Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

SEGURIDAD EN LOS SISTEMAS DE CONTROL INDUSTRIAL

María Lorena Rizzo López
Asesorado por el Ing. Luis Enrique Lima Guzmán

Guatemala, enero 2021

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

SEGURIDAD EN LOS SISTEMAS DE CONTROL INDUSTRIAL

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

MARIA LORENA RIZZO LOPEZ
ASESORADO POR EL ING. LUIS ENRIQUE LIMA GUZMAN

AL CONFERÍRSELE EL TÍTULO DE

INGENIERA ELECTRÓNICA

GUATEMALA, ENERO 2021

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANA	Inga. Aurelia Anabela Cordova Estrada
VOCAL I	Ing. José Francisco Gómez Rivera
VOCAL II	Ing. Mario Renato Escobedo Martínez
VOCAL III	Ing. José Milton de León Bran
VOCAL IV	Br. Christian Moisés de la Cruz Leal
VOCAL V	Br. Kevin Vladimir Armando Cruz
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Julio González Podszueck
EXAMINADOR	Ing. Enrique Ruiz Carballo
EXAMINADOR	Ing. Juan Carlos Cordova
EXAMINADOR	Ing. Julio Cesar Solares
SECRETARIO	Ing. Francisco Javier González López

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que estable la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

SEGURIDAD EN LOS SISTEMAS DE CONTROL INDUSTRIAL

Tema que me fuera asignado por la dirección de la Escuela de Ingeniería Mecánica Eléctrica con fecha 15 de enero de 2020.

María Lorena Rizzo López

Guatemala 15 de junio de 2020.

Ingeniero
Julio Solares
Coordinador del Área de Electrónica
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería USAC

Estimado Ingeniero Solares:

De la manera más atenta me dirijo a usted, para comunicarle que he revisado el proyecto de tesis **"SEGURIDAD EN LOS SISTEMAS DE CONTROL INDUSTRIAL."**, presentado por la estudiante **María Lorena Rizzo López** con el número de carné 1987-11813. Puedo concluir que este trabajo llena los requisitos y cumple con los objetivos propuestos para su desarrollo e implementación de su anteproyecto de tesis. Dando mí visto bueno para que proceda a realizar los trámites correspondientes.

Por tanto, el autor de esta tesis y yo como su asesor, nos hacemos responsables por el contenido y conclusiones de la misma.

Sin otro particular me suscribo como su seguro servidor.

Ing. Luis Enrique Lima Guzmán. MSc.

Colegiado 3653.

Ing. Luis Enrique Lima Guzmán. MSc.
Colegiado 3653.

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

Guatemala, 9 de julio de 2020

Señor Director
Armando Alonso Rivera Carrillo
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería, USAC

Estimado Señor Director:

Por este medio me permito dar aprobación al Trabajo de Graduación titulado **SEGURIDAD EN LOS SISTEMAS DE CONTROL INDUSTRIAL,** desarrollado por la estudiante **María Lorena Rizzo López,** ya que considero que cumple con los requisitos establecidos.

Sin otro particular, aprovecho la oportunidad para saludarlo.

Atentamente,

ID Y ENSEÑAD A TODOS

Ing. Julio César Solares Peñate
Coordinador de Electrónica

ESCUELA DE INGENIERÍA MECÁNICA ELÉCTRICA
FACULTAD DE INGENIERÍA
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

REF. EIME 257.2020.

El Director de la Escuela de Ingeniería Mecánica Eléctrica, después de conocer el dictamen del Asesor, con el Visto Bueno del Coordinador de Área , al trabajo de Graduación de la estudiante María Lorena Rizzo López titulado: **Seguridad en los Sistemas de Control Industrial,** procede a la autorización del mismo.

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
FACULTAD DE INGENIERIA

Ing. Armando Alonso Rivera Carrillo

Guatemala, 6 de octubre de 2020.

Decanato
Facultad de Ingeniería
24189101- 24189102

DTG. 006.2021.

La Decana de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Eléctrica, al Trabajo de Graduación titulado: **SEGURIDAD EN LOS SISTEMAS DE CONTROL INDUSTRIAL,** presentado por la estudiante universitaria: **María Lorena Rizzo López,** y después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, autoriza la impresión del mismo.

IMPRÍMASE:

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANA
FACULTAD DE INGENIERÍA

Inga. Anabela Cordova Estrada
Decana

Guatemala, enero 2021.

AACE/asga

ACTO QUE DEDICO A:

Dios	Padre mío que me has bendecido y me has permitido alcanzar mis metas.
Mi Mamá	Marta Enoé López. Su amor será siempre mi inspiración.
Mi familia	Por ser una importante influencia en mi carrera y por su infinito amor.
Mis hermanos	Por su apoyo incondicional.
Mis Amigos	Yuri Urbina, Juan Carlos Córdova, Carlos Pérez, Valeri Cordón y Francisco Gressi, por su interminable amistad.

AGRADECIMIENTOS A:

Universidad de San Carlos de Guatemala	Por ser buena enseñanza durante los años de estudio.
Facultad de Ingeniería	Por darme la oportunidad de formarme como ingeniera.
Ing. Luis Lima	Por su paciencia y por sus consejos en el tiempo de dedicación al realizar esta tesis.

ÍNDICE GENERAL

INDICE DE ILUSTRACIONES

FIGURAS

TABLAS

LISTA DE SÍMBOLOS

Símbolo	Significado
ARP	*Address resolution protocol* / *p*rotocolo de resolución de direcciones
AMD	*Advanced micro devices*/ compañía de semiconductores
APT	*Advanced persistent threats* / amenaza avanzada persistente
ANSI	*American national standards institute* / instituto nacional estadounidense de estándares
ASME	*American society of mechanical engineers* / *s*ociedad americana de ingenieros mecánicos
ASCII	*American standard code for information interchange* / código estándar estadounidense para el intercambio de información
AT&T	*American telephone and telegraph* / multinacional de telefonía y telégrafos
AMS	*Asset management software* / software de gestión de activos
BYOD	*Bring your own device* / trae tu propio dispositivo
BIM	*Building information modeling* / modelo de construcción de información
CPU	*Central processing unit* / unidad central de proceso
CISO	*Chief information security officer* / *director* de la oficina de seguridad

CIO	*Chief Information officer* / oficial en jefatura
CPO	*Chief privacy officer* / ejecutivo de gestión de privacidad
CVE	*Common vulnerabilities and exposures* / vulnerabilidades y exposiciones comunes
CVSS	*Common vulnerability scoring system* / sistema de puntuación de vulnerabilidades comunes
CAFM	*Computer aided facility management* / gestión de Infraestructuras asistida por computadora
CERT	*Computer emergency response team* / equipo de respuesta ante emergencias informáticas
CIM	*Computer integrated manufacturing* / fabricación integrada por computadora
CNC	*Computer numerical control* / control numérico computarizado
CMMS	*Computerized maintenance management system* / sistema de gestión de mantenimiento computarizado
BCH	Códigos de Bose-Chaudhuri-Hocquenghem
CIP	*Critical infrastructure protection* / protección de infraestructura crítica
XSS	*Cross-site scripting* / secuencia de comandos
Bot	Cuentas falsas que suelen suplantar identidad
CPD	*Data center* / centro de procesamiento de datos
DMZ	*Demilitarized zone* / red de zona desmilitarizada
DoS	*Denial of service* / denegación de servicio
DHS	*Department of homeland security* / departamento de seguridad de EE. UU.
DHCP	*Dynamic host configuration protocol* / protocolo de configuración dinámica de host

DDC	*Direct digital controller* / control digital directo
DCOM	*Distributed component object model* / modelo de objetos componentes distribuidos
DCS	*Distributed control system* / sistema de control distribuido
Ddos	*Distributed denial of service* / ataque distribuido de denegación de servicio
DNP3	*Distributed network protocol 3* / protocolo de red distribuida versión 3
DNS	*Domain name system* / sistema de nombre de dominio
ERP	*Enterprise resource planning* / planeamiento de recursos empresariales
E/S	Entrada/salida
XML	*Extensible markup language* / lenguaje de etiquetas
FIPPS	*Fair information practices* / principios de prácticas de información justa
FTP	*File transfer protocol* / protocolo de transferencia de archivos
FBD	*Functional block diagram* / diagrama de bloques de funciones
GIS	*Geographic information system mapping* / sistema de información geográfica
HMI	*Human machine interface* / interfaz hombre máquina
HTTP	*Hypertext transfer protocol* / protocolo de transferencia de hipertexto
HTTPS	*Hypertext transfer protocol secure* / protocolo seguro de transferencia de hipertexto
IPE	Imagen de procesos de entradas

IACS	*Industrial automation and control system* / sistemas de automatización y control industrial
ICS	*Industrial control system* / sistema de control industrial
ISA	*Industry standard architecture* / arquitectura estándar de la industria
IT	*Information technology* / tecnología de la información
IEEE	*Institute of electrical and electronic engineer*/ Instituto de ingenieros eléctricos y electrónicos
IL	*Instructions list* / listado de Instrucciones
IED	*Intelligent electronic device* / dispositivo electrónico inteligente
ICCP	*Inter-control center communications protocol* / protocolo de comunicación entre centros de control
IEC	*International electrotechnical commission* / comisión electrotécnica internacional
ISO	*International organization for standardization* / organización internacional de estandarización
ICMP	*Internet control message protocol* / protocolo de mensajes de control de internet
IETF	*Internet engineering task force* / grupo de trabajo de ingeniería de internet
IP	*Internet protocol* / protocolo de Internet
Ipsec	*Internet protocol security* / seguridad de protocolo de internet
IDS	*Intrusion detection system* / sistema de detección de intrusiones
JPEG	J*oint photographic experts group* / extensión de archivos de imagen

LD	*Ladder diagram* / diagrama de escala
LAN	*Local area network* / red de área Local
MES	*Manufacturing execution system* / sistema de ejecución de fabricación
MIT	*Massachusetts Institute of Technology* / Instituto tecnológico de Massachusetts
MAP	*Mobile application part* / protocolo de fabricación automatizada
MIMO	*Multiple Input multiple output* / múltiple entrada múltiple salida
MTU	*Maximum transmission unit* / unidad de transmisión máxima
NCCIC	*National cybersecurity and communications Integration center* / centro nacional de integración de comunicación y seguridad cibernética
NIST	*National institute of standard and technology* / Instituto nacional de estándares y tecnología
NAT	*Network address translation* / traducción de direcciones de red
NERC	*North america electric reliability corporation* / consejo de fiabilidad de electricidad de América del Norte
OLE	*Object linking and embedding* / incrustación y enlazado de objetos
OMB	*Office of management and budget* / oficina de administración y presupuesto
OPC	*Open platform communications* / plataforma de comunicación Abierta

OPC-UA	*Open platform communications unified architecture* / plataforma de comunicación abierta- arquitectura unificada
OSI	*Open system interconnection* / interconexión de sistemas abiertos
OT	*Operational technology* / tecnología operacional
OEM	*Original equipment manufacturer* / fabricante de equipos originales
PC	*Personal computer* / computador personal
PIT	*Platform information technology* / Plataforma informática.
PIV	*Personal identity verification* / verificación de identidad personal
PDS	Plan director de seguridad
PLC	*Programmable logic controller* / controlador lógico programable
LUA	*Programming language* / lenguaje de programación multiparadigma
PID	*Proportional integral derivative control* / controlador proporcional integral derivativo
RMF	*Risk mangement framework* / marco de gestión de riesgo
RPO	*Recovery point objective* / punto de recuperación objetivo
RTO	*Recovery time objective* / objetivo de tiempo de recuperación
Web	Red de internet
RJ	*Registered jack* / clavija registrada
RCP	*Remote copy / copia remota*

RSH	*Remote shell* / protocolo de acceso remoto
RTU	*Remote terminal unit* / unidad terminal remota
SIS	S*afety instrumented system* / sistema instrumentado de seguridad
SIL	*Safety integrity level* / nivel de integridad de seguridad
SMS	*Safety management system* / sistema de gestión de seguridad operacional
SFC	*Sequence function chart* / tabla de la secuencia de las funciones
SCP	*Secure copy protocol* / copia de seguridad
SFTP	*Secure file transfer protocol* / protocolo seguro de transferencia de archivos trivial
SSH	*Secure shell* / protocolo cifrado seguro
SSL	*Secure sockets layer* **/** capa de socket seguros
SISO	S*imple input simple output* / entrada,salida única
SMTP	*Simple mail transfer protocol* / protocolo simple de transferencia de correo
SNMP	*Simple network management protocol* / protocolo simple de administración de red
SOAP	*Simple object access protocol* **/** protocolo simple de acceso a objetos
SDIC	*Software defined infrastructure control* / control industrial definido por software
SDN	*Software defined networking* / *r*edes definidas por software
SAN	*Storage area network* / red de área de almacenamiento
ST	*Structured text* / texto estructurado

SQL	S*tructured query language* / lenguaje de consulta estructurada
SCADA	*Supervisory control and data acquisition* / supervisión y control en adquisición de datos
TIC	Tecnología de la información y la comunicación
3PL	*Third party logistics* / servicio subcontratado de logística
TSN	*Time sensitive networking* / red sensible de tiempo
TFTP	T*ransfer file trivial protocol* / protocolo de transferencia de archivos trivial
TCP	*Transmission control protocol* / protocolo de control de transmisión
TCP/IP	*Transmission control protocol / internet-protocol* protocolo de control de transmisión / protocolo de internet
TLS	T*ransport layer security* / seguridad de la capa de transporte
URL	*Uniform resource locator* / localizador uniforme de recursos
UK	*United Kingdom* / Reino Unido
USB	*Universal serial bus* / bus serial universal
UDP	U*ser datagram protocol* / *p*rotocolo de datagramas del usuario
VLAN	*Virtual local area network* / red de área local virtual
VPN	*Virtual private network* / red privada virtual
VoIP	*Voice over internet protocol* / *v*oz a través de internet
WAN	*Wide area network* / red de área amplia

GLOSARIO

AggreGate	Plataforma en sistemas de información de seguridad física que cubre todos los aspectos de gestión de seguridad física de grandes empresas.
Bypass	Forma de esquivar un sistema de seguridad informático.
BOTNET	Red de bots, programa informático.
Bacnet	Protocolo de comunicación de datos.
Cookies	Archivo pequeño enviado por un sitio Web y almacenado en el navegador del usuario.
Conatel	Comisión nacional de telecomunicaciones, organismo regulador independiente.
Crackers	Piratas informáticos que logran penetrar en las redes e intentar el acceso a zonas reservadas.
Dongles USB	Pequeño dispositivo que se conecta a una PC a través de puertos paralelos y que permite conectar dos dispositivos.

Ethernet	Es un estándar de redes de área local creadas por la unión de varios ordenadores a través de cable.
Fisma	Ley federal de modernización de la seguridad de la información.
Firewall	Programa informático que controla el acceso a una computadora o red.
Gateway	En español, puerta de enlace. Es un dispositivo normalmente un ordenador, que actúa de interfaz de conexión entre redes con protocolos y arquitecturas de diferentes niveles de comunicación.
Hardware	Partes físicas de un sistema informático, sus componentes eléctricos, electrónicos, electromecánicos y mecánicos.
Hacker	Persona con muchos conocimientos en informática y que se dedica a acceder ilegalmente a sistemas informáticos ajenos para manipularlos.
Insiders	Persona con acceso al sistema dentro del perímetro de seguridad y que puede divulgar información sensible de su empresa.
IAONA	Asociación de redes abiertas de automatización **i**ndustrial.

Jitter	Variación de tiempo en la llegada de los datos causada por la congestión de red, pérdida de sincronización o por las diferentes rutas seguidas por los paquetes a su destino.
Latencia de red	Es la suma de los retardos temporales dentro de una red.
Malware	Software malicioso.
Módems	Modulador-demodulador, dispositivo que convierte señales digitales en analógicas a través de la línea telefónica.
MODICON	*Modular digital controler.* Controlador digital modular, primera versión de PLC diseñado por *Bedford Associates.*
Phishers	Persona que hace *phishing.*
Phishing	Técnicas para engañar a una víctima al suplantar su identidad real con el objeto de robarle información personal, tales como claves.
Profibus	Derivado de las palabras process y fieldbus, es un estándar de comunicación para buses de campo.
Request	Permite el acceso a toda información que pasa desde un navegador del cliente al servidor.

Router	Enrutador o dispositivo para interconectar computadoras.
Rlogin	*Remote login.* Aplicación TCP/IP que comienza una sesión de terminal remoto sobre el anfitrión especificado como *host.*
Servlet	Es una clase en el lenguaje de programación JAVA.
Spyware	Software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento del propietario.
Spammers	Correo basura no deseado.
Software	Conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en una computadora.
Siemens	Empresa multinacional de origen alemán.
Staff	Conjunto de personas que forman un equipo de estudio, información o asesoramiento de una empresa u organización.
TELNET	*Telecommunication network*: Protocolo de red que se utiliza para acceder a una computadora remota y manejarla.

Testbeds	Banco de pruebas. Plataforma para experimentación de proyectos de gran desarrollo.
UNIVAC	Computadora automática universal.
Verizon	Operador de telefonía móvil de Estados Unidos.

RESUMEN

En el presente trabajo de graduación se muestra un análisis de los sistemas de controles industriales y su seguridad. Se desarrolla los aspectos teóricos que definen un ICS, cómo fue creado, su evolución y sus componentes.

Se describe cómo han ocurrido los ciberataques a los sistemas de control industriales. Se definen los ciberataques más relevantes que han transcurrido en los últimos años, además de aspectos de los sistemas que han logrado dañar.

También se desarrolla el tema de análisis de riesgos para los ICS., qué aspectos hay que considerar y los impactos que puede haber en un ICS.

Se muestra la implementación de un sistema de seguridad donde se analiza qué beneficios hay al incluir un sistema de seguridad a los ICS.

En el tema de arquitectura de la seguridad se muestra los beneficios de implementar esta arquitectura; además, introduce el concepto de los *firewalls* y cómo se pueden aplicar a los sistemas ICS.

Y se desarrolla cómo se pueden aplicar los controles de seguridad a los sistemas ICS, se describe cada método de seguridad y su aporte a los sistemas.

OBJETIVOS

General

Realizar una investigación de cuáles son los diferentes tipos de ataques que a los que pueden estar expuestos los sistemas de control industrial. Conocer cómo implementar un sistema de seguridad en un ICS, cómo restringir el acceso físico a la red y a los dispositivos de ICS, cómo proteger los componentes individuales del ICS, tener mantenimiento de las operaciones en condiciones adversas y restaurar el sistema después de un incidente.

Específicos

1. Definir el diseño de un sistema ICS aplicando el sistema de referencia CIM de arquitectura piramidal, para atender el control de los elementos que dan sentido al proceso productivo de un sistema

2. Aplicar la seguridad en todo el ciclo de vida del ICS, desde diseño de la arquitectura y la puesta en marcha de la instalación, hasta el mantenimiento y final de operación o vida útil del sistema.

3. Mostrar una topología de red para que el ICS tenga múltiples capas, que las comunicaciones críticas ocurran en la capa más segura y fiable y considerar en el diseño los PLC de seguridad.

4. Mejorar los sistemas de control al implantar políticas de seguridad que puedan potencializar y mejorar la confiabilidad y fiabilidad para disminuir

el impacto involuntario de manera inapropiada de los ICS, debido a pruebas, políticas y sistemas que se han desconfigurado.

5. Concientizar a los empleados, contratistas y colaboradores sobre los riesgos de ciberseguridad y garantizar que tengan los conocimientos y experiencia necesarios para dominar las nuevas tecnologías al alcance, y así cumplir con los objetivos de la compañía.

6. Conocer los diferentes ciberataques y sus métodos que se han dado a nivel mundial para considerar las herramientas apropiadas que pueden evitar ataques similares.

7. Desarrollar las prácticas del manejo de riesgo en la seguridad del sistema para proteger para mejorar las técnicas relacionadas con el riesgo de la organización y comunicación efectiva entre niveles, y así poder identificar sus amenazas y vulnerabilidades.

8. Determinar un plan de seguridad que pueda integrar todos los aspectos de seguridad al construir un equipo funcional, definir los procedimientos y alcances, las políticas de seguridad, y proveer el entrenamiento y crecimiento del personal a cargo.

9. Implementar el concepto de segregación y segmentación de red para determinar las partes críticas de un sistema ICS. Establecer dominios de seguridad y minimizar el método y nivel de acceso a la información confidencial.

10. Mostrar los dispositivos denominados protección de límites que controlan el flujo de información entre dominios y protegen el ICS; limitar el flujo de

información no autorizados y brindar más niveles de protección al sistema.

11. Dar a conocer los diferentes mecanismos de autenticación y credenciales de verificación de contraseñas para los usuarios tanto de la red del ICS como de la red corporativa, para reducir vulnerabilidades, y evitar que dichas contraseñas sean débiles o comunes.

12. Monitorear la gestión de configuración y el control de los componentes del sistema de información, el análisis de impacto de la seguridad, de los cambios en el sistema, la evaluación continua de los controles de seguridad y los informes de estado.

13. Analizar controles de seguridad tales como instalar software de detección de intrusiones, software antivirus y software para que cada empresa pueda comprobar la integridad de archivos, para prevenir, desalentar, detectar y mitigar la introducción, exposición y propagación de software malicioso.

INTRODUCCIÓN

El estudio de la seguridad en cualquier ámbito conlleva a conocer las fallas o invasiones a la que está expuesto cualquiera que sea el sistema que se desea analizar. Un sistema de control industrial es un conjunto de dispositivos encargados de administrar y controlar el comportamiento operacional físico del equipo de una planta de producción, que poco a poco ha evolucionado hasta lograr automatizarse.

Inicialmente, la infraestructura de los sistemas de control industriales era muy pequeña, pero a medida que ha crecido y automatizado en su evolución y se ha conectado a internet; ha tenido que protegerse, pues los protocolos de comunicación que normalmente utilizaban son antiguos y muy débiles en su seguridad. Estos sistemas tienen muchas variables, tales como: temperatura, presión, longitud, voltaje, corriente, energía, etc. Es importante crear un sistema de seguridad apropiado protegerse de vulnerabilidades en las que cada vez más se ve afectado.

Ahora, los sistemas de control industriales son sistemas altamente interconectados en la red y mutuamente dependientes. Suelen ser vitales para el funcionamiento de las infraestructuras de una organización. Se aplican en industrias tales como electricidad, agua, petróleo, gas natural, energía nuclear, transporte, química, farmacéutica, salud, alimentos, etc., pertenecientes a la infraestructura de desarrollo de un país.

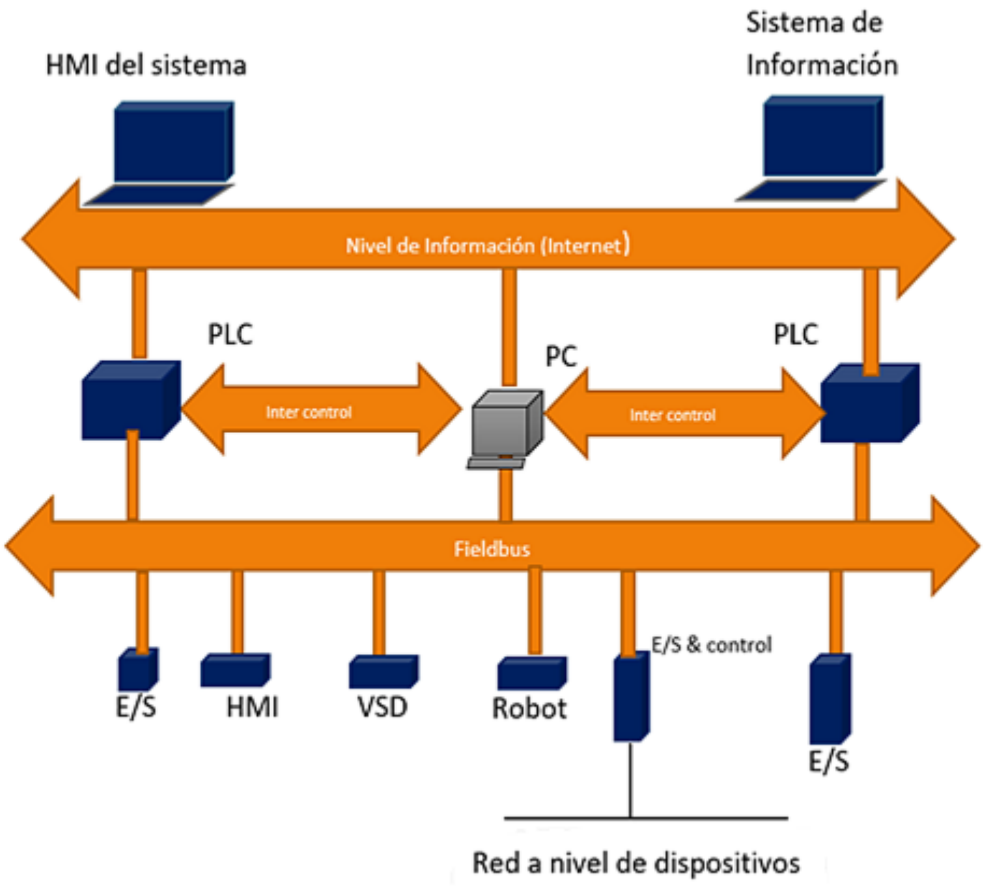
Por tanto, los sistemas de control industrial se han vuelto objeto de ataques informáticos y son cada vez más los incidentes de violación a la

seguridad de la infraestructura de estos. En este estudio se introducen las características generales que deben tomarse en cuenta en el diseño de una infraestructura de red de los ICS, analizando cada uno de los elementos de seguridad que se pueden encontrar en el diseño de una red típica.

1. BASES DEL SISTEMA DE CONTROL INDUSTRIAL

A continuación, se muestra un diseño básico de un sistema de control industrial:

Figura 1. **Diseño de un sistema de control industrial**



Fuente: elaboración propia.

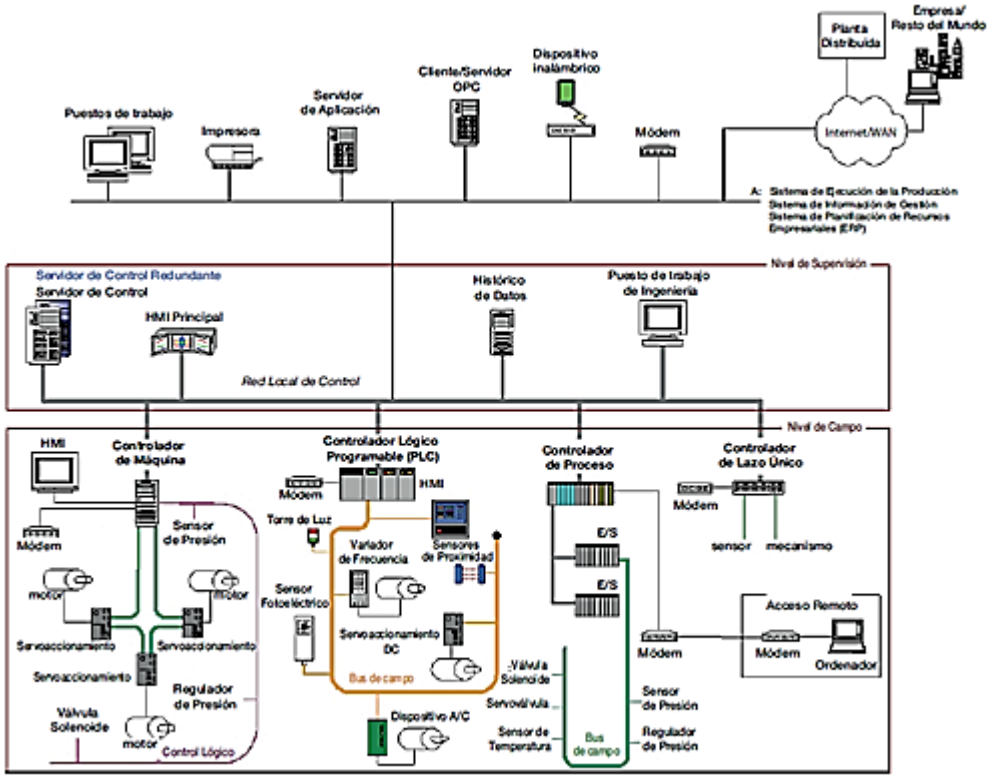
.

Un ICS es el grupo de dispositivos que administran, ordenan y regulan el comportamiento operacional de la parte física de un equipo o bien de una planta de producción, con el objetivo de exponerlo a fallos y lograr los mejores resultados. Estos sistemas operan en períodos largos y pueden ser modificables cuando se requiera.

Inicialmente, los sistemas ICS estaban apartados de la tecnología operacional OT y no estaban conectados a internet. Poco a poco evolucionaron y surgieron sistemas inteligentes, pasando de sistemas cerrados a otros muy modernos de arquitectura abierta basados en tecnología digital con los requerimientos de la tecnología de información IT, que son de dominio público. Surgieron situaciones de vulnerabilidad que están presentes en los sistemas IT.

Los ICS tienen componentes lógicos, eléctricos, mecánicos, hidráulicos y neumáticos que actúan mutuamente con el fin de desarrollar una industria de fabricación, control, etc. Estos sistemas pueden ser completamente automatizados o incluir situaciones donde aún pueda participar el hombre. Los sistemas se pueden operar en modo de lazo abierto, cerrado o manual. Un ICS puede contener todos estos tipos de lazos (HMI) y herramientas de diagnóstico. Existen diferentes configuraciones de ICS, como DCS, SCADA y PLC.

Figura 2. **Control de procesos**



Fuente: Pública tic. *Tipos de sistemas de control industrial.* https://blogs. deusto.es/master-informatica/tag/plc/?print=print-search. Consulta: 19 de enero de 2020.

Como vemos en la figura 2, el sistema tiene comunicación con los controladores autónomos. Pueden ser también autómatas programables, actuadores, interfaz gráfica, pantallas táctiles, cursores, ratones, lápices ópticos, etc. En general, cualquier dispositivo que permita acceso a los datos remotos y que pueda controlar el proceso desde un computador.

Los términos que podemos observar en la figura y su funcionamiento dentro del sistema se enumeran a continuación:

- Servidor de control: es el encargado de alojar el software de control de supervisión de los DCS o bien de los PLC. Se logra comunicar con los dispositivos ubicados en un nivel inferior.

- Servidor SCADA (MTU): es un dispositivo que trabaja para ser el maestro en un sistema SCADA.

- RTU: se define como una unidad de adquisición y control de datos de propósito específico y está diseñada para ser utilizada con los sistemas SCADA.

- IED: es un sensor o mecanismo denominado “inteligente” capaz de adquirir datos. Se puede comunicar con otros dispositivos y, además, puede realizar el procesamiento y control local.

- Un HMI es, básicamente, el software y hardware y les permite a los operadores hacer el trabajo de supervisión de un proceso. Es capaz de modificar las configuraciones de control y modificar al objetivo de control; es capaz de anular las operaciones de control automático de forma manual cuando ocurre una emergencia.

- Histórico de datos: se refiere a la información que está almacenada en la base de datos y que puede accederse para realizar algunos análisis, tales como: el análisis estadístico de los procesos y también una planificación en la empresa.

- El servidor de control: es el encargado del almacenamiento en la memoria intermedia (*buffer*) y también vela por el acceso para procesar la información que se encuentra en los subcomponentes de control, tales como PLC, RTU e IED.

1.1. Evolución del ICS

La evolución del sistema de control o automatización se dio con el propósito de aumentar la producción del sistema industrial y automatizarlo, y que un humano pudiera realizar más resultados en su sistema.

Los sistemas de control inicialmente daban a las personas una forma de utilizar la tecnología. Estos han evolucionado para obtener tiempos más cortos con más mejoras en sus sistemas.

La teoría de un sistema de control industrial se ocupa del comportamiento de los sistemas dinámicos. El principal objetivo es calcular las soluciones adecuadas para controlar los resultados de la estabilidad de un sistema. Existen dos tipos de prácticas en la teoría de los sistemas de control industrial, la clásica y la moderna. La teoría clásica se limita al diseño de sistemas de entrada y salida única (SISO); la teoría moderna incluye entrada múltiple, salida múltiple (MIMO); la más utilizada es la teoría de control moderna. Los beneficios del uso de la teoría moderna son la automatización y, por consiguiente, se reduce la cantidad de mano de obra; se ahorra energía a través de ganancias y eficiencia, se reduce la cantidad de materiales, se mejora la calidad, precisión, previsión de sus materiales.

Se consideran los controles industriales como una parte del proceso de una fábrica desde a mediados de 1800. Las sociedades griegas y arábigas

tenían algunos reguladores de válvula de flotador en dispositivos como relojes de agua, lámparas de aceite, dispensadores de vino y tanques de agua.

Uno de los primeros dispositivos de control con retroalimentación es un reloj de agua de Ctesibio en Alejandría, Egipto, cerca del año 250 antes de Cristo.

Este fue un diseño que utilizaba el agua para llenar y regular la exactitud del mecanismo del tiempo. El reloj mantuvo una exactitud del tiempo más que ningún otro reloj inventado en su época, hasta que llegó el reloj de péndulo.

Un filósofo griego matemático llamado Arquitas, diseñó una máquina en forma de pájaro que podía volar suspendida por un alambre. Se refirió a su diseño como ave de madera 10. Los autómatas danzantes empezaron a tomar forma como dispositivos mecánicos que podían realizar ciertos movimientos. Este tipo de tecnología es un ejemplo de sistemas de lazo abierto.

El periodo Clásico. (1935-1950)**.** El Dr. Bennet y C.C. Bissell lo nombraron de esta manera. Había 4 grupos en Estados Unidos trabajando en el desarrollo de controles y teoría de control durante este periodo. Los aportes de estos grupos fueron los siguientes:

- AT&T. Empresa que se enfocó en la manera de extender el ancho de banda de sus sistemas de comunicación.

- Ingenieros de proceso y físicos**.** Dirigidos por Ed Smith de la compañía de constructores con hierro fundido, comenzaron a desarrollar sistemáticamente una comprensión teórica que usaban. Vieron terminología común y persuadieron a la Sociedad Americana de

Ingenieros Mecánicos (ASME), de formar un comité de instrumentos reguladores industriales en 1936.

- Compañía Foxboro. Esta empresa se enfocó en el diseño del controlador *Stabilog,* el cual provee acción de control proporcional e integral a los sistemas de control Industriales.

- MIT (Instituto Tecnológico de Massachusetts) Este grupo ideó el concepto de diagrama de bloques y sistemas de control simulados.

El periodo entre las guerras y comienzo de la 2a Guerra Mundial reunió muchos expertos (incluyendo los anteriores) para resolver el llamado “problema de control en la línea de fuego”. Era básicamente problemas con la estabilidad de la plataforma, objetos en movimiento, seguimiento de objetos y apuntar con armas. La predicción fue la clave de las áreas que requerían las soluciones de estos expertos.

La guerra también reunió expertos en controles avanzados en Reino Unido, Alemania, Rusia, con un enfoque similar centrado en la guerra y en otros ámbitos. Se empezaron a publicar libros sobre Ingeniería de control automático y teoría de servomecanismos en 1946. La institución de ingenieros eléctricos celebró una conferencia sobre radar con muchos documentos relacionados a servomecanismos. El laboratorio de radiación del MIT se centró en mejorar los sistemas de radar y escribió varios libros relacionados a este tema.

En 1950, los ingenieros de control empezaron a realizar sistemas no lineales. Las mediciones reales contenían errores y se contaminaban de ruido. Se empezó a desarrollar nuevos diseños de modelos de sistemas de control industriales. Las plantas empezaron a utilizar temas como el balance físico

matemático de masa y energía, y las escuelas de ingeniería empezaron a enseñar cursos de servomecanismos y teoría del control.

La historia de sistemas de control modernos está enlazada a las comunicaciones y la generación de máquinas procesadoras de datos, y crearon la base para las computadoras. En 1950, la Corporations Sperry Rand, construyó el *UNIVAC* I, la primera máquina comercial procesadora de datos (CNC).

Antes de 1950, los sistemas de control eran análogos y se basaban en un simple *on-off* con dispositivos relés. El primer sistema de control distribuido, (DCS) se desarrolló en 1956 y empezó a operar en el puerto de la refinería Arthur de Texas, y al siguiente año operó en la planta de amoniaco en Monsanto Luling, Luisiana. Estos sistemas eran supervisores y los circuitos individuales estaban controlados por electricidad convencional, controles neumáticos e hidráulicos y monitoreados por computadora.

En la década de 1960 se crearon computadoras con control de procesos especializados, ofreciendo control digital directo (DDC). En el DDC, la computadora implementa un algoritmo de control de forma discreta. Desafortunadamente, estos sistemas DDC resultaron ser muy caros y se reemplazaron por microcomputadoras más baratas.

1.2. Sectores industriales de un ICS

Los sistemas de control industriales abarcan muchas aplicaciones, en control de instalaciones y sistemas automáticos.

Los ICS están conformados por las siguientes áreas:

- Proceso de alimentos
- Cementeras
- Acero
- Agregados
- Tuberías
- Pinturas y acabados
- Productos prefabricados y materiales para la construcción
- Maquinaria
- Equipo y distribuidores de materiales
- Agua
- Electricidad
- Academia
- Banca
- Finanzas
- Seguros

1.3. Operación de un ICS y sus componentes

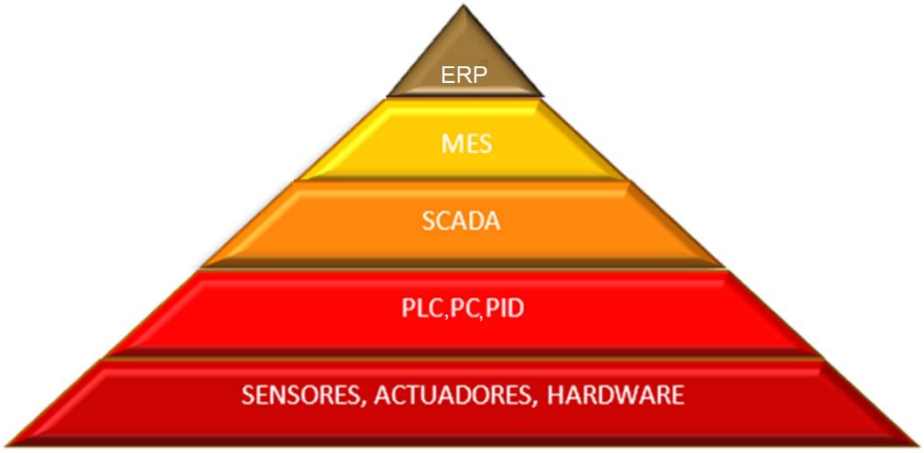
El término ICS se refiere a una variedad de sistemas compuestos por computadoras, dispositivos eléctricos, hidráulicos y mecánicos. Estos sistemas realizan el control automatizado de los equipos de muchas empresas.

1.3.1. Consideraciones del diseño de un ICS

Desde que evolucionó la tecnología de la información y las comunicaciones (ordenadores y redes de ordenadores) esto es, a principios de los años setenta, el modelo de CIM (se define como fabricación integrada por computadora) se ha utilizado para desarrollar e integrar estas tecnologías en el

área industrial para automatizar y lograr mejoras en los procesos productivos (mejorar la capacidad productiva y calidad de los productos, disminuir costos).

Figura 3. **Modelo de referencia CIM**



Fuente: elaboración propia.

Este modelo CIM se muestra en una arquitectura piramidal donde cada subnivel debe prestar servicios al nivel superior, puede proporcionar información o datos o realizar alguna acción. Al mismo tiempo sucede que el nivel superior procesa los datos y puede realizar acciones con el nivel inferior y con el superior.

La capa inferior (o nivel 0) del modelo CIM es el nivel de los sensores, actuadores y el hardware de un sistema. El siguiente nivel corresponde al monitoreo y control donde un conjunto de dispositivos tales como los PLC, en tiempo real, están diseñados para controlar y monitorear los procesos haciendo uso del hardware, sensores y actuadores. En el siguiente nivel, de supervisión, está el sistema SCADA y es el encargado de controlar toda la parte del sistema que realiza el proceso de producción. Los últimos niveles de MES y ERP son

los que gestionan las órdenes de trabajo necesarias para generar los productos que una empresa trabaja.

El nivel ERP (planificación de recursos empresariales) gestiona de forma global la producción dentro de una empresa, además de otros aspectos como la distribución, logística, inventario, facturación, etc. Constituye un apoyo en la toma de decisiones para la actividad, ya que agrupa fuentes de información y permite la mejora y mantenimiento de la unidad de negocio. Como vemos, este modelo piramidal es parecido a las arquitecturas utilizadas en sistemas y protocolos de telecomunicación (ver modelo de referencia OSI) y se puede considerar un éxito de la ingeniería gracias a que permite la separación de intereses de los diferentes niveles y los beneficios que de ello se derivan. Por ejemplo, la separación de intereses de cada nivel de la jerarquía, juntamente con la aparición de estándares, permite que equipos de diferentes fabricantes puedan interoperar, permitiendo una fácil integración y reduciendo el tiempo y los costos asociados.

Este modelo que se ha presentado, CIM, tiene que estar a la altura de lo que exige la implementación de la industria 4,0 que nos muestra nuevos requerimientos de acceso a la información; introduce temas como el mantenimiento predictivo, que minimiza el tiempo no deseado de espera de las máquinas y lo que representa en gastos.

Es necesario crear nuevas tecnologías de comunicación que puedan apoyar los nuevos conceptos de acceso a la información en tiempo real, crear protocolos de comunicación para acceder a la información de forma distribuida y, por último, crear una serie de mecanismos para lograr el mantenimiento y despliegue de las nuevas tecnologías en la parte de productividad.

En esta dirección, durante el último año hemos visto cómo las redes sensibles de tiempo TSN y OPC-UA (plataforma de colaboración abierta, arquitectura unificada) han tomado protagonismo en las diferentes áreas del sector industrial. Por un lado, TSN es una tecnología de red basada en Ethernet que permite (entre otros), garantizar el determinismo del tráfico de red (ancho de banda, latencia de red y *jitter*) y la sincronización entre los dispositivos que la forman para asegurar un correcto funcionamiento de los procesos industriales que la utilizan para intercambiar datos. Por otro lado, OPC-UA es un protocolo de comunicación que facilita la integración de los procesos industriales, incluyendo la estructura y el formato utilizado para el intercambio de los datos, así como aspectos de seguridad de la información.

En 2018, Intel presentó SDIC (*software defined industrial control*), basado en SDN (*software defined Networking*) que ha sido desarrollado en los últimos años en el área de computación, en la nube y en las telecomunicaciones para que los servicios y las redes se desplieguen de manera fácil y dinámica.

Este concepto anula el modelo de referencia CIM y muestra una arquitectura distribuida que permite la flexibilidad de los sistemas productivos y mantiene la seguridad necesaria en el ámbito industrial.

A la vista de lo expuesto, parece claro que la combinación de todas estas tecnologías en el ámbito industrial es clave para habilitar los conceptos de la Industria 4,0 mencionados. El diseño de estas tecnologías y la relación entre los beneficios y los costos que supone su implementación están cada vez más claros gracias a los *testbeds* y las pruebas piloto que han realizado los diferentes fabricantes de estos equipos. Es importante realizar las primeras pruebas en el campo y así darle valor a la integración con los equipos ya establecidos y la interacción de los técnicos en el área de informática; así como

el área de sistemas interacción de los técnicos en el área de informática; así como el área de sistemas de control, para que la tecnología esté presente en las diferentes fases de los procesos.

Hay que validar los aspectos de la integración con los equipos que están ya instalados; además, es necesario crear una buena relación entre los técnicos tanto de los sistemas de control como los técnicos de los sistemas IT, ya que esto hace que se puedan implantar las nuevas tecnologías en las fases de proceso de diseño, despliegue y mantenimiento.

1.3.2. Sistema SCADA

SCADA quiere decir adquisición de datos y control de supervisión. Es un software que funciona en ordenadores y está diseñado para el control de la producción por medio de comunicación digital con todos los dispositivos que pertenecen a una industria, tales como pantallas de control, controladores autónomos, instrumentos, cursores, etc. Estos permiten el control de los procesos automáticamente a distancia desde un ordenador, hardware o dispositivos móviles que puedan utilizar las personas en el proceso. Es muy utilizado en sistemas de control que abarcan una gran área geográfica.

.

Los sistemas SCADA fueron instalados a principios de 1920, donde algunas subestaciones de alto voltaje podían monitorear y controlar desde un cuarto de control de potencia, toda la planta.

De acuerdo con el Instituto Nacional de Estándares y Tecnología (NIST), los sistemas SCADA son sistemas altamente distribuidos usados para el control geográfico de bienes dispersos, regularmente alejados a muchos kilómetros

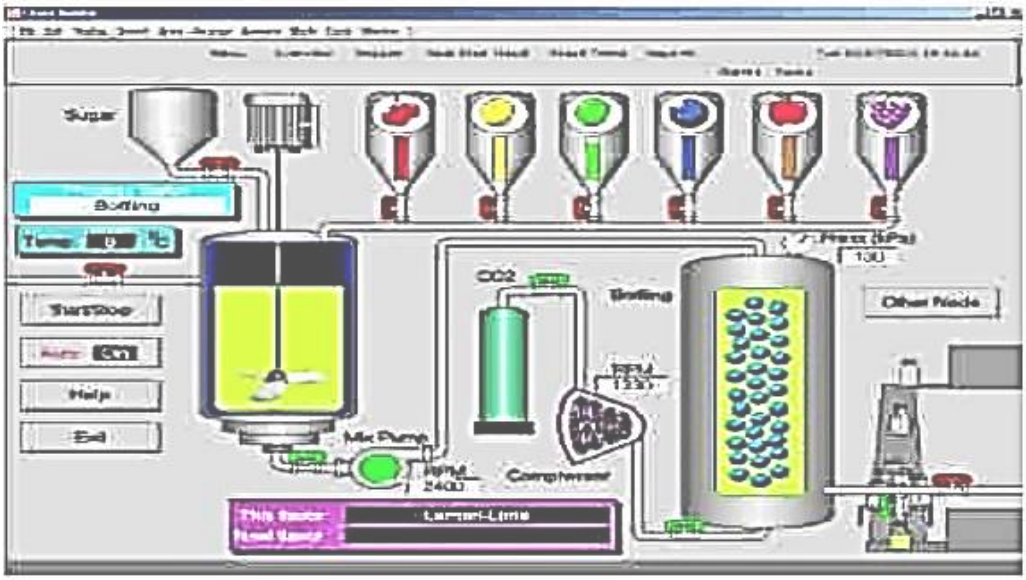
donde está centralizada la adquisición y control de datos de un sistema en operación.

Ellos son usados en sistemas de distribución tales como sistemas de distribución y recolección de agua, sistemas de manejo de aceite, de gas natural, redes de energía eléctrica y sistemas de transporte a través de trenes. Un centro de control SCADA permite el monitoreo y control de varios campos que están a grandes distancias a través de redes de comunicación, incluyendo alarmas de monitoreo, y estados de procesamiento de datos. Basados en la información recibida de estaciones remotas, automatizadas o manejadas por operadores, los comandos pueden ser enviados a dispositivos de control en una estación remota, y son referidos como dispositivos de campo. Los dispositivos de campo controlan operaciones locales como abrir o cerrar válvulas, o interruptores, recolectan datos de sistemas de sensores y monitorean el entorno local en condiciones de alarma.

Los sistemas SCADA son sistemas distribuidos que controlan activos ubicados en diferentes áreas geográficas donde el control y toma de datos son importantes y, a veces, difíciles de acceder en el funcionamiento de los sistemas. Es decir, que el sistema SCADA obtiene la información en un área muchas veces lejana, la transfiere al área central de informática y allí está el encargado de supervisar y controlar todo un sistema desplegado en áreas distantes y en tiempo real.

Un sistema SCADA se muestra en la figura 4.

Figura 4. **Sistema SCADA**



Fuente: Slideshare. *Control de Procesos Automatizados*. https//es.slideshare.net. Consulta: 25 de enero de 2020.

Al implementar los sistemas SCADA de forma remota se requirió el desarrollo de dispositivos llamados unidades terminales remotas (RTU). Los RTU fueron suministrados principalmente por el proveedor de SCADA. Utilizan componentes de estado sólido montados en tarjetas de circuito impreso y normalmente alojados en bastidores de tarjetas en gabinetes de equipos, adecuados para el montaje de subestaciones de alimentación remotas. Necesitan funcionar incluso si la energía está averiada. La estructura básica de una RTU consiste en una interfaz de comunicación, un controlador lógico central y un sistema de entrada/salida, tanto analógicas como digitales. Dado que las RTU funcionaban de forma continua y ya que es importante tener respuesta rápida a las operaciones de control en caso de perturbación del sistema, el protocolo de comunicación debía ser eficiente y muy seguro.

La seguridad era un factor principal, por lo que se transmitían caracteres de seguridad sofisticados de comprobación con cada mensaje. El esquema *select/before operate* se utilizaba en las operaciones de control. El código de control de seguridad más común utilizado era BCH, que era un código de comprobación de comunicación desarrollado en los años 60. Durante los años 60 y 70 la mayoría de los protocolos de comunicación RTU eran exclusivos del proveedor RTU.

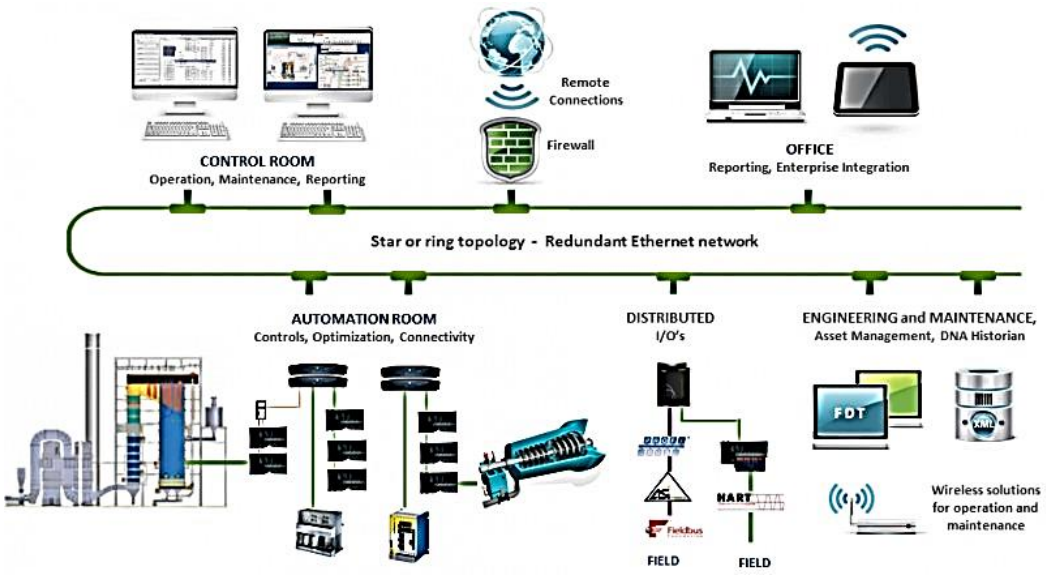
Debido a la necesidad de alta seguridad y eficiencia no se utilizaron protocolos comunes como ASCII. Con el fin de permitir diferentes marcas de RTU en un sistema SCADA, hubo un esfuerzo por estandarizar los protocolos liderados por la sociedad internacional de ingenieros eléctricos y electrónicos IEEE. El desarrollo de la interfaz de comunicación basado en microprocesadores resolvió algunos de los problemas de compatibilidad a medida que los microprocesadores comenzaron a aplicarse a relés de protección, medidores, varios controladores y otros dispositivos, especialmente aquellos componentes del sistema de energía con microprocesadores y un puerto de comunicación de un dispositivo electrónico inteligente.

1.3.3. Sistemas de control distribuidos

Los sistemas DCS controlan los procesos industriales en una misma área geográfica. Estos sistemas se utilizan ampliamente en industrias basadas en procesos; también están conectados con la red corporativa, para proporcionar visión de producción.

En la figura 5 se muestra la implementación de un DCS:

Figura 5. **Sistemas DCS**



Fuente: Optieng. *Redes de control DCS*. www.optieng.com/sistemas-controlo-dcs.php ?lang.es. Consulta 2 de febrero de 2020.

Los DCS se utilizan para controlar procesos industriales como la generación de energía eléctrica, refinerías de petróleo y gas, tratamiento de agua y aguas residuales y la producción de productos químicos alimentos y automóviles. Los sistemas DCS conforman los ICS, para integrarlos como una arquitectura de control que supervisan y controlan subsistemas integrados encargados de tener el control de los detalles de algún proceso. Contienen un nivel de supervisión y de control, logran supervisar múltiples subsistemas integrados que, a su vez, controlan el proceso de una industria, todo en un área localizada.

El control del producto y del proceso se consigue generalmente mediante la implementación de lazos de retroalimentación o de compensación, mediante los cuales las condiciones claves del producto y el proceso se mantiene

automáticamente alrededor de un punto de ajuste deseado. Para lograr el producto deseado y tolerancia del proceso alrededor de un punto determinado, se emplea un controlador lógico programable específico en el campo. Los ajustes proporcionales, integrales y/o diferenciales en el PLC se calibran de acuerdo con los resultados deseados y a la tasa de autocorrección en el momento de un desajuste del proceso. Los DCS se utilizan ampliamente en industrias basadas en procesos.

1.3.4. PLC y sus topologías

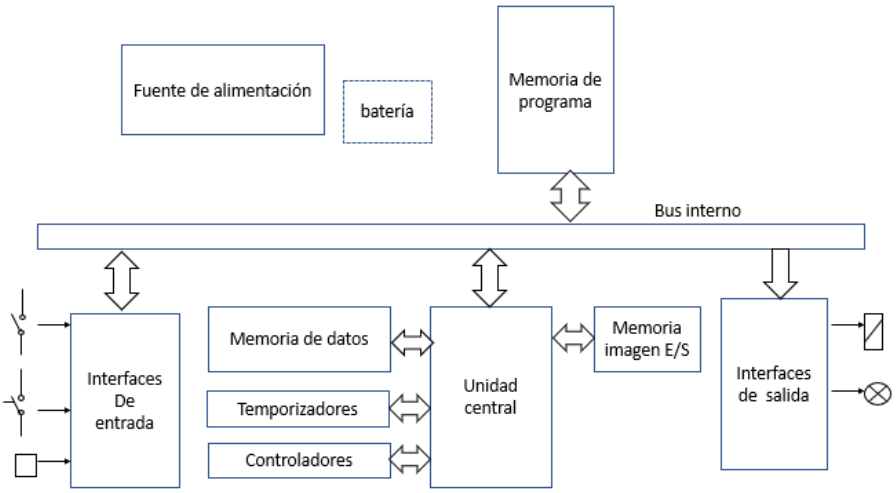
Los PLC son los dispositivos de estado sólido encargados de controlar los equipos y los procesos industriales. Son muy utilizados en los sistemas SCADA y DCS, y en ocasiones representan los componentes primarios en la configuración de los sistemas de control industriales de menor tamaño.

Figura 6. **Sistema PLC**

Fuente: Teknica web. *PLC vs arduino para control industrial.* https:/bonusCursos.com. Consulta 8 de febrero de 2020.

En la figura 7 vemos en diagrama de bloques, la arquitectura de un PLC:

Figura 7. **Arquitectura de un PLC**



Fuente: elaboración propia, empleando https://www.autrace.com.

Los sistemas PLC son dispositivos electrónicos programables formados por un CPU, módulo de memoria, fuente de poder y módulos de entradas y salidas. Fueron creados en 1960 en reemplazo a los sistemas convencionales de relés o controles individuales que trabajaban como parte de un sistema de control en una industria.

El PLC es un sistema que opera en tiempo real; lee todas las entradas, ejecuta la lógica y actúa de acuerdo con su programación para dar la información en las terminales de salida; el tiempo de esta ejecución es de apenas milisegundos.

La empresa Bedford Associates, propuso el sistema denominado *Modular Digital Controller* o MODICON creado en 1968 por el Sr. Dick Morley, llamado el padre del PLC.

A mediados de los años 70, los microprocesadores AMD am 2901 y am 2903 eran los más utilizados en los PLC *MODICON.* En esa época, los microprocesadores no eran tan rápidos y solo podían adaptarse a PLC pequeños.

El *MODICON* 084 fue el primer PLC producido comercialmente. Se diseñó para que su programación fuera fácil, debía ser durable y capaz de adaptarse a ambientes difíciles. El diseño reemplazó los relés por elementos de estado sólido.

Con el avance de los microprocesadores (cada vez más veloces), se fueron creando y mejorando los PLC y también la habilidad de comunicarse entre ellos. Los PLC se podían instalar lejos de la maquinaria; sin embargo, como los diseños no estaban estandarizados, se dificultó la comunicación entre otros PLC.

En 1982 se creó el primer PLC estándar y la General Motors creó un protocolo de automatización de manufactura (MAP), redujo el tamaño de los PLC y utilizó un ordenador personal para su programación.

En sus inicios, otras empresas crearon sus PLC cada una con su propio lenguaje de programación, lo que logró que no hubiera comunicación entre otro PLC de diferente empresa. Ahora existen lenguajes estándares para lograr la comunicación entre ellos.

Los 5 lenguajes estandarizados son:

- Diagrama de bloque de la función (FBD)
- Diagrama de escalera (LD)

- Texto estructurado (ST)
- Lista de instrucciones (IL)
- Tabla de secuencia de las funciones (SFC)

Ahora se han creado PLC de seguridad; es decir, que se ha modificado la arquitectura interna, el software, el firmware y la certificación para aplicaciones donde se requiera el complimiento de un cierto nivel de integridad de seguridad (SIL).

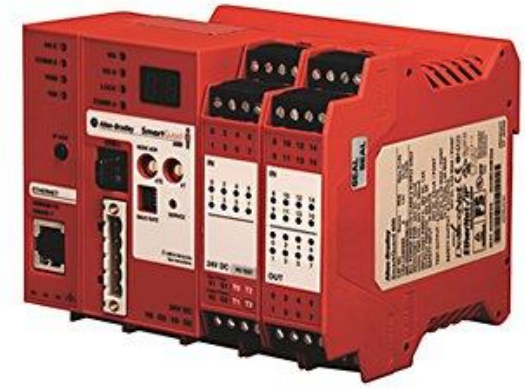
El PLC de seguridad incorpora muchas funciones de diagnóstico para detectar cualquier posible fallo interno en el hardware o firmware y lograr que no cause algún daño dicho fallo. Además, el PLC de seguridad cumple con los SIS que contempla la norma internacional IEC-51 508, IEC-61 511. IEC 62 061 y otras más. Las diferencias entre un PLC estándar y un PLC de seguridad son las siguientes:

- El PLC de seguridad está certificado por entidades encargadas de velar por las aplicaciones de seguridad hasta cierto nivel SIL.

- Incorpora rutinas de autodiagnóstico de todo el hardware y software para detectar cualquier fallo interno peligroso. En caso de que ocurra, actúa llevando la máquina o proceso a una situación segura.

- El costo de un PLC de seguridad es más alto en su inversión inicial, pero a largo plazo es más rentable.

Figura 8. **PLC de seguridad**



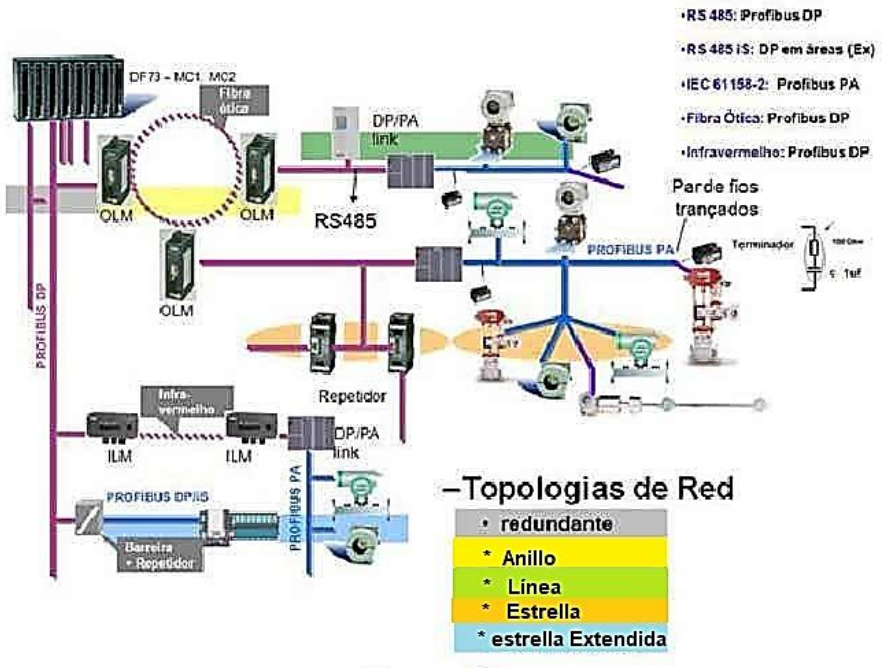
Fuente: Rockwell Automation.: *Controladores de seguridad SmartGuard 600*. https://ab.rockwellautomation.com/resources/images/allenbradley/gl/medlrgprod/1752_SmartGuard600Controllers_left1- large_312w255h.jpg. Consulta: 28 de abril de 2020.

Los estándares internacionales hacen clasificación de las aplicaciones según su nivel de riesgo: SIL-1, SIL-2, SIL-3, SIL-4 y SIL-5 y forman parte del análisis de riesgos que deben realizar los diseñadores del SIS (sistemas instrumentados de seguridad).

1.3.4.1. Las topologías de los sistemas ICS

Se definen de acuerdo con sus implementaciones. Una topología es el arreglo geométrico entre nodos y lazos que conforman una red. A continuación, se muestra en la figura 9 las diferentes topologías de los PLC:

Figura 9. **Topologías de los PLC**



Fuente: Lázaro. *La importancia de los protocolos industriales*. https://igluub.com/2016 /07/21/la-importancia-de-los-protocolos-industriales. Consulta: 1 de abril de 2020.

El sistema redundante se define como la duplicación de componentes que permiten que el sistema funcione de forma continua; aunque exista fallo en alguno de los dos componentes, el otro sigue funcionando. Por esto, estas redes aumentan la confiabilidad de la red y reducen el tiempo de inactividad.

1.3.4.1.1. Anillo

En este sistema se reduce el número de canales utilizados mejorando en la eficiencia del sistema y la complejidad de las operaciones del sistema SCADA. Cada nodo conectado a este sistema se comunica con otros dos nodos, formando una ruta de comunicación de datos a cada nodo. Por lo mismo

pueden ser unidireccionales o bidireccionales. La información se transfiere de un nodo a otro, cada nodo maneja sus componentes.

1.3.4.1.2. Lineal

Este tipo de topología se aplica en sistemas simples de automatización. Su forma de procesamiento es secuencial o cíclico y se programan las instrucciones en un solo bloque de programación.

En este tipo de distribución, la ejecución de las instrucciones es de una en una en el orden que se ha ingresado al sistema PLC, excepto las instrucciones de salto.

La imagen de proceso de entradas (IPE), memorias internas e intermedias y los datos actuales de los temporizadores y contadores, son los que determinan la ejecución de las instrucciones.

Después de la ejecución del programa se corre un ciclo de datos; los datos de la IPE se transfieren a los módulos de salida y posteriormente; de manera simultánea, se transfieren los datos de los módulos de entrada a la IPE.

Una vez actualizada la IPE, el programa vuelve a ejecutarse. Si hay diferentes funciones que se deban ejecutar simultáneamente, este diseño hace que se dificulte el procesamiento, se logra que:

- Se Incremente el tiempo de barrido
- Sea lento su diagnóstico si los programas son extensos
- Se dificulte el diseño y se vuelve difícil de interpretar

1.3.4.1.3. Estrella

La topología estrella es la adecuada para redes medianas y grandes, todas las estaciones están conectadas y comunicadas desde un punto central.

Los dispositivos no están conectados entre sí y no se permite tanto tráfico de información. Por su estructura, permite agregar nuevos componentes. Su reconfiguración es rápida, es fácil de prevenir daños ya que no afecta a los demás nodos en caso de que uno se dañe. La principal desventaja se da cuando el nodo central falla y, por consiguiente, toda la red deja de operar.

1.3.4.1.4. Estrella extendida

Esta topología es igual a la topología de estrella, con la variante de que cada nodo representa un nodo central para otra topología de estrella. Es sumamente jerárquica, y busca que la información se mantenga local.

Debido a que el cableado es más corto, se limita la cantidad de dispositivos que se pueden conectar al nodo central. Las desventajas es que si el nodo central falla, toda la red deja de transmitir.

Es similar al tipo modular, pero tiene la ventaja de poderse comunicar entre cada módulo y permite que la velocidad de trabajo sea más alta y mejore su funcionamiento.

1.3.5. Señales analógicas vs IP en la automatización industrial

Los inicios de los sistemas de control de procesos y de los ICS fueron controles neumáticos y controles hidráulicos. Originalmente se utilizaba

neumática (presión de aire, presión de vapor) o hidráulica (agua o fluidos presurizados) para convertir lecturas y enviar instrucciones básicas alrededor de la infraestructura a ser controlada. Las tuberías y accionamientos neumáticos fueron llamados sistemas de control. Cuando los sistemas análogos basados en electrónica transmitían señales a través de cableado, nacieron los sistemas de control modernos que eran resultado de emular las anteriores señales neumáticas e hidráulicas. Lo anterior resulto en una herencia de sistemas hidráulicos, neumáticos y electrónicos que perduró por mucho tiempo (1876-1976), controlando sistemas interconectados en oficinas postales, alrededor del mundo.

Posteriormente, con la llegada de la era digital y antes del IP, resultaron muchos protocolos propietarios de marcas. Estos sistemas utilizaban un protocolo diseñado para comunicaciones digitales sobre sistemas análogos (como los módems). Protocolos como *Modbus,* DNP3, ICCP, profibus y conatel por mencionar algunos, todos ellos destinados a utilizarse sobre comunicaciones con portadoras analógicas, en redes de conmutador telefónico con antiguos módems sobre una infraestructura de alambrados de bajo voltaje. Adicionalmente algunos protocolos como el Siemens H1 fue utilizado en una red ethernet, pero su uso fue parcial en el protocolo TCP/IP. Muchas de esas tecnologías no lograron converger como una red de IT debido a que muchos de sus problemas derivaron de un excesivo multitarea o tráfico el cual interrumpió las comunicaciones.

La herencia de protocolos diseñados para propósitos específicos y que no fueron diseñados para otras aplicaciones o en un contexto de sistema abierto fueron exclusivos de alguna marca. Regularmente no podían “hablar “con otra que no fuera su marca. Con ello lograban bloquear el desarrollo de alguna otra solución para una infraestructura de control determinada. Todo lo anterior se

origina por el lento desarrollo de tecnologías de portadores de señales análogas en los primeros protocolos de control, los cuales en esencia fueron diseñados poco robustos, limitados a necesidades pequeñas de control.

El paso final en la evolución del proceso de redes de control se da en el cambio de análogo a digital, el cual dio lugar a la evolución de los sistemas IP con caras de transporte/portadora sobre un estándar IEEE 802,3 o enlace de datos ethernet. El moverse a IP fue obvio para los fabricantes de ICS y dueños de infraestructuras y sistemas de control. Las redes IP y los equipos yoIP se vuelven únicos, fáciles de conectar y soportar, además de rápidos de implementar y económicos. El IP permite más eficiencia, inteligencia de manufactura, facilidad de interfase con sistemas de negocios IT, visibilidad de empresa por su naturaleza de tiempo real e información de tendencias de producción. Dichos cambios manejan una gran convergencia y dan paso a mejores, más rápidos y económicos reportes, monitoreos y administración para todos los elementos de infraestructura total de la empresa y no solo para el personal de la planta de producción. El movimiento del control de proceso a IP es un componente importante de un gran fenómeno en los sistemas de comunicación conocido como convergencia IP.

Entendiendo la convergencia IP y sus implicaciones para la seguridad en las comunicaciones, es un elemento importante para comprender la seguridad en los ICS en estos días, debido a que el ICS es un activo de muchos en una red moderna. No debemos olvidar que un protocolo industrial es vulnerable a ataques y puede contener pequeñas vulnerabilidades o escasa seguridad. Por ello pueden ser funcionales, pero no estar preparados para el cruel mundo de las redes y comunicaciones IP.

La seguridad se limitaba a poner barreras dentro de la industria. Las comunicaciones eran internas de un sistema, no diseñadas para estándares basados en IP como Ethernet TCP/IP. La tecnología *firewall* no existía.

La comunicación entre los controladores y dispositivos de campo se basan cada vez más en la tecnología de ethernet industrial con el propósito de que las comunicaciones sean muy rápidas. En este tipo de comunicación, el desarrollo de los protocolos se orienta en la dirección que impulsa el rendimiento del sistema y simplifica las redes de fábrica.

Figura 10. **Ethernet**

Fuente: Maquiclick. *Ethernet/IP como nexo de unión entre los dos mundos*. http://www.adfweb.com/sch_prod/schema660.png. Consulta: 5 de abril de 2020.

1.4. Comparativo de los sistemas de seguridad ICS e IT

La conectividad a internet para los ICS es cada vez más utilizada para el acceso remoto a los recursos de trabajo y por los proveedores para la resolución de problemas y mantenimiento del equipo.

Las organizaciones de IT se han enfocado en la seguridad. La IT generalmente se ha preocupado por proteger los sistemas que albergan datos como información financiera de los clientes, propiedad intelectual e información corporativa. Estos sistemas pueden consistir en servidores, estaciones de trabajo, sistemas de correo electrónico, aplicaciones y bases de datos

Figura 11. **Dominios IT y OT**

Fuente: elaboración propia, empleando Industrial cyber security for dummies.

El dominio de la organización OT es la base de una planta, la automatización de los procesos y los sistemas de producción. Estos sistemas

pueden incluir equipos distribuidos en una amplia geografía; por ejemplo, en estaciones de bombeo de agua o subestaciones de transmisión eléctrica. El dominio OT general se muestra en la figura 11 en los niveles tres a cero. Los equipos de OT están más preocupados por la seguridad y la disponibilidad de sus activos físicos y cibernéticos porque la interrupción podría causar daños humanos o pérdidas de producción.

Por lo general, IT tiene una ventaja inicial en habilidades de seguridad cibernética dentro de su dominio y con frecuencia tiene algún tipo de personal y presupuesto dedicado a la seguridad. Sin embargo, el equipo IT tiene por lo general poca comprensión de la configuración y los requisitos únicos dentro de las redes industriales, los puntos finales y los sistemas de control. Las mejores prácticas estándar de IT y las soluciones tecnológicas no se aplican automáticamente en OT y a menudo el personal de IT no puede tomarse el tiempo para conocer los procesos y demandas de producción o criterios de OT para medir el éxito. Se puede visualizar las prioridades de IT y OT con el modelo de seguridad/información llamada triada de la CIA (confidencialidad, integridad, y disponibilidad). La tabla I muestra los equipos de IT y OT.

Tabla I. **Prioridades de IT y OT**

IT	OT
Confidencialidad	Disponibilidad (y seguridad)
Integridad	Integridad
Disponibilidad	Confidencialidad

Fuente: elaboración propia, empleando Industrial cyber security for dummies.

Si IT tiene que cerrar los sistemas y el acceso de usuarios o clientes es debido a un ataque de malware, entonces se hará. La protección de la

información confidencial anulará la disponibilidad. OT diría que el tiempo de inactividad no es una opción. La seguridad y disponibilidad del sistema supera la seguridad para la mayoría de los entornos de producción. A continuación, vemos la tabla II que muestran las funciones típicas organizacionales entre IT y los ICS:

Tabla II. **Funciones típicas organizacionales**

Tipos de seguridad	Tecnología de la información	Sistemas de control Industrial
Antivirus y código móvil	Muy común, es fácilmente implementado y actualizado. Los usuarios tienen control sobre la personalización y pueden estar basados en los activos empresariales.	Requisitos de memoria pueden tener impacto en los ICS, las organizaciones solo protegen las soluciones heredadas con soluciones posteriores al mercado, generalmente requiere carpetas de exclusión para evitar cuarentena en archivos críticos.
Manejo de parches	Fácil de definir; en toda la empresa; remoto y automatizado.	Larga línea de tiempo para la instalación exitosa de parches. OEM específico; puede romper la funcionalidad del ICS. Los propietarios activos deben definir un riesgo aceptable.
Soporte tecnológico de por vida	De dos a tres años, es de múltiples proveedores. Actualizaciones ubicuas	Diez a veinte años generalmente el mismo proveedor, el fin de la vida útil del producto crea nuevos problemas de seguridad.
Métodos de prueba y auditoria	Utilizan métodos modernos, los sistemas son generalmente resistentes y robustos para manejar métodos de evaluación.	Ajustar pruebas al sistema, métodos modernos pueden ser inapropiados, el equipo puede fallar durante las pruebas.

Continuación tabla II.

Tipos de seguridad	Tecnología de la información	Sistemas de control Industrial
Gestión de cambio	Regular y programado; alineados con periodos de uso mínimo	Programación estratégica, proceso no trivial debido al impacto en la producción.
Clasificación de activos	Común y se realiza anualmente; los resultados impulsan el gasto	Realizado cuando está obligado. Inventarios precisos no comunes para activos no vitales, desconexión entre los activos y las contramedidas apropiadas.
Respuesta a incidentes y análisis forenses	Fácilmente desarrollado; requisitos reglamentarios integrados en la tecnología	Enfocado en las actividades de reanudación del sistema, procedimientos forenses inmaduros (más allá de la recreación de eventos). Requiere buena relación IT/ ICS
Seguridad física y ambiental	Varía de pobre (sistema de oficina) a excelente (sistemas críticos de operaciones IT).	Por lo general excelente para áreas críticas, la madurez varía según las instalaciones en función de la criticidad y cultura
Desarrollo de sistemas de seguridad	Parte integral del desarrollo del proceso.	Históricamente no es parte integral del desarrollo del proceso, los proveedores mejoran a velocidad menor que las IT. Las soluciones principales emblemáticas dificultan modernizar con seguridad.
Cumplimiento de seguridad	Supervisión regulatoria definitiva según el sector.	Guía reguladora específica dependiendo del sector .

Fuente: elaboración propia, empleando Industrial cyber security for dummies.

1.5. Otros tipos de sistemas de control

Hemos visto cómo se construye un ICS y es importante saber que existen otros tipos de sistemas de control que comparten características similares a los ICS en cuanto a su desarrollo; por lo tanto, muchas de las recomendaciones dadas en esta investigación, se pueden aplicar a estos otros sistemas y protegerlos contra ciberataques.

Estos sistemas de control pertenecen a sistemas de transporte, medicina, construcción, etc. y utilizan diferentes protocolos, puertos y servicios. Aunque algunos trabajan de una manera diferente a un ICS convencional, pueden tener características similares. Ejemplos de estos otros sistemas de control:

- Infraestructura de medición avanzada
- Sistemas de automatización y gestión de edificios
- Sistemas de vigilancia de circuito cerrado de televisión
- Sistema de gestión de video digital
- Sistemas de gestión de emergencia
- Sistemas de control de acceso físico
- Sistemas geotérmicos de energía renovables
- Sistemas de transporte vertical (ascensores y escaleras mecánicas)
- Sistemas de gestión de información de laboratorios

1.6. Comprendiendo la infraestructura crítica

En cada sociedad donde vemos servicios y desarrollo de industrias cada vez más complejos, la infraestructura de estas tiene que estar al margen de responder a sus demandas que pueden ser cada vez más exigentes.

Una infraestructura crítica se refiere al riesgo latente de interrupción o alteración al que pueden estar expuestas las industrias de un país. Si se altera su correcto funcionamiento desencadenaría grandes efectos nocivos. Por lo que es necesario entender que estos sistemas deben protegerse con márgenes de seguridad amplios para contrarrestar cualquier tipo de situación inesperada.

Con las infraestructuras que están en cada país, la seguridad es mucho más que proteger contraseñas o realizar copias de seguridad y que el entorno se muestre seguro. Es decir, que la infraestructura crítica es aquella cuyo funcionamiento es trascendental que esté activa y no permite soluciones alternas y si se llegara a afectar, aunque sea levemente, impactaría profundamente en la sociedad.

La infraestructura crítica abarca desde instalaciones que ayudan a su proceso de desenvolvimiento, hasta los sistemas informáticos que apoyan la correcta operación de los ICS. La violación de una infraestructura no solo se limita a ataques informáticos; existen muchos incidentes relacionados a otros factores como deterioro de los equipos, negligencia de los pocos operadores que aún están ubicados en los ICS.

Los sectores de infraestructuras crítica incluyen**:**

- Empresas químicas
- Centros comerciales
- Empresas de telecomunicaciones
- Empresas de manufactura
- Servicios de emergencia
- Energía
- Servicios financieros

- Alimentación y agricultura
- Asistencia sanitaria
- Tecnología de la información
- Instalaciones gubernamentales
- Sistemas de transporte
- Sistemas de aguas
- Sistemas de aguas residuales

2. COMPRENDIENDO LOS CIBERATAQUES INDUSTRIALES

Existen infinidades de incidentes a los que un ICS puede enfrentar como los siguientes eventos:

- Se puede bloquear la transferencia de datos en las redes, hasta interrumpir el correcto funcionamiento de algún proceso crítico.

- Alterar las instrucciones o comandos, dañando algún equipo, software, ambiente o poner en peligro a algún ser humano.

- Cortar la información a los operadores del sistema, con la intención de realizar cambios o que se dé alguna acción inapropiada.

- Cambios en el software de los ICS o sus parámetros de configuración, infectar el software de ICS con algún malware.

- Alterar el correcto funcionamiento de los sistemas de seguridad.

Se debe restringir el acceso lógico y actividad a la red del ICS, el acceso físico tanto de los dispositivos como a la red ICS. Se debe proteger sus componentes para mantener en funcionamiento la operación del sistema en condiciones de vulnerabilidad y restaurar el sistema si ocurrió un incidente no deseado y para cumplir con los objetivos de seguridad del sistema. Es decir, debemos:

- Restringir el acceso lógico a la red del ICS y a la actividad de la red: esto incluye el uso de una arquitectura de red DMZ con los *firewalls* para evitar que el tráfico de red pase directamente sin filtro entre las redes corporativas y la del ICS, y que tenga mecanismos de autenticación y autorización con credenciales separadas para los usuarios de las redes corporativas y del ICS. El ICS también debe utilizar una topología de red que tenga múltiples capas, para que las comunicaciones más críticas ocurran en la capa más segura y fiable.

- Restringir el acceso físico a la red y a los dispositivos del ICS, de lo contrario, puede alterarse el correcto funcionamiento del ICS. Es necesario utilizar varios controles de acceso físico tales como dispositivos biométricos, cerraduras especiales, y lectores de tarjetas.

- Desplegar parches de seguridad para la protección de los componentes individuales del ICS, comprobar su funcionamiento. Restringir los privilegios de los usuarios y permitir solo los indispensables. Deshabilitar todos los puertos y servicios que no se utilizan, hacer un monitoreo a las pistas de auditoría y utilizar software antivirus y de comprobación de integridad de archivos para prevenir un malware.

- Crear un mantenimiento de las operaciones de los procesos cuando ocurren incidentes. Se puede diseñar un ICS que contenga una parte redundante. Al ocurrir una falla, se desea que no cause tráfico innecesario en el ICS o bien en otras redes y no causar más problemas al sistema.

- Al ocurrir un incidente, se debe restaurar el sistema por medio de un buen sistema de seguridad capaz de actuar con rapidez para recuperarse lo antes posible.

- Un equipo multifuncional de ciberseguridad es importante para evaluar y disminuir los riesgos a los ICS. Puede constar de una persona de IT, un ingeniero de control, un operador del sistema de control, el experto en seguridad de sistemas y redes, una persona del equipo de dirección y una persona del departamento de seguridad física. Este equipo debe contactar al proveedor del sistema de control, y también con el integrador de sistemas para su continuidad e integridad. Este equipo debe, además, reportar a la máxima autoridad del sistema o bien al responsable de la ciberseguridad del ICS.

La estrategia de “defensa en profundidad” se debe aplicar. Este diseño consiste en capas de mecanismos de seguridad, el impacto de una falla en alguno de los mecanismos de alguna capa se compensa con los de otra capa. Las sugerencias de las normas ISO 27000 y NIST SP 800, además de una gran cantidad de soluciones técnicas, ayudan a proteger a los activos informáticos.

2.1. Como sucede un ciberataque

Aunque muchos ataques cibernéticos inicialmente no estaban dirigidos a los sistemas ICS, estos incidentes fueron el resultado de gusanos generalizados de internet que se encontraban en las redes ICS a través de conexiones en la red, accesos remotos y/o medios portátiles.

Las amenazas o vulnerabilidades contra los PLC utilizados en los ICS se pueden analizar, y dividir en amenazas básicas, avanzadas y persistentes avanzadas. Las amenazas básicas pueden ser como estafas genéricas de *phishing* o ataques contra organizaciones con poca seguridad o ninguna.

Las técnicas de ataque están disponibles en el internet o de código abierto. Las amenazas pueden ser *DDos,* (Ataque distribuido denegación de servicio) extracción de datos privados o extorsión mediante herramientas o técnicas personalizadas.

Los tipos de amenazas pueden ser atacantes, operadores de red de Bot, (BOTNET) grupos criminales, servicios de inteligencia extranjeros, *insiders, Phishers, Spammers,* autores de *spyware/*malware terroristas y espías industriales.

Los controladores utilizados en la red tipo A (redes muy grandes) tienen bajo riesgo porque están aislados e independientes. Los atacantes no tendrán acceso físico desde la red hacia ella. Los operadores de red de Bot son más sofisticados que los atacantes normales y utilizan varios sistemas de redes. Podrían catalogarse como amenaza avanzada, pero siguen representando poco riesgo para los controladores de la red tipo A por la misma razón.

Grupos criminales operan de manera conjunta con el objetivo de obtener ganancias monetarias a través de su amenaza.

Los espías industriales pertenecen a la misma categoría, pero su objetivo es la propiedad intelectual y los conocimientos, siempre de forma indirecta. Su objetivo es monetario.

En el área informática existen varios tipos de amenazas; como hackers, códigos maliciosos, virus, gusanos, etc. Con el uso de internet, los ICS enfrentan ataques de denegación de servicio y amenazas combinadas, tales como integración de herramientas automáticas de hackeo, accesos no autorizados a los sistemas y capacidad de identificar y explorar las vulnerabilidades de los sistemas operativos o aplicaciones para dañar los recursos informáticos.

Las amenazas pueden ser:

- Ataques dirigidos
- Accesos y controles no autorizados
- Código malicioso o no autorizado instalado en máquinas (gusanos, virus troyanos, *spam, phishing*, Bot, etc.)
- Espionaje: representa el obtener información de forma legal como: publicidad, promociones, muestra de producto o ilegal como la intrusión, la vigilancia o robo
- Sabotaje
- Vandalismo
- Intrusión (Crackers o hackers)
- Robo (electrónico)
- Bombas de tiempo
- Puertas traseras
- DOS (*Denial of Service*)
- Falta de supervisión
- Cambios lentos
- Falta de conocimiento de los dispositivos
- No entender el tráfico
- Agujeros de autenticación

Se piensa que los ICS y las redes SCADA están físicamente separadas de las redes IT. Algunas empresas lo manejan así; otras utilizan las mismas redes LAN y WAN, pero encriptan sus ICS y el tráfico SCADA a través de una infraestructura compartida. Poco a poco las redes requieren algún tipo de interconectividad con el fin de obtener la entrada operacional de datos y/o de exportación a sistemas externos de 3PL (*third party Logistics*). Los dispositivos SCADA, a diferencia de un sistema IT convencional, tiene las siguientes características:

- Regularmente se instala en lugares difíciles de acceder físicamente, muchas veces expuestos a circunstancias ambientales. Utilizan voltajes especiales.

- Sus sistemas operativos por lo general son exclusivos y por lo mismo, no tienen reglas de seguridad.

- El software no se puede actualizar o parchear con regularidad ya que tienen limitaciones de acceso.

Estas diferencias, básicamente, son un aliciente para los atacantes debido a su infraestructura y sus contraseñas débiles. Muchas redes SCADA /ICS sí incluyen en sus sistemas algún nivel de defensa perimetral, incluyendo segmentación de red y tecnología *firewall*. Los atacantes, por naturaleza, buscan entrometerse al sistema, activando alguna operación desde el interior de una organización que deje un canal abierto de comunicación con el exterior o a través de algún puerto que se deje abierto. Dichas amenazas pueden ser:

- Uso de puerto de acceso remoto utilizado por el proveedor para el mantenimiento.

- Hackear un canal legítimo entre los sistemas de IT y los ICS/SCADA.

- Persuadir a un usuario de darle *clic* a un enlace URL dentro de un correo electrónico desde una estación de trabajo conectada tanto para la red como a internet.

- Infectar ordenadores portátiles que no pertenecen al sistema pero que se conectarán al sistema interno conectado a la red, con el fin de adquirir datos o actualizar software.

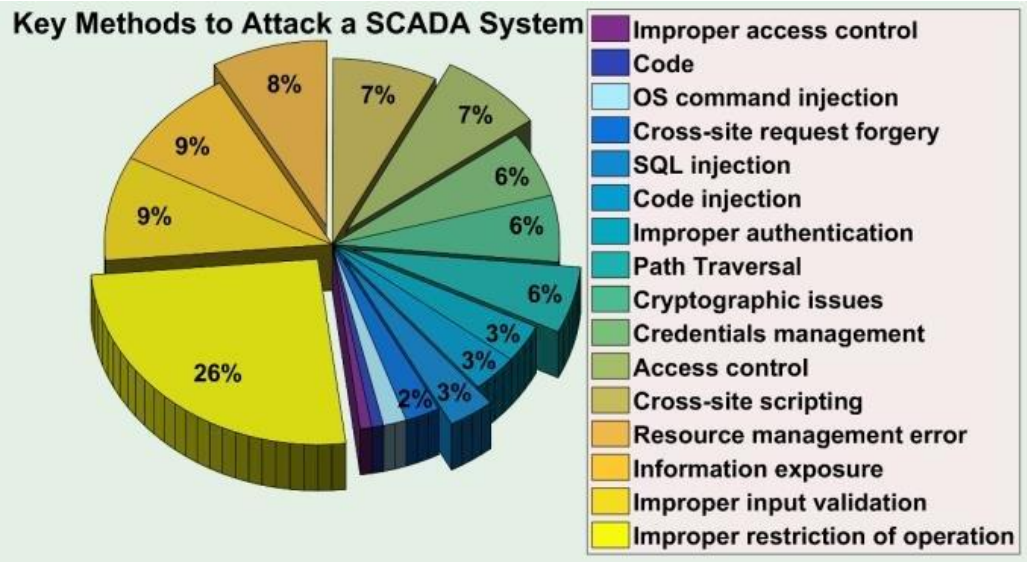
- Utilizar los errores en la configuración de seguridad.

Una vez que los hackers se han infiltrado en la red SCADA, se hace posible enviar comandos maliciosos a los dispositivos con el fin de alterar el correcto funcionamiento del sistema. Las vulnerabilidades más comunes son las siguientes:

- Vulnerabilidad de *cross-site scripting* (XSS)
- Vulnerabilidad de d*irectory transversal*
- Vulnerabilidad SQL *injection*
- Vulnerabilidad de escalado de privilegios
- Vulnerabilidad de *buffer overflow*
- Vulnerabilidad de ejecución de código arbitrario
- Vulnerabilidad de autenticación
- Vulnerabilidad de web *trojans*

- Vulnerabilidad de p*ath disclosure*
- Vulnerabilidad de DoS
- Vulnerabilidad de *spoof servers*

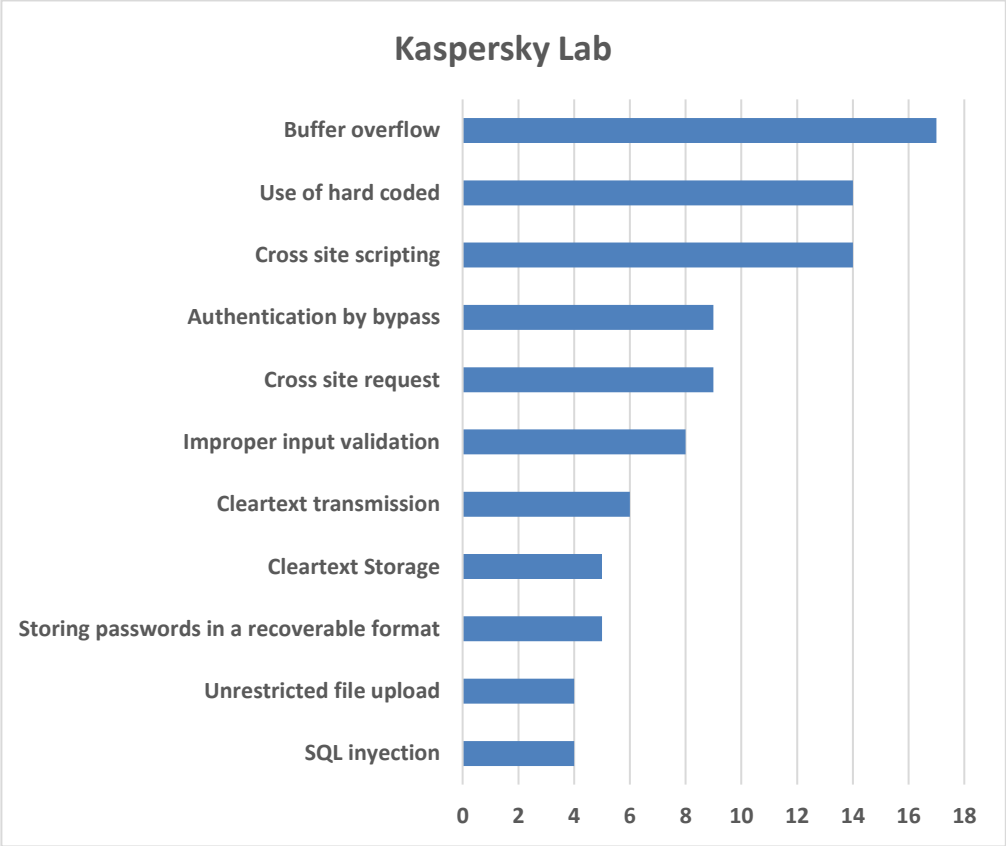
Figura 12. **Estadísticas de los métodos de ataques a los sistemas SCADA**



Fuente: Researchgate. *Métodos clave para atacar un sistema SCADA*. https://www.researchgate.net/figure/Key-methods-to-attack-a-SCADA-system-improper-restriction-of-operation-being-the-most_fig2_328083164. Consulta: 10 de abril de 2020

Las vulnerabilidades que más se presentaron en el 2015 en los sistemas ICS se han clasificado por *Kaspersky Lab*. como se muestra en la figura 13:

Figura 13. **Vulnerabilidades más frecuentes en 2015**



Fuente: elaboración propia

2.1.1. Buffer overflow

Desbordamiento buffer es un error de programación donde el software al escribir datos en el buffer sobrepasa el límite de este y sobrescribe las ubicaciones de memoria adyacentes; daña datos, bloquea el programa o causa la ejecución de un código malicioso. Esta vulnerabilidad se descubrió en diecisiete componentes diferentes de los ICS, (HMI, PLC, dispositivos de red y otros) y en ocho de los casos, tiene alto nivel de riesgo. Cuatro de estas vulnerabilidades tienen la puntuación CVSS (*Common Vulnerability Scoring*

System) más alta, diez, que corresponden al máximo impacto. Podría ser realizado por un atacante remoto no autenticado.

2.1.2. Hard-Coded credentials

Credenciales codificadas, esta vulnerabilidad crea un espacio de seguridad significativo que permite a un atacante omitir la autenticación configurada por el administrador de software. Se descubrió en catorce componentes diferentes de los ICS (HMI, PLC, dispositivos de red y otros) y contiene alto nivel de riesgo. Casi todas las vulnerabilidades que se encontraron podrían haber sido explotadas por un atacante remoto.

2.1.3. Cross site scripting

Secuencia de comandos de sitios cruzados, permite a los intrusos inyectar secuencias de comandos del cliente en páginas web vistas por los usuarios, que podrían utilizar para robar datos de autenticación de usuarios (*cookies*), realizar ataques de ingeniería social o difundir malware. Las vulnerabilidades de este tipo están presentes en catorce componentes de los ICS (la mayoría son sistemas SCADA).

2.1.4. Authentication by bypass

La autenticación por bypass se encontró en ocho tipos diferentes de componentes de los ICS, incluyendo HMI, un dispositivo de red RTU, y otros. Un atacante que explote esta vulnerabilidad puede ser capaz de capturar o modificar información privilegiada, inyectar código o eludir el control de acceso.

2.1.5. Cross site request forgery

La falsificación de petición de sitios cruzados existe cuando un servidor web está diseñado para recibir una solicitud de un cliente sin ningún mecanismo de verificación de si se envió intencionalmente. Podría ser un engaño y el cliente hace una petición involuntaria al servidor web, la cual será tratada como petición auténtica. Esto se puede hacer a través de una URL, la carga de imágenes, *XMLHttpRequest,* y se pueden exponer datos o ejecución de códigos incorrectos. Cuatro de las nueve vulnerabilidades descubiertas están presentes en los sistemas SCADA.

2.1.6. Improper input validation

La validación de entrada incorrecta no es válida o bien, valida incorrectamente las entradas que pueden afectar al flujo de datos de un programa. La mayoría de estos efectos están relacionados con la ejecución de código arbitrario. Ocho vulnerabilidades están presentes en el HMI, el sistema SCADA, RTO y el servidor OPC.

2.1.7. Cleartext transmission

La transmisión de texto no codificado se encontró en seis diferentes componentes de los ICS. Permite que un actor no autorizado detecte y/o capture datos sensibles o de seguridad críticos en un canal de comunicación porque el software transmite datos en texto sin codificar. Por ejemplo, debido a que no hay soporte SSL en la estación base de *Gateway* telemetría de Adcon A840, toda la comunicación está desencriptada, lo que hace que sea fácilmente legible a través de la red. (CVE-2015-7932 nivel medio).

2.1.8. Cleartext storage

Almacenamiento de texto no codificado: debido a que la información se almacena en texto sin formato, los atacantes podrían leerla. Incluso si la información está codificada de una manera que no sea legible para el ser humano, ciertas técnicas podrían determinar qué codificación se está utilizando y luego codificar la información.

2.1.9. Storing passwords in a recoverable format

El almacenamiento de contraseña en forma recuperable los hace vulnerables a ataques de reutilización de contraseñas por usuarios malintencionados. De hecho, debe tenerse en cuenta que las contraseñas cifradas recuperables no proporcionan ningún beneficio significativo sobre las contraseñas de texto sin formato, ya que están sujetas no solo a la reutilización por parte de los atacantes malintencionados, sino también por los intrusos. Si un administrador puede recuperar una contraseña directamente o utilizar una búsqueda de fuerza bruta en la información disponible, el administrador puede utilizar la contraseña en otras cuentas. Las HMI son las más afectadas.

2.1.10. Unrestricted file upload

La carga de archivos sin restricciones en el software permite a un atacante cargar o transferir archivos de tipo peligroso que se pueden procesar automáticamente dentro del ambiente de producción. Estas vulnerabilidades se descubrieron en cuatro componentes de los ICS, tres de ellos son sistema SCADA. Por ejemplo, a través de un *servlet,* es posible cargar código JAVA arbitrario en la versión 5.21.02 de la plataforma *AggreGate* y en versiones anteriores, y permiten que las propiedades de las aplicaciones se importen a

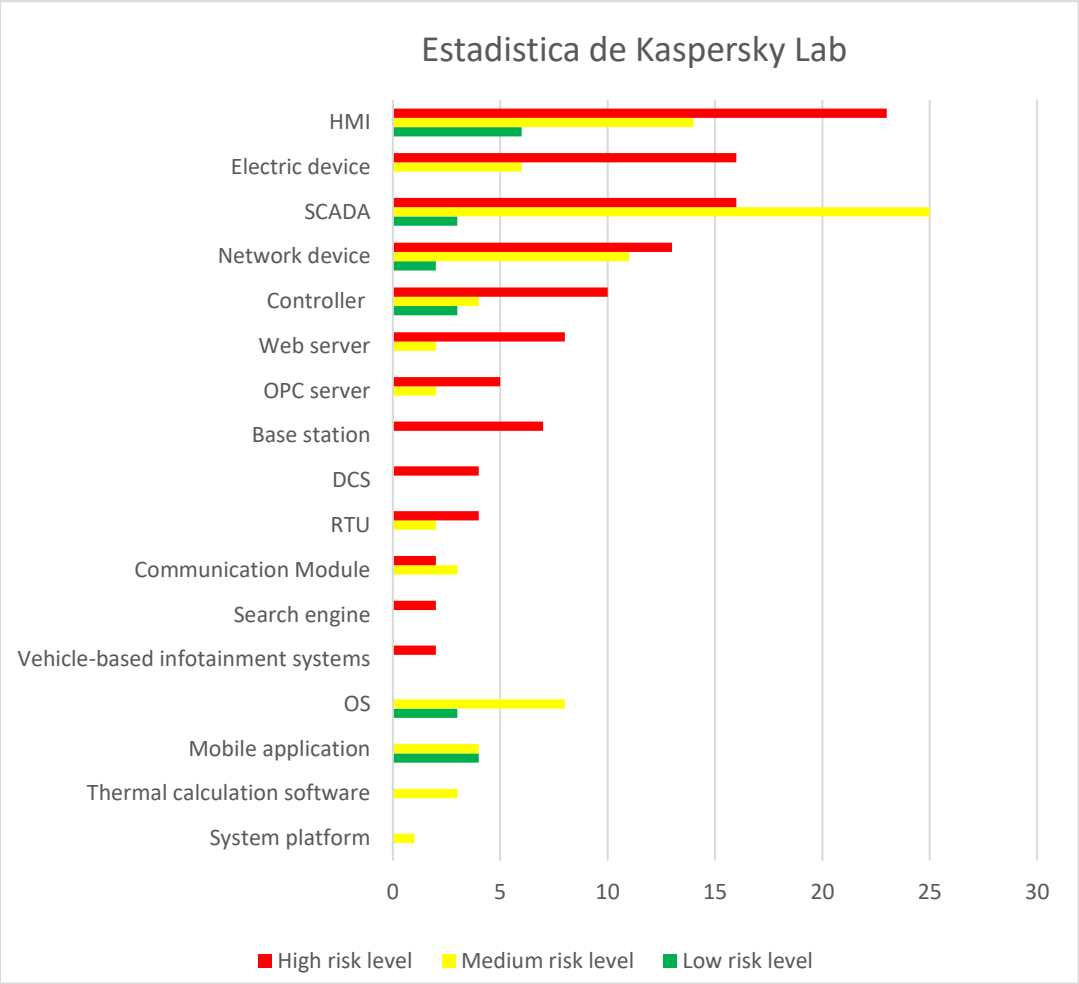
través de archivos cargados que podrían permitir la ejecución arbitraria de código y comando (CVE-2015-7912 de alto nivel).

2.1.11. SQL injection

La inyección de código SQL, describe la inserción directa de datos controlados por el atacante en variables que se utilizan para construir comandos SQL. Como resultado, un atacante puede manipular la consulta original al terminar permanente la cadena, anexando nuevos comandos. Las vulnerabilidades de este tipo están presentes en cuatro componentes de los ICS (tres de ellos son sistemas SCADA).

En un estudio estadístico realizado por *Kaspersky Lab*. se identifican a los componentes de un ICS que son los más afectados por los ataques no autorizados. A continuación, son descritos en la figura 14.

Figura 14. **Componentes afectados de un ICS**



Fuente: elaboración propia, empleando www.PLCdesign.xyz/cyberseguridad-industrial

Según se muestra en la figura 14, el componente que sufre más ataques es la HMI debido a su baja capacidad de almacenamiento y procesamiento. Se observa cómo el más recurrente es el denominado *Buffer overflow, hard-coded credentials*, y el de almacenamiento de contraseñas en formato recuperable. Por ejemplo, la vulnerabilidad de control de acceso incorrecto (CVE-2015-4051, alto nivel de riesgo) en *Beckhoff IPC Diagnostics* antes de 1,8 (HMI) permite que un atacante no autenticado pueda vulnerar el sistema al enviar paquetes ya

diseñados. Las acciones que se dan pueden reiniciar el dispositivo o añadir un nuevo usuario que sea capaz de administrar en el servidor web y en las ventanas incrustadas subyacentes.

En los dispositivos eléctricos, el problema más común es el uso de credenciales *(hard coded credentials*) (tres vulnerabilidades).

Para los sistemas SCADA, se observa que las ataques más frecuentes son *cross site scriptig* (siete vulnerabilidades) , *buffer overflow* (cinco vulnerabilidades), la falsificación de solicitudes entre sitios (cuatro vulnerabilidades) la carga de archivos sin restricción (tres vulnerabilidades), SQL *inyection* (tres vulnerabilidades) en el administrador de dispositivos de Emerson AMS antes de la versión 13, permite a los usuarios autenticados obtener privilegios administrativos mediante una entrada malformada. Veamos las fallas más comunes:

- Si el atacante vulnera algún servidor en la zona DMZ y escanea los puertos *firewall* que está localizada entre DMZ y la LAN corporativa, y este encuentra un puerto abierto, puede que sea capaz de infectar algún equipo de la red corporativa, traspasar la seguridad del *firewall/router* e intentar acceder a los equipos del centro de control y podría modificar la acción en la red.

- Se vuelve punto crítico al utilizar un solo *firewall/router* entre el bloque de red corporativa y el bloque de centro de control. En el sistema SCADA es muy importante la disponibilidad; si la comunicación se pierde entre dichos bloques e inhabilitan el *firewall/router* se denegará el servicio y el sistema no trabajará apropiadamente o lo hará de forma irregular.

- Deben mejorar la protección de sus sistemas. Un solo *firewall/route*r entre el centro de control y la red corporativa no es suficiente, así como la falta de una zona DMZ con equipos bastión del centro de control que permitan la comunicación de la red corporativa con el centro de control. Sin estos no habría la posibilidad de implementar servicio de filtrado de paquetes o de pasarelas a nivel de aplicación que permite la autenticación de los usuarios que realizan peticiones de conexión y el análisis de conexiones a nivel de aplicación.

- El protocolo que es más común en los sistemas SCADA es el *Modbus y* trabaja sobre líneas de transmisión en serie. La comunicación de estas redes es un esquema muy antiguo de petición-respuesta y hace que sea más difícil identificar un ataque ya que los sistemas no son capaces de distinguir entre peticiones legítimas o no legítimas.

- El protocolo *Modbus* está diseñado para trabajar sobre TCP, y no realiza autenticación ni tiene funcionalidades de confidencialidad de manera nativa. Si algún hacker entra a una red, es capaz de controlar una sesión.

- En el centro de control se mueven todo tipo de datos de la red corporativa, los equipos de campo y los propios. Si no hay segmentación de estas tres fuentes, un atacante podría llegar a el único segmento de red para infectar a los *routers* que se comunican con los equipos de la red de campo.

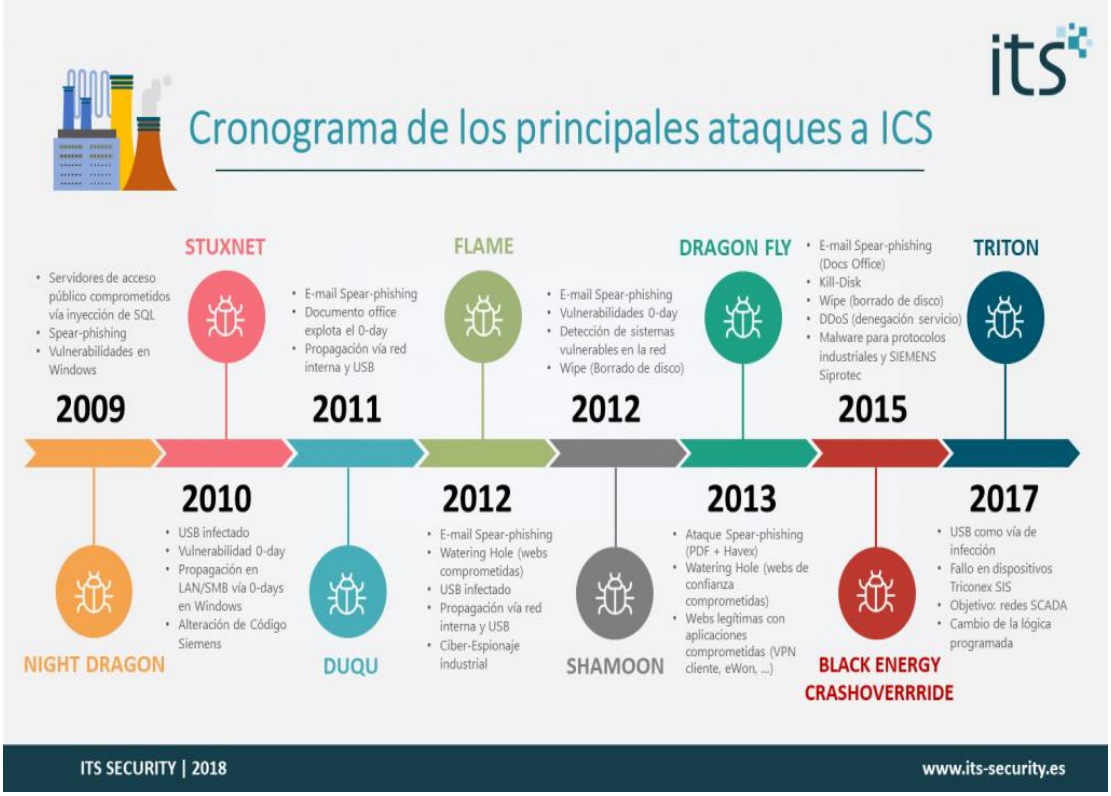
2.2. Incidentes en el mundo real

Una empresa de abastecimiento de agua Verizon experimentó patrones inexplicables de movimientos de válvulas y conductos durante un período de 50 días. Esta empresa descubrió que estaba siendo atacada y los atacantes manipulaban los productos químicos que mantienen potable el agua, alteraron los caudales del agua y causaron interrupciones en la distribución normal del agua.

En este caso, la seguridad física de esta empresa se encontraba vulnerable, sin embargo, no se reportaron fallas graves en el proceso, pues el sistema de seguridad alertó y fueron corregidos los cambios que el atacante quería alterar.

La investigación de seguridad encontró que tres direcciones de IP habían logrado tener acceso varias veces a los activos OT e IT.

Figura 15. **Cronograma de los ataques a ICS**



Fuente: Its security. *Claves de los principales ciberataques a ICS.* https://es.slideshare.net/ITS-Security/its-security-claves-de-los-principales-ciberataques-a-sistemas-de-control-industrial-ics-154464625. Consulta 15 de abril de 2020.

Observaron que todo el sistema ICS era vulnerable de la siguiente manera:

2.2.1. Contraseñas débiles

Cada consumidor del agua usaba una aplicación para el pago de su servicio y las credenciales eran débiles; nombre de usuario y contraseña, sin ningún factor de comprobación.

2.2.2. Acceso directo desde internet al sistema ICS

El servidor web orientado a internet que aloja la aplicación de pago del cliente, estaba directamente conectado por cable al sistema AS400, en donde se encontraba ubicado la gestión del SCADA que daba al administrador (y a los ciberatacantes) la facilidad de interactuar con el nivel de control.

2.2.3. Principales ataques de los ICS

Los principales ataques son los siguientes:

2.2.3.1. Night Dragon (2009)

Es un troyano de puerta trasera *(backdoor*) que se instala en un sistema utilizando un generador de troyanos, *trojan dropper,* que un atacante puede copiar en los equipos, por lo general en el momento de compartir recursos de Windows.

Los atacantes han invadido, con este sistema, empresas como multinacionales de petróleo, energía, empresas de petroquímica, con el objetivo de robar información confidencial.

2.2.3.2. Stuxnet

En 2010 se hizo notable el *stuxnet*, un malware que infectó la central nuclear Natanz (Irán), según la empresa de seguridad que los apoyó, el objetivo de *Stuxnet* era retrasar el programa nuclear iraní.

2.2.3.3. DUQU (2011)

Es una plataforma de malware altamente sofisticada que aprovecha hasta tres vulnerabilidades de día cero (ataque contra una aplicación o sistema con el objetivo de ejecutar un código malicioso).

Una parte del software es un lenguaje de alto nivel y aún es desconocido. Se le denomina como “Marco Duqu”. Las pruebas muestran que pudo haber sido escrito en lenguaje C. El robo de llaves privadas y certificados digitales son parte de las acciones de DUQU.

DUQU utiliza una imagen JPEG de 54X54 píxeles y un archivo cifrado para robar los datos y enviarlos a su centro de control. Este software malicioso se autoelimina después de 36 días.

2.2.3.4. Flame

Es un malware modular también conocido como *flamer skywiper*, descubierto en 2012, que ataca a equipos con sistema operativos Microsoft Windows. Se tiene conocimiento que se creó para ciberatacar y espiar al Medio Oriente. La universidad de tecnología de Budapest afirma que este es el malware más complejo que se ha encontrado. Tiene un tamaño de 20MB, está escrito en lenguaje de programación interpretado LUA con código C++. Ocurrida la infección de este virus, este permite que se pueda cargar módulos atacantes; además, utiliza cinco métodos de cifrado y para almacenar la información, crea una base de datos SQLite.

Flame puede propagarse a otros sistemas de la red LAN y mediante memoria USB, puede grabar audio capturas de pantalla, pulsaciones de teclado y tráfico de red.

2.2.3.5. Shamon

Es un virus conocido más como W32, *DistTrack.* Fue descubierto en 2012 con un comportamiento diferente de otros ataques de malware*,* debido a que es destructivo y es catalogado como el más destructivo de todos, pues se puede propagar desde una máquina infectada a otras. Si logra infectar un sistema, el virus recopilará archivos de ubicaciones específicas en el sistema, cargándolos al atacante y borrándolos. Este virus es parte de la guerra cibernética que han surgido contra las compañías petroleras nacionales de Arabia Saudita, Aramco y Rasgas de Qatar.

2.2.3.6. Dragonfly (2013)

Es un grupo de ciberespionaje que se cree que son parte de un colectivo de Europa conocido como *Dragonfly* que operan desde 2011. Tiene como objetivo atacar operadores de redes de energía y proveedores de equipos industriales tales como petróleo, agua, gas y datos por espionaje. Ochenta y cuatro países se vieron afectados, aunque la mayoría de las víctimas estaban en Estados Unidos, España, Francia, Italia, Alemania, Turquía y Polonia. Pero ha reaparecido en los años siguientes. El grupo *Dragonfly* está interesado tanto en aprender cómo operan las instalaciones de energía como en obtener acceso a los sistemas operativos. *Dragonfly* utiliza una variedad de vectores de infección en un esfuerzo por obtener acceso a la red de la víctima, incluidos correos electrónicos maliciosos y ataques de abrevaderos y software troyano.

2.2.3.7. Black energy crashoverride

Es el primer malware diseñado (2015) e implementado para atacar redes eléctricas. Es el cuarto del malware diseñado para atacar ICS, y para interrumpir procesos industriales físicos. Sus componentes principales son:

- Una puerta trasera principal para controlar todos los demás componentes del malware. Se conecta a sus servidores remotos, y controla para recibir comandos de los atacantes.

- Un componente iniciador, que es un ejecutable independiente responsable del lanzamiento de los componentes de la carga útil y limpiador de datos.

- Cuatro componentes de carga útil se dirigen a protocolos de comunicación industrial particulares especificados en las siguientes normas: IEC 60 870-5-101 IEC 61 850 y OLE para el acceso a datos de control de proceso.

- Un componente de limpieza de datos que está diseñado para borrar claves de registro en un sistema y sobreescribir archivos para que el sistema no se pueda arrancar y la recuperación del ataque sea más difícil.

2.2.3.8. Tritón

Es un virus malware de código basado en entrar en las redes e infraestructuras, y sabotear sus sistemas industriales. Lo han utilizado en plantas energéticas, refinerías de petróleo, donde es capaz de controlar

operaciones de estas instalaciones. En agosto de 2017, los ciberatacantes infectaron una petroquímica situada en Arabia Saudí con el objetivo no solo de inutilizar sus instalaciones sino también de hacerlo volar por los aires. Se vieron comprometidos cuando la tecnología de seguridad industrial Triconex hecha por Schneider Electric los detectó y tomó cartas en el asunto. La compañía de seguridad *Symantec* afirmó que Tritón explotó una vulnerabilidad en los computadores que ejecutan el sistema operativo Microsoft Windows.

3. ADMINISTRACIÓN Y EVALUACIÓN DE RIESGO EN ICS

Son tantas las vulnerabilidades de los sistemas ICS, que se recomienda a toda empresa que tome una evaluación de seguridad cibernética. Pueden empezar con una autoevaluación, o bien tomar la decisión de contratar empresas que se encarguen de dicha tarea.

3.1. Manejo de riesgo

Todos los días, las empresas se ven en la necesidad de evaluar sus procedimientos de trabajo y tener riesgos; pueden tener fallas en los equipos, del personal o financieros. Se ven en la necesidad de desarrollar procesos para evaluar los riesgos asociados a su entorno y deben tomar decisiones de cómo enfrentar dichos riesgos según las prioridades de su organización. Esta gestión de riesgo se realiza como un proceso interactivo y continuo, a través de buenas prácticas en seguridad e ingeniería. Estas prácticas siguen un protocolo establecido por reglamentos. La gestión de riesgos de seguridad de la información es una dimensión adicional que puede ser complementaria.

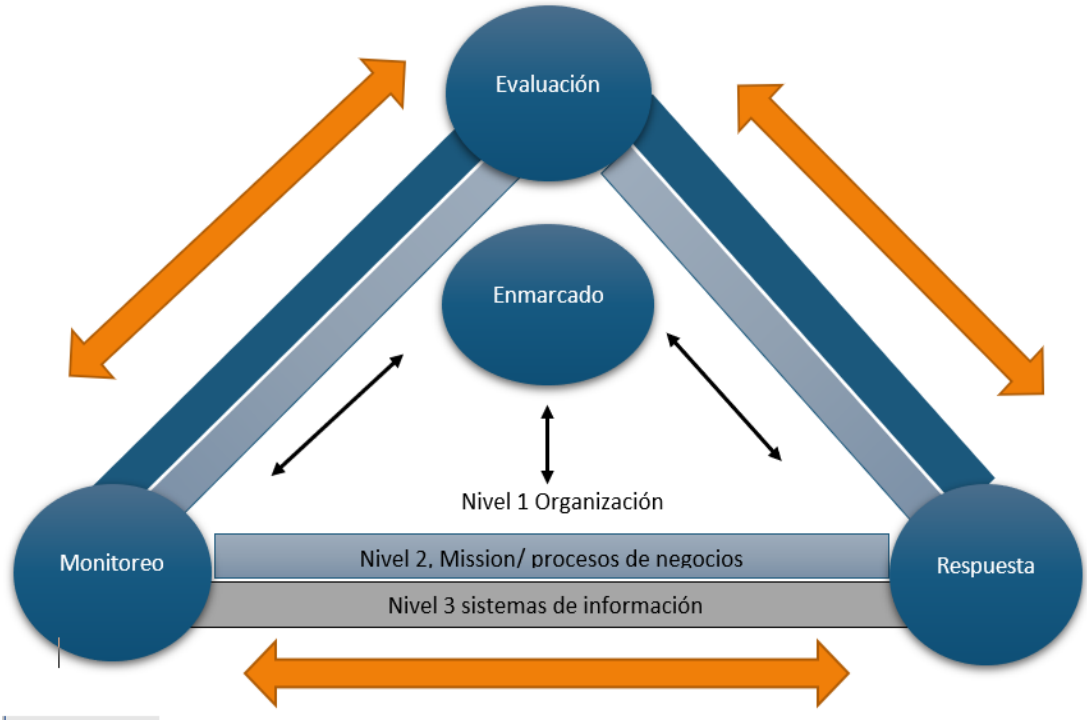
Para usar un proceso de gestión de riesgo, es importante tener tres niveles a los cuales se presenta el riesgo:

- Organización
- Misión/nivel de proceso
- Nivel de sistema de información (IT en ICS)

El proceso de manejo de riesgo se maneja en los tres niveles para mejorar las técnicas de riesgo de la organización y las técnicas de comunicación efectiva entre niveles y las pertenecientes a cada nivel, y en aquellas áreas que tienen un mismo interés en la misión y éxito empresarial de la organización.

El proceso de gestión de riesgos tiene cuatro componentes, como se muestra en la figura 16: enmarcado, evaluación respuesta y monitoreo. Cada una es interdependiente y a menudo ocurren de forma simultánea. Como el entorno en el que operan las organizaciones siempre está cambiando, la gestión de riesgos debe ser un proceso continuo en el que todos los componentes tengan actividades en curso.

Figura 16. **Proceso de gestión de riesgo**



Fuente: elaboración propia.

El componente de enmarcado en este proceso desarrolla un marco en las decisiones de gestión de riesgos a tomar. El nivel de riesgo que una empresa puede aceptar se deriva del grado de tolerancia que tienen al riesgo.

El componente de enmarcado debe incluir la revisión de la documentación existente, como evaluaciones previas de riesgos. Puede haber actividades relacionadas como la planificación de la gestión de desastres en toda comunidad que también debe considerarse, pues son requisitos que se toman en cuenta a la hora de una evaluación de riesgos.

.

El componente de evaluación requiere que las organizaciones identifiquen sus amenazas y vulnerabilidades, el daño que pueden causar a la organización y la probabilidad de que ocurran eventos adversos derivados de estos.

El componente de respuesta se basa en el concepto de una respuesta consistente de toda la organización a la identificación del riesgo. La respuesta a la identificación del riesgo (en oposición a la respuesta a un incidente) requiere que las organizaciones primero identifiquen posibles cursos de acción para abordar el riesgo, que evalúen esas posibilidades para obtener tolerancia al riesgo en la organización, y tomar en cuenta otras circunstancias que surgen en el momento de encuadre, para elegir la mejor opción para ellos.

En el componente de respuesta se debe incluir la implementación de las acciones que se han elegido para apoyar el riesgo que se ha establecido; tales como mitigación, transferencia, evasión o bien estas opciones combinadas.

El cuarto componente en el análisis de riesgos es el monitoreo. Todas las organizaciones monitorean el riesgo de forma permanente e incluyen la implementación de estrategias, cambios que sean necesarios para calcular el

riesgo, y crear las actividades eficientes para la reducción de riesgos. Estas actividades afectan los demás componentes.

3.2. Consideraciones para realizar un análisis de riesgo

La naturaleza de los ICS significa que una organización que hace un análisis de riesgo, puede que haga consideraciones adicionales que no existen cuando se hace un análisis de riesgo tradicional en el sistema IT. Debido a que el impacto de un ciberincidente en un ICS puede incluir ambos efectos, físicos y digitales, el análisis de riesgo debe incorporar esos efectos potenciales. Se debe analizar lo siguiente:

- Impactos en seguridad y uso de evaluaciones de seguridad.

- Impactos físicos de un incidente cibernético en los sistemas ICS incluyendo los ámbitos físicos, efectos en el proceso controlado y el efecto en el ICS.

- Qué consecuencias existen en la evaluación de riesgos en componentes de control que no son digitales de un ICS.

3.2.1. Seguridad dentro de una evaluación de riesgos de seguridad de la información de un ICS

La cultura de seguridad y evaluaciones de seguridad está bien establecida dentro de la mayoría de la comunidad de usuarios de los ICS.

Las evaluaciones de riesgo de seguridad de la información deben verse como complementarios de tales evaluaciones, aunque las evaluaciones pueden

usar diferentes enfoques y cubrir diferentes áreas. Las evaluaciones de seguridad se refieren principalmente al mundo físico. Las evaluaciones de riesgos de seguridad de la información se centran por lo general en el mundo digital. Sin embargo, en un entorno ICS, lo físico y lo digital están entrelazados y pueden producir una superposición significativa. Es importante que las organizaciones consideren todos los aspectos de la gestión de riesgos para la seguridad (por ejemplo, tolerancia al riesgo), así como los resultados de la evaluación de seguridad, al realizar evaluaciones de riesgo para la seguridad de la información. El personal responsable para la evaluación de riesgos de seguridad de la información debe poder identificar y comunicar la identidad de los riesgos que podrían tener implicaciones de seguridad. Por el contrario, el personal encargado de las evaluaciones de riesgos de seguridad de la información debe conocer qué impactos físicos puede haber y cuál es su posible incidencia.

3.2.2. Impactos físicos potenciales de un incidente de un ICS

Al evaluar el daño físico potencial de un incidente cibernético debe incorporar lo siguiente:

- Cómo un incidente podría manipular la operación de los sensores y actuadores al impactar el entorno físico.
- Qué controles redundantes existen en el ICS para prevenir el impacto.
- Cómo un incidente físico puede surgir basado en estas condiciones.

Un impacto físico puede afectar negativamente al mundo circundante a través de múltiples formas, incluyendo la liberación de materiales peligrosos

(como contaminación, petróleo crudo, entre otros) fuerzas cinéticas dañinas (como explosiones) y exposición a fuentes de energía (electricidad o vapor). El incidente físico podría afectar negativamente el ICS y la infraestructura de soporte, los diversos procesos realizados por el ICS, o el entorno físico más amplio. Una evaluación del potencial del impacto físico debe incluir todas las partes de un ICS, empezando con una evaluación de los impactos potenciales en los sensores y actuadores.

Al evaluar el impacto de un incidente cibernético en el entorno físico debe enfocar un daño potencial a la seguridad humana, los entornos ambientales y otras infraestructuras críticas. Los impactos en la seguridad humana deben evaluarse en función de si es posible sufrir lesiones, enfermedades o la muerte por un fallo en el funcionamiento del ICS. Esto debe incorporar cualquier evaluación de impacto en la seguridad realizada previamente por la organización con respecto a los empleados y al público en general.

Los impactos ambientales también pueden necesitar ser abordados. Este análisis debe incorporar cualquier evaluación de impacto ambiental disponible realizada por la organización para determinar cómo un incidente podría afectar los recursos naturales y la vida silvestre a corto o largo plazo.

Además, debe tenerse en cuenta que el ICS puede estar ubicado dentro de una única ubicación controlada y puede distribuirse en un área física amplia y exponerse a entornos no controlados.

Finalmente, el impacto en el entorno físico debería explorar la medida en que un ataque pueda afectar la infraestructura externa al ICS, (por ejemplo: empresas de generación y distribución de electricidad, infraestructuras de transporte y servicios de agua).

3.2.3. Impacto de la interrupción de un proceso ICS

Además del impacto en el ambiente físico, la evaluación de riesgo debería evaluar los efectos potenciales al proceso físico realizado por el ICS bajo consideración, tanto como a otros sistemas. Un incidente que impacta el ICS e interrumpe el proceso de dependencia puede causar impactos en cascada en otros procesos relacionados con el ICS y la dependencia del público en general de los productos y servicios resultantes. El impacto en los procesos ICS podrían relacionar tanto sistemas como procesos dentro de la organización o sistemas y procesos externos a la organización (por ejemplo, una empresa de servicios públicos que vende energía generada a una planta cercana).

Un ciberincidente también puede impactar negativamente al ICS físico en consideración. Este tipo de impacto primario incluye la infraestructura física de una planta (por ejemplo, depósitos, tanques, válvulas, motores, entre otros) junto a mecanismos de control digitales y no digitales (por ejemplo, cables, PLC, válvulas de presión). El daño al ICS, o la planta física puede causar interrupciones a corto o largo plazo, dependiendo de cómo ha sido el incidente. Un ejemplo de un incidente cibernético es el malware s*tuxnet*, que dañó las centrífugas e interrumpió los procesos dependientes.

3.2.4. Incorporación de aspectos no digitales dentro de las evaluaciones de impacto

Los impactos en los ICS no se pueden determinar adecuadamente al enfocarse solo en los aspectos digitales de un sistema, ya que hay, a menudo, mecanismos no digitales disponibles que proveen tolerancias a fallas y previene que el ICS actúe fuera de los parámetros aceptables. Por lo tanto, estos mecanismos pueden ayudar a reducir algún impacto negativo que un incidente

digital realice en un ICS y se debe incorporar dentro del proceso de evaluación de riesgos. Los ICS a menudo tienen mecanismos no digitales de control, que evitan que el ICS opere fuera de un límite seguro logrando que se atenúe los resultados de un ataque (ejemplo: una válvula de presión de alivio mecánica). Además, se pueden usar mecanismos analógicos para observar el estado del sistema físico para proporcionar a los operadores datos confiables si las lecturas digitales no están disponibles o están dañadas. La tabla III proporciona una categoría de los mecanismos de control no digitales que podrían estar disponibles para reducir el impacto de un incidente de ICS.

Tabla III**.** **Categorías de los mecanismos de control**

Tipo de sistema	Descripción
Pantalla analógica o alarmas	Mecanismos no digitales que miden y muestran el estado de un sistema físico (tales como: presión, voltaje, temperatura, corriente) y proveen al operador, información en situaciones en las que no hay pantallas digitales. Se puede dar la información al operador en una pantalla que no sea digital, (termómetros, válvulas de presión entre otros) y mediante alarmas audibles.
Mecanismos de control manual	Los mecanismos de control manual (controles de válvulas, interruptores) brindan a los operadores la habilidad de controlar manualmente un actuador sin depender del sistema de control digital. Esto asegura que se puede controlar un actuador incluso si el sistema de control no está disponible.
Sistemas de control analógicos	Controlan un proceso físico usando sensores y actuadores no digitales. Cuando no están disponibles los sistemas de control digital, los sistemas de control analógico pueden evitar que se dé un estado no deseado en el proceso físico. Dentro de estos dispositivos están: reguladores, relés electromecánicos.

Fuente: elaboración propia.

Determinar el impacto potencial que un incidente cibernético puede tener en un ICS debería incorporar análisis de todos los mecanismos de control no digitales y en la medida en que pueden mitigar los posibles impactos negativos para el ICS. Existen múltiples consideraciones que se toman en cuenta en la posible mitigación de los mecanismos de control no digitales:

- Es posible que se necesite realizar un monitoreo o bien funciones de control extras que implican inversión de tiempo adicional y una persona

que realice estas actividades. Por ejemplo, cuando un operador necesite realizar dichas funciones de control y tenga que moverse a diferentes lugares, dando resultados lentos en comparación de si dichas acciones son realizadas con controles automatizados.

- Sistemas manuales o analógicos: pueden proporcionar capacidades de monitoreo o control con el mismo grado de precisión y confiabilidad de los sistemas de control digitales. Por ejemplo, un relé de protección digital proporciona una detección de fallas más precisas y confiables que los relés análogos o estáticos, siendo posible que el sistema detecte la activación falsa de un relé cuando no estén disponibles los relés digitales.

3.2.5. Incorporando el impacto de los sistemas de seguridad

Los sistemas de seguridad pueden también reducir el impacto de un ciberataque a los ICS. Los sistemas de seguridad están regularmente desarrollados para ejecutar funciones de monitoreo específico y control para garantizar la seguridad de las personas, del ambiente, de los procesos y de los ICS. Mientras estos sistemas son implementados tradicionalmente para ser completamente redundantes con respecto principalmente a los ICS, ellos no pueden proveer redundancia completa de los ciberincidentes, específicamente de un ataque sofisticado. El impacto de los controles de seguridad implementados en el sistema de seguridad deberá ser evaluados para determinar que ellos no tienen impacto negativo al sistema.

3.2.6. Considerando la propagación del impacto a un sistema conectado

Es importante considerar cuando se esté realizando una evaluación del impacto de un incidente, cómo podría afectar a un ICS o bien al sistema conectado. Un sistema ICS que esté conectado a otros sistemas y que presente fallas, puede afectar a estos otros sistemas tanto dentro como fuera de la organización.

El impacto de la propagación puede ocurrir debido a ambas dependencias físicas y lógicas. La comunicación apropiada de los resultados de las evaluaciones de riesgos a los operadores de sistemas y procesos conectados o interdependientes es una manera de mitigar dichos impactos.

El daño lógico a un sistema ICS interconectado puede ocurrir si el ciber incidente se propagara a los demás sistemas de control que estén conectados con el ICS. Por ejemplo: si un virus se propaga e impacta al sistema físico de un ICS, podría afectar otros dominios físicos relacionados.

Por ejemplo, el impacto podría resultar ser un peligro físico, el cual degrada los entornos físicos cercanos. Además, el impacto podría también degradar las dependencias compartidas comunes, o provocar daño del material que es indispensable en el proceso industrial.

4. DESARROLLO E IMPLEMENTACIÓN DE UN PROGRAMA DE SEGURIDAD ICS

En este capítulo se combinan dos conceptos que conciernen a cómo desarrollar e implementar un programa de seguridad para un sistema ICS. Para lograrlo, debemos integrar los planes y programas con una buena base de experiencia de seguridad en IT, programas, prácticas, etc., pero enfocadas en cumplir con los requerimientos y características específicas de la tecnología ICS.

Las organizaciones deben estar conscientes de revisar y actualizar los programas y planes de seguridad de los ICS; además, reflejar los cambios de tecnología operacional, estándares y regulaciones.

La integración efectiva de la seguridad dentro de un sistema ICS, requiere definir y ejecutar un programa integral que direcciona todos los aspectos de seguridad que van desde identificar objetivos en todo momento de su operación, hasta cumplimientos de auditorías y mejoramiento.

Una administración adecuada de manejo de seguridad para un sistema ICS, debe poseer responsabilidad, objetivos claros y deben ser identificada su autoridad.

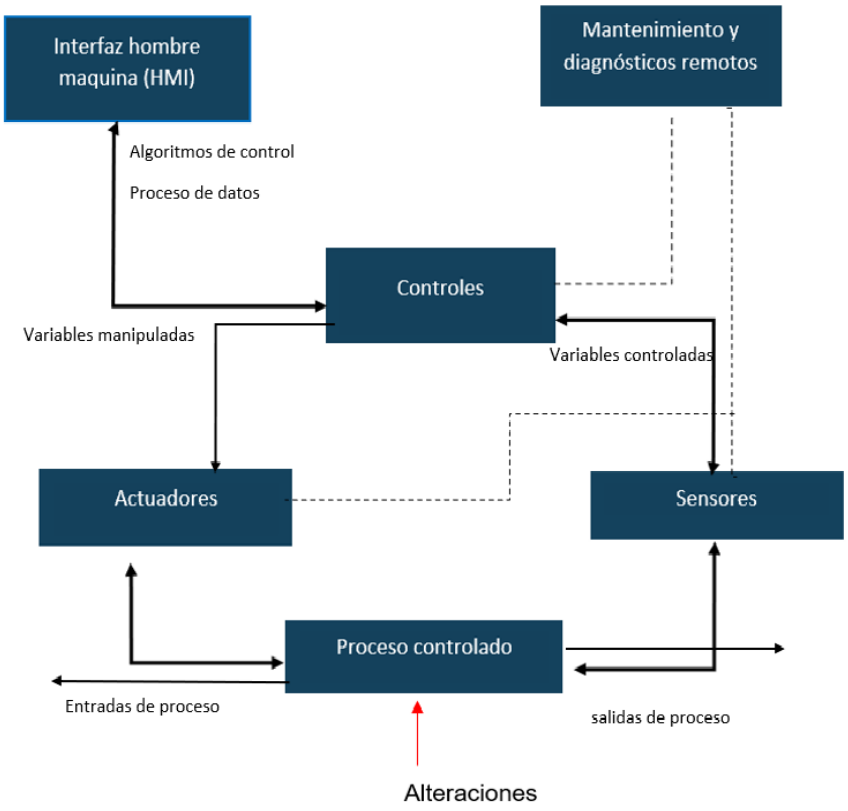
Los pasos indispensables que hay que desarrollar en un programa de seguridad para un sistema ICS, son los siguientes:

- Desarrollo de un caso para seguridad de negocio
- Construir y desarrollar un equipo funcional de seguridad
- Definir procedimientos y alcances
- Definir y especificar políticas y procedimientos
- Implementar un manejo de riesgo
- Proveer entrenamiento, crecimiento y concientización al *staff* del ICS

NIST ha publicado una guía de seguridad en los sistemas de control ICS, la cual pretende incrementar la seguridad de los ICS. Incluye los sistemas SCADA, los sistemas de control distribuidos y otros sistemas de control que forman parte del sistema ICS.

La estructura propuesta es:

Figura 17. **Estructura de seguridad de un ICS**



Fuente: elaboración propia, empleando www.incibe-cert.es.

4.1. Beneficio

Las políticas de manejo de riesgos deberían estar enfocadas en medir y monitorear los sistemas ICS para proteger los intereses de empleados, público, accionistas, clientes, proveedores, sociedad y la nación. El análisis de riesgos debe permitir costos y beneficios que deben ser considerados para tomar decisiones de acciones de protección. Al reducir los riesgos, y ejercer las debidas acciones en la muestra de responsabilidad, se ayuda a que la organización obtenga los siguientes beneficios:

- Mejorar la seguridad de los sistemas de control permitiendo fiabilidad y disponibilidad.
- Mejorar la moral de los empleados, su lealtad y retención.
- Reducir las preocupaciones de la comunidad.
- Cumplir requisitos reglamentarios.
- Mejorar la imagen y reputación corporativa.
- Ayudar con la cobertura del seguro y costo de este.
- Mejorar las relaciones entre la banca e inversionistas.

Un programa de seguridad de información y seguridad de activos muy completo es indispensable para la sostenibilidad del modelo de negocio.

Mejorar los sistemas de control específica políticas de seguridad que pueden potencializarse y mejorar la confiabilidad y fiabilidad. Con esto logramos disminuir el impacto involuntario de manera inapropiada de los ICS, debido a pruebas, políticas y sistemas que se han desconfigurado.

4.2. Consecuencias potenciales (de los incidentes)

La empresa *Kaspersky Lab* y *Business Advantage* revelaron, en una encuesta, que el 83% de los participantes, creen estar preparados para afrontar incidentes de ciberseguridad en los ICS; sin embargo, la mitad de las empresas reportaron haber tenido un incidente de seguridad en los últimos 12 meses. La ciberseguridad industrial mal diseñada les ha costado a las organizaciones pérdidas de más de $ 497 000 por año.

Las consecuencias más fuertes reportadas por los ciberataques industriales incluyen daños a la calidad del producto y servicios, pérdida de

patentes o información confidencial, también reducción o pérdida de la producción.

De las empresas a las que se les realizó la encuesta, aproximadamente la mitad reveló que algunos proveedores externos pueden acceder a las redes de control industrial de su empresa, lo que incrementa el riesgo.

Por tanto, podemos deducir la importancia de los sistemas de seguridad en los ICS. Estos deben enfatizarse en la manera que aumente la dependencia de la empresa a la conectividad. Los ataques de negación del servicio (Dos) y malware (gusanos, virus, entre otros) se han vuelto comunes para todos e impactan en los ICS. La mayoría de los impactos se caracterizan en:

- Impactos físicos: son todas aquellas consecuencias directas a fallas del ICS, los efectos potenciales de primordial importancia incluyen daño al personal y pérdidas de vidas. Otros efectos pueden ser pérdida de propiedad de la compañía (información) y daños potenciales.

- Impactos económicos: estos afectan un segundo plano después de que haya ocurrido el impacto físico debido a un incidente del ICS. Los impactos físicos podrían resultar en repercusiones a las operaciones de los sistemas, las cuales causan pérdidas económicas en la planta, organización o bien en otras dependencias de los ICS. La inhabilitación de la infraestructura crítica, por ejemplo, la energía eléctrica o su transporte, pueden impactar de forma económica, con más auge que los sistemas físicos directos. Estos efectos negativos pueden ser a nivel local, regional o incluso a la economía global.

- Impactos sociales: otro de los efectos en segundo plano es la pérdida de la confianza nacional o pública de una organización; es una consecuencia que podría resultar de un incidente en un ICS.

Existen consecuencias negativas de no tomar las precauciones de seguridad cibernética adecuadas para la industria:

- Paro total de las actividades de la planta.
- Accidentes dentro de la planta que pueden tener consecuencias fatales. como la muerte de algún personal de esta.
- Secuestro de información personal como claves de acceso.
- Impacto económico debido a la suspensión de labores.
- La confiabilidad de la empresa se puede ver afectada tras un ataque cibernético.
- Fuga de información.
- Impacto en seguridad nacional, actos de terrorismo.
- Reducción o pérdidas de producción en sitio o múltiples sitios.
- Daños ambientales.
- Contaminación de productos.
- Pérdida de información confidencial.
- Pérdida de imagen o confianza de la marca.

Los incidentes indeseables de cualquier tipo restan valor a una organización, pero los incidentes de seguridad pueden tener impactos negativos a más largo plazo que otros tipos de incidentes en todos los interesados: empleados, accionistas, clientes y comunidades.

4.3. Recursos para construir la situación

La industria ha respondido a las amenazas de ciberseguridad creando estándares para ayudar a los usuarios finales y a proveedores de equipos a través del proceso de asegurar los sistemas de control industrial. Hay una serie de estándares clave disponibles en el mercado hoy.

Se ha creado un conjunto de normas denominadas ISA99 con el objetivo de crear una base para la seguridad de los sistemas de control; así se logra incrementar la protección de estos sistemas contra los ataques informáticos. La ISA creó diferentes conjuntos de normas que son las siguientes:

- ANSI/ISA-99.01.01-2007, *Security for industrial automation and control systems: concepts, terminology and models*. (Seguridad para sistemas de automatización y de control industrial: conceptos terminología y modelos). Este documento es el primero que se creó, y describe las bases que se utilizarán en el resto de la serie.

- ANSI/ISA-TR99.01.02.2007, *Security technologies for manufacturing and control systems*. (Tecnologías de seguridad para sistemas de fabricación y control). Este documento se creó con el objetivo de hacer revisiones periódicas y recolectar aspectos nuevos del mercado. Incluye ciertas herramientas de seguridad describiendo como implementarlas y configurarlas en los ICS.

- ANSI/ISA-99.02.01-2009, *Establishing an industrial automation and control systems security program*. (Establecimiento de un programa de seguridad de sistemas de automatización y control industrial). Documento que fue el último en publicarse de esta serie de ISA99.

Recolecta los elementos indispensables para crear un sistema de gestión de seguridad. Incluye una guía que contiene los requerimientos de sus elementos.

- ANSI/ISA-99.02.02, *Operating an industrial automation and control system security program.* (Operación de un programa de seguridad del sistema de automatización y control industrial). Este documento no logró concretarse; tenía como objetivo la operación, diseño e implementación del programa de seguridad de un ICS. Esta operación del programa incluía parámetros tales como medir la efectividad del programa para cuantificarlo.

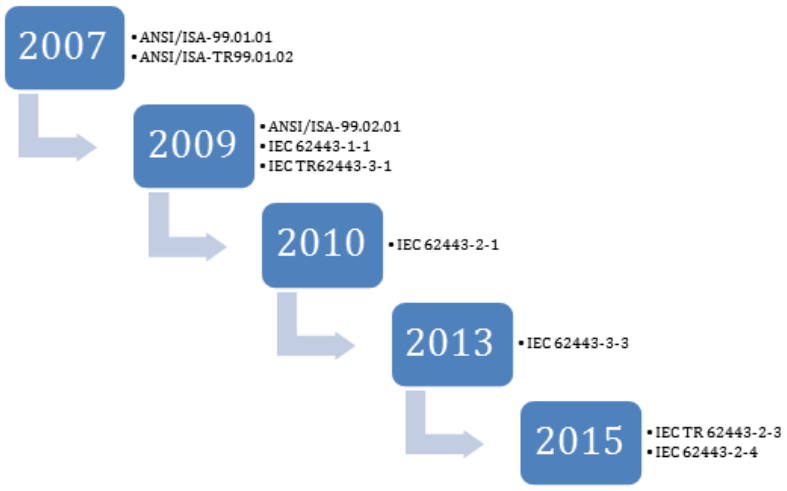
- ANSI/ISA–99.03.xx, *Technical security requirements for industrial automation and control systems*. (Requisitos técnicos de seguridad para sistemas de automatización y control industrial). Este documento no logró realizarse, aunque incluía una descripción de las características de automatización industrial y de los ICS que son diferentes a los de los sistemas IT en cuanto a seguridad, y definía sus requerimientos propios de estos sistemas. Existen dos aspectos de las medidas ISA99 muy importantes y son *security zones y conduits* (zonas de seguridad y conductos).

Security zone: es un conjunto de activos físicos o bien lógicos que contienen aspectos de seguridad comunes. Esta zona limita el grupo y realiza un límite lógico o físico separando los componentes externos e internos.

Conduit: se define como el conducto de comunicación entre las zonas de seguridad de forma confiable. Desde el punto de vista de la seguridad, este

aspecto es muy importante y logra que de manera individual se pongan las medidas de seguridad a los activos.

Figura 18. **Publicaciones ISA99 e IEC 62443**



Fuente: Incibe-cert. *IEC 62443: Evolución de la ISA 99.* https://www.incibe-cert.es/blog/iec62443-evolucion-isa99. Consulta 22 de abril de 2020.

Desde el 2010, los documentos de ISA99 evolucionan y desde entonces se denominan normas ANSI/ISA-62443, alineando los documentos con los de IEC. Desde esta fecha, ya no se sigue desarrollando la ISA99 y se empieza a crear las estrategias de la IEC 62443 con los informes técnicos.

IEC 62443 ha sido desarrollado por los comités ISA99 e IEC para mejorar la seguridad, disponibilidad, integridad y confidencialidad de los componentes o sistemas utilizados en automatización industrial y control. Se puede utilizar la serie de normas IEC 62443 en todos los segmentos de control industrial, y ha sido aprobado por muchos países. IEC 62443 está evolucionando para

convertirse en un estándar clave en la industria. La norma IEC 62443 incluye el concepto de niveles de garantía de seguridad.

En las normas IEC 62443 se integra lo establecido en ISA99, y las primeras publicaciones corresponden a lo que ya se publicó por ISA99, pero actualizadas y modificadas a los nuevos ICS. A continuación, se describen las normas IEC 62443:

- IEC 62443-1-1 *Models and concepts,* modelos y conceptos: Primer documento que publicó la ISA99.

- IEC TR 62443-1-2 *Máster glossary of terms and abbreviations,* glosario principal de términos y abreviaturas.

- IEC 62443-1-3 *System security compliance metrics,* describe las medidas de cumplimiento de seguridad en el sistema.

- IEC TR 62443-1-4 *Security life cycle and use cases,* ciclo de vida de seguridad y uso de casos: ve los aspectos del ciclo de vida de seguridad de los ICS y ejemplos de su uso.

- IEC 62443-2-1 *Requirements for an IACS security management system,* requisitos para un sistema de gestión de seguridad IACS.

- IEC TR 62443-2-2 *Operating a control systems security program,* operando un programa de seguridad de un ICS.

- IEC TR 62443-2-3 "*Patch management in the IACS environment*" gestión de parches en el entorno IACS.

- IEC 62443-2-4 *Certification of IACS supplier security policies and practices,* certificación de políticas y prácticas de seguridad de proveedores de IACS.

- IEC TR62443-3-1 *Security technologies for IACS,* tecnologías de seguridad para los IACS. Es una actualización del publicado dentro de la ISA 99 ANSI/ISA-TR99.01.02-2007.

- IEC 62443-3-2 *Security risk assessment and system design,* evaluación de riesgos de seguridad y diseño de sistemas. Describe los conceptos de *security zone y conduit* introducidos en la ISA99.

- IEC 62443-3 *System security requirements and security levels.* Requisitos de seguridad del sistema y niveles de seguridad. Esta norma crea una interrelación entre los requisitos que se definen en IEC 62443-1-1. El rendimiento tanto como la disponibilidad no deben afectarse cuando se toman en cuenta estos aspectos

- IEC 62443-4-1 *Product development requirements.* Requisitos de desarrollo de productos. Define el proceso de desarrollo que tienen que llevar a cabo los nuevos dispositivos que se crean para los sistemas de control, aunque también puede ser aplicado a los dispositivos ya existentes.

- IEC 62443-4-2 *Technical security requirements for IACS components,* requisitos técnicos de seguridad para componentes IACS. En este documento se incluyen los aspectos no publicados de ANSI/ISA-99.03.03 y reúne los aspectos técnicos que mejoran la seguridad de los componentes de una red industrial en forma individual.

El concepto de defensa en profundidad es uno de los principales objetivos de la IEC 62443, al hacer un análisis de los conceptos descritos por ISA99 y ampliar la seguridad desde los fabricantes hasta los operadores del sistema. La mayoría aún está en fase de desarrollo y revisión, se han integrados los cambios los ICS. EL IEC 62443 se ha convertido el estándar más relevante en el tema seguridad.

4.4. Construyendo y entrenando al grupo funcional

Construir y desarrollar un equipo de seguridad es esencial. Como mínimo, el equipo de seguridad debe consistir en un miembro de IT, un ingeniero de control, un operador del sistema, un experto en temas de seguridad y un miembro de manejo de riesgos de la compañía. El conocimiento de la seguridad y las experiencias deben ser incluidos en la arquitectura de la red o diseño, procesos de seguridad y sus prácticas, operación de diseño e infraestructura segura. Para completar al equipo debe incluirse a los proveedores del sistema de control y/o los integradores de sistemas.

El equipo de seguridad de la información debe reportar directamente al administrador de seguridad de la información, al proceso de misión de negocio o al nivel organizacional; este, a su vez, reporta al CIO o CISO, respectivamente. Este último tiene la responsabilidad y autoridad en primer nivel de proveer la información necesaria para comprender el riesgo en su organización. La función de manejo del riesgo por parte del ejecutivo trabaja con el nivel más alto gerencial para aceptar un nivel de riesgo residual y contabilizar la información de seguridad en el ICS.

Los ingenieros de control juegan un papel importante en la seguridad del ICS, pero no podrán hacer nada sin la colaboración y soporte de los departamentos de IT y administración.

IT a menudo tiene años de experiencia en seguridad, muchos de los cuales son aplicables a los ICS, pero no deben olvidar que las culturas de ingeniería de control e IT son diferentes; por ello, su integración es esencial para un desarrollo colaborativo para el diseño y operación del sistema de seguridad en el ICS.

4.5. Definiendo políticas y procedimientos

Las políticas de ciberseguridad se basan en los siguientes principios básicos:

- Garantizar que los sistemas IT y OT de un sistema ICS, implementen un grado seguridad y resiliencia adecuados y utilicen todos los aspectos tecnológicos necesarios para que la operación de las infraestructuras críticas sea respaldada.

- Utilizar las medidas de seguridad que se necesiten y que protejan la confidencialidad, integridad de la información y de los sistemas operacionales tomando en cuenta el grado de criticidad y riesgos latentes, según el punto de vista del riesgo.

- Estimular que se apliquen aspectos de seguridad y resiliencia para los sistemas y operaciones que realizan terceros prestando diferentes servicios a la empresa.

- Capacitar de forma tecnológica, con conocimientos, habilidades y experiencia a los colaboradores, empleados y contratistas para que puedan detectar los riesgos de la ciberseguridad y puedan respaldar los objetivos de la empresa.

- Realizar acciones para prevenir, detectar reaccionar, analizar, responder, investigar y coordinar incidentes de ciberataques.

Dentro de los procedimientos que se deben considerar para mantener una política de seguridad adecuada tenemos los siguientes:

- Prevención: para un buen control de seguridad, algunas medidas son:

    - Control de acceso al sistema
    - Identificación y autentificación
    - Seguridad en las comunicaciones

- Detección: detectar señales en caso de ocurrir intentos de violación o violación a los sistemas de seguridad.

- Recuperación: acción que se da cuando ha ocurrido una violación al sistema de seguridad con el objetivo de recuperar el funcionamiento normal del sistema.

Se debe diseñar normas y procedimientos internos como:

- Normativa de uso de dispositivos BYOD, e-mail corporativo, etc.
- Medidas de carácter técnico como políticas de contraseñas.
- Prohibición de publicar o compartir contraseñas.

- Obligaciones de bloquear la sesión al ausentarse del puesto.
- Usar adecuadamente medios de almacenamiento extraíbles.
- Obligación de notificar cualquier incidente.

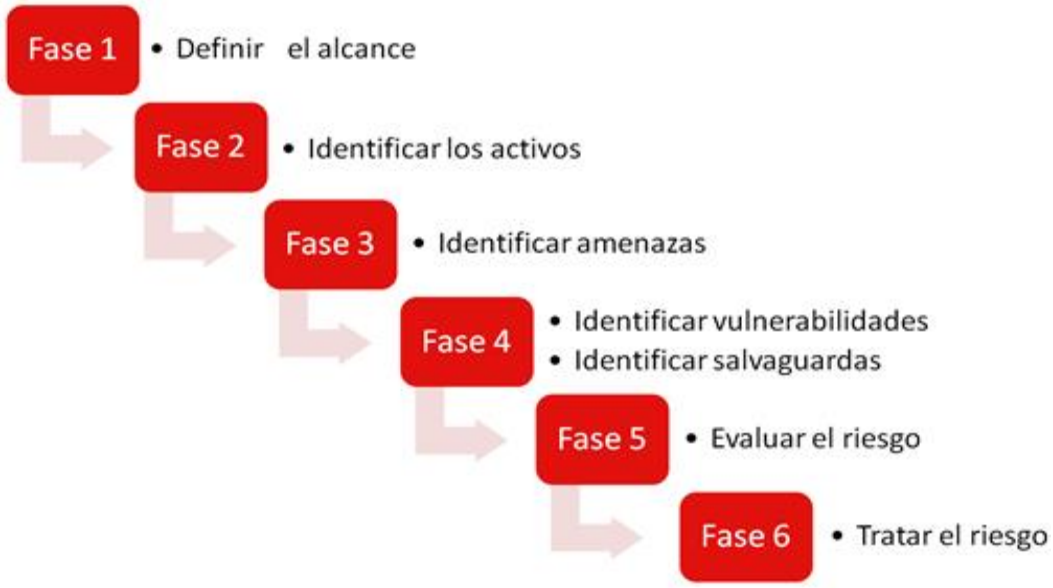
4.6. Implementando la estructura de análisis de riesgo

Con el objetivo de crear proyectos e iniciativas para mejorar la protección de la información de un sistema, una de las acciones más importantes es el análisis de riesgos. Tomando en cuenta los activos e información que están en riesgo debemos de tomar en serio un plan director de seguridad (PDS).

El PDS se puede definir como un conjunto de proyectos en materia de seguridad de la información y activos. Está orientado a reducir los riesgos presentes en todo sistema ICS en niveles aceptables, a partir del análisis de la situación inicial. Hacer un análisis exhaustivo permite que se enfoque en los riesgos que presentan los sistemas, procesos y elementos en el PDS, y poder evitar que ocurra un incidente de ciberseguridad.

A continuación, se enumeran las fases del análisis de riesgos, donde podemos analizar cómo podría llevarse a cabo, tomando en cuenta las diferentes particularidades de este.

Figura 19. **Fases del análisis de riesgo**



Fuente: Incibe. *Análisis de riesgos en 6 pasos*. https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos- sencillo. Consulta 25 de abril de 2020.

- Fase 1: definir alcance**:** es el primer paso que se realiza en el análisis de riesgos. Consideremos que este análisis de riesgos forma parte del PDS. Entonces, se recomienda que se abarque la totalidad del alcance del PDS donde se han seleccionado las áreas estratégicas sobre las que se debe mejorar la seguridad.

- Fase 2: Identificar los activos**:** una vez se ha establecido cuál es el alcance, se deben tomar en cuenta los activos importantes que están relacionados con el sistema, departamento o proceso en estudio. Se puede realizar una tabla como la siguiente, con la finalidad de mantener un inventario de activos.

Tabla IV**.** **Hardware computacional**

Id	nombre	descripción	responsable	tipo	ubicación	critico
Id_01	Servidor 01	Servidor de contabilidad	Director financiero	Servidor (físico)	Sala de PD1	Si
Id_02	Router Wifi	Router para la red WIFI de clientes	Departamento informático	Router (físico)	Sala CPD1	No
Id_03	Servidor 02	Servidor para la página web corporativa	Departamento Informático	Servidor (físico)	CPD externo	Si

Fuente: elaboración propia, empleando www.incibe.es.

La tabla anterior es un ejemplo de categorización de hardware computacional que interactúa entre el ICS y las redes de software. El enfoque debe estar en estos dispositivos, pero no deben olvidarse los PLC, DCS, SCADA e instrumentos basados en el uso de monitoreo como los HMI. Los activos que utilicen protocolos enrutables o accesos por medios de acceso telefónico a internet deben ser documentados. El equipo debe revisar y actualizar los activos completos del ICS para definir su continuidad o eliminación por ser un riesgo potencial.

La importancia de llevar este control es que se obtendrán herramientas de evolución que pueden localizar impactos adversos en los sistemas de producción, lo cual depende de la naturaleza de la información o el volumen de tráfico en la red. Mientras que el impacto puede ser aceptable en los sistemas de IT, este no podría ser aceptable en los ICS.

Un sistema de inventarios automatizado como CMMS *(computer maintenance management system*), CAFM (*computer aided facility management system*), BIM (*building information model*), GIS (*geospatial information system*), SMS (*safety management system*), permiten a la

organización ser precisos en el conteo que está en el sistema por razones de seguridad y que está por razones presupuestarias.

- Fase 3: Identificar amenazas: se debe identificar las amenazas que se pueden dar, una vez que se identifiquen los principales activos. Existen infinidades de amenazas, por lo que se debe mantener un enfoque práctico y aplicado.

- Fase 4: Identificar vulnerabilidades y salvaguardarlas: se estudian las características de los activos con el objetivo de encontrar los puntos que pueden ser débiles o vulnerabilidades. Por ejemplo, una serie de activos para los que no existen soporte ni mantenimiento.

- Fase 5: Evaluar el riesgo: en esta fase, se consideran los siguientes aspectos.

    - Inventario de activos
    - Grupo de amenazas a las que cada activo está expuesto
    - Vulnerabilidades asociadas a cada activo
    - Medidas de seguridad establecidas

Con estos aspectos por considerar, ya se puede calcular el riesgo presente en cada par activo y amenaza. Se calcula cuál es la probabilidad de que se lleve a cabo la amenaza y su impacto. En el cálculo de riesgo se utilizan criterios cuantitativos y cualitativos, como en la siguiente tabla:

Tabla V. Factores de probabilidad

Cualitativo	Cuantitativo	Descripción
Baja	1	La amenaza se lleva a cabo como máximo, una vez al año
Media	2	La amenaza se lleva a cabo como máximo, una vez al mes
Alta	3	La amenaza se lleva a cabo una vez a la semana

Fuente: elaboración propia, empleando www.incibe.es.

Cuando calculemos el riesgo si se desea hacer el análisis cuantitativo, se debe calcular multiplicando la probabilidad e impacto.

Riesgo=PROBABILIDAD X IMPACTO

- Fase 6. Tratar el riesgo: si ya se ha calculado el riesgo, se debe tomar en cuenta los riesgos que superan el límite que hemos establecido. Hay 4 estrategias principales:

  - Transferir el riesgo a un tercero.
  - Eliminar el riesgo.
  - Asumir el riesgo siempre que se justifique.
  - Implantar medidas para mitigarlo.

Al realizar el análisis de riesgos a un PDS, toda acción que se realice será parte del mismo. Por esto, debemos clasificar y definir prioridades considerando el resto de los proyectos que conforman el PDS. Al realizar el análisis de

riesgos nos proporcionará información importante que ayudará a mejorar la seguridad de la organización.

5. ARQUITECTURA DE LA SEGURIDAD DE UN ICS

La arquitectura de una red de un ICS es muy diferente de las redes corporativas. El acceso al tráfico es muy diferente en FTP, email, y accesos remotos; pueden ser válidos para los sistemas IT mientras que podrían no ser accesibles para las redes ICS.

Es probable que en las redes IT no se den procedimientos de control rigurosos, si el tráfico de la red ICS se transporta en la red corporativa podría ser interceptado o estar sujeto a ataques en DoS o m*ain in the middle*.

Al configurar redes separadas, no deberían de afectar las redes de ICS los problemas de seguridad y rendimiento en la red corporativa.

5.1. Segregación y segmentación de red

Básicamente, segmentar una red, significa dividir la red en subredes, por lo que cada división representa un segmento.

En las redes OT de los sistemas ICS y los sistemas SCADA es necesario segmentarlos, lo que mejorará la protección de la infraestructura crítica. Estas soluciones, además de operar en ambientes hostiles, deben manejar los protocolos específicos de SCADA, tales como BACnet, DNP3, IEC 60 870-6 y otros.

La segmentación y segregación es uno de los conceptos arquitectónicos más efectivos que una organización puede implementar para proteger su ICS.

El análisis de riesgos operacionales debería realizarse para determinar partes críticas de cada red y operación de ICS y ayudar a definir qué partes del sistema ICS necesitan ser segmentados. Por ejemplo, una red grande de ICS está dividida en múltiples redes ICS donde la división está basada en factores como manejo de autoridad, la política uniforme y nivel de confianza, criticidad funcional y cantidad de tráfico de comunicaciones que cruza el límite del dominio. La segmentación establece dominios de seguridad o enclaves que están típicamente definidos como administradores por la misma autoridad, haciendo cumplir la misma política y tener el nivel uniforme de confianza. La segmentación puede minimizar el método y nivel de acceso a la información confidencial, la comunicación del ICS y configuración del equipo, y puede hacerlo significativamente más difícil para los adversarios cibernéticos maliciosos y puede contener los efectos de errores no maliciosos y accidentes.

Una consideración práctica al definir el dominio de seguridad es la cantidad de tráfico en la comunicación que cruza el límite del dominio, porque la protección de dominio típicamente implica examinar el límite del tráfico y determina si está o no permitido. El objetivo de la segmentación y la segregación de la red es minimizar el acceso a la información confidencial para aquellos sistemas y personas que no lo necesitan, mientras se aseguran de que la organización puede continuar operando efectivamente. Esto se puede realizar utilizando técnicas y tecnologías dependiendo de la arquitectura de la red y la configuración.

Tradicionalmente, la segmentación y segregación de red se implementan en la puerta de enlace entre dominios. Los entornos de los ICS a menudo tienen múltiples dominios bien definidos, tales como LAN operativas, LAN de control y DMZ operativas, así como puertas de enlace a dominios que no son de un ICS, y dominios menos confiables como internet y LAN corporativas.

Cuando hay atacantes internos, la ingeniería social, dispositivos móviles y otras vulnerabilidades y condiciones predispuestas son consideradas, es apropiado proteger las puertas del enlace de dominio y vale la pena considerarlo.

La segregación de red comprende el desarrollo y la aplicación de un conjunto de reglas que controlan qué comunicaciones están permitidas a través del límite. Las reglas típicamente se basan en la identidad del origen y destino y el tipo o contenido de los datos que serán transferidos.

Cuando se implementa la segmentación y segregación de la red correctamente, se minimiza el método y nivel de acceso a la información confidencial. Esto se logra utilizando una variedad de tecnologías y métodos. Dependiendo de la arquitectura y configuración de la red, algunas tecnologías y métodos comunes utilizados incluyen:

- Separación de red lógica impuesta por encriptación o partición impuesta por dispositivo de la red.

- VLAN.

- VPN que usan mecanismos criptológicos para separar el tráfico combinado en una red.

- Puertas de enlace unidireccionales que restringen la comunicación entre conexiones en una sola dirección, es decir la segmentación.

- Separación física de la red para prevenir alguna interconectividad del tráfico entre dominios por completo.

- Filtrado de tráfico de la red, el cual puede utilizar una variedad de tecnologías en varias capas de la red para hacer cumplir los requerimientos y dominios de seguridad.

- Filtrado de capa de red, que restringe qué sistemas pueden comunicarse con otros en la red en función de la información de IP y del enrutador.

- Filtrado basado en el estado que restringe qué sistemas se pueden comunicar con otros en la red, basado en sus funciones o estado actual de operación.

- Filtrado a nivel de puerto y/o protocolo que restringe el número y tipo de servicios que cada sistema puede usar para comunicarse con otros en la red.

- Filtrado de aplicaciones que comúnmente filtran el contenido de comunicación entre sistemas en la capa de aplicación. Esto incluye *firewalls* de nivel de aplicación*, proxys* y filtros basados en contenido.

Algunos proveedores están haciendo productos para filtrar protocolos de ICS, a nivel de aplicación, el cual comercializan como *firewalls* para ICS. Independiente de la elección de tecnología para implementar la segmentación y segregación, hay cuatro temas comunes que implementan el concepto de defensa en profundidad al proporcionar una buena segmentación y segregación de red:

- Aplicar tecnologías no solo en la capa de red. Cada sistema y red debería ser segmentada y segregada cuanto sea posible, desde la capa de enlace de datos hasta la capa de aplicación incluida.

- Uso de principios de menor privilegio y que deben conocerse. Si un sistema necesita comunicarse con otro sistema, no debe permitírselo. Si un sistema necesita hablar solo con otro sistema en un puerto específico o protocolo y nada más o si este necesita transferir un conjunto limitado de datos etiquetados o de formato fijo, debe restringirse como tal.

- Información e infraestructura separada basada en requisitos de seguridad. Esto se puede incluir usando diferentes hardware o plataformas basadas en diferentes entornos de amenazas y riesgos en los cuales cada sistema o red segmentada, opera. Los componentes más críticos requieren aislamiento más estricto de otros componentes. Adicional a la separación de red, el uso de la virtualización podría ser empleado para acompañar el aislamiento requerido.

- Implementar la lista blanca en lugar de lista negra, esto es, acceso al bien conocido en lugar de negar accesos al mal conocido. El conjunto de aplicaciones que se ejecutan en un ICS es esencialmente estático, haciendo que la lista blanca sea más práctica. Esto mejorará la capacidad de una organización para analizar los archivos de registro.

5.2. Protección de limites

Los dispositivos de protección de límites controlan el flujo de información entre dominios de seguridad interconectados para proteger el ICS contra ciberadversarios maliciosos, errores y accidentes no maliciosos. La transferencia de información entre sistemas que representan diferentes dominios de seguridad, con diferentes políticas de seguridad; introducen un riesgo que dicha transferencia viola a uno o más políticas de seguridad. Los dispositivos de protección de límites son componentes clave de soluciones

arquitectónicas específicas, que aplican políticas de seguridad específicas. Las organizaciones pueden aislar los ICS de los componentes del sistema empresarial que realizan diferentes misiones y/o funciones comerciales. Dicho aislamiento limita los flujos de información no autorizados entre los componentes del sistema y también brinda la oportunidad de implementar mayores niveles de protección para los componentes seleccionados.

La separación de los componentes del sistema con mecanismos de protección de límites proporciona la capacidad para una mayor protección de los componentes individuales y un control más efectivo de los flujos de información entre esos componentes.

Los controles de protección de límites incluyen compuertas de enlace, enrutadores, *firewalls*, protectores, análisis de código malicioso basado en red y sistemas de virtualización, sistemas de detección de intrusos (en red y basados en *host)* túneles cifrados, interfaces administrativas, puertas de enlace de correo y puertas de enlace unidireccionales. Los dispositivos de protección de límites determinan si se permite la transferencia de datos, a menudo examinando los datos y metadatos asociados.

Los arquitectos de seguridad de redes y de ICS deben decidir qué dominios permitirán comunicación directa, las políticas que rigen la comunicación permitida, los dispositivos a ser utilizados para cumplirlas y la topología para implementar y validar estas decisiones, las cuales están normalmente basadas en relación de confianza entre dominios. La confianza implica el grado de control que la organización tiene sobre el dominio externo.

Los dispositivos de protección de límites están diseñados dependiendo de la arquitectura de seguridad organizacional. Una construcción arquitectónica común es las zonas desmilitarizadas (DMZ) un *host* o segmento de red insertado como “zona neutral” entre dominios de seguridad. El objetivo es hacer cumplir las políticas de seguridad de información del dominio ICS para el intercambio de información externa y para proporcionar dominios externos con acceso restringido al tiempo que protege el dominio ICS de amenazas externas.

Consideraciones adicionales de la arquitectura y funciones adicionales pueden ser ejecutadas por los dispositivos de protección de límites para la comunicación entre dominios. Estas incluyen:

- Denegar el tráfico de comunicaciones por falla, permitiendo el tráfico de comunicaciones por excepción (quiere decir, denegar todo y permitir por excepción). Una política de tráfico de comunicaciones de negación de todo y permitiendo por excepción, asegurar que solo se permitan conexiones que están aprobadas. Esto se conoce como política de listado blanco.

- Implementar servidores *proxy* que actúan como intermediario para dominios externos que solicitan recursos del sistema de información del dominio de ICS. Solicitudes externas establecidas a través de una conexión inicial al servidor *proxy* son evaluadas para manejar la complejidad y proporcionar protección adicional por medio de limitar la conectividad directa.

- Prevenir la infiltración no autorizada de información. Las técnicas incluyen, por ejemplo, *firewalls* de inspección profunda de paquetes y puertas de enlace XML. Estos dispositivos verifican el cumplimiento de

los formatos de protocolo y la especificación en la capa de aplicación y sirven para identificar vulnerabilidades que los dispositivos que operan en la red o capas de transporte no pueden detectar. El número limitado de formatos, especialmente la prohibición de texto en forma libre en el correo electrónico facilita el uso de esas técnicas en los límites de un sistema ICS.

- Solo permite comunicación entre pares de direcciones de origen y destino autorizadas y autenticadas por uno o más de la organización, sistema, aplicación e individuo.

- Extendiendo el concepto de DMZ a otras subredes separadas es muy útil, por ejemplo, aislando un ICS para prevenir adversarios y descubriendo el análisis y técnicas forenses de las organizaciones.

- Imponer el control de acceso físico para limitar el acceso autorizado a los componentes del ICS.

- Ocultar direcciones para descubrir la red de los componentes del ICS (por ejemplo, direcciones de la red no públicas o ingresadas en los sistemas de nombres de dominio) que requieren conocimiento a priori para el acceso.

- Deshabilitar los servicios y protocolos de control y solución de problemas, especialmente aquellos que emplean mensajes de difusión que pueden facilitar la exploración de la red.

- Configurar los dispositivos de protección de límites por fallar en un estado predeterminado. Los estados de falla preferidos para los ICS

envuelven múltiples factores que se deben balancear incluyendo seguridad y protección.

- Configurar dominios de seguridad con direcciones de red separadas (es decir, subredes disjuntas).

- Deshabilitar la retroalimentación a los remitentes cuando exista una falla en el formato de validación de protocolo para evitar que adversarios estén obteniendo información.

- Implementación de flujo de datos unidireccionales, especialmente entre diferentes dominios de seguridad.

- Establecer monitoreo pasivo de redes ICS para detectar activamente anomalías en la comunicación y proporcionar alertas.

5.3. Los firewalls

Se denomina *firewall* a un software o hardware que evita que atacantes como *hackers* o algún tipo de malware llegue a su equipo a través de una red o internet. No es lo mismo que una aplicación antivirus o antimalware. Los f*irewalls* ayudan a proteger la red contra gusanos.

Los *firewalls* son muy importantes pues bloquean amenazas de incidentes cibernéticos internos que podrían alterar la seguridad confiabilidad y productividad de un ICS. Estos pueden controlar el flujo de comunicación y son capaces de filtrar paquetes, bloquear o contener tráfico dañino presente en la red.

Los *firewalls* de red son dispositivos o sistemas que controlan el flujo del tráfico entre redes que emplean diferentes posturas de seguridad. En la mayoría de las aplicaciones, los *firewalls* y ambientes de *firewalls* son discutidos en el contexto de la conectividad a internet y el conjunto de protocolos UDP/IP. Sin embargo, los *firewalls* se aplican en ambientes de redes que no requieren estar conectados a internet. Por ejemplo, muchas redes corporativas emplean *firewalls* para restringir la conectividad hacia y de redes internas que prestan servicios a funciones más sensibles como los departamentos de contabilidad o de recursos humanos. Los *firewalls* pueden además restringir las comunicaciones entre subredes ICS y dispositivos de seguridad funcionales. Empleando *firewalls* al control de conectividad en estas áreas, una organización puede prevenir accesos no autorizados a los respectivos sistemas y recursos dentro de las áreas más sensibles. Hay 3 clases generales de *firewalls:*

5.3.1. Firewalls de filtrado de paquetes

El tipo más básico de *firewall* es llamado filtro de paquetes. Estos son esencialmente dispositivos de enrutamiento que incluyen funcionalidad de control de acceso para las direcciones de los sistemas y las sesiones de comunicación. El control de acceso es gobernado por un grupo de directivas denominadas como conjunto de reglas. En su forma más básica los filtros de paquetes operan en la capa 3 (de red) de la interconexión de sistemas abiertos (ISO) modelo ISO/ IEC 7498. Este tipo de *firewall* verifica la información básica de cada paquete como las direcciones IP, con un conjunto de criterios antes de reenviar el paquete. Dependiendo del paquete y los criterios, el *firewall* puede descartar el paquete, reenviarlo o enviar un mensaje al originador. Este tipo de *firewall* puede ofrecer un alto nivel de seguridad, pero podría generar una sobrecarga y retrasar el rendimiento de la red.

5.3.2. Firewalls de inspección con estado

Son filtros de paquetes que incorporan un conocimiento adicional de los datos del modelo OSI en la capa 4 (transporte). Los *firewalls* de inspección con estado filtran los paquetes en la capa de red, determinan si los paquetes de sesión son legítimos y evalúan el contenido de los paquetes en la capa de transporte (por ejemplo, TCP, UDP). También la inspección con estado realiza un seguimiento de las sesiones activas y utiliza esa información para determinar si los paquetes deben enviarse o bloquearse. Ofrece un alto nivel de seguridad y un buen rendimiento, pero puede ser más costoso y complejo de administrar. Se pueden requerir conjuntos de reglas adicionales para aplicarse en ICS.

5.3.3. Los firewalls de puerta de enlace proxy de la capa de aplicación

Esta clase de *firewalls* examina los paquetes en la capa de aplicación y filtra el tráfico en función de reglas de aplicación específicas, (por ejemplo, navegadores) o protocolos (por ejemplo, FTP). Los *firewalls* de este tipo pueden ser muy efectivos para prevenir ataques al acceso remoto y a los servicios de configuración proporcionados por los componentes de ICS. Ofrecen un alto nivel de seguridad, pero podrían tener una sobrecarga y retrasar los impactos en el rendimiento de la red, lo que puede ser inaceptable en un entorno ICS.

En un entorno ICS, los *firewalls* se implementan con mayor frecuencia entre la red ICS y la red corporativa. Configurados correctamente, pueden restringir en gran medida el acceso no deseado hacia y desde las computadoras y controladores host del sistema de control, mejorando así la seguridad. También pueden mejorar la capacidad de respuesta de una red de control al eliminar el tráfico no esencial de la red. Cuando se diseñan,

configuran y mantienen adecuadamente, los *firewalls* de hardware dedicados pueden contribuir significativamente a aumentar la seguridad de los entornos ICS actuales.

Los *firewalls* proporcionan varias herramientas para hacer cumplir una política de seguridad que no se puede lograr localmente en el conjunto actual de dispositivos de control de procesos disponibles en el mercado, incluida la capacidad de:

- Bloquear todas las comunicaciones con excepción de las comunicaciones específicamente habilitadas entre dispositivos en la LAN desprotegida y las redes ICS protegidas. EL bloqueo se puede basar, por ejemplo, en pares de direcciones IP de origen o destino, servicios, puertos, estado de la conexión y aplicaciones o protocolos específicos admitidos por el *firewall.* El bloqueo puede ocurrir en los paquetes entrantes y salientes, lo cual es útil para limitar las comunicaciones de alto riesgo, como el correo electrónico.

- Hacer cumplir la autenticación de todos los usuarios que buscan obtener acceso a la red ICS. Hay flexibilidad para emplear diferentes niveles de protección de los métodos de autenticación que incluyen contraseñas simples, complejas, biometría, tarjetas inteligentes.

- Hacer cumplir la autorización del destino. Se puede restringir a los usuarios y permitirles llegar solo a los nodos en la red de control necesarios para su función de trabajo. Esto reduce el potencial de que los usuarios controlen o tengan acceso a los dispositivos que no tienen autorización, pero aumenta la complejidad para los empleados en capacitación laboral o cruzada.

- Registro del flujo de información para el monitoreo de tráfico, el análisis y la detección de intrusos.

- Permitir que el ICS implemente políticas operativas apropiadas para el ICS pero que podrían no ser apropiadas para una red IT como la prohibición de comunicaciones menos seguras (correo electrónico, uso de nombres de usuarios y contraseñas grupales).

- Estar diseñado con conexiones documentadas y mínimas que permitan que la red ICS se separe de la red corporativa en caso de que se tome esa decisión en momentos de incidentes cibernéticos graves.

Otras posibles implementaciones incluyen el uso de *firewalls* basados en *host* o pequeños *firewalls* de hardware independientes frente a dispositivos de control individuales o que se ejecutan en ellos.

El uso de *firewalls* en un dispositivo individual puede generar una sobrecarga de administración significativa, especialmente en la administración de cambios de las configuraciones de *firewalls;* sin embargo, esta práctica también simplificará los conjuntos de reglas de configuraciones individuales. Hay varios problemas que deben tomarse en cuenta al implementar *firewalls* en entornos ICS, en particular los siguientes:

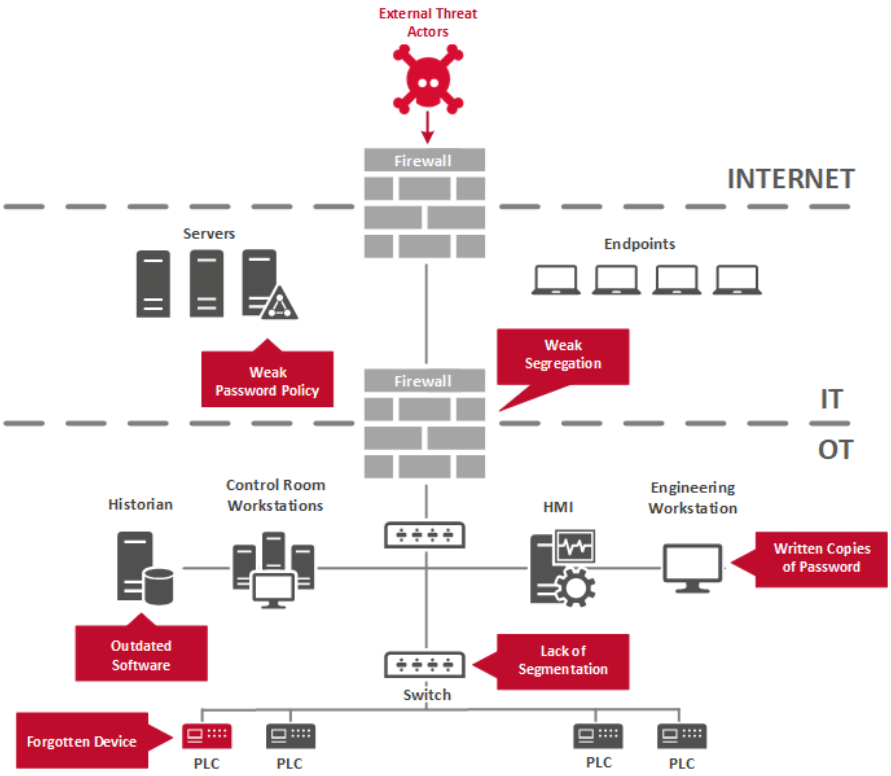
- Implementan un retraso para controlar las comunicaciones del sistema.

- Falta de experiencia en el diseño de conjuntos de reglas adecuadas para aplicaciones industriales.

- Los *firewalls* usados para proteger los sistemas de control deben configurarse de manera que no permitan el tráfico entrante o saliente de forma predeterminada. La configuración predeterminada debe modificarse sólo cuando sea necesario permitir conexiones hacia o desde sistemas confiables para realizar funciones autorizadas de ICS.

Los *firewalls* requieren soporte continuo, mantenimiento y respaldo. Los conjuntos de reglas deben revisarse para asegurarse de que brinden protección adecuada a la luz de las amenazas de seguridad en constante cambio. Las capacidades del sistema deben monitorearse para asegurarse de que el *firewall* este realizando sus tareas de recopilación de datos y que se pueda confiar en caso de una violación a la seguridad. Se requiere monitoreo en tiempo real de los *firewalls* y otros sensores de seguridad para detectar e iniciar rápidamente la respuesta a incidentes cibernéticos.

Figura 20. **Ejemplo de uso de *firewalls***



Fuente: Wizlyngroup. *Servicios de evaluación de la seguridad de ICS*. https://www.wizlynxgroup.com/mx/ciberseguridad-mexico/evaluacion-de-la-seguridad-de-los-sistemas-de-control-industrial. Consulta:28 de abril de 2020.

5.4. Control de red con lógica separada

La red ICS debería tener como mínimo una lógica separada de las redes corporativas en los dispositivos de red físicamente separados. Basados en la configuración de la red ICS, se necesita considerar separaciones adicionales para los sistemas instrumentados de seguridad y los sistemas de seguridad, (por ejemplo, monitoreo físico y control de acceso, puertas, portones, cámaras VoIP, lectores de tarjeta de acceso) que a menudo son parte de la red ICS o

utilizan la misma infraestructura de comunicación para sitios remotos. Cuando se requiere que exista conectividad empresarial:

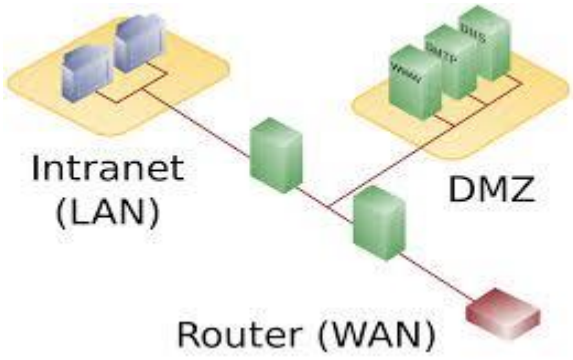
- Debe haber puntos de acceso documentados y mínimos entre la red ICS y la red corporativa. Puntos de acceso redundantes y, si están presentes, deben documentarse.

- Se debe configurar un *firewall* con estado entre red ICS y red corporativa para denegar todo el tráfico, excepto el que es explícitamente autorizado.

- Las reglas de *firewall* deben, como mínimo, proveer filtrado de la fuente y destino (es decir, filtro en la dirección de control de acceso a medios); además, filtrado de puertos TCP y el protocolo de datagramas del usuario UDP y el tipo de protocolo de mensajes de control de internet ICMP y filtrado de códigos.

Un enfoque aceptable para habilitar la comunicación entre la red ICS y la red corporativa es implementar una red DMZ intermedia. La DMZ debe estar conectada a los *firewalls* de manera tal, que pueda producirse una comunicación específica (restringida) solo entre la red corporativa y la DMZ, y la red ICS y la DMZ. La red corporativa y la red ICS, no deben comunicarse directamente entre sí.

Figura 21. **Red DMZ**



Fuente: Security insider: *Zona desmilitarizada (informática).* https://es.wikipedia.org/wiki/Zona _desmilitarizada_ inform%C3%A1tica). Consulta: 30 de abril de 2020.

5.5. Arquitectura recomendada en defensa en profundidad

El concepto de defensa en profundidad no es un concepto nuevo, se refiere a una estrategia militar que tiene por objeto hacer que el atacante pierda el empuje inicial y se vea detenido en sus intentos de ingresar a un sistema y debe superar varias barreras (capas) en lugar de una.

Un producto simple, tecnología o solución de seguridad, no puede proteger adecuadamente un ICS por sí mismo. Es necesario una estrategia de múltiples capas que involucre dos o más mecanismos diferentes de seguridad superpuestos, una técnica también conocida como defensa en profundidad para minimizar el impacto de una falla en cualquier mecanismo.

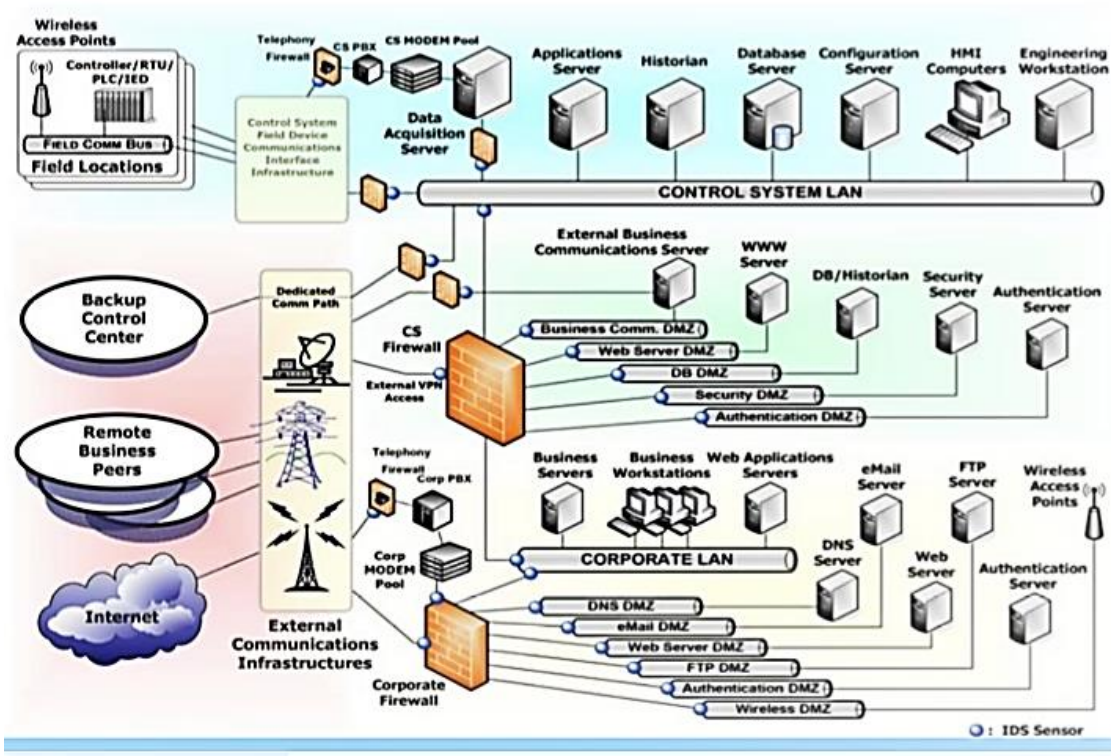
Una estrategia de la arquitectura de defensa en profundidad incluye el uso de *firewalls*, la creación de DMZ, capacidad de detección de intrusos junto con políticas de seguridad efectivas, programas de capacitación, mecanismos de

respuesta a incidentes y seguridad física. Además, una estrategia efectiva de defensa en profundidad requiere un conocimiento profundo de los posibles vectores de ataque en un ICS. Estos incluyen:

- Puertas traseras y agujeros en el perímetro de la red
- Ataques en dispositivos de campo
- Ataques a la base de datos
- Ataques de suplantación de identidad
- Ataques a cuentas privilegiadas o compartidas

La figura 22 muestra una estrategia de una arquitectura de defensa en profundidad de un ICS que ha sido desarrollada por el comité de prácticas recomendadas del programa de seguridad de sistemas de control de DHS (CSSP) NCCIC/ICS CERT, como describe las estrategias en el documento “Los sistemas de control de Seguridad Cibernética”.

Figura 22. **Red de estrategias de defensa en profundidad**



Fuente: Keith, Stoufer. *Arquitectura recomendada de defensa en profundidad.* https://nvlpubs.nist. gov/nistpubs/ SpecialPublications/NIST.SP.800-82r2.pdf. Consulta: 2 de mayo de 2020.

El documento *Estrategias de defensa en profundidad* provee una guía y dirección para el desarrollo de estrategias de arquitectura de defensa en profundidad para organizaciones que usan redes de control de sistemas, mientras mantienen una arquitectura de información de varios niveles que requiere lo siguiente:

- Mantenimiento de varios dispositivos de campo, recolección de telemetría, y/o sistemas de proceso a nivel industrial.

- Acceso a instalaciones a través de enlace de datos vía remota o módem.
- Servicios públicos para operaciones corporativas de clientes.

La estrategia incluye *firewalls,* el uso de DMZ y capacidades de detección de intrusos en toda la arquitectura ICS. El uso de muchas DMZ en la figura 22 proporciona la capacidad adicional de separar funcionalidades y privilegios de acceso y ha sido comprobado que es muy efectivo en la protección de grandes arquitecturas compuestas de redes con diferentes mandatos operativos.

La implementación de detección de intrusión aplica diferentes conjuntos y reglas y firmas únicas para cada dominio que se está monitoreando.

5.6. Reglas de firewalls recomendadas para servicios específicos

Además de reglas generales, es difícil delinear reglas de uso múltiple para protocolos específicos.

Las necesidades y prácticas recomendadas varían significativamente entre industrias para cualquier protocolo dado y deben analizarse de organización en organización. La asociación de redes abiertas de automatización Industrial (IAONA) ofrece una plantilla para llevar a cabo este análisis, evaluando cada uno de los protocolos comúnmente encontrados en entornos industriales en términos de función, riesgo de seguridad, impacto en el peor de los casos y medidas sugeridas.

Algunos de los puntos clave del documento de IAONA se resumen en esta sección:

5.6.1. Sistema de nombres de dominio (DNS)

Se usa básicamente para traducir entre nombres de dominio y direcciones IP. Por ejemplo, un DNS podría asignar un nombre de dominio como *control.com* a una dirección IP como *192.168.1.1*. La mayoría de los servicios de internet dependen en gran medida del DNS, pero su uso en la red de control es relativamente raro en ese momento.

En la mayoría de los casos hay pocas razones para permitir que las solicitudes DNS salgan de la red de control a la red corporativa y no hay ninguna razón para permitir que las solicitudes DNS ingresen a la red de control.

Las solicitudes de DNS de la red de control a DMZ deben abordarse caso por caso. Se recomienda el DNS local o el uso de archivos *host.*

5.6.2. Protocolo de transferencia de hipertexto (HTTP)

HTTP es el protocolo subyacente a los servicios de navegación web a internet. Al igual que DNS, es fundamental para la mayoría de los servicios de internet. Desafortunadamente tienen poca seguridad inherente, y muchas aplicaciones HTTP tienen vulnerabilidades que pueden ser explotadas. HTTP puede ser un mecanismo de transporte para muchos ataques realizados manualmente y gusanos automatizados.

En general, no se debe permitir que el HTTP cruce de la red pública/corporativa a la red de control. Si las tecnologías basadas en la web son absolutamente necesarias, se deben aplicar las siguientes mejores prácticas:

- Control de acceso a los servicios basados en la web en la capa física o de red usando listas blancas.

- Aplicar control de acceso a la fuente y al destino.

- Implementar autorización para acceder al servicio en la capa de aplicación (en lugar de las verificaciones físicas o de la capa de red).

- Implementar el servicio usando solo las tecnologías necesarias.

- Verificar el servicio de acuerdo con las prácticas de seguridad de aplicaciones conocidas.

- Registrar todos los intentos de uso del servicio.

- Usar HTTPS en lugar de HTTP, y solo dispositivos autorizados específicos.

5.6.3. Protocolo de transferencia de archivos trivial y FTP (TFTP)

FTP y protocolo trivial de transferencia de archivos (TFTP) se utilizan para transferir archivos entre dispositivos. Se implementan en casi todas las plataformas, incluido muchos sistemas SCADA, DCS, PLC, y RTU, porque son muy conocidas y utilizan mínima potencia en el procesamiento. Desafortunadamente, ninguno de los protocolos fue creado con la seguridad en mente; para FTP, la contraseña de inicio de sesión no está cifrada y para TFTP, no es necesario iniciar sesión en lo absoluto; además, algunas implementaciones de FTP tienen un historial de vulnerabilidad de

desbordamiento de buffer. Como resultado, todas las comunicaciones TFTP deben bloquearse, mientras que las comunicaciones FTP deben permitirse sólo para sesiones salientes o si están aseguradas con autenticación multifactorial basada en *token* adicional y un túnel encriptado. Siempre que sea posible se deben emplear protocolos más seguros, como FTP, seguro (SFTP) o copia segura (SCP).

5.6.4. TELNET

El protocolo TELNET define una sesión interactiva de comunicaciones basadas en texto entre un cliente y un *host*. Se utiliza principalmente para servicios de inicio de sesión remoto y control simple para sistemas con recursos limitados o para sistemas con necesidades de seguridad limitadas. Es un grave riesgo de seguridad porque todo el tráfico de TELNET, incluidas las contraseñas, no está encriptado y puede permitir a un individuo remoto un control considerable sobre un dispositivo. Se recomienda utilizar el protocolo *Secure shell* (SSH) para la administración remota. Se deben prohibir las sesiones entrantes de TELNET desde la red corporativa a la de control a menos que se asegure con autenticación multifactorial basada en *token* y en túnel encriptado. Las sesiones de TELNET salientes solo se deben permitir a través de túneles encriptados a dispositivos autorizados específicos.

5.6.5. Protocolo de configuración dinámica de host (DHCP)

Se utiliza en redes IP para distribuir dinámicamente los parámetros de configuración de la red, como las direcciones IP para interfaces y servicios. El DHCP base no incluye ningún mecanismo para autenticar servidores y clientes.

Los servidores DHCP no autorizados pueden proporcionar información incorrecta a los clientes. Los clientes no autorizados pueden obtener acceso al servidor y provocar el agotamiento de los recursos disponibles (por ejemplo, direcciones IP). Para evitar esto, se recomienda utilizar la configuración estática en lugar de la asignación dinámica de direcciones, que debería ser la configuración típica para dispositivos ICS. Si es necesaria una asignación dinámica, se recomienda habilitar la inspección DHCP para defenderse contra servidores DHCP no autorizados, el protocolo de resolución de direcciones (ARP) y la suplantación de IP. Los servidores DHCP deben colocarse en el mismo segmento de red que el equipo configurado, no se recomienda la retransmisión DHCP.

5.6.6. Shell seguro (SSH)

SSH permite el acceso remoto a un dispositivo. Proporciona autenticación y autorización seguras basadas en criptografía. Si se requiere acceso remoto a la red de control se recomienda SSH como alternativa a TELNET, rlogin, RSH, RCP, y otras herramientas de acceso remoto inseguras.

5.6.7. Protocolo simple de acceso a objetos (SOAP)

SOAP es una sintaxis de formato basada en XML para intercambiar mensajes. Los flujos de tráfico relacionados con los servicios basados en SOAP deben controlarse en el *firewall* entre los segmentos de red corporativos e ICS. Si estos servicios son necesarios, se deben usar *firewalls* de inspección profunda de paquetes o capa de aplicación para restringir el contenido de los mensajes.

5.6.8. Protocolo simple de transferencia de correo (SMTP)

Es el principal protocolo de transferencia de correo electrónico en internet. Los mensajes de correo electrónico a menudo contienen malware, por lo que el correo electrónico entrante no debe permitirse en ningún dispositivo de red de control. Los mensajes de correo SMTP salientes de la red de control a la red corporativa son aceptables para enviar mensajes de alerta.

5.6.9. Protocolo simple de administración de red (SNMP)

Es usado para proporcionar servicios de administración de red entre una consola de administración central y dispositivos de red como enrutadores, impresoras y PLC. Aunque SNMP es un servicio extremadamente útil para mantener una red, su seguridad es muy débil. Las versiones 1 y 2 de SNMP usan contraseñas sin cifrar para leer o configurar dispositivos (incluidos dispositivos como PLC) y en muchos casos las contraseñas son conocidas y no se pueden cambiar. La versión 3 es considerablemente más segura, pero todavía tiene un uso limitado. Se deben prohibir los comandos SNMP V1 y V2 hacia y desde la red de control a menos que se encuentren en una red de administración segura y separada, mientras que los comandos SNMP V3 pueden enviarse al ICS utilizando las características de seguridad inherentes a V3.

5.6.10. Modelo de objetos componentes distribuidos (DCOM)

DCOM es el protocolo subyacente para OLE para control de procesos (OPC). Utiliza el servicio de llamada a procedimiento remoto (RPC) de Microsoft, cuando no está parcheado, tiene muchas vulnerabilidades. Estas vulnerabilidades fueron la base de las vulnerabilidades de *Blaster worm* 14.

Además, OPC que utiliza DCOM, abre dinámicamente una amplia gama de puertos (1024 a 65535) que pueden ser extremadamente difíciles de filtrar en el *firewall.* Este protocolo solo debe permitirse entre la red de control y las redes DMZ y debe bloquearse explícitamente entre la red DMZ y la red corporativa. Además, se aconseja a los usuarios que restrinjan los rangos de puertos utilizados al realizar modificaciones de registro en los dispositivos que utilizan DCOM.

5.6.11. SCADA y protocolos industriales

SCADA y los protocolos industriales, como Modbus / TCP, ethernet/ IP, IEC 61850, ICCP y DNP 315, son críticos para las comunicaciones con la mayoría de los dispositivos de control. Desafortunadamente, muchos de estos protocolos fueron diseñados sin seguridad incorporada y generalmente no requieren ninguna autenticación para ejecutar comandos de forma remota en un dispositivo de control. Estos protocolos solo deben permitirse dentro de la red de control y no deben cruzarse a la red corporativa.

6. APLICANDO CONTROLES DE SEGURIDAD A ICS

Hemos visto en los capítulos anteriores cómo se conforma un sistema ICS, cuáles son sus vulnerabilidades, qué ataques se han dado a nivel mundial a estos sistemas y cómo utilizar estrategias para minimizar estos ataques. En este capítulo se pretende analizar qué controles están disponibles para lograr que el sistema de seguridad esté completo y evitar lo más posible un ciberataque.

Un producto de seguridad o tecnología de seguridad por sí solo no puede proteger adecuadamente un ICS. Debe ser una combinación de políticas de seguridad configuradas adecuadamente y un conjunto de controles configurados apropiadamente.

La selección e implementación de controles de seguridad aplicados a un ICS puede tener mayores implicaciones en las operaciones, por lo que es bueno considerar lo siguiente:

- Determinar qué controles de seguridad son necesarios para mitigar adecuadamente el riesgo a un nivel aceptable que respalden las misiones de la organización y las funciones comerciales.

- Implementar controles de seguridad seleccionados o crear un plan de implementación realista.

- Analizar el nivel de garantía requerido para que los controles de seguridad seleccionados se implementen correctamente y funcionen

según lo previsto y produzcan los resultados deseados. Considerando lo anterior, se logra que el proceso de gestión de riesgos sea eficaz y así crear una estrategia de seguridad cibernética que identifique, mitigue y supervise continuamente los riesgos para su ICS.

Una estrategia de ciberseguridad efectiva para un ICS debe aplicar una defensa en profundidad. El uso de dicha estrategia se explora dentro de las discusiones de control de seguridad y sus aplicaciones para ICS que siguen.

6.1. Ejecutando tareas del manejo de riesgo para ICS (RMF)

Existen muchos métodos para la evaluación de riesgos de los ICS. Las siguientes técnicas de análisis de seguridad de los ICS son más utilizadas. No representa un análisis de todos los enfoques disponibles, sino una muestra representativa de las prácticas actuales en la evaluación de riesgos de los ICS. En la mayoría de estos casos son metodologías de vulnerabilidades de los sistemas IT, que han sido modificadas y reconocidas, pero no se tiene conocimiento si lo utilizan los profesionales de ICS.

Entidades como el Departamento de Seguridad de EE. UU. (DHS) y el Instituto NIST, han desarrollado la primera generación de evaluación de riesgos de los ICS desde 2003 y 2004; en ese entonces, suponían que había un equilibrio de los requisitos de confidencialidad, integridad y disponibilidad en los sistemas IT y los ICS, pero ahora se sabe que no era una situación exacta.

6.1.1. Consejo de Fiabilidad de Electricidad de América del Norte (NERC)

La misión de NERC es mejorar la confiabilidad y seguridad de los sistemas de gran potencia en USA, Canadá y parte de México. La organización tiene como objetivo hacer cumplir no solo los estándares de confiabilidad obligatorios sino también actuando como un catalizador para un cambio positivo, mostrar las debilidades del sistema, ayudar a los participantes de la industria a operar y planificar de manera exitosa.

NERC es uno de los usuarios del ICS de más alta exigencia en América del Norte y está concentrado en lograr altos estándares en la seguridad. Representa las mejores técnicas de evaluación de seguridad de los ICS. La guía NERC para evaluar la seguridad consta de cuatro pasos:

- Identificación de los impactos de activos y pérdidas.
- Identificación y análisis de vulnerabilidades.
- Evaluación de riesgos y determinación de prioridades para la protección de activos críticos.
- Identificación de contramedidas su costo y compensación.

Sin embargo, también ha publicado sus propios estándares de protección de infraestructura crítica (CIP), conocidos como NERC-CIP. NERC-CIP es una guía relacionada a temas como:

- Reporte de sabotaje
- Identificaciones críticas de activos cibernéticos
- Controles de gestión de seguridad
- Ciberseguridad: personal y capacitación
- Ciberseguridad: perímetro de seguridad electrónica
- Seguridad física de los activos cibernéticos
- Ciberseguridad: informe de incidentes
- Ciberseguridad: planes de recuperación

Dentro del contenido de este documento, NERC proporciona orientación relacionada con la evaluación de riesgos dentro de CIP-002-3: identificación de activos críticos.

La guía en CIP-002 se concentra en solicitar que las entidades responsables “identifiquen y documenten una metodología de evaluación, basada en el riesgo” BERC-CIP y solo requiere que evalúen los sistemas críticos.

6.1.2. Proceso de aplicación del marco de gestión de riesgo a un ICS

El proceso incluye una descripción de cada actividad e identifica los documentos que sirven de apoyo al NIST. A continuación, se muestran los pasos que se pueden implementar en un orden diferente para ser coherentes con los procesos establecidos de gestión y desarrollo del sistema.

Figura 23. **Tareas de manejo de gestión de riesgo**

Fuente**:** elaboración propia.

6.1.2.1. Paso 1: categorizar el sistema de información

La primera actividad en RMF es para categorizar el sistema y la información según el impacto potencial de pérdida. Para cada tipo de información y sistema de información bajo investigación, los objetivos de seguridad definidos por FISMA (confidencialidad, integridad y disponibilidad) están asociados con uno de los tres niveles de impacto potencial en caso de incumplimiento de la seguridad. Es importante recordar que, para un ICS, la disponibilidad es normalmente lo más importante. NIST está en proceso de

actualizar NIST SP 800-60 para proporcionar orientación adicional sobre la categorización de los ICS. FIPS 199 (publicación estándar de procesamiento de información federal 199), trata de que los sistemas de información se clasifiquen como: bajo impacto, impacto moderado, o alto impacto, para los objetivos de seguridad de integridad, disponibilidad y confidencialidad.

En la tabla VI se proporcionan posibles definiciones de niveles de seguridad bajos, moderados y altos, basados en el impacto para ICS, según ISA99. Las posibles definiciones de los niveles de impacto de ICS en función del producto producido, de la industria y de las preocupaciones de seguridad, se muestran en la tabla VII:

Tabla VI. **Posibles definiciones para los niveles de impacto ICS**

Categoría	Bajo Impacto	Impacto moderado	Alto impacto
Lesión	Contusiones requieren primeros auxilios	Requiere hospitalización	Pérdida de vida o extremidades
Pérdidas financieras	$1 000	$100 000	Millones
Lanzamiento ambiental	Daño temporal	Daño duradero	Daño permanente, daño fuera de sitio
Interrupción de producción	Minutos	Días	Semanas
Imagen pública	Daño temporal	Daño duradero	Daño permanente

Fuente: elaboración propia, empleando https://nvlpubs.nist.gov.

Tabla VII. **Definiciones de los niveles de impacto ICS en función de las preocupaciones sobre la producción**

Categoría	Bajo impacto	Impacto moderado	Alto impacto
Producto producido	- Productos o materiales no peligrosos - Productos de consumo no ingeridos	- Algunos productos peligrosos o pasos durante la producción - Alta cantidad de información del propietario	- Infraestructura crítica - Materiales peligrosos - Productos ingeridos
Ejemplos de industrias	- Moldeo de inyección de plástico -Aplicaciones de almacenes	- Industrias de metal para automóviles - Papel y pulpa - Semiconductores	- Utilidades - Petroquímicas - Comidas y bebidas - Farmacéuticas
Preocupaciones de seguridad	-Protección contra leves daños -Garantizar el tiempo de actividad	- Protección contra leves daños - Garantizar el tiempo de actividad - Inversión de capital	- Protección contra daños mayores - Pérdidas de vida - Garantizar el tiempo de actividad - Inversión capital - Asegurar servicios básicos

Fuente: elaboración propia, empleando https://nvlpubs.nist.gov.

6.1.2.2. Paso 2: selección de controles de seguridad

Esta actividad incluye la selección inicial de controles mínimos de seguridad planificados o implementados para proteger el sistema de información en función de un conjunto de requisitos. FIPS 200 trata de un

conjunto de requisitos mínimos, cubriendo 18 áreas relacionadas a la seguridad con respecto a la protección de la confidencialidad, integridad y disponibilidad de los sistemas de información federales y la información procesada, almacenada y transmitida por esos sistemas.

Los controles de línea de base representan el inicio en la selección de controles de seguridad y se eligen en función de la categoría de seguridad y el nivel de impacto asociado a los sistemas de información determinados en el paso 1. Para analizar la necesidad de desarrollar conjuntos de controles de seguridad, se introduce el concepto de superposiciones. Una superposición es un conjunto de controles de seguridad completamente especificados y mejoras de control y orientación complementaria derivada de la aplicación de la "orientación de adaptación a las líneas de base de control" descritas en NIST SP 800-53.

Las superposiciones están diseñadas para reducir la necesidad de personalización apropiada de las líneas de base por parte de las organizaciones, mediante la selección de un conjunto de controles y mejoras de control que se definen según las circunstancias, situaciones o condiciones comunes. Sin embargo, el uso de superposiciones no impide que las organizaciones realicen una personalización adicional para reflejar las necesidades, o limitaciones específicas de la organización.

6.1.2.3. Paso 3: implementación de controles de seguridad

Este paso se concentra en la implementación de controles de seguridad en sistemas de información nuevos o heredados.

Para los nuevos sistemas de control en desarrollo, el proceso de selección de control de seguridad se aplica desde una perspectiva de definición de requisitos, ya que los sistemas aún no existen y las organizaciones están realizando su diseño de seguridad inicial. Los controles de seguridad incluidos en los planes de seguridad para los IT sirven como una especificación de seguridad y se espera que se incorporen a los sistemas durante las fases de desarrollo e implementación.

En los sistemas de información heredados, el proceso de selección de control de seguridad se aplica incluyendo un análisis de brechas cuando las organizaciones saben que tienen cambios significativos en los sistemas. Dado que los sistemas de información ya existen, es probable que las organizaciones hayan completado los procesos de categorización de seguridad y selección de control de seguridad.

6.1.2.4. Paso 4: evaluación de sistemas de control de seguridad

En este paso se determina hasta qué punto los controles de seguridad en el sistema de información son efectivos en su aplicación a los sistemas ICS. NIST SP 800-53A proporciona orientación para evaluar los controles de seguridad seleccionados inicialmente de NIST SP 800-53 para asegurar que están correctamente implementados, operando apropiadamente y logrando el resultado deseado con respecto al cumplimiento de los requisitos de seguridad del sistema. NIST SP 800-53A. Proporciona expectativas basadas en los requisitos de garantía definidos en NIST SP 800-53 para categorizar la expectativa de las evaluaciones de seguridad según el nivel de impacto FIPS 199.

6.1.2.5. Paso 5: autorizar el sistema de información

En este nivel se toman decisiones en la administración para autorizar la operación de un sistema de información y se acepta el riesgo para las operaciones de la agencia, los activos de la agencia o las personas en función de la implementación de un conjunto acordado de controles de seguridad.

6.1.2.6. Paso 6: supervisar los controles de seguridad

En este nivel se rastrea continuamente los cambios en el sistema de información que pueden afectar los controles de seguridad y evalúa la efectividad del control. NIST SP 800-137 proporciona orientación sobre la seguridad de la información de monitoreo continuo.

6.2. Guía de aplicación de controles de seguridad a ICS

Actualmente, los sistemas ICS son una combinación de sistemas heredados, frecuentemente con una vida útil planificada de 20 a 30 años o bien son sistemas híbridos que han crecido en software y hardware más nuevos, conectados a otros sistemas y normalmente es difícil aplicar algunos de los controles de seguridad contenidos en NIST SP 800-53. Si bien muchos controles de NIST SP 800-53 son aplicables a los ICS, varios de estos, requieren un análisis antes de poder utilizarse correctamente. Estos controles están divididos en 18 familias. Cada familia contiene controles de seguridad propios y son:

6.2.1. Controles de acceso (AC)

Es el proceso de otorgar y denegar solicitudes específicas para obtener y usar información y servicios de procesamiento de información relacionados, para el acceso a áreas dentro del entorno del sistema de información.

Los controles de seguridad que pertenecen a la familia NIST SP 800-53 de control de acceso (AC) especifican controles para administrar las cuentas del sistema de información, incluido el establecimiento, activación, modificación, revisión, desactivación y eliminación de cuentas. Los controles cubren problemas de acceso y aplicación de flujo como separación de tareas, privilegios mínimos, intento de inicio de sesión fallidos, notificación de uso del sistema, notificación de inicio de sesión anterior, control de sesión recurrente, bloqueo de sesión y finalización de sesión. También hay controles para el uso de dispositivos portátiles y remotos.

Se encuentra orientación adicional para los controles AC en los siguientes documentos:

- NIST SP 800-63 proporciona orientación sobre la autenticación electrónica remota.

- NIST SP 800-48 proporciona orientación sobre la seguridad de la red inalámbrica con especial énfasis en los estándares IEEE 802.11b estándares de bluetooth 0.

- NIST SP 800-97 provee una guía sobre la seguridad de la red inalámbrica IEEE 802.11i.

- FIPS 201 proporciona requisitos para la verificación de identidad personal de empleados y contratistas federales.

- NIST SP 800-96 proporciona orientación sobre la tarjeta PIV para interoperabilidad del lector.

- NIST SP 800-73 proporciona orientación sobre interfaces para la verificación de identidad personal.

- NIST SP 800-76 Proporciona orientación sobre biometría para la verificación de identidad personal.

- NIST SP 800-78 Proporciona orientación sobre algoritmos criptográficos y tamaños de claves para la verificación de identidad personal.

Si la nueva verificación de identidad personal PIV federal se utiliza como un *token* de identificación, el sistema de control de acceso debe cumplir con los requisitos de FIPS 201 y NIST SP 800-73 y emplear verificación criptográfica o verificación biométrica. Si emplea verificación criptográfica, el sistema de control de acceso debe cumplir con los requisitos de NIST SP 800-78. Si es verificación biométrica, el sistema de control de acceso debe cumplir con los requisitos de NIST SP 800-76.

6.2.1.1. Control de acceso basado en roles (RBAC)

Es una tecnología que tiene el potencial de reducir la complejidad y el costo de la administración de seguridad en redes con gran cantidad de dispositivos inteligentes. Al utilizar RBAC la administración de seguridad se simplifica a través del uso de roles de jerarquías y restricciones para organizar

los niveles de acceso de los usuarios. RBAC reduce el costo en una organización, porque acepta que los empleados cambien los roles y responsabilidades con más frecuencia que los deberes dentro de los roles y responsabilidades.

6.2.1.2. Servidores web

Las tecnologías web y de internet se están agregando a una gran variedad de productos ICS porque hacen que la información sea más accesible y los productos, más fáciles de usar y de configurar de forma remota. Sin embargo, también puede agregar riesgos cibernéticos y crear nuevas vulnerabilidades de seguridad que deben abordarse.

6.2.1.3. VLAN

VLAN divide las redes físicas en pequeñas redes lógicas para aumentar el rendimiento, mejorar la capacidad de administración y simplificar el diseño de la red. VLAN se logra mediante la configuración de conmutadores ethernet. Cada VLAN consta de un único dominio de difusión que aísla el tráfico de otras VLAN, reemplaza los concentradores por conmutadores y reduce las colisiones. El uso de VLAN limita el tráfico de transmisión, tanto como para permitir que subredes lógicas abarquen múltiples ubicaciones físicas. Existen dos categorías de VLAN:

- Estática: regularmente se conoce como basada en el puerto, donde los puertos del conmutador se asignan a una VLAN para que sea transparente para el usuario final.

- Dinámica: Donde un dispositivo final negocia las características de la VLAN con el conmutador o determina la VLAN en función de las direcciones IP o de hardware.

Aunque más de una subred IP puede coexistir en la misma VLAN la recomendación general es usar una relación uno a uno entre subredes y VLAN. Esta práctica requiere el uso de un enrutador o conmutador multicapa para unir varias VLAN. Las VLAN no son generalmente implementadas para abordar las vulnerabilidades del *host* o de la red en la forma que se implementan los *firewalls* o los IDS. Cuando se configuran correctamente, las VLAN permiten que los conmutadores apliquen políticas de seguridad y segreguen el tráfico en la capa de ethernet.

6.2.1.4. Módems de acceso telefónico

Los sistemas ICS tienen estrictos requisitos de confiabilidad y disponibilidad. Cuando sea necesario solucionar problemas y repararlos, es posible que los recursos técnicos no se encuentren físicamente en la sala de control o en las instalaciones. Por lo tanto, los ICS a menudo usan módems para permitir a los proveedores, sistemas integrados o Ingenieros de control, mantener el sistema y diagnosticar, reparar, configurar y ejecutar mantenimiento en la red o componente.

Si bien esto permite un fácil acceso para el personal autorizado, si los módems de acceso telefónico no están debidamente asegurados, también pueden proporcionar entradas de puerta trasera para uso no autorizado.

6.2.1.5. Wireless

El uso de tecnología inalámbrica dentro de un ICS es una decisión basada en el riesgo que debe determinar la organización. En general, las LAN inalámbricas solo deben implementarse donde las implicaciones para la salud, seguridad, el medio ambiente y las finanzas son bajas. NIST SP 800-48 y SP 800-97 proporcionan orientación sobre la seguridad de la red inalámbrica.

6.2.2. Entrenamiento y conciencia (AT)

Los controles de seguridad que pertenecen a la familia NIST SP 800-53 (AT) (*awareness and training*) brindan políticas y procedimientos para garantizar que todos los usuarios de un sistema de información reciban materiales básicos de capacitación de seguridad del sistema de información, antes de que se otorgue la autorización para acceder al sistema. La capacitación del personal debe ser monitoreada y documentada.

6.2.3. Auditoría y responsabilidad (AU)

Una auditoría es una revisión y examen independiente de registros y actividades para evaluar la idoneidad de los controles del sistema, para garantizar el cumplimiento de las políticas establecidas y los procedimientos. Los controles de seguridad que pertenecen a la familia NIST SP 800-53 de Auditoría y responsabilidad (AU) proporcionan procedimientos para generar registros de auditoría, su contenido, capacidad y requisitos de retención. Los controles también proporcionan garantías para reaccionar ante problemas tales como una falla de auditoría o la capacidad de registro de auditoría que se está alcanzando. (ver NIST SP 800-61).

6.2.4. Evaluación y autorización (CA)

Los controles de seguridad que pertenecen a la familia NIST SP 800-53 (CA) proporcionan la base para realizar evaluaciones periódicas y certificar los controles de seguridad implementados en el sistema de información, para determinar si los controles se implementan correctamente, funcionan según lo previsto y producen el resultado deseado para cumplir con los requisitos de seguridad del sistema. Un funcionario superior de la organización es responsable de aceptar el riesgo residual y autorizar la operación del sistema. Además, todos los controles de seguridad deben ser monitoreados de manera continua. Las actividades de monitoreo incluyen gestión de la configuración y el control de los componentes del sistema de información, el análisis de impacto de la seguridad de los cambios en el sistema, la evaluación continua de los controles de seguridad y los informes de estado. Ver NIST SP 800-53A, 800-37 y 800-100.

6.2.5. Planificación de contingencia (CP)

Los planes de contingencia están diseñados para mantener o restaurar las operaciones comerciales, incluidas las operaciones informáticas, posiblemente en una ubicación alternativa en caso de emergencia, fallas del sistema o desastres. Los controles de seguridad que pertenecen a la familia NIST SP 800-53 (CP) proporcionan políticas y procedimientos para implementar un plan de contingencia especificando roles y responsabilidades y, asignando personal y actividades asociadas con la restauración del IT después de una interrupción o falla.

6.2.5.1. Planificación de continuidad de negocios (BCP)

Aborda el problema general de mantener o restablecer la producción de una empresa en caso de interrupción. Estas interrupciones pueden ser: un desastre natural, (huracán tornado, inundación, terremoto) un evento no intencional o intencional provocado por el hombre o una falla del equipo y que implica que hay un tiempo de recuperación. Debido a que existe una disciplina que se ocupa de la confiabilidad y el mantenimiento eléctrico / mecánico, algunas organizaciones eligen definir la continuidad del negocio de una manera que excluya estas fuentes de falla. La continuidad del negocio es muy importante; algunas organizaciones también optan por establecer un límite mínimo de interrupción en los riesgos a considerar. Para los propósitos de ciberseguridad de los ICS, se recomienda que no se imponga ninguna de estas restricciones. Deben considerarse interrupciones a largo y corto plazo, debido a que algunas de estas interrupciones potenciales involucran eventos provocados por el hombre. Antes de crear un plan BCP, es importante especificar los objetivos de recuperación para los diversos sistemas y subsistemas involucrados en función de las necesidades comerciales típicas. Hay dos tipos de objetivos: recuperación del sistema y recuperación de datos.

Recuperar el sistema significa la recuperación de enlaces de comunicación y capacidades de procesamiento y se especifica en términos de un objetivo de tiempo de recuperación (RTO). La recuperación de datos implica la recuperación de datos que describen la producción o las condiciones del producto en el pasado, y generalmente se especifica en términos de un objetivo de punto de recuperación (RPO). Esto se define como el periodo de tiempo más largo durante el cual se puede tolerar la ausencia de datos.

6.2.5.2. Planificación de recuperación de desastre (DRP)

Un DRP es un conjunto de procedimientos que se deben cumplir para recuperar y proteger una infraestructura de IT en el momento que ocurra un desastre. Representan una serie de acciones importantes que se toman antes o bien en el momento del desastre.

6.2.6. Gestión de configuración (CM)

Representa las políticas y procedimientos para controlar las modificaciones de hardware, firmware, software y también la documentación que garantiza que el sistema de información está protegido contra modificaciones inadecuadas, antes, durante y después de la implementación del sistema.

Los controles de seguridad que pertenecen a la familia NIST SP 800-53 (CM) proporcionan políticas y procedimientos para establecer controles de línea base para los sistemas de información. Debe haber acceso restringido a los ajustes de configuración y la configuración de seguridad de los productos IT de acuerdo con los requisitos operativos de un ICS.

6.2.7. Identificación y autenticación (IA)

Es el proceso de verificar la identidad de un usuario, un proceso o dispositivo, mediante el uso de credenciales específicas, es requisito previo que va a permitir el acceso a los recursos en un sistema IT.

La autenticación describe el proceso de identificación positiva de usuarios potenciales de la red, *hosts*, aplicaciones, servicios y recursos mediante una combinación de factores de identificación o credenciales. Existen varios factores posibles para determinar la autenticidad de una persona, dispositivo o sistema. Cuantos más factores se utilicen en el proceso de identificación, más seguro será el sistema. Los controles de seguridad que pertenecen a la familia NIST SP 800-53 (IA) proporcionan políticas y orientación para la identificación y autenticación de usuarios y dispositivos dentro del IT.

6.2.7.1. Autenticación de contraseña

Las tecnologías de autenticación de contraseña están diseñadas para determinar la autenticidad y se basan en la función de una prueba de algo que el dispositivo o el humano que solicita acceso debe saber, por ejemplo, un número de pin o contraseña. Los esquemas de autenticación de contraseña se consideran las formas más simples y comunes en la seguridad. Las vulnerabilidades de las contraseñas se pueden reducir mediante el uso de un verificador de contraseñas activo, que prohíbe las contraseñas débiles de uso reciente o común.

Otra debilidad es la facilidad de espionaje de terceros. Las contraseñas escritas en un teclado se observan o graban fácilmente, especialmente en áreas donde los adversarios podrían plantar cámaras inalámbricas pequeñas o registradores de pulsaciones de teclas. La autenticación del servicio de red a menudo transmite las contraseñas como texto sin formato (sin cifrar), lo que permite que cualquier herramienta de captura de red, exponga las contraseñas.

6.2.7.2. Autenticación de desafío / respuesta

La autenticación de desafío y respuesta requiere que tanto el solicitante del servicio como el proveedor, conozcan de antemano un código secreto.

Cuando se solicita el servicio, el proveedor del servicio envía un número aleatorio como desafío al solicitante del servicio. El solicitante genera una respuesta única para el proveedor del servicio. Si es correcta, demuestra que tiene acceso al “secreto” sin exponer el secreto en la red.

La autenticación de desafío y respuesta aborda las vulnerabilidades de seguridad de la autenticación de contraseña tradicional. Cuando se envían contraseñas (*hashed* o sin formato) a través de una red, se envía una parte del secreto real en sí, y el secreto del dispositivo remoto, realiza la autenticación.

6.2.7.3. Autenticación de *token* físico

Es similar a la autenticación de contraseña, pero esta tecnología determina la autenticidad al probar el código secreto o clave producida por un dispositivo o *token* que la persona solicitante del acceso tiene en su poder como *tokens* de seguridad o tarjetas inteligentes. Cada vez más las claves privadas se están integrando a dispositivos físicos como *dongles* USB. Algunos *tokens* sólo admiten la autenticación de factor único, de modo que simplemente poseer el *token* es suficiente para autenticarse. Otros admiten la autenticación multifactorial que requiere el conocimiento de un pin o contraseña además de poseer el *token*.

La principal vulnerabilidad de las direcciones de autenticación de *tokens* es duplicar fácilmente un código secreto o compartirlo con otros. Un segundo

beneficio es que la información secreta dentro de un *token* físico puede ser muy grande, físicamente seguro y generado aleatoriamente. Debido a que está incrustado en metal o silicio, no tiene los mismos riesgos que las contraseñas ingresadas manualmente. Las formas comunes de autenticación física o *token* incluyen:

- Cerraduras físicas tradicionales y llaves.
- Tarjetas de seguridad (magnética, chip inteligente, codificación óptica).
- Dispositivos de radiofrecuencia en forma de tarjetas, llaveros o etiquetas montadas.
- *Dongles* con claves de cifrado seguras, que se conectan a los puertos USB serie o paralelo de las computadoras.
- Generadores de códigos de autenticación únicos.

La autenticación física/*token* es más segura cuando se combina con una segunda forma de autenticación, como PIN memorizado.

6.2.7.4. Autenticación de tarjeta inteligente

Es similar a la autenticación de *token,* pero pueden proporcionar funcionalidad adicional. Las tarjetas inteligentes se pueden configurar para ejecutar múltiples aplicaciones, también actúan como la identificación personal incluyendo foto de la compañía para el individuo.

Las tarjetas inteligentes mejoran las soluciones solo de software, como la autenticación de contraseña, al ofrecer el factor adicional de autenticación, se elimina el elemento humano en la memorización de secretos complejos.

6.2.7.5. Autenticación biométrica

La tecnología de este tipo es aquella que determina la autenticación utilizando características biológicas únicas del ser humano. Las características biométricas utilizables incluyen minucias de los dedos, geometría facial, firmas de retina e iris, patrones de voz, patrones de escritura y geometría de la mano. Al igual que los *tokens* físicos y las tarjetas inteligentes, la autenticación biométrica mejora las soluciones solo de software al ofrecer un factor adicional y eliminar el elemento humano para el almacenamiento de datos. Los problemas notados con la autenticación biométrica incluyen:

- Distinguir un objeto real de un falso.
- Manejo de factores ambientales como la temperatura y la humedad que pueden afectar algunos dispositivos biométricos.
- Abordar las aplicaciones industriales en las que los empleados pueden tener lentes o guantes de seguridad, productos químicos industriales que puedan afectar los escáneres.
- Requerir asistencia técnica y verificación cara a cara.
- Denegar el acceso al sistema de control debido a una falla temporal del dispositivo sensor para reconocer a un usuario.

- Ser aceptado este tipo de autenticación socialmente. Para los usuarios algunos dispositivos son más aceptables que otros.

6.2.8. Respuesta a incidentes (IR)

Son las políticas y procedimientos relacionados con la capacitación de respuesta a incidentes, las pruebas, el manejo, monitoreo, los informes y los servicios de soporte.

Un plan de respuesta a incidentes es la documentación de un conjunto predeterminado de instrucciones para detectar y responder a las consecuencias de incidentes contra los sistemas de información de una organización. Si se descubre un incidente, debe realizarse una evaluación rápida del riesgo para evaluar el efecto del ataque y las opciones a responder. Este tipo de procedimiento pertenece a la familia NIST SP 800-53 (IR).

6.2.9. Mantenimiento (MA)

Los controles de seguridad que pertenecen a la familia NIST SP 80-53 (MA) son los encargados de realizar el mantenimiento preventivo y de rutina en los componentes de un IT. Incluye el uso de herramientas de mantenimiento (locales y remotas) y la gestión del personal de mantenimiento.

6.2.10. Protección física y ambiental (PE)

Son las políticas y procedimientos que abordan el control de acceso físico, de transmisión y de pantalla, así como los controles ambientales para el acondicionamiento y disposiciones de emergencia.

Los controles de seguridad de la familia NIST SP 800-53 de PE incluyen puntos de entrada y salida designados, medios de transmisión y de visualización. Estos incluyen controles para monitorear el acceso físico, mantener registros y manejar visitantes. Esta familia también incluye controles para el despliegue y la gestión de controles de protección de emergencia, como el apagado de emergencia del IT, respaldo de energía e iluminación, controles de temperatura y humedad y protección contra incendios y daños por agua.

6.2.10.1. Centro de control / salida de mando

El objetivo es brindar seguridad física para el centro de control o sala de mando que es esencial para reducir el potencial de la amenaza. Los centros de control frecuentemente tienen consolas conectadas continuamente al servidor de control primario, donde la velocidad de respuesta y la visión continua de la planta es de suma importancia. Es importante que el acceso a estas áreas se limite a usuarios autorizados utilizando métodos como tarjetas de identificación inteligentes, magnéticas o dispositivos biométricos.

6.2.10.2. Dispositivos portables

Las computadoras o dispositivos computarizados que se utilizan para las funciones del ICS, como las que programan el PLC, nunca deben salir del área del ICS, deben estar bien aseguradas y nunca se debe permitir su uso fuera de la red ICS.

6.2.10.3. Cableado

El diseño de cableado para los ICS debe abordarse al plan de ciberseguridad. No debe aceptarse cables sin blindaje, debido a su

susceptibilidad a la interferencia de campos magnéticos, ondas de radio, temperaturas extremas, humedad, polvo y vibraciones. Los conectores RJ-45 deben usarse en lugar de otros tipos de conectores de par trenzados, para proporcionar protección contra la humedad, el polvo y la vibración. El cable de fibra óptica y coaxial son buenas opciones de cableado de la red ICS porque son inmunes a muchas condiciones ambientales, como interferencias eléctricas y de radiofrecuencia que se encuentran en el entorno de sistemas control industrial.

6.2.11. Planificación (PL)

Un plan de seguridad es un documento formal que proporciona una visión general de los requisitos de seguridad para un sistema de información y describe los controles de seguridad establecidos o planificados para cumplir con esos requisitos. Los controles de seguridad que pertenecen a esta familia NIST SP 800-53 (PL) proporcionan la base para desarrollar un plan de seguridad. Es un conjunto de reglas que describe las responsabilidades del usuario y el comportamiento esperado con respecto al uso del IT con la provisión de un reconocimiento firmado de los usuarios que indica que han leído, entendido y aceptado cumplir las reglas de comportamiento antes de autorizar el acceso al IT.

6.2.12. Personal de seguridad (PS)

Los controles de seguridad que pertenecen a la familia NIST SP 800-53 (PS) proporcionan políticas y procedimientos para reducir el riesgo humano, robo, fraude u otro mal uso de los IT. Hay tres aspectos importantes:

- Políticas de contratación
- Políticas y prácticas de la organización
- Términos y condiciones del empleo

6.2.13. Evaluación de riesgos (RA)

Los controles de seguridad pertenecen a la familia NIST SP 500-53 (RA) proporcionan políticas y procedimientos para desarrollar y mantener una evaluación de riesgos documentada y describe el propósito, alcance, roles, responsabilidades y cumplimiento, así como la política de implementación de procedimientos. Un sistema de información y datos asociados se clasifican en función de los objetivos de seguridad y una gama de niveles de riesgo. Se hace este tipo de evaluación para identificar los riesgos y magnitud del daño que podría resultar de un acceso no autorizado, su uso, divulgación, modificación o destrucción de un IT.

6.2.14. Adquisición de sistemas y servicios (SA)

Es la asignación de recursos para la seguridad del sistema de información que se mantendrá durante todo el ciclo de vida de los sistemas y el desarrollo de políticas de adquisición basadas en los resultados de evaluación de riesgos, incluidos los requisitos, los criterios de diseño, los procedimientos de prueba y la documentación asociada.

Los controles de seguridad pertenecen a la familia NIST SP 500-53 (SA), se basan en requisitos y especificaciones de seguridad. Como parte de estos procedimientos, un IT se gestiona utilizando una metodología del ciclo de vida de desarrollo del sistema, que incluye consideraciones de seguridad de la información. Se debe mantener documentación adecuada sobre el sistema

información y los componentes constitutivos. La familia SA también aborda los sistemas subcontratados y la inclusión de controles de seguridad adecuados por parte de los proveedores según lo especificado por la organización respaldada.

6.2.15. Protección del sistema y comunicaciones (SC)

Son los mecanismos para proteger tanto el sistema como los componentes de transmisión de datos. Los controles de seguridad pertenecen a la familia de NIST SP 800-53 (SC) y son:

6.2.15.1. Cifrado

Es la transformación criptográfica de datos (llamado texto plano o cifrado) que oculta el significado original de los datos para evitar que se conozcan o usen. Si el proceso es reversible se denomina descifrado. Es necesario determinar si el cifrado es una solución adecuada para un ICS, porque la autenticación y la integridad son generalmente problemas de seguridad clave para los ICS. El uso en ICS podría introducir latencia en comunicaciones debido al tiempo adicional y recursos informáticos necesarios para cifrar cada mensaje.

6.2.15.2. Red virtual privada (VPN)

Un método para cifrar los datos de comunicación es a través de un VPN (red privada), que funciona como una superposición en una infraestructura pública; es decir, que la red privada puede funcionar a través de una red pública. Los tipos más comunes de VPN son:

- Seguridad del protocolo de internet (IPsec): es un conjunto de estándares definidos por IETF para gobernar las comunicaciones seguras de datos a través de redes públicas en la capa IP.

- Capa de *sockets* seguros (SSL): proporciona un canal seguro entre dos máquinas que encripta el contenido de cada paquete. El IETF realizó ligeras modificaciones al protocolo SSL versión 3 y creó un nuevo protocolo llamado *Transport Layer Security* (TLS). SSL se reconoce con mayor frecuencia para proteger el tráfico HTTP, la implementación de este protocolo se conoce como HTTP *Secure* (HTTPS). Sin embargo, SSL no está limitado al tráfico HTTP se puede usar para asegurar muchos programas de capa de aplicaciones diferentes.

- *Secure Shell* (SSH): es un interfaz de comando y un protocolo para acceder de forma segura a una computadora remota. Es ampliamente utilizado por los administradores de red para controlar de forma remota, los servidores web y otros tipos de servidores.

6.2.16. Integridad del sistema de la información (SI)

Son las políticas y procedimientos para proteger los sistemas de información y sus datos de fallas de diseño y modificación de datos mediante la verificación de la funcionalidad, verificación de la integridad de datos, la detección de intrusos, la detección de códigos maliciosos y los controles de alerta y advertencia de seguridad.

Mantener la integridad del sistema y la información, asegura que los datos confidenciales no se hayan modificado o eliminado de manera no autorizada y sin ser detectados. Estos controles de seguridad pertenecen a la familia NIST

SP 800-53 (SI). Existen controles para la detección de códigos maliciosos, la protección contra *spam y spyware* y la detección de intrusos, aunque pueden no ser apropiados para todas las aplicaciones de ICS. También se proporcionan controles para recibir alertas y avisos de seguridad y la verificación de las funciones de seguridad en el sistema de información.

6.2.16.1. Detección de virus y códigos maliciosos

Los productos de detección de códigos de malware y antivirus evalúan los archivos en los dispositivos de almacenamiento de una computadora contra un inventario de archivos de firmas de malware conocidas. Si uno de los archivos en una computadora coincide con el perfil de un virus conocido, el virus se elimina mediante un proceso de desinfección para que no pueda infectar otros archivos locales o comunicarse a través de una red para infectar otros archivos. El software antivirus se puede implementar en estaciones de trabajo, servidores, *firewalls* y dispositivos de mano.

6.2.16.2. Detección y prevención de intrusiones

Los sistemas (IDS) monitorean eventos en una red, como patrones de tráfico o un sistema como entradas de registro o accesos a archivos, para que puedan identificar a un intruso entrando o intentando entrar en un sistema. Los IDS aseguran que la actividad inusual, como los nuevos puertos abiertos, los patrones de tráfico inusuales o los cambios en los archivos críticos del sistema operativo sean señalados al personal de seguridad apropiado. Los tipos de IDS más utilizados son:

- IDS basados en red: estos sistemas monitorean el tráfico de red y generan alarmas cuando identifican el tráfico que consideran un ataque.

- IDS basados en *host:* este software monitorea uno o más tipos de características de un sistema, como entradas de archivos de registro de aplicaciones, cambios en la configuración del sistema y acceso a datos confidenciales en un sistema y responde con una alarma o contramedida cuando el usuario intenta violar la seguridad.

6.2.16.3. Manejo de parches

Los parches son piezas de código adicionales que se han desarrollado para abordar problemas o fallas específicas en el software existente. Las vulnerabilidades son fallas que pueden explotarse, lo que permite el acceso no autorizado a los sistemas de IT o permite a los usuarios tener acceso a mayores privilegios que los autorizados. Un enfoque sistemático para administrar y usar parches de software puede ayudar a las organizaciones a mejorar la seguridad general de sus sistemas IT de una manera rentable. El NIST SP 800-40 revisión 3 proporciona orientación para los gerentes de seguridad de la organización que son responsables de diseñar e implementar parches de seguridad y programas de gestión de vulnerabilidades.

6.2.17. Gestión de programas (PM)

Proporciona controles de seguridad a nivel organizacional en lugar de a nivel de sistema de información.

Los controles de seguridad que se incluyen en el NIST SP 800-53 (PM) se centran en los requisitos de seguridad de la información de toda la organización, que son independientes de cualquier sistema de información en particular, y son esenciales para administrar los programas de seguridad de la información.

6.2.18. Controles de privacidad

Es fundamental proteger la privacidad de la información de identificación personal (PII) recopilada por los programas y sistemas de información, dados los avances en las tecnologías de la información y sus aplicaciones. La privacidad efectiva para las personas depende de las garantías empleadas dentro de los sistemas de información de la organización que procesan almacenan y transmiten la PII. Los controles de privacidad se basan en los "principios de práctica de información justa" (FIPP) incorporados en la ley de privacidad de 1974, sección 208 de la ley de gobierno electrónico de 2002 y la orientación relacionada de la oficina de administración y presupuesto (OMB).

Los controles de privacidad son las garantías administrativas técnicas y físicas empleadas dentro de las organizaciones para proteger y garantizar el manejo adecuado de la PII. Hay ocho familias de control de privacidad con cada familia alineada con uno de los FIPP. Las familias de control de privacidad se pueden implementar a nivel de organización o sistema de información.

Los controles de privacidad están estructurados de manera similar a los controles de seguridad del sistema de información. En la parte de privacidad de NIST 800-53 REV 4, proporciona un conjunto estructurado de controles de privacidad, basados en estándares internacionales y mejores prácticas para ayudar a las organizaciones a hacer cumplir los requisitos derivados de la legislación, de privacidad y orientación.

Se promueve una cooperación más estrecha entre los funcionarios de seguridad y privacidad dentro del gobierno federal para ayudar a lograr los objetivos de los líderes o ejecutivos de alto nivel en la aplicación de los

requisitos de la legislación, políticas, reglamentos federales sobre privacidad. Las 8 familias de control de seguridad incluyen:

- Autoridad y propósito (AP)
- Responsabilidad, auditoría, y gestión de riesgos (AR)
- Calidad e integridad de los datos (DI)
- Minimización y retención de datos (DM)
- participación individual y compensación (IP)
- Seguridad (SE)
- Transparencia (TR)
- Limitación de uso (UL)

CONCLUSIONES

1. Con la llegada de la industria 4,0, los sistemas de control están prácticamente conectados en línea a internet o una intranet, lo que genera una integración entre los sistemas IT y OT.

2. Las organizaciones IT han diseñado su seguridad para proteger los datos como información financiera, propiedad intelectual, mientras que los ICS, demandan que la seguridad se extienda a su infraestructura crítica, la cual está totalmente relacionada e interconectada a la red IT.

3. Todo sistema que incluye al menos un sistema PLC debe contener un sistema de seguridad, debido a la posibilidad de que puedan ser alterados los datos en su memoria a través de internet o una intranet.

4. Aunque los PLC estándares han ido incorporando funciones de diagnóstico para mejorar la seguridad, siempre son menores a las que contienen los PLC de seguridad. Estos cumplen con SIS y están certificados con normas IEC, además, están diseñados para cumplir determinado nivel de SIL, aumentando la productividad del sistema ICS.

5. La seguridad no solo se centra en proteger las contraseñas de los usuarios, sino que también debe enfocarse en las instalaciones donde se realizar el proceso de desenvolvimiento de una Industria y la protección de sus ocupantes.

6. Los principales objetivos de seguridad para una implementación de un ICS deben incluir lo siguiente: restricción del acceso lógico a la red del ICS y a la actividad de la red, restricción del acceso físico a la red y a los dispositivos de ICS, protección de los componentes individuales del ICS, mantenimiento de las operaciones en condiciones adversas y restauración del sistema después de un incidente.

7. Las vulnerabilidades a las que están expuestos los ICS han logrado escribir datos en el buffer, cambiar su funcionamiento, dañar datos, bloquear programas de ejecución de tareas, inyectar secuencias de comandos de los clientes, alterar información privilegiada y eludir el control de acceso. La información que se almacena en texto sin formato puede ser fácilmente hackeada.

8. Para analizar el riesgo de una industria es necesario manejarlo a nivel de la organización, nivel de proceso y del sistema de información. Es importante considerar el enmarcado del proceso, planificación y evaluación.

9. Los sistemas de seguridad deben minimizar los efectos de un ciber ataque a los ICS ejecutando tareas de monitoreo y control que garantice la seguridad de las persona, datos, efectos y componentes de los ICS.

10. Un equipo de seguridad debe contener de un miembro de IT, un ingeniero de control, operador de sistema, el experto en temas de seguridad y el encargado de manejo de riesgos.

11. Se debe garantizar que los sistemas OT e IT tengan un sistema de seguridad apropiado utilizando la tecnología más avanzada para la

prevención detección y recuperación de la seguridad, en caso de haber sufrido un ataque.

12. Para mejorar la seguridad de los sistemas ICS se puede segmentar y segregar la red; es decir, dividir la red en subredes pequeñas para establecer dominios de seguridad Son conceptos muy efectivos para implementarse en la búsqueda de proteger un ICS.

13. El uso de *firewalls*, software que evita malware, bloquea amenazas cibernéticas, controla el flujo de comunicación, bloquea tráfico que puede ser dañino para los ICS y proporciona herramientas para hacer cumplir la seguridad.

14. Es importante que las industrias cumplan las normas NIST SP 800-53 que cubre la gestión y las prácticas operativas de seguridad de la información.

15. Se debe seleccionar los controles mínimos de seguridad que protegerán el sistema de información en función de los requisitos que solicita FIPS 200.

16. El control de acceso basado en roles reduce el costo de administrar la seguridad en redes de muchos dispositivos inteligentes. Restringe privilegios de los usuarios de ICS logrando el principio de privilegio mínimo. Ofrecen mecanismos de autorización en el área de IT.

17. El uso de VLAN mejora el rendimiento y administración simplificando el diseño de la red. Cada VLAN aísla el tráfico de otras VLAN limitando el tráfico de transmisión.

18. Es importante instalar controles de autenticación de los usuarios de un sistema ICS. Debe concentrarse en el análisis propio de las personas y evitar suplantación.

19. Implementar mecanismos de autenticación sólidos para educar a los empleados sobre cómo proteger sus credenciales.

RECOMENDACIONES

1. Aplicar un adecuado sistema de seguridad debido a que la tecnología 4,0 hace que los sistemas ICS estén conectados a internet en tiempo real y sean más vulnerables aumentando el riesgo de ciberataques.

2. Realizar un análisis de los ciberataques registrados a los sistemas ICS de compañías similares, para que las empresas mejoren la protección y el sistema de seguridad que implementan.

3. Garantizar los sistemas de información (IT) y sistemas de operación (OT) creando un nivel de seguridad que cumpla con los requisitos de las empresas. Se debe aplicar los estándares más avanzados en los activos tecnológicos que respaldan la operación de infraestructuras críticas y que cumplan con los controles de seguridad contenidos en NIST SP 800-53.

4. Desarrollar una estrategia de la arquitectura de defensa en profundidad con el uso de firewalls, creando una DMZ que tenga la capacidad de detección de intrusos y políticas de seguridad efectivas. Buscar los mecanismos de respuesta a incidentes y seguridad física.

5. Aplicar los controles de seguridad que sean necesarios para mantener protegido el sistema de información en sistemas nuevos o ya establecidos y que puedan contener diferentes planes de seguridad para producir el resultado deseado.

6. Utilizar tecnologías de control de acceso, ya que ayudarán en el filtrado, bloqueo y regulación de la información entre dispositivos o sistemas.

7. Realizar evaluaciones periódicas con el fin de determinar si los controles de seguridad se han implementado correctamente y se pueda obtener los resultados deseados.

8. Crear un plan de contingencia que pueda mantener operando un ICS en caso de emergencia, fallas o desastres.

BIBLIOGRAFÍA

1. Adaptix networks*. Ciberseguridad Industrial.* [en línea]. <https:// www.adaptixnetworks.com/ciberseguridad-industrial/>*.* [Consulta: 10 de enero de 2020].

2. DEHOF, Matthias. *The IAONA Handbook for Network Security.* Alemania; 2006. 81 p.

3. FIPS pub 200*. U.S. Department of commerce, federal information processing minimum security requirements for federal Information and Information Systems.* [en línea]. <https: //csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf>. [Consulta: 30 de abril de 2020].

4. Genbeta*. Stuxnet: Historia de la primera arma de la ciberguerra.* [en línea]. <https://www.genbeta.com/seguridad/stuxnet-historia-del-primer-arma -de-la-ciberguerra>. [Consulta: 9 de febrero de 2020].

5. HAYDEN, Ernie. *An abbreviated history of automation and ICS cybersecurity.* Maryland, Estados Unidos: 2014. 32 p.

6. Instituto Nacional de ciberseguridad. *Análisis de riesgo en 6 pasos.* [en línea]. <https://www.incibe.es/protege-tu-empresa/blog/análisis-riesgos-pasos-sencillo>. [Consulta: 3 de abril de 2020].

7. International society of automation. *ISA-62443, Security for industrial automation and control systems.* [en línea]. https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99. [Consulta: 15 de febrero de 2020].

8. JEFF, Lund. *ICS security essential firewall concepts*. [en línea].<https://www.belden.com/blog/industrial-security/ics-security-essential-firewall-concepts>. [Consulta: 2 de abril de 2020].

9. KEENEY, Michelle. *Insider threat study. Computer system sabotage in critical Infrastructure sectors*. [en línea]. <http://www.cert.org/archive/pdf/insidercross051105.pdf. [Consulta: 6 de marzo de 2020].

10. LAURRIEU-LET, Enrique. *Seguridad en los sistemas de control industrial.* [en línea]. <https://www.editores-srl.com.ar/revistas/aa/2/larrieu_let_sistemas_de_control_industrial>_[Consulta: 8 de febrero de 2020].

11. LUND, Jeff. *ICS security essential firewall concepts*. [en línea]. <https://www.belden.com/blog/industrial-security/ics-security-essential-firewall-concepts>. [Consulta: 2 de abril de 2020]

12. MELTZER, David. *Industrial Cybersecurity for dummies.* Estados Unidos. 2017. 29 p.

13. MACAULAY, Tyson. *Cybersecurity for Industrial control systems.* Estados Unidos: CRC press, 2011. 330 p.

14. National Institute of standards and technology. *Guide for Applying the Risk Management Framework to Federal Information Systems.* [en línea]. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf. [Consulta: 28 de abril de 2020].

15. PLC design*. Qué es un PLC de seguridad.* [en línea]. <https://plcdesign.xyz/que-es-un-plc-de-seguridad/*>.* [Consulta: 8 de febrero de 2020].

16. Risoul. *Beneficios de contar con soluciones de ciberseguridad para tu empresa.* [en línea].<https://www.risoul.com.mx/blog/beneficios-de-contar-con-soluciones-de-ciberseguridad-para-tu-empresa*>.* [Consulta: 3 de abril de 2020].

17. ROMERO, Henry. *Ciberseguridad en sistemas de control Industrial ICS.* Trabajo de tesis., Universidad Distrital Colombia D.C, 2018. 70 p.

18. SCARFONE, Karen*. Guidelines on firewalls and firewalls policy.* [en línea]. <https://csrc.nist.gov/publications/PubsSPs.html. [Consulta: 30 de marzo de 2020].

19. STEVEN, Rinaldi. *Identifying understanding and analyzing critical Infrastructure Interdependencies.* [en línea]. <https://www.osti.gov/biblio/949367-identifying-understanding-analyzing-critical-infrastructure-interdependencies>. [Consulta: 12 de abril de 2020].

20. STINE, Kevin*. Guide for mapping types of information and information systems to security categories.* [en línea].

>https://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.Nist.gov/publications/PubsSPs.html#800-60>. [Consulta: 20 de mayo de 2020].

21. STOUFFER, Keith. *Guide to industrial control systems ICS security.* [en línea]. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/*NIST-SP.800-82r2.pdf.* [Consulta: 25 de enero de 2020].

22. Zonavirus. *McAfee informa sobre la peligrosidad del night dragon.* [en línea]. <https://www.zonavirus.com/noticias/2011/mcafee-informa-sobre-la peligrosidad-del-night-dragon.asp>. [Consulta: 25 de febrero de 2020].