CONVERGENCIA DE SEGURIDAD EN SISTEMAS DE TECNOLOGÍAS OPERACIONALES Y TECNOLOGÍAS DE LA INFORMACIÓN

CAMILO ANDRES OSPINA ARDILA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTACIA
UNAD
ESCUELA CIENCIAS BASICAS TECNOLOGIAS E INGENIERIA

ESPECIALIZACION EN SEGURIDAD INFORMATICA
MEDELLIN
2019

CONVERGENCIA DE SEGURIDAD EN SISTEMAS DE TECNOLOGÍAS OPERACIONALES Y TECNOLOGÍAS DE LA INFORMACIÓN

CAMILO ANDRES OSPINA ARDILA

Monografía sobre Convergencia de Seguridad en Sistemas IT a OT para otorgar el título de Especialista en Seguridad Informática

Director
Ingeniero John Fredy Quintero

UNIVERSIDAD NACIONAL ABIERTA Y A DISTACIA
UNAD
ESCUELA CIENCIAS BASICAS TECNOLOGIAS E INGENIERIA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
MEDELLIN
2019

Nota de Aceptación:

_____
_____
_____
_____
_____
_____
_____

_____
Firma del presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Medellín, 22 de agosto, 2019

Dedicatoria

_____
_____
_____
_____
_____

_____
_____
_____
_____

Agradecimientos

TABLA DE CONTENIDO

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

GLOSARIO

OT**:** Tecnología Operacional, infraestructura de los procesos industrializados, compuesta por elementos componentes lógicos que controlan sensores e integran múltiples plataformas de control a través de protocolos como el SCADA.

IT: Tecnología de la Información, buenas prácticas y procedimientos enfocados en el servicio con infraestructura tecnológica para el manejo de los servicios de información, el procesamiento, almacenamiento y transporte de información.

Convergencia: lugar donde se genera una unión.

MSPI: modelo de seguridad y privacidad de la información el cual fue decretado por MINTIC para que sea acogido por las Empresas del sector público.

LAN: redes de área local.

WAN: redes de área amplia.

Riesgo: probabilidad que se materialice una amenaza.

PLC: controlador lógico programable.

HMI: Interfaz usuario máquina.

SACADA: software en ordenadores que permite supervisar y controlar procesos

Industriales.

OSI: modelo de interconexión de sistemas abiertos, opera como referencia para los

protocolos de red.

ERP: sistema de planificación de recursos empresariales.

ISO 27001-2013: norma para los sistemas de gestión de seguridad de la

información en las organizaciones.

Criptografía: técnicas de cifrado y encriptado de la información para hacerla

inteligible a personas no autorizados a la misma.

PHVA: estrategia cíclica que permite planear, hacer, verificar y actuar en los procesos empresariales.

Amenaza. probabilidad latente de que ocurra un hecho de peligro.

Tecnología: ciencia aplicada a la resolución de problemas concretos.

Seguridad: ausencia del riesgo, estado de tranquilidad.

IoT: internet de las cosas.

Big Data: conjunto de datos masivos en alto volumen.

Vulnerabilidad: debilidad o falló en un sistema de información.

MAC: Médium Access Control, se encuentra ubicado en la capa dos del modelo

OSI.

Confidencialidad: la información solo debe ser accedida por personal autorizado.

Integridad: preservar el contenido de información generada.

Disponibilidad: disponer y acceder a la información en el momento que se requiera, desde los lugares destinados para tal fin.

ICS: Sistemas de Control Industrial.

RESUMEN

Con el avance tecnológico y el crecimiento de la industria, los sistemas, llamados Tecnologías Operacionales (OT), han traído consigo infinidad de vulnerabilidades en los procesos, convirtiéndose así en una infraestructura crítica. Lo anterior, porque las OT han presentado un crecimiento desorganizado y carente de buenas prácticas para un control en los sistemas de información.

Por lo anterior, el presente documento describe un modelo que permite adoptar las buenas prácticas de las Tecnologías de la Información en sus modelos de seguridad, específicamente en el Modelo de Seguridad y Privacidad de la Información, con el cual se puede alcanzar un orden y mitigar los riesgos asociados a los sistemas de información de las operaciones, dando a conocer los puntos más importantes para implementar en los procesos industrializados que son críticos y que requieren de toda la seguridad posible.

El Modelo de Seguridad y Privacidad contiene guías que aplican para la convergencia y el control de los procesos de seguridad de la información, y los elementos de esta. Además, contiene herramientas para implementar dichas guías en tecnologías que requieren de un alto grado de confidencialidad, integridad y disponibilidad.

El Modelo de Seguridad y Privacidad de la Información está basado en la norma ISO27001-2013, la cual relaciona los requerimientos, controles y recomendaciones para la seguridad de la información, a través de la realización de planes y procedimientos estructurados con base en las necesidades de protección de información de los procesos de la empresa.

Palabras claves: Tecnologías operaciones, Tecnologías de la Información, convergencia, vulnerabilidades, redes, riesgo, integridad, confidencialidad, disponibilidad, amenaza.

INTRODUCCIÓN

Los procesos operacionales en muchas empresas dependen de equipos industriales, los cuales generan información. Esta información necesita ser cuidada y, por tanto, tratada de una manera segura. Por su parte, con el apoyo de las buenas prácticas de las Tecnologías de Información (IT), se generan soluciones informáticas que operan en infraestructura con altos estándares de servicio y manejo de los procedimientos que se desarrollan en arquitecturas tecnológicas con procesamiento de la información, solucionando necesidades del manejo de transacciones lógicas.

Las Tecnologías Operacionales son sistemas que vienen evolucionando y complementándose a través de la creación de nuevos enlaces, en este caso con los sistemas de información. Los sistemas de información son de suma importancia porque aportan unas buenas prácticas, tanto para el manejo de la información, como en la seguridad de esta.

La convergencia entre IT - OT en seguridad de la información ayudará a que los procesos operacionales sean más controlados y seguros, generando una cultura. Adicional a esto, la convergencia entre IT - OT permitirá que se genere confianza, dentro de la industria y en usuario final que recibe un producto o servicio.

Por otro lado, los sistemas industriales de control fueron diseñados y desarrollados, en primera instancia, para un manejo seguro y controlado mediante la utilización local. Sin embargo, con los años y la evolución de estos dispositivos, se hizo necesario contar con conexiones externas, las cuales tienen como consecuencia que la industria corra el riesgo de ser atacada. Por lo tanto, se requiere de un manejo de la información, que esté fundamentando en las buenas prácticas de seguridad de IT, frente a cada uno de los procesos en que se puede generar información importante y confidencial dentro de aquellas operaciones que son parte fundamental del negocio.

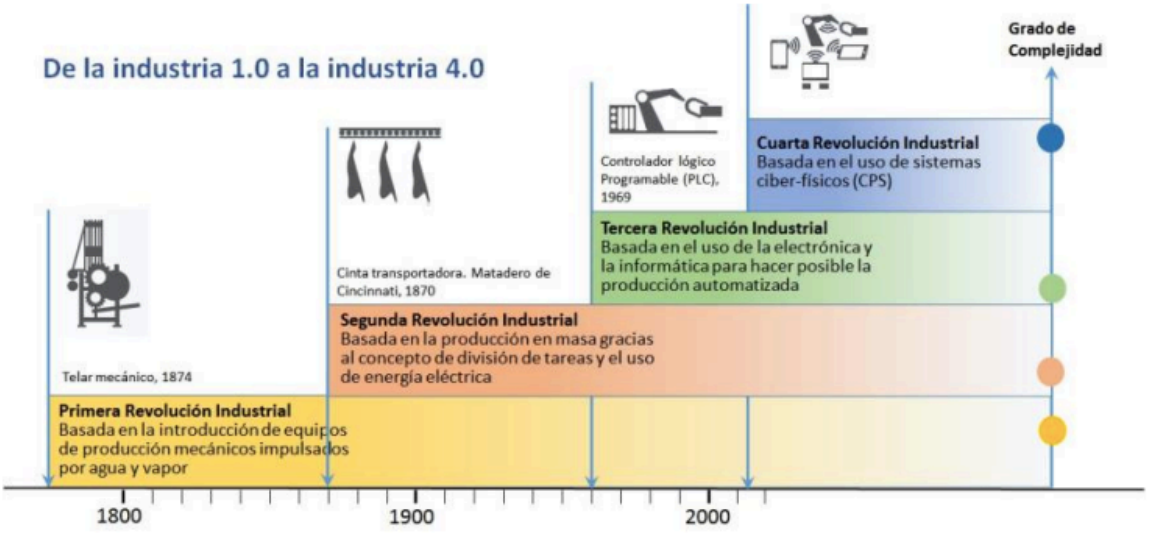
Para lo anterior, es necesario contar con plataformas tecnológicas, en las operaciones, que brinden disponibilidad, integridad y confidencialidad de los datos. Pues, los datos deben ser almacenados y custodiados de acuerdo con las recomendaciones y controles dados por la norma ISO27001-2013. Adicional a esto, los datos se deben procesar y tratar como un insumo generador de recursos para las empresas, pues son el resultado de un proceso productivo en las tecnologías operacionales.

Actualmente, servicios como el transporte, que en su evolución y necesidad de prestar un servicio con valores agregados y mantener al usuario conectado,

generaron otra oportunidad para los atacantes, los cuales buscan las vulnerabilidades en estos sistemas para el robo de información y/o el control de los dispositivos o sensores presentes en estas soluciones.

Según el portal Vitriko[1], en la actualidad se habla de los ataques a la industria 4.0, corresponde a la cuarta revolución industrial que se presenta por la relación y evolución de los componentes electrónicos, procesos y tecnologías, a través de comunicaciones entre máquinas, Internet de las cosas (IoT) y el manejo de la información. La evolución de la industria hasta la cuarta revolución industrial puede observarse en la Figura 1. Uno de los métodos para evitar los ataques masivos, hacia esta industria, consiste en acondicionar una red separada, es decir, sin conexión al exterior. Este método ha comenzado a perder valor, pues, actualmente, es una práctica frecuente, contar con un acceso a la internet desde los sistemas industrializados, para el control y monitoreo remoto, lo cual genera un alto riesgo para la información obtenida desde los procesos de producción.

Figura 1. Evolución de la Industria



Fuente: VAL ROMÁN, José Luis. Industria 4.0: la transformación digital de la industria. En: Coddiinforme, 2016, p. 3. Recuperado de http://coddii.org/wp-content/uploads/2016/10/Informe-CODDII-Industria-4.0.pdf

Entonces, aunque es más fácil operar con redes dedicadas a cada sistema, se genera la necesidad de accesos remotos, los cuales permiten mayor comodidad al

[1] VITRIKO, Smart Solutions for IoT. Ataques a la industria 4.0, 2016, párr.1. Recuperado de https://vitriko.eu/ataques-la-industria-4-0/

momento de realizar actualizaciones, soportes y mantenimientos. Muchas veces, los sistemas operacionales se encuentran por fuera del mapa de seguridad. Estos sistemas que se encuentran por fuera del mapa de seguridad son la opción más frecuentada para vulnerar las máquinas de producción industrial, consiguiendo acceso a elementos como PLCs, HMIs o SCADA, para así encontrar información de los sistemas y procesos, paralizarlos, robarlos o reprogramarlos, además de que a través de estas redes operacionales se puede acceder a los sensores, usados para atacar.

Para mitigar los riesgos asociados a las redes operacionales en los equipos o sensores de borde, es fundamental contar con la actualización de hardware y software, contar, además, con la posibilidad de herramientas como cortafuegos, antivirus, entre otras y con una buena segmentación de la red. Es fundamental, también, tener una conexión de todos los dispositivos entre sí, y controlar los usos, ingresos y estado de los dispositivos, ayudando así a disminuir la posibilidad de ser vulnerados. Además, las buenas prácticas de IT en OT son complemento para la operación sólida y certera en seguridad de la información.

La tecnología y los grandes logros industriales permiten que se generen complementos que facilitan los procesos, haciéndolos más rápidos, automatizándolos y volviéndolos seguros para el usuario que utiliza el producto final. Entonces, resulta incoherente no tener en cuenta estos complementos para mejorar los sistemas productivos de las empresas, además de enriquecerse de ellos para mantener la seguridad de la información y de las operaciones de la industria.

En el presente documento se encontrará, en primer lugar, la presentación del problema, el cual es principalmente la alta vulnerabilidad que presentan las Tecnologías Operacionales. Se encontrarán también los objetivos del documento, los cuales van orientados a solventar y mitigar el problema anteriormente expresado, junto con las razones que hacen fundamental el logro de estos objetivos.

En el primer capítulo del documento se encontrará información sobre el modelo OSI en redes industriales, modelo a través del cual, por medio de tres capas, se transmite información relevante, para el funcionamiento de la organización, de un equipo a otro, evitando riesgos y mitigando amenazas. Más adelante, en el segundo capítulo, se introducirá el tema de las Tecnologías Operacionales, haciendo hincapié en sus funciones dentro de la industria, además se mostrarán las buenas prácticas con las que las Tecnologías Operacionales cumplen frente a la seguridad de la información que manejan, dentro de esté capitulo se encontrará información sobre IoT, fundamental para comprender la evolución de OT durante los últimos años, y se encontrará también información sobre ICS.

En el capítulo tres se hará referencia a las Tecnologías de la Información y a las buenas prácticas de estas tecnologías que ayudan a toda la organización en sus

procesos tecnológicos y de información. Estas buenas prácticas son las fundamentales para comprender la convergencia IT-OT que se presentará más adelante.

La seguridad informática, entendida esta como un proceso que permite asegurar los recursos y procesos de la organización, se explorará en el capítulo cuatro junto con la seguridad física y lógica, fundamentales para la protección de la información que permite la productividad eficaz y eficiente de una empresa. En el capítulo cinco se expondrá el modelo de seguridad y privacidad de la información y la forma de evaluar al mismo cuando se aplica en alguna organización.

En el capítulo seis se expondrán las características y principales aplicaciones de la convergencia IT-OT, además se expondrán las razones que dan cuenta de la importancia de esta convergencia para la seguridad de una organización. Este capítulo sirve permite comprender algunos conceptos para entender de una manera más completa el capítulo siete, en el cuál se muestra el modelo de convergencia, con cada una de las recomendaciones y procedimientos que se deben seguir para llevar a cabo una buena gestión de la seguridad de la información y mantener la organización entre los estándares de calidad necesarios para sobresalir en el mercado. Finalmente, en el séptimo capítulo se comparte la arquitectura ideal para ejecutar el modelo planteado en el capítulo anterior.

PLANTEAMIENTO DEL PROBLEMA

Existen información en los medios, dada por el MINTIC y por algunos grandes empresarios colombianos, en la cual se asegura que en Colombia la tecnología de punta va cogiendo cada vez más fuerza dentro de las empresas, pues se tiene el objetivo de que, en el 2025, Colombia sea un referente digital. Es por esto por lo que "el país ha creado esfuerzos que buscan incentivar la apertura hacía tecnologías que garanticen el almacenamiento acertado de los datos, como también un llamado preventivo hacía la vulnerabilidad de estos." Estos esfuerzos por incentivar la apertura hacia tecnologías no se dan solo por cumplir el objetivo de ser un referente digital, sino que, "actualmente, para tener una transformación exitosa es necesario contemplar un protocolo y esquema de seguridad de recuperación en desastres previstos o no previstos, que garantice la continuidad del negocio, al igual que una columna vertebral como el centro de datos cuyo propósito sea ofrecer especificaciones críticas para una transformación exitosa sin importar el tamaño de la compañía".[2] Para lo cual es fundamental contar con tecnología de punta y buenas prácticas en el manejo de estas.

En los años 2015. 2016 y 2017, según afirma la viceministra de Economía Digital, Juanita Rodríguez[3], se ha dado un despliegue y masificación del acceso a infraestructura digital y de fortalecimiento de la industria TI. Lo cual permite el fortalecimiento de la conectividad, que puede considerarse como el principal eslabón en la cadena de digitalización.

"En ese contexto de grandes avances en materia de infraestructura, y con el fin de maximizar los beneficios del desarrollo de la economía digital en el país, el Gobierno ha creado el Viceministerio de Economía Digital en el Ministerio de Tecnologías de la Información y las Comunicaciones , con el fin de promover la economía digital en todas sus dimensiones."[4] Gracias a la creación de este viceministerio, es posible conocer datos como los que se presentan en la figura 2, los cuales muestran el porcentaje de empresas que, cuentan con protocolos para incidentes digitales, es decir, empresas que se le han apostado a la seguridad digital.

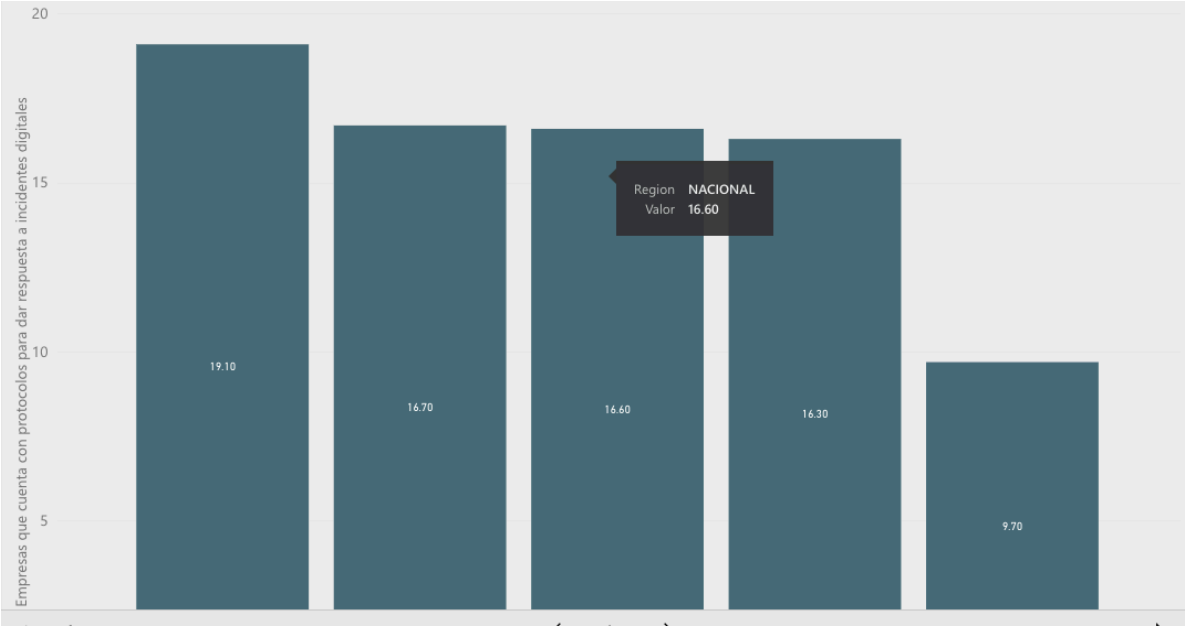
---

[2] MIER, Camilo, citado por PORTAFOLIO. Colombia se perfila a una infraestructura tecnológica de punta. En: Portafolio [online]. Octubre, 2018. Recuperado de https://www.portafolio.co/negocios/colombia-se-perfila-a-una-infraestructura-tecnologica-de-punta-522093

[3] RODRÍGUEZ, Juanita. Citada por DINERO. Analítica de datos, una de las tecnologías con más futuro en el 2018 en Colombia. En: Dinero [online]. Enero, 2018. Recuperado de https://www.dinero.com/emprendimiento/articulo/tendencias-de-tecnologia-mas-importantes-en-colombia/254681

[4] Ibíd., párr. 8

Figura 2. Empresas con protocolos para incidentes digitales



Fuente: COMISIÓN DE REGULACIÓN DE COMUNICACIONES. Indicadores de la economía digital en Colombia: Empresas con protocolos para incidentes digitales. 2016, Colombia. Recuperado de https://www.postdata.gov.co/landing/index

Son las grandes empresas las que lideran los avances digitales en Colombia, y las que pueden apostarle al uso de las tecnologías de punta, pues, según la revista Juanita Rodríguez[5], la transformación digital se limita a las empresas líderes grandes que buscan transformar mercados domésticos o necesitan insertarse en la economía mundial. Adicional a esto, para encajar entre en las empresas líderes de la transformación digital, es importante que se cuente con una buena estructura de costos y cadena de valor que permita que se beneficien más por la digitalización de procesos productivos (industrias en redes o con altos costos de transacción).

Por otro lado, el hecho de que sea dentro de las grandes empresas donde comienza a verse la transformación digital y la adopción de tecnologías de punta, se da porque "Las medianas, pequeñas y microempresas generalmente presentan una baja acumulación de capital intangible, definida como la baja capacitación de empleados para operar en el nuevo entorno digitalizado, una ausencia de cambios en procesos productivos para asimilar la tecnología, y una falta de restructuración organizativa."[6]

[5] Ibíd., párr. 12.
[6] Ibíd., párr. 10.

Entonces, según Garcés[7], gerente general de Intel Colombia, la formas más viable de adecuarse a la manera en que el mercado se está enfocando en la transformación que viene de los dispositivos, que son cada vez más inteligentes y están cada vez más conectados, es apostarle a la tecnología de punta, para optimizar costos y mejorar las habilidades de sus empleados y el servicio para sus clientes. Pues una de las ventajas que tiene es que brinda mayor productividad haciendo los procesos mucho más fáciles y rápidos.

> Me atrevo a decir que nos estamos acercando a la cuarta revolución industrial, que fusiona lo físico, lo biológico y lo tecnológico, lo cual genera un gran cambio en cómo el mundo y las empresas están operando. Y como en toda revolución lo que sucede es que la tecnología nos permite hacer cosas que antes nos tomaba mucho tiempo, pero es ahí donde cambia la composición de la fuerza laboral y debemos ser agradecidos con esto, no verlo como una amenaza.[8]

A pesar de lo anterior, muchas empresas industriales realizan procesos en su operación sin la seguridad y sin las prácticas de TI adecuadas para un correcto manejo de la información. Si bien, existen organizaciones que cuentan con tecnología de punta para la operación de sus múltiples sistemas y procesos, como se afirma en los anteriores párrafos, estás carecen de procedimientos que les ayuden a mejorar y controlar la información producida por los equipos y sensores utilizados en la producción. Esta carencia hace las empresas más vulnerables ante los ataques industriales, que cada vez son más y mejor elaborados. Lo anterior puede evidenciarse en el siguiente párrafo.

> Las informaciones publicadas en los últimos años sobre ataques a sistemas industriales revelan una situación creciente con más ataques dirigidos a los sistemas de control tal y como demuestra Symantec a través de sus informes Internet Security Threat Report, con un apartado dedicado en exclusiva a la ciberseguridad industrial. En el año 2012, McAfee afirmaba que los “atacantes suelen elegir sistemas que pueden ser fácilmente comprometidos y los SCI han demostrado ser un entorno rico en posibles vulnerabilidades” a través de sus informes de Threats Predictions, que siguen recogiendo amenazas para la industria en sucesivos informes anuales. Verizon también sigue en la misma línea publicando varios informes al año.[9]

---

[7] GARCÉS, Juan Carlos. Citado por PORTAFOLIO. Las compañías le apuestan a la tecnología de punta. En: Portafolio [online]. Febrero, 2018, párr. 3. Recuperado de https://www.portafolio.co/economia/las-companias-le-apuestan-a-la-tecnologia-de-punta-513970

[8] Ibíd., párr.5

[9] INSTITUTO NACIONAL DE CIBERSEGURIDAD - INCIBE. España. 22, octubre, 2015. [blog institucional]. Recuperado de https://www.incibe-cert.es/blog/ciberseguridad-industria-4-0

Para los procesos productivos, es necesario contar con plataformas tecnológicas y softwares especializados, los cuales están comunicados por medio de redes que soportan en gran parte la operación. En muchos casos, se requiere de conexiones externas, salidas a internet o enlaces entre sucursales, lo que hace necesaria una infraestructura de seguridad estable.

Dichos procesos industriales cuentan con elementos tanto de OT como de IT para su funcionamiento y operación, que se lleva a cabo mediante las señales que reciben de otros equipos, los cuales llegan a servidores y, posteriormente, a las bases de datos. Con estos componentes se realiza el seguimiento y la explotación de las operaciones, apoyándose en sistemas de comunicaciones que se encargan de transportar la información, a través de redes de gestión, control y operación, estás redes realizan la comunicación entre los diferentes dispositivos de la operación.

Anteriormente, solo se presentaban ataques dirigidos hacia sistemas de información con infraestructura de IT. Sin embargo, con la evolución de los ataques, estos han comenzado a dirigirse a equipos industriales, los cuales no cuentan con equipos, procedimientos ni personal preparados para aplicar una buena defensa desde las OT. Por lo tanto, en la actualidad, donde los ataques informáticos se dirigen también hacia empresas industriales, se hace necesario que las empresas opten por generar procedimientos internos y comprar equipos de apoyo en seguridad, tanto física como lógica, para mitigar los nuevos riesgos que presentan ante dichos ataques. Para esto se hace necesario entender ¿cómo pueden ser aplicadas las buenas prácticas de IT en OT?

JUSTIFICACIÓN

El tema de Tecnologías Operacionales se encuentra en constante evolución, complementándose con las buenas prácticas de los sistemas de información, que aportan conceptos y modelos para mitigar los riesgos asociados al manejo, almacenamiento y procesamiento de la información. Por lo tanto, como se ha dicho anteriormente, las buenas prácticas de IT en OT ejercen una función de complemento para lograr una operación más confiable y un tratamiento infalible para la seguridad de la información.

Con la evolución de las Tecnologías Operacionales también se ha dado la evolución de las amenazas y los ataques programados para debilitarlas. Con el crecimiento del internet se ha dado también un crecimiento significativo en OT. “la evolución de las amenazas relacionadas con el ciberespacio en los últimos anos también ha aumentado las preocupaciones sobre el uso real y potencial de Internet con fines ilegales. Datos recientes muestran que el costo de la delincuencia cibernética ha alcanzado U$S8 mil millones en Brasil, U$S3 mil millones en México y U$S 464 millones en Colombia.”[10]

Desde el virus conocido como Stuxnet, virus que fue lanzado para atacar estructura crítica, es decir OT, es imposible negar la existencia del crecimiento de los riesgos contra esta infraestructura y todos sus componentes de información y de los diferentes sistemas y procesos que permiten el funcionamiento adecuado y productivo de una organización.

> En junio de 2010, una ciberamenaza fue descubierta de manera accidental por investigadores de una pequeña empresa bielorrusa llamada VirusBlockA- da. Esta amenaza informática, conocida como *software* malicioso (*malware*), se propagaba infectando memorias Pen Drive USB. Lo particular de este *malware* es el interés y la preocupación que despertó en los expertos de seguridad a medida que se lo iba analizando, dado el nivel de sofisticación y de estragos que era capaz de producir, marcando un hito en la historia de las ciberamenazas.
>
> El virus de nombre *Stuxnet* fue considerado una revolución en asuntos militares (RMA) por trasgredir los límites de lo virtual produciendo estragos en el mundo real, lo cual supuso un giro en la naturaleza del concepto de ciberguerra. Como resultado, se produjo la afectación de equipos industriales, con pruebas que indican que se

[10] ORGANIZATION OF AMERICAN STATES y MICROSOFT. Protección de la infraestructura crítica en américa latina y el caribe. [documento virtual] 2018, p. 10. Recuperado de https://info.microsoft.com/LA-AzureMig-CNTNT-FY19-10Oct-24-Protecciondelainfraestructura-MGC0003227_01Registration-ForminBody.html

> cumplieron los objetivos del virus, poniendo de manifiesto un adelanto significativo en el desarrollo de *software* maliciosos, por las consecuencias producidas.[11]

El virus Stuxnet demuestra que si pueden desarrollarse ataques contra gobiernos, los cuales deben contar con tecnología, estrategias y prácticas muy avanzadas para la seguridad, es posible que estos ataques puedan traspasar las barreras de algunas empresas. Es por esto, por lo que adquirir unas buenas prácticas de seguridad se hace fundamental, el modelo que se plantea a través de este documento busca mitigar los riesgos relacionados con estos ataques que buscan descompensar la estructura y la productividad de una organización.

> Los gobiernos de todo el mundo están centrando su atención en la ciberseguridad. Sus prioridades van desde el aumento de las habilidades de seguridad cibernética, a la adopción de nuevas leyes de cibercrimen y la comprensión de cómo las reglas internacionales nuevas o existentes podrían aplicarse al nuevo panorama Una prioridad comúnmente identificada es la protección de las infraestructuras críticas - los servicios, sistemas y funciones de las que dependen las naciones modernas- del ataque cibernético.[12]

Por otro lado, los proveedores de OT, como Siemens y Schneider Electric, se han alejado de los sistemas propietarios a sistemas operativos abiertos y comercializados y con nuevas capas en las comunicaciones, para que los productos puedan ser controlados y monitoreados por otras plataformas y cuenten con toda la seguridad de la información. Para una convergencia de los sistemas de IT y OT se requieren de plataformas abiertas y compatibles con múltiples protocolos, pero muy seguras con la información.

Los proveedores de gestión de activos y software de IT como IBM están comenzando a considerar dentro de sus productos de administración de software de IT, la administración de componentes de OT para el control de software, activos, inventarios, ciclos de vida de los componentes de las operaciones. Con estos aportes la seguridad en OT toma otra connotación al ser tenida en cuenta por los grandes fabricantes y proveedores de tecnología.

OT son sistemas fundamentales, “la importancia de estos sistemas radica en como los daños que sufra la infraestructura crítica puede afectar el poder nacional. Éste

---

[11] SILVA G, Francisco. StuxNet – El software como herramienta de control geopolítico. En: Revista PUCE [online], 2018. No. 106, p. 300. Recuperado de http://www.revistapuce.edu.ec/index.php/revpuce/article/view/141/243

[12] ORGANIZATION OF AMERICAN STATES y MICROSOFT. Protección de la infraestructura crítica en américa latina y el caribe. [documento virtual] 2018, p. 10. Recuperado de https://info.microsoft.com/LA-AzureMig-CNTNT-FY19-10Oct-24-Protecciondelainfraestructura-MGC0003227_01Registration-ForminBody.html

tiene sus factores como lo es económico, político, social, militar y tecnológico. También dentro de estos factores se encuentra la industria. Y si una amenaza afecta la industria de un estado, este pierde sus capacidades de generar y producir, y por lo tanto los efectos los siente la población".[13]

Entonces, la seguridad de la información toma un papel relevante para asegurar que los recursos de los sistemas de información de OT (material informático o programas) de una organización, sean utilizados bajo las buenas prácticas de IT generando una nivelación entre disponibilidad y confidencialidad de la información, manteniendo siempre la Protección de Infraestructuras Críticas de Información (CIIP), definiendo esta como "Todas las actividades destinadas a garantizar la funcionalidad, continuidad e integridad de CII para disuadir, mitigar y neutralizar una amenaza, riesgo o vulnerabilidad o minimizar el impacto de un incidente"[14]

[13] INTECO citado en BAQUERO SALAMANCA, Germán Darío. Seguridad de la información en sistemas SCADA [online]. Universidad Piloto de Colombia. Recuperado de http://polux.unipiloto.edu.co:8080/00001512.pdf

[14] GFCE, 2016 citado en ORGANIZATION OF AMERICAN STATES y MICROSOFT. Protección de la infraestructura crítica en américa latina y el caribe. [documento virtual] 2018, p. 10. Recuperado de https://info.microsoft.com/LA-AzureMig-CNTNT-FY19-10Oct-24-Protecciondelainfraestructura-MGC0003227_01Registration-ForminBody.html

OBJETIVO GENERAL

Recomendar un modelo de seguridad de la información para la convergencia de IT y OT mediante el Modelo de Seguridad y Privacidad de la Información (MSPI) Decreto 612.

OBJETIVOS ESPECIFICOS

- Investigar y plasmar los conceptos de Tecnologías Operacionales.
- Documentar sobre las redes de comunicaciones industriales actuales y más utilizadas.
- Describir los principales conceptos de Tecnologías de la Información.
- Plasmar las necesidades en seguridad Informática.
- Recomendar un modelo de convergencia IT-OT

1. EL MODELO OSI EN LAS REDES INDUSTRIALES

El modelo OSI permite dividir el proceso de transmisión de información, entre los equipos de una organización, en siete capas, además cumple con ciertos servicios de seguridad los cuales se pueden observar en la Tabla 1. Este modelo surgió de la necesidad de que diferentes redes pudieran comunicarse entre sí y trabajar en conjunto. Sin embargo, el modelo OSI ha presentado diferentes dificultades, por ejemplo, según Álvaro Yunta[15] , el modelo resulta ineficiente en redes industriales con requerimientos de baja latencia o automatizados, pues, debido a las recomendaciones y lineamientos que este modelo propone en cada una de estas capas, estas suelen sobrecargarse generando fallas en el funcionamiento.

Tabla 1. Servicios de Seguridad en las Capas de Modelo OSI

Servicio	Capas					
	1	2	3	4	5/6	7
Autenticación de entidades			Y	Y		Y
Autenticación de origen			Y	Y		Y
Control de acceso			Y	Y		Y
Confidencialidad con conexión	Y	Y	Y	Y		Y
Confidencialidad sin conexión		Y	Y	Y		Y
Confidencialidad de un campo selectivo						Y
Confidencialidad de flujo de tráfico	Y		Y			Y
Integridad con conexión con recuperación				Y		Y
Integridad con conexión sin recuperación			Y	Y		Y
Integridad con conexión de un campo selectivo						Y
Integridad sin conexión			Y	Y		Y
Integridad con conexión de un campo selectivo						Y
No repudio del origen						Y
No repudio del destinatario						Y

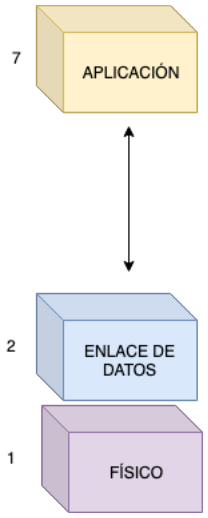
Fuente: AREITIO BERTOLÍN, Javier. Seguridad de la información. Redes, informática y sistemas de información. España: Editorial Paraninfo, 2008. 566p. ISBN: 9788497325028. Recuperado de https://books.google.es/books?hl=es&lr=&id=_z2GcBD3deYC&oi=fnd&pg=IA1&dq

[15] ÁLVARO YUNTA, Miguel. Implementación de las comunicaciones PC-autómata-robot mediante interfaz Ethernet industrial. Trabajo de grado Ingeniería Técnica Electrónica. Universidad Carlos III de Madrid. Madrid, 2009, p.22. Recuperado de https://e-archivo.uc3m.es/handle/10016/6907

=modelo+OSI+en+redes+industriales&ots=wsniyGA_Qg&sig=wpmhG-yXISXZYry2HhEQp15M5KM#v=onepage&q=OSI&f=false

Álvaro Yunta[16] afirma, también, que para solventar los inconvenientes presentados por el modelo OSI al momento de trabajar para industrias con redes de baja latencia o automatizadas, la mayoría de las redes industriales utilizan únicamente tres capas de estos niveles: el nivel físico, el nivel de enlace y el nivel de aplicación. En la Figura 3 se muestran las tres capas del modelo OSI en las redes Industriales.

Figura 3.Capas Modelo OSI Industrial



Fuente: El autor.

El nivel físico establece el medio que se utiliza en la transmisión y las características físicas del mismo. En el área industrial la fiabilidad ha de ser superior a los niveles físicos empleados en las redes de oficina, pero manteniendo el requisito de un reducido coste económico y rendimiento.

La capa de enlace se encarga de mover los datos por la conexión física definiendo los formatos de trama y los mecanismos de protección ante erros lógicos. Esta capa está conformada por dos subcapas, el Control Lógico del Enlace y el Control de Acceso al Medio. En la mayoría de las redes industriales, la capacidad de satisfacer los requerimientos de tiempo real de las aplicaciones industriales depende, en gran medida, del mecanismo de acceso al medio, este determina la capacidad de interoperabilidades de los equipos o sensores. En este nivel se introduce el retraso

[16] Ibid., p. 22

de acceso al medio, el cual se define como la diferencia de tiempo entre la llegada de la trama a enviar y el envío de ésta al medio. Este tiempo tiene una influencia considerable en el retraso de transmisión, que abarca desde la llegada de la trama hasta la completa recepción en el destino. Para ofrecer un comportamiento adecuado, es necesario garantizar los tiempos de transmisión y recepción. Con el objeto de mejorar el comportamiento estos sistemas, en el nivel dos es necesario la utilización de prioridades del contenido de la información para la transmisión y recepción con la prioridad de los elementos a controlar o monitorear.

A través de estas prioridades se pretende que, a las tramas, consideradas vitales para el funcionamiento del sistema, se les dé un mejor tratamiento, en la competición por el acceso al medio, que a las tramas que transportan información que no es vital dentro de los procesos. Si el protocolo de acceso al medio es centralizado, es más factible garantizar unas comunicaciones eficientes. Si el protocolo de acceso al medio es totalmente distribuido, se pueden producir situaciones poco deseables, como que el acceso al medio esté asignado a una estación que está transmitiendo tráfico de baja prioridad, mientras otra estación con tráfico de alta prioridad debe esperar. En general el subnivel MAC debe garantizar un mínimo de ancho de banda a todas las estaciones, mediante una política de reparto justo de ancho de banda que cumpla con las necesidades de cada estación. Otro aspecto importante de la MAC es la productividad, en este sentido, se dice que un protocolo MAC es estable si mantiene un flujo de datos equilibrado, que permita que cuando un dispositivo este transmitiendo se encuentre con un espacio libre para impedir las colisiones. La capa de enlace puede variar y estar sujeta a cambios especiales del ámbito de aplicación. Por ejemplo, el diseño de redes de comunicaciones, en la capa de enlace, permite la construcción y la recepción de señales sensoriales y de equipos industriales a un coste razonable.

El nivel de aplicación concentra todas las señales de los dispositivos conectados y el monitoreo de todo el proceso que se ejecuta, denominado bus de campo. Permite generar una conexión entre las aplicaciones usadas para la comunicación y la red en la que se transmiten los mensajes, es decir, permite la creación de un interfaz entre el software de comunicaciones y cualquier aplicación que necesite usar la red para comunicarse. En este nivel se define el perfil o profile, que permite la organización de protocolos como el comportamiento de ciertos dispositivos, sensores o sistemas que hacen parte de la organización y están conectados a la red.

En los sistemas y procesos industrializados modernos, se cuenta con otras capas adicionales del modelo OSI. Los sensores y equipos industriales, actualmente, son elementos que entregan información en protocolos estándar que pueden ser transportados en la capa de red y de transporte del modelo OSI, donde el equipo final es un servidor que almacena y administra toda la información de los procesos

industriales y automatizados. Para una operación productiva y con seguridad de la información se hace necesaria la convergía entre IT y OT.

Entre los medios físicos se utilizan interfaces como RS-485 para la transmisión y recepción de señales en cortas distancias y con pulsos eléctricos de bajo nivel, para distancias más largas el medio utilizado es la fibra óptica donde se aprovechan las características para las comunicaciones del nivel físico.

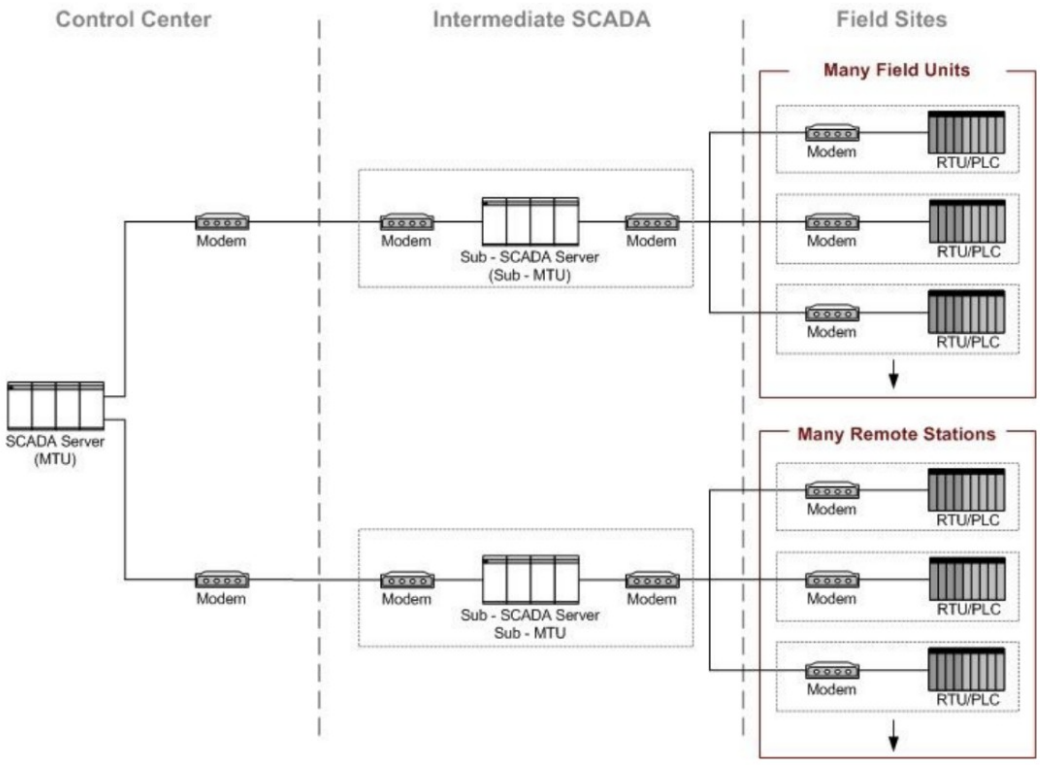
En la capa de enlace de datos se encuentran la comunicación en el caso del Profibus, el bus de datos donde convergen todas las señales de los dispositivos como: sensores, PLC, estaciones pasivas, entre otros. En la actualidad esta estructura está cambiando drásticamente con los dispositivos que operan con IoT, capaces de ser censados y monitoreados y generar información para ser consultada o archivada en bases de datos, utilizan otros medios como redes inalámbricas o cableado estructurado, donde se utilizan diferentes protocolos y cifrados para la seguridad en las comunicaciones. En esta capa las comunicaciones se realizan en ocasiones con protocolos propietarios.

Por último, en el nivel de aplicación se encuentran las herramientas o programas donde se concentran los datos procesados o compartidos entre los sensores, dispositivos de control lógico (PLC) y las órdenes dadas para la activación, movimiento, monitoreo o toma de información para los procesos industriales.

Los niveles de las capas del modelo OSI industrial pueden evidenciarse dentro de la red SCADA, la cual es definida como “un sistema complejo cuyo objetivo principal es el de llevar a cabo los procesos de supervisión y gestión de otros sistemas complejos, cuyos recursos son considerados críticos (por ejemplo, sistemas de control de agua, gas, energía, transporte). Estos sistemas de control han ido evolucionando con el paso de la historia, estando actualmente basados en entornos distribuidos y con componentes (hardware y software) muy variados”[17] En la Figura 4 se puede observar los diferentes componentes que conforman una red SCADA, mostrando los elementos en cada una de sus capas.

[17] ALCARAZ, Cristian *et al.* Gestión segura de redes SCADA. Nuevas tendencias en gestión de redes, Novática. En: NICS Lab. Publications, 2008. p. 20-25. Recuperado de https://www.nics.uma.es/pub/papers/Alcaraz2008a.pdf

Figura 4. Red SCADA



Fuente: STOUFFER, Keith *et al.* Guide to Industrial Control Systems (ICS) Security. En: NIST, revisión 2, mayo, 2015, 7 p. Recuperado de http://dx.doi.org/10.6028/NIST.SP.800-82r2

2. TECNOLOGIAS OPERACIONALES (OT)

Al hablar de Tecnología Operacional, se habla de "hardware y software que detecta o provoca un cambio a través de la supervisión directa y / o control de dispositivos físicos, procesos y eventos en la empresa".[18] Con el avance tecnológico y el crecimiento de la industria, estos sistemas llamados Tecnologías Operacionales (OT), han traído consigo infinidad de vulnerabilidades en los procesos, convirtiéndose así en una infraestructura crítica. La infraestructura crítica se entenderá como todos aquellos sistemas y activos vitales para el funcionamiento de una empresa. Son críticos porque si algo en el funcionamiento de estos sistemas y/o activos falla, se generaría un impacto negativo en la seguridad de la información y de la producción de la organización.

Se puede afirmar que el objetivo principal de OT es "facilitar en tiempo real la retroalimentación del sistema, controlando automáticamente el proceso con los datos de los diferentes sensores que lo conforman. Asimismo, suministra datos en tiempo real del estado del proceso, pudiendo tener información sobre el control de calidad, los niveles de producción, y otras variables que ayudan a la gestión del proceso.

"Debido al aumento de las amenazas externas e internas, las organizaciones responsables de la infraestructura crítica deben tener un enfoque constante e iterativo para identificar, evaluar y administrar el riesgo de seguridad cibernética. Este enfoque es necesario independientemente del tamaño de una organización, exposición a amenazas o actual sofisticación de seguridad cibernética."[19] Es decir, las operaciones y transacciones operacionales en muchas empresas dependen de equipos industriales, los cuales generan información que debe tratarse y cuidarse de manera segura.

Es por lo que los diferentes sectores de la industria se han percatado de la necesidad de procurar un manejo seguro y viable de las Tecnologías Operacionales. Países como Estados Unidos, desde North American Electric Reliability Corporation (NERC), el organismo regulador de energía, han creado diferentes guías

---

[18] GARTNER. Operational Technology (OT) Traducido y citado por HACHI. La tecnología operacional: Otro reto para PRTG. En: Hachi [página web], 2016. Recuperado de http://hachi.co/newsletter-prtg/

[19] INSTITUTO NACIONAL DE ESTÁNDARES Y TECNOLOGÍA. Marco para la mejora de la seguridad cibernética en infraestructuras críticas. NIST Estados Unidos: Abril, 2018, 55 p. Recuperado de https://www.nist.gov/sites/default/files/documents/2018/12/10/frameworkesmellrev_20181102mn_clean.pdf

relacionadas con ciberseguridad. Por ejemplo, se ha establecido el Critical Infrastructure Protection Committee (CIPC) para apoyar a NERC en el avance de la seguridad física y la ciberseguridad de las estructuras eléctricas críticas. A continuación, se presentan las funciones de este comité, según NERC[20]:

- Coordinar y comunicar con las organizaciones responsables de la seguridad física y la ciberseguridad en todos los segmentos de la industria eléctrica y otros segmentos con infraestructura crítica, según sea necesario.
- Crear enlace con gobiernos en asuntos de protección de infraestructura crítica (PIC)
- Coordinar con los otros comités NERC y trabajar en equipo asegurando el mayor grado de colaboración posible en cuanto a la seguridad.
- Establecer y mantener un reporte de información del procedimiento para el CIP entre los segmentos de la industria y con los gobiernos, según corresponda.
- Desarrollar, repasar periódicamente y revisar (según corresponda) las pautas de seguridad.
- Asistir en el desarrollo e implementación de los estándares de confiabilidad NERC.
- Realizar foros y talleres relacionados con el alcance de CIPC.

Es importante para las empresas, de cualquier lugar, adoptar este tipo de prácticas y contar con el personal o los aliados adecuados para mantener la seguridad de OT y de la información generada en los diferentes procesos productivos, pues la industria puede enfrentarse ante ataques que no solo vulneren su información y funcionamiento, sino también el de toda la industria, afectando así, gravemente, la seguridad de productores, consumidores e incluso del desarrollo de la economía y tecnología nacional. Pues se sabe que "los ataques a la infraestructura critica tienen el potencial de alterar significativamente el funcionamiento del gobierno y las empresas por igual y dar lugar a un efecto dominó en los ciudadanos de nuestras naciones." [21]

Para comprender más a fondo todos los elementos que hacen parte de OT, es fundamental comprender el concepto de internet de las cosas, en adelante IoT. Pues, el IoT, al ser una combinación de sensores capaces de recibir y dirigir

---

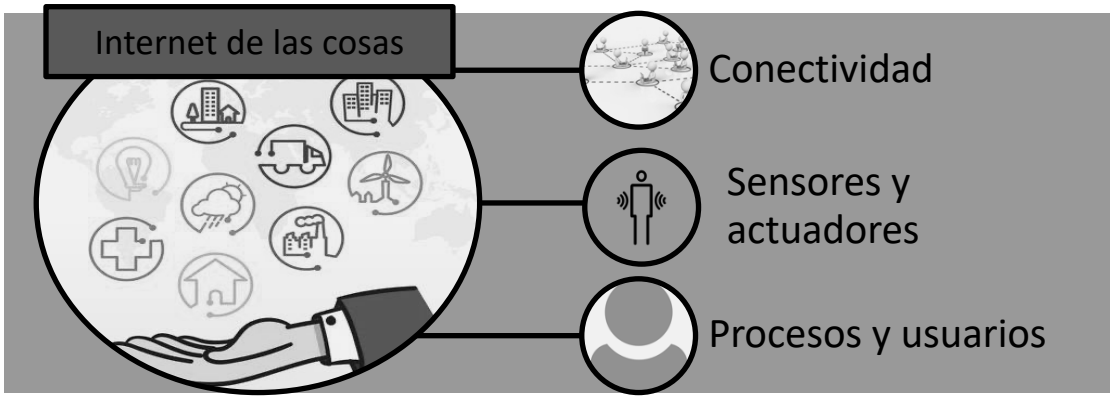
[20] NERC. Critical Infrastructure Protection Committee (CIPC). En: NERC [página web], 2017 Recuperado de https://www.nerc.com/comm/CIPC/Pages/default.aspx

[21] ORGANIZATION OF AMERICAN STATES y MICROSOFT. Protección de la infraestructura critica en américa latina y el caribe. [documento virtual] 2018, p. 8. Recuperado de https://info.microsoft.com/LA-AzureMig-CNTNT-FY19-10Oct-24-Protecciondelainfraestructura-MGC0003227_01Registration-ForminBody.html

información a través de redes bidireccionales, permite los avances de las estructuras críticas. IoT trae consigo muchas mejoras en comunicaciones, control y monitoreo, pero las mejoras pueden verse afectadas por la seguridad en los protocolos de encriptación con contienen estos dispositivos, la Figura 5, describe el entorno de las conexiones de IoT que pueden verse afectadas en la seguridad.

> La IoT se refiere a la interconexión en red de todos los objetos cotidianos, que a menudo están equipados con algún tipo de inteligencia. En este contexto, Internet puede ser también una plataforma para dispositivos que se comunican electrónicamente y comparten información y datos específicos con el mundo que les rodea. Así, la IoT puede verse como una verdadera evolución de lo que conocemos como Internet añadiendo una interconectividad más extensa, una mejor percepción de la información y servicios inteligentes más completos.[22]

Figura 5. Conexiones de IoT



Fuente: El autor

IoT ha permitido el avance de OT, por lo tanto, su arquitectura debe ser entendida para poder conocer el funcionamiento y los complementos que permiten el adecuado funcionamiento de las infraestructuras críticas. Además, comprender IoT se hace fundamental porque "en la actualidad hay cerca de 25 mil millones de dispositivos conectados a la IoT. Más o menos un dispositivo inteligente por persona"[23] La arquitectura de IoT está compuesta por cuatro capas, las cuáles se pueden observar en la Tabla 2.

---

[22] SALAZAR, Jordi y SILVESTRE, santiago. Internet de las cosas. En: České vysoké učení technické v Praze Fakulta elektrotechnická [online]. 2016, 7 p. Recuperado de https://core.ac.uk/download/pdf/81581111.pdf

[23] Ibíd., p. 7

Tabla 2. Arquitectura de IoT

Capa	Descripción
Detección	Sensores, los objetos físicos y la obtención de datos.
Intercambio de datos	Transmisión trasparente de datos a través de redes de comunicaciones
Integración de información	El procesamiento de la información incierta adquirida de las redes, filtrado de datos no deseados e integración de información principal en conocimiento útil para los servicios y los usuarios finales.
Servicio de aplicación	Da servicios de contenidos a los usuarios.

Fuente: SALAZAR, Jordi y SILVESTRE, santiago. Internet de las cosas. En: České vysoké učení technické v Praze Fakulta elektrotechnická [online]. 2016, 8 p. Recuperado de https://core.ac.uk/download/pdf/81581111.pdf

IoT encuentra su relación con OT cuando se habla de procesos de automatización y con los sensores que la conforman, permitiéndole así optimizar la producción de las diferentes empresas, explorar y crear nuevos modelos de negocio, conectar con nuevos dispositivos inteligentes, realizar unos procesos de mantenimiento efectivos reduciendo costos, entre otras funciones fundamentales para el funcionamiento de una industria que se apoye en la infraestructura crítica para la realización de sus tareas.

Por otro lado, el hardware y el software de OT cuentan con componentes de seguridad, en el entorno físico y lógico, muy importantes para una correcta operación. No obstante, se requiere de otro enfoque para obtener y proteger toda la información que es generada y compartida a otros lugares o usuarios.

Anteriormente, no se hablaba de seguridad en OT. Sin embargo, con la evolución de los sistemas industrializados y automatizados, y la cantidad de fabricantes, se ha logrado identificar la necesidad de contar con unas buenas prácticas de IT, en el empleo de la de la información.

Un ejemplo muy claro sobre Tecnologías Operacionales, son las empresas de transporte ferroviario, las cuales direccionan señales emitidas por equipos y sensores, a lo largo de sus sistemas, hacia controladores PLC, que posteriormente las transportan, a través de la red de comunicaciones de datos, hasta los equipos

centrales, en este caso servidores, donde toda esta información es almacenada y administrada por bases de datos dedicadas a tal fin.

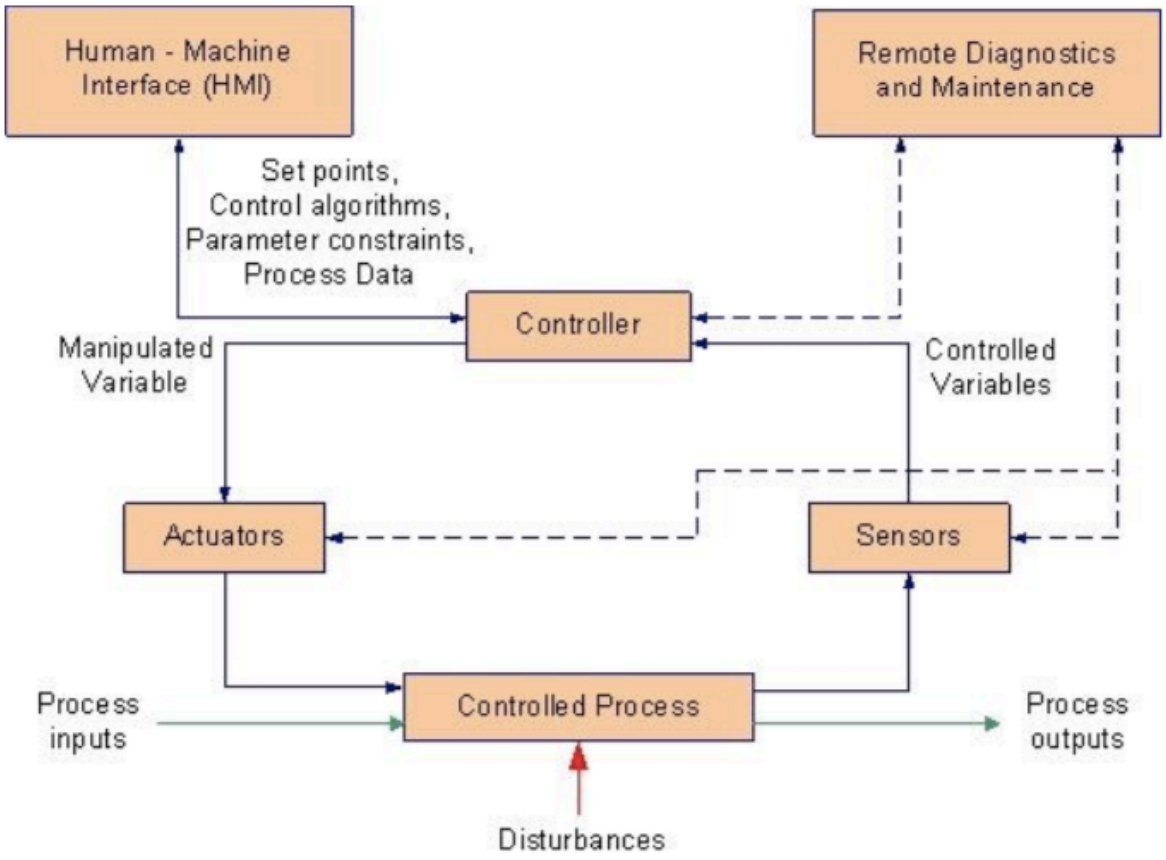
2.1 SISTEMAS DE CONTROL INDUSTRIAL (ICS)

Los Sistemas de Control Industrial hacen referencia a todos aquellos sistemas de control, incluyendo las redes SCADA, mencionadas anteriormente, que son redes o sistemas de control de supervisión y adquisición de datos, los ICS incluyen también los Sistemas de Control Distribuido (DCS) y otros sistemas como Controladores Lógicos Programables (PLC). Generalmente los ICS se encuentran en sectores industriales que cuentan con infraestructura crítica, es por esto por lo que los ICS hacen parte de las Tecnologías Operacionales.

Un ICS consiste en combinaciones de componentes de control (por ejemplo, eléctrico, mecánico, hidráulico, neumático) que actúan juntos para lograr un objetivo industrial. Los ICS son sistemas que han reemplazado los mecanismos de control físico, permitiendo mejoras en el costo y rendimiento del proceso productivo, dando paso a grandes avances como por ejemplo las tecnologías llamadas inteligentes. Los sistemas de control se utilizan en muchos sectores industriales diferentes e infraestructuras críticas, que incluyen fabricación, distribución y transporte, arquitectura y proceso de ICS. Normalmente un ICS debe contener múltiples bucles de control, interfaces humanas y herramientas de diagnóstico y mantenimiento remotas creadas utilizando una serie de protocolos de red, en arquitecturas de red en capas. Para formar un buen circuito de control deben utilizarse sensores, es decir dispositivos que produzcan medición de alguna propiedad física y la envié al controlador, deben usarse también controladores y actuadores. Los controladores son encargados de interpretar señales y generar las correspondientes variables manipuladas, basadas en un algoritmo de control y puntos de ajuste de destino. Después, los controladores transmiten las variables a los actuadores, los cuales se utilizan para manipular directamente el proceso controlado según los comandos del controlador.

Dentro del proceso de los ICS es fundamental contar con operarios e ingenieros que monitoreen, configuren y brinden mantenimiento a cada uno de los dispositivos de ICS, los algoritmos de control y los parámetros del controlador. Los operarios e ingenieros hacen parte de la conocida como interfaz humana, la cual debe responder ante la organización mostrando la información de estado del proceso e información histórica del mismo. La interfaz humana debe encargarse del diagnóstico y mantenimiento para prevenir, identificar y recuperarse de operaciones anormales o fallas. Entre los bucles de control, se cuenta con los bucles de nivel de supervisión y los bucles de nivel inferior, los cuales funcionan de manera continua durante un proceso cíclico. En la figura 6 pueden observarse los componentes de los ICS.

Figura 6. Componentes de ICS



Fuente: STOUFFER, Keith *et al.* Guide to Industrial Control Systems (ICS) Security. En: NIST, revisión 2, mayo, 2015, 4 p. Recuperado de http://dx.doi.org/10.6028/NIST.SP.800-82r2

Los elementos de ICS son descritos en diferentes factores, dados por Stouffer *et al.*[24] en Guide to Industrial Control Systems (ICS) Security, son fundamentales al momento de diseñar los sistemas de control, comunicación, confiabilidad y redundancia de un ICS, estos factores facilitan el diagnóstico y la toma de decisiones una vez se hayan determinado las necesidades de un sistema.

[24] STOUFFER, Keith *et al.* Guide to Industrial Control Systems (ICS) Security. En: NIST, revisión 2, mayo, 2015, 5 p. Recuperado de http://dx.doi.org/10.6028/NIST.SP.800-82r2

- Requisitos del tiempo de control: los procesos de ICS cumplen con muchos requisitos relacionados con el tiempo, por ejemplo, debe mantener una alta velocidad, consistencia y sincronización. Como los seres humanos no representan un nivel muy alto de confiabilidad al momento de cumplir con estos requisitos, surge la necesidad de utilizar controladores automáticos. Algunos sistemas pueden requerir que el cálculo se realice lo más cerca posible del sensor y los actuadores para reducir la latencia de la comunicación y realizar las acciones de control necesarias a tiempo.

- Distribución geográfica: se conoce que los sistemas deben tener grados de distribución, que deben ir desde un sistema pequeño (por ejemplo, un proceso controlado por PLC local) hasta sistemas grandes y distribuidos (por ejemplo, oleoductos, redes eléctricas). Es necesario, además, entender que una mayor distribución implica un área amplia (por ejemplo, líneas arrendadas, conmutación de circuitos y conmutación de paquetes) y comunicación móvil.

- Jerarquía: se debe utilizar un buen control de supervisión para proporcionar una publicación central que puede agregar datos desde varias ubicaciones para respaldar las decisiones de control basadas en el estado del sistema. A menudo, se utiliza un control jerárquico / centralizado para proporcionar a los operadores humanos una visión integral de todo el sistema.

- Complejidad de control: las funciones de control se pueden realizar mediante controladores simples y algoritmos preestablecidos. Sin embargo, los sistemas más complejos (por ejemplo, el control del tráfico aéreo) requieren que los operadores humanos se aseguren de que todas las acciones de control sean apropiadas para cumplir con los objetivos más grandes del sistema.

- Disponibilidad: los requisitos de disponibilidad del sistema son un factor fundamental para tener en cuenta al momento de diseñar un ICS. Debe tenerse en cuenta que los sistemas con fuertes requisitos de disponibilidad pueden requerir implementaciones alternativas en todas las comunicaciones y el control.

- Impacto de los fracasos: el fallo de una función de control podría incurrir en impactos altos en otras funciones. Los sistemas con mayor impacto a menudo requieren la capacidad de continuar las operaciones a través de controles redundantes, o la capacidad de operar en un estado degradado. El diseño debe abordar estos requisitos, pues es fundamental que en caso de que un riesgo o amenaza no pueda evitarse, el sistema pueda mitigar los daños y seguir funcionando de una manera adecuada.

- La seguridad: es fundamental tener en cuenta los requisitos de seguridad del área y del sistema para el diseño. Los sistemas deben ser capaces de detectar

condiciones inseguras y desencadenar acciones para reducir las condiciones inseguras. En la mayoría de las operaciones críticas para la seguridad, la supervisión humana y el control de un proceso potencialmente peligroso son parte esencial del sistema de seguridad

3. TECNOLOGIAS DE LA INFORMACIÓN (IT)

Las Tecnologías de la Información hacen referencia a plataformas tecnológicas capaces de brindar soluciones informáticas transnacionales, arquitecturas multicapas y la adopción del servicio al usuario como eje principal dentro del ecosistema tecnológico. Ríos Huércano en ITIL[25], recomienda como herramienta el servicio, tanto en los sistemas de información, como en el usuario final, con los procesos y los equipos que conforman las Tecnologías de la Información, como eje fundamental para conseguir las metas propuestas buscando la mejora continua como fuente de crecimiento de los procesos en las organizaciones.

Existe una gran responsabilidad, por parte de IT, con la implementación, soporte, mantenimiento y administración de los servicios, asegurando el ciclo de vida y la adopción de nuevas tecnologías para los procesos de la organización en su infraestructura de IT, manteniendo la gestión de otros procesos como la red de datos y los softwares especializados.

Un área de TI es la encargada de todos los procesos de tecnologías de la información la información y de la Seguridad de esta. Además, según Ríos Huércano[26], un área TI cuenta con procedimientos basados en buenas prácticas, para ayudar a toda la organización en los procesos tecnológicos y de información para cumplir con los objetivos organizacionales.

---

[25] RÍOS HUÉRCANO, Sergio. Manual de ITIL V3 Integro, Sevilla, Biable Management: Excellence and Innovation, 2015, p.4. Recuperado de https://docs.supersalud.gov.co/PortalWeb/planeacion/AdministracionSIG/GSDE01.pdf

[26] Ibid., p. 4.

4. SEGURIDAD INFORMÁTICA

La seguridad informática se refiere al proceso en el cual se aseguran los recursos del sistema de información, detectando y previendo los riesgos a los cuales estos recursos se enfrentan, tales como el uso no autorizado de los sistemas informáticos. El proceso de seguridad informática se apoya en herramientas lógicas y físicas para preservar la seguridad de la información, por lo que abarca una serie amplia de medidas de prevención y seguridad, como programas firewalls, antivirus, entre otras. La seguridad informática cumple con los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad.

Confidencialidad: la información solo debe ser accedida por personal autorizado, es fundamental para las organizaciones clasificar la información y generar niveles y contratos de confidencialidad para los empleados, proveedores y contratistas que presten servicios con manejo de información de alta importancia.

Integridad: preservar el contenido de información generada, con comunicaciones cifradas de extremo a extremo, almacenarlas en lugares con condiciones necesarias para brindar un medio ambiente que brinde durabilidad y temperaturas requeridas por los dispositivos, en caso de ser necesario contratar custodia externa o dotar los lugares de almacenamiento con ayudas lógicas y físicas para mantener en su estado original.

Disponibilidad: disponer y acceder a la información en el momento que se requiera, desde los lugares destinados para tal fin, contar con respaldos tanto en la información como con los componentes eléctricos, contratar almacenamiento externo como opción de backup y de respaldo en caso de fallo en los dispositivos de la organización.

Para la Seguridad Informática lo esencial es mitigar los riesgos asociadas a las diferentes amenazas que se ven expuestos las instalaciones y cada uno de los dispositivos que se utilizan para el transporte y procesamiento de la información, las amenazas pueden estar presentarse por actos mal intencionados que pretenden vulnerar las instalaciones o dispositivos que forman parte de la infraestructura de información, valiéndose de prácticas o herramientas para obtener información confidencial o causar la indisponibilidad de los sistemas en su infraestructura Física y/o Lógica.

4.1 SEGURIDAD FÍSICA

La seguridad física se refiere a los mecanismos de prevención y detección que se concentran en proteger la confidencialidad, integridad y disponibilidad de la información. La seguridad física, es entonces, todo el conjunto de medidas y herramientas que buscan evitar destrucción física a los sistemas de información y preservar los datos almacenados.

Los problemas que se deben prevenir con unas buenas prácticas de seguridad física van desde el acceso físico a los elementos hasta los desastres naturales. Dentro de las medidas que se pueden encontrar están: muros, rejas, personal de seguridad física, cámaras de seguridad, alarmas y sensores, estos elementos ayudan a complementar la seguridad informática. Para esta prevención es importante Identificar los activos, formar a los trabajadores de las empresas en cuanto a materias de seguridad y concientizar a los trabajadores sobre la importancia de la seguridad informática en la empresa. Es importante, además, "Evaluar los riesgos, considerando el impacto que se puede producir sobre los activos y las vulnerabilidades del sistema."[27] Y revisar de manera activa las medidas de seguridad adoptadas, sean estas partes de la seguridad pasiva o activa, es decir, revisar aquellas medidas que tratan de minimizar los impactos producidos o aquellos que traten de prevenir riesgos futuros.

La seguridad física es fundamental para la prevención de amenazas, que "consisten en la fuente o causa potencial de eventos o incidentes no deseados que pueden resultar en amenazas para los insumos informáticos de la organización y ulteriormente a ella misma."[28] Entre estos daños, caben señalar:

- La pérdida, destrucción, alteración, o sustracción de información por parte de personal de la organización debido a negligencia, dolo, mala capacitación, falta de responsabilidad laboral, mal uso, ignorancia, apagado o elusión de dispositivos de seguridad y/o buenas prácticas.

---

[27] QUIROZ-ZAMBRANO, Silvia M. y MACÍAS-VALENCIA, David G. Seguridad en informática: consideraciones En: Dominio de las Ciencias [online]. Julio, 2017. vol. 3, no. 5, p 687. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=6137824

[28] QUIROZ-ZAMBRANO, Silvia M. y MACÍAS-VALENCIA, David G. Seguridad en informática: consideraciones En: Dominio de las Ciencias [online]. Julio, 2017. vol. 3, no. 5, p 682. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=6137824

- La pérdida, destrucción, alteración, sustracción, consulta y divulgación de información por parte de personas o grupos externos malintencionados.
- El acceso no autorizado a conjuntos de información.

- La pérdida, destrucción o sustracción de información debida a vandalismo.

- La pérdida o destrucción de información debida a accidentes y fallas del equipo: fallas de energía, fallas debidas a calentamiento, aterriza miento, desmagnetización, rayadura o descompostura de dispositivos de almacenamiento, etcétera.

- La pérdida o destrucción de información debida a catástrofes naturales: inundaciones, tormentas, incendios, sismos, etcétera.[29]

Estos eventos no deseados, pueden generar grandes pérdidas para la organización, las consecuencias son efectos nocivos y a veces irreversibles contra la información de la empresa. Algunos impactos que pueden darse al materializarse una amenaza física informática son:

- Disrupción en las rutinas y procesos de la organización con posibles consecuencias a su capacidad operativa.

- Perdida de la credibilidad y reputación de la organización por parte del consejo directivo de la organización, público en general, medios de información, etcétera.

- Costo político y social derivado de la divulgación de incidentes en la seguridad informática.

- Violación por parte de la organización a la normatividad acerca de confidencialidad y privacidad de datos de las personas.

- Multas, sanciones o fincado de responsabilidades por violaciones a normatividad de confidencialidad.

- Pérdida de la privacidad en registros y documentos de personas.

- Pérdida de confianza en las tecnologías de información por parte del personal de la organización y del público en general.

- Incremento sensible y no programado en gastos emergentes de seguridad.

---

[29] Ibíd., p. 683

- Costos de reemplazo de equipos, programas, y otros activos informáticos dañados, robados, perdidos o corrompidos en incidentes de seguridad.[30]

Para mantener una buena seguridad física, es importante entender y aplicar los principales conceptos de esta, en la Figura 7, se describen los diferentes elementos con que debe contar y visualizar las categorías o conceptos de la seguridad física como complemento para la seguridad de la información, que según Giménez Albacete[31], son:

- Obstrucciones físicas: deben generar un reto o un grado de dificultad alto a que pretenda traspasarlas.

- Técnicas de vigilancia: deben alertar a las personas encargadas de cualquier movimiento o actividad extraña que se presente en el perímetro de acceso al área de activos.

- Los sistemas de inteligencia: estos deben analizar la información de vigilancia y permitir desarrollar buenas estrategias tácticas y operativas, que representen una ventaja frente a cualquier tipo de amenaza.

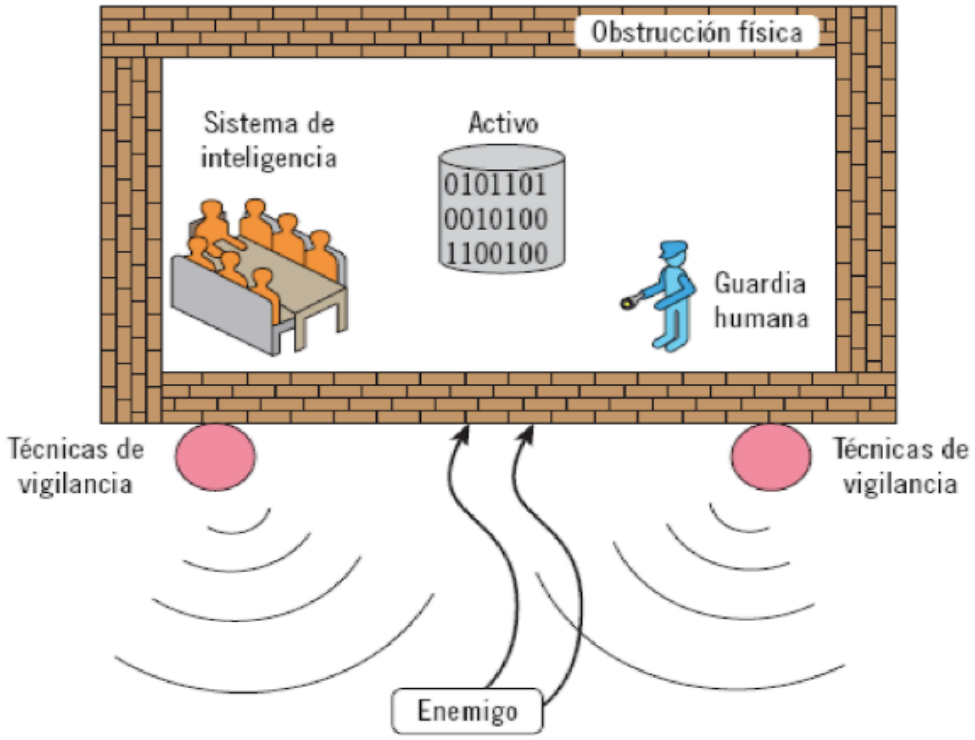
- Guardias o personal de seguridad: deben aportar la inteligencia humana y efectividad operacional frente a una amenaza, deben responder de la forma más adecuada frente a cualquier tipo de alarma.

---

[30] VOUTSAS M., J. citado por QUIROZ-ZAMBRANO, Silvia M. y MACÍAS-VALENCIA, David G. Seguridad en informática: consideraciones En: Dominio de las Ciencias [online]. Julio, 2017. vol. 3, no. 5, p 686. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=6137824

[31] GIMÉNEZ ALBACETE, José Francisco. MF0486_3: Seguridad en Equipos Informáticos [online]. 1 ed. Málaga: IC Editorial, 2014. ISBN: 978-84-16433-23-0. Recuperado de https://books.google.es/books?id=8a3KCQAAQBAJ&hl=es&source=gbs_navlinks_s

Figura 7. Categorías de diferentes elementos de seguridad física



Fuente: GIMÉNEZ ALBACETE, José Francisco. MF0486_3: Seguridad en Equipos Informáticos [online]. 1 ed. Málaga: IC Editorial, 2014. ISBN: 978-84-16433-23-0. Recuperado de https://books.google.es/books?id=8a3KCQAAQBAJ&hl=es&source=gbs_navlinks_s

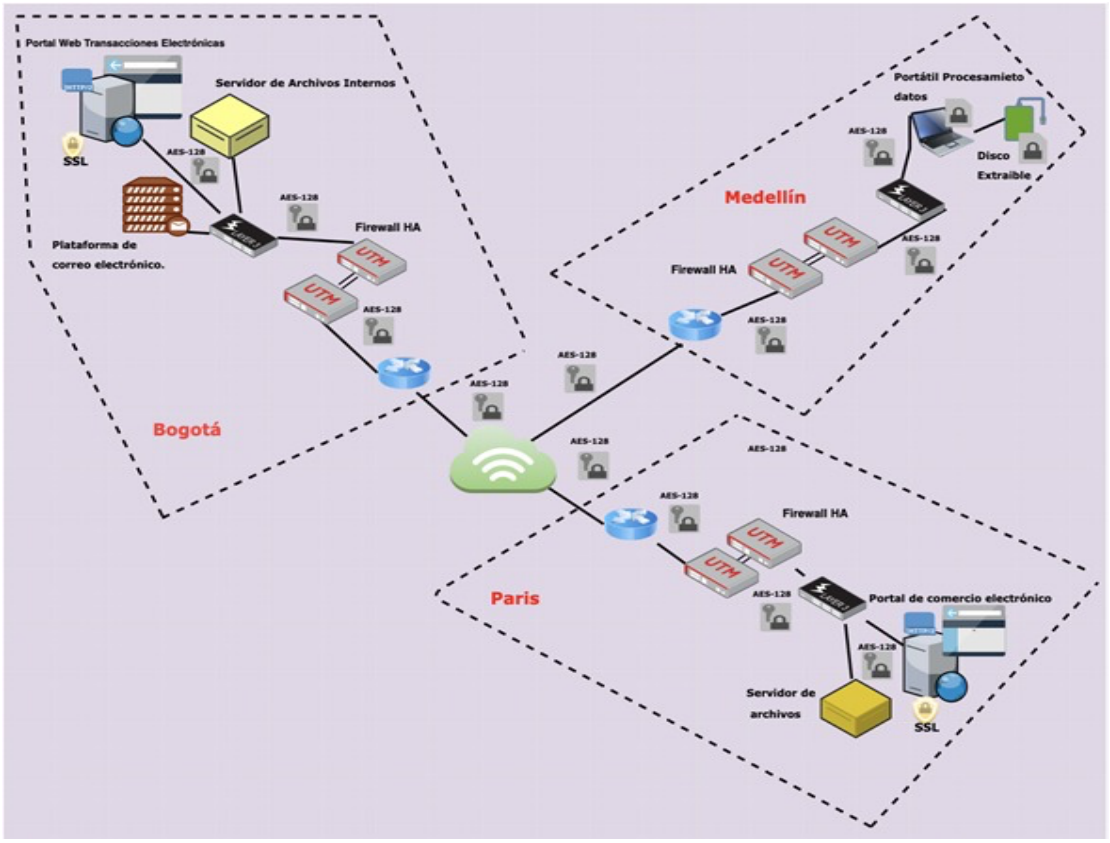
La seguridad física y/o ambiental es fundamental para evitar las amenazas e impactos anteriormente explicados, en la norma ISO27002, se contempla un capítulo en dedicado a la explicación de la seguridad física, estableciendo como se da un área segura que evite el acceso físico no autorizado a diferentes áreas de la empresa donde puede almacenarse información delicada. Establece entonces que "los sistemas de información deben ser usados en áreas seguras, protegidas por los perímetros de seguridad que se definan, con barreras de seguridad y controles apropiados."[32].

[32] Ibíd.

4.2 SEGURIDAD LÓGICA

Es el grupo de procesos orientados a garantizar la seguridad de la información y las plataformas informáticas, para que solo personas autorizadas tengan acceso a la información. En la figura 9 se puede observar un esquema que muestra los elementos principales que se deben cumplir para mantener una buena seguridad lógica.

Figura 8. Seguridad lógica



Fuente: El autor

Entonces, la seguridad lógica es un mecanismo que impone barreras y procedimientos que permiten, a la empresa, mantener la certeza de que solo los usuarios autorizados tienen acceso a la información de los equipos y redes. La seguridad lógica busca mitigar los riesgos asociados a los siguientes impactos:

- El advenimiento y proliferación de "malware" o "malicious software", programas cuyo objetivo es el de infiltrase en los sistemas sin conocimiento de su dueño, con objeto de causar daño o perjuicio al comportamiento del sistema y por tanto de la organización

- Los ataques de negación de servicio o de intrusión a los sistemas de la organización por parte de ciber–criminales: personas o grupos malintencionados quienes apoyan o realizan actividades criminales y que usan estos ataques o amenazan con usarlos, como medios de presión o extorsión.

- Los "phishers", especializados en robo de identidades personales y otros ataques del tipo de "ingeniería social".

- Los "spammers" y otros mercadotecnitas irresponsables y egoístas quienes saturan y desperdician el ancho de banda de las organizaciones.[33]

Cuando se habla de seguridad lógica, se debe tener en cuenta que la medida más importante consiste en la constante actualización de las políticas de seguridad corporativa, pues las empresas deben establecer las órdenes y directrices necesarias para la correcta operación de un sistema informático. Es decir, las políticas de seguridad corporativa establecen los lineamientos generales para utilizar el sistema, evitando virus, errores de usuario, errores de operación, accesos externos no autorizados, fraude informático, entre otras problemáticas que se pueden presentar en los sistemas. Entre las políticas relacionadas se encuentran:

- Instalación, mantenimiento y actualización de los equipos.
- Procedimiento para la configuración de equipos nuevos dentro de la organización con los permisos y aplicaciones a las cuales puede acceder, se deben mantener actualizados con los parches que generan los proveedores de software para la seguridad de la información y cronogramas de mantenimiento, que garanticen la disponibilidad de los equipos y del software instalado, todos con la licencia para su operación.
- Control de acceso a áreas críticas de la empresa y a recursos críticos del sistema.
- Se debe controlar el acceso a las áreas críticas de la empresa, donde se cuenta con equipos que generan y almacenan información importante para las operaciones de la organización, estos deben estar protegidos por cortafuegos y detención de intrusos en la red y en las máquinas.
- Utilización de recursos de las redes informáticas.

---

[33] VOUTSAS M., J. citado por QUIROZ-ZAMBRANO, Silvia M. y MACÍAS-VALENCIA, David G. Seguridad en informática: consideraciones En: Dominio de las Ciencias [online]. Julio, 2017. vol. 3, no. 5, p 686. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=6137824

- Resulta fundamental garantizar que los recursos de las redes informáticas se controlen, apoyándose en el uso de inventarios de estado y su ubicación.
- Mantenimiento de las redes de datos.
- Las redes de datos para la seguridad de la información son fundamentales, la correcta administración, de estas, es parte esencial para la disponibilidad. Se debe controlar y gestionar con las buenas prácticas que recomiendan los proveedores de los equipos, además llevar a cabo un control de cambios sobre las actividades realizadas en la red.
- Adquisición, instalación y actualización de software.
- Es necesario seguir los procedimientos para controlar la adquisición de equipos que cumplan con las características solicitadas y con la posibilidad de aplicarle las políticas de seguridad de la información.
- Privacidad de la información.
- Contar con las bases de la seguridad de la información, confidencialidad, integridad y disponibilidad.
- Autenticación de usuarios.
- Es fundamental cumplir con las políticas creadas para ingresar a los equipos y aplicaciones.
- Información de errores o de accesos al sistema.
- Es importante gestionar los registros de información generados por errores e ingresos a los sistemas de información.
- Contraseñas.

Para esto, se han establecido medidas o mecanismos desde las políticas de seguridad. Algunos mecanismos son:

- Identificación de usuarios: a través de un nombre de usuario y una contraseña.
- Control de acceso: perfiles, roles o grupos de usuarios con segregación de funciones en los sistemas.
- Criptografía: adquisición de mecanismo de cifrado a través de algoritmo para el almacenamiento, transformación y comunicación de la información de una manera segura. Cifrado de discos, unidades o sistemas de archivos para proteger la integridad.
- Certificados: documentos digitales, para la identificación, cifrado y desencriptado de la información a través de claves privadas o públicas.

- Firmas digitales: información digital utilizada para la identificación de forma electrónica.

5. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

El modelo de seguridad y privacidad de la información, que está basado en la norma ISO 27001, se construyó para que las empresas públicas en Colombia lo adopten como opción para diseñar los procesos de seguridad de la información en la organización, además para organizar la estructura de la información de forma segura, mitigando los riesgos de ser víctimas de los cyberdelincuentes.

El MSPI es actualizado periódicamente, para cumplir con el requisito de estar acorde con las buenas prácticas de seguridad, "reuniendo los cambios técnicos de la norma 27001 del 2013, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información."[34] Adicional a esto, El MSPI "se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión."[35]

"A nivel metodológico es importante tener presente que el (MSPI) cuenta con una serie de guías anexas que ayudarán a las entidades a cumplir lo solicitado permitiendo abordar de manera detallada cada una de las fases del modelo"[36]

El Modelo que se desarrollará está fundamentado en las buenas prácticas que describe el MSPI, el cual ofrece muchas herramientas para ser aplicadas en las Tecnologías Operacionales y construir operaciones más seguras para la información. La aplicación del MSPI en el Modelo a presentar, está determinado por las necesidades objetivas y los requisitos de seguridad de OT, con la necesidad de mantener la confidencialidad, integridad, disponibilidad en los procesos y plataformas de información.[37]

5.1 INSTRUMENTO DE EVALUACIÓN MSPI

---

[34] MINTIC. Seguridad TI: Modelo de seguridad. Fortalecimiento de la gestión TI en el estado, 2018, párr. 2. Recuperado de https://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html
[35] Ibíd., párr. 1
[36] Ibíd., párr. 3
[37] Ibíd., párr. 5

El Modelo de Seguridad y privacidad de la información, se creó como un instrumento para realizar diagnósticos del estado de la seguridad de la información en las organizaciones públicas, con herramientas que indican el nivel de madurez y la gestión en seguridad de la información. El Modelo de Seguridad y privacidad de la información está basado en la norma ISO27001/2013, y cuenta con todos los requisitos y controles necesarios para aplicar en una organización, e instaurarlos dentro de los procedimientos y políticas.

El MSPI va dirigido a entidades públicas de orden nacional y territorial, así como proveedores de servicios de Gobierno en Línea, y terceros que deseen adoptar el Modelo de Seguridad y Privacidad de la información en el marco de la Estrategia de Gobierno en Línea.[38] Además, fue elaborado con la recopilación de las mejores prácticas, nacionales e internacionales, para suministrar requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno en Línea – GEL.

A continuación, se presentan las guías que se cuentan dentro del instrumento de evaluación del MSPI.

Instructivo Instrumento de Evaluación MSPI:

- Guía - Seguridad de la información Mis pymes
- Guía 1 - Metodología de pruebas de efectividad
- Guía 2 - Política General MSPI v1
- Guía 3 - Procedimiento de Seguridad de la Información
- Guía 4 - Roles y responsabilidades
- Guía 5 - Gestión Clasificación de Activos
- Guía 6 - Gestión Documental
- Guía 7 - Gestión de Riesgos
- Guía 8 - Controles de Seguridad de la Información
- Guía 9 - Indicadores Gestión de Seguridad de la Información
- Guía 10 - Continuidad de Negocio
- Guía 11 - Análisis de Impacto de Negocio
- Guía 12 - Seguridad en la Nube
- Guía 13 - Evidencia Digital (En actualización)
- Guía 14 - Plan de comunicación, sensibilización, capacitación
- Guía 15 - Auditoria
- Guía 16 - Evaluación de Desempeño
- Guía 17 - Mejora continua
- Guía 18 - Lineamientos terminales de áreas financieras de entidades públicas
- Guía 19 - Aseguramiento de protocolo IPv4_IPv6
- Guía 20 - Transición IPv4_IPv6

[38] Ibíd., párr. 6

- Guía 21 - Gestión de Incidentes
- Modelo de Seguridad y Privacidad[39]

El MSPI se aplicará de acuerdo con los numerales que sean pertinentes para la convergencia IT-OT en seguridad de la información, permitiendo un acercamiento por parte OT hacia las buenas prácticas requeridas para la administración de los riesgos y el mejoramiento en la manipulación de los datos.

En la Tabla 3 se describe otros modelos los cuales son utilizados en la implementación de sistemas de información basados en procesos de gestión del riesgo, herramientas y metodologías aplicables de acuerdo con la necesidad del negocio para su utilización como soporte de la seguridad de la información.

Tabla 3. Otros Modelos

Modelo	Característica
Octave	Basado en el estudio de la infraestructura de la información, como soporte de un proceso auto dirigido, dúctil y progresivo, enfocado a resultados.
Magerit	Análisis completo cuantitativo y cualitativo, ayuda a mantener los procesos bajo control en todo momento a través de análisis de riesgos.
NIST SP 800-30	Análisis de riesgo de bajo costo, facilita la guía de riesgos en infraestructura de TI, asegura los sistemas informáticos que almacenan, procesan y transmiten información.
Coras	Contiene diversas herramientas de ayuda para el análisis de riesgos, contiene un listado de experiencias basada en modelos de riesgos de sistemas de seguridad críticos.
Cramm	Se puede utilizar en sistemas y redes de información en todos los ciclos de vida del sistema de información desde la planificación y viabilidad, por medio del desarrollo.

Fuente: El autor

[39] Ibíd., párr. 7

6. CONVERGENCIA IT-OT

Las empresas y distribuidores de software como Microsoft y Linux ofrecen sistemas operativos de nivel básico de productos de IT y OT. Actualmente, se presenta la tendencia de los proveedores de OT a pasar de los sistemas operativos patentados a los sistemas comercializados o estandarizados (un proceso al que se llamará "convergencia"), este cambio se produce en la forma en que se administran los sistemas OT.

Los proveedores de consultoría e integración de sistemas, como IBM, están expandiendo sus capacidades para incluir los conceptos de IT y OT en procesos productivos. IBM ha sido un pionero con la iniciativa Smarter Planet (esencialmente sobre la integración de IT - OT), Incluso ahora, también, se está expandiendo la capacidad para que lograr la convergencia de los productos y negocios que ofrece en el campo de IT y OT. Empresas con larga historia en implementaciones de OT han notado el interés del cliente hacia el escenario convergente de IT y OT, por lo que están expandiendo sus capacidades para habilitar un servicio integrado que combine aspectos de IT y OT.

La convergencia de las Tecnologías de Información y Operación permite aumentar la competitividad empresarial, pues al lograr un adecuado e íntegro proceso de seguridad de la información, demuestra innovación tecnológica. Es necesario entender que esta convergencia es una herramienta más de la gestión organizacional y debe ser administrada como tal, además de manejarse como un instrumento de aquellos procesos que tienen como fin proveer a la organización de la información necesaria para un funcionamiento eficiente, eficaz y con calidad de servicio y productos. Además, se afirma que la convergencia o integración IT-OT, puede mejorar los siguientes procesos industriales:

Energéticos: A través de los dispositivos, adaptar el consumo energético en aquellas horas que la energía es más económica y reducirlo en aquellas que es más cara.
Medio ambiente: Los dispositivos inteligentes pueden medir datos meteorológicos, energéticos, etc. para que la planta pueda cumplir con los niveles de polución medioambientales establecidos por ley y adaptar toda la producción a estos.
Productivos: hace posible adaptar la demanda del cliente a la producción, para optimizar ésta y ahorrar costes.
Control de calidad: Permite fabricar con precisión y rapidez sin afectar al ritmo de producción y ajustar los tiempos para cumplir con las metas planificadas en el cronograma, generando un producto con las condiciones óptimas de producción y el cumplimiento de las características de diseño.
Mantenimiento: con la posibilidad de proceder a un mantenimiento predictivo que reduzca las averías y nos permita diseñar mejor el mantenimiento para reducir las pérdidas que éste puede ocasionar.

Asimismo, las mejoras también se incorporan en el proceso comercial y logístico y agilizarán el proceso de venta del producto.[40]

Los comparativos tecnológicos entre IT-OT, muestran un acercamiento y crecimiento de la industria con los avances tecnológicos que hacen que sus nuevos dispositivos y sensores sean más controlables y verificables. A continuación, en la Tabla 3, se pueden observar algunas de las diferencias entre IT y OT, en cuanto al entorno, compatibilidad, seguridad, homogeneización y las comunicaciones.

Tabla 4. Diferencias entre IT y OT

Característica	IT	OT
Entorno	Multifuncional condición favorable. Se prima la rapidez y se puede permitir el reinicio. Recambios entre 2 y 5 años	Limitación de funciones, condiciones desfavorables. Se prima la fiabilidad, integridad y cero paradas. Recambio entre 10 y 20 años.
Compatibilidad	Selección de equipos por funcionalidad, rápida adaptabilidad.	Dependencia de terceros. Acondicionamiento en el proceso de pruebas de estrés e imprevistos.
Seguridad	Concepto maduro, tanto para acceso físico como electrónico.	Aplicabilidad de conocimientos IT en un entorno distinto. Vulnerabilidades
Homogenización	Funcionalidades claras y concretas. Equipamiento homogéneo.	Variabilidad de entornos y elementos. Distinción de equipamiento de múltiples marcas y funciones.
Comunicaciones	Topología IP, protocolos de accesos, gestión estándar de puertos.	Protocolos de procesos, variabilidad de tipología de tecnologías (series, IP, buses de control, etc.)

Fuente: FERNÁNDEZ MARTÍN, Marcos; OLMEDA ARROYO, Roberto y LARREA JASPE, Marta. Por qué debe plantearse la convergencia entre sistemas OT e IT. Red Computerword, 2016. Recuperado de https://red.computerworld.es/actualidad/por-que-debe-plantearse-la-convergencia-entre-sistemas-ot-e-it

[40] OASYS, Redacción. Integración OT e IT para una Industria 4.0 En: Oasys Barcelona [blog] 2015. Recuperado de https://oasys-sw.com/integracion-ot-e-it-para-una-industria-4-0/

La convergencia IT-OT, consiste en buscar para OT mejoras en los procesos y en la seguridad de toda su estructura, mediante buenas prácticas, que en primer paso generen un orden, con procedimientos en cada uno de los procesos en los cuales está involucrada la información, y que es determinante para contribuir a la seguridad.

6.1 TECNOLOGÍA Y APLICACIONES DE IT EN OT

La tecnología de base converge en IT-OT, en los sistemas propietarios, los cuales hacen su aporte a través de la mayor utilización de protocolos y estándares genéricos que aportan en las soluciones de arquitecturas híbridas, con capacidad de soportar las operaciones de la infraestructura critica aportando soluciones de seguridad, almacenamiento y procesamiento, adoptando opciones como la nube u otros procesos industrializados capaces de soportar la demanda de OT.

La integración IT-OT, a nivel del modelo OSI en la capa de aplicación, está condicionado por las buenas prácticas del manejo de la información en los procesos industriales y por los desarrollos que ofrecen los proveedores en soluciones de seguridad del software. Aplicaciones para la gestión de energía, transporte, producción en serie, entre otros. Predominan aplicativos que son desarrollados con una arquitectura tradicional para OT.

Las tendencias en soluciones para OT incluyen en la actualidad protocolos y una mayor adopción de compatibilidad para aportar a la seguridad de la información de infraestructuras críticas. Finalmente, los fabricantes de motores de bases de datos y aplicaciones móviles están adoptando las tecnologías operacionales para aportar en el mantenimiento de la disponibilidad, integridad y confidencialidad en todos los procesos de información.

6.2 GOBIERNO Y ARQUITECTURA

La integración del Gobierno de IT - OT es un factor complejo por todas sus implicaciones basadas en los procesos y buenas prácticas de IT. Para realizar una transformación en los procesos de OT, es necesario contar con la iniciativa y la voluntad del cambio en muchos de sus procedimientos, y con la creación de procesos que empiecen a dar un orden lógico y seguro a la información producida.
Para generar un gobierno de OT basado en el servicio confiable y capaz de cubrir las necesidades de los procesos de información, se requiere de un líder o representante de la dirección que cuente con el apoyo y la capacidad de comprometer recursos para el cumplimiento de los objetivos a través de una gestión de riesgos y el manejo de eventos e incidentes basado en una dirección estratégica.
La adopción del gobierno de IT en OT representa la base para el cumplimiento de los procedimientos y normas al fin de integrar estándares que operen con

arquitecturas modulares de IT y OT en un nivel estratégico capaz de adoptar e implementar tecnologías que suplan las necesidades para el manejo de la información.

6.3 BUENAS PRÁCTICAS EN OT

6.3.1 Inventario de equipos. Se requiere de un inventario de los equipos, de OT, que se pueden catalogar como elementos de los sistemas de información operacionales, que hacen parte de un sistema de producción y pueden ser vulnerados remota o físicamente. El inventario de equipos debe contar con toda la información básica que se le debe tomar a un equipo, como: sistema al cual pertenece, serial, modelo, licencias, ubicación, activo de la organización y estado actual.

Adicional a lo anterior, es fundamental contar con todas las licencias de los aplicativos con los que se disponen, las versiones, actualizaciones y los parches de seguridad. Si se cuenta con un inventario, es más fácil identificar cada uno de los componentes del sistema operacional, con las necesidades a corto y largo plazo, tanto para actualizar por obsolescencia o por mejoras tecnológicas.

6.3.2 Niveles de servicio. Es necesario construir un catálogo con los niveles de servicio de los procesos de la operación, estudio de roles y responsabilidades en todas las etapas, y en caso de ser necesario, contratar apoyo externo para solución de fallas o incidentes para los cuales no se pueda dar una respuesta oportuna desde el personal interno.

En IT han existido generalmente procesos de desarrollo, roles, responsabilidades, niveles de servicio, gestión de hardware, aplicaciones, con administración, que estaban tradicionalmente planificados y programados siguiendo un ciclo de vida planificado del software o del hardware. En cambio, en OT, los sistemas son mantenidos mayoritariamente por ingeniería como una parte menor de una infraestructura, esto se da por los pocos conocimientos de las buenas prácticas de IT, porque, además, su mantenimiento se realiza de manera poco estructurada y sin coordinación con IT, haciendo que el soporte y mantenimiento de los sistemas de OT no sea eficaz ni eficiente, incrementando los costes, de los mismos, a largo plazo. Por lo general, en la gestión de incidencias y peticiones en OT, están presentes las malas prácticas. Una mala práctica común es la atención de incidentes solo en el momento de la ocurrencia, no existe inventario, gestión de configuración, gestión del cambio y es habitual carecer de una estrategia y gestión de proveedores.

Para las organizaciones, IT se ha caracterizado por mantener una gestión “centralizada”, con una estructura orientada al servicio de los usuarios (en lugar de ofrecer simplemente tecnología), y con una atención estructurada y sistemática. En cambio, OT se caracteriza, a nivel general, por carecer de una plataforma de soporte para la gestión de incidentes y servicios a los usuarios que permita el análisis y el desarrollo, para la comprobación de las especificaciones a implementar en los proyectos, así como los roles y perfiles necesarios para el cumplimiento de los requerimientos de la norma ISO27001-2013.

IT lleva años enfrentándose a la rápida evolución tecnológica, mejorando sus prácticas constantemente, lo que genera aprendizaje rápido de sus perfiles informáticos. Por el contrario, esta situación es nueva para OT, que está gestionada por perfiles que no cumplen con las necesidades técnicas y tecnológicas, para una gestión, planificación y atención de IT.

En las Empresas donde se manejan Tecnologías Operacionales, los procesos son muy importantes y dependen de la disponibilidad de los equipos, generando una confidencialidad para contratar y mostrar al exterior lo que se hace. En muchas ocasiones se cuentan con excelentes procesos de servicios o fabricación, pero no con los procesos informáticos documentados para la atención de fallas e incidentes, lo que hace que se dependa, exclusivamente, de la rapidez del personal para la atención en caso de una parálisis de la operación. No contar con niveles de servicios hace que las fallas no sean catalogadas, además lleva a que el personal de la empresa, poco capacitado frente a este tema, deba atender los incidentes que ocurran.

Los niveles de servicios mantienen un orden en los procesos y en las fallas de los sistemas de información que puedan aparecer. para identificar esos niveles, ITIL recomienda:

- La funcionalidad y características del servicio.
- El nivel de calidad del servicio.
- La interacción del servicio con su infraestructura TI.
- La planificación de la implantación del servicio.
- La disponibilidad del servicio.
- La continuidad del servicio.

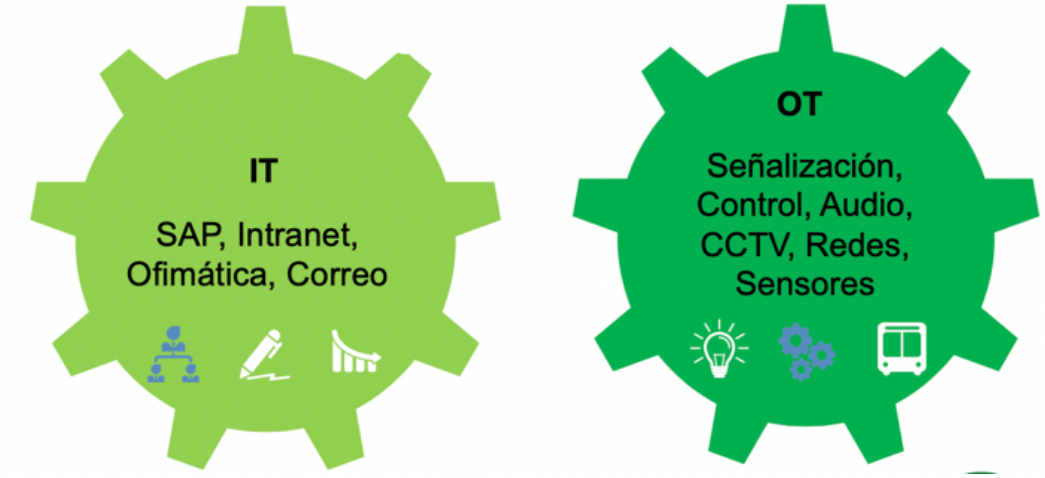
- La integración del servicio con otros servicios del cliente. [41]

[41] RÍOS HUÉRCANO, Sergio. Manual de ITIL V3 Integro, Sevilla, Biable Management: Excellence and Innovation, 2015, p.22. Recuperado de https://docs.supersalud.gov.co/PortalWeb/planeacion/AdministracionSIG/GSDE01.pdf

7. MODELO DE CONVERGENCIA

Resulta necesario realizar una comparación de los elementos que representan a IT-OT, tal y como se muestra en la Figura 9, en IT la descripción es a nivel de aplicaciones y se encuentran procedimientos de accesos a correos y aplicaciones de ofimáticas, las cuales requieren de servidores y elementos de la Seguridad Lógica. OT en su estructura cuenta con elementos que se pueden asociar con la Seguridad Física, como sensores, equipos de borde y terminales que generan datos para el monitoreo y control.

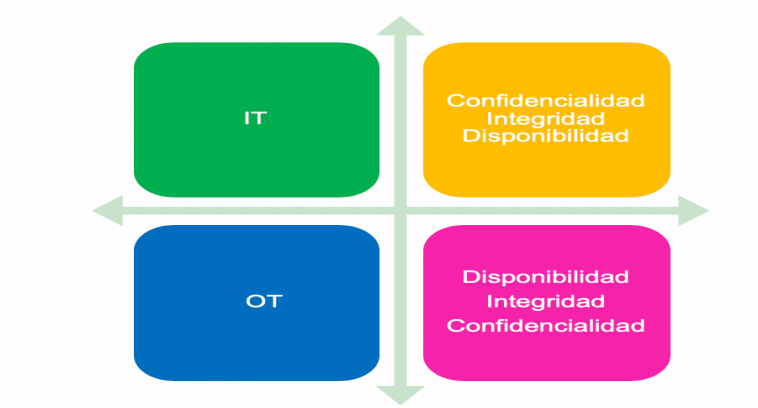
Figura 9. Elementos de IT y OT



Fuente: El autor.

Para los pilares de la seguridad de la información, IT y OT cuentan con una estructura diferente, pues mientras para IT lo más importante es la confidencialidad, para OT es la disponibilidad, la cual es necesaria para mantener las operaciones y contar con la producción o el servicio que se está ofreciendo. Para la empresa es necesario contar tanto con la disponibilidad como la confidencialidad, sobre todo en sus procesos y la información producida, manteniendo otro pilar como la integridad, la cual en IT y OT se maneja en un mismo nivel intermedio, como se observa en la Figura 10.

Figura 10. Pilares de la seguridad de la información en IT y OT



Fuente: El autor.

7.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Para OT es necesario crear una política de seguridad que trabaje en la misma dirección y línea de IT, pero teniendo presente las implicaciones de las Tecnologías Operacionales. Se debe tener en cuenta, en la política, las implicaciones y las necesidades operacionales para no describir o visionar elementos que no se puedan cumplir. El MSPI recomienda un modelo para la política de seguridad de la información.

> La Política de Seguridad de la Información es la declaración general que representa la posición de la dirección con respecto a la protección de los activos de información, que soportan los procesos de la organización y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, a través de la generación y publicación de sus políticas, procedimientos, directrices e instructivos, así como de la asignación de roles y responsabilidades generales y específicas para la gestión de la seguridad de la información. La política de seguridad de la información debe estar direccionada a:
>
> - Minimizar el riesgo de los procesos misionales de la entidad.
> - Cumplir con los principios de seguridad de la información.
> - Cumplir con los principios de la función administrativa.
> - Mantener la confianza de los funcionarios, contratistas y terceros.
> - Apoyar la innovación tecnológica.
> - Implementar el sistema de gestión de seguridad de la información.
> - Proteger los activos de información.

- Garantizar la continuidad del negocio frente a incidentes. Alcance/Aplicabilidad[42]

La dirección, como líder y primer responsable del proceso, debe apropiarse de las políticas de seguridad, aplicándolas como herramientas para la toma de decisiones. Junto con dichas políticas, debe usarse también la gestión de riesgos como medio para la identificación de las amenazas frente a las cuales se encuentra la organización y los procesos que esta desarrolla en su actividad económica.

7.2 PROCEDIMIENTO DE SEGURIDAD DE LA INFORMACIÓN

Dentro del procedimiento de seguridad de la información se contemplan los recursos necesarios para la convergencia de IT-OT, como la gestión de los activos que representan un valor económico para la organización e, igualmente, las necesidades de recursos humanos para el cumplimiento de las políticas de seguridad de la información y los procedimientos para los controles de acceso a los diferentes sistemas de información. También, se contempla, la seguridad física como soporte de seguridad para los equipos e infraestructura critica, su nivel de cifrado y la seguridad en el transporte de la información.

7.2.1 Control del recurso humano. Para OT es necesario contar con personal comprometido que cumpla con los requisitos y políticas establecidas por la organización, con base en los diferentes perfiles establecidos por la empresa, generando gestión del cambio y sensibilización en los procesos que interactúan dentro del manejo de la información de una manera segura. Se debe realizar un cronograma de capacitaciones y sensibilización para todo el personal, de acuerdo con su actividad, suministrar la información necesaria con los procedimientos que deben cumplir en sus obligaciones laborales.

Cuando se ingresa o se realiza retiro de personal se debe gestionar adecuadamente la información, para esto, puede ser conveniente, generar un procedimiento en el cual se establezcan las cláusulas de confidencialidad necesarias y las responsabilidades tanto de las personas que ingresan como de las que se retiran.

7.2.2 Gestión de activos. Para IT la gestión de activos es parte fundamental. Por otro lado, para OT no es una práctica que se realice con frecuencia. Es por esto que se debe generar un inventario de activos de los equipos de OT, como, por ejemplo, softwares, hardware, aplicaciones y licencias, para obtener todos los datos

[42] MINTIC. Elaboración de la política general de seguridad y privacidad de la información. Colombia, 2016, p.10. Recuperado de https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

necesarios e identificar la cantidad real con los que se cuenta lo que permitirá controlar de una manera más organizada los elementos que se tienen, poder generar un presupuesto acorde con las necesidades e identificar los valores de los activos de información para fortalecer la seguridad de la información.

En OT es necesario la gestión de activos para tener un control de actualizaciones de hardware, software y obsolescencia tecnológica. En Tecnologías Operacionales, es común encontrar equipos con la fecha de fin de vida útil vencida, como no se encuentra en el plan de renovación y su funcionamiento es, al parecer, óptimo no se realiza el cambio, ignorando las vulnerabilidades que va obteniendo, un sistema, con los avances en tecnologías de la información. Para la gestión de activos de una empresa, se debe realizar un procedimiento de organización donde se ingresen los siguientes datos:

- Nombre del equipo: como se le conoce al equipo de acuerdo con las caracterizaciones escogidas.
- Nombre del sistema que soporta: describir que plataforma tecnológica soporta el equipo dentro de la estructura de la organización.
- Sistema operativo: Windows o Linux, entre otros.
- Aplicaciones con las que cuenta: nombre de las aplicaciones con que cuenta el dispositivo.
- Fecha de compra
- Garantía: inicio y fin
- Soporte: si cuenta con el soporte y hasta cuándo puede recibirlo del proveedor o contratista que lo realiza.
- Software actualizado: definir si cuenta con software actualizado y cuál fue la última versión.
- Modelo, serial y características técnicas.

7.2.3 Procedimiento para el ingreso seguro. La entidad debe dejar claro como maneja, controla y gestiona el acceso a los sistemas y equipos que tienen información. Demostrando que el acceso se da de una manera segura y que, además, la empresa se encuentra preparada para enfrentar los ataques que puedan presentarse y que emplea los métodos necesarios para validar la identidad de quien intenta acceder a las redes.

En OT no se practica el manejo seguro de los sistemas. Por tanto, se requiere emplear métodos para evitar ser atacados, o caer en equivocaciones, que puedan generar pérdidas económicas por no controlar el ingreso a los sistemas de

información. Es importante, entonces, generar un procedimiento con políticas de ingreso seguro a cada uno de los sistemas y equipos que lo soporten para controlar y registrar los cambios o configuraciones realizadas.

7.2.4 Procedimiento de gestión de usuarios y contraseñas. En el procedimiento de gestión de usuarios y contraseñas, la organización deberá describir el proceso de creación de usuarios y contraseñas, la clasificación de los roles y perfiles con que cuenta la entidad, el nivel de seguridad para la creación de contraseñas seguras y la selección y utilización de un cifrado que soporte un nivel aceptable de acuerdo con las políticas definidas por la entidad.

Para OT, se debe generar un procedimiento para obtener una adecuada gestión de los ingresos a las plataformas operativas y poder controlar, y actuar, de la manera indicada en los procedimientos, para que en caso de un ataque interno se pueda identificar fácilmente quien lo realizó y desde donde.
Muchas de las aplicaciones desarrolladas para las Tecnologías Operacionales no cuentan con la posibilidad de modificar el usuario y contraseña, se presenta por defecto un usuario y una contraseña que no permiten ser modificado. Por tanto, al momento de realizar actualizaciones de las aplicaciones o software especializado, se debe realizar gestión de cambio y contar con procedimiento para la compra y actualización.

Además, para los dispositivos operacionales que cuentan con usuario y contraseña de fábrica, se recomienda realizar un control de usuario y contraseña por medio de la utilización de otro dispositivo o equipo de cómputo que gestione el acceso en el caso de que no pueda estar enlazado con el directorio activo de la organización. Con esto se generará un registro y podrá ser monitoreado. Se puede tener como opción la instalación de un HIPS (Control de intrusión en máquinas) en los equipos que tienen el usuario y la contraseña de fábrica, para controlar e identificar si alguien realizó un cambio que no es normal.

7.2.5 Criptografía. El proceso criptográfico en la organización como herramienta que soporte la disponibilidad, integridad y confidencialidad de la información y el uso correcto de las llaves criptográficas durante todo el proceso de seguridad de la información. Para las Tecnologías Operacionales la criptografía no es usada con regularidad, la seguridad se basa en el cifrado de los dispositivos adquiridos, que en muchas ocasiones son textos planos, fáciles de encontrar.

La criptografía en OT requiere de un cifrado que ayude con los procesos de transmisiones seguras y de almacenamiento de toda la información que se recibe de los sensores o de los diferentes dispositivos usados para controlar procesos. Una oportunidad de mejora para las tecnologías operacionales es IoT (internet de las cosas), pero la seguridad con que estos dispositivos salieron al mercado no es

muy adecuada para la seguridad de las operaciones, a medida que evolucionan, mejoran en seguridad, son una opción para las Tecnologías Operacionales con las mejoras en cifrado de las comunicaciones y los datos que generan para controlar los procesos. Otra posibilidad, para implementar, es encriptar los mensajes que se transmiten, de las operaciones al personal involucrado, de una manera segura, con claves o llaves para su visualización y tener un control para la generación y caducidad de las llaves.

7.2.6 Seguridad física y del entorno. Este numeral hace referencia a los cuidados que se deben tener para prevenir el acceso a todas aquellas áreas en las que puede generarse algún daño a la infraestructura, las instalaciones y la información. Para mantener la seguridad física y la del entorno, pueden plantearse procedimientos en los cuales se cuente con la participación del área de seguridad y vigilancia de la entidad. Algunos procedimientos son:

Control de Acceso Físico: Se debe realizar un procedimiento para el control de áreas seguras con registros o tecnología necesaria para identificación y control. Además, la empresa debe velar por la seguridad de las instalaciones donde se cuenta con infraestructura crítica, realizando un control de acceso físico, por medio de acceso con tarjetas lectoras, las cuales preferiblemente deben estar apoyadas por cámaras de seguridad. Los sistemas de seguridad física deben estar en la capacidad de generar reportes que apoyen a las investigaciones de seguridad y al cuidado de áreas denominadas críticas. Los equipos que se instalan como apoyo a la seguridad física también brindan un control para la protección de los activos y deben estar en el procedimiento de control de acceso físico, asegurando las zonas vulnerables que albergan infraestructura crítica y de valor para la operación.

7.2.7 Seguridad de las operaciones. Para IT una buena práctica es la gestión del cambio, la cual se genera a partir de la programación de las actividades y de los resultados obtenidos en los procedimientos de los niveles de servicio, los cuales deben ser registrados y analizados por un comité de cambios, encargado de desarrollar el análisis de las diferentes situaciones.

En las Empresas donde se trabaja con OT no se cuenta con una buena práctica para evidenciar los cambios realizados a los equipos o registrar la solución de incidentes ocurridos. Muchas veces, se cae en reprocesos por no registrar las soluciones realizadas. Por lo anterior, se debe implementar un comité de cambios que gestione y programe las intervenciones en los equipos, y contribuya al registro de las soluciones a los incidentes de la operación, lo cual generará una ganancia en tiempo de solución de fallas. Los comités de gestión de cambio deben contar con un acta donde se plasme la información suministrada durante la duración y sea compartida entre los interesados.

En Tecnologías Operacionales es común hacer pruebas de infraestructura en el ambiente de producción, es decir, en plena operación, emplear configuraciones nuevas o actualizaciones, lo cual genera un riesgo muy grande para las infraestructuras críticas, en muchas ocasiones es difícil recuperarse de las fallas que puedan presentarse. Es importante contar con un ambiente de calidad donde se prueben y se dejen en observación los cambios a realizar. Por lo tanto, se hace necesario adquirir un ambiente de calidad o de pruebas que ayude a simular la operación y evite que ocurran fallas innecesarias, además, el ambiente de calidad o de pruebas es importante porque permite identificar las fallas que posiblemente se pueden presentar y actuar antes de que estas fallas se manifiesten.

En la gestión de operaciones de OT nunca se hablaba de la protección contra código malicioso, es una falencia muy grande en Tecnologías Operacionales. El hardware y el software son fabricados sin la posibilidad de ser compatibles con un antivirus lo que lo hace muy vulnerable ante los ataques informáticos. En las OT, se hace fácil infectar los equipos, no se cuentan con políticas que restrinjan el uso de dispositivos extraíbles que usan para trasladar información de un equipo a otro sin un control. Se debe generar un control y procedimiento para el uso de unidades extraíbles, y si es necesario no utilizarlas. Es importante, también, adquirir tecnología que opere de la mano de los antivirus, o realizar una separación de ambientes de producción y calidad, para probar las reglas del antivirus, además de aplicarle los ajustes necesarios que el mismo antivirus presente.

7.2.8 Seguridad de las comunicaciones. Para la protección de la red es necesario describir la información detallada de todos sus componentes, equipos, direccionamiento y los protocolos que se están utilizando, así como, información de los datos que se están transportando. En este caso, es necesario contar con una infraestructura de red que soporte las necesidades, y que esté acorde con la criticidad de las operaciones. En adición a lo anterior, se debe contar con dispositivos que brinden un apoyo, como sistemas de detección de intrusos y firewall que ayudaran a mitigar el riesgo de ser víctimas de ataques.

Para las Tecnologías Operacionales lo más importante siempre ha sido la disponibilidad de sus sistemas para una óptima operación, pero con la intensificación de los ataques hacia las infraestructuras críticas, también se hace necesario la confidencialidad de la operación, y es importante crear un procedimiento donde se identifique los elementos más críticos al momento de transportarlos o enviarlos a otros lugares, internos o externos, además de, cómo se hará el transporte, qué medidas de privacidad se le dará a la información de acuerdo a la clasificación que se tenga, y quién es el responsable de estos procedimientos y las acciones a tomar en todos los casos. Es necesario que se conozcan por parte de OT las tecnologías y las herramientas existentes para para un transporte seguro que aporte privacidad a la información.

7.2.9 Relación con los proveedores. Para los acuerdos con los proveedores es necesario tener en cuenta las cláusulas de confidencialidad, en caso de ser necesario suministrar información. Generar controles para evitar fuga de información. Si el proveedor realiza actividades constantemente sobre las plataformas o Tecnologías Operacionales de la empresa, se deben programar gradualmente auditorias y solicitar informes sobre el manejo de la información. Para realizar un cambio debe presentarse ante el comité de cambios, y, una vez llevado a cabo, debe mostrarse al mismo los resultados obtenidos.

7.2.10 Adquisición, desarrollo, y mantenimiento. Se deben realizar procedimientos para la adquisición de software, que involucren todas las características de seguridad para verificar que el software cumpla para con los lineamientos necesarios para su operación, con módulos de mantenimiento que siempre brinden disponibilidad, integridad y confidencialidad frente a la información.

7.3 ROLES Y RESPONSABILIDADES

Los roles y responsabilidades son fundamentales en los sistemas de gestión de seguridad de la información. Se recomienda identificar los responsables de la Seguridad, pues es necesario, definir quién se va a hacer cargo de las actividades de seguridad de la información, quién llevará acabo los proyectos que se inicien y quién tendrá a su disposición los recursos necesarios para que se realicen los procedimientos de la mejor manera. Debe ser una persona capaz y con conocimientos en el área. El responsable debe ser elegido por la dirección y debe contar con todo el apoyo para llevar a cabo los cambios que sean necesarios en pro de la seguridad.

En OT es necesario contar con personal que tenga los suficientes conocimientos para impartir las mejores medidas. Es necesario, además, que el equipo de trabajo de OT, se conformado por personas de las diferentes áreas que conocen la operación, esto ayudará a tomar mejores decisiones y realizar unos procedimientos más acordes a las necesidades, teniendo presente las diferentes circunstancias que se generan y a las cuales se enfrentan cada una de las personas, del equipo, en su rol laboral, para poder generar una cultura de seguridad de la información.

Se describe a continuación algunas de las responsabilidades con las cuales debe contar el líder o el equipo de la convergencia en seguridad de IT a OT:

- Apoyarse en herramientas y en el conocimiento adquirido en otros proyectos para una adecuada convergencia.

- Coordinar la búsqueda de casos de éxito para apoyarse y tomar las buenas prácticas de estos que puedan aportar.
- Realizar un autodiagnóstico de cómo se encuentra OT e identificar la brecha con la que cuenta la organización con IT para generar las acciones más adecuadas.
- Generar un plan de trabajo con las descripciones de las actividades. En OT se conocen muy bien el paso a paso del qué hacer en las áreas operativas, pero en la mayoría de estas no se cuenta con una documentación adecuada, como procedimientos y registros, que pueda ser utilizada para implementar mejoras.

Se debe generar un plan donde se describa cada una de las fases con la especificación de lo que allí se realizará, de los recursos necesarios para el cumplimiento y, finalmente, el cronograma.

Se pueden definir estas fases para OT con base en el PHVA (Planear, Hacer, Verificar, Actualizar), donde en la Fase uno, se podría generar un autodiagnóstico, levantamiento de información, identificación de riesgos, clasificación de los componentes, identificando, además, cuales se pueden controlar dentro de la seguridad, se deberá buscar alternativas en el medio o, de ser necesario, solicitar un cambio gradual. En esta fase también se diseña y se definen los entregables en cada fase. La fase dos es la fase de pruebas, implementación y ajustes necesarios. Para la fase tres se requiere monitoreo, control de todos los procedimientos realizados y los registros que se presentan de cada fase. Es necesario monitorear adecuadamente, realizar mejoras o replantear si es necesario.

7.4 GESTIÓN Y CLASIFICACIÓN DE LOS ACTIVOS

Para administrar los activos que generan información es necesario contar con el inventario. El inventario debe estar completo, debe permitir identificar casa elemento, con una clasificación detallada de los activos que poseen o son parte de la información de la organización. En OT, como ya se ha mencionado, la clasificación de los activos de información no es una buena práctica. No obstante, es importante considerar el uso de una aplicación que apoye con la gestión para la clasificación, y generar un valor al activo identificando el grado de protección que requiere, soportado en un análisis de riesgos.

7.5 GESTIÓN DE RIESGOS

Para OT es necesario apoyarse en la gestión del riesgo para identificar las vulnerabilidades con las que se cuenta, las amenazas y la posibilidad de que un

riesgo se materialice. Es por lo anterior que la gestión e identificación de los riesgos, en los sistemas de información, es fundamental para la conformación e implementación de un sistema de seguridad de la información.

Para IT-OT la identificación y análisis de los riesgos debe ser una práctica en la cual, ambos se complementen. Existen controles y tratamientos que son soportados, tanto por IT como por OT, y en ocasiones deben ser compartidos. Las etapas que se recomienda para la gestión de activos en OT son:

- Identificación del riesgo: se debe identificar cada uno de los riesgos que se presentan en todas las actividades operacionales y que atentan contra la seguridad de la información.
- Identificación de las causas: es importante distinguir aquellos procesos, elementos y demás que pueden generar que un riesgo se materialice. Junto con esta identificación, se debe hacer una descripción detallada y asignarle un valor a cada posible causa.
- Consecuencias del riesgo: se deben detallar las consecuencias presentadas por la materialización del riesgo, como la perdida de la credibilidad hacia los clientes, perdida en producción, perdida de la reputación y perdida de negocios. Se acuerdo con las causas seleccionadas se pueden prever y prevenir las consecuencias que se pueden presentar.
- Identificación de controles: en muchos de los procesos ya se cuenta con controles, los cuales se ejecutan, sin ser identificados de una manera oficial. Sin embargo, estos controles aportan a mitigar las diferentes amenazas y vulnerabilidades que se tienen, es importante describirlos y de ser necesario generar un procedimiento para cada uno.
- Para las causas que no se tengan controladas se debe crear un tratamiento, en el cual se describa el elemento que presenta el riesgo sin control, las actividades a realizar, los tiempos de implementación, los responsables y el control que soportará y permitirá que este tratamiento sea aplicado con éxito.

Para las organizaciones, es necesario valorar los riesgos y describir cuales se asumirán. Se debe crear un procedimiento y un formato donde queden plasmadas todas las actividades mencionadas, poder realizarles seguimiento y cerrarlas en el momento que sea necesario, por ejemplo, cuando un riesgo está totalmente controlado y se ha vuelto parte de las actividades normales.

7.6 INDICADORES GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

En IT es normal soportar la información con indicadores de servicios y de seguridad, en OT se utilizan para medir la producción y la indisponibilidad de los sistemas, pero no para medir los procesos de seguridad de la información. Para OT es fundamental, como aporte a la administración de la seguridad de la información, realizar mediciones de sus procesos. Se recomienda medir:

- La efectividad de la implementación de los controles de seguridad tanto los que se tenían como los nuevos que se implementan.
- La eficiencia de la convergencia en seguridad de IT y OT.
- Donde se requiere tener un mayor control y auditoria.
- Las Comunicaciones al interior.
- Insumos al plan de análisis y tratamiento de riesgos.

7.7 CONTINUIDAD DE NEGOCIO

En IT se cuentan con planes de continuidad ante contingencias de ataques que afectan el negocio, en OT es necesario diseñar un plan que contenga los procedimientos para continuar con las operaciones en caso de ataques o fallos en los sistemas de información y recuperar la disponibilidad de la infraestructura crítica.

Entonces, contar con un plan de continuidad del negocio es primordial para las Tecnologías Operacionales. La disponibilidad, como parte fundamental en OT, puede ser afectada en caso de materializarse un riesgo, por lo tanto, es fundamental tener un plan para continuar con la operación en forma degradada.

Para el plan de continuidad, se debe tener en cuenta los planes y cronogramas de copias de respaldo, restauraciones y reemplazo de ser necesario, identificar los tiempos que podemos asumir y hasta qué punto podemos degradar la operación de los sistemas críticos y cuanto riesgo está la organización dispuesta asumir.

7.8 PLAN DE COMUNICACIÓN, SENSIBILIZACIÓN, CAPACITACIÓN

Generar un plan de comunicaciones, sensibilización y capacitación es una de las partes más importantes y debe hacerse con mucho cuidado dentro de una organización. La información que se comparta y la cultura de la seguridad de la

información que se pueda generar a raíz de estas comunicaciones, pueden llevar al éxito de la adopción de las buenas prácticas.

Se requiere comunicar, al personal de la organización, los diferentes comités que se conformaron y los procedimientos, controles y registros que se deben cumplir para mantener la seguridad de la información. Es determinante que el personal entienda que todas las medidas que se tomen son por el bien de la organización y de cada uno de ellos, pues si no se tiene un buen control informático implementado, el personal también puede verse afectado en un ataque informático, por ejemplo, siendo víctima de suplantación de identidad.

Durante la estructuración del plan de comunicaciones y sensibilización, se debe analizar cada uno de los perfiles del equipo de trabajo OT, las funciones y las capacidades con el fin de determinar quién requiere de una mayor capacitación o sensibilización en los temas tratados y las buenas prácticas que llevaran a las OT a una convergencia con IT y controlar de una manera más segura las operaciones.

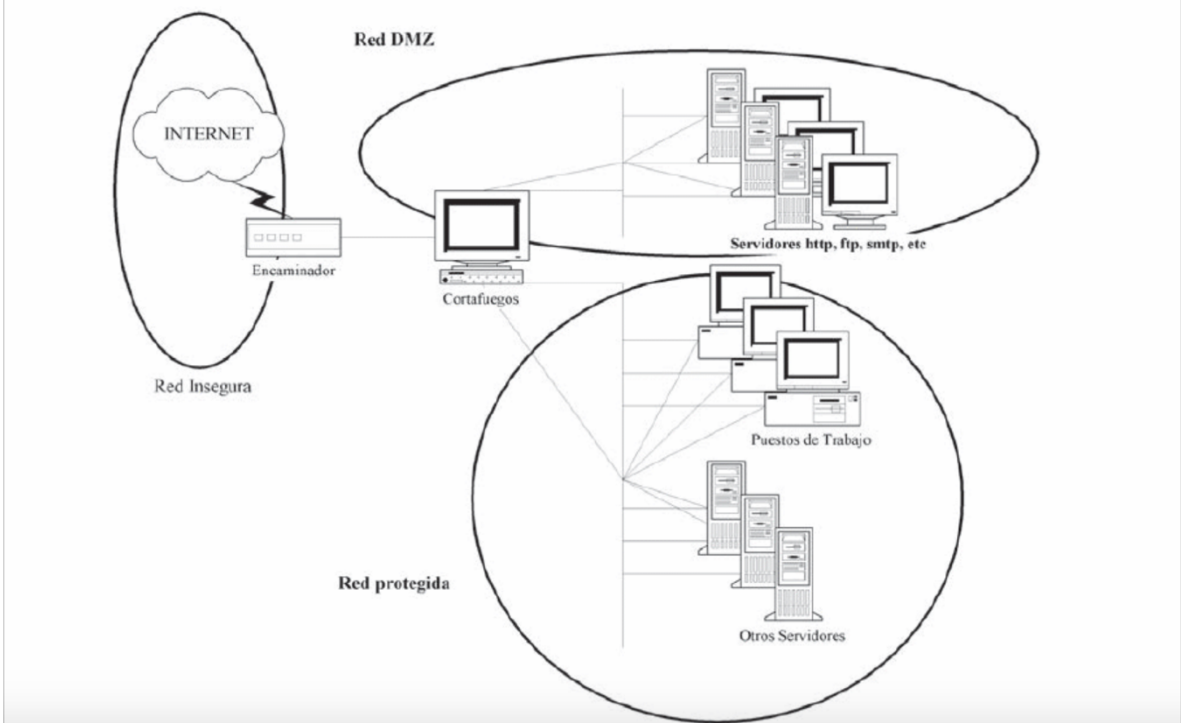
8. ARQUITECTURA DE CONVERGENCIA SUGERIDA

Las redes industriales como todas las redes en su arquitectura y diseño es fundamental contar con una segmentación que brinde servicios independientes que de acuerdo con su criticidad se encuentren protegidos. Las redes corporativas deben estar lo más lejana posible y de ser necesario aislada de las redes con salida al exterior, en este caso internet. En caso de requerir publicar un servicio para consultar desde el exterior es muy importante tomar las medidas de seguridad para proteger la red operativa.

Para el apoyo de la seguridad lógica en las redes industriales existen diferentes equipos y aplicaciones que ayudaran a mitigar los riesgos asociados a las infraestructuras críticas, generando arquitecturas convergentes entre IT y OT en las redes y en las aplicaciones que se utilizan entre las cuales podemos describir:

DMZ (demilitarized zone): Los servicios, información, monitoreo o control de la red industrial debe ser publicada a internet, es necesario contar con una zona desmilitarizada, en la cual se publicarán los datos necesarios o solicitados sin necesidad de exponer los procesos internos industriales. En la Figura 11 se describe una configuración típica de una DMZ, con los servicios que se publican.

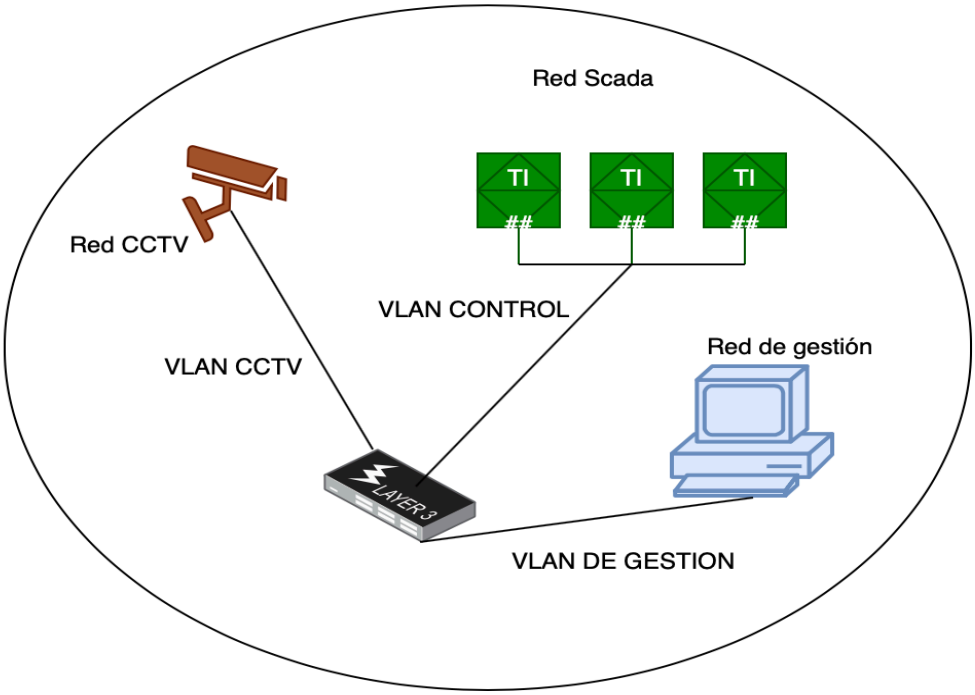
Figura 11. Topología de una DMZ Típica



Procesos y herramientas para la seguridad de redes, UNED - Universidad Nacional de Educación a Distancia, 2014. ProQuest Ebook Central, https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/detail.action?docID=3220062.

VLAN (Red de Área local Virtual): Cuando se habla de segmentación de red y de servicios independientes las configuraciones en VLAN son una opción de aportar a la seguridad, al no mezclar tráfico e independizar los servicios que se utilizan en las redes industriales. Las VLAN son interfaces lógicas basadas en el IEEE 802.1Q por los cuales se desplaza solo el trafico autorizado y direccionado para viajar, al cual se le da una número que identifica a cual VLAN pertenece y por esta se ingresa el servicio que solo llevara el trafico seleccionado, por ejemplo: CCTV (circuito cerrado de televisión), el video que se utiliza para la verificación de los procesos o para el apoyo de la seguridad física, este tráfico al ser video es mucho más pesado que el resto y se hace necesario que viaje por una sola VLAN muy diferente a otra que pueda llevar las tramas de control de los equipos de borde como sensores o PLC. En la figura 12 se muestra buenas prácticas de segmentación de redes a través de VLANs.

Figura 12. Segmentación por VLANs



Fuente: El autor.

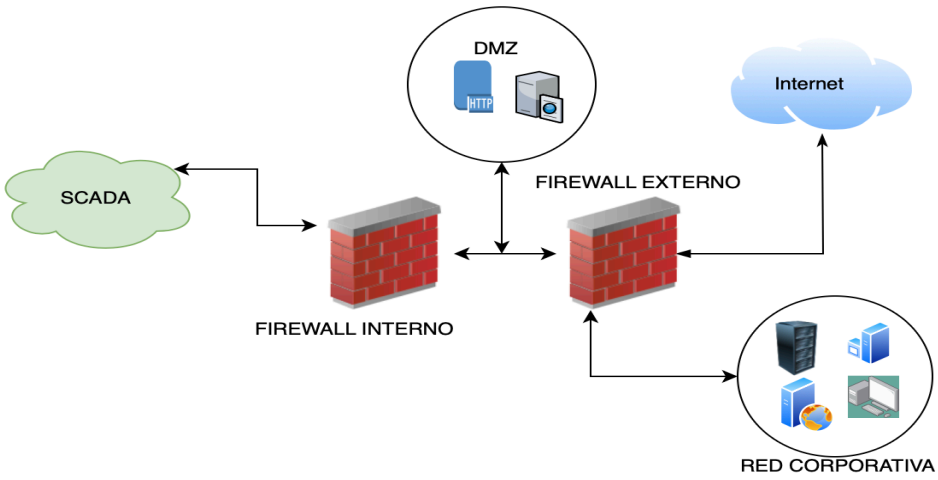
Configuraciones de Red: las buenas prácticas para las configuraciones de red industrial se basan en tener los dominios de trafico identificados y separados, para no tener problemas o fallos con los datos que deben transportarse desde un trasmisor hasta un receptor de manera óptima sin pérdida de estos y con integridad para cuando se dé una orden de encender o apagar o cambiar de estado un sensor este responda de forma adecuada realizando la instrucción solicitada. Los puertos de red y de datos que no se utilicen deben ser desactivados para no contar con conexiones que no se encuentren autorizadas y que puedan causar daños o congestiones en la red que no permita que los flujos de datos de alta prioridad lleguen.

Firewall (Cortafuego): dispositivo lógico de hardware o software utilizado para controlar el tráfico entre diferentes redes de datos (Segmentos), a través de la generación de reglas, la utilización de VPN (Red Privada Virtual) es una de sus funciones útiles para comunicar con sistemas aislados y que requieren de seguridad. Otra de las características es el filtrado de paquetes en la capa de red,

la conexión con los países que se tienen comunicaciones de salida o de entrada, o con el tráfico que sea autorizado.

Los firewalls en las redes industriales hacen parte de una manera activa, para las redes que requieren una conexión con el exterior, una de las configuraciones de firewall es contar con uno interno y otro externo, así se segmenta y se protege la red de control industrial (ICS), de ataques externos y de las redes corporativas, se generan reglas entre los dominios internos sin necesidad que estos se vean o mezclen el tráfico, los firewall de hardware prestan mayor disponibilidad en los entornos configurados de manera eficiente. En la figura 13 se muestra una configuración típica para los firewalls en una red ICS.

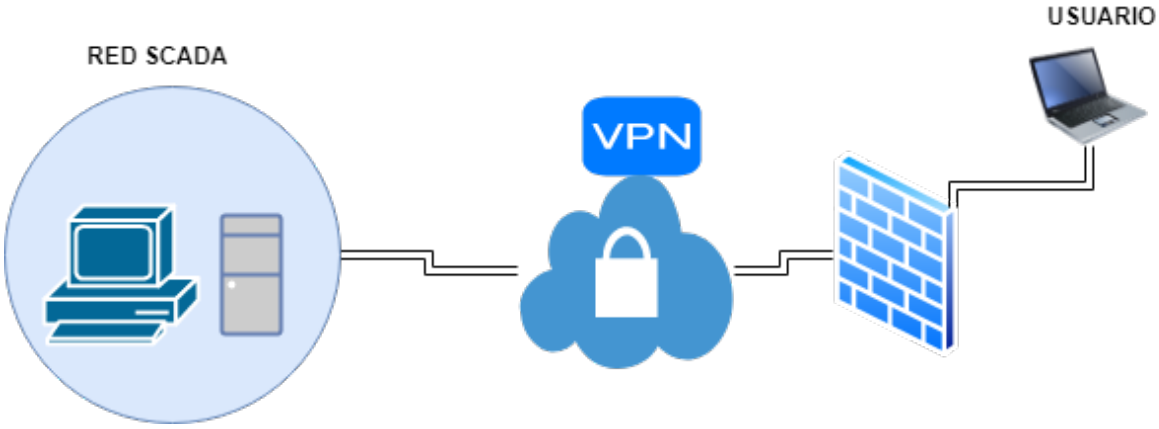
Figura 13. Configuración Típica Firewall Red ICS



Fuente: El autor.

Encriptación: para las comunicaciones ICS, es necesario contar con un cifrado que garantice integridad de la información en las conexiones y en el almacenamiento de la información en todos sus niveles. Las VPNs suministradas por los firewalls son la opción más adecuada para no combinar redes y garantizar una conexión segura de usuarios externos con servicios internos con un grado de encriptación para los datos que se están transportando, en la Figura 14, se describe la comunicación administradora, visualizador o gestor de la red SACDA a través de una VPN encriptada.

Figura 14. Comunicación por VPN

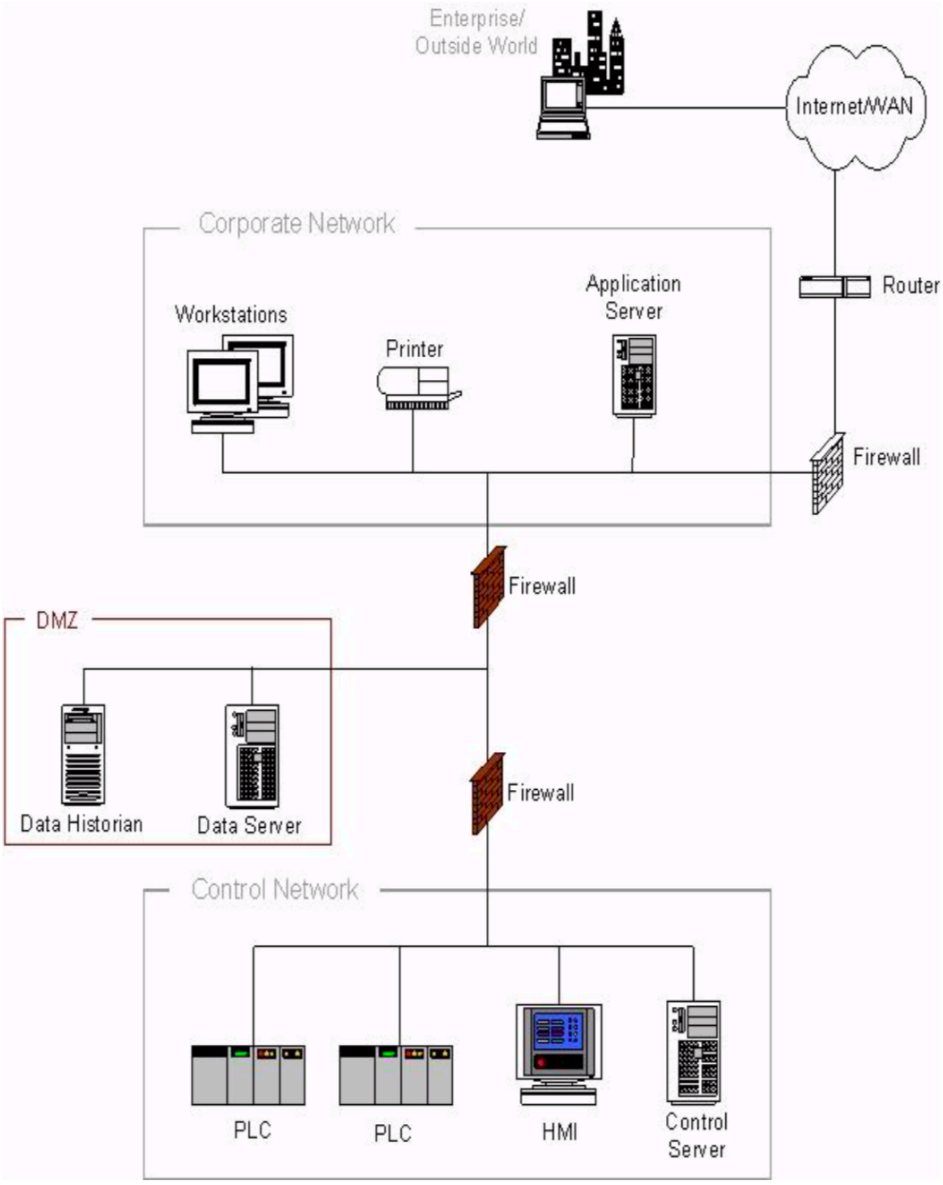


Fuente: El autor.

Para una arquitectura final de OT se deben tener en cuenta todos los elementos mencionados del modelo de convergencia de IT a OT, para generar mecanismos de seguridad por capas, también llamada Defensa en Profundidad, para que el atacante le sea más difícil pasar cada uno de los controles construidos y seleccionados para la para la seguridad de los ICS.

En la Figura 15, se describe una arquitectura final, sugerida para el modelo de convergencia, para el trabajo en conjunto de la red corporativa de una organización (IT) y la red operativa (OT), con los elementos necesarios para la protección de los ICS y como parte fundamental de protección de la producción industrial.

Figura 15. Arquitectura IT-OT



Fuente: STOUFFER, Keith *et al.* Guide to Industrial Control Systems (ICS) Security. En: NIST, revisión 2, mayo, 2015, 7 p. Recuperado de http://dx.doi.org/10.6028/NIST.SP.800-82r2

9. CONCLUSIONES

- La convergencia IT-OT que trae grandes beneficios para las organizaciones que operan las infraestructuras críticas con buenas prácticas de la seguridad de la información. Se pueden mencionar elementos como la protección de la información producida, la reducción en costos por contar con un inventario al día y con las necesidades descritas en temas de equipos, identificación de los riesgos, lo cual mitigara la materialización, el acceso a los sistemas de información, zonas seguras y la gestión de otros componentes que hacen de las tecnologías operacionales menos vulnerables.

- El modelo de convergencia de IT y OT permite la adopción de las mejores prácticas de IT, en materia de seguridad de la información, y de las necesidades con que cuenta OT en sus procesos.

- El modelo de convergencia IT-OT permite la adopción de estrategias que proporcionen elementos para disminuir los riesgos y las amenazas que se encuentran en el entorno y que a menudo son blanco de ataques, generando una indisponibilidad de las infraestructuras críticas.

- Este documento presentó una a una las posibles soluciones y acciones para permitir que la seguridad informática sea una práctica cada vez más completa e implementada dentro de las diferentes organizaciones.

10. RECOMENDACIONES

Para satisfacer la necesidad de brindar seguridad en los procesos de las tecnologías operacionales se vienen presentando dispositivos y sensores de borde (IoT), los cuales brindan la información a los servidores de OT y redes de comunicaciones, es necesario tener en cuenta las condiciones de seguridad que presentan y el cifrado que ofrecen para el transporte de la información, los cuales son el insumo más importante en las Tecnologías Operacionales. Por el crecimiento sin control de dispositivos se ha masificado su uso, sin controlar la seguridad. IoT ha hecho que se mejoren las condiciones de los equipos o sensores finales que antes, difícilmente, podían ser monitoreados, y, hoy en día, suministran información fundamental para las operaciones.

BIBLIOGRAFÍA

ALCARAZ, Cristian et al. Gestión segura de redes SCADA. Nuevas tendencias en gestión de redes, Novática. En: NICS Lab. Publications, 2008. p. 20-25. Recuperado de https://www.nics.uma.es/pub/papers/Alcaraz2008a.pdf

ÁLVARO YUNTA, Miguel. Implementación de las comunicaciones PC-autómata-robot mediante interfaz Ethernet industrial. Trabajo de grado Ingeniería Técnica Electrónica. Universidad Carlos III de Madrid. Madrid, 2009, 156 p. Recuperado de https://e-archivo.uc3m.es/handle/10016/6907

AREITIO BERTOLÍN, Javier. Seguridad de la información. Redes, informática y sistemas de información. España: Editorial Paraninfo, 2008. 566p. ISBN: 9788497325028. Recuperado de https://books.google.es/books?hl=es&lr=&id=_z2GcBD3deYC&oi=fnd&pg=IA1&dq=modelo+OSI+en+redes+industriales&ots=wsniyGA_Qg&sig=wpmhG-yXISXZYry2HhEQp15M5KM#v=onepage&q=OSI&f=false

COMISIÓN DE REGULACIÓN DE COMUNICACIONES. Indicadores de la economía digital en Colombia: Empresas con protocolos para incidentes digitales. 2016, Colombia. Recuperado de https://www.postdata.gov.co/landing/index

GARCÉS, Juan Carlos. Citado por PORTAFOLIO. Las compañías le apuestan a la tecnología de punta. En: Portafolio [online]. Febrero, 2018, párr. 3. Recuperado de https://www.portafolio.co/economia/las-companias-le-apuestan-a-la-tecnologia-de-punta-513970

GARTNER. Operational Technology (OT) Traducido y citado por HACHI. La tecnología operacional: Otro reto para PRTG. En: Hachi [página web], 2016. Recuperado de http://hachi.co/newsletter-prtg/

GIMÉNEZ ALBACETE, José Francisco. MF0486_3: Seguridad en Equipos Informáticos [online]. 1 ed. Málaga: IC Editorial, 2014, 312 p. ISBN: 978-84-16433-23-0. Recuperado de https://books.google.es/books?id=8a3KCQAAQBAJ&hl=es&source=gbs_navlinks_s

INSTITUTO NACIONAL DE CIBERSEGURIDAD - INCIBE. España. 22, octubre, 2015. [blog institucional]. Recuperado de https://www.incibe-cert.es/blog/ciberseguridad-industria-4-0

INSTITUTO NACIONAL DE ESTÁNDARES Y TECNOLOGÍA. Marco para la mejora de la seguridad cibernética en infraestructuras críticas. NIST Estados Unidos: Abril, 2018, 55 p. Recuperado de

https://www.nist.gov/sites/default/files/documents/2018/12/10/frameworkesmellrev_20181102mn_clean.pdf

INTECO citado en BAQUERO SALAMANCA, Germán Darío. Seguridad de la información en sistemas SCADA [online]. Universidad Piloto de Colombia. Recuperado de http://polux.unipiloto.edu.co:8080/00001512.pdf

MIER, Camilo, citado por PORTAFOLIO. Colombia se perfila a una infraestructura tecnológica de punta. En: Portafolio [online]. Octubre, 2018. Recuperado de https://www.portafolio.co/negocios/colombia-se-perfila-a-una-infraestructura-tecnologica-de-punta-522093

MINTIC. Elaboración de la política general de seguridad y privacidad de la información. Colombia, 2016. 25 p. Recuperado de https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

MINTIC. Seguridad TI: Modelo de seguridad. Fortalecimiento de la gestión TI en el estado. 2018. 7 párr. Recuperado de https://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

NERC. Critical Infrastructure Protection Committee (CIPC). En: NERC [página web], 2017 Recuperado de https://www.nerc.com/comm/CIPC/Pages/default.aspx

OASYS, Redacción. Integración OT e IT para una Industria 4.0 En: Oasys Barcelona [blog] 2015. Recuperado de https://oasys-sw.com/integracion-ot-e-it-para-una-industria-4-0/

ORGANIZATION OF AMERICAN STATES y MICROSOFT. Protección de la infraestructura crítica en américa latina y el caribe. [documento virtual] 2018. Recuperado de https://info.microsoft.com/LA-AzureMig-CNTNT-FY19-10Oct-24-Protecciondelainfraestructura-MGC0003227_01Registration-ForminBody.html

QUIROZ-ZAMBRANO, Silvia M. y MACÍAS-VALENCIA, David G. Seguridad en informática: consideraciones En: Dominio de las Ciencias [online]. Julio, 2017. vol. 3, no. 5, p 676 – 688. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=6137824

RÍOS HUÉRCANO, Sergio. Manual de ITIL V3 Integro, Sevilla, Biable Management: Excellence and Innovation, 2015. 101 p. Recuperado de https://docs.supersalud.gov.co/PortalWeb/planeacion/AdministracionSIG/GSDE01.pdf

RODRÍGUEZ, Juanita. Citada por DINERO. Analítica de datos, una de las tecnologías con más futuro en el 2018 en Colombia. En: Dinero [online]. Enero, 2018. Recuperado de https://www.dinero.com/emprendimiento/articulo/tendencias-de-tecnologia-mas-importantes-

en-colombia/254681

SALAZAR, Jordi y SILVESTRE, Santiago. Internet de las cosas. En: České vysoké učení technické v Praze Fakulta elektrotechnická [online]. 2016, 24 p. Recuperado de https://core.ac.uk/download/pdf/81581111.pdf

SILVA G, Francisco. StuxNet – El software como herramienta de control geopolítico. En: Revista PUCE [online], 2018. No. 106, p. 297 – 314. Recuperado de http://www.revistapuce.edu.ec/index.php/revpuce/article/view/141/243

STOUFFER, Keith et al. Guide to Industrial Control Systems (ICS) Security. En: NIST, revisión 2, mayo, 2015, 7 p. Recuperado de http://dx.doi.org/10.6028/NIST.SP.800-82r2

Fuente: VAL ROMÁN, José Luis. Industria 4.0: la transformación digital de la industria. En: Coddiinforme, 2016, p. 3. Recuperado de http://coddii.org/wp-content/uploads/2016/10/Informe-CODDII-Industria-4.0.pdf

VITRIKO, SmartSolutions for IoT. Ataques a la industria 4.0, 2016, 12 párr. Recuperado de https://vitriko.eu/ataques-la-industria-4-0/

AGUTTER, Claire. ITIL Lifecycle Essentials: Your Essential Guide for the ITIL Foundation Exam and Beyond. IT Governance Publishing. Reino Unido: IT Governance Publishing, 2013. 375 p. ISBN 978-1-84928-418-9. Recuperado de http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=571562&lang=es&site=eds-live&scope=siteBAENA PAZ, Guillermina María Eugenia. Metodología de la investigación. 3 ed. México: Grupo Editorial Patria, 2014. 157 p. ISBN 9786077447528 Recuperado de https://bibliotecavirtual.unad.edu.co:2538/lib/unadsp/detail.action?docID=3228423

BORDA PÉREZ, Mariela. El proceso de investigación: visión general de su desarrollo. Barranquilla, Colombia: Universidad del Norte, 2013. 79 p. ISBN 978-958-741-913-9 Recuperado de http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=710213&lang=es&site=eds-live&ebv=EB&ppid=pp_79

BORONAT SEGUÍ, Fernando, y MONTAGUD CLIMENT, Mario. El nivel de red en el modelo de interconexión de redes basado en capas. España: Editorial de la Universidad Politécnica de Valencia, 2012, 113 p. ISBN 978-84-8363-881-1. Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=6&docID=10638261&tm=1449612703200

BORONAT SEGUÍ, Fernando, y MONTAGUD CLIMENT, Mario. Direccionamiento e interconexión de redes basada en TCP/IP: IPv4/IPv6, DHCP, NAT, Encaminamiento RIP y

OSPF. España: Editorial de la Universidad Politécnica de Valencia, 2013, 175 p. ISBN 978-84-9048-061-8. Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=10820977&p00=ipv6

BURNETT, Mark y KLEIMAN, David. Perfect Passwords: Selection, Protection, Authentication. Rockland: Syngress Publishing, 2006, 181 p. ISBN 1-58749-041-5. Recuperado de http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=149590&lang=es&site=ehost-live

CANO MARTÍNEZ, Jeimy José. El peritaje informático y la evidencia digital en Colombia: conceptos, retos y propuestas. Colombia: Universidad de los Andes, 2010, 374 p. ISBN 9789586955713. Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=10592650&p00=Firma+digital

CHEMA, Alonso. Captura de claves en PLCs industriales CP1L-EM de Omron. En: Un Informático en el lado del mal [blog personal]. 29, octubre, 2013. Recuperado de http://www.elladodelmal.com/2013/10/captura-de-claves-en-plcs-industriales.html

CHICANO TEJANO, Ester. Auditoría de seguridad informática (MF0487_3). Madrid: IC Editorial, 2014, 314 p. ISBN 9788416433230. Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=11126290&p00=seguridad+en+sistemas+operativos

CHICANO TEJANO, Ester. Gestión de incidentes de seguridad informática (MF0488_3). Madrid: IC Editorial, 2014, 317 p. ISBN 9788416351701. Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=11126339&p00=seguridad+en+sistemas+operativos

COLOBRAN HUGUET, Miquel; ARQUÉS SOLDEVILLA, Josep María y MARCO GALINDO, Eduard. Administración de sistemas operativos en red. Barcelona: Editorial UOC, 2008, 309 p. ISBN 9788490294871. Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=10638510&p00=seguridad+en+sistemas+operativos

COLOMBIA, UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD. Acuerdo 0029 Reglamento Estudiantil (13 de diciembre de 2013). Por el cual se expide el Reglamento Estudiantil de la Universidad Nacional Abierta y a Distancia. Bogotá, DC, Colombia, 2013, 48 p. Recuperado de https://sgeneral.unad.edu.co/consejo-superior/acuerdos/2013/472-acuerdo-029-13-de-diciembre-de-2013

COSTAS SANTOS, Jesús. Seguridad informática. España: RA-MA Editorial, 2014, 301 p. ISBN 9788499643137. Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=11038505&p00=seguridad+basica+en+redes+de+datos

COSTAS SANTOS, Jesús. Seguridad y alta disponibilidad. Madrid: RA-MA Editorial, 2014, 227 p. ISBN 9788499643458. Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=11046042&p00=seguridad+en+sistemas+operativos

DÍAZ ORUETA, Gabriel; ALZÓRRIZ ARMENDÁRIZ, Ignacio y SANCRISTÓBAL RUIZ, Elio. Procesos y herramientas para la seguridad de redes. Madrid: UNED - Universidad Nacional de Educación a Distancia, 2014, 568 p. ISBN 9788436268386. Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=10862475&p00=seguridad+redes

ELDER, Laurent; GALPERIN, Hernan; GILLWALD, Alison y SAMARAJIVA, Rohan. Los Pobres En la era de la información: Combatiendo La Pobreza Con Tecnología. Canadá: En Foco, 2013, 111 p. ISBN 1552505766. Recuperado de https://idl-bnc-idrc.dspacedirect.org/bitstream/handle/10625/52415/IDL-52415.pdf?sequence=1&isAllowed=y

ESCRIVÁ GASCÓ, Gema; ROMERO SERRANO, Rosa María y RAMADA, David Jorge. Seguridad informática. Madrid: Macmillan Iberia, S.A, 2013, 218 p. ISBN 9788415991410. Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=10820963&p00=seguridad+informatica

ESTEVE, Jaume. 'Hackear' la red ferroviaria es posible: así se paraliza todo un país. En: El Confidencial, Diario Digital Español. 30, diciembre, 2015. Recuperado de https://www.elconfidencial.com/tecnologia/2015-12-30/asi-se-puede-poner-en-jaque-a-la-red-ferroviaria_1128591/

FERNÁNDEZ MARTÍN, Marcos; OLMEDA ARROYO, Roberto y LARREA JASPE, Marta. Por qué debe plantearse la convergencia entre sistemas OT e IT. En: Red Computerword [artículo de página web], 2016. Recuperado de https://red.computerworld.es/actualidad/por-que-debe-plantearse-la-convergencia-entre-sistemas-ot-e-it

FERNÁNDEZ, Marcos *et al.* Convergencia entre IT y OT: Resultados del estudio sobre el estado de la Tecnología de Operaciones y su convergencia con las Tecnologías de la Información. Madrid: Altran Innovación S.L, 2017, 56 p. Recuperado de http://blog.altran.es/wp-content/uploads/2017/07/ALTRAN_Estado-OT_03_02.pdf

FERNÁNDEZ SÁNCHEZ, Carlos Manuel y PIATTINI VELTHUIS, Mario. Modelo para el gobierno de las TIC basado en las normas ISO. España: AENOR - Asociación Española de Normalización y Certificación, 2009, 435 p. ISBN 9788481437645. Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=1&docID=10637138&tm=1456691942576

FERREYRO, Adriana y LONGHI, Ana Lía De. Metodología de la investigación. Argentina: Encuentro Grupo Editor, 2014, 128 p. ISBN 978-987-192-532-2 Recuperado de:http://bibliotecavirtual.unad.edu.co:2051/login.aspx?direct=true&db=nlebk&AN=847673&lang=es&site=eds-live

FLORES RUIZ, Eric, MIRANDA NOVALES, María Guadalupe, y VILLASÍS KEEVER, Miguel Ángel. El protocolo de investigación VI: cómo elegir la prueba estadística adecuada. Estadística inferencial. En: Revista Alergia De México: 2017, vol. 64, no. 3, 364-370. Recuperado de: http://bibliotecavirtual.unad.edu.co:2051/login.aspx?direct=true&db=a9h&AN=125899428&lang=es&site=eds-live

GARCÍA PÉREZ, Alfonso. La interpretación de los datos: una introducción a la estadística aplicada. Madrid: UNED - Universidad Nacional de Educación a Distancia 2015, 142 p. ISBN 9788436269475. Recuperado de http://eds.a.ebscohost.com.bibliotecavirtual.unad.edu.co/eds/detail/detail?vid=3&sid=61d16736-1ff2-4865-ac3d-cf02ce678276%40sdc-v-sessmgr01&bdata=Jmxhbmc9ZXMmc2l0ZT1lZHMtbGl2ZSZzY29wZT1zaXRl#AN=edselb.3227747&db=edselb

GÓMEZ, Ricardo, *et al*. Metodología y gobierno de la gestión de riesgos de tecnologías de la información. En: Revista de Ingeniería, mayo, 2010. no. 31, p. 109 –118. Recuperado de http://eds.b.ebscohost.com.bibliotecavirtual.unad.edu.co/eds/detail/detail?vid=2&sid=eff95f3b-5d22-4b74-8946-636966184c5d%40sessionmgr102&bdata=Jmxhbmc9ZXMmc2l0ZT1lZHMtbGl2ZSZzY29wZT1zaXRl#AN=edsbas.2C3C8C11&db=edsbas

GÓMEZ LÓPEZ, Julio y GÓMEZ LÓPEZ, Oscar. David. Administración de sistemas operativos. Madrid: RA-MA Editorial, 2014, 325 p. ISBN 9788499643472 Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=11046063&p00=seguridad+sistemas+operativos

GÓMEZ VIETES, Álvaro. Auditoría de seguridad informática. España: RA-MA Editorial, 2014, 147 p. ISBN: 9788499643281 Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=11046196&p00=seguridad+basica+en+redes+de+datos

GÓMEZ VIETES, Álvaro. Gestión de incidentes de seguridad informática. España: RA-MA Editorial, 2014, 124 p. ISBN 9788499643311 Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=11046422&p00=amenazas+redes+de+datos

GÓMEZ VIETES, Álvaro. Seguridad en equipos informáticos. España: RA-MA Editorial, 2014, 165 p. ISBN 9788499643304. Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=13&docID=11046412&tm=1466006343174

GUERRERO, Manuel. Necesitamos el entendimiento IT & OT. En: Kaizen, Mejora Continua [blog empresarial], 2018. Recuperado de https://manuelguerrerocano.com/it_ot_convergencia/

LERMA GONZÁLEZ, Héctor Daniel. Metodología de la investigación: propuesta, anteproyecto y proyecto, 4 ed. Bogotá: Ecoe ediciones, 2009, 190 p. ISBN: 978-958-648-602-6. Recuperado de http://bibliotecavirtual.unad.edu.co:2051/login.aspx?direct=true&db=nlebk&AN=483354&lang=es&site=eds-live

LONG, Johnny. Google Hacking for Penetration Testers, Vol. 2 [e-book]. Burlington: Syngress, 2008, 540 p. Recuperado de de http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=230833&lang=es&site=ehost-live

LONG, Johnny. Penetration Tester's Open Source Toolkit. Rockland, MA: Syngress, 2006, 706 p. Recuperado de http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=149572&lang=es&site=ehost-live

LÓPEZ, MATACHANA, Yansenis. Los virus informáticos: una amenaza para la sociedad. Cuba: Editorial Universitaria, 2009, 33 p. ISBN 9789591611369. Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=4&docID=10357400&tm=1466006227313

MCCLURE, Stuart; SCAMBRAY, Joel y KURTZ, George. Hackers 6: secretos y soluciones de seguridad en redes. México, D.F: McGraw-Hill Interamericana, 2006, 717 p. ISBN 9786071502216. Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=10433876&p00=seguridad+redes

OLIVA, Nuria *et al.* Redes de comunicaciones industriales. Madrid: UNED - Universidad

Nacional de Educación a Distancia, 2013, 485 p. ISBN 9788436265491. Recuperado de http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edselb&AN=edselb.3216642&lang=es&site=eds-live

PAREDES FLORES, Carlos Iván. Hacking. Argentina: El Cid Editor | apuntes, 2009, 29 p. Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=1&docID=10316240&tm=1466006313060

RAYA CABRERA, José Luis y RAYA GONZÁLES, Laura. Implantación de sistemas operativos. Madrid, ES: RAMA Editorial, 2014, 588 p. ISBN 9788499643144 Recuperado dehttp://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=11038541&p 00=seguridad+en+sistemas+operativos

REYES KRAFFT, Alfredo Alejandro. Las firmas electrónicas y las entidades de certificación. México: D - Universidad Panamericana, 2009, 322 p. ISBN: 9788468862613 Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=167&docID=10287252&tm=1449622074063

ROA BUENDÍA, José Fabián. Seguridad informática. España: McGraw-Hill España, 2013, 226 p. ISBN: 9788448185695 Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=10692460&p00=firewall

ROJAS CÓRSICO, Ivana Soledad. Trabajo de auditoría normas COBIT. Argentina: El Cid Editor | apuntes, 2009, 36 p. Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=1&docID=10317247&tm=1456692028784

ROSS, Jeanne W. y WEILL, Peter. Seis decisiones de TI que no debe dejar en manos del departamento de TI. España: Ediciones Deusto - Planeta de Agostini Profesional y Formación S.L, 2004, 10 p. Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=1&docID=10063648&tm=1456691972039

ROUSE, Margaret. IT/OT Convergence. Essential Guide [blog]2016. Recuperado de https://searchitoperations.techtarget.com/definition/IT-OT-convergence

STEENSTRUP, Kristian. IT and Operational Technology Alignment Innovation Key Initiative Overview. En: Gartner [blog], 2011. Recuperado de https://www.gartner.com/doc/1746622/it-operational-technology-alignment-innovation

TREMOSA, Laura. Confluencia IT y OT, ¿desaparecerán los sistemas MES? En InfoPLC: Estado del arte de la tecnología industrial [página web], 2017. Recuperado de http://www.infoplc.net/plus-plus/mercado/tribuna/item/104142-confluencia-it-ot-desapareceran-sistemas-mes

UNIVERSIDAD DE OVIEDO. Comunicaciones Industriales. Docencia de Ingeniería Electrónica y Automática, 2006, 33 p. Recuperado de http://isa.uniovi.es/docencia/iea/teoria/comunicacionesindustrialesdocumento.pdf