

UNIVERSIDAD ABIERTA INTERAMERICA



**La Seguridad de la Información en los
Sistemas SCADA tras su Integración
con los Sistemas de Gestión**

Tutor: Jorge Kamlofsky

Tesista: Hernán Bottinelli

Trabajo Final de carrera presentado para obtener el título
de Licenciado en Gestión de Tecnología Informática

Marzo 2021

Resumen

La producción de bienes a gran escala se automatiza mediante los sistemas de control, que conectados entre sí, conforman las redes de industria operacional, denominadas tecnologías de la operación (OT). En cambio para procesar los datos y la información, se conforman las redes de computadoras interconectadas donde se trabaja sobre tecnologías digitales. Por ello se las denomina, tecnologías de la información (IT).

Ambas tecnologías son notoriamente diferentes, así como sus prioridades: mientras que en el mundo OT es fundamental la disponibilidad para mantener la continuidad de la producción, en el mundo IT importa más la confidencialidad y la integridad de los datos.

Muchas organizaciones para control de la información utilizan los sistemas de gestión, denominados ERP. Y para supervisar las redes industriales utilizan equipos con software gráfico, llamados SCADA.

En el presente trabajo final se investigó cómo la convergencia de OT e IT beneficia la sinergia de las infraestructuras, incorporando agilidad en los procesos industriales aunque considerando el uso sensible de la información.

Las redes integradas son parte de una nueva revolución industrial o industria 4.0, donde se fusionan tecnologías físicas y digitales, permitiendo el diálogo entre las redes SCADA y los sistemas ERP.

Se analizaron experimentalmente casos de convergencia, evidenciándose vulnerabilidades ocasionadas, donde se verificó la importancia de contar con auténticas políticas de seguridad informática aplicadas dentro de la industria 4.0.

Esta investigación permitió demostrar que aplicar políticas poco robustas y controles no eficientes puede exponer la infraestructura crítica e información confidencial a potenciales vulnerabilidades y ciberataques. De concretarse un incidente de ciberseguridad podría alterar el funcionamiento de la industria, llegando a ocasionar desastres naturales y sociales para una nación que podrían evitarse.

Palabras clave: ciberataques, convergencia it, convergencia ot, infraestructuras críticas, redes scada, seguridad informática, sistemas erp

Abstract

Large-scale production of goods is automated through control systems, which, connected to each other, make up the operational industry networks, called operation technologies (OT). Instead, to process data and information, interconnected computer networks are formed where work is done on digital technologies. For this reason they are called, information technology (IT).

The two technologies are notoriously different, as well as their priorities: while in the OT world availability is essential to maintain production continuity, in the IT world data confidentiality and integrity matters more.

Many organizations for information control use management systems, called ERP. And to supervise industrial networks they use equipment with graphical software, called SCADA.

In the present final work, it was investigated how the convergence of OT and IT benefits the synergy of infrastructures, incorporating agility in industrial processes while considering the sensitive use of information.

Integrated networks are part of a new industrial revolution or industry 4.0, where physical and digital technologies merge, allowing dialogue between SCADA networks and ERP systems.

Convergence cases were experimentally analyzed, showing vulnerabilities caused, where the importance of having authentic IT security policies applied within Industry 4.0 was verified.

This research demonstrated that applying weak policies and inefficient controls can expose critical infrastructure and confidential information to potential vulnerabilities and cyberattacks. If a cybersecurity incident occurs, it could alter the operation of the industry, causing natural and social disasters for a nation that could be avoided.

Keywords: computer security, critical infrastructures, cyberattacks, erp systems, it convergence, ot convergence, scada networks

Acrónimos

DEV (Development System)

ERP (Enterprise Resource Planning)

GRC (Governance Risk Compliance)

HMI (Human Machine Interface)

ICS (Industrial Control System)

IP (Internet Protocol)

IOT (Internet of things)

IIOT (Industrial Internet of Things)

ISACA (Information Systems Audit and Control Association)

IT (Information Technology)

LAN (Local Area Network)

MES (Manufacturing Execution System)

MTBF (Medium Time Between Faults)

OMS (Organismo Mundial de la Salud)

OT (Operational Technology)

PLC (Programmable Logic Controller)

PRD (Productive System)

QAS (Quality Access Control)

RISI (Repository of Industrial Security Incidents)

RTU (Remote Terminal Unit)

SAP (System Application Products)

SCADA (Supervisory Control And Data Acquisition)

SGSI (Sistemas de Gestión de Seguridad de la Información)

SI (Seguridad Informática)

SOA (Service Oriented Architecture)

SOD (Segregation of Duties)

TCP (Transmission Control Protocol)

TDMS (Test Data Migration Server)

VPN (Virtual Private Network)

Dedicatoria

La dedicatoria es a quienes contribuyeron con ideas y fueron pilares para el desarrollo de la investigación para presentación de la Tesis Final y alcanzar el título de Licenciado en Gestión y Tecnología Informática en la Universidad Abierta Interamericana.

Quiero realizar una mención especial al equipo de Ingeniería de la firma ALLTERM por su enorme compromiso y dedicación y el hecho de conversar sobre su experiencia en implementaciones de equipos electrónicos con automatización industrial. La explicación consistió en detallar sus trabajos realizados e implementaciones vigentes en distintas fábricas del rubro textil industrial. Entre otras empresas nos contaron los casos de las firmas Mafissa, Rhodia y Dupont.

Agradecimientos

Se agradece a todas las personas que fueron partícipes de este proceso, ya sea de forma directa o indirecta, confiaron e hicieron posible el desarrollo de la Tesis de Investigación.

También quiero destacar el enorme compromiso y esfuerzo de mis padres, Mirta y Ricardo por la educación brindada, a mi hermano Leandro por el apoyo incondicional, a mis sobrinos Pedro y Lucas por el cariño mutuo y el gran aporte y experiencia del Ingeniero Sergio Martínez.

Gracias a la UAI (Universidad Abierta Interamericana), al equipo de profesionales, docentes e investigadores del CAETI y una gran mención por su dedicación a Marcela Samela, docente universitaria y Jorge Kamlofsky, tutor de Tesis, quienes fueron los que me guiaron y acompañaron a lo largo del proyecto con gran dedicación y constancia para el alcance de la investigación.

Por último, a mis compañeros de estudio, colegas de trabajo, amistades y familiares, a todos ellos, “gracias totales”.

Indice

Resumen.....	2
Abstract	4
Acrónimos	6
Dedicatoria	8
Agradecimientos	9
Indice.....	10
Índice de figuras.....	14
Índice de tablas.....	16
1. Introducción	17
1.1. Trabajos relacionados.....	17
1.2. Alcance de la investigación.....	18
1.3. Propuesta de trabajo	18
1.4. Objetivo principal.....	19
1.4.1. Objetivos específicos	19
1.5. Justificación del tema	20
1.6. Enfoque metodológico	20
1.7. Contribuciones principales.....	20
2. Marco Teórico.....	22
2.1. Sistemas industriales	22
2.1.1. Visión de la industria 4.0	22
2.1.2. Niveles de automatismo	23
2.1.3. Tecnologías big data	24
2.2. Redes SCADA.....	25

2.2.1.	Infraestructuras críticas	27
2.2.2.	Priorización de redes	28
2.3.	Sistemas ERP	29
2.3.1.	Ventajas de los ERP	30
2.3.2.	Los ERP en las industrias.....	31
2.4.	Seguridad informática.....	32
2.4.1.	Consideraciones en seguridad IT / OT.....	33
2.4.2.	Gestión de la seguridad	34
2.4.3.	Cumplimiento y normas de seguridad.....	35
2.4.4.	Organizaciones y normativas	36
2.4.5.	Buenas prácticas de seguridad	37
2.5.	Ciberseguridad.....	37
2.5.1.	Tipos de ciberataques.....	38
2.5.2.	Malware Stuxnet	39
2.5.3.	Covid-19.....	39
3.	Desarrollo Técnico.....	41
3.1.	Planteo del problema	41
3.2.	Hipótesis de la investigación.....	42
3.3.	Convergencia.....	42
3.3.1.	Redes OT.....	43
3.3.2.	Oposición al cambio.....	43
3.3.3.	Amenazas de riesgo.....	45
3.4.	Riesgos en ERP	46
3.4.1.	Control interno	47
3.4.2.	Matriz de riesgos	47

3.4.3.	Accesos críticos.....	49
3.5.	Seguridad en ERP.....	50
3.5.1.	Controles y auditorías	51
3.5.2.	Aspectos de la seguridad.....	52
3.5.3.	Políticas de prevención	53
3.6.	Vulnerabilidades.....	54
3.6.1.	Análisis de incidentes.....	55
3.6.2.	Simulación ERP	55
4.	Datos Experimentales	57
4.1.	Presentación.....	57
4.2.	Preparación de servidor	57
4.2.1.	Especificaciones.....	57
4.2.2.	Configuración de firewall	58
4.2.3.	Administración de usuarios.....	58
4.3.	Requisitos y componentes	59
4.3.1.	Plataforma java.....	59
4.3.2.	SQL server.....	60
4.4.	Restore ERP	62
4.4.1.	Pre-requisitos	62
4.4.2.	Inicio de instalación	63
4.4.3.	Actualización kernel.....	68
4.4.4.	Finalización de instalación.....	68
4.5.	Post - instalación	69
4.6.	Detalle teórico matriz SoD	69
4.7.	Resultados y hallazgos	71

Conclusiones	73
Líneas Futuras de Investigación.....	74
Bibliografía	75

Índice de figuras

Figura 1. Industria 4.0 - Niveles de automatismo	23
Figura 2. Esquema redes SCADA.....	27
Figura 3. Centro de monitoreo SCADA.....	29
Figura 4. ERP en las industrias	31
Figura 5. Configuración host virtual	57
Figura 6. Especificaciones del servidor	58
Figura 7. Configuración firewall.....	58
Figura 8. Administración de usuarios	58
Figura 9. Variable de entorno.....	59
Figura 10. Sistema de variable	59
Figura 11. Java version	60
Figura 12. Instalar DB SQL	60
Figura 13. Confirmación de instalación	61
Figura 14. Instalación en curso	61
Figura 15. Instalación SQL completada.....	61
Figura 16. Chequeo pre-requisitos	62
Figura 17. Progreso de ejecución	62
Figura 18. Iniciar instalación.....	63
Figura 19. Nota de instalación	63
Figura 20. Parámetros SID.....	64
Figura 21. Claves maestras	64
Figura 22. Copias homogéneas	64
Figura 23. Conexión de base de datos.....	64

Figura 24. Esquema base de datos	65
Figura 25. Número de instancia	65
Figura 26. Instancia / parámetros	65
Figura 27. SAPCryptolib.....	66
Figura 28. Usuario de sistema.....	66
Figura 29. Cryptographic	66
Figura 30. Progreso de instalación.....	67
Figura 31. Opciones de instalación	67
Figura 32. Kernel	68
Figura 33. Instalación completa	68

Índice de tablas

Tabla 1. Matriz de riesgos SoD.....	48
Tabla 2. Detalle de SoD	70

1. Introducción

La gestión de la ciberseguridad en redes SCADA integradas con sistemas ERP es muy sensible y delicada de afrontar ya que son tecnologías con distinto nivel de prioridades.

Los motivos de la formación de software para control, supervisión y adquisición de datos en la industria, en convivencia con tecnologías de sistemas de gestión, deben contar con verdaderas políticas de seguridad.

En los sistemas de gestión, se prioriza la protección de la información, deteniendo la operación si el sistema no está disponible, en cambio en los sistemas de control industrial, se tiene como prioridad, la continuidad de la producción y seguridad de las personas. Que el sistema no esté disponible puede significar desde fallas en productos o instalaciones hasta un peligro para las personas y su entorno.

Con el crecimiento de las amenazas informáticas, los hackers disponen de nuevos objetivos en centros operativos de las organizaciones, apuntando a los sistemas de información y amenazando a las redes industriales con posibles ciberataques.

Se propone en este trabajo, profundizar el estudio de la ciberseguridad, enfocándose en la identificación y protección de servicios complejos que son críticos en la integración entre las redes industriales y las redes corporativas. En especial, en la conexión entre redes SCADA y sistemas ERP.

1.1. Trabajos relacionados

- Convergencia de redes IT y OT. (Secure, 2019)
- Ciberseguridad SCADA y ERP. (García, 2019)
- Estado del arte de sistemas ERP. (Masoero, 2015)
- Un enfoque para disminuir los efectos de los ciberataques a las infraestructuras críticas. (Kamlofsky, 2015)

1.2. Alcance de la investigación

La siguiente investigación fue seleccionada debido al incremento de ciberataques en áreas industriales que ocurren cuando no se aplican correctamente los controles en el uso de tecnologías de la información integrados con las redes OT.

En este trabajo se analizan experimentalmente algunos casos de integración entre sistemas SCADA con sistemas de gestión, donde se evidencian vulnerabilidades ocasionadas.

Para ejemplificar se cita un caso de automatización industrial, donde se conectaron equipos PLC (programmable logic controller), distribuidos a lo largo de una máquina textil, donde se deseaba monitorear los distintos valores de variables y poder ser controlados para el correcto funcionamiento de la línea de producción.

Estos equipos fueron contruidos específicamente para cada aplicación de uso donde la comunicación se realizaba a través de líneas de transmisión RS-485 con protocolo MODBUS de comunicación basada en arquitectura RTU. Estos PLC se encargaban de controlar distintas variables (temperatura, presión, caudal y tiempos de producción). El servidor interrogaba a los PLC de manera secuencial consultando el estado de cada variable, y verificando que los valores fueran correctos y en caso contrario, se reconfiguraban los que fueran necesarios.

La red industrial OT se conectaba a la misma red de datos IT, donde se utilizaban las mismas políticas de seguridad y donde operaba el sistema ERP con los de la SCADA.

El motivo y tendencia de conexión de las redes OT a internet es para obtener datos en tiempo real, contar con monitoreo y mejorar la planificación de mantenimientos predictivos, aunque no siempre focalizándose en la protección de las redes industriales.

1.3. Propuesta de trabajo

En este trabajo se explica la convergencia entre los sistemas ERP y redes SCADA.

Para la implantación del software de control, supervisión y adquisición de datos en la industria, en convivencia con tecnologías de información de sistemas de gestión, es fundamental contar con verdaderas políticas de seguridad informática.

Para la aplicación de dichas políticas, se debe validar y verificar entre el control interno y auditoría para que seguridad informática tomando las normativas vigentes, pueda implementarlas.

Una de las ventajas de este esquema, es que a través de la integración de redes, se puede controlar el proceso de forma automática y sin la necesidad de estar frente la maquina industrial con operación asistida.

Se detallan todas las prestaciones y requisitos necesarios para lograr el máximo beneficio de un sistema de OT. Se especifica la estructura interna, así como sus componentes básicos que permiten las actividades de supervisión y adquisición de datos. Estos componentes permiten una comunicación entre distintas aplicaciones, como ser las bases de datos, las aplicaciones, herramientas de métricas y de gestión.

El presente trabajo tiene como objetivo investigar las relaciones de analogía involucradas en el tratamiento de la información que maneja los sistemas SCADA con los sistemas de gestión.

Si bien el reto en ciberseguridad es complejo, las ventajas en el marco son mucho mayores, y es necesario aplicar una metodología capaz de fortalecer las redes industriales sin entorpecer la eficiencia de los nuevos medios de producción.

1.4. Objetivo principal

El objetivo de la tesis es investigar los problemas de seguridad de la información en la convergencia de las redes SCADA y los sistemas ERP.

1.4.1. Objetivos específicos

Profundizar el estudio de la ciberseguridad, enfocándose en la identificación de servicios críticos de las redes industriales para la correcta conexión con los sistemas de gestión de ERP.

Presentar las vulnerabilidades que surgen de la convergencia entre sistemas IT / OT.

Proponer enfoques para solucionar las vulnerabilidades presentadas.

1.5. Justificación del tema

El tema propuesto como tesis final de investigación fue elegido en función a la combinación de las diversas tecnologías de la información y las amenazas que presentan el hecho de conectar las redes SCADA a internet para integrarse con los sistemas ERP.

En las telecomunicaciones se utilizan tecnologías de la información como uno de los principales beneficios de la industria 4.0, aunque la ciberseguridad no siempre es considerada con la misma jerarquía en los sistemas industriales.

1.6. Enfoque metodológico

El siguiente trabajo de investigación, tendrá principalmente un abordaje descriptivo, ya que luego del análisis de distintas fuentes bibliográficas se realizará el análisis del tipo explicativo de los distintos temas abordados.

El material de estudio será enfocado en la línea de investigación con búsqueda bibliográfica en proyectos de industria y prevención de ataques a la ciberseguridad.

1.7. Contribuciones principales

Las amenazas a redes industriales y líneas operativas en la actualidad son tendencia porque la gran mayoría de los ataques informáticos, están enfocados en obtener un beneficio económico o terrorismo para los ciberdelincuentes.

Durante la última década, los ataques a las industrias aumentaron considerablemente, donde personas y empresas están obligadas a una recompensa económica para recuperar información sensible de la organización. Se hacen más frecuentes los ataques a los procesos industriales, donde los hackers tienen puesto su objetivo en el corazón productivo de las empresas, donde funcionan las redes industriales conectadas a redes de computadoras.

Entre otros, podemos destacar el caso de Stuxnet, que fue uno de los malware pioneros en ciberataques, donde el virus ingresaba por una memoria USB a través de una PC y llegaba a

tomar el control de la infraestructura causando desastres industriales. Este virus Stuxnet atacaba equipos con ejecución de software SCADA de la marca Siemens, usando un exploit llamado MS08-067, (vulnerabilidad para la ejecución remota de código), que si bien contaba con los parches dispuestos por Microsoft al año 2010, estos serían vulnerados. Los ataques cibernéticos, desconcertarían a especialistas de todo el mundo y mostrarían cierta preocupación por la seguridad de los sistemas industriales interconectados. (Kamlofsky, 2015)

2. Marco Teórico

2.1. Sistemas industriales

Un sistema industrial representa la gestión de técnicas y distintas metodologías donde la tecnología, la información, los equipos y las materias primas conforman bienes y servicios que luego de completada su fabricación son distribuidos para su comercialización.

Para agregar funcionalidad a la producción industrial donde se integran y fusionan procesos físicos con digitales, se da lugar al concepto de industria 4.0 que dispone de técnicas avanzadas para la producción y operaciones de procesos inteligentes que se integran dentro de las organizaciones, las personas, los bienes y activos, concluyendo en la cuarta revolución industrial.

Con la cuarta revolución industrial se fusionan tecnologías digitales (IT) y físicas (OT), marcando la aparición de nuevas técnicas como la robótica, la analítica, la inteligencia artificial y el internet de las cosas (IoT). Las organizaciones utilizan estas tecnologías que satisfacen sus necesidades y requerimientos en los procesos, por ejemplo, en las industrias, la utilización de sistemas en redes SCADA conectados a internet.

Con anterioridad a la industria 4.0, las redes industriales se encontraban aisladas de otras infraestructuras, en su mayoría con utilización de protocolos críticos. De esta forma, los entornos digitales para las actividades de producción resultaban completamente aislados.

La seguridad que presentaban los sistemas OT era por ocultamiento, ya que al estar aislados no eran víctimas de ciberataques, pero con la llegada de las nuevas exigencias tecnológicas, las empresas se vieron en la necesidad de conectar todas sus redes administrativas para obtener flujos de trabajo más ágiles. Esto puede dejar de manifiesto los servidores con protocolos de redes TCP/IP, sistemas de control de dispositivos PLC, SCADA y SCI. (Carrasco, 2013)

2.1.1. Visión de la industria 4.0

Los requisitos que promueven la convergencia en los diferentes mercados cambian de una

industria a otra. En mercados, como el del petróleo y el gas, se considera que la convergencia de SCADA con sistemas ERP ofrece beneficios significativos. Esto podrá ayudar a abordar algunos de los diversos desafíos que se enfrentan.

En las diferentes industrias, siempre que sea posible, se busca incorporar la mayor conectividad en las estructuras operativas.

Con la industria 4.0 se favorece la capacidad de comunicar y compartir información entre las redes, para que los dispositivos, sistemas y personas estén en continua asociación. En particular, la utilización de tecnología electrónica y de la información dentro de los sistemas OT, facilita el control centralizado del monitoreo y la seguridad aplicada.

El desarrollo de sistemas que proporciona información en tiempo real sirve para optimizar los tiempos y monitoreo permanente de los procesos de las líneas de producción. (Aguilar, 2017)

2.1.2. Niveles de automatismo

Los sistemas de la Industria 4.0 presentan distintos niveles de automatismo: la respuesta en tiempo real, seguimiento de procesos, cumplimiento de objetivos y lograr rentabilidad. (Trend, 2019)

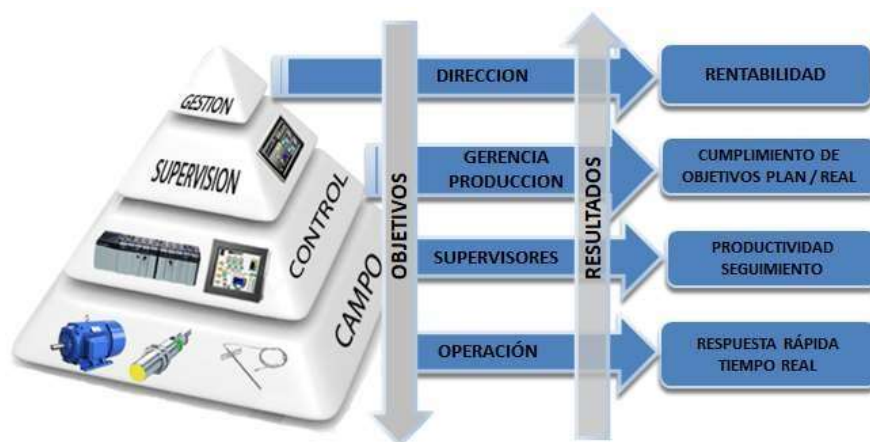


Figura 1. Industria 4.0 - Niveles de automatismo

La digitalización pasó de ser un elemento relevante en el avance de los sistemas de automatización industrial a transformarse orientando su foco a una nueva etapa, conocida como la industria 4.0 que surge de la convergencia de sistemas de negocio con redes OT y la unión de varias tecnologías de la información.

La industria 4.0, es la innovación que se caracteriza por la asociación entre lo físico y digital y presenta un escenario integral donde se disuelven conceptos tradicionales conocidos como cadenas de valor y fronteras geográficas de empresas que brindan productos y servicios.

Además de crear un nuevo desafío para los actuales modelos de industrias productivas, facilita nuevas oportunidades de crecimiento económico, así como reformas esenciales a la competitividad, flexibilidad y eficiencia de los procesos de producción industrial. La combinación con la tecnología de la información se traduce en la optimización e interacción de los procesos de investigación y desarrollo, diseño, producción y asistencia de servicios asociados. Dentro de la competencia económica, las organizaciones tienden a evolucionar hacia una variedad de servicios, para lograr la transformación de bienes y activos.

La revolución industrial 4.0 es viable gracias a la concurrencia de varias tecnologías destacables. Entre ellas vale la pena destacar la conectividad entre los centros de producción y los servicios de nube a través de redes de alta velocidad y capacidad, conocido como fibra óptica o servicios 5G, que son las redes de quinta generación de tecnologías de la telefonía celular.

Las redes 5G incrementarán el uso de tecnologías Big Data y mejorarán la conectividad reduciendo considerablemente el tiempo de latencia y fortaleciendo la llegada del IIoT (internet de las cosas de uso industrial). Las redes que conforman internet y los sensores industriales instalados en localizaciones remotas de la red OT, facilitarán la inteligencia autónoma en los procesos y servicios cloud ofreciendo capitales de automatización y capacidad de almacenamiento bajo demanda a través de internet con escalabilidad y flexibilidad. (Lecuit, 2019)

2.1.3. Tecnologías big data

Las tecnologías de big data admiten el estudio de un extenso marco de información, desde

las particularidades de los usuarios a las mejoras de la producción.

La utilización de la inteligencia artificial en el análisis de la información, con ejecución en los sistemas robotizados de producción y en aplicaciones de realidad aumentada, permiten determinar las técnicas industriales y optimar la competitividad de la producción industrial.

De esta manera, se obtiene una exclusiva relevancia en la recepción de especificaciones, estándares y mejores prácticas, así como la regulación que agiliza la transferencia y utilización de la información en las organizaciones.

La integridad y resguardo de los datos y los sistemas de información en las industrias y redes de comunicaciones en internet, es una ventaja estratégica en los ámbitos privado y público, específicamente en la protección de infraestructuras críticas. (Lecuit, 2019)

El gobierno de los datos es el conjunto de los procesos, funciones, políticas, normas y mediciones que garantizan el uso eficaz y eficiente de la información para que la organización cumpla sus objetivos.

Se establece una serie de métodos y responsabilidades que certifican la calidad y seguridad de los datos dentro de las organizaciones.

La gobernanza de datos define quién puede emprender acciones, sobre qué datos, en qué situaciones y mediante qué métodos. La estrategia de gobernanza de datos debe ser bien diseñada fundamentalmente para cualquier organización que utilice tecnologías de big data, y tener presente las ventajas de los procesos y responsabilidades compartidos que reportan a la empresa.

Los factores de cada negocio indican el tipo de datos que se controlan en la estrategia de la gobernanza, así como las ventajas que se quieren obtener. (Souppaya, 2013)

2.2. Redes SCADA

Los sistemas informáticos utilizados para monitorear grandes infraestructuras críticas son conocidos como sistemas de control de supervisión y adquisición de datos. Son los SCADA los sistemas de software que constituyen el avance de gran impacto de la automatización industrial. Con ellos, es posible controlar y supervisar el funcionamiento de los procesos

productivos. Mediante representaciones gráficas en pantalla se reproducen en tiempo real estados y alarmas de los diferentes dispositivos que actúan en el proceso y se puede intervenir sobre ellos en forma remota, sin necesidad de exponerse a riesgos presentes en la planta.

En los sistemas de control SCADA, para las comunicaciones con HMI, PLC e ICS se utilizan protocolos basados en TCP / IP y pueden comunicarse con redes corporativas.

La conexión de redes OT con redes IT conlleva riesgos inherentes que son naturalmente introducidos, y es por esta razón que, muchos sistemas industriales se aislaron intencionalmente.

La mayoría de las organizaciones que prestan servicios públicos críticos como los sistemas de transporte público y o las centrales de generación y/o distribución de energía industrial, utilizan sistemas SCADA para el trabajo y conviven en la importancia de resguardar los sistemas de las amenazas existentes.

Las redes OT presentan una estructura basada en un servidor o granja de servidores centralizados con PLCs interconectados que controlan los distintos dispositivos, pantallas para monitoreo y control de la información.

Los sistemas SCADA se empezaron a utilizar para responder a comenzaron en función de la necesidad de lograr el progreso del método de control y monitoreo de los diferentes módulos y procesos que hacen parte de las empresas, haciendo utilización de las herramientas de software que sirve para el uso de interfaces entre los PLC y los sistemas de gestión.

En un comienzo las redes operacionales SCADA eran sistemas que funcionaban en forma independiente, con elementos aislados creados a la medida de las necesidades tanto a nivel de software como de hardware. La capacidad de procesamiento de estos elementos eran limitados y no podían desarrollar más tareas de las inicialmente propuestas, adicionalmente los protocolos propietarios de comunicaciones eran desarrollados para permitir el significado del tiempo de duración de los procesos. (Franklin, 2016)

Los sistemas SCADA presentan una estructura basada en un servidor o granja de servidores centralizados, PLCs que controlan los distintos dispositivos y pantallas para realizar el monitoreo y control de los sistemas de la base de datos de los históricos. Se puede visualizar el esquema de redes SCADA en la “Figura 2”. (Ardita, 2016)

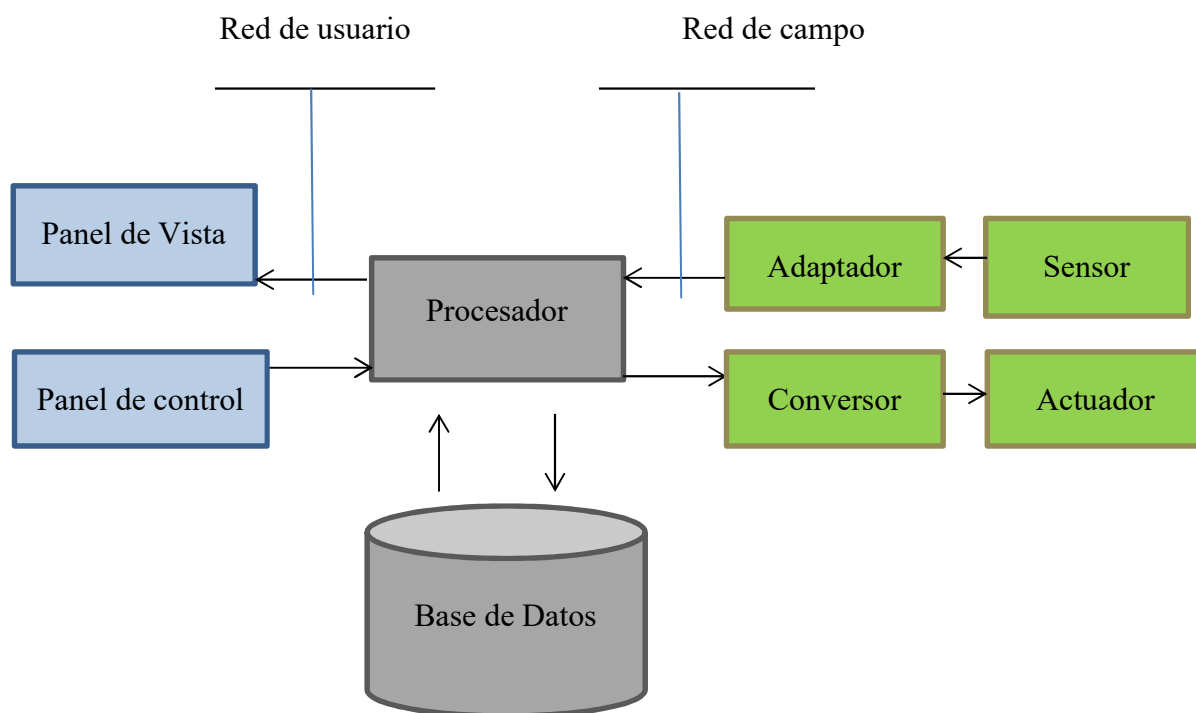


Figura 2. Esquema redes SCADA

2.2.1. Infraestructuras críticas

Los sistemas de información de las infraestructuras críticas son el conjunto de activos tecnológicos imprescindibles, que interactúan entre sí para ofrecer servicios importantes a las sociedades. Los activos pueden ser instalaciones físicas o virtuales, redes industriales, sistemas de información, sistemas de control industrial, redes y bases de datos, procesos automatizados o cualquier dispositivo tecnológico que permite la asistencia o la supervisión de servicios fundamentales de la industria o en mayor escala de la organización de una sociedad. La falta de controles en ciberseguridad para el resguardo de los bienes y activos ocasiona potenciales riesgos tanto para la industria como la nación.

La realidad es que los bienes y activos no están libres de sufrir algún tipo de incidente en ciberseguridad, debido a la gran cantidad de amenazas que existen en el ciberespacio. El impacto de un incidente logra afectar a diferentes divisiones de un país como el de la administración pública, la salud, las telecomunicaciones, los proveedores de energía y las finanzas.

Las estrategias de ciberseguridad facilitan la necesidad de identificar y clasificar los servicios

según la criticidad, para luego protegerlos debidamente frente a las amenazas.

Dentro de las infraestructuras críticas en el rubro industrial, se encuentran clasificadas de acuerdo con su arquitectura.

Las infraestructuras críticas, en su gran mayoría están aisladas y se encuentran distribuidos dentro de las redes LAN, tienen software de desarrollado para el correcto funcionamiento y métodos complejos para su monitoreo y administración.

Las infraestructuras industriales utilizan redes de datos privadas y públicas que tienen sistemas de información y procesos automatizados implementados mediante PLC (Controlador Lógico Programable). La administración y monitoreo de las redes PLC se realiza de manera remota utilizando el sistema SCADA que se encuentra conectado a redes corporativas para el análisis de información en tiempo real y toma de decisiones.

2.2.2. Priorización de redes

En el entorno industrial, se trabaja con los conceptos de IT (tecnologías de la información) y OT (tecnologías de la operación), y ambos métodos son necesarios para la operatividad de la compañía u organización. Desde el enfoque de la seguridad, los sistemas de las tecnologías de la información priorizan la confidencialidad de los datos por encima de otros aspectos. Pero, en el caso de los sistemas de control industrial, se prioriza la disponibilidad y la funcionalidad sobre la seguridad.

En la actualidad, internet conecta millones de redes, incluidas aquellas que hacen trabajar infraestructuras y servicios críticos, donde se encuentran los SCADA en conexión con los sistemas de gestión dentro de las diferentes entidades.

Organizaciones de gran importancia para la sociedad como alimenticias, laboratorios, petroleras y bancarias son focos para los ciber-atacantes, ya que forman parte de infraestructuras críticas, donde pueden obtener información sensible de las naciones o bien un ataque a estas infraestructuras podría ocasionar un desastre natural, generado un terrorismo social para cualquier nación.

Los sistemas de control SCADA, como se presenta en la “Figura 3”, obtenida del monitoreo mediante sistemas SCADA, tienen como prioridad la disponibilidad de la producción donde

utilizan monitoreo constante, con alarmas, sensores y actuadores configurados dentro de los parámetros establecidos. (Intellymation, 2019)



Figura 3. Centro de monitoreo SCADA

2.3. Sistemas ERP

Los ERP (Enterprise Resource Planning) son sistemas de gestión de la información que integran procesos de negocio, con el objetivo de promover la sinergia dentro de las organizaciones.

Los sistemas ERP implementan en las industrias un modelo de planificación mediante la introducción de procesos basados en buenas prácticas utilizadas en el mercado. Una de las principales ventajas es la implantación que logra la eficiencia en las operaciones y la integración de los equipos a través de la visibilidad de los flujos de información, logrando la reducción de costos y disponer de la información correcta para la toma de decisiones.

Los sistemas de información que integran procesos de negocio, denominados ERP, tienen el objetivo de crear y lograr la disponibilidad en el correcto uso de la información de los recursos adecuados en el momento correcto para optimizar el funcionamiento de los sistemas de gestión de forma proactiva.

El objetivo de los sistemas ERP es integrar, capturar, almacenar, procesar y distribuir la información generada por las diferentes unidades de la empresa.

Antes que los sistemas ERP comenzaran a desarrollarse durante la segunda guerra mundial, existían los sistemas MRPS, que se utilizaban en los sectores productivos llevando a cabo

tareas como la facturación, administración de nómina y el control del inventario. El desarrollo de las tecnologías y computadoras permitió que estos sistemas se desarrollaran, pasando a manejar cada vez más información y de manera más rápida.

Los sistemas comenzaron a tratar factores relacionados con la planificación de las capacidades de manufactura, teniendo en cuenta contextos como interrupciones en la operación de las empresas o las relaciones entre clientes y proveedores.

Los ERP son sistemas de gestión global para organización y planificación de distintos procesos y circuitos de gestión de información que de forma estructurada satisfacen la demanda de la gestión empresarial. En los sistemas de gestión ERP se prioriza la protección de la información, deteniendo la operación si el sistema no está disponible. (Masoero, 2015)

2.3.1. Ventajas de los ERP

Antes de la existencia de los sistemas ERP las empresas usaban un sistema diferente para cada área, provocando duplicidad en los datos, dificultad en los accesos a los sistemas, creando problemas de integridad e impidiendo que estuviesen compartidos los datos procesados, generando numerosas dificultades en las tareas de gestión de la empresa.

Las ventajas que proporcionan los sistemas ERP dentro de las organizaciones son la automatización y simplificación de los procesos que se realizaban de forma manual como resultado de la imposición de una nueva distribución lógica, reservando tiempo para optimizar la productividad, la operación y el aumento de la competitividad de la empresa.

Permiten la integración de todas las áreas de una organización, mejora del control sobre las operaciones y la coordinación entre los diferentes departamentos, para facilitar los procesos de auditoría.

Por lo general tienen la gestión de la base de datos, la cual es centralizada e integrada donde se registran, procesan, monitorizan y controlan todas las funciones que realiza la empresa. Los ERP logran agrupar todo el software en un gran sistema.

La implementación de un software ERP especializado para un modelo de negocio, permite optimizar las cadenas de valor de la producción, y se obtiene como beneficio la optimización de procesos, la digitalización, la evaluación continua y el intercambio de datos en tiempo

real, para garantizar que la gestión empresarial resulte flexible y eficaz.

Las nuevas industrias se caracterizan por el enfoque en el cual la cadena de valor va más allá de las instalaciones, promoviendo un compromiso entre clientes, proveedores y entidades financieras. (Camara, 2012)

2.3.2. Los ERP en las industrias

Los sistemas ERP son aceptados como soluciones globales de buenas prestaciones, y tienen gran aceptación en el mercado empresarial por tratarse de sistemas robustos.

Otro paso esencial de los ERP en convergencia con los sistemas SCADA dentro de la industria 4.0 implica la incorporación de los MES, (sistemas de ejecución de manufactura). En conjunto con los ERP, estas soluciones inteligentes establecen un vínculo más profundo entre el control de producción y la gestión empresarial para lograr una integración más eficiente. Desde el punto de vista funcional y de arquitectura técnica, estos sistemas pueden definirse como un software abierto, diseñado para integrar distintos procesos.

Los sistemas de gestión son la posible solución para ejecutar las tareas de gestión de las empresas y para facilitar la interconexión entre toda la infraestructura automatizada de equipos y máquinas de aplicación trascendental para en las técnicas de manufactura.

Los programas, la conectividad y los sensores relacionados con los productos o servicios se pueden servir del IoT (internet de las cosas) para alcanzar mayores niveles de rentabilidad y competitividad. (García, 2019)



Figura 4. ERP en las industrias

2.4. Seguridad informática

La seguridad informática tiene como principal objetivo la preservación y mantenimiento de la confidencialidad, integridad, disponibilidad y continuidad de los sistemas y de la información. También es el área relacionada de la informática que se orienta hacia la protección de la infraestructura de hardware, software, redes, bases de datos, archivos de configuración crítica y certificados.

El sector de seguridad informática dentro de una organización se encarga de los controles periódicos de las aplicaciones, gestión de licenciamiento, cumplimiento de auditorías de sistemas con resguardo de la información y controles realizados en función de los estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para mitigar los posibles riesgos en la organización.

Es posible clasificar distintos tipos de la seguridad informática según el enfoque:

- Por hardware con la implicancia de la protección perimetral y control preventivo que asegura resguardo de los servidores, bases de datos, conexiones de redes, enlaces y canales de comunicación por internet.
- Por software de firewall, proxy, vpns, routers y dispositivos de comunicación que requieren políticas y reglas para accesos y denegaciones.

Las políticas de control, resguardo de activos, autenticación de contraseñas seguras, renovación de certificados, tipos de claves criptográficas, controles biométricos, copias de seguridad y planes de restauración son tareas esenciales del equipo de seguridad informática.

Para la disposición de buenas prácticas y principales recomendaciones se presentan 10 normas de seguridad informática que se describen a continuación. (ISACA, 2006)

1. Privilegio mínimo, dar solo la información relevante para que el usuario pueda realizar su trabajo diario.
2. Cerrado por defecto, sacar todo lo que no utiliza y asignarlo en caso de que lo requiera.
3. Segregación de tareas y funciones con reducción al mínimo de los conflictos de interés.

4. Defensas en profundidad, colocando varias capas de acuerdo con los riesgos asociados con los activos de la información de la organización.
5. Lo diversificado y lo coherente, evitar la dependencia de un cliente o proveedor para un servicio para asegurar la supervivencia.
6. Seguridad con criterios simples, todo lo que es complejo está perjudicando al negocio y por lo tanto a la seguridad de la empresa.
7. Transparencia con un sistema abierto, tender la seguridad a lo más sencillo posible y el acceso a la cibercriminalidad a los sistemas más complejos.
8. Usuario como eslabón débil, donde la mayor cantidad de errores que se cometen en ciber-seguridad se basan en el desconocimiento o falta de atención por parte de los empleados.
9. Auditoría regular, realizar estudios periódicos para detectar continuamente las fallas y corregirlas antes de que fuentes externas las conozcan y las aprovechen.
10. Estrategia clara, tener en claro cuál es la estrategia para realizar en el momento en que se materializa un ataque contra los activos de información.

2.4.1. Consideraciones en seguridad IT / OT

Los mundos de IT y OT evolucionan con diferentes consideraciones y prioridades. Mientras que los sistemas de IT están diseñados para conectarse entre sí, los sistemas industriales de redes OT estuvieron aislados.

En los sistemas IT, los componentes generalmente se implementan con una vida útil deseable de 10 años. En una red industrial, en cambio, se puede esperar que los dispositivos o componentes duren varias décadas sin modificaciones.

Los sistemas de IT están diseñados con la capacidad de actualización y mantenimiento regular, mientras que con los sistemas OT, las ventanas de mantenimiento y la capacidad de actualizar y substituir módulos son más difícil una vez que están operativos, ya que son dispositivos que funcionan continuamente y el tiempo de inactividad tiene que ser programado en una parada de planta con detención total y gran coordinación de los sectores

intervinientes en mantenimiento, logística y producción.

La seguridad de la información se definió por la necesidad de preservar la confidencialidad, integridad y disponibilidad de la información, donde se incluyeron otras propiedades, como la autenticidad, la responsabilidad y la fiabilidad.

Muchos enfoques fueron evolucionando para la seguridad de IT, y casi todos con el objetivo de la confidencialidad explícita o implícitamente por encima de todas las demás propiedades. Los especialistas de redes OT, deben velar y garantizar que los controles de procesos de las plantas industriales sean seguros, eficientes y estén continuamente disponibles. (WisePlant, 2019)

En referencia a los enfoques presentados de ciberseguridad, podemos citar al investigador Jorge Kamlofsky: “Mientras que según las ISO 27000 los pilares de la seguridad en los sistemas IT son la confidencialidad, la integridad y la disponibilidad, en los sistemas operacionales, sólo es de interés la disponibilidad. Por eso, las soluciones de ciberseguridad en estos sistemas deberían enfocarse en los aspectos faltantes: confidencialidad e integridad”. (Kamlofsky, 2015)

2.4.2. Gestión de la seguridad

Para garantizar la gestión de la seguridad, en las organizaciones se debe definir un conjunto de objetivos de seguridad en redes SCADA que vayan en consecuencia con los objetivos del negocio de la empresa.

Estos objetivos se conocen como estructura de control y pueden asegurarse con buenas políticas de seguridad, planes y guías de implantación. La seguridad es un proceso continuo que no termina luego de la implementación de los sistemas de tecnología.

Los sistemas de control se deben realizar periódicamente sobre hardware, firmware, comunicaciones y software para supervisar y controlar las funciones y servicios vitales. Además de los dispositivos tecnológicos para el control de accesos, es importante contar con verdaderas políticas de seguridad de la información.

También es fundamental realizar auditorías internas como externas. La diferencia radica, que en auditorías internas, el juicio de valor de los resultados puede verse influenciado por

conflicto de intereses por ser personal de la organización, en cambio las auditorías externas al ser realizadas por personas ajenas a la organización con uso de técnicas independientes y vasta experiencia en varias auditorías están pueden tener mayor aceptación y de resultados imparciales de ser emitidos por entidades de confianza. (ISACA, 2006)

Los sistemas de control industrial no fueron diseñados y explotados por expertos en seguridad de tecnología, donde la participación de ingenieros informáticos fue muy limitada y en varios casos sin contemplar la seguridad en la transmisión de los datos.

Para el diseño de los nuevos sistemas y modificaciones existentes se adoptaron por profesionales que desarrollaron su actividad en el ámbito de la ingeniería industrial, la obra civil y la explotación de infraestructuras.

2.4.3. Cumplimiento y normas de seguridad

Los siguientes puntos favorecen al cumplimiento de las normas de seguridad informática. Tener las licencias de los sistemas operativos, antivirus y demás software actualizados, contar con los equipos de resguardo perimetral adecuados y configurados como ser firewalls, DMZs y proxys de navegación, requerir a los usuarios corporativos acceso mediante múltiples factores de autenticación a los sistemas.

Es vital para el buen funcionamiento y cumplimiento de las políticas de seguridad, contar con un plan de capacitación permanente al personal, tener todas las copias de backups de sistemas productivos y disponer de un plan detallado de recuperación ante desastres.

A nivel estructural, las organizaciones muchas veces tienen dentro de una misma gerencia de sistemas, las áreas de comunicaciones, desarrollo de aplicaciones y seguridad informática. Sin embargo, las normas recomiendan que, el área de seguridad debe estar diferenciada del área de tecnología de la información, donde existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura y la información que gobierna seguridad informática.

2.4.4. Organizaciones y normativas

2.4.4.1. ISA99

ISA, International Society of Automation, es una norma creada en 1945 y desarrolla estándares globales extensamente usados y publicados en libros y artículos técnicos por especialistas, que proporcionan programas de desarrollo de carrera y gestión de redes que son utilizados en todo el mundo.

La publicación de normas sobre seguridad en los sistemas de control se fue incrementado, hasta lograr el conjunto de las normas ISA99, que comenzaron a desarrollarse pretendiendo dar un nuevo empuje a la seguridad de los sistemas de control industrial y creando un conjunto de documentos que ayuden al incremento de la protección de los sistemas frente a los ataques informáticos. (Ardita, 2016)

2.4.4.2. ISO 27001

La norma ISO 27001 es el estándar internacional que proporciona un marco para los sistemas de gestión de seguridad de la información (SGSI) para proporcionar confidencialidad continua, integridad y disponibilidad de información, así como el cumplimiento legal. La certificación ISO 27001 es fundamental para resguardar los bienes y activos, como información de empleados, cuentas de bancos, proveedores y otra información privada de la organización.

La ISO 27000 es una serie de normas, donde están la ISO 27001 y 27002 para seguridad informática en general, pero también hay normas en esta serie como por ejemplo la 27037 que es informática forense para procedimientos judiciales.

El estándar ISO 27001 es una norma estructurada para ser compatible con otros estándares de sistemas de gestión, como ISO 9001 y aplica para cualquier tipo de tecnología, completamente independientemente de cualquier plataforma IT.

Para alcanzar la certificación acreditada ISO 27001 se debe demostrar que la compañía está dedicada a seguir las mejores prácticas de seguridad de la información. Además, la certificación ISO 27001 le proporciona una evaluación experta de si la información de la

organización está adecuadamente protegida. (WisePlant, 2019)

Todas las normas proporcionan información que resguarda la gestión y las prácticas operativas de la seguridad de la información.

2.4.5. Buenas prácticas de seguridad

1. Contar con la configuración correcta de los firewalls.
2. Los sistemas deben contar con contraseñas sólidas.
3. Contar con más de un factor de autenticación de acceso.
4. Realizar copias de seguridad ante amenazas de ciberataques.
5. Capacitación y concientización de los empleados de la organización.
6. Contar con buenas políticas de la seguridad integral en OT / IT.
7. Aplicación y actualización de parches a los sistemas de información, acá ocurre el problema que los vendors de SCADA retiren la garantía en caso de actualizar el sistema operativo.
8. Utilización de sitios seguros HTTPS con certificados correspondientes.
9. Habilitar el mínimo nivel de acceso según lo requerido.
10. Realizar auditorías de los controles aplicados sobre los sistemas.

2.5. Ciberseguridad

Las redes de planta y las redes corporativas se unen cada día más y presentan protocolos en común y otros que no son contruidos bajo seguridad de normas estándar. Las bases de datos de los PLC que están interconectados con herramientas de industria son el claro objetivo de los hackers para los ciberataques.

La detección de vulnerabilidades para su remediación es una práctica que va en aumento, aunque sin embargo deberá pasar de ser una práctica netamente reactiva a una práctica más

preventiva, donde la seguridad de los sistemas de control comience de forma profunda desde las primeras etapas de diseño y no una vez que los productos ya estén siendo utilizados en las plantas industriales.

Según el informe presentado por RISI, donde se registran los casos de vulnerabilidad y ciberataques, se revelaron resultados con índices del 80 % de que los incidentes de seguridad ocurridos en manufacturas críticas no son intencionales.

Una importante cantidad de los incidentes no intencionales son generados por causas externas, tales como bugs, virus, malware, fallas de red o errores el personal interno.

En otro estudio realizado, del total de los incidentes ocurridos, los indicadores arrojaron valores del 53 % (empleados en disconformidad) y el 47 % de hackers informáticos.

El uso de tecnología interconectada e interrogada permite el acceso remoto donde la información técnica puede estar disponible públicamente y es donde los hackers tienen una puerta de acceso para vulnerar, siendo de su interés, las infraestructuras críticas. (RISI, 2015)

2.5.1. Tipos de ciberataques

Los ataques contra los sistemas de control pueden resultar desde la interrupción de servicios, ocasionando daños físicos, prejuicios económicos y efectos en cascada, causando la interrupción de las máquinas y deteniendo la producción de la planta industrial.

Existen distintos tipos de ataques, por disponibilidad e integridad.

En los ataques a la disponibilidad, se cambian señales de control para causar daño en los dispositivos, pudiendo afectar la disponibilidad de la red. En los ataques de integridad, los mensajes de control podrían ser manipulados y así comprometer la autenticación.

En los ataques por confidencialidad, que es la propiedad por la cual se garantiza el acceso a la información únicamente a quien esté autorizado, para evitar su divulgación inapropiada.

“Se debe evitar el acceso de intrusos manteniendo la confidencialidad, integridad, disponibilidad y control de la red. Es útil disponer de un sistema de seguridad en capas: firewalls, sistemas de detección de intrusos, sistemas de prevención de intrusos, listas de control de accesos y sistemas de autenticación”. (Kamlofsky, 2015)

2.5.2. Malware Stuxnet

En el año 2010 el malware Stuxnet se usó como instrumento para lograr exitosamente un ciberataque y tuvo lugar en una central nuclear de Irán, donde se detuvo la producción, causando grandes daños en la industria del uranio. Se puede enmarcar este ataque dentro del concepto de “ciberguerra” ya que EEUU no quería que Irán se desarrollara militarmente.

Este malware ingresaba a través de una memoria USB y alcanzaba el sistema informático de la planta que controlaba las máquinas centrifugadoras, que giraban a velocidades muy altas para separar los diferentes componentes del uranio y así aislar el uranio enriquecido. Esta técnica de separación sería fundamental para la generación de energía y el desarrollo de armas nucleares.

El malware luego de controlar las centrifugadoras tomaría el control de las máquinas con una propagación escalonada para no generar sospechas de los administradores de infraestructura y detendría el apagado de los interruptores manuales.

Durante el ataque cibernético, alrededor del 20 % de las centrifugadoras en la planta de Natanz quedaron fuera de servicio y el malware Stuxnet destruyó alrededor de 1000 máquinas centrifugadoras y retrasó el programa de armas nucleares de Irán, aunque probablemente no tuvo el impacto que esperaban los creadores, significó un desastre de una gran naturaleza para la ciberseguridad industrial. (Langner, 2013)

2.5.3. Covid-19

Los ciberdelincuentes siempre están buscando nuevas oportunidades para robar datos de los usuarios, acceder a la información de las empresas y obtener información confidencial. La actual situación provocada por el coronavirus abrió un abanico de posibilidades, sobre todo por la gran cantidad de uso de herramientas como, Skype, WhatsApp y Zoom, siendo esta última el principal objetivo de ataque de los cibercriminales.

En lo que va del año 2020, Zoom duplicó sus usuarios a 200 millones, pero también aumentaron los ataques cibernéticos, tales como el envío de notificaciones falsas por email, robo de credenciales y publicación de enlaces a reuniones falsas.

Los ciberdelincuentes, utilizaron técnicas de ingeniería social, haciéndose pasar por una persona o empresa de confianza que mediante la comunicación electrónica introducía por técnicas de phishing la inclusión de malware en los dispositivos para espionaje y robo de credenciales e información confidencial. (TechNocio, 2020)

En estudios realizados durante el primer semestre del 2020, las palabras covid-19 y coronavirus se utilizan cada vez con mayor frecuencia en nombres de dominio apócrifos, spam, phishing y malware a nivel mundial, donde se observa un incremento del volumen de las estafas por correo y otros medios electrónicos por medio de palabras clave para captar la atención de los usuarios.

Es natural que los ciber-atacantes se hagan pasar por la organización mundial de la salud (OMS), los centros de prevención o bien por medios que brindan información. Es por eso importante chequear los sitios y fuentes de acceso para no caer en la trampa de una estafa.

Los cibercriminales generan campañas que se benefician de los cuidados y prevención del coronavirus y por tal motivo no resultan ser complejas de introducir cualquier tipo de amenaza. Por eso se recomienda verificar que la información consultada respecto al Covid-19 sea de fuentes oficiales, tales como el sitio de la OMS y plataformas de los ministerios de salud nacional. (Trend M. , 2020)

3. Desarrollo Técnico

3.1. Planteo del problema

Los sistemas SCADA fueron desarrollados antes del surgimiento de internet y considerados para ser sistemas aislados y sin conexión en red. Continuaron su evolución en una dirección diferente al desarrollo de IT, enfocándose en la eficiencia operacional, y muchas veces, sin importar aspectos relacionados con la seguridad, mientras tanto, en la tecnología IT crecieron los desarrollos de dispositivos de seguridad como los firewalls, sistemas de cifrado y software de antivirus.

Sin embargo y teniendo en cuenta que la tendencia actual en los sistemas es que haya una interrelación entre ellos dentro de las mismas compañías, y en vista de lograr una mayor productividad y buscando acuerdos entre diferentes organizaciones que brinden cooperación mutua, son los sistemas parte fundamental de la seguridad de la información.

Sin contradecir las tendencias, los SCADA en la actualidad son sistemas que trabajan en conjunto donde todas las variables controladas hacen de un gran sistema conectado a internet y redes IT.

Cuando las áreas gerenciales solicitan la ampliación de la capacidad del trabajo, hacen que las empresas se incorporen a plataformas estándar de hardware y software como lo son distintos sistemas operativos, uso de protocolos de comunicaciones y de aplicaciones web, que al realizar esta inclusión también introducen las vulnerabilidades propias que poseen cada una de las redes de las organizaciones.

Una de las características de los sistemas SCADA es que la mayoría de sus componentes (hardware y software) se desarrollan para un funcionamiento continuo en ambientes exigentes. Poseen un elevado tiempo medio entre fallas (MTBF: Medium Time Between Faults) lo que los hace altamente confiables. Entonces, su ciclo de duración es mayor y su frecuencia de recambio es menor que muchos otros dispositivos. Así, aunque vigentes, son dispositivos en promedio notoriamente más antiguos, de modo que no se actualizan de la misma forma como si lo hace el resto de la tecnología, y esto puede representar una grieta en la seguridad. Estos sistemas no suelen estar preparados para ciberataques.

Adicionalmente el personal de IT no posee el conocimiento o la sensibilización necesaria que se requiere proteger una red SCADA, es decir en los sistemas que existen vulnerabilidades que normalmente no se pueden considerar de alto impacto en las redes corporativas, pero en el marco del sistema si lo son produciendo grandes pérdidas o también puede presentarse el caso que las medidas de control usadas normalmente por TI no son aceptadas a los sistemas SCADA, por lo que la implementación de las medidas no pueden ser lo suficientemente buenas para proteger el entorno. (Franklin, 2016)

3.2. Hipótesis de la investigación

En el marco de la adopción de conceptos de Industria 4.0 en las infraestructuras críticas, la convergencia entre los sistemas ERP (de tecnología IT) con los SCADA (de tecnología OT) conduce a nuevas vulnerabilidades en estos sistemas, si no se cuenta con efectivas políticas de seguridad informática, donde la prioridad de continuidad del negocio es semejante tanto para redes SCADA como sistemas ERP.

3.3. Convergencia

La convergencia es la capacidad de compartir y conectar diversos sistemas y procesamiento de datos usando tecnologías de redes, conectores de plataformas, actuadores y dispositivos de IIoT. Para las organizaciones, la comunicación en línea y el intercambio de información y datos, permiten la reducción en el desarrollo del producto y los plazos de entrega, logrando un alto nivel de la productividad y la eficiencia. Para achicar los ciclos de resolución de problemas, se debe mejorar la competitividad con el aporte de la capacidad operativa.

Las redes OT facilitan el procesamiento en tiempo real de grandes cantidades de datos, que permite que los sistemas de control automatizados tomen decisiones y expresen órdenes locales que regulan, controlan y cambian los procesos industriales que administran. En sistemas industriales sin conexión a internet, los ERP no cuentan con los datos de retroalimentación en tiempo real impidiendo la construcción de una visión global de las operaciones.

Sin embargo, es posible introducir la tecnología IT en los sistemas OT, de modo que el flujo de información entre los sistemas de gestión ERP y el control de supervisión de las redes SCADA, mejore el control de la información para la toma de decisiones.

También es posible tener una visión ampliada, precisa y en tiempo real de múltiples sistemas industriales dispersos geográficamente, para responder de forma rápida ante cualquier cambio del proceso que pueda ocurrir. (WisePlant, 2019)

3.3.1. Redes OT

Desde la revolución industrial, se generaron y desarrollaron nuevas industrias, donde los procesos se hicieron cada vez más eficientes y la productividad de los procesos industriales sumaría eficacia y agilidad de los servicios. Las utilidades y productos fueron impulsando el desarrollo de la sociedad, permitiendo monitorear, administrar y supervisar los procesos industriales.

En los sistemas de control industrial (ICS) se producen continuamente servicios públicos y distintos productos manufacturados y las tecnologías operacionales (OT) aseguran que las industrias funcionen día a día.

La mayoría de las redes OT están (o se implementan) en industrias que operan de modo aislado, sin conexión con otras industrias ni con el mundo exterior. Los responsables de tecnología en las redes OT, se especializan en la eficiencia en cada una de las industrias. Sin embargo, desde el punto de vista de la seguridad de la información requiere un enfoque que asegure la confidencialidad, integridad y disponibilidad.

El mundo de la tecnología que gestiona y controla las industrias, está conectado mediante las redes operacionales OT, en cambio, el mundo de la tecnología que gestiona negocios, internet y la capacidad de compartir datos e información, está conectado mediante a las redes corporativas IT. (Franklin, 2016)

3.3.2. Oposición al cambio

En el universo de la gestión IT, se necesitaron muchos años de educación y generación de

conciencia para capacitar a los empleados sobre la seguridad, ayudando a comprender el riesgo de ataques cibernéticos y malware.

Los desafíos en la educación de quienes trabajan en la industria de redes OT se hacen más complejos por el hecho de que los sistemas y los vectores de ataque pueden ser diferentes. Por lo tanto, el desafío principal es que los involucrados en la convergencia sean conscientes y conozcan el alcance total de cualquier riesgo al que la convergencia los exponga a pesar de que pueden estar familiarizados con el tipo de riesgo.

Uno de los desafíos de la seguridad informática es implementar y fortalecer las defensas cibernéticas en sistemas OT, ya que pueda ignorarse que los componentes de los procesos industriales ocasionen vulnerabilidades a los ataques, sin una comprensión completa de los vectores por los cuales podrían ser atacados o cómo el malware podría afectar los sistemas.

Al asegurar las redes SCADA, no se trata simplemente de tomar sistemas de seguridad diseñados y mapearlos con las redes IT, donde las arquitecturas de seguridad para OT deberán considerarse cuidadosamente. Por ejemplo, la función de un firewall en las redes de sistemas ERP suele tener una configuración diferente a la aplicación en las redes OT que debe evaluarse en detalle con otras soluciones en relación de las necesidades de asegurar las comunicaciones en los sistemas industriales.

Para asegurar redes OT, se deben comprender cuáles son los procesos y sistemas críticos, y qué amenazas se enfrentan. Al priorizar los controles de seguridad que se implementan, se pueden abordar las amenazas más relevantes del sistema o proceso dentro de la organización.

A medida que se optimizan los procesos de gestión, se puede encontrar una resistencia al cambio, por lo cual es recomendable incorporar campañas de educación para los empleados ante las nuevas formas de afrontar los procesos de seguridad con el régimen de pautas que la industria considera implementar.

En los sistemas de OT, la seguridad cibernética debe convertirse en una consideración primordial. En varios casos, se introducen leyes y pautas a seguir. En las industrias no reguladas, deberán acordarse e implementarse nuevos estándares y procedimientos de seguridad especificados y apropiados para cada industria y que pasen a formar parte de todas las consideraciones diarias.

La falta de conocimiento de los problemas de seguridad, junto con la comprensible renuncia a alterar los sistemas y los procesos industriales que funcionaron durante muchos años, puede conducir a situaciones en las que se consolide o superpongan nuevas tecnologías sobre los sistemas preexistentes. (Franklin, 2016)

3.3.3. Amenazas de riesgo

Cuanto más expuesto al mundo exterior se vuelven los sistemas industriales, mayor es la amenaza a la que se exponen los sistemas de redes SCADA y mayor es el riesgo de interrupción operativo ante una posible amenaza cibernética. Los encargados de proteger los sistemas ERP y las redes corporativas disponen de sus experiencias implementando las mejores prácticas para enfrentar al riesgo de estar conectados a internet y a sistemas externos.

Sin dudas, la amenaza de los programas maliciosos y ataques cibernéticos es un riesgo potencial y latente en industrias interconectadas a internet, donde existen riesgos de que una persona con conocimiento de la organización utilice sus habilidades para manipular un sistema con efectos perjudiciales. También existe el riesgo de que un error de proceso o un error numérico involuntario se propague a través de un sistema causando distintos daños dentro de un entorno de la red IT.

Estos errores de proceso pueden tener un efecto limitado dentro de la red convergente. Los cambios en procesos de IT requieren una mayor organización y deben planificarse cuidadosamente con la debida consideración del entorno en el que se implementó el sistema de gestión, entendiendo que la tecnología OT que rodea las redes puede ser muy sensible al reinicio de servidores, la instalación de software o la aplicación de parches para actualizaciones.

Cada una de las medidas de seguridad cibernética, debe ponerse en práctica cuando alguien quiere perpetrar un ciberataque contra un artefacto de IT / OT, ya que el éxito dependerá de los recursos y técnicas de prevención contra los conocimientos y tiempo dedicado del ciberdelincuente.

Es fundamental que los administradores de OT comiencen a compartir esta realidad, porque se aplicará a ellos también. Para la red convergente, los riesgos que comparten redes IT y OT

son similares, no necesariamente en cómo se puede perpetrar un ataque, sino en que, en algún momento u otro, será atacado.

Los ciber-atacantes identifican y atacan los enlaces más débiles que pueden encontrar. Los sistemas industriales heredados que anteriormente no estaban conectados al mundo exterior se construyeron sin consideraciones de seguridad cibernética, conformando la red convergente. Por lo tanto, el enfoque del atacante cibernético puede pasar de la organización a las conexiones más frágiles dentro de OT, donde tiene mayores posibilidades de éxito. (Grupo, 2017)

3.4. Riesgos en ERP

Se define riesgo al impacto por la probabilidad de que una amenaza pueda afectar de manera adversa la consecución de los objetivos. Un riesgo de acceso identifica una posible situación inapropiada que puede causar un problema o una pérdida. Existen evaluaciones cuantitativas y cualitativas de los factores potenciales que dan origen al riesgo, donde la evaluación y calibración es realizada por los dueños de los procesos y el control interno.

Dentro de las organizaciones existen diferentes áreas, perfiles y roles para los empleados que, según su tipo de perfil y posición, tienen asociados un conjunto de tareas que se conocen como acciones. Las acciones o transacciones (así llamadas en ERP) agrupadas en conjunto forman roles simples o compuestos, que agrupados forman los procesos de negocio o posiciones de áreas. Adicionalmente, la suma de acciones según el proceso de negocio se agrupa por funciones que, según su combinación, presumen un riesgo potencial, previamente definido por los dueños de procesos.

Todo análisis de riesgo se realiza utilizando un determinado conjunto de reglas que, sumados a los controles por funciones, forman una colección de riesgos de acceso. Se utiliza por el set de reglas del sistema para medir riesgos de errores o irregularidades, identificar problemas y asegurar qué acciones correctivas serán tomadas. Esto se logra asegurando que ningún individuo tenga control sobre varias o todas las fases de un proceso.

Para analizar y mitigar los riesgos de procesos de negocios, se identifican y regulan por segregación de funciones y acciones críticas definidas por el control interno. (Camara, 2012)

3.4.1. Control interno

Debido a los riesgos a los que se exponen las organizaciones, actualmente es necesario desarrollar una cultura de ciberseguridad entre los miembros de la organización con lineamiento en las políticas de la empresa determinadas por el control interno, que es el plan junto a todos los métodos y procedimientos que en forma coordinada se adoptan en una entidad para lograr la protección de activos, obtención de información correcta y promoción de la eficiencia de la operación y adhesión a las políticas prescritas por la dirección.

El directorio y dueños de procesos junto con las áreas de seguridad y auditoría velan por el cumplimiento de lo establecido en el control interno que, si bien el objetivo no es convertir a los empleados y directivos en expertos de seguridad de la información, sí deben tener el consentimiento de que el manejo de los datos de la organización implica tener resguardo de las aplicaciones de controles y herramientas de protección de la información.

Por eso es importante, introducir las mejores prácticas en materia de seguridad para que se adopten normas de comportamiento seguro en los diferentes ambientes de los sistemas de gestión. Estas prácticas son desde la utilización de firewalls, reglas de acceso, filtrado de contenidos, control con bloqueo o habilitación a demanda de puertos y protocolos, segregación de redes por distintas vlans, utilización de credenciales con doble factor de autenticación y segregación de funciones según el rol de los empleados.

El control interno junto a seguridad informática y auditoría, definen la matriz donde se describen los procesos de negocio y potenciales riesgos, donde la probabilidad por el impacto de ocurrencia determina el tipo de riesgo y su control mitigante.

3.4.2. Matriz de riesgos

La matriz de riesgos se utiliza para identificar los riesgos inherentes a las actividades de una empresa, tanto de los procesos como de la fabricación de productos y administración de servicios. Es la herramienta para optimizar el control y mitigación de riesgos en conjunto con las normas vigentes de la seguridad de una organización.

A través de la matriz se puede realizar un diagnóstico objetivo y global de la seguridad de la información de la empresa sin importar la dimensión del sector o actividad. Asimismo,

mediante el análisis de las distintas variables cargadas en la matriz, es posible evaluar la efectividad de la gestión de los riesgos, tanto financieros como operativos y estratégicos, que impactan en la misión de la organización. (Ercoli, 2017)

En la siguiente matriz de riesgos, se pueden observar los distintos procesos de finanzas que agrupados en funciones generan diferentes riesgos para la organización. Para mayor detalle, véase *Tabla 1*, donde se presenta un ejemplo por SoD (segregation of duties) agrupadas por accesos críticos asociados a procesos del negocio.

Tabla 1. Matriz de riesgos SoD

	ZAP0 1	ZAP02	ZAP03	ZAP04	ZAP05	ZAP06	ZAP07	ZAP08	ZAP09	ZAP1 0	ZAP1 1	ZAP1 2	ZAP1 3	ZAP1 4	ZAP1 5
ZAP01		C24												C43	C2
ZAP02	C24		C49										C3	C31	
ZAP03		C49												C55	C11
ZAP04									C73						C13
ZAP05							C78	C71		C85				C5	C10
ZAP06								C68	C88						
ZAP07					C78					C81					
ZAP08					C71	C68									
ZAP09				C73		C88									
ZAP10					C85		C81								
ZAP11															
ZAP12													C138		
ZAP13		C3										C138			
ZAP14	C43	C31	C55		C5										
ZAP15	C2		C11	C13	C10										

3.4.3. Accesos críticos

Sumado a los riesgos identificados por segregación funcional, tal cual lo indicado en la Matriz SoD, están los accesos críticos, definidos por el sistema dada su complejidad de ser utilizados sin un control estricto ya que la suma de funciones son un riesgo en su ejecución.

Los roles son combinaciones de funciones de aplicación que se asignan a los usuarios del sistema y que tienen acceso a las funcionalidades comunes, por ejemplo, cargar, autorizar y registrar facturas de venta, todas posiciones o puestos de trabajo de la compañía que deben ser realizados por diferentes roles según la función. Cada rol es un subconjunto de funcionalidades que el usuario necesita para desempeñar sus responsabilidades de trabajo.

Los roles al combinarse con otros consiguen cubrir la totalidad de las funciones que cada usuario requiere en el desempeño de su tarea, por lo tanto, un usuario puede requerir la asignación de más de un rol. Por ejemplo, un responsable de compras puede necesitar los roles de gestión de órdenes de compra, mantener la lista de acuerdos y reportes de compras, para poder realizar las actividades diarias de trabajo de acuerdo con su puesto de trabajo en la empresa.

En el sistema ERP, los roles tienen autorizaciones que otorgan acceso a las transacciones y pueden limitar el acceso a los distintos grupos de los datos organizativos. Los usuarios obtienen sus accesos desde el maestro de usuario, en el cual se asocia al usuario con los roles asignados.

Al momento de asignar los roles a los usuarios es de vital importancia considerar a la segregación de funciones establecidas por la compañía, a fin de evitar la existencia de usuarios con incompatibilidades.

El diseño de los roles se define entre los especialistas de seguridad del sistema y los usuarios funcionales que son aquellos que tienen el conocimiento del proceso de negocio. El trabajo se desarrolla en sesiones periódicas para establecer las autorizaciones y funcionalidades a las que debe acceder cada puesto de trabajo que posteriormente tendrá un usuario o grupo de usuarios asociados. Una vez definidos, se realiza la construcción y posterior prueba, para verificar que los mismos cumplan con los requerimientos establecidos por los usuarios clave y los procesos definidos. Para verificar la correcta segregación de funciones, se ejecuta la

revisión de los roles por medio de la herramienta llamada GRC.

Dentro de las funciones que se realizan dentro de la empresa, es posible identificar actividades que son críticas y que dada su condición serán monitoreadas periódicamente para determinar si los usuarios que las poseen son los adecuados.

Los accesos críticos se clasifican en acciones críticas que se dan por la conjunción de transacciones y autorizaciones. Las autorizaciones críticas se dan en permisos que son riesgosos por el permiso en sí.

Los usuarios o roles que tengan funciones críticas deben ser mitigados y observados como funciones conflictivas, permitiendo identificar inmediatamente a los usuarios que poseen accesos críticos. (Ercoli, 2017)

3.5. Seguridad en ERP

No sólo los ataques a sistemas IT se incrementan, sino que también son afectados por ataques cibernéticos los sistemas ERP. Para evitar que los atacantes pongan en peligro los sistemas, se requiere un enfoque global de la seguridad, donde deben tener participación de las definiciones de riesgos, tanto el negocio como el directorio y seguridad informática.

Para buenas estrategias de control se requiere tener en cuenta todas las capas y niveles del sistema ERP. La desprotección de una capa o nivel puede poner en peligro la seguridad de todo el sistema. Por eso se recomienda en toda implementación considerar la seguridad informática como un factor primario en la definición de los pasos a seguir y contar con varias etapas de control y así poder adelantarse a posibles conflictos de ciber-seguridad. También es importante tener planes actualizados para la aplicación de buenas políticas de seguridad informática utilizadas por las organizaciones y con control de auditorías periódicas internas y externas realizadas por entidades reconocidas.

Para contar con buenas políticas de seguridad es fundamental contar con personal idóneo y capacitado en la materia y velar por el cumplimiento de las medidas definidas por la organización, que se citan como ejemplo a continuación: divulgación de la información, copia o transmisión de las bases de datos, accesos indebidos a los sistemas, divulgar

información confidencial fuera del ámbito laboral.

Otra medida muy importante para resguardar la información de los ambientes ERP es el enmascaramiento u ofuscamiento de los datos mediante la técnica de data scrambling, que es la transferencia de información entre ambientes y/o instancias realizada de manera segura con la información de ambientes productivos que debe mantenerse resguardada y enmascarada para su uso en otros entornos de sistemas como ser ambiente de calidad.

Data scrambling es una técnica de enmascaramiento de datos confidenciales y sensibles de la organización y es utilizada por TDMS, (Sap Test Data Migration Server), que es una herramienta de extracción de datos de alta velocidad con la que se pueden transferir datos relevantes del sistema productivo al sistema no productivo para test. (Ercoli, 2017)

3.5.1. Controles y auditorías

Según estudios de consultoría IT de los últimos 10 años, se puede determinar cómo los ataques informáticos provocaron grandes pérdidas en conocidas empresas, a las que le robaron información de +500 millones de registros. Estos ataques no fueron realizados de manera aislada, los estudios indican que los ataques fueron el inicio de una nueva tendencia. Por eso como medida de control es fundamental contar con buenas medidas de seguridad informática y realización de auditorías periódicas.

Desde las auditorías, se puede observar que los puntos de mejora son similares a cualquier entorno de los sistemas ERP, por lo tanto, es de esperar que los atacantes intenten abordar primero las vulnerabilidades presentes en infraestructuras de controles débiles, escasas políticas de seguridad y sin monitorización de los sistemas de gestión. Para lograr un nivel aceptable de resguardo de los activos y poder evitar la gran mayoría de los ataques comunes es importante estar alineados en la estrategia de prevención de ataques y estar en la vanguardia con herramientas de control vigentes aplicables a la industria OT.

Varios de los problemas existentes están en las malas configuraciones y el uso de credenciales por defecto, que es un punto crítico el hecho de no cambiarlas luego que los sistemas son implementados, deben ser entregados al área de seguridad informática para que tome curso del procedimiento de cambio de contraseñas y resguardar las nuevas credenciales

con herramientas seguras de procesos de ensobrado y workflow de aprobaciones antes requerimientos de aperturas para su acceso. (García, 2019)

3.5.2. Aspectos de la seguridad

Para la convergencia con dispositivos heredados y nuevos diseños técnicos funcionales se detalla el nivel de requerimientos deseado para contemplar el uso de protocolos de comunicación seguros de los ERP y aspectos de seguridad de programas, transacciones y tablas desarrolladas.

Programas: Todo programa ejecutable debe poseer sentencias de autorización incluidas en su código fuente ABAP, que posibiliten limitar el uso de la transacción asociada. Se debe asignar grupo de programa a los desarrollos para que un usuario solo pueda acceder a los grupos de programas asignados en su perfil.

Se deben incluir authority-checks, que son objetos de autorización con sus correspondientes campos y valores, controlados en el código de la transacción y asociados al programa para limitar la tarea de ejecución por sí mismo. Hacer uso de los objetos de autorización asociados a la funcionalidad que el programa lleva a cabo, creando una transacción asociada al programa.

Transacciones: Toda transacción desarrollada debe tener un objeto de autorización opcional habilitado que limite el acceso a la misma.

Por medio de transacciones se agregan los objetos de autorización correspondientes de forma que los mismos puedan ser propuestos automáticamente durante el mantenimiento de los roles de usuario.

Tablas: Toda nueva tabla creada requiere complementariamente que se apliquen los pasos detallados para permitir la correcta gestión de accesos sobre la misma. Agregar un grupo de tabla a utilizar por los existentes siempre que sea posible. Si la nueva tabla no guarda relación con los grupos de tablas construidos en el sistema se deberá crear uno nuevo y asociarlo a la tabla acorde a la nomenclatura solicitada por el modelo estándar.

Asociar la transacción para vista de actualización y si la tabla requiere interacción directa de parte del usuario deberá crearse adicionalmente una transacción que permita su consulta o

modificación según corresponda mediante la validación de los objetos asociados. (Camara, 2012)

3.5.3. Políticas de prevención

Promover la utilización de mecanismos de encriptación para la gestión de interfaces.

Solicitar el consentimiento de la organización para cualquier actividad que requiera accesos de terceros o intervenciones externas más allá de las personas que integran el convenio de servicios.

Mantener el debido cuidado profesional sobre cualquier información proporcionada para el desarrollo de las funciones.

Aplicar en la metodología de trabajo, las mejores prácticas de seguridad del mercado enmarcadas dentro de las normas ISO 27001.

Ante los controles de acceso inadecuados, se debe contar con comprobaciones de control de accesos, políticas de contraseñas con doble factor de autenticación y monitorización para análisis del comportamiento de los usuarios.

Para el caso de los desarrollos de software se deben tener control de la seguridad en las transacciones y con separación de entornos en ambientes de desarrollo (DEV), pruebas (QAS) y producción (PRD).

Tener el análisis, escaneo y corrección de código con vulnerabilidades y planificación de parches para las correcciones.

Coordinación y evaluación de vulnerabilidades, con pruebas de penetración o evaluación de seguridad perimetral.

Monitorización continua de los problemas de seguridad con análisis en profundidad de la configuración y programa de gestión de vulnerabilidades con análisis de riesgos y soluciones. (WisePlant, 2019)

3.6. Vulnerabilidades

En el mundo de IT, la gran mayoría de los ataques cibernéticos se lanzan al explotar vulnerabilidades en los sistemas de software. Los especialistas en seguridad informática reconocen la necesidad de actualizar las redes para detectar vulnerabilidades conocidas y aplicar parches de software autorizados. De esta forma es posible que se elimine la vulnerabilidad y que el riesgo sea mitigado. Sin embargo, en muchos procesos industriales existen varios obstáculos a considerar para la aplicación de parches.

En primer lugar, en los sistemas críticos, los parches solo pueden aplicarse en ventanas de mantenimiento específicas durante períodos donde los procesos pueden interrumpirse con tiempo autorizado según la exigencia de otros problemas que requieren mantenimiento, significando que los parches puedan retrasarse o no aplicarse.

En segundo lugar, en los sistemas antiguos que funcionan de forma continua durante largos períodos de tiempo, se evita realizar cambios, debido a que cualquier interrupción, provoque alguna modificación y luego el sistema no comience de nuevo.

En tercer lugar, antes de que se aplique un parche, debe ser aprobado y verificado, ya sea por el proveedor, el referente de OT o ambos. En el mundo de IT, los parches normalmente se prueban en un laboratorio o en una red de test. En el mundo industrial de OT, esto no es tan simple de hacer, poder recrear un sistema verdaderamente representativo en el que medir el impacto de cualquier parche representa un desafío significativo.

En estas circunstancias, se convierte en una compensación de riesgos. Donde se cuestiona, cuál es el mayor riesgo, de que un sistema no actualizado sea atacado por un malware, frente al riesgo de que en un sistema si actualizado, su algoritmo sea alterado con modificación de las distintas variables y su configuración. Los sistemas ERP también se puede ver afectados por vulnerabilidades y nuevos ataques, que pueden venir desde el exterior o desde el interior de la organización, por tal razón se debe contar con las medidas de prevención y aplicación de buenas prácticas para el diseño de módulos de programas por acciones requeridas de los aspectos de control y seguridad para resguardo de la información. (WisePlant, 2019)

3.6.1. Análisis de incidentes

Con el análisis obtenido en función de la línea de investigación realizada en el marco de las redes OT y redes IT y basándonos en incidentes registrados en la base de datos de ciberseguridad, y tomando como referencia las evidencias y las fallas de no contar con controles por acción crítica y segregación de funciones, se presentará la recuperación de un sistema ERP que fuera sometido a un ciberataque dentro de la red IT.

Se detallará el paso a paso de la recuperación de un sistema ERP de la tecnología SAP, donde se instala el servidor de aplicación en una red de laboratorio y aplicando las buenas prácticas de seguridad de SAP se procederá a su instalación con método de backup – restore de la base de datos e instalación según guía oficial del ERP. (RISI, 2015)

3.6.2. Simulación ERP

Para la recuperación del sistema ERP, se debe contar con el manual de las buenas prácticas que se detalla a continuación y en el próximo capítulo se presenta el caso de la simulación del restore de un sistema ERP, que fue desarrollado en un ambiente de laboratorio con recursos virtuales sobre plataforma VMware ESXI, con servidor de aplicación, datastore con la base de datos y binarios de ejecución “sapinst”, para instalación del sistema SAP ERP. (García, 2019)

1. Contar con backup full de ambientes SAP de forma periódica.
2. Configuración de red y evaluación de arquitectura de Landscape.
3. Seguridad del sistema operativo donde se implementa SAP.
4. Contar con la seguridad aplicativa de SAP NetWeaver.
5. Evaluación interna del control de acceso.
6. Evaluación de componentes como SAP portal, Saprouter y SAP GUI.
7. Cambio y evaluación del procedimiento de transporte.
8. Evaluación del cumplimiento de los estándares SAP.
9. Aplicación de notas según componentes y módulos.

10. Licenciamiento adecuado según funcionalidades.

4. Datos Experimentales

4.1. Presentación

En este capítulo se presenta el proceso de instalación y puesta en funcionamiento de un sistema ERP SAP junto con los hallazgos presentados. Los datos experimentales se presentan conformando una matriz de riesgos en los sistemas ERP y los riesgos que ocurren sin tener controles periódicos y revisión de procesos con control interno y auditorías de seguridad informática.

4.2. Preparación de servidor

Escenario de trabajo: Sistema ERP SAP ECC 6.0 con base de datos SQL Server 2008 R2 y sistema operativo Windows Server 2008 R2 Standard sobre plataforma virtual VMware ESXI 6.0. (SAP, 2018)

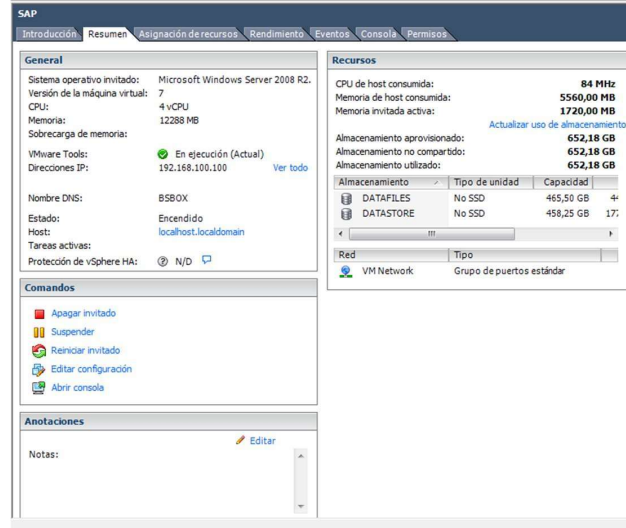


Figura 5. Configuración host virtual

4.2.1. Especificaciones

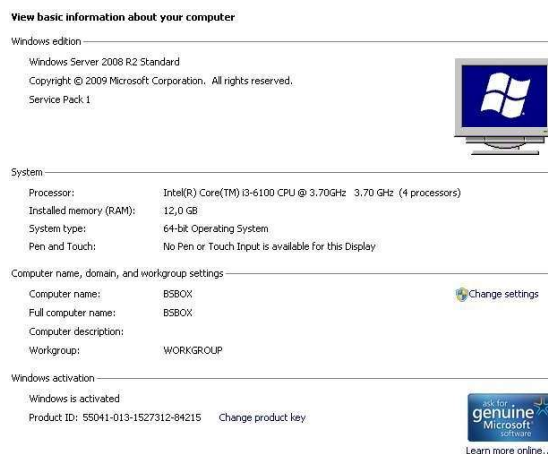


Figura 6. Especificaciones del servidor

4.2.2. Configuración de firewall

Windows Event Collector	This service manages persistent subscriptions t...		Manual
Windows Event Log	This service manages events and event logs. I...	Started	Automatic
Windows Firewall	Windows Firewall helps protect your computer ...		Disabled
Windows Font Cache Service	Optimizes performance of applications by cachi...		Manual
Windows Installer	Adds, modifies, and removes applications provi...		Manual
Windows Management Instrumentation	Provides a common interface and object model ...	Started	Automatic
Windows Modules Installer	Enables installation, modification, and removal ...	Started	Manual
Windows Presentation Foundation Font C...	Optimizes performance of Windows Presentati...		Manual

Figura 7. Configuración firewall

4.2.3. Administración de usuarios

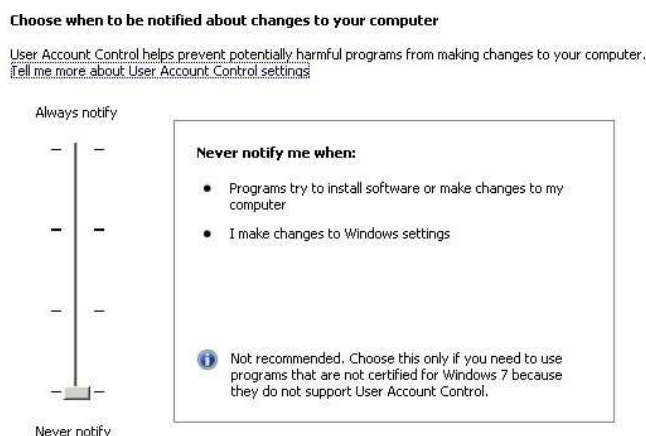


Figura 8. Administración de usuarios

4.3. Requisitos y componentes

4.3.1. Plataforma java

Una vez instalado normalmente, va a generar una carpeta en el C:\jdk1.4.2_17-x64

Esta carpeta hay que configurarla como variable de entorno JAVA_HOME

Start >> Click derecho en computer >> properties >> advanced system settings >> advanced >> environment variables...

En “system variables” >> new...



Figura 9. Variable de entorno

Sobre “path” clic en -> edit.

Agregar “;C:\jdk1.4.2_17-x64\bin”

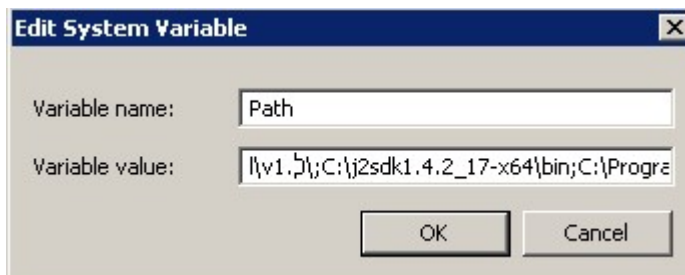


Figura 10. Sistema de variable

Versión actual de java

Ejecutar >> cmd >> **java -version**

```
C:\Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\sapinst>java -version
java version "1.4.2_17"
Java(TM) 2 Runtime Environment, Standard Edition (build 1.4.2_17-b06)
Java HotSpot(TM) 64-Bit Server VM (build 1.4.2_17-b06, mixed mode)

C:\Users\sapinst>_
```

Figura 11. Java version

4.3.2. SQL server

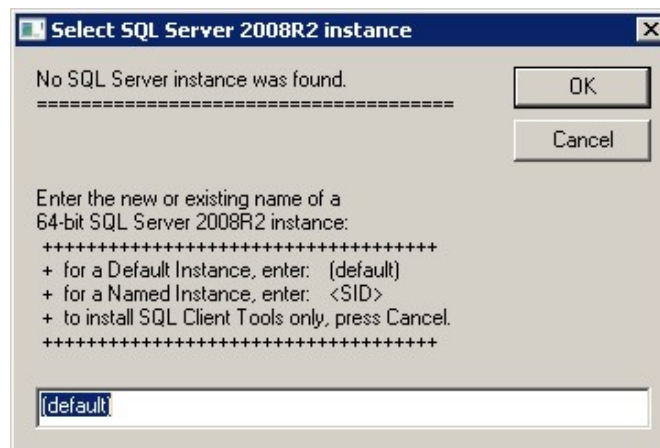


Figura 12. Instalar DB SQL

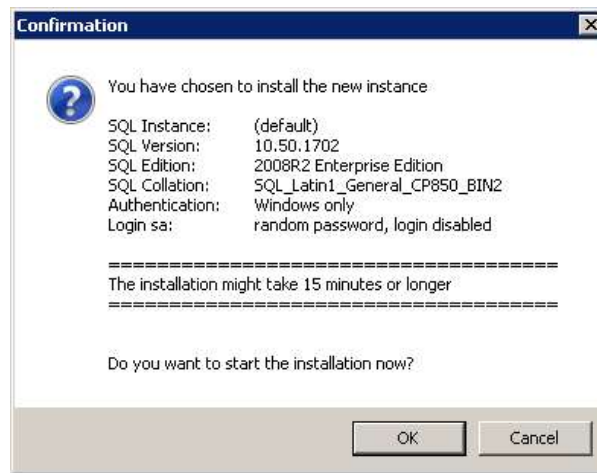


Figura 13. Confirmación de instalación



Figura 14. Instalación en curso

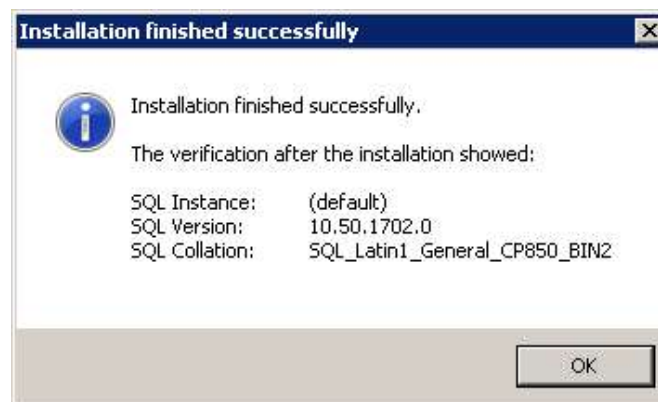


Figura 15. Instalación SQL completada

4.4. Restore ERP

4.4.1. Pre-requisitos

Welcome to SAP Installation Master

Before starting the installation, make sure that you have ide

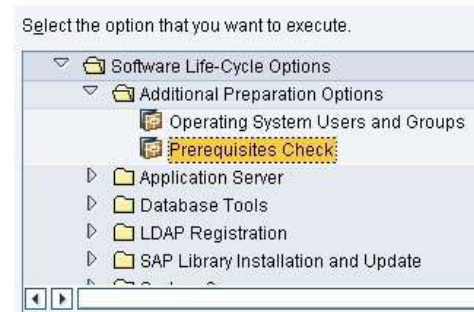


Figura 16. Chequeo pre-requisitos

Task Progress

The task has been completed successfully.

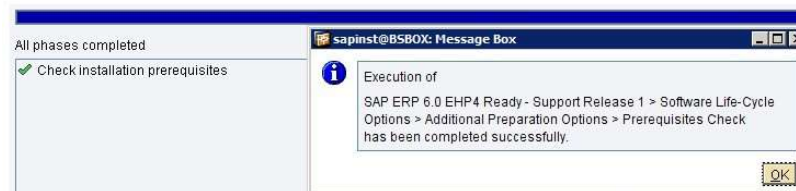


Figura 17. Progreso de ejecución

4.4.2. Inicio de instalación

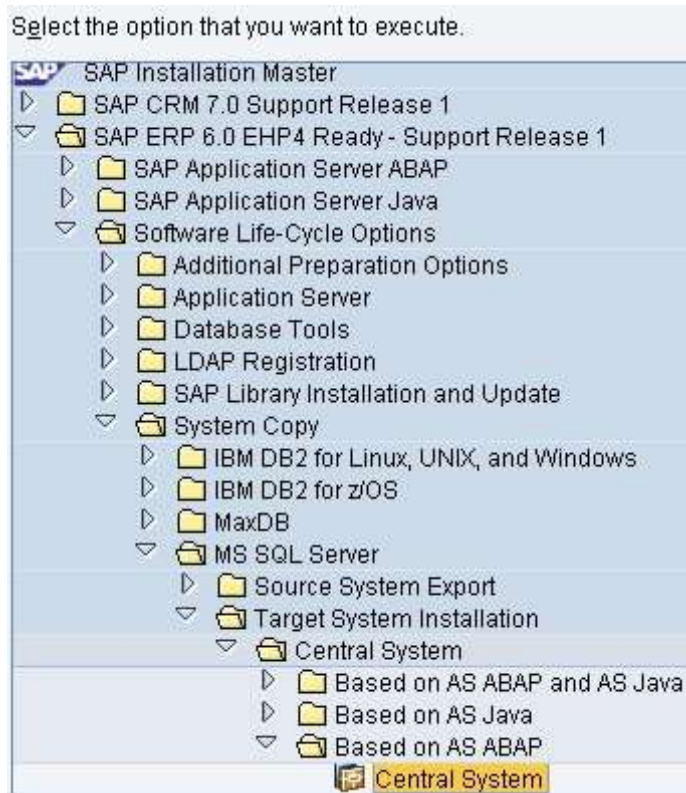


Figura 18. Iniciar instalación

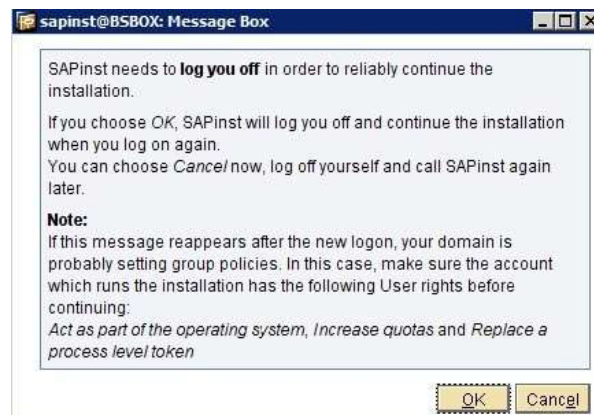


Figura 19. Nota de instalación

Enter the system ID and installation drive



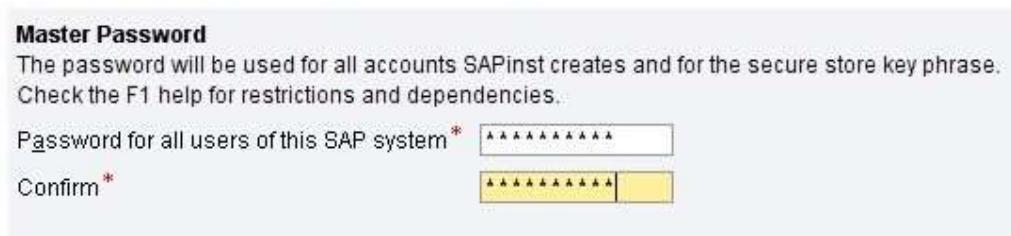
SAP System Parameters

SAP System ID (SAPSID)*

Installation Drive 

Unicode System (recommended) ☒

Figura 20. Parámetros SID



Master Password

The password will be used for all accounts SAPinst creates and for the secure store key phrase. Check the F1 help for restrictions and dependencies.

Password for all users of this SAP system*

Confirm*

Figura 21. Claves maestras

Select the database installation method



Database Installation

Installation Method

☐ Standard System Copy / Migration (load-based)

☒ Homogeneous System Copy (MS SQL Server-specific: Detach/Attach or Backup/Restore)

Start Migration Monitor manually ☐

Figura 22. Copias homogéneas

Enter the MS SQL Server instance name.



Database Connection

Local MS SQL Server Instances 

Additional Information

Make sure that your database is running. The database server cannot be started without MS SQL Server for this installation type.

Figura 23. Conexión de base de datos

MS SQL Server > Database Schema

Enter the password of the SAP database schema.

Database Schema

MS SQL Server login and user: *box*

Password of ABAP Schema *

Confirm *

Figura 24. Esquema base de datos

Central Instance Parameters

Central Instance Number *

Additional Information

The *Instance Number* for the central host.

Figura 25. Número de instancia

SAP System > Central Instance

Enter the central instance parameters

Central Instance Parameters

ABAP Message Server Port

Internal ABAP Message Server Port

Host with Transport Directory *

Additional Information

The instance-specific *Internal ABAP Message Server Port*

Figura 26. Instancia / parámetros

SAP System > SAP Cryptographic Software

Provide the path to the SAP Cryptographic Library

Prepare SSL Activation

Install the SAP Cryptographic Library ☒

Path to SAPCRYPTO.SAR *

C:\INSTALL\SAPCRYPTOLIB\90000114.SAR

Additional Information

The *SAP Cryptographic Library* is required to enable Secure Sockets Layer (SSL) encryption from <http://service.sap.com/swdc> -> Download -> *SAP Cryptographic Software*.

Figura 27. SAPCryptolib

SAP System > DDIC Users

DDIC Users in SAP System Clients

Account: *DDIC*, client *000*

Password of 'DDIC' in client 000 in the source system *

Additional Information

SAPinst needs to create an RFC connection to the system that you are installing.

A *SAP System Client* is a self-contained unit in an SAP system with separate master

Figura 28. Usuario de sistema

SAP System > Cryptographic Library

Choose the cryptographic library that you want to install for this system

Cryptographic Library

The specified archive contains multiple versions of the SAP cryptograp

Install	Library Path Inside Archive
☒	nt-x86_64/sapcrypto.dll

Figura 29. Cryptographic

Choose Option Define Parameters

Task Progress

Running phase: Install common system files

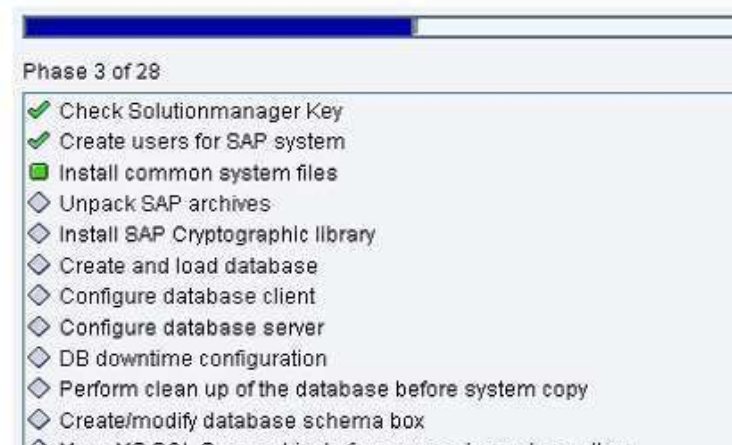


Figura 30. Progreso de instalación

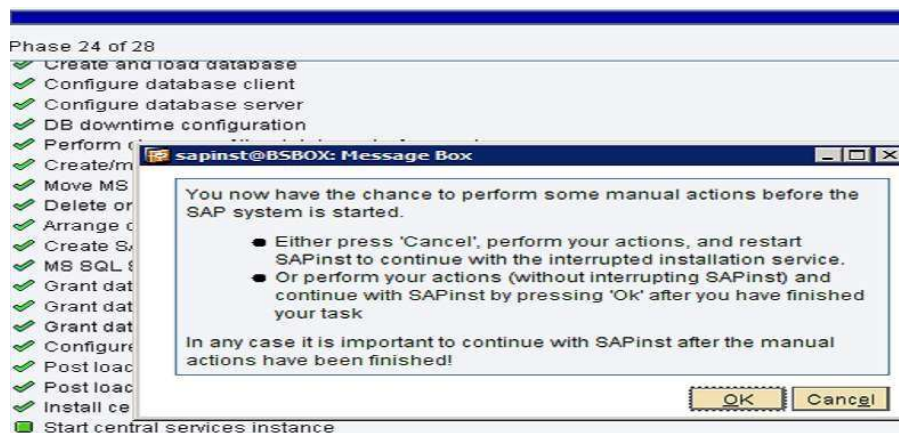


Figura 31. Opciones de instalación

4.4.3. Actualización kernel



Figura 32. Kernel

4.4.4. Finalización de instalación

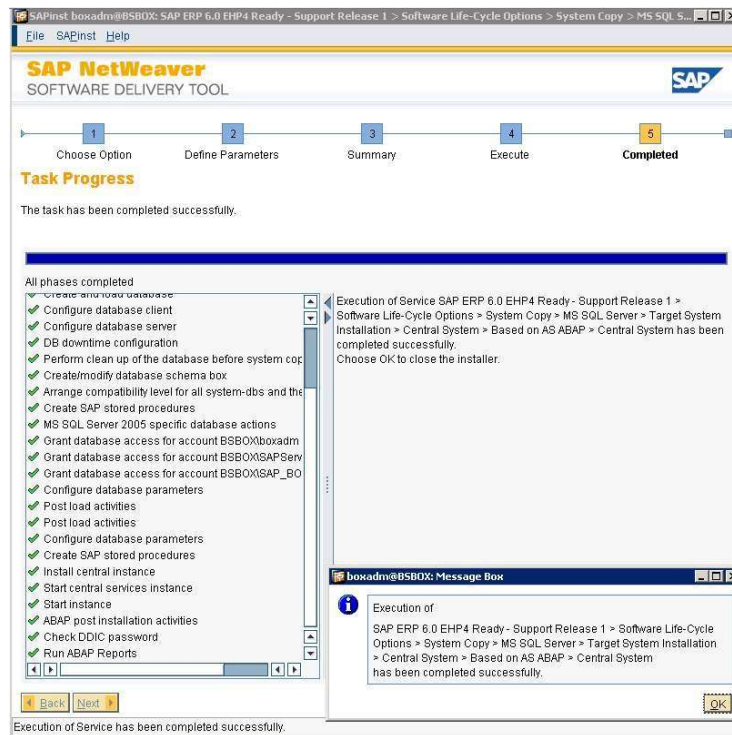


Figura 33. Instalación completa

4.5. Post - instalación

Luego de completada la instalación del SAP ERP ECC 6.0 se deben ejecutar tareas desde la aplicación GUI previamente configurada con los datos de conexión a la instancia.

Para tener la aprobación de la post - instalación se presenta la matriz de riesgos de SoD donde se realizan las mediciones de los procesos y ejecutan los controles mitigantes ante los riesgos planteados en caso de segregación funcional o acciones críticas anteriormente detalladas.

Luego de los controles y revisión de seguridad informática, se avanza con la puesta a punto de la configuración para conectar a los usuarios nuevamente y acceso de la red de negocio. Realizado esto, se da disponibilidad a los usuarios al sistema recuperado en ambiente de producción. (SAP, 2018)

4.6. Detalle teórico matriz SoD

En función de la matriz de SoD (Segregation of duties) o segregación de funciones definida en la “*Tabla 1*”, el sistema identifica los riesgos de accesos presentes en los usuarios, roles y perfiles del sistema gestionado. Es posible realizar dicho análisis tanto online como offline, y puede efectuarse a pedido (cuando el usuario lo desee), o bien programarse como proceso de fondo. Luego de que el sistema determina los conflictos, el administrador puede remediar o mitigar los accesos observados.

Son los controles utilizados para mitigar riesgos informados, por ejemplo, para mitigar un riesgo de acceso con un control automático válido es la configuración de un registro de doble nivel de firma en las estrategias de liberación en las órdenes de compras.

A continuación, se presenta la tabla 2 donde se puede visualizar una matriz de riesgos en la cual se pueden observar los distintos procesos de finanzas que agrupados en funciones forman diferentes riesgos.

Tabla 2. Detalle de SoD

#	LEV	ID RISK	RIESGO	FUNC 1	DESC FUNC 1	FUNC 2	DESC FUNC 2
C2	ALTO	ZF005	Actualizar cuenta bancaria contabilizar pago desde ella	ZAP01	Pagos AP	ZAP15	Actualizar datos maestros bancarios
C24	ALTO	ZP003	Crear factura de vendedor ficticio e iniciarle el pago	ZAP01	Pagos AP	ZAP02	Procesar facturas de vendedor
C43	ALTO	ZP038	Introducir pago no autorizado y realizar reconciliación bancaria	ZAP01	Pagos AP	ZAP14	Reconciliación bancaria
C3	ALTO	ZF006	Pagar una factura de vendedor y ocultar depreciación de activos fijos	ZAP02	Procesar facturas de vendedor	ZAP13	Actualizar documento de activo fijo
C31	ALTO	ZP014	Puede ocultar diferencias entre pagos bancarios y archivos AP contables.	ZAP02	Procesar facturas de vendedor	ZAP14	Reconciliación bancaria
C49	ALTO	ZP052	Crear factura de un vendedor ficticio e iniciar sus cheques manuales	ZAP02	Procesar facturas de vendedor	ZAP03	Tratamiento de verificación manual
C11	ALTO	ZF025	Actualizar cuenta bancaria y crearle cheques manualmente	ZAP03	Tratamiento de verificación manual	ZAP15	Actualizar datos maestros bancarios
C55	ALTO	ZP058	Crear un cheque manual y realizar reconciliación bancaria	ZAP03	Tratamiento de verificación manual	ZAP14	Reconciliación bancaria
C13	ALTO	ZF032	Actualizar cuenta bancaria contabilizar pago desde ella	ZAP04	Pagos AR	ZAP15	Actualizar datos maestros bancarios
C10	ALTO	ZF017	Actualizar cuenta bancaria y diferir pagos entrantes	ZAP05	Aplicación de caja	ZAP15	Actualizar datos maestros bancarios
C5	ALTO	ZF008	Ocultar efectivo depositado y diferencias de colecciones efectivo	ZAP05	Aplicación de caja	ZAP14	Reconciliación bancaria
C73	MEDIO	ZS012	Iniciar un pago creando memos. de crédito ficticias	ZAP04	Pagos AR	ZAP09	Tratar nota de crédito de cliente

C71	MEDIO	ZS010	Crear facturación y contabilizar pago de forma inapropiada	ZAP05	Aplicación de caja	ZAP08	Actualizar documentos de facturación
C78	MEDIO	ZS017	Autorizar crédito, modificar importe de efectivo recibido	ZAP05	Aplicación e caja	ZAP07	Gestión de créditos
C85	MEDIO	ZS026	Actualizar una factura e introducir o modificar pagos en ella	ZAP05	Aplicación de caja	ZAP10	Tratar facturas de cliente
C68	MEDIO	ZS006	Reinicializar saldo y modificar documento facturación al mismo cliente	ZAP06	Liquidar balance de cliente	ZAP08	Actualizar documentos de facturación
C88	MEDIO	ZS029	Crear una nota de crédito y reinicializar el cliente para incitar al pago	ZAP06	Liquidar balance de cliente	ZAP09	Tratar nota de crédito de cliente
C81	MEDIO	ZS022	Introducir facturas de ventas y autorizar límites de crédito	ZAP07	Gestión de créditos	ZAP10	Tratar facturas de cliente
C138	MEDIO	ZF012	Actualizar activos fijos y capitalizar o añadir costes a archivo maestro	ZAP12	Actualizar documento de activo fijo	ZAP13	Actualizar maestro de activos fijos

4.7. Resultados y hallazgos

En caso de no contar con los controles adecuados, los riesgos se trasladan automáticamente al sistema SCADA. Y serán los nuevos riesgos de los sistemas productivos, por lo tanto es requisito tener los controles mitigantes con las evidencias adecuadas.

Las industrias suelen enfocarse en lograr la mayor productividad sin contemplar problemas de ciberseguridad y al estar las redes aisladas, el hecho de conectar los sistemas IT con OT, genera nuevas oportunidades como también posibles riesgos y vulnerabilidades.

Las soluciones cerradas, los protocolos y lenguajes específicos, durante años fueron parte de las operaciones industriales, como un mundo desconocido y totalmente aislado de las

tecnologías de información.

A medida que en la Industria 4.0 fueran aumentando los datos para la toma de decisiones, las tecnologías como el big data y el internet de las cosas, coincidieron para mejorar la gestión y monitoreo de los procesos en las líneas productivas.

Todos los cambios generaron grandes ventajas hacia el mundo de industria 4.0, permitiendo a la operación de los equipos industriales sin importar la distancia geográfica.

Esto generó que la ciberseguridad sea un tema importante en el manejo del tráfico de datos entre las redes IT a las redes OT, para la búsqueda de amenazas que pueden estar presentes o que podrían causar algún gap de disponibilidad, y significar pérdidas millonarias en la industria si no se cuenta con medidas de seguridad. (García, 2019)

En función de la matriz de SoD (Segregation of duties) o segregación de funciones definida en la “*tabla 2*”, el sistema identifica los riesgos de accesos presentes en los usuarios, roles y perfiles del sistema gestionado. Es posible realizar dicho análisis tanto online como offline, y puede efectuarse a pedido (cuando el usuario lo desee), o bien programarse como proceso de fondo. Luego de que el sistema determina los conflictos, el administrador puede remediar o mitigar los accesos observados.

Son los controles utilizados para mitigar riesgos informados, por ejemplo, para mitigar un riesgo de acceso con un control automático válido es la configuración de un registro de doble nivel de firma en las estrategias de liberación en las órdenes de compras.

Conclusiones

En este trabajo, se estudiaron los mundos de IT y OT, donde se examinaron y analizaron los beneficios y problemas que surgen a través de la convergencia de la interconexión en las redes de la Industria 4.0.

Reconociendo qué las principales preocupaciones de seguridad son diferentes, confidencialidad en IT y disponibilidad en OT, ambas son amenazas que se presentan si no se cuenta con buenas políticas de seguridad y una adecuada definición de la matriz de riesgos.

Esta matriz se utiliza para identificar los riesgos inherentes a las actividades de una empresa, tanto de los procesos como de la fabricación de productos y administración de servicios. Es la herramienta para optimizar el control y mitigación de conflictos en conjunto con las normas vigentes de la seguridad de una organización.

La ciberseguridad en la mayoría de las industrias se desarrolla de manera aislada e independiente en cada rubro y sector, dejando en muchas situaciones la configuración librada a los expertos de cada tecnología.

Ante la necesidad de la continuidad del negocio o bien por desconocimiento luego de una implementación SCADA se deja para una segunda etapa, pocas veces desarrollada, la aplicación de políticas con un plan de seguridad establecido para los sistemas de redes OT.

De los resultados obtenidos, se puede resaltar la creciente demanda de seguridad en las redes OT y sistemas ERP, debido a que, en la última década, los sistemas industriales pasaron a ser el foco de ataques y víctimas de un nuevo escenario a nivel mundial.

Para evitar que los atacantes pongan en peligro los sistemas de gestión, se requiere contar con un enfoque global de la seguridad, pero pocas veces existe una clara dirección de la organización para las políticas de prevención de ciberataques a las infraestructuras críticas y el funcionamiento de los sistemas ERP. Este método requiere tener en cuenta todas las capas protegidas de la misma manera, ya que la falta de seguridad de una capa podría poner en peligro la seguridad de todo el sistema de la organización.

La necesidad de establecer verdaderas políticas de seguridad constituye a las operaciones industriales de redes SCADA en convergencia con los sistemas de gestión ERP.

Líneas Futuras de Investigación

En este trabajo final se investigó la interconexión de redes SCADA con sistemas ERP SAP, donde se experimentaron casos de convergencia con potenciales vulnerabilidades ante la aplicación de políticas débiles de seguridad informática.

Una futura línea de investigación sería la de estudiar en profundidad aspectos puramente de ciberseguridad entre los ERP y los SCADA. Donde el impacto de las tecnologías IoT sobre sensores basados con comunicación y procesamiento propio, carecen de medidas de seguridad pudiendo generar fallas en la red industrial.

Otra futura línea de investigación podría consistir en estudiar la convergencia de redes SCADA con otros sistemas ERP como Odoo, Geinfor o Softland.

Bibliografía

- Aguilar, J. P. (2017). *CiberSeguridad en Redes Industriales*. Obtenido de <https://www.scribd.com/document/354626790/Ciber-Seguridad-en-Redes-Industriales-pdf>
- Anabalón, J. (2014). *Seguridad en Sistemas SCADA un Acercamiento Práctico a Través de EH e ISO 27001:2005*. Santiago, Chile: MonkeysLab Research. Obtenido de https://www.researchgate.net/publication/324918959_Seguridad_en_Sistemas_SCADA_un_Acercamiento_Practico_a_Traves_de_EH_e_ISO_270012005
- Ardita, J. C. (2016). *Los desafíos de la ciberseguridad y la ciberdefensa*. Buenos Aires: CYBSEC. Obtenido de http://www.cybsec.com/upload/Ardita_Arias_Segurinfo_AR_2016_Ciberseguridad.pdf
- Baretto, J. F. (2017). *La Defensa Nacional y la Estrategia Militar de Seguridad Cibernética*. Escuela Superior de Guerra Conjunta, Buenos Aires.
- Camara, J. G. (2012). *Seguridad Y Auditoría Aplicadas en los ERP*. Leganes. Obtenido de https://e-archivo.uc3m.es/bitstream/handle/10016/16805/PFC_Javier_Garcia_Camara.pdf?sequence=1&isAllowed=y
- Carrasco, A. V. (2013). *Una visión global de la ciberseguridad de los sistemas de control*. España: S2 Grupo.
- Ercoli, C. E. (2017). *Control de Accesos en Sistemas ERP*. Buenos Aires: UBA. Obtenido de http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1192_ErcoliCE.pdf
- Franklin, F. R. (2016). *Políticas de seguridad en los Sistemas SCADA*. Colombia. Obtenido de <http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2983/Trabajo%20de%20grado1484.pdf?sequence=1>

- García, G. C. (2019). *Jornada de Ciberseguridad*. Madrid: Uni. Obtenido de <https://otdingenierosindustrialescv.com/wp-content/uploads/2019/05/JORNADA-CIBERSEGURIDAD-Colegio-de-Ingenieros-Industriales.pdf>
- Grupo, Z. (2017). *El impacto de los ERP en la industria de producción*. Extremadura. Obtenido de https://www.elperiodicoextremadura.com/noticias/sociedad/impacto-erp-industria-produccion_1059759.html
- IEEE. (2020). *Created by The Institute of Electrical and Electronics Engineers*. IEEE Taxonomy. Obtenido de <https://www.ieee.org/content/dam/ieee-org/ieee/web/org/pubs/ieee-taxonomy.pdf>
- Intellymation. (2019). *Soluciones Tecnológicas para la Industria*. Buenos Aires. Obtenido de <http://www.intellymation.com.ar>
- ISACA. (2006). *Estandar de Auditoria Seguridad Informática*. Information Systems Audit and Control Association.
- Kamlofsky, J. (2015). *Un Enfoque para Disminuir los Efectos de los Ciber-ataques a las Infraestructuras Críticas*. Buenos Aires: CAETI - Universidad Abierta Interamericana. Obtenido de <http://imgbiblio.vaneduc.edu.ar/fulltext/files/TC121046.pdf>
- Langner, R. (2013). *A Technical Analysis of What Stuxnet's Creators Tried to Achieve*. Munich: The Langner Group. Obtenido de <https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf>
- Lecuit, J. A. (2019). *Hacia la fusión entre la ciberseguridad industrial y los sistemas de información corporativos*. Madrid: Elcano. Obtenido de http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ciberseguridad/ari6-2019-lecuit-hacia-fusion-entre-ciberseguridad-industrial-y-sistemas-informacion-corporativos
- López, J. F. (2015). *Amenazas en los sistemas SCADA*. Madrid. Obtenido de https://cybercamp.es/cybercamp2015/sites/default/files/contenidos/material/cybercamp_amenazasscada.pdf

- Masoero, P. (2015). *Estado del Arte de sistemas ERP*. Universidad de San Andrés. Buenos Aires: UBA. Obtenido de <http://repositorio.udesa.edu.ar/jspui/handle/10908/2739>
- Ponce, A. A. (2017). *Ciberseguridad en Infraestructuras Críticas de Información*. Buenos Aires: Universidad de Buenos Aires. Obtenido de http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1115_AguirrePonceAA.pdf
- RISI. (2015). *Risidata.com/Database*. New York: RISI. Obtenido de <https://www.risidata.com/index.php?/Database>
- SAP. (2018). *Installation Guide PUBLIC Software Provisioning Manager 1.0*. SAP. Obtenido de https://help.sap.com/doc/49fcf0c674191014b16dce901bb0590d/CURRENT_VERSION/en-US/NW70X_inst_abapjava_win_sql.pdf
- Secure, I. (2019). *Convergencia de Redes IT y OT*. Madrid.
- Souppaya, M. (2013). *Guide to Enterprise Patch Management Technologies*. New York. Obtenido de <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf>
- TechNocio. (2020). *COVID-19 El disfraz de moda entre ciberatacantes*. Obtenido de <https://technocio.com/covid-19-el-disfraz-de-moda-entre-ciberatacantes/>
- Trend. (2019). *Industria 4.0 Automatismo por niveles*. Buenos Aires.
- Trend, M. (2020). *Phishing Activity Trends Report*. Granada, España. Obtenido de https://www.trendmicro.com/es_es/business/products/all-solutions.html
- WisePlant. (2019). *Ciberseguridad Industrial e infraestructuras críticas*. Florida. Obtenido de <https://wiseplant.com/>