FUNDACIÓN UNIVERSITARIA LOS LIBERTADORES

Luis Carlos López Prieto
Diego Alejandro Moreno
Diego Armando Moreno Chingaté
Yenny Isabel Serrato Rodríguez

ADOPCIÓN DE BUENAS PRÁCTICAS EN SEGURIDAD DE LA INFORMACIÓN ENFOCADO EN AMBIENTES OT

Resumen

Las ventajas del uso de la tecnología, la digitalización y la conectividad actualmente en la industria operacional OT son bastante significativas, pero al mismo tiempo aumenta la posibilidad de sufrir un ataque cibernético debido a la mayor exposición de la superficie de intrusión.

Sumado a esto, en la actualidad industrias de todo tipo (eléctrica, gas, manufactura, salud, etc.) son objetivo de los ciberdelincuentes debido al gran impacto que pueden causar en la empresa y/o sociedad la materialización de un riesgo, cuyo resultado tendría consecuencias tales como: económicas, reputacionales, ambientales, a la integridad de las personas, etc.).

De otra parte, la convergencia entre el mundo IT con OT, asociado al creciente uso de la computación y automatización para los entornos industriales, hace necesario blindar estas tecnologías apoyado en la aplicación de normas, controles, estándares y políticas de seguridad de la información con el fin de identificar las mejores prácticas en dichos ambientes.

De acuerdo con esto, es imprescindible analizar e identificar las brechas de seguridad de la información a las

cuales se ven expuestos los ambientes operacionales (OT) que no poseen los controles mínimos y/o adecuados en seguridad de la información, para las industrias que principalmente usan sistemas de automatización para la ejecución de sus procesos productivos.

Palabras clave: SCI (sistemas de control industrial), OT (Tecnología Operacional), Seguridad de la Información, IT (Tecnología de la Información) Riesgo, Amenaza, Convergencia.

Abstract

The advantages of the use of technology, digitization and connectivity currently in the OT operational industry are quite significant, but at the same time the possibility of suffering a cyber attack increases due to the greater exposure of the intrusion surface.

In addition to this, currently industries of all kinds (electricity, gas, manufacturing, health, etc.) are targets of cybercriminals due to the great impact that the materialization of a risk can have on the company and/or society, the result of which is would have consequences such as: economic, reputational, environmental, to the integrity of people, etc.).

On the other hand, the convergence between the IT world with the OT, associated with the growing use of computing and automation for industrial environments, makes it necessary to shield these technologies supported by the application of norms, controls, standards and information security policies with in order to identify the best practices in these environments.

Accordingly, it is essential to analyze and identify information security gaps to which operational environments (OT) that do not have the minimum and/or adequate information security controls are exposed, for industries that mainly they use automation systems for the execution of their production processes.

Keywords: SCI (industrial control systems), OT (Operational Technology), Information Security, IT (Information Technology) Risk, Threat, Convergence.

1. INTRODUCCIÓN

Los sistemas de control industrial (SCI), son dispositivos que permiten a las organizaciones de diferentes sectores la automatización de sus procesos operaciones y/o productivos, los SCI facilitan la interacción física con la infraestructura de sus plantas de producción y el alineamiento con los sistemas IT, por ende, este conjunto de tecnologías se convierte en un sistema crítico.

Como referente actual, se tiene la búsqueda constante de las diferentes organizaciones a nivel mundial en generar transformaciones tecnológicas de sus procesos productivos, lo cual ha acelerado y pone al descubierto la urgente necesidad de tener una comunicación segura en los procesos industriales. Ante este escenario, las redes industrializadas no son la excepción y con la llegada de la cuarta revolución industrial (4.0), que se vive actualmente, se busca que los entornos IT y OT operacionales sean más convergentes y seguros.

Dicho esto, el desarrollo del artículo busca asentar la base para la adopción de buenas prácticas en seguridad de la información, teniendo en cuenta aspectos claves como: el acelerado desarrollo de la industria en la automatización de sus procesos, la importancia de la seguridad de la información en los SCI, la identificación de las amenazas, vulnerabilidades y riesgos asociados, la definición de los principales controles de seguridad a partir del análisis de la normatividad vigente y artículos especializados en la materia.

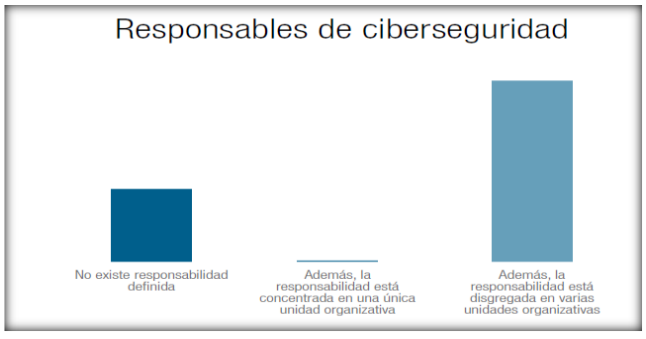
Sumado a esto, se ejecuta un estudio de campo en donde se visibiliza esta problemática en un entorno operacional productivo; el cual fue debidamente analizado y con base en esto se desprenden una serie de sugerencias y/o recomendaciones que puedan ser adoptadas por la organización sujeta del estudio para la mitigación de los posibles riesgos asociados a la operación.

2. PLANTEAMIENTO DEL PROBLEMA

Los diferentes sectores de la industria han venido experimentando un acelerado ritmo de crecimiento en la búsqueda de automatización de sus procesos industriales. A su vez, se evidencia el descuido en la adopción de buenas prácticas de seguridad de la información en ambientes OT, que aseguren una protección adecuada de los activos físicos y los activos de información.

Según el estudio sobre la ciberseguridad industrial en Colombia Centro de "Ciber Seguridad Industrial". Según Asensio Susana, Menéndez Miguel G., Valiente José, Zuluaga Diego (2018). En las diferentes empresas no han definido el área dentro de la organización que debe realizar temas propios de seguridad en infraestructuras operacionales, ni un modelo de ciberseguridad orientado a operaciones físicas; sobre el 55% de las empresas, dicha tarea es asignada al área de seguridad de la información y en pequeñas empresas, esta revisión la toman áreas como: HSE (Riesgo Laboral y Medioambiental). Escenarios que pueden ser resultado, del estado de madurez de la empresa o al desconocimiento de que pueden ser objeto de ataques de infraestructura.

Ilustración 1. *Responsable de la Ciberseguridad*



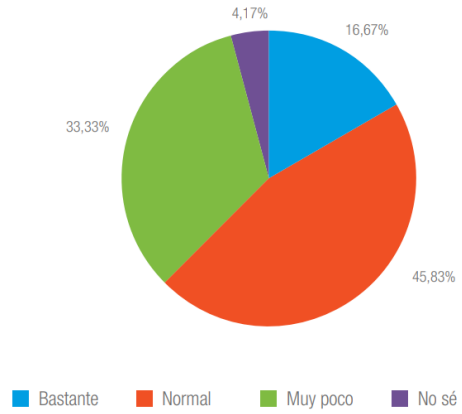
Nota. En el estudio realizado se muestra que un alto porcentaje de las empresas encuestadas asigna la responsabilidad al área de la Seguridad de la Información, enfocado a un nivel más cibernético

asociado a procesos. Fuente: Estudio sobre la Ciberseguridad Industrial en Colombia Edición, 2018.

En concordancia, con lo anterior los responsables del negocio no son conscientes de las regulaciones y menos, de los riesgos a los que se exponen las infraestructuras operacionales.

Las empresas en sus diferentes jerarquías tanto administrativas como operacionales deben tener una relación la cual permita una validación, gestión, adquisición y control de redes en los diferentes sistemas de organización. Por esto es importante el grado de sensibilización en los responsables del negocio, permitiendo así comprender los riesgos y la complejidad de las diferentes actividades diarias que permiten la actividad continúa.

Ilustración 2. *Nivel de Sensibilización de los responsables del negocio*



Nota. En el estudio realizado se muestra que la mitad de las personas con un porcentaje del 45.83% tienen un grado de sensibilización normal frente a riesgos y normas en las redes industriales, mientras que un porcentaje del 33.33% dicen estar poco muy poco sensibilizados siendo un grupo objetivo, en el cual se debe trabajar y profundizar en los temas para así tomar conciencia del peligro

en el cual está expuesta la organización. Fuente: Estudio sobre la Ciberseguridad Industrial en Colombia Edición, 2018.

Las cifras anteriormente expuestas podrían mejorar si existiera una adopción de buenas prácticas de seguridad y se asignará un área responsable de la adopción de la normatividad enfocada a la seguridad en sistemas de control industrial en convergencia a la seguridad IT, ya que, en la mayoría de las empresas, dicha orientación está dada a la seguridad de la información IT.

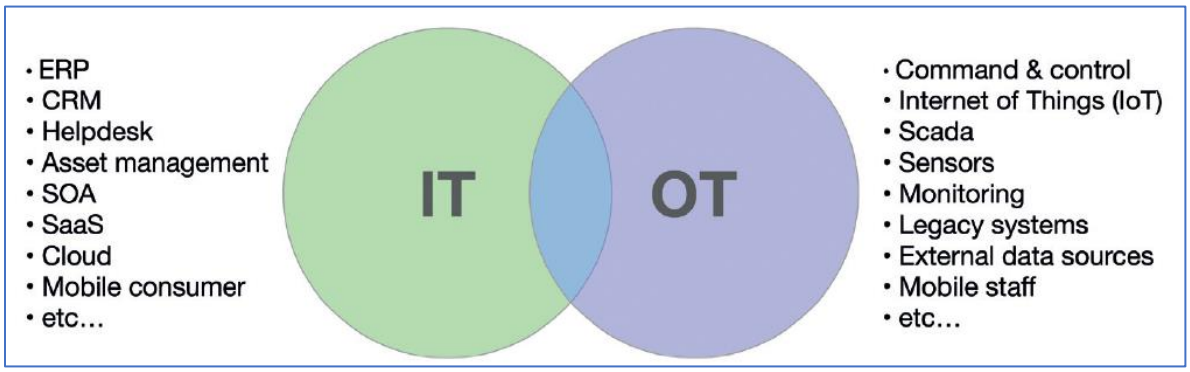
Por otra parte, según el estudio el proceso de gestión de incidencias de seguridad indica que el 18% de las empresas cuenta con un proceso de gestión de incidencias, en el 6.9% no existe el proceso y el 17.2% de las empresas actúa de forma reactiva cuando ocurren eventos de seguridad, el 28% indica que el proceso se encuentra en estado de definición, ya que, evidenciaron la necesidad de implementar seguridad OT, debido a el Ransomware WannaCry del 2017.

Así mismo, sobre un estudio encargado de Fortinet a la consultora Forrester Consulting, a nivel internacional advierte también que la tradicional separación de las funciones y departamentos de IT y OT, en el sector industrial, supone un problema a la hora de implementar las medidas de seguridad necesarias, ya que no está claro a qué área le corresponde la tarea. Según esta nueva investigación, el 51% de los encuestados declararon operar en sitio, lo que significa que el equipo de OT gestiona los equipos industriales críticos y la ciberseguridad de OT, mientras que el equipo de TI es responsable de la gestión de la ciberseguridad de las TI; por lo tanto, se observa la necesidad de una convergencia de IT y OT con el fin de garantizar una seguridad a nivel industrial y en consecuencia mayor competitividad según: La falta de coordinación de los equipos de Ciberseguridad. (14 de enero de 2020).

3. ANÁLISIS DE LAS BUENAS PRACTICAS EN SEGURIDAD DE LA INFORMACIÓN

Con la llegada de las aplicaciones industriales a la infraestructura de los sistemas de información se encontró la necesidad de establecer una sinergia, donde se adopten buenas prácticas y una convergencia de seguridad IT y OT, agrupando varias tareas asociadas a cada área.

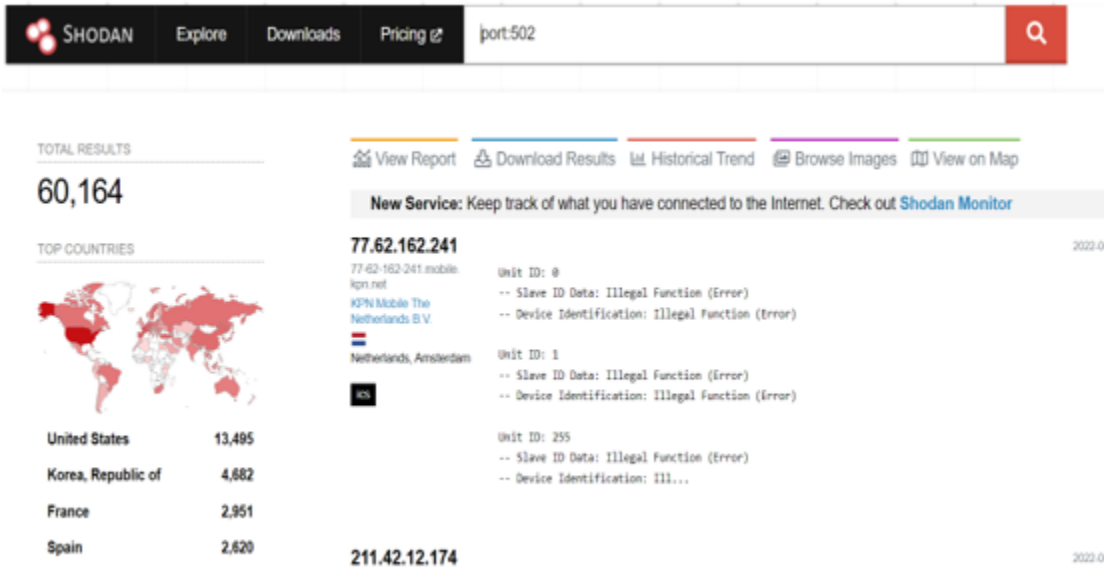
Ilustración 3. *Convergencia entre IT y OT*



Fuente: Convergencia IT / OT: Un reto clave para la Industria 4.0, 2022.

Por otro lado, los sistemas de control industrial utilizaban protocolos específicos como: Modbus o Profibus que eran utilizados inicialmente por expertos, sin embargo, con la evolución tecnológica estos sistemas han evolucionado y en la actualidad, se encuentran utilizando protocolos Ethernet o TCP/IP los cuales son ampliamente conocidos por áreas de IT, en consecuencia, aumentan los riesgos y vulnerabilidades asociadas; así las cosas, tan solo con realizar una búsqueda sobre el portal SHODAN al puerto 502, que es el puerto utilizado por uno de los protocolos industriales mencionados , proporcionó 60164 resultados, lo que quiere decir, que existe una alta probabilidad, que estos dispositivos puedan ser accesibles desde internet ya que no cuentan con ningún tipo de protección y a la fecha estos dispositivos puedan ser accesibles desde internet sin tener ningún tipo de protección.

Ilustración 4. *Exposición de Internet Inseguro - Portal Shodan*



Fuente: Exposición de Internet Inseguro**,** SHODAN- Puerto 502, 2022.

Dado el resultado que muestra el puerto 502, es de suma importancia tener una mayor sensibilización hacia la ciberseguridad en operaciones industriales OT, con el fin, de seguir pautas que reduzcan la superficie de exposición a un ataque en entornos industriales y disminuir las vulnerabilidades, por lo tanto, disminuir el riesgo en dichos sistemas OT.

Así las cosas, se determina que se tiene un desconocimiento de los ataques a los que se puede ver expuesta una infraestructura OT, es el momento oportuno, de revisar el concepto tradicional de seguridad que se tiene actualmente, ya que a mayor conectividad aumentan a un ritmo directamente proporcional, las amenazas como ejemplo: el caso Stuxnet Irán.

3.1 Antecedentes - Caso Stuxnet

El gusano Stuxnet fue descubierto en una computadora iraní en 2010. Este malware sorprendió a los expertos informáticos debido a su sofisticación y al uso de cuatro exploits de día

cero. Más tarde, se descubrió que el malware no estaba diseñado para espiar, sino para sabotear centrífugas en las instalaciones eléctricas de Natanz en Irán. Se cree que EE. UU. Construyó Stuxnet con el apoyo de Israel con el objetivo de detener o retrasar el programa nuclear iraní. El gusano probablemente se implantó en la red de la central eléctrica de Natanz mediante el uso de una unidad USB comprometida. Esta técnica permitió que el gusano penetrará en una red que normalmente está aislada de otras redes.

Stuxnet es el nombre de un gusano específico, es decir, una pieza de malware informático que se dirige a los sistemas de control de supervisión y adquisición de datos (SCADA) en los controladores industriales. Es difícil, si no imposible, saber exactamente cómo se desarrolló el malware, pero no cabe duda de que su desarrollo requirió recursos considerables en mano de obra, tiempo y finanzas. Los especialistas que evalúan el desarrollo del gusano estiman que debe haber requerido un equipo de cinco a diez programadores trabajando a tiempo completo durante al menos seis meses.

Stuxnet lanzó su ataque cambiando la velocidad de los rotores de centrífugas, causando daños irreparables. Una centrífuga es un cilindro con una rotación rotor en el que se alimenta uranio en forma de gas isotópico. El objetivo es utilizar la fuerza centrífuga para separar el gas más pesado del más ligero. El primero se empobrece y el segundo se enriquece con uranio (Institute for Science and International Security, nd).

Adicional al daño de las centrífugas a nivel operacional, afectó directamente al sector tecnológico. Las empresas que habían desarrollado software con vulnerabilidades que fueron explotadas para infectar y controlar las computadoras en Irán se vieron obligadas a reaccionar para contener el malware. Microsoft emitió parches para resolver los exploits de día cero relevantes y

Siemens ofreció parches y herramientas de eliminación a los clientes para eliminar Stuxnet en los meses posteriores al descubrimiento del malware. (Langner, 2011, p. 50; Lindsay, 2013, p. 391).

Los daños causados por Stuxnet a las centrífugas iraníes demostraron que las infraestructuras críticas pueden ser objeto de ciberamenazas. El hecho de que las redes operativas estuvieran separadas de otras redes no las protegía suficientemente contra el malware. Como consecuencia, los Estados deben tener en cuenta que las infraestructuras críticas requieren integrarse en las estrategias de ciberseguridad. Las consideraciones pertinentes darían como resultado una mayor protección contra las amenazas cibernéticas y estándares de ciberseguridad más altos y, al mismo tiempo, promoverían una cooperación más estrecha entre los gobiernos y los actores, ya sean públicos o privados, que administran estas infraestructuras. El objetivo sería aumentar la protección contra las amenazas cibernéticas, al tiempo que aumenta la resiliencia, en caso de ataques cibernéticos.

3.2 Contexto Actual

Actualmente en un mundo conectado y orientado a la globalización, diferentes organizaciones se encuentran en un proceso de transformación tecnológica de sus procesos productivos. Evidentemente, con la llegada de la pandemia 2020 y la necesidad de continuar, se acelerado aún más el ritmo del cambio y la velocidad de la transformación obligando a los rezagados a apresurar el paso para igualar a los líderes digitales y productivos. Con la eminente llegada a la cuarta Revolución Industrial, también conocida como industria 4.0, se está cambiando la forma en que los negocios operan y por lo tanto los entornos digitales y productivos se ven obligados a competir generando nuevos objetivos y retos a nivel de seguridad en tecnologías de la información como en sistemas de control industrial.

"La Industria 4.0 implica la promesa de una nueva revolución que combina técnicas avanzadas de producción y operaciones con tecnologías inteligentes que se integrarán en las organizaciones, las personas y los activos". (Mark Cotteleer, Brenna Sniderman (2017). Las organizaciones deben identificar las tecnologías que mejor satisfagan sus necesidades, para invertir en ellas. Para los líderes tradicionales acostumbrados a los datos y las comunicaciones lineales, el cambio que supone esta nueva revolución industrial, proporcionará acceso en tiempo real a los datos. La inteligencia del negocio transformará la forma en que llevan a cabo los negocios, el acceso en tiempo real a la información estará impulsado por el continuo y cíclico flujo de información y acciones entre los entornos físicos y digitales por la automatización y la alta digitalización de los procesos industriales, sin embargo, este nuevo modelo hace más eficiente la industria, pero, amplía exponencialmente los riesgos en materia de ciberseguridad y este será el reto más grande que conlleva la transformación digital y productiva de la industria 4.0.

3.3 Funcionamiento SCI

El funcionamiento básico de un sistema de control industrial reúne los siguientes componentes:

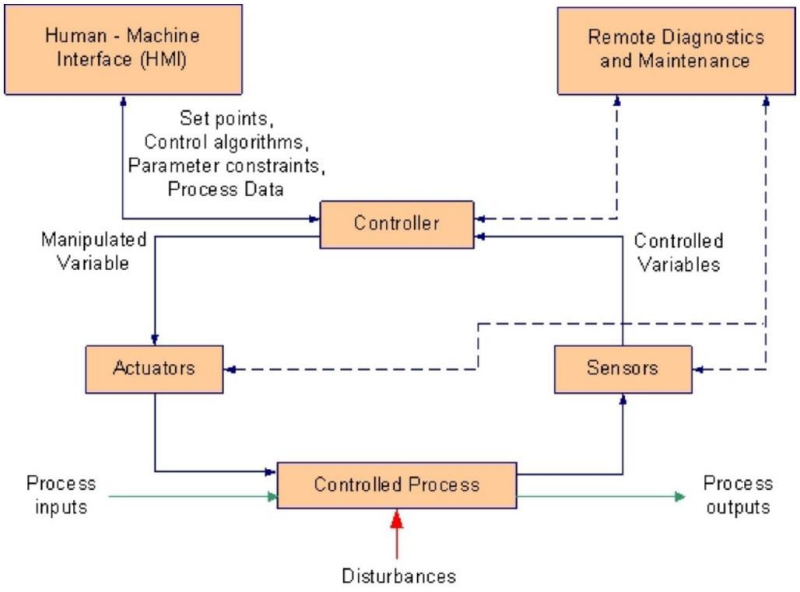
- **Bucle de control**: Es un proceso de control que consta de sensores para medición, es decir, elementos de hardware y controladores PLCS.

- **PLC:** Controlador Lógico Programable es una pequeña computadora industrial diseñada originalmente, para realizar las funciones lógicas ejecutadas por el hardware eléctrico (relés, interruptores y temporizadores/contadores mecánicos).

- **Interfaz Hombre-Máquina (HMI).** Los operadores e ingenieros usan HMI para monitorear y configurar puntos de referencia, controlar algoritmos, ajustar y establecer parámetros en el

controlador. La HMI también muestra información sobre el estado del proceso e información histórica.

Ilustración 5. *ICS Operation*



Fuente: Guide to Industrial Control Systems (ICS) Security, 2015.

- **Servidor de control.** El servidor de control, aloja el software de control de supervisión DCS o PLC que se comunica con los dispositivos de control de nivel inferior. El servidor de control accede a los módulos de control subordinados a través de una red ICS.
- **Servidor SCADA o Unidad Terminal Maestra (MTU).** Es el dispositivo que actúa como maestro en un sistema SCADA.
- **Unidad Terminal Remota (RTU).** La RTU, también llamada unidad de telemetría remota, es una unidad de control y adquisición de datos de propósito especial diseñada para admitir estaciones remotas.

- **Historiador de datos.** El historial de datos es una base de datos centralizada para registrar toda la información del proceso dentro de un ICS.
- **Servidor de entrada/salida (IO).** El servidor IO es un componente de control responsable de recopilar, almacenar en búfer y brindar acceso a la información del proceso desde los subcomponentes de control, como PLC, RTU.
- **Adopción de seguridad de la información**

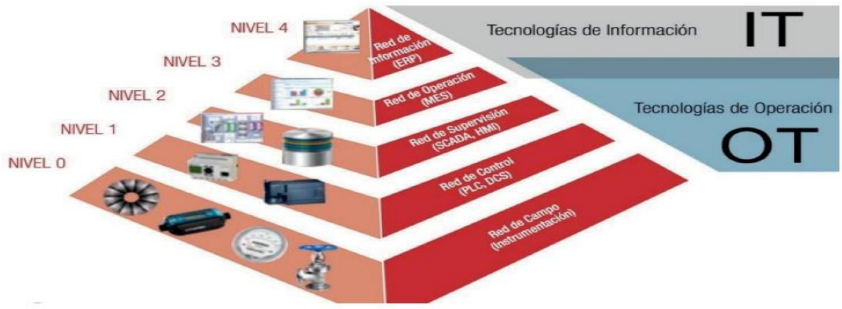
Buscando la convergencia de IT y OT, es necesario identificar las tres etapas productivas de un sistema de control industrial, las cuales son:

1. Medición de los datos en proceso (Monitorización),
2. Evaluación de la información obtenida en cuanto a parámetros estándar,
3. Control del proceso en base a la información medida y evaluada,

Estos sistemas de control pueden ser completamente manuales, automatizados en su totalidad, o de ambas formas (híbridos).

A continuación, se describen cuáles son los componentes habituales de una red OT:

Ilustración 6. *Pirámide de Automatización Industrial*



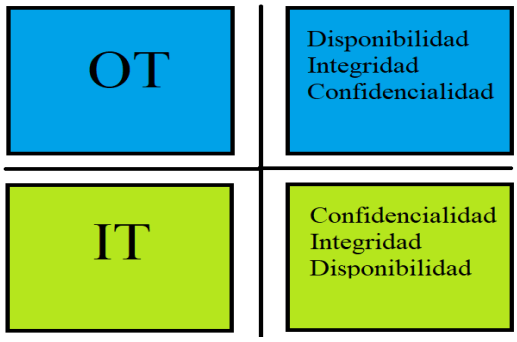
Fuente: Ciberseguridad en la Pirámide de Automatización Industrial, 2021.

Es clave identificar los puntos clave que corresponden a entornos IT y que pueden afectar al mismo tiempo entornos OT, por tal razón es necesaria una convergencia de IT y OT para generar buenas prácticas y mejorar los procesos en la seguridad de toda la industria.

3.4 Pilares de Seguridad de la Información

La seguridad de la información es la protección de los activos de información, contra una gran variedad de amenazas que existen en el mundo y debe cumplir los 3 pilares básicos que son: Confidencialidad, Integridad y Disponibilidad. Para los ambientes IT el pilar más importante es la confidencialidad, sin embargo, para los ambientes OT el pilar más importante hace referencia a la disponibilidad ya que en un medio de producción industrial una interrupción de servicio inesperada en los sistemas que controlan los procesos industriales no es aceptable. Las interrupciones a menudo deben planificarse y programarse con días/semanas de anticipación. Las pruebas previas a la implementación, son esenciales para garantizar un alto rendimiento en la operación y, en consecuencia, seguir una política de seguridad de la información.

Ilustración 7. *Pilares de la seguridad de la información en IT y OT*



Fuente: Convergencia de Seguridad en Sistemas de Tecnologías Operacionales y Tecnologías de la información. (2019).

3.5 Convergencia de Seguridad IT y OT

Como punto de partida en el análisis de la seguridad en los sistemas de control industrial es importante señalar la convergencia entre IT y OT en relación con los aspectos tecnológicos, la red IP de una empresa de producción se haya habitualmente segmentada en tres subredes de distintas características y diseño. La subred IT es una red corporativa de datos diseñada para entornos transaccionales. La subred OT está destinada para la supervisión de los procesos y la operación de la maquinaria de producción. Una tercera subred conocida como DMZ industrial o "zona industrial desmilitarizada" Convergencia de Seguridad en Sistemas de Tecnologías Operacionales y Tecnologías de la Información. (2019), intermedia entre la subred IT y la subred OT, evita el tráfico directo entre ambas, por motivos de seguridad y facilita el intercambio de información y el uso de aplicaciones comunes a las dos redes para llevar a cabo la gestión y administración integrada de la producción.

La subred OT, esta segmentada en 5 niveles según las funciones que se realizan, en planta (modelo Purdue):

- Red de campo (nivel 0): conecta los sensores, instrumentación y actuadores de la planta.
- Red de control (nivel 1): está formada por controladores lógicos programables (PLC) y sistemas de control distribuido (DCS).
- Red de supervisión (nivel 2): está formada por los sistemas SCADA (Supervisión, Control y Adquisición de Datos) y las interconexiones hombre-máquina.
- Red o sistema de operación de planta (nivel 3): se encarga de ejecutar las órdenes de trabajo e instrucciones al operador o de conocer el estado de los procesos.
- Red de información de planta (ERP) (nivel 4): está encaminada a la comunicación con el negocio sobre funciones de planificación, inventario, demanda y estado de la producción. Los

cuatro niveles inferiores dan servicio a las tecnologías de operación, a diferencia del nivel superior, orientado a tecnologías de la información.

3.6 Política de Seguridad de la Información

La Política de seguridad de la información es la declaración general de una serie de normas y medidas que permiten garantizar una gestión sólida en cuanto a la protección del entorno IT/OT y su enfoque orientado a:

- Minimizar los riesgos de los procesos productivos.
- Establecer roles y responsabilidades de seguridad que definan la separación de roles y responsabilidades para los sistemas de IT/OT.
- Visibilizar el ciber riesgo en los programas IT/OT.
- Crear un canal y una comunidad dedicada a la seguridad cibernética, incluida la seguridad de TI y OT.
- Aumentar la conciencia de OT entre el personal de TI y viceversa para comprender la seguridad convergente en consecuencia formar equipos de OT en ciberseguridad TI para que hablen el mismo idioma y por el contrario formar equipos de ciberseguridad TI en OT para que sean conscientes de los problemas que se están abordando.
- Apoyar la innovación tecnológica.
- Proteger los activos de información.
- Garantizar la disponibilidad del negocio como pilar fundamental ante cualquier tipo de incidente que se presente.

3.7 Gestión de Riesgos

En tiempos pasados se tenía conocimiento de que únicamente se presentaban incidentes de seguridad de información hacia infraestructuras IT, sin embargo, con el auge y la evolución de las tecnologías de operación OT, los ataques se han dado últimamente a equipos con sistemas de control industrial SCI, aquellos no cuentan con procedimientos, controles y personal idóneo para implementar una buena defensa ante los constantes ataques a los que se ven inmersas las infraestructuras OT, debido a ello se hace necesario que las organizaciones opten por generar políticas y procedimientos internos como: la gestión de riesgos a fin de mitigar las amenazas que día a día se ven incrementadas por el uso de estas tecnologías.

En entornos operacionales OT se debe tener muy presente la gestión de riesgos a fin identificar de manera proactiva las vulnerabilidades a que se ven expuestos y mitigar la probabilidad de que el riesgo sea materializado.

Seguido a esto se debe realizar un análisis e identificación de riesgos donde se evidencien controles y planes de acción en caso de ocurrencia de alguno de estos, para OT se deberían adoptar:

- **Identificación del riesgo:** Se debe realizar una identificación de cada uno de los riesgos asociados a las actividades operacionales OT que atentan contra la seguridad de la información.
- **Identificación de las causas:** Es importante distinguir todos los procesos, elementos, procedimientos y acciones que pueden generar que un riesgo se materialice junto con esta identificación, se debe realizar una descripción detallada y asignarle un valor a la posibilidad de ocurrencia a cada uno de que se materialice.
- **Consecuencias del riesgo:** Se deben detallar los posibles efectos adversos presentados por la materialización del riesgo tales como: la pérdida de la credibilidad hacia los clientes, pérdida

en producción, pérdida de la reputación y pérdida de negocios de acuerdo con las causas seleccionadas se pueden prever y prevenir las consecuencias que se presenten a futuro.

- **Identificación de controles:** En muchos de los procesos ya se evidencian algunos controles para la operación y son ejecutados sin ser identificados de manera oficial, sin embargo, estos controles mitigan las diferentes amenazas y vulnerabilidades que se tienen en los SCI, es importante describirlos y de ser necesario generar un procedimiento para cada uno.

En el caso de los factores de que no se tienen controlados, es necesario describir el riesgo sin control y crear un plan de tratamiento con las siguientes actividades: listar las actividades a ejecutar, los tiempos de su implementación, los responsables y el control que soportará la permitirá que este plan de acción sea aplicado con éxito.

Por último y no menos importante para las organizaciones es necesario valorar los riesgos y describir cuales de estos se asumirán por diversos factores tales como: económicos, de bajo impacto para la organización, etc. Creando un procedimiento donde quede formalizado para las partes involucradas todas las actividades que a su consideración y evaluación se puedan asumir y no representan un alto impacto, en caso de su materialización; así mismo, se debe realizar un seguimiento continuo con el fin de considerarlo un riesgo controlado.

Adicionalmente, se debe realizar una medición sobre el impacto que tiene un incidente de seguridad de la información en una infraestructura productiva y sus posibles efectos. La explotación de una vulnerabilidad conlleva a impactos de diversa índole tales como:

- **Impactos sobre la seguridad física y del entorno:** Estos impactos abarcan el conjunto de consecuencias directas de los fallos producidos en sistemas de control industrial. Dependiendo de la industria afectada este tipo de impactos pueden ser extremadamente

críticos, por la posible pérdida de vidas o lesiones personales. Otros efectos, incluyen la pérdida de datos y el daño potencial para el medio ambiente.

- **Impactos económicos:** Tras los impactos personales y de entorno, los económicos son los más importantes dentro de los posibles incidentes a los que se enfrenta un sistema de control industrial. Las pérdidas económicas pueden incidir de forma directa en el correcto funcionamiento de la empresa, debido a daños en dispositivos o infraestructuras que necesitan ser cambiadas; o bien, indirectamente, a causa de una parada en la cadena de producción y distribución del servicio.
- **Impactos sociales y mediáticos:** En orden de criticidad, las consecuencias de impacto social se sitúan en última posición, pero no por ello están carentes de importancia. "La consecuencia de la pérdida de confianza en una organización afecta directamente a su imagen social lo que se traduce en pérdida de clientes y las consiguientes pérdidas económicas, además de afectar su potencial crecimiento y competitividad". Según el Articulo Amenazas en los Sistemas de control Industrial, Blog Incibe Cert (2015).

Aunado a esto, se evidencian algunas consecuencias en caso de explotar una vulnerabilidad en infraestructuras OT, a continuación, se mencionan algunas de ellas:

- Reducción o pérdida de la producción en uno o varios sitios simultáneamente.
- Daño en los equipos.
- Lesiones de personas.
- Liberación, desvío o robo de materiales peligrosos (por ejemplo, vertidos tóxicos).
- Violación de los reglamentos.

- Pérdida de información confidencial o de propiedad intelectual.
- Pérdida de imagen o de la confianza.

3.8 Inventario de activos

En el proceso de diseño de un sistema de seguridad de la información para OT, es necesario contar con un inventario de equipos, para determinar aquellos hacen parte del sistema de producción y tienen el riesgo de ser manipulados de forma local o remota. En dicho inventario se debe recolectar la información básica como el serial, modelo, licencias, ubicación física, entre otros.

Otro aspecto fundamental es tener claro el licenciamiento de las aplicaciones, versiones vigentes, actualizaciones y parches de seguridad aplicados. Contar con un inventario, permite agilizar los procesos de renovación tecnológica, para facilitar la identificación de necesidades a corto y largo plazo, cubriendo renovación por obsolescencia o por mejoras a los sistemas actuales.

3.9 Acuerdo de niveles de servicio.

Se debe tener en cuenta, los procesos involucrados en la operación y a partir de esto, generar la creación de un catálogo de servicio, además deben visibilizar los roles y las responsabilidades fundamentales en cada etapa de los procesos. En ciertas ocasiones y en diversas empresas la solución a incidentes se transfiere a un tercero ya que no se cuenta con personal interno, que logre solventarlos de forma oportuna.

Los sistemas OT son administrados, generalmente, por áreas de ingeniería, mantenimiento eléctrico o de comunicaciones y tienden a minimizar la importancia que realmente tiene el sistema, es por esto que se sugiere que como buena práctica el mantenimiento de estos equipos y su software

estén en la cobertura de IT lo que disminuye los costos de mantenimiento, permite mejorar los tiempos y organiza la frecuencia de la actividad.

A diferencia de IT donde se evidencia una gestión centralizada y sistematizada para la atención de los usuarios, OT carece de una plataforma que permita gestionar los incidentes asociados al sistema, además este tipo de herramienta sirve para hacer seguimiento que conduzcan a la resolución de problemas de forma oportuna, incluso los registros sirven de apoyo para planificación del presupuesto y proyectos asociados a la infraestructura. Es importante manejar un plan de atención de incidentes bien estructurado y basado en una gestión de configuración, la adopción de gestión de cambio, administración de proveedores para agilizar los tiempos de respuesta y solución a dichos incidentes.

Otra diferencia marcada con IT, es que ha tenido la ventaja de contar con una rápida evolución y así mismo la evolución del recurso humano ha tenido la adaptación necesaria, mientras que en OT, dicha evolución no se ha dado con la misma rapidez lo que se traduce en falencias en el cumplimiento de las necesidades de carácter técnico y los procesos de planificación y gestión de proyectos.

Dado que los procesos que abarcan la infraestructura OT tienden a manejarse de forma muy reservada, esto porque los procesos productivos de la mayoría de compañías no se pueden revelar, es necesario generar acuerdos de confidencialidad con los proveedores e inclusive con el personal interno esto conlleva a que los procesos de atención de incidentes se puedan tardar un poco más ya que algún tipo de solución no puede provenir de cualquier fuente, basados en estos argumentos es donde, sobresale la importancia de documentar los procesos industriales.

Se deben restringir los accesos de terceros gestionando el nivel de privilegios mínimos que se deben otorgar a los terceros, personal de soporte, técnicos de campo, operadores de la cadena

de suministro y proveedores de servicios administrados. Extrayendo el orden y la importancia de los procesos en la gestión de incidentes desde la metodología de ITIL, se recomienda seguir los siguientes:

- Propender y mantener una excelente calidad del servicio
- La debida planificación para la implementación de herramientas, equipos y/o servicios.
- Garantizar un nivel mínimo de disponibilidad de los servicios atendidos.
- Mantener continuidad en la operación de los servicios establecidos.

3.10 Seguridad de redes.

Dentro de las buenas prácticas, un aspecto fundamental es asegurar las redes de datos, para esto es necesario que el equipo de redes o quien haga la administración tenga conocimiento de la topología y el detalle de cada uno de los componentes y sus características, (switches, firewall, pcs, equipos de automatización en red) a que capa pertenece, direccionamiento IP, protocolos de transporte, entre otros.

Como se mencionaba anteriormente, la red OT es una infraestructura crítica, por ende, se debe contar con un medio robusto y fiable que soporte la operación de todos los equipos involucrados en el sistema y todo el intercambio de datos necesarios para su correcto funcionamiento.

Debido a la tendencia creciente de ataques hacia las infraestructuras OT, para este caso en específico, se deben tener en cuenta aspectos mínimos de seguridad para proteger estas redes y equipos, con el fin de mitigar el riesgo a ser víctimas de ataques, a continuación, se enuncian y se describen brevemente algunos de ellos:

- Firewall. Es necesario contar con un firewall interno que limite el acceso de otros equipos LAN no pertenecientes a la red OT a través de políticas y reglas de seguridad diseñadas por expertos de red.
- Segmentación de red: La red OT como buena práctica debe estar separada de la red IT, a pesar de que, para los temas de análisis, es necesario acceder desde la red IT a los datos que se tienen en los equipos OT, debe existir un acceso seguro, esto se puede lograr con el uso de equipos especializados como: el firewall.
- Acceso Físico, Gestionar el acceso físico mediante una combinación de controles basados en cerraduras, lectores de tarjetas y sistemas biométricos, registrando todos los accesos autorizados y protegiendo las interfaces, físicamente accesibles como: puertos USBs, etc.
- Protección de Aplicaciones y Servidores: Es necesario garantizar la configuración segura de las diferentes aplicaciones empezando con el propio SCADA, actualizándolos con los parches disponibles es recomendable utilizar una combinación de SIEM, IDS/IPS y antivirus para proteger, prevenir y registrar amenazas.
- Mantenimientos preventivos: Se debe planear el mantenimiento físico de la red, pero con un mayor grado de importancia se debe hacer el manteamiento a la parte lógica, lo que debe contener revisión de logs, actualización de firmware, actualizaciones de seguridad, para el fortalecimiento de la infraestructura.
- Documentación de los procesos de red: Contando con una adecuada documentación de los elementos de la red OT, se facilita la toma de decisiones para la atención de incidentes, así como para planes de renovación tecnológica.

3.11 Continuidad de Negocio.

No obstante, de ser catalogado como una buena práctica sino como un resultado de las buenas prácticas es conseguir planes y estrategias para la continuidad de negocio, en este apartado se enfocan esos esfuerzos hacia OT. Por parte de la organización se deben diseñar los planes que contengan los procedimientos de respuesta ante incidentes de seguridad en el peor de los escenarios ataques a la seguridad informática, fallos en la operación de los equipos, daños en la infraestructura y cualquier otro incidente que obstruya la operación normal.

En dichos planes se debe estimar el impacto de cada riesgo y tener los procesos que permitan un retorno de las operaciones OT a la normalidad en el menor tiempo posible, apoyándose en medidas contingentes tales como: copias de respaldo de la información, red alterna, equipos físicos de copias de respaldo, documentación de los procesos con sus elementos y responsables.

3.12 Sensibilización

Tal como se mencionó anteriormente, tomando como ejemplo el caso Stuxnet gran parte de los ataques producidos en infraestructuras críticas, son a través de las personas que abren accidentalmente correos o usan elementos infectados o acceden a páginas maliciosas. Por tal razón, es de suma importancia concienciar al personal sobre la protección proactiva y reactiva, con el fin de que sean capaces de identificar situaciones fuera de lo común tomando las siguientes pautas básicas según el Kit de Conciencia del Instituto Nacional de Bioseguridad, (Incibe, 2017):

- No abrir archivos desconocidos de remitentes desconocidos o sospechosos.
- Cambiar contraseñas con frecuencia y no dejarlas en sitios accesibles ni compartirlas con otras personas.
- Evitar las descargas y los accesos a sitios web sospechosos.
- Tener copias de seguridad.

- No conectar dispositivos externos que no hayan pasado por un antivirus.
- Mantener actualizados los navegadores.
- Implementar medidas técnicas como pueden ser SPF DKIM o DMARC.
- Establecer medidas para el acceso al correo.

4. CONCLUSIONES

A lo largo del documento se hacen recomendaciones transversales para las organizaciones, teniendo en cuenta, la importancia de generar convergencia entre IT y OT, donde se involucran los procesos, la tecnología y las personas con el fin de minimizar el impacto de un ciberataque y garantizar la continuidad de una operación productiva, sin desconocer que la seguridad no existe en un 100%.

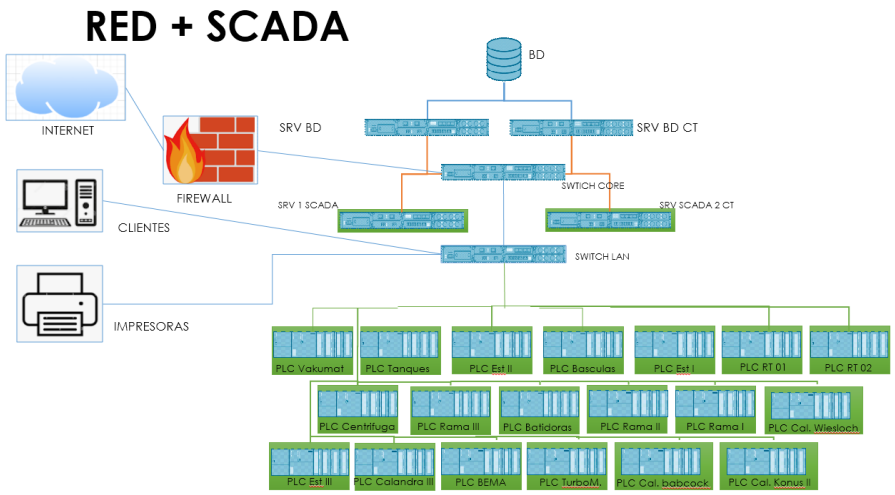
Con la adopción de buenas prácticas en seguridad de la información para ambientes OT, se logra el apalancamiento a la continuidad de negocio, ya que permite el diseño de los planes de acción para recuperar y continuar las operaciones IT y OT.

Con los controles sugeridos en este artículo se busca minimizar los riesgos para la infraestructura OT y disminuir la brecha de la materialización de un riesgo a través del cumplimiento de los procesos, procedimientos, sensibilizaciones, entre otras.

A partir de la exploración e investigación de las prácticas habituales en un entorno de la industria OT, se evidenciaron una serie de riesgos que comprometen la seguridad de la información, los equipos y la integridad de las personas, los cuales deben ser mitigados a través de una serie de controles y mejoras que dan lugar a evitar la interrupción de los procesos productivos y finalmente, minimizar el impacto económico, social y reputacional en la organización.

Según el análisis efectuado al trabajo de campo y con base en el estudio de la adopción de buenas prácticas a la seguridad de la información para industrias OT. El equipo de trabajo propone una serie de mejoras para minimizar los riesgos asociados a la seguridad informática de la infraestructura crítica para la organización.

Ilustración 8. *Situación Actual*

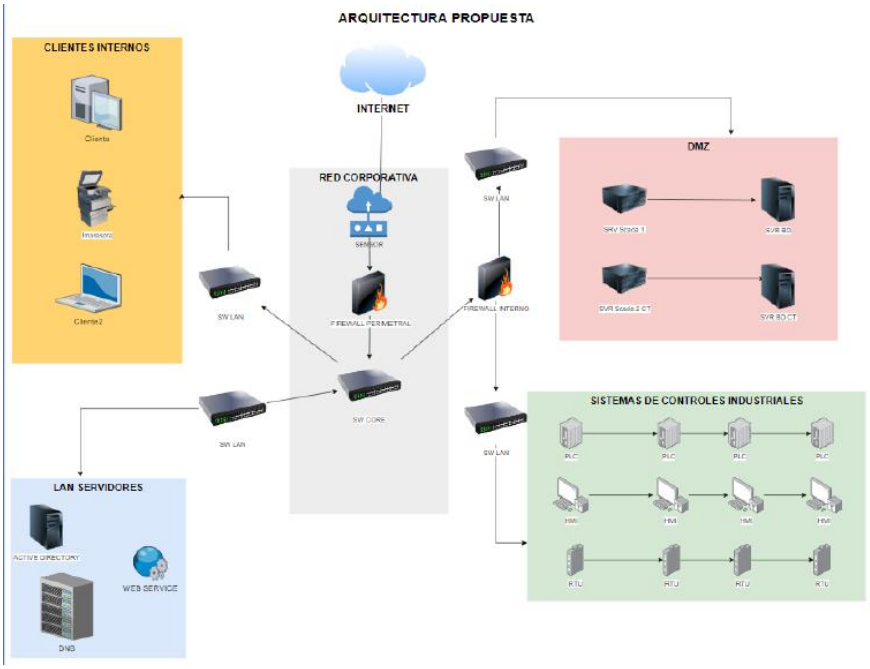


Fuente: Autores

En ese orden de ideas se presentan las siguientes oportunidades de mejora:

- Implementar un sensor de Internet (IPS/IDS/SIEM)
- Configurar una red DMZ para los servidores SCADA
- Instalar un Firewall interno para configurar la segmentación de la red, aislando la red SCI de las demás redes de la organización.
- Instalar un Switch independiente para la conexión de los servidores SCADA
- Instalar un Switch independiente para la red DMZ
- Generar planes de mantenimiento de para la infraestructura de red que soporta SCADA

Ilustración 9. *Arquitectura Propuesta*



Fuente: Autores

5. REFERENCIAS BIBLIOGRÁFICAS

Asensio Susana, Menéndez Miguel G., Valiente José, Zuluaga Diego (2018). Centro de Ciber Seguridad Industrial.www.cci-es.org.

Centro de Ciberseguridad Industrial (2021). Pirámide de Automatización Industrial. (https://www.cci-es.org/activities/guia-de-bolsillo-ciberseguridad-en-la-piramide-de-automatizacion-industrial)

Explore the Platform**,** Shodan Search Engine for the Internet of Everytinig- Puerto 502. (2022). Consulta en línea https://www.shodan.io/.

La falta de coordinación de los equipos de Ciberseguridad. (14 de enero de 2020). Recuperado de https://www.itdigitalsecurity.es/.

(Langner, 2011, p. 50; Lindsay, 2013, p. 391). Css Cyber Defense Project. https://arato.inf.unideb.hu/

Mark Cotteleer, Brenna Sniderman (2017). Forces of change: Industry 4.0. https://www2.deloitte.com/ec/es/pages/consumer-business/articles/-que-es-la-industria-4-0-.html.

Ospina Camilo. (2019). Convergencia de Seguridad en Sistemas de Tecnologías Operacionales y Tecnológicas de la Información. Monografía Universidad Nacional Abierta y a Distancia UNAD. Bogotá Colombia. https://repository.unad.edu.co/bitstream/handle/10596/31643/71782435.pdf?sequence=1&isAllowed=

Stouffer Keith, Pilitteri Victoria, Lightman Suzanne, Abrams Marsall, Hahn Adam (2015). Guide to Industrial Control Systems (ICS) Security. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.

Sobre los Autores

Diego Alejandro Moreno González, Nació en Bogotá Colombia, candidato a Especialista en Seguridad de la Información de la Fundación Universitaria Los Libertadores, Ingeniero Electrónico. Email: damorenog@libertadores.edu.co Diplomado en Gestión de proyectos TIC, Universidad de San Buenaventura, Certificado ITIL V3 Fundamentos, CCNA Cisco, IoT Essentials. JNCIA Juniper, Fortinet NSE1 NSE2 NSE4, Oracle Cloud Infraestructura, Azure AZ900 Fundamentos, AZ104 Administrador, AZ500 Seguridad, AZ 700 Diseño e implementación, SC 900 Security complimiento, SC300 Identidad, SC400 Protección DP 900 Datos fundamentos.

Diego Armando Moreno Chingaté, Nació en Bogotá Colombia, candidato a Especialista en Seguridad de la Información de la Fundación Universitaria Los Libertadores, Ingeniero de sistemas de la Universidad Ecci, Email: damorenoc02@libertadores.edu.co, Certificado en Scrum Foundations, con conocimiento en administración de sistemas operativos Linux y Aix, administración de infraestructura de redes y gestión de proyectos de tecnología.

Luis Carlos López Prieto, Nació en Bogotá Colombia, candidato a Especialista en Seguridad de la Información de la Fundación Universitaria Los Libertadores, Ingeniero de Sistemas de la Fundación Universitaria Panamericana, Email: lclopezp@libertadores.edu.co Administrador de Infraestructura Tecnológica de Servidores bajo ambientes Microsoft Windows Server, Virtualización en VMware, Hyper-v, Correo electrónico Exchange Server, Office365 y Herramientas de Colaboración, Transferencia de conocimiento y experiencia en desarrollo de proyectos desde su etapa de diseño hasta su implementación.

Yenny Isabel Serrato Rodríguez, Nació en Bogotá Colombia, Especialista en Seguridad de la Información de la Universidad Sergio Arboleda e Ingeniera en Telemática de la Universidad Distrital Francisco José de Caldas. Email: yiserrator@libertadores.edu.co. Es certificada como: CEH, Auditor Líder e interno ISO 27001:2013, Auditor interno ISO 22301:2019, ITIL, Cobit, Scrum Foundations, entre otros. Adicional, posee conocimientos en informática forense, ciberseguridad, auditoría interna y manejo de proyectos. Se ha desempeñado como Oficial de seguridad de la información para empresas multinacionales, consultor para empresas públicas y privadas liderando equipos de trabajo multidisciplinarios, además docente universitario en varias universidades.