenido en cuenta algunas de las medidas básicas de protección. Medidas como la adecuada formación del personal para evitar phishing con código dañino, políticas de gestión de usuarios para quitar privilegios, el cambio periódico de contraseñas, o la monitorización de redes y equipos para detectar actividad ilícita, hubieran reducido considerablemente el número de ataques. Es necesario que las empresas y los responsables de IC tomen conciencia de la importancia de invertir en seguridad y apliquen medidas para evitar posibles ataques que vulneren sus infraestructuras y afecten incluso a la seguridad de un país.

Bibliografía

Blog Incibe-Cert (15 de Septiembre de 2015). https://www.incibe-cert.es/blog/amenazas-sci , "*Amenazas en SCI",* consultado Noviembre 2019.

Blog Incibe-Cert https://www.incibe-cert.es/blog/dispositivos-extraibles-entornos-industriales-amenazas-y-buenas-practicas , "Dispositivos extraíbles en entornos industriales" , consultado en Noviembre 2019.

Blog Incibe-Cert. (26 de Marzo de 2019). https://www.incibe.es/protege-tu-empresa/blog/erp-desactualizado-incidente-asegurado "ERP desactualizado, incidente asegurado", consultado Octubre 2019.

Blog Incibe-Cert. (01 de Abril de 2019). https://www.incibe-cert.es/blog/operacion-sharpshooter-ciberataques-dirigidos-infraestructuras-criticas , *" Operación sharpshooter"* , consultado Noviembre 2019.

Blog Incibe-Cert. (17 de Enero de 2019). https://www.incibe-cert.es/blog/seguridad-industrial-2018-cifras "*Seguridad Industrial 2018 en cifras"*, consultado Octubre 2019.

Blog Incibe-Cert. (18 de Enero de 2018). https://www.incibe-cert.es/blog/seguridad-industrial-2017-cifras "*Seguridad Industrial 2017 en cifras"*, consultado Octubre 2019.

Blog Incibe-Cert. (26 de Septiembre de 2019). https://www.incibe-cert.es/blog/vulnerabilidad-aurora-origen-explicacion-y-soluciones. *" Vulnerabilidad Aurora"* , consultado Noviembre 2019.

Centro Criptológico Nacional. (2019). "Ciberamenazas y tendencias 2019. Resumen Ejecutivo".

Centro Criptológico Nacional. (2010). https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/209-ccn-stic-480a-seguridad-en-sistemas-scada-guia-de-buenas-practicas/file.html , *"Seguridad en el control de procesos y Scada. Guía de buenas practicas"* , consultado Noviembre 2019.

Centro Criptológico Nacional. (Mayo 2019). "Informe Ciberamenazas y tendencias. Edición 2019."

Centro de Ciberseguridad Industrial (CCI). (Octubre 2013). "*La protección de IC y la ciberseguridad industrial."*

Check Point Research. (Julio 2018). https://research.checkpoint.com/wp-content/uploads/2018/07/Cyber-Attack-Trends-2018-Mid-Year-Report.pdf *,"Cyber Attack Trends 2018 Mid" consultado Octubre 2019.*

Ciberseguridad Industrial by Logitek. (Noviembre 2019) https://www.ciberseguridadlogitek.com/estrategia-de-defensa-en-profundidad-en-ciberseguridad-industrial/ , "Estrategia de Defensa en profundidad en ciberseguridad industrial", consultado Noviembre 2019.

Ciberseguridad Industrial by Logitek. https://www.ciberseguridadlogitek.com/propuesta-en-ciberseguridad/soluciones-para-la-fortificacion-basadas-en-la-defensa-en-profundidad/ , *"Soluciones para la fortificación basadas en la defensa en profundidad*", consultado Noviembre 2019.

Escuela Superior del Ejercito (Peru). http://esge.edu.pe/ciberseguridad-en-la-infraestructura-crítica-mediante-el-sistema-scada-en-planta-de-tratamiento-de-agua-de-lima/ , *"Ciberseguridad en IC mediante Scada en planta de tratamiento de aguas" ,* consultado Noviembre 2019.

Francisco Bolivar, Juan. (2019) "Infraestructuras críticas y sistemas industriales". Ed.0XWord.

Friginal López, Jesus, Martínez Rega Miquel. *"Cibercamp Amenzanas en sistemas Scada de 4ª Generación"* Publicado INCIBE.

GlobbSecurity. https://globbsecurity.com/ciberataque-red-electrica-israeli-37626/ , *"La red electrica israelí sufre un ciberataque masivo que deja inoperativos sus sistemas"* , Consultado Noviembre 2019.

Herrero Collantes, Miguel , López Padilla Antonio. *"Protocolos y seguridad de red en infraestructuras SCI"*. Publicado INCIBE.

Info PLC. (Marzo 2017). https://www.infoplc.net/blogs-automatizacion/item/104093-top-10-empresas-automatizacion-2017 , *"Top 10 empresas de automatización en 2017"* , consultado Octubre 2019.

Karpesky.
https://www.kaspersky.es/about/press-releases/2017_zero-day-attacks-and-ransomware-on-the-rise-this-has-been-the-second-quarter-apt-of-2017 , *"Ataques dia 0 y ramsonware",* consultado Noviembre 2019.

Karpesky.
https://media.kaspersky.com/es/business-security/enterprise/kl-industrial-cybersecurity-for-energy.pdf , *"Ciberseguridad para infraestructuras eléctricas"* , consultado Noviembre 2019.

Nacked Security.
https://nakedsecurity.sophos.com/es/2013/02/09/bit9-hacked-used-to-inject-malware-into-customers-networks/ , "bit 9 Hackeado", consultado Noviembre 2019.¡

National Instruments. (17 de Septiembre de 2019).
https://www.ni.com/es-es/innovations/white-papers/14/the-modbus-protocol-in-depth.html , *"Información detallada del protocolo Modbus"* , consultado Noviembre 2019.

Panda Antivirus.
https://www.pandasecurity.com/spain/mediacenter/src/uploads/2018/10/1611-WP-InfraestructurasCríticas-ES.pdf , *"Infraestructuras críticas"*, consultado Noviembre 2019.ó

Siemens Automation. https://mall.industry.siemens.com/mall/es/WW/Catalog/Products/10016018 , *"Simatic Batch"* , consultado Octubre 2019.

Universitat de València. https://www.uv.es/rosado/courses/sid/Tema3_Profibus_transp.pdf , *"Sistemas Industriales Distribuidos. Profibus"* , consultado Noviembre 2019.

Welivesecurity.
https://www.welivesecurity.com/la-es/2016/01/05/troyano-blackenergy-ataca-planta-energia-electrica-ucrania/ , *"El troyano BlackEnergy ataca a una planta de energia electrica en Ucrania"*, consultado Noviembre 2019.

Wikipedia. https://es.wikipedia.org/wiki/Ataques_ransomware_WannaCry , *"Ataque ramsonware WannaCry"* , consultado en Noviembre 2019.

Wikipedia. https://es.wikipedia.org/wiki/Customer_relationship_management , "Customer relationship management", consultado Noviembre 2019.

Wikipedia. https://es.wikipedia.org/wiki/IEC_61131-3 , *"IEC 61131-3"*, consultado Octubre 2019.

Wikipedia. https://es.wikipedia.org/wiki/Lenguaje_ladder , *"Lenguaje Ladder"*, consultado Octubre 2019.

Wikipedia. https://es.wikipedia.org/wiki/Manufacturing_Execution_System , *"MES"*, consultado Octubre 2019.

Wikipedia. https://es.wikipedia.org/wiki/OPC , "OPC" , consultado Noviembre 2019.

Wikipedia. https://en.wikipedia.org/wiki/SCADA, *"Scada"* , consultado Octubre 2019.

Wikipedia.
https://es.wikipedia.org/wiki/Sistema_de_planificaci%C3%B3n_de_recursos_empresariales ,
"Sistemas de planificación de recursos empresariales" , consultado Octubre 2019.

Anexos

Anexo A: Glosario

A

APT – Advanced Persistence Threat – Ataques avanzados persistentes

AWL - Anweisungsliste (en Aleman) – Lista de Instrucciones.

C

CEO – Chief Executive Officer – Jefe Oficial Ejecutivo.

CI – Ciberseguridad Industrial – Conjunto de herramientas que buscan garantizar disponibilidad, integridad y confidencialidad en un sistema de control industrial o infraestructura crítica.

CWE – Common Weakness Enumeration – Enumeración común de debilidades.

CRM – Customer relationship management – Gestión de relaciones con los clientes.

D

DCS – Distributed Control System – Sistema de control distribuido.

DMZ – Zona Desmilitarizada.

DoS – Denied of Service – Ataque consistente en interrumpir un servicio.

E

ENISA – European Network and Information Security Agency - Agencia Europea para la ciberseguridad.

ERP – Enterprise Resource Planification – Planificación de recursos empresariales.

F

FUP - Funktionsplan – Diagrama de funciones usado en SCI de Siemens. (Alemán)

H

HMI – Human Machine Interface – Interface Hombre Maquina.

Honeypot – Tarro de Miel – Trampa digital que actúa como sistema vulnerable para detectar ataques.

I

IEC – International Electrotechnical Commission. Comisión internacional Electrotécnica.

IL – Instruction List – Lista de instrucciones.

IoT – Internet of Things – Internet de las cosas. Concepto que se refiere a la capacidad de conexión de objetos cotidianos.

IIoT – Industrial Internet of Things – Internet industrial de las cosas. Concepto de industria avanzada en que se incorporara la IA y el bigdata en la industria, para mejorar procesos y detectar problemas o ineficiencias.

IDS – Intruder Detection System – Sistema de detección de intrusos.

IoC – Indication Of Compromise – Indicadores de compromiso. Trazas observadas en una red o sistema operativo que pueden indicar una intrusión informática.

IPS – Intrusion Prevention System – Sistema de Prevención de Intrusos.

Protección en infraestructuras críticas. Análisis de seguridad en los sistemas de control industrial.

K

KOP: Kontakplan , diagrama de contactos en SCI de marca Siemens. (Alemán)

L

LD: Ladder , diagrama de contactos en SCI.

M

Malware: Software dañino.

MES: Manufacturing Execution System

MitM – Man in the Middle. Ataque basado en la interceptación o modificación de mensajes, colocándose el atacante entre 1 o varias víctimas.

P

PAC: Programmable Automation Controller , PLC de capacidades avanzadas.

PCS: Sistema de control de procesos.

Phishing: Suplantación de identidad, técnicas que permiten aparentar ser otra persona o entidad.

PLC: Programmable Logic Controller , controlador lógico programable.

PV: Process Value – Valor de proceso, el valor de una magnitud.

R

Ransonware - Software maliciosa que impide el acceso a datos del ordenador de la víctima. Y solicita un rescate para su devolución.

RAT – Remote Access Tool – Herramientas de Acceso Remoto.

S

SCADA – Supervision Control And Data Adquisition

SIEM – Security Information and Event Management – Gestor de eventos e información de seguridad.

SOC-OT – Security Operation Center – Operation Technologies

T

TI – Tecnologías de la información – IT – Information Technologies.

TO - Tecnologías de la operación. OT – Operation Technologies.

W

WEF – World Economic Forum – Foro económico mundial.