

ESCUELA SUPERIOR POLITECNICA DEL LITORAL



Facultad de Ingeniería en Electricidad y Computación Maestría en Seguridad Informática Aplicada MSIA

“DISEÑO DE UN ESQUEMA DE SEGURIDAD PARA LA RED DE
DATOS DE UN CENTRO DE CONTROL QUE USE UN SISTEMA
SCADA”

EXAMEN DE GRADO (COMPLEXIVO)

PREVIO A LA OBTENCIÓN DEL GRADO DE:

MÁGISTER EN SEGURIDAD INFORMÁTICA APLICADA

CARLOS ALBERTO VITERI CHÁVEZ

GUAYAQUIL – ECUADOR

AÑO: 2015

AGRADECIMIENTO

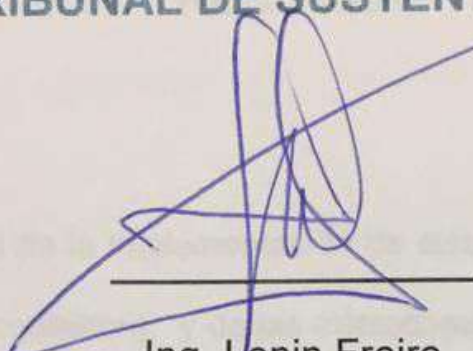
Agradezco a primero Dios, quien me brinda su apoyo y protección en todo momento, a mis padres que siempre han estado pendiente y apoyándome en mis estudios y mi bienestar, a mi esposa e hijos que son la razón de todos mis esfuerzos y mis alegrías.

TRIBUN DEDICATORIA FACULTAD

El presente proyecto les dedico a mis padres Carlos Viteri e Isabel Chavez, a mi esposa Pamela Cruz, mi princesa Sophie y mi hijo Carlitos Julián quien nació para estar en mi graduación.



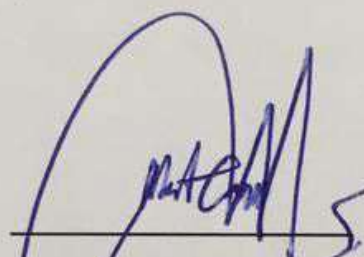
TRIBUNAL DE SUSTENTACIÓN



Handwritten signature of Ing. Lenin Freire in blue ink, written over a horizontal line.

Ing. Lenin Freire

DIRECTOR DEL MSIA

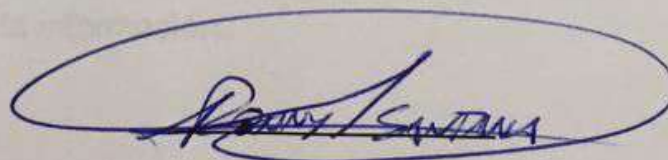


Handwritten signature of Mgs. Albert Espinal in blue ink, written over a horizontal line.

Mgs. Albert Espinal

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA



Handwritten signature of Mgs. Ronny Santana in blue ink, written over a horizontal line.

Mgs. Ronny Santana

PROFESOR DELEGADO

POR LA UNIDAD ACADEMICA

RESUMEN

La necesidad actual de la implementación de sistemas SCADA (Supervisory Control and Data Acquisition), y de las interconexiones con otras redes para convivir con otros servicios informáticos crea un desafío en el diseño de una arquitectura de red que brinde la confianza necesaria en la seguridad de la información.

El principal objetivo de este trabajo es diseñar un esquema de seguridad adecuado y óptimo para cualquier red de datos que se implemente en un Centro de Control y Monitoreo que utilice un sistema SCADA, con el fin tomar las medidas necesarias para garantizar la confidencialidad, integridad y disponibilidad de la información.

En este trabajo se indica un breve resumen de sistemas SCADA indicando sus componentes, aplicaciones y principales ataques reconocidos en el mundo, luego se realiza un análisis y gestión de riesgos, finalmente con los

resultados obtenidos en la gestión de riesgos se propone un esquema de seguridad físico y lógico adecuado para estas redes.

Con este proyecto cualquier empresa que desee la implementación de un sistema SCADA podrá contar con un esquema de seguridad en la red de datos base, diseñado en base a riesgos generales y activos críticos generales de estas redes.

ÍNDICE GENERAL

AGRADECIMIENTO	ii
DEDICATORIA	iii
TRIBUNAL DE SUSTENTACIÓN	iv
RESUMEN.....	v
ÍNDICE GENERAL	vii
ABREVIATURAS Y SIMBOLOGÍA	ix
ÍNDICE DE FIGURAS.....	xi
ÍNDICE DE TABLAS.....	xii
INTRODUCCIÓN.....	xiii
GENERALIDADES	1
1.1 Descripción del problema	1
1.2 Solución propuesta.....	2
1.3 Sistemas SCADAS	3
1.4 Ataques a sistemas SCADAS.....	7
CAPÍTULO 2.....	12
ANÁLISIS Y GESTIÓN DE RIESGOS	12
2.1 Criterios de evaluación	13
2.2 Identificación y valoración de activos críticos de la red de datos	15
2.3 Identificación y análisis de amenazas y vulnerabilidades.....	18
2.4 Evaluación de riesgos.....	21
2.5 Tratamiento de riesgos potenciales	30
CAPÍTULO 3.....	34
DISEÑO DE LA SEGURIDAD EN LA RED	34
3.1 Seguridad Lógica.....	34
3.1.1 Esquema de seguridad lógica general de la red de datos.....	34
3.1.2 Esquema de las redes corporativas y de control.....	37
3.1.3 Almacenamiento y respaldo de la información.....	39

3.1.4	Control de accesos lógicos	40
3.1.5	Protección contra código malicioso.....	41
3.2	Seguridad física.....	41
3.2.1	Áreas seguras	42
3.2.2	Seguridad de los equipos	42
3.3	Monitoreo y gestión de logs	44
CONCLUSIONES Y RECOMENDACIONES		46
BIBLIOGRAFÍA.....		50

ABREVIATURAS Y SIMBOLOGÍA

CIP	Common Industrial Protocol (Protocolo Industrial Común)
CERT	Computer Emergency Readiness Team (Equipo de Respuesta ante Emergencias Informáticas)
DCS	Distributed Control System (Sistemas de Control Distribuidos)
DNP	Distributed Network Protocol (Protocolo de red distribuido)
DMZ	Demilitarized Zone (Zona desmilitarizada)
FIREWALL	Cortafuegos diseñado para impedir el acceso no autorizado.
HMI	Humman Machine Interface (Interfaz Hombre Máquina)
ICS	Industrial Control System (Sistemas de Control Industrial)
IED	Intelligent Electronic Device (Equipo Electrónico Inteligente)
IPS	Intrusion Prevention System (Sistema de Prevención de Intrusos)
IPsec	Internet Protocol security (Seguridad en Internet Protocol)
LAN	Local Area Network (Red de Área Local)
MAGERIT	Metodología de Análisis y Gestión de Riesgos de los Sistemas de la Información
NIST	National Institute of Standards and Technology (Instituto Nacional de Estándar y Tecnologías)
PLC	Programmable Logic Controller (Controlador lógico Programable)
SCADA	Supervisory Control And Data Acquisition (Supervisión, Control y Adquisición de datos).
SCI	Sistemas de Control Industrial

S.O.	Sistema Operativo
RTU	Remote Terminal Unit (Unidad Terminal Remota)
TCP-IP	Protocolo de Control de Transporte- Protocolo internet.
UPS	Sistema de alimentación ininterrumpida
VLAN	Virtual Local Area Network (Red de Área Local Virtual)
VPN	Virtual Private Network (Red Privada Virtual)
WAN	Wide Area Network (Red de Área Ampliada)

ÍNDICE DE FIGURAS

FIGURA 1.1.- Esquema básico de un sistema SCADA.....	4
FIGURA 1.2.- Reporte de vulnerabilidades ICS en 2013 por ICS-CERT.....	9
FIGURA 1.3.- Reporte de incidentes ICS en 2014.....	10
FIGURA 1.4.- Reporte de vulnerabilidades ICS año 2011-2014 por ICS-CERT.....	11
FIGURA 2.1.- Matriz de Riesgos.....	14
FIGURA 3.1.- Esquema de seguridad lógica general de la red.....	36
FIGURA 3.2.- Esquema de red de Control.....	38
FIGURA 3.3.- Esquema de red corporativa.....	39
FIGURA 3.4.- Esquema de Gestión centralizada de logs.....	45

ÍNDICE DE TABLAS

Tabla 1.- Protocolos de sistemas SCADAS	6
Tabla 2.- Ataques confirmados a sistemas SCADA	8
Tabla 3.- Tabla de valoración de activos.....	13
Tabla 4.- Valoración de la probabilidad de ocurrencia de amenazas.	14
Tabla 5.- Valoración del impacto de ocurrencia de amenazas	14
Tabla 6.- Criterio de tratamiento de riesgos	15
Tabla 7.- Identificación de activos de la Red.....	15
Tabla 8.- Valoración de activos.....	16
Tabla 9.- Categorías de vulnerabilidades.....	18
Tabla 10.- Listado de Vulnerabilidades y Amenazas potenciales.....	19
Tabla 11.- Tratamientos de riesgos.....	31

INTRODUCCIÓN

La necesidad de automatizar y simplificar los procesos de negocio de las empresas crea la necesidad de la implementación de sistemas que permitan mejorar la gestión de estos procesos y disminuir sus costos operativos.

Bajo este criterio se ha evidenciado el aumento de uso de sistemas SCADA y con ello la creación de Centros de Control y Monitoreo, permitiendo así la gestión centralizada de procesos de negocio mediante la recolección de datos locales y de lugares dispersos geográficamente.

Los sistemas SCADA generalmente se emplean en sectores de electricidad, agua, petróleo, entre otros, considerados como sectores críticos para la industria y gobiernos de países.

Considerando la criticidad de sus aplicaciones y la tendencia de interconexión con otras redes como la de internet se ha convertido en un objetivo clave para atacantes externos por lo cual se requiere tener un esquema de seguridad adecuado.

En este documento se describe el análisis y diseño de un esquema de seguridad para la red de datos de un Centro de control y monitoreo que use un sistema SCADA, en base a un análisis de riesgos de las amenazas y vulnerabilidades más comunes en estos sistema que se pueden materializar en los activos críticos de estas redes, basados en los principios de la seguridad de la información.

CAPÍTULO 1

GENERALIDADES

1.1 Descripción del problema

La necesidad de mejorar la administración de sistemas y procesos industriales mediante la recolección y tratamiento centralizado de datos locales y remotos hace que hoy en día se incremente el uso de sistemas SCADA, con los cuales se tienen beneficios de monitoreo, supervisión y adquisición de datos de una manera centralizada de sistemas electrónicos y/o equipos locales y remotos que se encuentran geográficamente distantes.

El uso de estos sistemas requiere la implementación de un Centro de control y monitoreo con una conexión de una red LAN para los equipos locales y una red WAN para los equipos o sistemas remotos de donde se recolectará la

información, así también la necesidad del uso de servicios informáticos como el internet, correo electrónico entre otros, hace que la seguridad de las redes en donde convergen estos sistemas y servicios mencionados se torne compleja y vulnerable de amenazas que van en continuo crecimiento.

Considerando el uso y la criticidad de la información recolectada y almacenada de los sistemas SCADA en todo el mundo y la necesidad de interconectarlas con otras redes y servicios informáticos en Centros de control y monitoreo, es indispensable el diseño de una red segura y confiable que permita la disponibilidad, integridad y confidencialidad de la información.

1.2 Solución propuesta

Debido a que el uso de los sistemas SCADA requieren la gestión de seguridad de la información basados principalmente en la disponibilidad de los enlaces, la integridad de los datos recolectados y almacenados, así como la confidencialidad de la información, es necesario realizar un diseño de seguridad en la red de datos adecuado para el uso de este sistema, conexiones internas, externas y el uso de aplicaciones informáticas necesarias para la normal operación de un centro de control y monitoreo.

Los sistemas SCADA fueron diseñados para operar en redes cerradas y aisladas de otras redes, por lo cual estos sistemas no contemplan parámetros de seguridad nativos en su diseño, pero que son necesarios cuando se

interconectan con otras redes que usan el protocolo TCP/IP, sobre el cual funcionan la mayoría de aplicaciones y servicios informáticos que hoy en día son considerados como herramientas básicas de toda empresa, como lo es el Internet, correo electrónico, compartición de archivos, entre otros.

El diseño propuesto se basa en un análisis de riesgos de los activos críticos de estas redes y contemplará un esquema de seguridad lógica y física, así como la estrategia de monitoreo y gestión de logs para garantizar la seguridad de la información y minimizar los riesgos identificados.

1.3 Sistemas SCADAS

Los sistemas SCADA cuyas siglas significan (Supervisory, Control and Data Acquisition) que se traduce como Sistemas de Supervisión, Control y Adquisición de Datos, son una combinación de hardware y software que permite supervisar y controlar en tiempo real uno o varios procesos remotos través de datos recolectados en campo.

Los sistemas SCADA son parte de los Sistemas de Control Industrial (SCI), que es un término general que engloba a diferentes sistemas de control y que también incluyen los Sistemas de Control Distribuidos DSC.

El esquema básico de un sistema SCADA se presenta a continuación: [1]

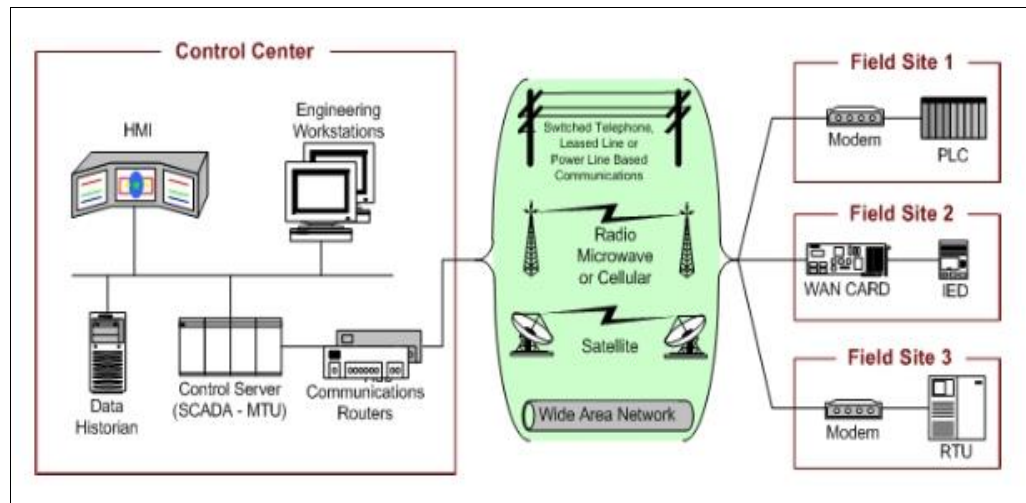


FIGURA 1.1.- Esquema básico de un sistema SCADA

Como se aprecia en este gráfico, los componentes básicos de un sistema SCADA son:

- 1) Servidor SCADA o MTU. Equipo principal que recibe la información de los dispositivos de campo en tiempo real.
- 2) Servidor de históricos.- Equipo donde se almacena la información histórica de los datos recolectados.
- 3) Software HMI (Human machine interface). - Software con interfaces gráficas para la gestión y uso de la funcionalidad de sistema SCADA.
- 4) Comunicaciones.- Medio por el cual se comunican los dispositivos de campo hacia el servidor principal o MTU. Existen diversas tecnologías como fibra óptica, cobre, radioenlace, satelital.

- 5) Dispositivos de campo.- Son los dispositivos recolectores de datos como RTU (Remote Terminal Unit), PLC (Programmable Logic Controllers) e IED (Intelligent Electronic Device).

Los sistemas SCADA generalmente se emplean en sistemas de distribución de electricidad, agua, petróleo, gas, transportación, entre otros, por lo cual su uso se considera crítico ya que un error o fallo de todo el sistema implicaría un daño importante, paralización de un servicio de uso masivo y hasta poner en peligro vidas humanas. [2] [3].

Inicialmente los sistemas SCADAS eran simples y aislados que solo monitoreaban y controlaban procesos industriales con lo cual no había mayores riesgos de seguridad, sin embargo en la actualidad su concepto se ha ampliado y hoy en día se monitorean adicionalmente otros tipos de dispositivos como cámaras, sensores, interruptores y otros elementos mecánicos. Así mismo su uso ya no es aislado y se ha integrado con otras redes como la de internet, aumentando así los riesgos de ataques externos. [1]

Los protocolos de sistemas SCADAS fueron diseñados para ser eficientes pero no seguros, ya que no se implementaron con mecanismos de seguridad y muchos de ellos transmiten la información en texto plano, puesto que su aplicación inicial no contemplaba la interconexión con otras redes, sin embargo debido al desarrollo y crecimiento de estos sistemas fueron integrándose al protocolo TCP/IP con el fin de ahorro de costes.

Los protocolos nativos de SCADA más comunes se los detalla en el siguiente cuadro: [1] [4] [5]

Tabla 1.- Protocolos de sistemas SCADAS

PROTOCOLO	DESCRIPCION	VENTAJAS	DEBILIDADES
FOUNDATION FIELDBUS	Sistema de comunicación seria de dos vías completamente digital. Versión HSE (Ethernet de alta velocidad).	Soporta cableado multipunto y fibra óptica.	Uso complejo. No cuenta con seguridad.
PROFIBUS	(Process Field Bus) Norma internacional de bus de campo de alta velocidad para control de procesos normalizada en Europa por EN 50170.	Diferentes versiones como PROFINET, que es PROFIBUS sobre Ethernet (TCP/UDP).	Ausencia de autenticación, cifrado, etc.
MODBUS	Protocolo propietario muy utilizado. Tiene una versión Modbus TCP que trabaja en la capa de aplicación.	Es simple. Tiene 127 funciones. Se integra con redes Ethernet/IP y DeviceNet.	No hay elementos de seguridad
OPC	Usado para control y monitorización de sistemas.	Provee integridad del mensaje, autenticación de usuario, confidencialidad y log de auditoria. Protección contra DoS, mensajes malformados	Descubrimiento de niveles y servicios de seguridad de los servidores. Uso de protocolos sin cifrado como http.
Dnp3	Del acrónimo en inglés Distributed Network Protocol. Actualmente tiene una versión secure DNP3 que trabaja en la capa de aplicación.	Protocolo abierto, permite interconexión entre diferentes fabricantes	Ausencia de medidas de seguridad. La versión secure DNP3 viene con el algoritmo PSK.
EtherCAT	Protocolo que trabaja directamente sobre Ethernet.	Comunicación con otras redes a través de gateways. Interoperabilidad	Envío de datos a todos los conectados sobre el bus de datos

		con otros protocolos.	
DeviceNet	Red de bajo nivel que opera con el protocolo de comunicación CIP	Es un protocolo abierto. Usa diferentes tipos de comunicaciones.	Ancho de banda limitado y tamaño limitado de mensajes. No cuenta con seguridad.

1.4 Ataques a sistemas SCADAS

Debido a que un ataque a estos sistemas puede causar un daño físico de equipos e incluso vidas humanas, se vuelve un objetivo atractivo para los hackers, así como también para el terrorismo.

Aunque es difícil conocer todos los ataques a estos sistemas en el mundo, ya que las empresas o gobiernos no están obligados a reportarlos, existen varios reportes de ataques confirmados a estos sistemas siendo el más conocido el gusano informático **STUXNET**, descubierto en junio de 2010 por VirusBlokAda, una empresa de seguridad radicada en Bielorrusia y del cual se expresa que fue creado por los gobiernos de Israel y EEUU para atacar los programas nucleares de Irán. Este gusano es capaz de reprogramar controladores lógicos programables (PLC) y ocultar los cambios realizados. [6]

A continuación un resumen de los ataques confirmados a estos sistemas en orden cronológico. [7] [8]

Tabla 2.- Ataques confirmados a sistemas SCADA

FECHA	DESCRIPCIÓN
2009	El virus Night Dragon descubierto y bautizado por McAfee atacaron las operaciones de empresas petroleras, químicas y de gas. Utilizó un ataque conocido como spear phishing que permitía controlar los equipos de forma remota.
2010	El Virus STUXNET , que permite reprogramar PLC y que destruyó una quinta parte de las centrifugadoras de Irán.
2014	Un troyano conocido como HAVEX que se descargaba de páginas comprometidas de fabricantes de estos sistemas. También se conoce que un grupo de hacker rusos denominado Oso Energético utilizó este malware para provocar daños en empresas energéticas de EEUU de acuerdo a firma de seguridad CrowdStrike
2014	Malware Blacken que controla por completo y de forma remota un sistema comprometido, utiliza la vulnerabilidad sandworm (CVE-2014-4.114). Descubierto por investigadores de Trend Micro.
2014	A finales de 2014 un ataque a contra una planta de acero alemana provocó daños físicos según reporte de la Oficina Federal para la Seguridad de la Información de Alemania, o la BSI

El Equipo de Respuesta a Emergencias de Sistemas Informáticos de Control Industrial (ICS-CERT por sus siglas en inglés) del Departamento de Seguridad Nacional de los Estados Unidos (DHS) público en abril de 2014, un análisis de vulnerabilidades de Sistemas de Control Industrial (ICS) durante el año 2013, en este reporte se destaca que la mayor vulnerabilidad fue la de autenticación con un

33%, segundo por la negación de servicio con 14% y Buffer Overflow (sobrecarga de memoria) con un 10%. [9]

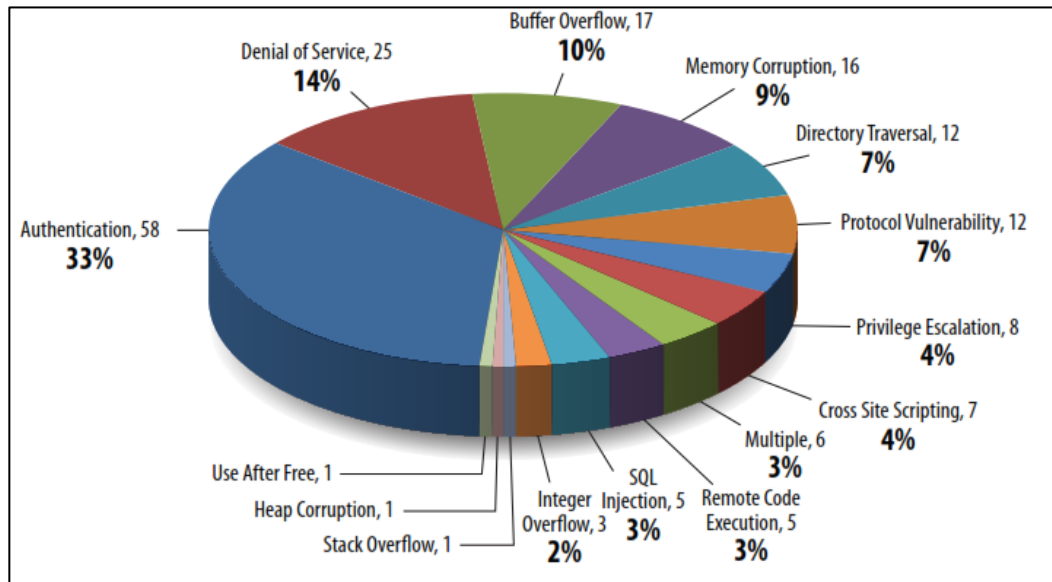


FIGURA 1.2.- Reporte de vulnerabilidades ICS en 2013 por ICS-CERT

FUENTE: NCCIC/ICS-CERT Monitor for January-April 2014

La misma organización ICS-CERT en su publicación Monitor (ICS-MM201502) September 2014-February 2015, indicó que le fueron reportados 245 incidentes de seguridad en el año 2014 de los cuales un 38% fueron desconocidos. [10]

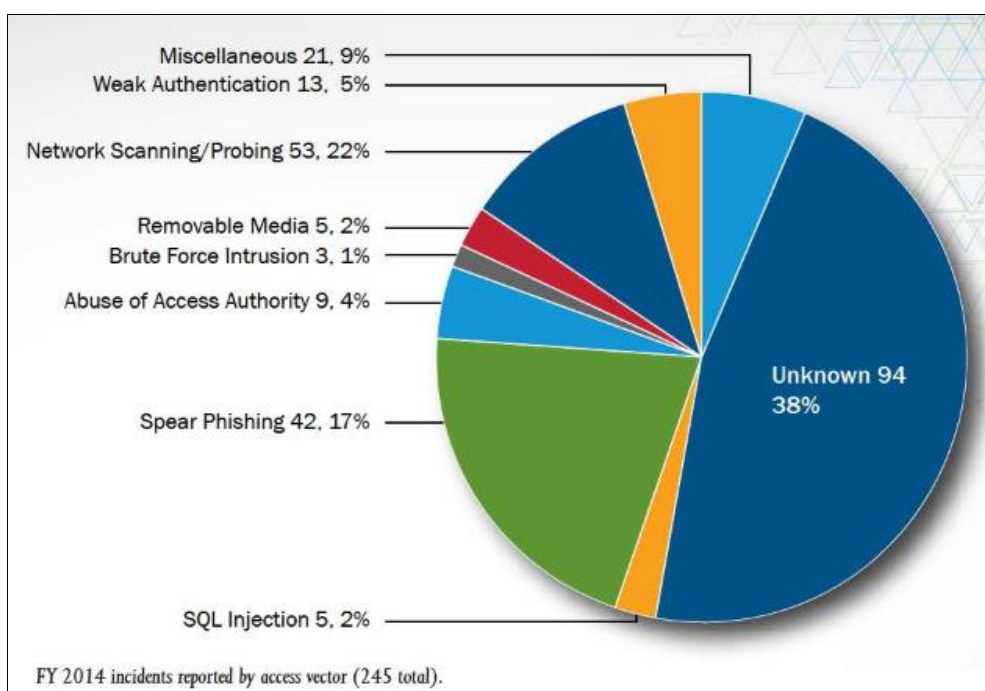


FIGURA 1.3.- Reporte de incidentes ICS en 2014

Fuente: ICS-CERT_Monitor_Sep2014-Feb2015.pdf

Esta misma organización reportó una estadística de las vulnerabilidades encontradas desde el año 2011 al 2014, en donde las más comunes vulnerabilidades son la autenticación, buffer overflow (sobrecarga de memoria) y negación de servicio. [10]

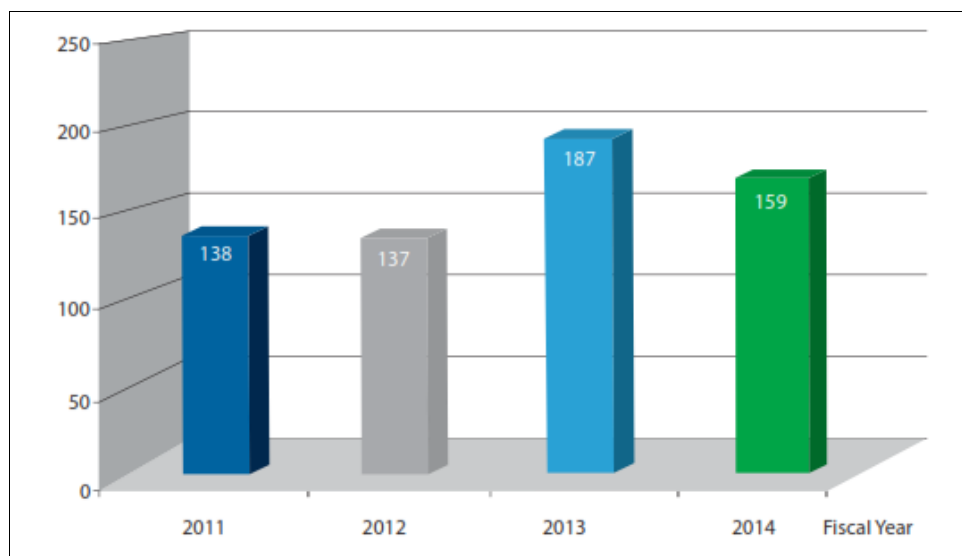


FIGURA 1.4.- Reporte de vulnerabilidades ICS año 2011-2014 por ICS-CERT

Fuente: ICS-CERT_Monitor_Sep2014-Feb2015.pdf

Estas estadísticas nos demuestran que los sistemas SCADA o ICS son objetos de ataques constantes y en continuo crecimiento debido a los procesos que controlan, sin embargo de todos los reportes indicados, un gran porcentaje han sido considerados como desconocidos principalmente debido a la falta de capacidades de detección y monitoreo de las redes comprometidas.

CAPÍTULO 2

ANÁLISIS Y GESTIÓN DE RIESGOS

Para realizar el análisis de riesgos es necesario contemplar el modelo del negocio donde se implementará el sistema SCADA, el cual parametriza o personaliza las principales amenazas, sin embargo para este documento se realizará un análisis de riesgos de manera general contemplando los activos básicos de una red SCADA y listando las amenazas y vulnerabilidades más comunes sobre estos sistemas que se han conocido o presentado en informes públicos.

Para el siguiente análisis de riesgos se ha tomado en cuenta alguna recomendaciones de metodología MAGERIT (acrónimo de “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información”) en su versión 3.0 y la NIST 800-82.

Para el análisis y gestión de riesgos se realizarán los siguientes pasos:

- 1) Criterios de evaluación

- 2) Identificación y valoración de activos críticos de la red de datos
- 3) Identificación y análisis de amenazas y vulnerabilidades
- 4) Evaluación de riesgos
- 5) Tratamiento de riesgos potenciales

2.1 Criterios de evaluación

Para el realizar el análisis de riesgos se indican los siguientes criterios de evaluación:

La valoración de los activos de acuerdo a los principios de la seguridad se realizará de manera cualitativa de acuerdo a la siguiente tabla:

Tabla 3.- Tabla de valoración de activos

VALORACIÓN	DESCRIPCIÓN
CRITICO	Una falla del activo afecta gravemente a la organización
ALTO	Una falla del activo afecta por un tiempo a la organización
MEDIO	Una falla del activo es manejable para la organización
BAJO	Una falla del activo afecta en menor grado a la organización
MUY BAJO	Una falla del activo es despreciable para la organización

El criterio de evaluación de la probabilidad de que una amenaza explote una vulnerabilidad es la siguiente:

Tabla 4.- Valoración de la probabilidad de ocurrencia de amenazas.

VALORACIÓN	DESCRIPCIÓN
5	Muy alta
4	Probable
3	Posible
2	Poco Probable
1	Muy rara vez

El criterio de evaluación del impacto o severidad cuando se materialice una amenaza es el siguiente:

Tabla 5.- Valoración del impacto de ocurrencia de amenazas

VALORACIÓN	DESCRIPCIÓN
5	Muy Alto
4	Alto
3	Medio
2	Bajo
1	Muy Bajo

Una vez que se hayan evaluado la probabilidad y el impacto de materialización de una amenaza, calcularemos el riesgo multiplicando los dos valores.

IMPACTO	RIESGO				
	5	10	15	20	25
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
	PROBABILIDAD DE OCURRENCIA				

FIGURA 2.1.- Matriz de Riesgos

Con esta matriz de riesgos se calificarán y tratarán los riesgos de acuerdo al siguiente criterio:

Tabla 6.- Criterio de tratamiento de riesgos

COLOR	CRITICIDAD	DESCRIPCIÓN
	CRITICO	Acciones inmediatas para eliminar o minimizar riesgo
	ALTO	Acciones preventivas para minimizar riesgo
	MEDIO	Riesgo aceptable
	BAJO	Riesgo despreciable

2.2 Identificación y valoración de activos críticos de la red de datos

Tomando en consideración la Figura 1.1 de este documento donde se detalla el esquema básico de un sistema SCDADA y considerando los elementos principales de una red corporativa, la cual se interconectará con la red de Control SCADA, se presenta a continuación la siguiente tabla de activos: [11]

Tabla 7.- Identificación de activos de la Red

TIPO DE RED	CATEGORÍA DEL ACTIVO	ACTIVO
RED SCADA	DATOS	Base de datos
RED SCADA	SOFTWARE	Aplicación HMI SCADA
RED SCADA	HARDWARE	MTU principal
RED SCADA	HARDWARE	Servidor Históricos

RED SCADA	HARDWARE	Equipos de campo (RTU/PLC/IED)
RED SCADA	COMUNICACIONES	Red de Control
RED CORPORATIVA	SERVICIO	INTERNET
RED CORPORATIVA	SERVICIO	Correo electrónico
RED CORPORATIVA	COMUNICACIONES	Red corporativa

Una vez identificados los activos básicos tanto de la red SCADA y la Corporativa procedemos a realizar una valoración de estos activos en base a los principios de la seguridad de la información: disponibilidad, integridad y confidencialidad.

Tabla 8.- Valoración de activos

ACTIVO	CONFIDENCIALIDAD		INTEGRIDAD		DISPONIBILIDAD	
	Valoración	Justificación	Valoración	Justificación	Valoración	Justificación
Base de datos	ALTO	Información operativa debe ser exclusiva para los operadores y funcionarios autorizados	ALTO	La integridad de los datos es vital para esta solución.	CRÍTICO	Los disponibilidad de los datos es crítico para la supervisión, monitoreo y respuesta.
Software HMI SCADA	ALTO	El software solo debe estar disponible para los usuarios autorizados con su respectivo nivel de permisos.	MEDIO	La aplicación será garantizada por el fabricante.	CRÍTICO	La aplicación debe estar disponible en las computadoras de la red de control para supervisión y monitoreo

MTU principal	MEDIO	Información operativa que no es confidencial	ALTO	Si la información no es confiable se la obtiene directo de los RTU/PLC/IED	CRÍTICO	Si la información no está disponible se la obtiene de directo de los RTU/PLC/IED
Servidor Histórico	ALTO	El acceso de usuarios no autorizados a la información histórica es grave para cualquier empresa	CRÍTICO	La información histórica es muy importante para realizar estadísticas y proyecciones de comportamiento	ALTO	Se requiere tener disponible la información actual e histórica para una toma de decisiones efectiva
Equipos de campo (RTU/PLC/IED)	CRÍTICO	El control de estos equipos puede implicar un daño o suspensión de un servicio.	CRÍTICO	Estos equipos recopilan la información que va a ser monitorizada y gestionada.	ALTO	La recolección de los datos debe estar en línea y disponible
Red de Control	MEDIO	Información operativa que no es confidencial	ALTO	Si en la red de control se compromete la integridad de la información. Esta será presentada en la sala de control.	CRÍTICO	Sin la red de control no se podría visualizar en tiempo real la información
Servicio de Internet	ALTO	El acceso de usuarios no autorizados puede comprometer a toda la red.	BAJO	La información concerniente a SCADA que se transmite por este servicio puede ser corregida	MEDIO	El servicio de Internet no es indispensable para la operación del control y monitoreo
Servicio de correo Electrónico	MAYOR	El acceso de usuarios no autorizados a este servicio puede comprometer a la red de ataques externos e	MEDIO	La información que se transmite por este medio debe ser clasificada y enviada con protección de acuerdo a su	MEDIO	La disponibilidad del correo electrónico local o externo no influye en la tarea de supervisión y control

		infecciones		nivel de criticidad.		
Red corporativa	MEDIO	Información operativa que no es confidencial	MEDIO	No aplica	MEDIO	La red corporativa debe estar disponible para actividades administrativas pero no influye en la supervisión y control

De acuerdo a esta valoración, solo los activos valorados como críticos en alguno de los principios de la seguridad son considerados para la evaluación de riesgos.

2.3 Identificación y análisis de amenazas y vulnerabilidades

Luego de haber identificado los activos y valorados en base a los principios de la seguridad, se procede a identificar las amenazas y vulnerabilidades que puedan afectar la red.

Para la identificación de vulnerabilidades se tomó en cuenta las potenciales vulnerabilidades de ICS que se encuentran en la publicación NIST 800-82, las cuales se detallan a continuación: [12]

Tabla 9.- Categorías de vulnerabilidades

GRUPOS DE VULNERABILIDADES	DE	DESCRIPCIÓN
Políticas y procedimientos de seguridad	y de	Falta de políticas y procedimientos, programas de concienciación de seguridad.
Plataforma	(software,	defectos, errores de configuración, actualización

hardware, antimalware)	y parchado de plataformas de software, aplicaciones y hardware
Configuración de redes	Malas configuraciones, arquitectura de seguridad, almacenamiento de configuraciones, claves sin cifrado y sin expiración, controles de acceso inadecuados
Equipos físicos de redes	Acceso físico no controlado a equipos, puertos, falta de protección de equipos, puntos únicos de fallas
Red perimetral	Seguridad perimetral no definida, malas configuraciones, falta de control de tráfico
Monitoreo y reporte de logs	Inadecuada configuración de logs
Comunicaciones	Falta de control de caminos, autenticación y chequeo de integridad en las comunicaciones
Redes inalámbricas	Inadecuada autenticación y protección con respecto a otra redes

Para la identificación de las posibles amenazas se escogió del listado de amenazas de la metodología Magerit, y se evaluó las potenciales amenazas que pueden explotar los grupos de vulnerabilidades ya mencionados y que se detallan a continuación:

Tabla 10.- Listado de Vulnerabilidades y Amenazas potenciales

VULNERABILIDAD	AMENAZAS
Falta de políticas, procedimientos y conciencia de seguridad	Errores de los usuarios
	Errores del administrador
	Divulgación de la información
	Fuga/robo de información
Inadecuado administración de las plataformas (vulnerabilidad, actualización , parchado de plataformas en software y hardware y protección antimalware)	vulnerabilidades de programas
	Errores de mantenimiento/actualización de sw (software)
	Difusión software dañino (malware)
	destrucción de la información
Configuración incorrecta o inadecuada de la red	Errores de configuración
	Abuso de privilegios de acceso

	Uso no previsto Acceso no autorizado Manipulación de la configuración Suplantación de identidad de usuarios Análisis de tráfico Denegación de servicios Caída del sistema por agotamiento de recursos
Falta de controles en hardware de red	Errores de mantenimiento/actualización de equipos Acceso físico no autorizado a equipos Pérdida de equipos infección de software dañino a través de puertos físicos Manipulación de equipos Condiciones inadecuadas de temperatura y humedad
Falta o inadecuada configuración de red perimetral	Errores de configuración Accesos no autorizados Análisis de tráfico Denegación de servicios Difusión software dañino (malware) Manipulación de la configuración Caída del sistema por agotamiento de recursos
Falta o inadecuada configuración de monitoreo y registro de logs	Errores de configuración Errores de monitorización Manipulación de los registros de actividad
Comunicaciones no administradas e inseguras	Acceso no autorizado Intercepción de la información
Mala configuración de Conexión de inalámbrica	Errores de la configuración Intercepción de la información Fuga de la información Suplantación de identidad de usuarios Abuso de privilegios de acceso

	Acceso no autorizado
	Uso no previsto
	Caída del sistema por agotamiento de recursos
	Denegación de servicios

2.4 Evaluación de riesgos

A continuación se muestran las evaluaciones de riesgos de cada activo crítico de acuerdo a las vulnerabilidades y amenazas identificadas:

ACTIVO: BASE DE DATOS SCADA

VULNERABILIDAD	AMENAZAS	PROBABILIDAD	IMPACTO	RIESGO
Falta de políticas, procedimientos y conciencia de seguridad	Divulgación de la información	5	3	15
	Fuga/robo de información	4	3	12
	Errores de los usuarios	3	4	12
	Errores del administrador	2	3	6
Plataforma de protección de Malware	Destrucción de la información	4	5	20
Configuración incorrecta o inadecuada de la red	Abuso de privilegios de acceso	3	5	15
	Acceso no autorizado	4	5	20
	Manipulación de la configuración	3	5	15
	Errores en la configuración	3	5	15
	Errores del administrador	2	5	10
	Suplantación de identidad de usuarios	1	5	5

Falta o inadecuada configuración de red perimetral	Accesos no autorizados	4	5	20
	Manipulación de la configuración	3	5	15
Falta o inadecuada configuración de monitoreo y registro de logs	Errores de monitorización	4	4	16
	Manipulación de los registros de actividad	3	4	12

ACTIVO: SW SCADA HMI

VULNERABILIDAD	AMENAZAS	PROBABILIDAD	IMPACTO	RIESGO
Falta de políticas, procedimientos y conciencia de seguridad	Errores de los usuarios	3	4	12
	Errores del administrador	2	5	10
	Divulgación de la información	3	4	12
	Fuga/robo de información	2	4	8
Inadecuado administración de las plataformas (vulnerabilidad, actualización , parchado de plataformas en software y hardware y protección antimalware)	vulnerabilidades de programas / S.O.	3	5	15
	Errores de mantenimiento /actualización de sw	4	5	20
	Difusión software dañino (malware)	4	5	20
	destrucción de la información	3	5	15
Configuración incorrecta o inadecuada de la red	Errores de configuración	3	4	12
	Abuso de privilegios de acceso	4	4	16
	Uso no previsto	2	3	6
	Acceso no autorizado	4	5	20
	Manipulación de la configuración	3	5	15
	Suplantación de identidad de usuarios	4	4	16

	Denegación de servicios	5	5	25
Falta o inadecuada configuración de red perimetral	Errores de configuración	3	5	15
	Accesos no autorizados	3	5	15
	Denegación de servicios	5	5	25
	Difusión software dañino (malware)	4	5	20
Falta o inadecuada configuración de monitoreo y registro de logs	Errores de monitorización	4	4	16
	Manipulación de los registros de actividad	4	4	16
Comunicaciones no administradas e inseguras	Acceso no autorizado	4	4	16
	Intercepción de la información	3	2	6
Mala configuración de Conexión de inalámbrica	Errores de la configuración	4	5	20
	Intercepción de la información	3	4	12
	Suplantación de identidad de usuarios	3	4	12
	Abuso de privilegios de acceso	4	4	16
	Acceso no autorizado	3	3	9
	Uso no previsto	3	3	9
	Denegación de servicios	3	5	15

ACTIVO: SERVIDOR MTU

VULNERABILIDAD	AMENAZAS	PROBABILIDAD	IMPACTO	RIESGO
Falta de políticas, procedimientos y conciencia de seguridad	Errores del administrador	3	5	15
Inadecuado administración de las plataformas (vulnerabilidad,	vulnerabilidades de programas / S.O	4	5	20
	Errores de mantenimiento	4	5	20

actualización , parchado de plataformas en software y hardware y protección antimalware)	/actualización de S.O			
	Difusión software dañino (malware)	5	5	25
	destrucción de la información	2	5	10
Configuración incorrecta o inadecuada de la red	Errores de configuración	3	4	12
	Abuso de privilegios de acceso	3	5	15
	Acceso no autorizado	4	5	20
	Manipulación de la configuración	3	5	15
	Suplantación de identidad de usuarios	3	5	15
	Denegación de servicios	5	5	25
	Caída del sistema por agotamiento de recursos	4	5	20
Falta de controles en hardware de red	Errores de mantenimiento /actualización de equipos	3	4	12
	Acceso físico no autorizado a equipos	3	4	12
	Pérdida de equipos	2	3	6
	infección de software dañino a través de puertos físicos	2	5	10
	Manipulación de equipos	2	4	8
	Condiciones inadecuadas de temperatura y humedad	2	4	8
Falta o inadecuada configuración de red perimetral	Errores de configuración	4	5	20
	Accesos no autorizados	4	5	20
	Denegación de servicios	5	5	25
	Difusión software	5	5	25

	dañino (malware)			
	Manipulación de la configuración	3	5	15
	Caída del sistema por agotamiento de recursos	4	5	20
Falta o inadecuada configuración de monitoreo y registro de logs	Errores de configuración	4	5	20
	Errores de monitorización	4	4	16
	Manipulación de los registros de actividad	3	4	12
Comunicaciones no administradas e inseguras	Acceso no autorizado	3	5	15
	Intercepción de la información	4	5	20
Mala configuración de Conexión de inalámbrica	Errores de la configuración	4	4	16
	Intercepción de la información	4	5	20
	Suplantación de identidad de usuarios	3	5	15
	Abuso de privilegios de acceso	4	5	20
	Acceso no autorizado	4	5	20
	Uso no previsto	3	5	15
	Caída del sistema por agotamiento de recursos	3	5	15
	Denegación de servicios	4	5	20

ACTIVO: SERVIDOR HISTÓRICOS

VULNERABILIDAD	AMENAZAS	PROBABILIDAD	IMPACTO	RIESGO
Falta de políticas, procedimientos y conciencia de seguridad	Errores del administrador	3	4	12
Inadecuado administración de las plataformas	vulnerabilidades de programas / S.O	4	5	20
	Errores de	4	5	20

(vulnerabilidad, actualización, parchado de plataformas en software y hardware y protección antimalware)	mantenimiento /actualización de S.O			
	Difusión software dañino (malware)	5	5	25
	destrucción de la información	2	5	10
Configuración incorrecta o inadecuada de la red	Errores de configuración	3	4	12
	Abuso de privilegios de acceso	3	5	15
	Acceso no autorizado	4	5	20
	Manipulación de la configuración	3	5	15
	Suplantación de identidad de usuarios	3	5	15
	Denegación de servicios	5	5	25
	Caída del sistema por agotamiento de recursos	4	5	20
Falta de controles en hardware de red	Errores de mantenimiento /actualización de equipos	3	4	12
	Acceso físico no autorizado a equipos	3	4	12
	Pérdida de equipos	1	3	3
	infección de software dañino a través de puertos físicos	2	5	10
	Manipulación de equipos	2	4	8
	Condiciones inadecuadas de temperatura y humedad	2	4	8
Falta o inadecuada configuración de red perimetral	Errores de configuración	4	5	20
	Accesos no autorizados	4	5	20
	Denegación de servicios	5	5	25

	Difusión software dañino (malware)	5	5	25
	Manipulación de la configuración	3	5	15
	Caída del sistema por agotamiento de recursos	4	5	20
Falta o inadecuada configuración de monitoreo y registro de logs	Errores de configuración	4	5	20
	Errores de monitorización	4	4	16
	Manipulación de los registros de actividad	4	4	16
Comunicaciones no administradas e inseguras	Acceso no autorizado	3	5	15
	Intercepción de la información	4	5	20
Mala configuración de Conexión de inalámbrica	Errores de la configuración	4	4	16
	Intercepción de la información	4	5	20
	Suplantación de identidad de usuarios	3	5	15
	Abuso de privilegios de acceso	4	5	20
	Acceso no autorizado	4	5	20
	Uso no previsto	3	5	15
	Caída del sistema por agotamiento de recursos	3	5	15
	Denegación de servicios	4	5	20

ACTIVO: EQUIPOS DE CAMPO: RTU/PLC/EID

VULNERABILIDAD	AMENAZAS	PROBABILIDAD	IMPACTO	RIESGO
Falta de políticas, procedimientos y conciencia de seguridad	Errores del administrador	2	4	8
Configuración incorrecta o	Errores de configuración	3	4	12

inadecuada de la red	Acceso no autorizado	4	5	20
	Manipulación de la configuración	5	5	25
	Caída del sistema por agotamiento de recursos	4	5	20
Falta de controles en hardware de red	Acceso físico no autorizado a equipos	4	4	16
	Pérdida de equipos	2	3	6
	infección de software dañino a través de puertos físicos	3	5	15
	Manipulación de equipos	2	4	8
Comunicaciones no administradas e inseguras	Acceso no autorizado	3	5	15
	Intercepción de la información	4	5	20
	Modificación deliberada de la información	3	5	15

ACTIVO: RED DE CONTROL

VULNERABILIDAD	AMENAZAS	PROBABILIDAD	IMPACTO	RIESGO
Falta de políticas, procedimientos y conciencia de seguridad	Errores del administrador	3	3	9
Configuración incorrecta o inadecuada de la red	Errores de configuración	3	4	12
	Abuso de privilegios de acceso	3	4	12
	Uso no previsto	4	5	20
	Manipulación de la configuración	3	4	12
	Suplantación de identidad de usuarios	3	4	12
	Análisis de tráfico	4	3	12
	Denegación de servicios	5	5	25

Falta de controles en hardware de red	Errores de mantenimiento /actualización de equipos	3	4	12
	Acceso físico no autorizado a equipos	3	4	12
	Pérdida de equipos	2	4	8
	Manipulación de equipos	2	4	8
	Condiciones inadecuadas de temperatura y humedad	2	4	8
Falta o inadecuada configuración de red perimetral	Errores de configuración	4	5	20
	Accesos no autorizados	3	5	15
	Análisis de tráfico	4	3	12
	Denegación de servicios	5	5	25
	Difusión software dañino (malware)	5	5	25
	Manipulación de la configuración	3	5	15
Falta o inadecuada configuración de monitoreo y registro de logs	Errores de configuración	4	4	16
	Errores de monitorización	4	4	16
	Manipulación de los registros de actividad	4	4	16
Comunicaciones no administradas e inseguras	Acceso no autorizado	3	4	12
	Intercepción de la información	4	4	16
	Fuga de información	2	4	8
Mala configuración de Conexión de inalámbrica	Errores de la configuración	4	4	16
	Intercepción de la información	3	4	12
	Fuga de la información	2	4	8
	Suplantación de identidad de usuarios	3	4	12
	Abuso de privilegios de acceso	3	4	12

Acceso no autorizado	3	4	12
Uso no previsto	4	4	16
Denegación de servicios	4	5	20

2.5 Tratamiento de riesgos potenciales

Una vez que se realizó la evaluación de riesgos de todos los equipos críticos de acuerdo a las vulnerabilidades y amenazas potenciales, procedemos a realizar el tratamiento de riesgos potenciales que fueron indicados en la tabla 6 “Criterios de tratamientos de riesgos”, en donde se definió que se tratarán los riesgos críticos (puntaje 20 y 25) y los altos (puntaje 15 y 16).

A continuación se presenta una tabla con todas las vulnerabilidades y amenazas de mayor riesgo para cada activo y los controles necesarios para mitigar o minimizar los riesgos.

Tabla 11.- Tratamientos de riesgos

VULNERABILIDAD	AMENAZAS	B.D.	SW SC HMI	SV. MTU	SV. HST.	EQ. CP.	RC	CONTROLES
Falta de políticas, procedimientos y conciencia de seguridad	Errores del administrador			15			15	Documentación de procedimientos y configuraciones de equipos
	Divulgación de la información	15						Concientización de seguridad de la información. Investigación de personal antes de la contratación.
Inadecuado administración de las plataformas (vulnerabilidad, actualización, parchado de plataformas en software y hardware y protección antimalware)	Vulnerabilidades de programas		15	20	20			Esquemas de pruebas y actualizaciones.
	Errores de mantenimiento /actualización de sw		20	20	20			Procedimientos de aplicación de parches. Ambientes de pruebas.
	Difusión software dañino (malware)		20	25	25			Implementar protección antimalware.
	destrucción de la información	20	15					Implementar políticas de respaldos y controles estrictos en la base de datos.
Configuración incorrecta o inadecuada de la red	Abuso de privilegios de acceso	15	16	15	15			Administración de roles y privilegios, acuerdos de confidencialidad
	Uso no previsto						20	Segmentación de redes, control de servicios en la red
	Acceso no autorizado	20	20	20	20	20	15	Segmentación de redes, sistema de autenticación fuerte
	Manipulación de la configuración	15	15	15	15	25		Esquemas de pruebas y control de cambios
	Suplantación de identidad de usuarios		16	15	15			Administración de roles y privilegios. Uso de políticas de claves
	Denegación de servicios		25	25	25		25	Implementación de IPS, antimalware
	Caída del sistema por agotamiento de recursos				20	20	20	
Falta de controles	Acceso físico no					16		Controles de acceso

en hardware de red	autorizado a equipos							físicos de áreas de equipos
	infección de software dañino a través de puertos físicos					15		Configuración de usos de puertos en equipos
Falta o inadecuada configuración de red perimetral	Errores de configuración		15	20	20		20	Esquemas de seguridad, mejores prácticas de configuración, entrenamiento de personal, continua gestión de riesgos.
	Accesos no autorizados	20	15	20	20			Protecciones de equipos críticos en DMZ, control de puertos y aplicaciones estrictas y necesarias
	Denegación de servicios		25	25	25		25	Implementación de IPS en zona perimetral
	Difusión software dañino (malware)		20	25	25		25	Implementación de antimalware
	Manipulación de la configuración	15		15	15		15	sistema de autenticación fuerte, monitoreo y control de logs
	Caída del sistema por agotamiento de recursos			20				Implementación de IPS, comportamientos anómalos, limitar número de conexiones posibles
Falta o inadecuada configuración de monitoreo y registro de logs	Errores de configuración			20	20		16	Implementar monitoreo y control continuo de logs en todos los activos críticos
	Errores de monitorización	16	16	16	16		16	Implementar procedimientos, alarmas en monitoreo de logs
	Manipulación de los registros de actividad		16		16		16	Implementar fuertes controles de autenticación, respaldo y almacenamiento de logs
Comunicaciones no administradas e inseguras	Acceso no autorizado			15	15	15	Implementar sistemas fuertes de autenticación y monitoreo de logs	

	Intercepción de la información			20	20	20	16	Uso de protocolos seguros.
Mala configuración de Conexión de inalámbrica	Errores de la configuración		20		16		16	Segmentación de redes, control de tráfico de puertos y servicios por la red
	Intercepción de la información				20			Uso de protocolos seguros. Cifrado de la información
	Suplantación de identidad de usuarios			15	15			Segmentación de redes. Administración de roles y privilegios. Uso de políticas de claves
	Abuso de privilegios de acceso		16	20	20			Administración de roles y privilegios
	Acceso no autorizado			20	20			Implementar sistemas fuertes de autenticación y monitoreo de logs
	Uso no previsto			15	15			Administración de roles y privilegios, control de servicios en la red
	Caída del sistema por agotamiento de recursos			15	15			Monitoreo y control de recursos de equipos
	Denegación de servicios		15	20	20		20	Control de tráfico en la red, limitar cantidad de conexiones o peticiones en la red

Nomenclatura:

BD: Base de Datos

SW SC: Software SCADA HMI

SV. MTU: Servidor MTU

SV. HST: Servidor de históricos

EQ. CP.: Equipos de Campo

RC. Red de Control

CAPÍTULO 3

DISEÑO DE LA SEGURIDAD EN LA RED

3.1 Seguridad Lógica

En base al cuadro de tratamiento de los principales riesgos encontrados y considerando las diferentes recomendaciones para la seguridad de los sistemas SCADA, se han considerado los siguientes componentes en la seguridad lógica.

3.1.1 Esquema de seguridad lógica general de la red de datos

A continuación se listan los requerimientos para el diseño de la red en base a los controles para minimizar los riesgos: [1] [2] [12] [13] [14] [15]

- 1) Separar las redes de control con las demás redes a través de una zona desmilitarizada (DMZ).
- 2) Solo la red corporativa tendrá acceso a internet, correo electrónico y otros servicios corporativos.
- 3) Los servidores de la red corporativa deben estar separados de los servidores de la red de control.
- 4) Se debe controlar el flujo de datos (puertos de servicios y aplicaciones) sobre la red de control.
- 5) Se debe implementar un sistema de protección de antivirus y parchado para todos los equipos de la red.
- 6) La red corporativa debe tener segmentación de redes (VLANs), sobre todo para implementación de la red Wireless, la cual debe estar controlada por ambos firewall para que solo pueda acceder a internet y a equipos específicos.
- 7) La red corporativa debe tener acceso al servidor de históricos con el fin de visualizar y generar reportes estadísticos que serán analizados o serán insumos de otros sistemas de análisis y tratamiento de la información.
- 8) Se debe implementar una adecuada gestión de monitoreo y análisis de logs de todos los equipos de la red.

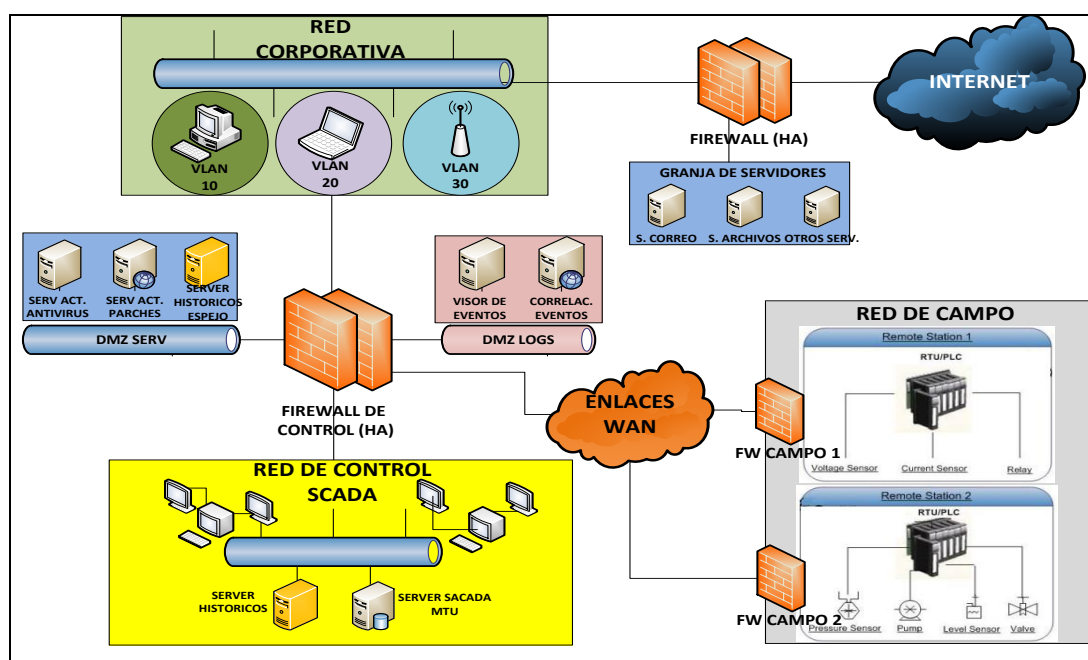


FIGURA 3.1.- Esquema de seguridad lógica general de la red

Con esta arquitectura de red cada equipo tendrá las siguientes funciones:

- El primer firewall perimetral controlará todo el acceso de Internet de la red y adicionalmente controlará el tráfico de servidores que estarán en una DMZ y servirán exclusivamente para la red corporativa. Este firewall debe tener la capacidad de trabajar como IPS, antimalware, anti spam y control de contenido web para toda la red.
- El segundo firewall (de control) segmentará las redes de corporativas, de control, de campo, una DMZ adicional para colocar los servidores de actualización de antivirus y parchado y otra DMZ para colocar un sistema de monitoreo y almacenamiento de logs. Este equipo tendrá el rol de controlar los accesos de la red corporativa a la red de control de

acuerdo a lo establecido en una política de seguridad (como el acceso al servidor histórico espejo), así como las conexiones entre los equipos de la red corporativa y de control hacia los servidores de antivirus y parchado y el tráfico de la red de campo hacia la red de control.

- El firewall de control tendrá la capacidad de trabajar como IPS y antimalware con el fin de monitorear y actuar en caso de anomalías respecto a las reglas de tráfico establecidas en cada interfaz.
- Los enlaces WAN que conectan la red de campo con la red del centro de control deben ser configurados utilizando protocolos seguros como VPN IP SEC, así mismo se requiere un equipo concentrador de todos los enlaces y un switch de capa 2 con manejo de VLANs para la interconexión en alta disponibilidad hacia los dos firewall de control.

3.1.2 Esquema de las redes corporativas y de control

Para las redes de control y corporativa se contempla un esquema de alta disponibilidad de equipos de redes como se aprecia en el siguiente gráfico.

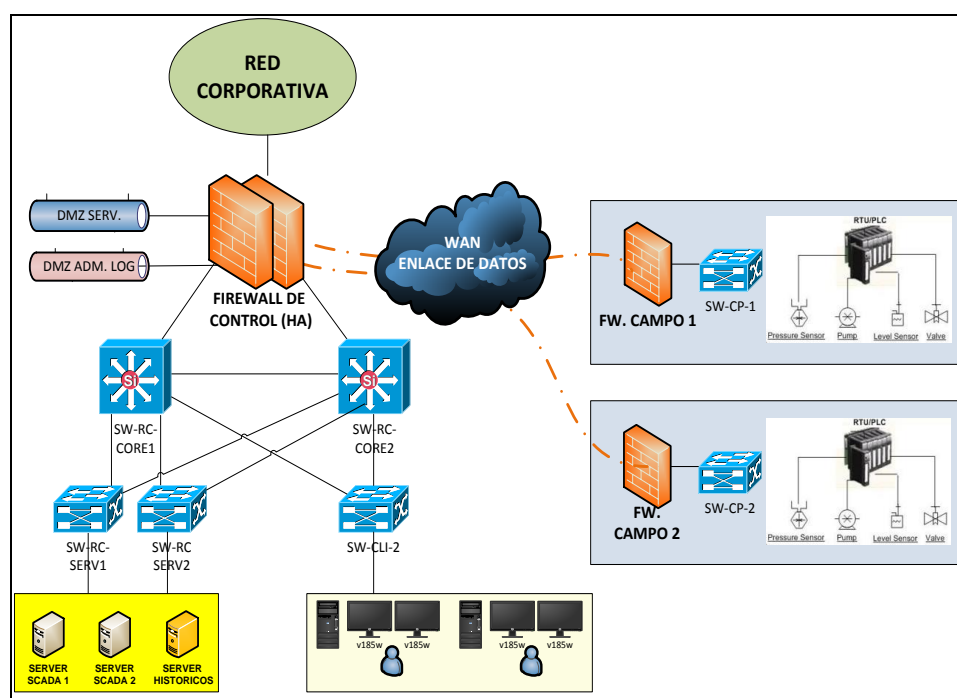


FIGURA 3.2.- Esquema de red de Control

En este esquema podemos observar también un diseño de alta disponibilidad en la red de servidores, contemplando 2 servidores principales en configuración de clúster y también la configuración del servidor de históricos con un clúster en la dmz del firewall de control.

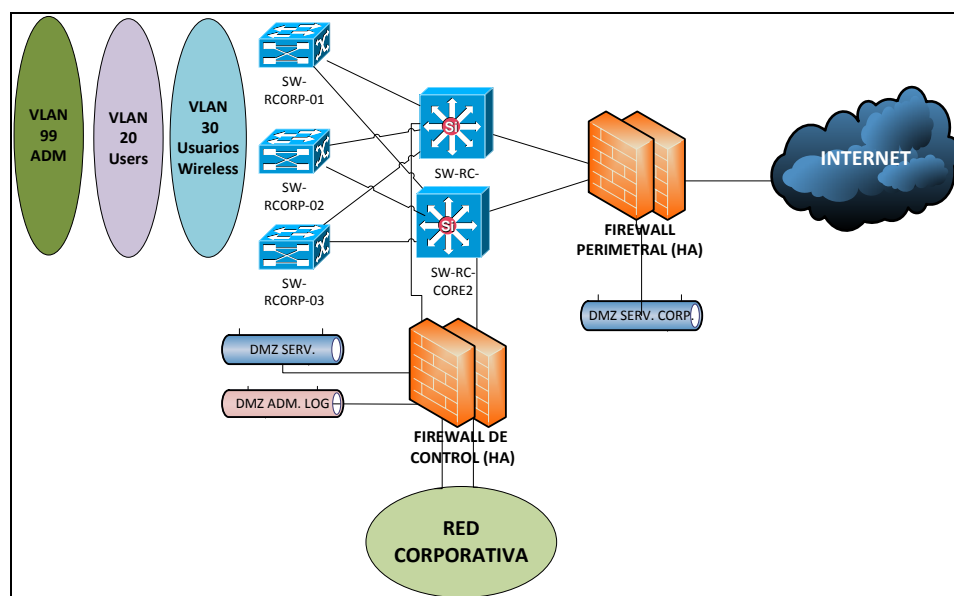


FIGURA 3.3.- Esquema de red corporativa

En este esquema de red se observa también un esquema de alta disponibilidad en los equipos de red core y distribución, así como la implementación de VLANs para segmentación de la red y configuraciones de control adecuados.

3.1.3 Almacenamiento y respaldo de la información

Es muy importante tener el almacenamiento y respaldo adecuado de la base de datos del servidor de históricos, ya que se tiene dos servidores históricos se debe adquirir un sistema de almacenamiento en cinta considerando una adecuada frecuencia de almacenamiento.

3.1.4 Control de accesos lógicos

Toda la red debe basarse en roles y privilegios, por lo cual todo acceso a equipos de redes, servidores y computadores de usuarios debe autenticarse con credenciales de menor privilegio y solo si se requiere una configuración avanzada deberá autenticarse con una clave de mayor privilegio. Se debe asignar y gestionar continuamente los perfiles de usuarios a través de una política donde se incluya, la creación, cambio y eliminación de perfiles y credenciales de usuarios.

La gestión de credenciales de usuarios debe formar parte de una política de seguridad y debe contener por lo siguiente:

- Se requieren contraseñas mayores a 8 dígitos, inclusión de letras, números y por lo menos 1 signo.
- No se debe utilizar la misma contraseña para diferentes equipos.
- Las contraseñas deben cambiarse con una frecuencia de 6 meses y no se debe permitir el uso de las 10 últimas claves utilizadas.
- Se debe configurar un bloqueo de 2 minutos de la cuenta por 3 intentos fallidos de contraseña.
- Las sesiones de los usuarios permitirán un tiempo de inactividad de 5 minutos, luego de este tiempo todos los sistemas y acceso deben bloquearse y obligar nuevamente el ingreso de las credenciales.

3.1.5 Protección contra código malicioso

Con el fin de proteger a las redes de control y corporativa de código malicioso se debe adquirir un software de antivirus corporativo con un esquema de actualizaciones centralizada, así como la implementación de un servicio de actualizaciones de sistemas operativos (parches). Para ambos servicios de actualizaciones centralizadas se ha contemplado una DMZ en el firewall de control con el fin de que solo estos servidores puedan acceder al internet y los equipos de la red de control.

Así mismo conociendo la criticidad de la red de control y el software HMI SCADA que utiliza, se pueden presentar incompatibilidades del software HMI con las actualizaciones de parches y antivirus, por lo cual es necesario realizar un procedimiento de pruebas antes ponerlos en producción para detectar posibles anomalías.

3.2 Seguridad física

En base a tabla de riesgos del anterior capítulo se observan que los principales riesgos en cuanto a la seguridad física son el acceso físico no autorizado a equipos y la infección de software dañino a través de puertos físicos, por lo cual se ha considerado como diseño de la seguridad física los siguientes aspectos.

3.2.1 Áreas seguras

Con el fin de evitar el acceso no autorizado de personal a zonas donde se encuentran los equipos de la red se deben realizar las siguientes indicaciones:

- 1) En el edificio del centro de control se deben implementar por lo menos dos zonas de control, una a la entrada del edificio con la presencia de un guardia y un sistema electrónico de acceso como tarjetas magnéticas y otra para el datacenter con sistema de control de acceso. Todo el edificio debe contar con cámaras de seguridad.
- 2) En el cuarto de servidores se debe separar un área de acceso para proveedores y otro de servidores y equipos críticos del SCADA.
- 3) En los lugares remotos donde hay equipos electrónicos y mecánicos debe haber una zona de seguridad con un guardia y sistema de vigilancia.

3.2.2 Seguridad de los equipos

1) ***Ubicación y protección de los equipos.***

Todos los equipos deberán ser ubicados en lugares adecuados donde no puedan ser afectados por amenazas físicas y ambientales como manipulación, robo, polvo, lluvia, etc. Los equipos que no pueden ser instalados en el cuarto de control deberán tener una protección adecuada para que no puedan ser manipulados o robados

fácilmente. Se debe mantener y actualizar un inventario de todos los equipos.

Inhabilitar los puertos externos de los equipos de cómputo para la red de Control como puertos USB, CD, diskettes, etc.

2) *Suministro eléctrico*

Todos los equipos deben contar con una adecuada protección eléctrica como fuentes de poder redundantes, sistemas de UPS redundantes y autonomía adecuada para el correcto apagado de todos los equipos. Los equipos de la red de control deberán tener un sistema de protección eléctrica independiente.

3) *Seguridad del cableado*

El cableado estructurado debe cumplir los estándares respectivos para evitar daños físicos y manipulación de los mismos.

Con el fin de tener una separación adecuada de la red de control con la red corporativa se deberá tener separado el cableado estructurado de ambas redes, con el fin de que el acceso al cableado de la red de control tengo un control sumamente estricto.

4) *Mantenimiento de equipos*

Se debe contar con un plan de mantenimiento preventivo de todos los equipos de la red de control y corporativa por separado, así como llevar una administración adecuado de los daños y fallas ocurridos.

3.3 Monitoreo y gestión de logs

Toda la arquitectura de red propuesta permite minimizar las amenazas analizadas en este documento, sin embargo hay un continuo crecimiento de las amenazas y ataques externos que intentarán comprometer y romper todas las barreras implementadas. Así mismo existe un alto riesgo de amenazas internas que puede comprometer la seguridad de toda la red.

Para ambos casos se requiere un continuo monitoreo y gestión de logs efectivos, con el fin de verificar los intentos de violaciones de seguridad y tomar acciones preventivas; y también el de poder identificar si la red ya ha sido comprometida y poder contar con registros y evidencia de los ataques.

Por lo expuesto se requiere implementar una política y procedimiento para el almacenamiento y gestión centralizado de logs de todos los equipos de redes, servidores y equipos de cómputo de sistema SCADA, considerando el tiempo máximo de almacenamientos, configuración de alarmas y periodicidad de generación de reportes.

Para el monitoreo y gestión centralizado de logs se debe contemplar un esquema de servidores recolectores de información de la diferentes procedencias (equipos de redes, servidores, base de datos) y un software que permita visualizar de manera gráfica los eventos y pueda realizar análisis estadísticos de los datos recolectados.

[16]

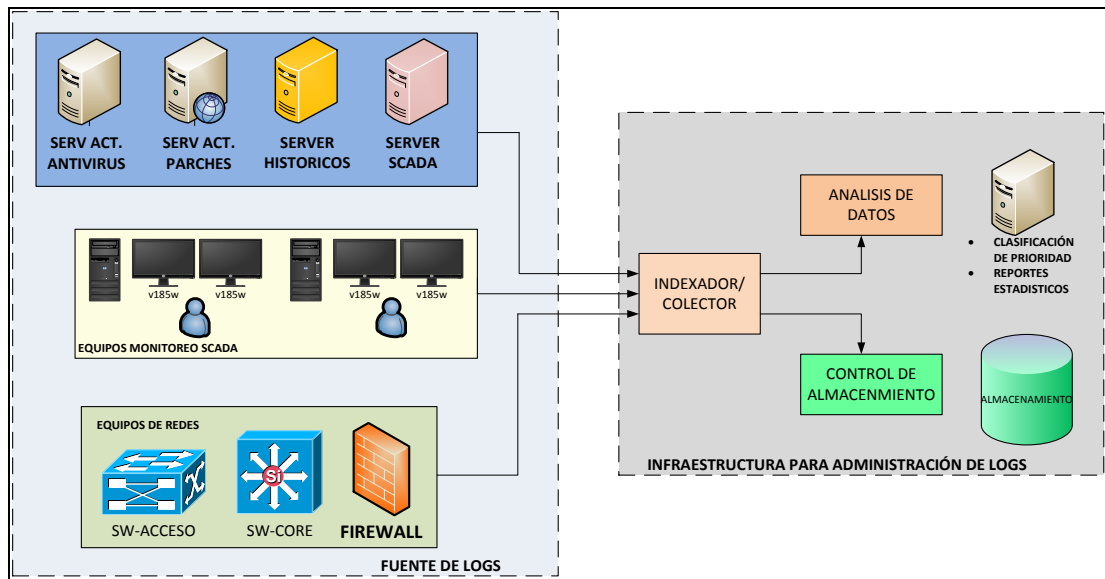


FIGURA 3.4.- Esquema de Gestión centralizada de logs

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

Del análisis de riesgo realizado y la arquitectura de red propuesta se concluye lo siguiente:

1. La arquitectura propuesta permite una minimizar los principales riesgos encontrados en el capítulo de análisis y gestión de riesgos, ya que al tener una separación de las redes de control, corporativa, enlaces WAN y el internet se podrá controlar y configurar el tráfico necesario que debe circular en cada una de estas redes, dando la mayor criticidad a la red de control.
2. Para que un atacante externo puede acceder a la red de control deberá primero cruzar los dos firewall y llegar primero a los servidores de actualizaciones y parchados o acceder a un equipo de la red corporativa que pueda acceder al servidor de históricos. Con lo cual los servidores indicados se vuelven puntos críticos y deben tener un monitoreo y control permanente.

3. Los protocolos usados por los equipos de campo, no brindan mayor seguridad o cifrado de la información, por lo cual una estrategia clave es la seguridad física de estos equipos y el aislamiento total de acceso por la red. En el diseño de la red se propone la instalación de firewalls en los puntos remotos para realizar enlaces VPN con protocolo IP sec hacia el centro de control y monitoreo, minimizando la probabilidad de que la información sea interceptada.
4. Toda la arquitectura propuesta debe formar parte de una política de seguridad de la información, que es el pilar fundamental para una buena de gestión de la seguridad y que permitirá mantener, monitorear y responder a incidentes de seguridad que se produzcan en la empresa de manera inintencionada o deliberada.
5. Una red Wireless mal configurada es siempre una gran amenaza a la seguridad en cualquier red de datos, ya que con el afán de brindar los permisos de servicios a los clientes Wireless muchas veces los técnicos de TI olvidan o cometen errores de configuraciones de seguridad. En este diseño se considera una red Wireless dentro de la red corporativa en un VLAN específica para identificar y separar esta red de las demás, así como el control de permisos y accesos respectivos desde el firewall perimetral y de control.

RECOMENDACIONES

Se detallan las siguientes recomendaciones que complementan la seguridad de la información en las redes SCADA y están fuera del alcance de este documento:

1. Se recomienda que los operadores tengan su equipo de la red de control y otro equipo que pertenezca a la red corporativa, con la cual tendrá acceso a internet y correo electrónico para facilitar sus funciones.
2. Una buena gestión de seguridad requiere de una continua gestión de riesgos, por lo cual se recomienda contar con un equipo de trabajo que evalúe los riesgos de seguridad de manera periódica con una frecuencia mínima de 6 meses o cuando suceda un severo incidente de seguridad, cambio o adición de servicio que requiera la empresa implementar en la red.
3. Se recomienda la compra e implementación de un sistema centralizado de logs con el esquema propuesto que permita almacenar y realizar análisis estadísticos de los logs y almacenamiento de versiones de configuraciones o implementar una solución de software libre.
4. Con el fin de concientizar a todos los usuarios sobre las amenazas y riesgos de la seguridad se recomienda implementar un programa de capacitación semestral o anual para todos los usuarios, además de comunicarles de manera escrita junto con las políticas generales de la empresa al inicio de las contrataciones de personal y de manera periódica.

5. Toda la arquitectura propuesta tiene el fin de minimizar los riesgos potenciales analizados, sin embargo no elimina totalmente la probabilidad de que se realice un ataque, por lo cual se recomienda tener un plan de contingencias adecuado y un plan de continuidad del negocio, para minimizar el impacto de un incidente de seguridad y se pueda restablecer toda la red en el menor tiempo posible.
6. Se recomienda realizar auditorías periódicas de seguridad para confirmar el estado y cumplimiento de políticas implementadas y análisis de incidentes registrados.
7. Si se dese implementar una solución de acceso remoto a la red SCADA debe primero realizar un análisis de riesgos adecuado para luego considerar el mejor mecanismo de seguridad apropiado que por lo menos tenga dos niveles de credenciales.
8. Los sistemas SCADA solo realizan la tarea de control, supervisión y monitoreo de los datos recolectados y no incluyen herramientas de análisis de datos, proyecciones o tendencias, por lo cual es común que se incluyan otros sistemas que realicen esta tareas, para ello se recomienda realizar esquemas seguros de extracción de datos del servidor de históricos espejo, con el fin de asegurar la integridad de la información del servidor de históricos principal.

BIBLIOGRAFÍA

- [1] Instituto Nacional de las Tecnologías de la comunicación INTECO, Estudio sobre la seguridad de los sistemas de monitorización y control de procesos e infraestructuras (SCADA), fecha de publicación marzo 2012.
- [2] Centro Criptológico Nacional CCN, GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-480) SEGURIDAD EN SISTEMAS SCADA, <https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/215-ccn-stic-480c-seguridad-en-sistemas-scada-implementar-una-arquitectura-segura/file.html>, fecha de publicación marzo 2010.
- [3] Urtiaga Javier, Duperier Luis, Gestión de la seguridad en redes de control y sistemas SCADA, <http://www.redseguridad.com/opinion/articulos/gestion-de-la-seguridad-en-redes-de-control-y-sistemas-scada>, fecha de consulta 29 de noviembre.
- [4] Carolina Lagos, Comité de Automatización y Control Industrial de la AIE, Protocolos de Comunicación Industrial, fecha de consulta 02 de enero 2016.

[5] César Fernández Lorenzana, S21Sec Labs, Protocolos SCADA y seguridad, <http://blog.s21sec.com/2008/12/protocolos-scada-y-seguridad.html>, fecha de consulta 02 de enero 2016.

[6] WIKIPEDIA, STUXNET, <https://es.wikipedia.org/wiki/Stuxnet>, fecha de consulta 21 de diciembre 2015.

[7] CHANNELBIZ, Anatomía de los ataques a sistemas SCADA, <http://www.channelbiz.es/2015/06/17/anatomia-de-los-ataques-a-sistemas-scada/>, fecha de consulta 21 de diciembre 2015.

[8] Intel Security, Inc., Global Energy Industry Hit In “Night Dragon” Attacks by George Kurtz, <https://blogs.mcafee.com/business/global-energy-industry-hit-in-night-dragon-attacks/>, fecha de publicación 09 Febrero de 2011.

[9] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), NCCIC/ICS-CERT Monitor for January-April 2014, <https://ics-cert.us-cert.gov/monitors/ICS-MM201404>, fecha de consulta 21 de diciembre 2015.

[10] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), NCCIC/ICS-CERT Monitor September 2014-February 2015, <https://ics-cert.us-cert.gov/monitors/ICS-MM201502>, fecha de consulta 21 de diciembre 2015.

[11] Gobierno de España, Ministerio de Hacienda y Administraciones Públicas, MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos, Ministerio de Hacienda y Administraciones Públicas, fecha de publicación octubre 2012

[12] NIST. National Institute of Standard and Technology, Keith Stouffer, Joe Falco, Karen Kent , Special publication 800-82 “Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security”, fecha de publicación septiembre 2006.

[13] CPNI Centre for the Protection National Infrastructure, SECURING THE MOVE TO IP-BASED SCADA/PLC NETWORKS, www.cpni.gov.uk/documents/publications/2011/2011035-securing-move-to-ip-based-networks.pdf?epslanguage=en-gb, fecha de publicación noviembre 2011.

[14] CNPI Center for the Protection of National Infrastructure, Good Practice Guide: PROCESS CONTROL AND SCADA SECURITY, http://www.cpni.gov.uk/documents/publications/2008/2008031-gpg_scada_security_good_practice.pdf, fecha de consulta 05 de diciembre 2015.

[15] CNPI Center for the Protection of National Infrastructure, Process Control and SCADA Security Guide 2: Implement Secure Architecture, www.cpni.gov.uk/documents/publications/2008/2008025gpg_scada_implement_secure_architecture.pdf, fecha de consulta 5 de diciembre 2015.

[16] Manuel Vieda, Administración de logs, <http://manuelvieda.com/2013/07/administracion-de-logs/>, fecha de consulta 02 de enero 2016