JUNIO 2024

Alberdi, Juan Ignacio
Arone, Cecilia
Belaustegui, Enrique
Calvache, Daniel
Constanzo, Bruno
Curti, Hugo
Ferrari, Leandro
García, Edith
Girotti, Adrián
González Avellaneda, Manrique
González, Gerardo Fabián
Kamlofsky, Jorge
Manrique, Daniel Arnaldo
Romero, Oscar
Ruiz De Angeli, Gonzalo
Trigo, Santiago

GUÍA-ICI

GUÍA PARA EL ABORDAJE DE INCIDENTES DE CIBERSEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS INDUSTRIALES

UNIVERSIDAD FASTA
FACULTAD DE INGENIERÍA
InFo-Lab
INSTITUTO DE CIENCIAS FORENSES
UNIVERSIDAD FASTA
UNDEF
FACULTAD DE INGENIERÍA DEL EJÉRCITO
UAI
Universidad Abierta Interamericana

GUÍA-ICI : guía para el abordaje de incidentes de ciberseguridad en infraestructuras críticas industriales / Juan Ignacio Alberdi ... [et al.]. - 1a ed - Mar del Plata : Universidad FASTA ; Ciudad Autónoma de Buenos Aires : Universidad Abierta Interamericana ; Universidad de la Defensa Nacional, 2024.
Libro digital, PDF

Archivo Digital: descarga y online
ISBN 978-631-90546-3-7

1. Ciberdelitos. 2. Seguridad Industrial. 3. Infraestructuras. I. Alberdi, Juan Ignacio
CDD 004.02

Índice de Contenidos

Índice de Figuras

Índice de Tablas

Presentación

El presente trabajo fue desarrollado por el Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense (InFo-Lab), dependiente de la Facultad de Ingeniería de la Universidad FASTA, el Ministerio Público de la provincia de Buenos Aires y la Municipalidad de General Puyerredón; La Facultad de Tecnología Informática de la Universidad Abierta Interamericaca (UAI) y la Facultad de Ingeniería del Ejército (FIE) de la Universidad de la Defensa Nacional. Está dirigido por el Ing. Santiago Trigo (InFo-Lab) y tiene como co-directores al Mg. Lic. Jorge Kamlofsky (UAI) y al Ing. Adrián Girotti (FIE). Los autores son: Alberdi, Juan Ignacio (FI-UFASTA); Arone, Cecilia (FIE); Belaustegui, Enrique (UAI); Calvache, Daniel (FIE); Constanzo, Bruno (FI-UFASTA); Curti, Hugo (FI-UFASTA); Ferrari, Leandro (FI-UFASTA); García, Edith (FIE); Girotti, Adrián (FIE); González Avellaneda, Manrique (FIE); González, Gerardo Fabián (FI-UFASTA); Kamlofsky, Jorge (UAI); Manrique, Daniel (UAI); Romero, Oscar (UAI); Ruiz De Angeli, Gonzalo (FI-UFASTA); Trigo, Santiago (FI-UFASTA).

Las entidades demandantes de este trabajo son la empresa “Trend Ingeniería” y Dirección Nacional de Ciberseguridad (Jefatura de Gabinete de Ministros, Presidencia de la Nación). Por otra parte, las entidades adoptantes son: “Trend Ingeniería”, Comando Conjunto de Ciberdefensa (Elemento operativo), Dirección de Ciberdefensa del Ejército (Elemento operativo) y la Facultad de Ingeniería del Ejército (Difusor del conocimiento científico - tecnológico de Ciberdefensa y Ciberseguridad en el Ejército Argentino).

El trabajo aquí expuesto se encuentra en el “El Banco Nacional de Proyectos de Desarrollo Tecnológico y Social (Banco PDTS)” y es coordinado por el Ministerio de Ciencia, Tecnología e Innovación de la Nación, bajo el número de proyecto PDTS-0478.

Agradecimientos

Se hace especial mención y agradecimiento a los alumnos Renzo Agustín Romeo (UNMDP), Lucas De Lellis (UNMDP), Santiago Nicolás Lapiana (UNMDP) y Valentina Funes (FI-UFASTA) por la colaboración en la validación, edición, ajuste, compilación y diseño de la presente Guía. En el caso de los alumnos de la Universidad Nacional de Mar del Plata (UNMDP), su trabajo estuvo comprendido dentro de su Práctica Profesional Supervisada (PPS) como parte de formación como futuros ingenieros informáticos. Para el caso de Valentina Funes, la misma fue en el marco como investigadora alumna de la FI-UFASTA dentro del presente proyecto.

1. Introducción

En el marco de la Estrategia Nacional de Ciberseguridad, **la Resolución N°1523/2019** define las infraestructuras críticas como *"aquellas que resultan indispensables para el adecuado funcionamiento de los servicios esenciales de la sociedad, la salud, la seguridad, la defensa, el bienestar social, la economía y el funcionamiento efectivo del Estado, cuya destrucción o perturbación, total o parcial, los afecte y/o impacte significativamente"* y las infraestructuras críticas de información como *"las tecnologías de información, operación y comunicación, así como la información asociada, que resultan vitales para el funcionamiento o la seguridad de las infraestructuras críticas.";* resulta imperioso contar con métodos y herramientas que salvaguarden los activos para este tipo de organizaciones.

La automatización de los procesos industriales se ha convertido en un proceso clave en la industria, y ha abierto las puertas a la Industria 4.0. En Argentina, la automatización industrial se encuentra presente en varios procesos, como por ej.: Semaforización, generación y transporte de energía eléctrica, Agua corriente, procesos de refinación, extracción de petróleo, salud entre otros, muchos de los cuales forman parte de la denominada "infraestructura crítica", tanto en el ámbito privado como público.

Estos sistemas de automatización y control de procesos no pueden apagarse, no pueden detenerse sin programación previa, ya que podría generar que sus sistemas operativos y aplicativos no se actualicen y podría generar una puerta de entrada tanto para el robo de información como para la modificación de procesos, entre otros.

Las *infraestructuras críticas industriales,* ante esta situación, precisan contar con una guía que contemple tanto un análisis y evaluación del riesgo, como recomendaciones para mitigarlo e instrucciones de actuación básica de primera respuesta a incidentes.

Se estima que los ataques a infraestructuras críticas y servicios públicos aumenten en gran medida cada año y que los conflictos entre países estarán basados en ataques informáticos. Entre los ataques más comunes y perjudiciales a las industrias se pueden mencionar el **ransomware y el phishing.**

Resulta de suma relevancia contar con una guía que contemple las medidas de Ciberseguridad imprescindibles para el abordaje de la problemática en infraestructuras que puedan

generar el colapso de los servicios esenciales para la población, además de reducir los riesgos, ya sean monetarios, de reputación o físicos, que podrían ocasionarse ante un ataque informático.

Esta guía permitirá trabajar tanto *ex ante* (prevención) como *ex post* (actuación, remediación, resiliencia) en el abordaje de incidentes de ciberseguridad en infraestructuras que requieren una gestión de extrema seguridad, por su condición de criticidad para la propia organización y la población en general; especialmente, en instalaciones industriales del Estado o de empresas que brindan servicios esenciales (agua, energía, comunicaciones, combustibles, etc.). Un problema de seguridad en estas instalaciones puede significar el colapso de servicios vitales para la población. De ahí la importancia de desarrollar un producto tecnológico de soporte a la gestión.

2. Definiciones Iniciales

Esta **Guía para el abordaje de Incidentes de Ciberseguridad en Infraestructuras Críticas Industriales** pretende recoger una referencia de los aspectos esenciales de ciberseguridad relativos a los sistemas de control industrial y de cómo estos, a través de los años, han sido conectados "a la red" quizás sin tener el debido control en su gestión.

Con el fin de unificar y normalizar lenguaje y conocimientos se incluye una breve introducción de conceptos sobre la organización y la gestión de la seguridad para luego ingresar en los aspectos técnicos los cuales son tratados en forma agnóstica, aplicable prácticamente a todas las marcas y proveedores de tecnología. Somos conscientes que las características, necesidades y tecnologías sectoriales específicas presentes en determinadas infraestructuras pueden limitar la aplicación directa de algunas medidas o recomendaciones y para esto se sugiere valorar de forma proporcional a los factores tecnológicos, propiedades técnicas de los sistemas a proteger y el modelo de negocio.

La palabra seguridad proviene de la palabra latina *securitas* y se refiere a la seguridad como la ausencia de riesgo o, también, a la falta de confianza en algo o alguien.

Además, la palabra seguridad también puede ser traducida del inglés con dos términos: ***Safety*** **y** ***Security*** que definen dos conceptos diferentes. ***Safety*** se define como la condición de estar protegidos contra eventos accidentales, por lo tanto, se debe asociar la seguridad proveniente

de *safety* con todas aquellas medidas que ayudan a evitar la ocurrencia de un accidente. Dentro de los sistemas de control industrial se asocia la palabra *safety* con la prevención de daños a nivel de equipamiento, instalaciones, personas o la misma sociedad, que pudieran impactar accidentalmente en las actividades o elementos relacionados: operación, automatización, control y supervisión del proceso industrial.

En cambio, ***security*** se define como el grado de resistencia o de protección frente a daños intencionados. Se aplica a cualquier activo vulnerable y valioso, como una persona, vivienda, comunidad, nación u organización. En definitiva, *security* está relacionado con la prevención de eventos malintencionados, potencialmente dañinos como sabotajes, robos, ciberataques, etc., y abarca todas aquellas medidas específicas para prevenir un incidente malintencionado y mitigar los posibles daños.

En el ámbito de las organizaciones, la palabra *security* suele identificarse con los cuerpos de seguridad como policía, militares, seguridad privada, etc., que son los que han utilizado históricamente el término. Hoy en día también se asocia con los ingenieros informáticos para hablar de *information security* (seguridad de la información) o ciberseguridad, es decir, con la seguridad de los sistemas computacionales y del ciberespacio.

Resumiendo, los conceptos de **Safety y Security**, podemos decir que **Safety** protege a las personas y el medio ambiente del daño que el equipamiento le puede causar, y **Security** protege al equipamiento del daño que las personas pueden hacerle. Por eso, más adelante veremos cómo la Tecnología de la Operación de los sistemas industriales se concentra en la consecuencia al analizar el riesgo, mientras que IT (Tecnología de la información) lo hace sobre el incidente.

En los sistemas de automatización y control y en los sistemas de información relacionados se hace uso del término *security*, tanto en el ámbito de la seguridad lógica, donde se utilizarían elementos como cortafuegos, antivirus, etc., como en el ámbito de la seguridad física, donde se utilizan cámaras de vigilancia, sensores de presencia, control de acceso con huella o lectura facial, etc. para proteger estos mismos sistemas, las máquinas físicas y otras infraestructuras frente a ataques en el ámbito de lo físico.

Como punto de partida, y a raíz de la necesidad de interconectar a los sistemas de automatización industrial, se infiere que existen dos áreas que convergen en este tipo de organizaciones: el área IT (*Information Technology* - Tecnología de la Información) y el área OT

(*Operational Technology* - Tecnología operativa). La primera de ellas refiere a aquella tecnología utilizada para manejar información que puede estar presente en cualquier tipo de organización. En cambio, la tecnología operativa es la que está directamente ligada al proceso industrial y se refiere a aquella tecnología utilizada en una planta de producción que contempla el uso de hardware y software específico.

Al realizar un enfoque directo sobre el área IT, y específicamente en aquella materia que intenta proteger los activos digitales -la Seguridad Informática-, se encuentran 3 (tres) pilares utilizados para tal fin: la *confidencialidad, la integridad y la disponibilidad*. Estos podemos representarlos en una pirámide tal como se muestra en la figura 1.

Figura 1: Pirámide de los pilares de IT (Fuente: Elaboración propia)

La **confidencialidad** es el pilar de la seguridad de la información por la que se garantiza el nivel de secreto necesario, su tratamiento y que sólo será accesible por personal autorizado. La **integridad** es el pilar por el que se garantiza que los datos siempre serán correctos y fiables y que no sufrirán modificaciones malintencionadas o no, en todo su ciclo de vida. Por último, la **disponibilidad** es el pilar que garantiza el acceso a los datos cuando se lo requiera y necesite. Como se puede observar, para la Seguridad Informática en el área de IT, esta pirámide presupone un orden de prioridades donde la **confidencialidad y la integridad** poseen mayor prioridad que la **disponibilidad.**

Ahora bien, cuando se trata de aplicar estos conceptos en el área OT, se obtiene una pirámide similar, pero con algunos cambios, como se muestra en la figura 2:

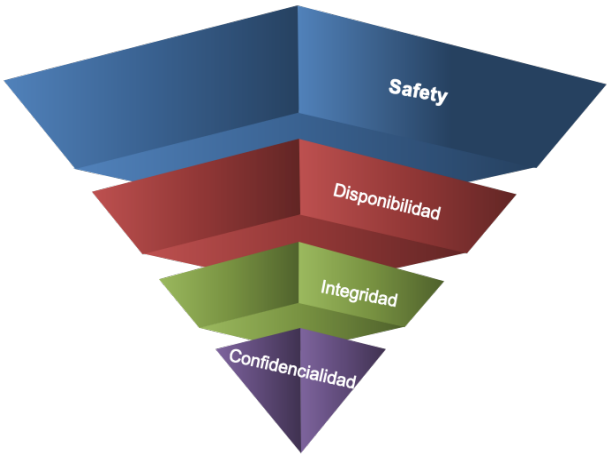


Figura 2: Pirámide de los pilares de OT (Fuente: Elaboración propia)

Aquí es donde aparece fuertemente el término **"*Safety*".** Este es el principal principio en OT: *la protección y seguridad física de los operarios en la planta de producción, el medio ambiente y la sociedad*. Luego, se observa que los principios son los mismos que para el área IT, pero están invertidos, donde **la disponibilidad toma mayor preponderancia frente a la confidencialidad y la integridad**. Esto tiene que ver con que el acceso a la información, al hardware o al software de la planta debe estar garantizado en todo momento, ya que una interrupción en la disponibilidad podría afectar el normal funcionamiento del proceso de una planta de producción, afectando tanto a la organización como a la sociedad.

Es en este juego de prioridades donde la convergencia entre el área IT y el área OT presenta un nuevo desafío. Cuando se intenta conectar a la red IT al área OT, el área de IT suele pretender utilizar los mismos mecanismos de control y protección aplicados para su área de injerencia, desconociendo este cambio de prioridades que el área de OT presenta. Es aquí donde no hay consenso entre estos sectores y, en muchas ocasiones, el sector OT queda desprotegido y expuesto a diferentes tipos de ataques.

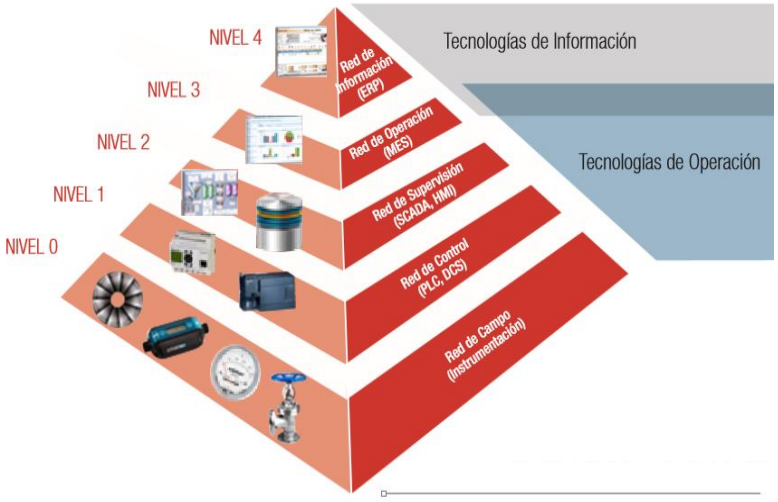
Es por todo lo aquí expuesto, que **lo que se enunciará durante todo el desarrollo de esta guía, tendrá como eje fundamental las prioridades que presenta el sector OT, contemplando sus características y diseñando planes que, se considera, puedan llevarse a cabo**. Pero también, **es importante destacar que esta guía pretende ser lo más abarcativa posible, poder aplicarse en cualquier tipo de infraestructura de automatización industrial, desarrollando lineamientos generales, y que la aplicación específica y particular de cada organización, deberá llevarse a cabo por los miembros de aquella organización que pretenda aplicarla.**

3. Marco Conceptual

Como referencia para el diseño y aplicación de la guía, se ha utilizado la pirámide de automatización -ISA95- desarrollada por Sociedad Internacional de Automatización (ISA por sus siglas en inglés), la cual describe una topología de red, con sus diferentes niveles y componentes que actúan en cada uno de ellos, en una organización de automatización industrial. Esta pirámide integra sistemas de control y de negocio y propone un modelo denominado PERA -ver figura 3-, que establece 5 niveles lógicos bajo los cuales se agrupan en segmentos de red los elementos arquitectónicos con diferentes funciones. Esta división ayuda a diseñar políticas que emplean medidas específicas en cada nivel y establecen mecanismos de seguridad para el flujo de información.

Al diseñar una arquitectura de red, siempre se recomienda construir un modelo con segmentos de red diferenciados desde una perspectiva de seguridad. Al dividir la red en segmentos con diferentes funciones y objetivos, se puede aplicar una mayor granularidad en las medidas de seguridad y se puede evitar el flujo de información innecesario. De acuerdo con esta recomendación, el proceso y redes del sistema de control industrial deben separarse de la red corporativa ya que la naturaleza del tráfico de estas áreas está perfectamente diferenciada. En la zona de red corporativa son necesarios servicios como acceso a Internet, correo electrónico, microinformática, FTP, etc., que suponen un riesgo para la zona de red de SCI (Sistemas de Control Industrial).

Por lo tanto, como primer paso en la planificación de una infraestructura SCI, se recomienda establecer diferentes niveles en la arquitectura de la red, identificar cada parte según su función en la plataforma y definir mecanismos de control de flujo de datos entre diferentes segmentos de red.



NIVEL 0

Nivel de adquisición de datos de campo o instrumentos, es decir, sensores y actuadores que se encuentran repartidos por el proceso y que permiten el control de las máquinas y equipos de producción.

Este documento se centra en los **sensores inalámbricos.**

NIVEL 1

Nivel que agrupa a todos **controladores locales** tales como: ordenadores, PLCs, etc.

Los equipos de este nivel utilizarán **datos del proceso** proporcionados por los instrumentos del NIVEL 0 y darán **consignas a los actuadores.**

NIVEL 2

Nivel de supervisión con equipos destinados a **controlar la secuencia de fabricación y/o producción** como: SCADA, estaciones de operaciones o servidores de ingeniería.

NIVEL 3

Nivel de operaciones de fabricación donde se **gestionan los flujos de trabajo** para producir u optimizar los productos finales.

NIVEL 4

Nivel de **gestión** donde se desarrolla todas las actividades relacionadas con el negocio necesarias en una **organización** industrial, **comunicando** distintas plantas y manteniendo **relaciones** con proveedores y clientes.

Figura 3: Niveles Purdue (Fuente: Centro de Ciberseguridad Industrial - CCI)[1]

Una vez comprendidos estos diferentes niveles que se encuentran en este tipo de organizaciones es preciso comprender que, en cada una de ellas, coexisten hardware, software y firmware, que pueden ser susceptibles a diversos tipos de ataques. Donde el **hardware** podría ser definido, en sentido amplio, como las partes físicas, tangibles, sus componentes eléctricos, electrónicos, electromecánicos y mecánicos de un activo. Esto incluye las conexiones entre diferentes componentes, ya sea con cables o fichas de cualquier tipo. Se incluyen, también, los gabinetes o cajas, los periféricos de todo tipo, y cualquier otro elemento físico involucrado.

El **software** es el soporte lógico al sistema formal (sistema abstracto compuesto por un lenguaje formal, axiomas, algoritmos, entre otros) de un sistema informático. Comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas. La interacción entre el software y el hardware hace operativo un dispositivo ya que el

[1] *https://www.cci-es.org/*

software envía instrucciones para que el hardware las ejecute utilizando la funcionalidad de sus partes. Este puede ser dividido en varios grupos como el Sistema Operativo o software de base y aplicaciones en general. El Sistema Operativo es el encargado de gestionar los recursos de hardware y brindar soporte a las aplicaciones mientras que las aplicaciones son las encargadas de agregar funcionalidades específicas al sistema.

El **firmware** es un programa informático integrado en el hardware (chips, placas y circuitos), que posee la característica de ser inalterable y establece la lógica de más bajo nivel que controla sus circuitos electrónicos. Se encuentra almacenado de forma permanente en el hardware y se ejecuta directamente desde allí. Está íntimamente integrado con la electrónica del dispositivo, es el software que tiene directa interacción con el hardware, siendo así el encargado de controlarlo para ejecutar correctamente las instrucciones externas. Dada su relevancia se ha decidido separarlo tanto del hardware como del software para su estudio particular.

Por lo tanto, al contemplar estas características sobre la pirámide antes descrita, se puede entender que estos componentes se encuentran presentes y son transversales a cada uno de sus niveles.

3.1. Dominios

Para un mejor entendimiento de lo que se desarrollará durante todo este trabajo, se han identificado dominios para agrupar los diferentes activos presentes en una organización y, de esta forma, poder elaborar un plan de acción según cada uno de ellos. Un dominio es un área de conocimiento específico para un tema dado que trata las mejores prácticas para el mismo. Comprende un análisis de los principales puntos dentro de esa área en particular y un conjunto de controles para el cumplimiento adecuado de las mejores prácticas definidas.

En la Figura 4 pueden observarse los dominios existentes, que serán desarrollados en el presente trabajo.

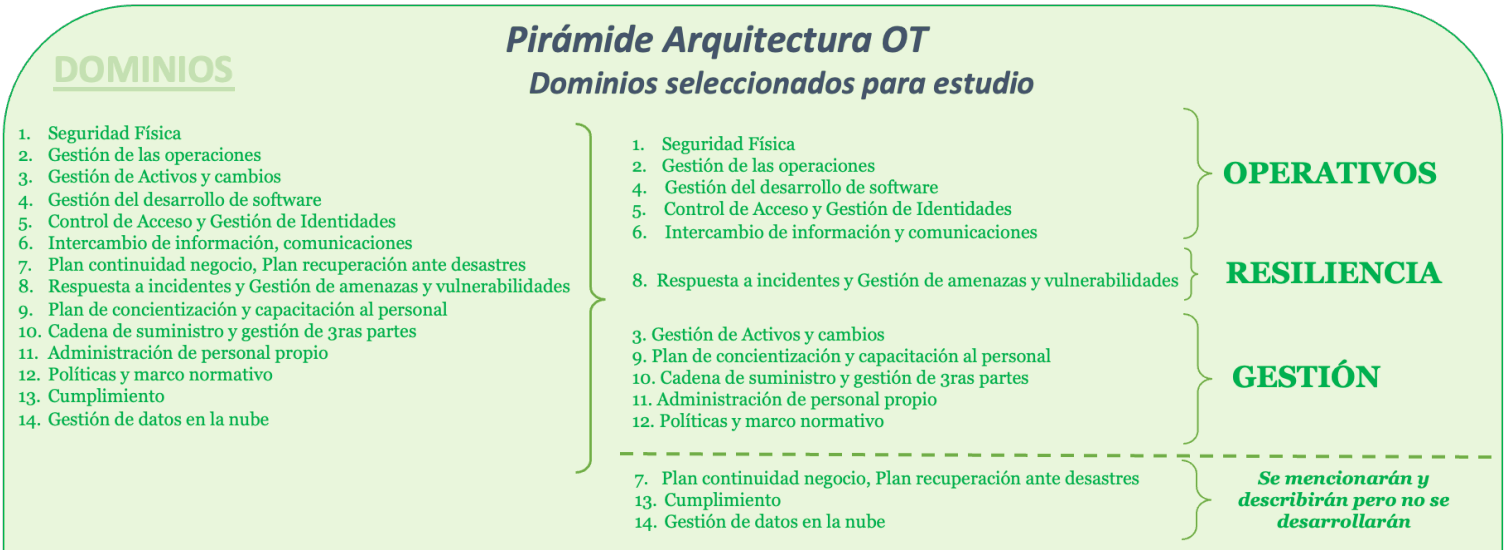


Figura 4: Dominios seleccionados para estudio. (Fuente: Elaboración propia) [2]

A continuación, se describirán cada uno de los dominios identificados en la imagen anterior.

1. **Seguridad Física:** Aborda los procedimientos de seguridad relacionados con empleados que ingresan, se desplazan, operan y dejan una organización. El objetivo de este dominio es prevenir el daño, la interferencia y el acceso físico no autorizado a las instalaciones, equipamiento e información y a los recursos de tratamiento de la información de los Sistemas Informáticos e Industriales. Incluye las medidas necesarias para proteger el medioambiente y a las personas de personal propio o contratado, así como a la comunidad misma.
2. **Gestión de las operaciones**: El objetivo de este dominio es asegurar el correcto funcionamiento y operación de los Sistemas Informáticos e Industriales, así como de los dispositivos que los componen en forma directa e indirecta, con el fin de minimizar riesgos de fallas y evitar daños a los activos, los sistemas y las personas.

[2] Fuentes consultadas para su elaboración:
- https://attack.mitre.org/resources/
- https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2
- ISO/IEC 27000:2021

3. **Gestión de activos y cambios:** El objetivo de este dominio es identificar los ciber-activos de la organización y definir las responsabilidades de protección adecuadas (concepto de propiedad) en un inventario, así como también el esquema de clasificación para la información y los mismos ciber-activos. Se debe asegurar que la información reciba un nivel adecuado de protección de acuerdo con su importancia/criticidad para la organización.
4. **Gestión del desarrollo de software:** El objetivo de este dominio es garantizar la seguridad de la información en el diseño, desarrollo, implementación y mantenimiento (ciclo de vida del desarrollo) del software, tanto de aplicación como de base y en cualquier lenguaje que fuera desarrollado.
5. **Control de Acceso y Gestión de Identidades**: El objetivo de este dominio es asegurar el control de acceso a los Sistemas Industriales y a los datos e información procesada y/o almacenada en los mismos, garantizando el acceso de usuarios autorizados y evitando el acceso no autorizado a los sistemas, aplicaciones, dispositivos y servicios.
6. **Intercambio de información, comunicaciones:** Este dominio tiene por objetivo velar por la seguridad en la información que se transfiere dentro de una organización y con cualquier entidad externa, así como en las redes, dispositivos, sistemas y aplicaciones en la cual la misma se consume. Incluye el acceso a los diversos medios de comunicación, garantizando la identificación y autenticación de todos los usuarios (personas, procesos o dispositivos de software) que participan en la comunicación alámbrica e inalámbrica, con el fin de minimizar riesgos de fallas, evitar daños e interrupciones en las actividades del proceso. Se busca principalmente proteger la integridad de los sistemas y de los datos e información que estos procesan, transmiten y/o almacenan.
7. **Plan continuidad negocio / Plan recuperación ante desastres**: Este dominio tiene por objetivo garantizar la continuidad del negocio ante cualquier falla o evento de interrupción. Debe ser parte de un Plan destinado a la continuidad de negocio de la organización.
8. **Respuesta a incidentes y Gestión de amenazas y vulnerabilidades:** El objetivo de este dominio es determinar y gestionar las acciones de resguardo, aislación, y los procesos de continuidad del negocio para la recuperación de los Sistemas ante la ocurrencia de incidentes de Ciberseguridad que pudieran perturbar, limitar o condicionar el normal funcionamiento de los mismos, siguiendo lineamientos acordes a los objetivos de recuperación del negocio. Debe asegurar un enfoque coherente y eficaz para la gestión de

incidentes de seguridad de la información, incluida tanto la comunicación de eventos de seguridad y debilidades, como el análisis forense de información.

9. **Plan de concientización y capacitación al personal**: Este dominio tiene por finalidad asegurar que, en todo momento, los empleados y personal de terceras partes que brinden servicio a la organización conozcan, entiendan y sepan que deben cumplir con el marco normativo existente y las medidas de protección adoptadas en materia de Ciberseguridad, advirtiéndoles de los riesgos que puede suponer un mal uso de los dispositivos, su operación y toda solución tecnológica que esté a su alcance.
10. **Cadena de suministro y gestión de terceras partes**: En este dominio se debe establecer lo necesario para mantener un nivel acordado de seguridad y de provisión de servicios en línea con acuerdos con proveedores, asegurar la protección de los activos de la organización que sean accedidos por los proveedores y definir requisitos y pautas de seguridad en contratos con terceros.
11. **Administración de personal propio:** El objetivo de este dominio es establecer un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización. Para así, asegurarse que los empleados y contratistas entiendan sus responsabilidades y que son adecuados para las funciones para las que se les consideran dentro del modelo de gestión establecido por la organización.
12. **Políticas y marco normativo**: En este dominio se contempla la existencia de un marco normativo formal, escrito y disponible a toda la organización. Debe proporcionar orientación y apoyo a la gestión de la seguridad de la información de acuerdo con los requisitos del negocio, las leyes y normativa pertinentes, abordando las restricciones y los comportamientos de los miembros de una organización y especificando cómo se puede acceder a los datos y quién puede acceder a determinados datos. Debe definir claramente el QUÉ, CÓMO, QUIÉN y PARA QUÉ se hacen las tareas y ejercen las funciones de forma responsable en cada posición.
13. **Cumplimiento:** Este dominio tiene por objetivo la revisión de todo el programa o plan de seguridad de la información teniendo en cuenta el cumplimiento de los requisitos legales, contractuales y reglamentarias relativas a la seguridad de la información o de los requisitos de seguridad. Debe garantizar que la seguridad de la información se diseña, desarrolla, implementa y opera de acuerdo con las políticas y procedimientos de la organización. Describe el proceso de garantizar el cumplimiento de las políticas, los estándares y las

regulaciones de seguridad informática con el fin de realimentar y mejorar en forma continua el plan vigente.

14. **Gestión de datos en la nube:** El objetivo de este dominio es proporcionar los controles mínimos para todas aquellas aplicaciones que residan o procesen datos en la denominada "nube" en términos tecnológicos. En este dominio se abordan los principales puntos para asegurar que los sistemas de servicios orientados a la nube garanticen la confidencialidad, integridad y disponibilidad de los datos.

3.2. Sistema de Gestión de la Seguridad de la Información

Si se entiende que la SI (Seguridad de la información) es una inversión, se podrá actuar de una manera metodológica en un plan de Seguridad Informática que proteja de manera sistemática a los activos digitales de una organización. Esta metodología es el Sistema de Gestión de Seguridad Informática o SGSI. Básicamente esta metodología tiene 4 fases, basadas en el ciclo de Deming conocido como PDCA (Plan – Do – Check – Act) o en español Planificar, Hacer, Verificar y Actuar.

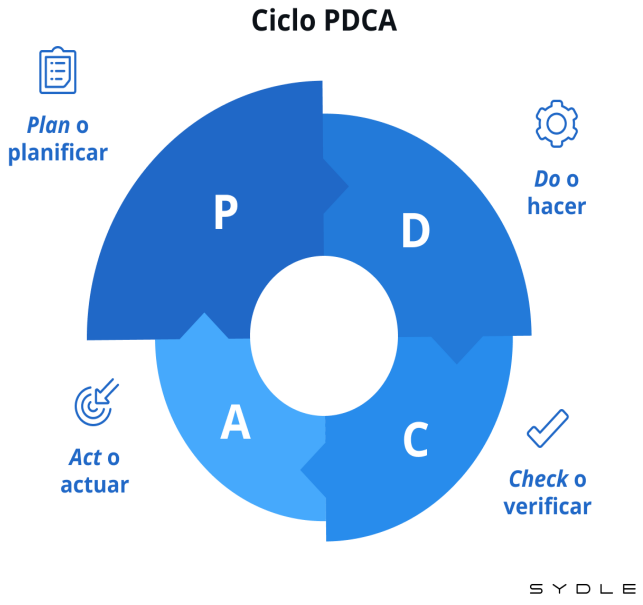


Figura 5: Ciclo PDCA (Fuente: SYDLE)

[3]https://www.sydle.com/es/blog/ciclo-pdca-61ba2a15876cf6271d556be9

La primera de ellas tiene que ver con fijar los objetivos y alcances de este plan que, generalmente, son decisiones que tomará la dirigencia de la organización, realizar una gestión de los riesgos, asignar responsables y establecer políticas para cada uno de los activos que se intentará proteger. La segunda fase tendrá por objetivo implementar las directrices definidas en la fase anterior como, por ejemplo, las políticas de mitigación de los riesgos. En la tercera fase se controlarán todos los procesos implementados en la fase anterior para medir su eficacia y detectar errores en los mismos y por último, en la cuarta fase del ciclo, se tomarán medidas correctivas a las fallas detectadas en los procesos para así mejorarlos. También, a esta última fase se la suele llamar fase de mejora. Así, nuevamente, el ciclo vuelve a comenzar.

Es importante destacar que la documentación es fundamental en todas las fases de este proceso. Sin registro de lo que se hace, cómo se hace y puntos débiles detectados, será imposible abordar un SGSI de una forma correcta.

3.2.1. Amenazas y vulnerabilidades

Es importante enfatizar que, para realizar una correcta identificación de los "problemas" presentes en una organización, se puedan identificar amenazas y vulnerabilidades. Sin una identificación de éstas , será imposible poder realizar una correcta gestión del riesgo. Existen diferentes divisiones con respecto a estos conceptos. Por lo tanto, se transcriben a continuación las definiciones utilizadas por los autores de esta guía.

De esta manera, una **amenaza** representa un evento que puede desencadenar un incidente, produciendo daños materiales o pérdidas sobre la información. Es una acción capaz de modificar de manera negativa el estado de seguridad de un activo. Una **vulnerabilidad**, en cambio, representa la posibilidad de ocurrencia de una amenaza sobre un activo. Es una propiedad de la relación entre un activo y una amenaza, representando el mecanismo de paso desde una amenaza a la agresión materializada.

3.2.2. Gestión del Riesgo

Como se mencionó en el apartado anterior, la gestión del riesgo comienza en la fase de Planificación del SGSI. Pero es importante que se defina primero qué es el riesgo. Muchas veces se suele confundir riesgo con amenaza, vectores de ataque, incidentes, vulnerabilidad, etc.

Un riesgo es un valor, es el resultado de una multiplicación. El riesgo será el producto entre la probabilidad de ocurrencia y el impacto que genera una amenaza que explota una vulnerabilidad en la organización.

Entonces el riesgo de una amenaza quedará definido por la siguiente fórmula:

$$\boldsymbol{R_A = P_A . I_A}$$

Con:

R_A: Riesgo de la amenaza *A* sobre la organización.

P_A: Probabilidad de ocurrencia de la amenaza *A*.

I_A: Impacto de la amenaza *A*.

Tanto para la probabilidad como para el impacto se definen escalas y valores para cada una de ellas. Estos valores pueden ser cualitativos como cuantitativos. Por lo tanto, el **riesgo** será la magnitud de los daños que puede causar el hecho de que una amenaza explote una vulnerabilidad causando impacto y consecuencias negativas en el sistema. Las vulnerabilidades y las amenazas, por separado, no representan un peligro. Ambas combinadas representan un riesgo a ser considerado en la respectiva gestión de riesgos.

De igual forma, la **gestión del riesgo** implica ejercer la administración de todos los recursos disponibles y llevar a cabo, en forma proactiva, las acciones necesarias para minimizar impactos negativos en todo el sistema desde la prevención, la vigilancia y la resiliencia, mitigando, transfiriendo, asumiendo o eliminando los riesgos hallados.

3.2.3. Las “4T” de la Gestión del Riesgo

Existen varias respuestas potenciales al riesgo. Las organizaciones pueden tomar una o una combinación de acciones en cada situación, dependiendo de las circunstancias. Básicamente hay 4 formas de responder a los riesgos, conocida como las “4T”:

- **Tolerar**: El riesgo es conocido y aceptado por la Organización. Es el costo de hacer negocios. Las organizaciones deben asumir algunos riesgos y no siempre se pueden mitigar o transferir de manera rentable.
- **Transferir**: El riesgo se transfiere a un tercero, aunque el mismo no sea eliminado. Puede ser posible establecer algún tipo de seguro o acuerdo que transfiera parte o la totalidad del riesgo a una tercera entidad.

- **Terminar**: se detiene el proceso, la actividad, o eliminamos las premisas, sistema, etc. Entonces el riesgo deja de existir.
- **Tratar**: El riesgo es mitigado o reducido o bien se reduce la probabilidad de que la amenaza sea explotada o se produzca el incidente, reduciendo o conteniendo el impacto. Los riesgos pueden reducirse a un nivel aceptable mediante la aplicación de contramedidas que reduzcan la probabilidad de ocurrencia o las consecuencias de un ataque. Es necesario lograr un nivel de seguridad lo suficientemente bueno. No se elimina el riesgo.
    - **Diseñar el riesgo**: Una forma de mitigación es cambiar el diseño del sistema para que el riesgo sea mitigado. Algunos riesgos existen simplemente porque se dispone de acceso a algo a lo que nunca se necesita acceso, por lo cual es recomendable deshabilitar completamente las funciones innecesarias.

Para el caso del presente trabajo, se tomará como premisa que el riesgo siempre será tratado y que será la organización quien realice la gestión del riesgo y tome las medidas necesarias para su mitigación.

3.2.4. Las "5D" para tratar el Riesgo

Otro modelo que existe de gestión del riesgo es el modelo de las "5D" que sirve para tratar o mitigar el riesgo. Es utilizado por la Seguridad de Armas Nucleares, Seguridad Perimetral o Física y la Defensa Militar.

El modelo se centra en diferentes aspectos para garantizar la protección integral de los sistemas. Estos aspectos son:

- **Deter:** Consiste en disuadir los ataques. Para eso se advierte que el sistema está vigilado. La disuasión se puede lograr haciendo que la instalación sea más difícil de ingresar, con barreras de estacionamiento, tarjetas de acceso y seguridad física o tecnológica. También advirtiendo, como con un cartel de "Sonría, le estamos filmando"
- **Detect:** Si la disuasión falla, un sistema debe garantizar la detección inmediata de la presencia de un intruso no deseado. Por ejemplo, uso de cámaras, configuración de sistemas de detección de movimientos, SIEM, firewall, entre otros.
- **Delay:** Luego de la detección, los sistemas de seguridad y el personal deben demorar la intención de los intrusos de obtener acceso no autorizado al lugar, oficina o ciberactivos. El retraso puede incluir barreras físicas, como puertas o pasillos de entrada con tarjeta de

acceso, honeypot, hardening, patching, segmentación de redes, control de acceso, entre otros.

- **Deny:** Si el retardo falla, se debe negar el acceso. Por ejemplo, control de acceso de varios factores, nuevas barreras internas como Firewalls, whitelisting, IPS, entre otros.
- **Defend:** Esta etapa es el último recurso si las anteriores fallan. Si se pueden implementar las primeras cuatro D, la última D rara vez entra en juego. Eso implicaría intentar remover el malware, ejercer acciones legales de políticas y procedimientos, y hasta atacar al atacante, lo cual puede traer perjuicios legales.

3.3. Clasificación de Medidas de Seguridad

La siguiente clasificación permite buscar y catalogar medidas de seguridad que pueden tomarse para reducir riesgos. La clasificación tiene dos ejes: por enfoque y por planos. Y la ponderación de la medida de seguridad se hace según la gravedad del riesgo. Los riesgos se presentan en los diferentes planos, y normalmente las medidas de seguridad deben aplicarse en el mismo plano donde está el riesgo, pero no siempre es así. Puede pasar que una medida de seguridad en el plano humano pueda ayudar a reducir un riesgo en el plano físico (por ejemplo). Lo ideal es encontrar al menos una medida de seguridad por cada enfoque para cada riesgo, aunque puede pasar que haya riesgos para los cuales algunos enfoques no tengan sentido.

3.3.1. Los Enfoques

El enfoque de seguridad determina la estrategia mediante la cual se busca mitigar el riesgo. Normalmente, una medida de seguridad busca reducir la probabilidad de ocurrencia, o reducir el impacto del daño, o bien eliminar la amenaza por completo. Es decir, busca reducir el riesgo. Es muy probable que varias medidas de diferentes enfoques, combinadas sinérgicamente terminen siendo mucho más efectivas y económicas que una sola medida aplicada en forma profunda, o varias medidas del mismo enfoque. Los tres enfoques generales se describen a continuación.

Enfoque Precavido o de Precaución

El enfoque de precaución busca tomar medidas que eliminen la amenaza por completo, de forma tal que el riesgo desaparezca junto con ella. Suelen ser las medidas más efectivas para eliminar los riesgos, sin embargo, en general son de largo plazo y se basan más en la experiencia o en la intuición que en la ciencia. Es preferible incluirlas siempre en los planes de seguridad, aunque a veces sean de muy largo plazo o a sabiendas de que no se implementarán en forma completa.

Enfoque Preventivo, de Prevención o Proactivo

El enfoque preventivo busca tomar medidas que reduzcan la probabilidad de ocurrencia, o el impacto del daño, o ambas. Son medidas efectivas, de mediano o corto plazo, y normalmente tienen una fuerte fundamentación científica. Complementan muy bien a las medidas de precaución cuando estas no pueden implementarse en un tiempo razonable o de manera efectiva.

Enfoque Reactivo o de Reacción

El enfoque reactivo se basa en tomar medidas que busquen detectar la ocurrencia de la amenaza analizada, y responder rápidamente a ella a fin de reducir el impacto del daño que ésta vaya a producir. Normalmente involucran un proceso de vigilancia y un conjunto de medidas urgentes que se aplicarán cuando se detecte el problema, considerando que ya las medidas de los otros enfoques no alcanzaron o fallaron.

Ejemplos:

Tabla 1: Ejemplos de medidas contra riesgos según enfoque (Fuente: Elaboración propia)

Riesgo/Enfoque	**Precaución**	**Prevención**	**Reacción**
Electrocución con la puerta de la heladera.	Nunca abrir la puerta de la heladera descalzo.	Instalar una buena toma de tierra y un interruptor diferencial.	Resucitación cardiopulmonar. Llamar a una ambulancia.
Toma de cuenta de superusuario a través de SSH por contraseña.	Deshabilitar el acceso a la cuenta de superusuario a través de SSH por contraseña.	Utilizar contraseñas largas, aleatorias y de un espacio grande con cambios periódicos.	Vigilar en busca de actividad sospechosa. Si se detecta, anular el acceso y eliminar todos los procesos sospechosos.

3.3.2. Los Planos

En la seguridad de sistemas informáticos, se pueden clasificar tanto las amenazas (y por lo tanto las vulnerabilidades y los riesgos) como las medidas de seguridad en función de la posición en el sistema donde las mismas existen. Tener en cuenta los planos es importante por dos causas principales: la primera es la completitud.

Dada nuestra tendencia a estudiar de forma analítica y compartimentada, es fácil caer en plantear, por ejemplo, un software muy seguro en términos de integridad, corriendo en una computadora completamente expuesta a fenómenos naturales, o al robo. La seguridad se orientó demasiado al plano lógico y se descuidó el plano físico.

La segunda causa es la interferencia entre planos. A veces, una medida que se toma en un plano puede interferir negativamente con la seguridad en otro plano. Por ejemplo, desde el plano lógico se puede tomar la medida de cambiar las contraseñas en períodos cortos, exigiendo un nivel de aleatoriedad alto, con la idea de reducir el riesgo de que la contraseña se comprometa. Sin embargo, esto suele impactar negativamente en el plano humano, porque afecta mucho a la disponibilidad y hace que los usuarios terminen usando claves seriadas. Como resultado, el riesgo de que la clave se comprometa es mayor en vez de menor. Se proponen tres planos generales.

El Plano Físico

El plano físico incluye todas aquellas amenazas o medidas de seguridad que intervienen directamente en componentes de hardware. Incluye computadoras, dispositivos de comunicación (switches, routers, antenas, etc.), conductores (cables eléctricos, fibras ópticas, etc.), espectro radioeléctrico en el caso que se utilice, etc. Incluye también la provisión de energía y conectividad, la regulación de temperatura, y la exposición a los fenómenos naturales y/o humanos que puedan atentar contra la integridad física de los equipos. La frontera entre el plano físico y el plano lógico puede ubicarse en el acceso a una consola local de un dispositivo. No incluye el acceso por la red, pero sí un acceso por un puerto serie, o por un teclado y un monitor conectado directamente a la máquina. Esto se debe a que normalmente a través del acceso físico a un dispositivo, o a la consola del mismo, se pueden reiniciar todas las medidas de seguridad del plano lógico (por ejemplo, blanquear la contraseña de superusuario de un sistema). Y en principio eso es deseable para poder recuperar genuinamente un sistema en caso de que se pierda el acceso. Por esta razón, las medidas que implican proteger el acceso al dispositivo o a su consola pertenecen al plano físico, mientras que si se involucra la red, ya pasa al plano lógico.

El Plano Lógico

El plano lógico incluye todas las amenazas o medidas de seguridad que intervienen directamente en los componentes de Software del Sistema. Incluye fallas de diseño o de programación (bugs), fallas de implementación o despliegue, fallas de configuración, fallas en protocolos de comunicación, fallas en protocolos criptográficos, y todo tipo de política de respaldo

de información y actualización de software. Como se mencionó antes, la posibilidad de reiniciar los sistemas de seguridad del plano lógico desde una consola pertenece al plano físico. Sin embargo, una vez que el acceso al dispositivo es a través de la red, tanto las amenazas como las medidas de seguridad corresponden al plano lógico. Por otra parte, la frontera entre el plano lógico y el humano puede situarse entre la elaboración de las medidas de seguridad en el plano lógico, y la ejecución de las mismas por parte de los humanos. Toda amenaza que pueda ser materializada sin que un ser humano intervenga (del lado defensivo) pertenece al plano lógico. Por ejemplo, pertenecen al plano lógico las amenazas de un desbordamiento de memoria en un servidor, que hace que un atacante desde lejos pueda sacarlo de servicio, o incluso controlarlo, o un código malicioso que se ejecuta automáticamente al insertar una unidad de memoria en una máquina, o al conectar la máquina a una red. Por otra parte, la amenaza de ejecución de un código malicioso como consecuencia de una acción humana (ej. seguir un enlace, descargar y ejecutar un archivo, etc.) pertenece ya al plano humano. Un protocolo semiautomático de actualización de software pertenece al plano lógico, mientras que la correcta ejecución de la parte no automática del mismo, o la amenaza presente en que esto no se haga correctamente, pertenecen al plano humano.

El Plano Humano

El plano humano incluye todas las amenazas o medidas de seguridad que requieren el accionar humano para su materialización, siempre sin contar las acciones de los atacantes. O sea, son todas aquellas cosas que los humanos hacen, o fallan al hacer, que inciden en la seguridad del sistema de información. Por ejemplo, el resguardo de las contraseñas por parte de los usuarios, y las amenazas presentes en que los usuarios fallen en este resguardo, pertenecen al plano humano. Una medida de seguridad que implica una capacitación, o una campaña de concientización, sobre el uso de las herramientas de seguridad pertenecen también al plano humano. La frontera entre el plano lógico y el plano humano puede situarse allí donde la amenaza o la medida de seguridad requiere determinada acción u omisión por parte del humano para poder materializarse. Un protocolo de respaldo que requiere que el administrador realice determinada tarea (ej. cambiar una cinta) pertenece al plano lógico. Sin embargo, la amenaza de que el administrador se olvide de realizar esa tarea, pertenece al plano humano. La ausencia de un protocolo de respaldo puede ser claramente una vulnerabilidad en el plano lógico. Por otra parte, si el protocolo existe, pero el administrador no lo ejecuta, la vulnerabilidad pasa a manifestarse en el plano humano.

3.3.3. Completitud de las Medidas de Seguridad

Al hablar de completitud de las medidas de seguridad nos referimos a la identificación de todos los riesgos y amenazas presentes en un sistema. La completitud es utópica en estos sistemas. Aún si se consiguiera detectar todas las amenazas, y determinar todos los riesgos, la naturaleza dinámica de los sistemas de información haría que el análisis quede obsoleto en poco tiempo. Sin embargo, la búsqueda de amenazas siguiendo los diferentes planos puede llevar a cubrir mucho mejor el espectro de amenazas posibles. Facilita luego la determinación de vulnerabilidades e impactos, para finalmente poder calibrar los riesgos. La recomendación es concentrarse en un plano por vez al buscar las amenazas. Una vez que están determinados los riesgos, la recomendación es buscar primero medidas de seguridad que pueden aplicarse desde el mismo plano donde está el riesgo, y luego buscar medidas de seguridad en otros planos que, o bien eliminen o minimicen la amenaza, o bien reduzcan la probabilidad de ocurrencia o el impacto del daño. Por ejemplo, la amenaza de que un código malicioso se ejecute en forma automática al insertar una unidad de memoria en una máquina puede remediarse mediante la anulación de la ejecución automática de código (medida de precaución en el plano lógico), o mediante la instalación de un software antimalware (medida de prevención en el plano lógico), o mediante la prohibición del uso de unidades de memoria externas (medida de prevención en el plano humano).

En general, resultan más apropiadas las medidas que se toman desde el mismo plano donde está el riesgo, aunque puede haber excepciones. Por ejemplo, buscar reducir el impacto del error humano tomando medidas en el plano lógico o en el plano físico puede ser beneficioso o perjudicial dependiendo de cómo se aplica: un lomo de burro en la calle fuerza a un conductor a frenar, previniendo una colisión en una esquina. Sin embargo, no facilita la concientización del conductor. En la siguiente esquina, donde no hay lomo de burro, es más probable que se produzca una colisión. Por otra parte, un cartel de alto o de cruce peligroso promueve la concientización, y si bien podría no ser tan efectivo en el corto plazo, con el tiempo prevendría más colisiones.

Todo esto significa que las medidas de seguridad deben ser lo suficientemente completas como para proteger contra una amplia gama de amenazas potenciales y deben ser revisadas y actualizadas regularmente para garantizar su eficacia continua.

3.3.4. Calibración de las Medidas de Seguridad

Las medidas de seguridad que se tomen para reducir un riesgo deben calibrarse correctamente para evitar que produzcan efectos colaterales no deseados, muchas veces en otros planos. En ese sentido, riesgos más altos justifican y necesitan contramedidas de seguridad más fuertes, pues, se necesita mitigar más riesgo. Una contramedida de seguridad es más fuerte cuando es más costosa (en tiempo, esfuerzo o dinero), o cuando impacta negativamente en la disponibilidad del sistema. A modo de recomendación general para buscar y calibrar contramedidas de seguridad, puede seguirse el siguiente procedimiento.

1. Ordenar los riesgos de mayor a menor.
2. Clasificar los riesgos según su plano.
3. Tomar el primer riesgo y buscar medidas de precaución que puedan aplicarse en el mismo plano del riesgo. Luego continuar con medidas de precaución que puedan aplicarse en otros planos. Al menos una medida de precaución es deseable.
4. Buscar medidas de prevención que puedan aplicarse al mismo plano del riesgo. Luego continuar con medidas de prevención que puedan aplicarse en otros planos. Al menos una medida de prevención es deseable.
5. Buscar medidas de reacción que puedan aplicarse al mismo plano del riesgo. Luego continuar con medidas de reacción que puedan aplicarse en otros planos. Al menos una medida de reacción es deseable.
6. Estudiar cada una de las medidas propuestas en función de su costo de implementación, y del nivel de perjuicio que puedan crear a la disponibilidad.
7. Estudiar posibles interferencias de planos que cada una de las medidas propuestas puedan tener.
8. Decidir en función de lo anterior si vale la pena recomendar la medida, recomendarla parcialmente o en forma condicionada (por ejemplo, para aplicarse en caso de un ataque), no recomendarla en absoluto, o recomendarla negativamente (o sea, recomendar que no se implemente).
9. Dar este riesgo por estudiado, sacarlo de la lista, y si quedan riesgos en la lista volver al paso 2 y repetir desde allí.

Una metodología puede ser la de buscar los riesgos que puedan mitigarse con menos esfuerzo y costo, buscando así los "quick wins" o "ganancias rápidas" que son eficaces por su bajo costo y esfuerzo y la relación de mitigación de riesgo es alta.

Por ejemplo, una medida de seguridad podría obligar a los usuarios a cambiar sus claves periódicamente, para mitigar el riesgo de compromiso de la clave. Es una medida preventiva en el plano lógico. Sin embargo, suele impactar negativamente en el plano humano como ya se mencionó antes, haciendo que al final aumente el riesgo de que la clave quede comprometida. Luego de hacer este análisis, quizá convenga recomendar que solamente se obligue a cambiar la clave al usuario la primera vez que ingresa, y cuando haya signos claros de compromiso de la clave (o sea, una medida de reacción en el plano lógico), y recomendar negativamente los cambios de claves obligatorios con períodos muy cortos. Esto va a depender, naturalmente, del impacto que tenga el compromiso de la clave. No es lo mismo si es una cuenta de correo electrónico que si es una cuenta bancaria.

4. Guía de Identificación de Riesgos en ICIs

De acuerdo con lo mencionado en el apartado anterior, se procedió a identificar cuáles serían las amenazas existentes en organizaciones de este tipo. Se ha procedido, entonces, a definir categorías de amenazas de una manera macro para un mejor entendimiento del problema. Estas categorías son:

- **Ataque físico a los equipos (AFE)**: Rotura de equipos, golpes de tensión, inundación, incendio, corte de suministro eléctrico, a la refrigeración de los equipos.
- **Ataque a los procesos (AP)**: ataque a los procesos en busca de fallas que generen mal funcionamiento o filtración de datos.
- **Ataque a los protocolos de comunicación (APC)**: relacionado estrictamente con el funcionamiento de la red de datos de la organización.
- **Ataque al sistema operativo (ASO)**: ataque que afecte directamente la correcta funcionalidad de un sistema operativo, y de esta manera, pueda escalar privilegios dentro del mismo, entre otras cuestiones.
- **Ataque a las aplicaciones s/sistema operativo (AAS)**: tipo de ataque que intenta alterar el normal funcionamiento de una aplicación para obtener información relevante para el delincuente.

- **Ataque a las personas (APP)**: tipo de ataque que no está dirigido a los sistemas ni a sus procesos, sino a las personas que los utilizan. Puede mencionarse la ingeniería social como principal técnica de ataque.

Dentro de cada una de estas categorías, se detallarán distintos procesos detectados de manera general junto con el dominio -*véase en sección "Dominios" del Marco Conceptual*- al que pertenece, identificando su amenaza específica a nivel macro, vulnerabilidad, impacto, medidas de protección y riesgo. Si se requiere conocer un detalle pormenorizado de las amenazas que podrían estar presentes en cada uno de los procesos, diríjase al ANEXO I.

Además, y según el estudio realizado, se ha detectado que no existen amenazas específicas para el sector OT de una organización. La necesidad de la industria 4.0 por conectar todos sus dispositivos a Internet, ha hecho que las problemáticas existentes hoy en día en el sector IT pasen a ser problemáticas compartidas entre ambos sectores.

Por lo tanto, la identificación de amenazas, vulnerabilidades y riesgos quedan definidos como se presenta a continuación.

4.1. Tipos de Ataque

4.1.1. Ataque físico a los equipos (AFE)

AFE01 - Control de ingreso y egreso a la planta operacional.

Dominio: Seguridad Física; Cadena de suministros y control de terceras partes.

Amenaza: Una persona puede provocar, accidentalmente o no, una falla en el sistema aprovechándose de controles de ingreso deficientes.

Vulnerabilidad: Deficiente control de ingreso y egreso de personas a la planta operacional.

Medidas de protección: En cuanto a la administración de estos controles de ingreso/egreso, se debe considerar una robustez adecuada según el nivel de seguridad que se desee. Algunos ejemplos son la implementación de autenticación por tarjetas magnéticas o RFID, identificación biométrica u otro mecanismo, con dos o más factores de autenticación. Estos debieran complementarse con personal de seguridad y planes de acción frente a la detección de intrusos según sea necesario.

Impacto Muy Alto: Un ingreso no autorizado con intenciones hostiles puede devenir en un sabotaje que puede generar desde un daño menor hasta la destrucción total de la planta y alrededores.

Riesgo Medio: El nivel de seguridad de los mecanismos de control de ingreso y egreso debe elevarse rápidamente en la medida en que la probabilidad de que ocurra un sabotaje aumente.

El control de ingreso de personal a una organización permite llevar un registro de la identidad de quien ingresa o egresa, el horario y la sede de la organización involucrada, en caso de haber varias. Éste, tiene el objetivo de supervisar que quienes entren en la organización, sean personal de la misma o una persona externa autorizada. De esta forma, se minimiza el riesgo de que se realice alguna actividad con intenciones de generar alguna falla en el sistema de la organización o se manipule algún activo de la misma, poniendo en peligro su integridad.

AFE02 - Control de ingreso de dispositivos.

Dominio: Gestión de Activos.

Amenaza: Ingreso de dispositivos no autorizados a la organización.

Vulnerabilidad: Deficiente control de ingreso y egreso de dispositivos a la planta operacional.

Medidas de protección: Control de ingreso de dispositivos. Instalación de mecanismos de bloqueo o protección en computadoras, servidores y equipos de infraestructura de red (encaminadores, switches, etc.).

Impacto Medio: Depende fuertemente de la protección instalada en los dispositivos de la planta, fundamentalmente computadoras, servidores y equipos de infraestructura de red.

Riesgo Medio: Con medidas de seguridad relativamente simples en los dispositivos instalados se obtiene una protección razonable.

El ingreso de dispositivos no autorizados, como por ejemplo pendrives, notebooks, celulares, etc., puede ser utilizado como herramienta para un ataque. El ataque Stuxnet es un ejemplo de dicha amenaza.

Los atacantes pueden interferir en la normal operación de la organización a través del uso de un dispositivo incorrectamente manipulado, con el propósito de comprometer los datos de un sistema completo. El compromiso de la cadena de suministro puede tener lugar en cualquier etapa de la misma, y puede implicar la manipulación de herramientas o entorno de desarrollo, la infección de imágenes del sistema por dispositivos extraíbles, la venta de productos falsificados, entre otras.

Si bien el compromiso de la cadena de suministro puede afectar a cualquier activo, sea software o hardware, gran parte de los ataques se centran en adiciones maliciosas a software legítimo en canales de distribución o actualización de software[4].

AFE03 - Control/Gestión de ubicación física del activo.

Dominio: Gestión de Activos.

Amenaza: Pérdida de activos.

Vulnerabilidad: Falta de control adecuado que lleva al desconocimiento de la ubicación física de activos de la organización por no llevar un control adecuado.

Medidas de protección: Registro adecuado de los activos en la organización.

Impacto Alto: La pérdida de activos no tiene una cota de daño estimable, pudiendo llegarse a pérdidas económicas o de tiempo muy altas.

Riesgo Bajo: En general, es relativamente sencillo implementar mínimas medidas de control que ofrezcan una protección razonable, y el riesgo se reduce rápidamente conforme aumenta el nivel de control implementado.

Poseer un conocimiento incompleto de la ubicación y control de los activos de la organización los puede dejar expuestos a accesos no autorizados.

4.1.2. Ataque a los procesos (AP)

AP01 - Acceso a los recursos de la organización por parte de los empleados o terceros.

Dominio: Administración de personal propio; Cadena de suministros y control de terceras partes ; Gestión de las identidades.

Amenaza: Un tercero no autorizado, o un empleado excediendo su rol en la organización, podría acceder a información sensible dentro de la organización.

Vulnerabilidad: Deficiente administración de cuentas de usuarios y permisos.

Medidas de protección: Implementar políticas tanto para la creación de vías de acceso a los recursos de la organización con el nivel adecuado de privilegios, como también para su anulación llegado el momento en que no son necesarias.

Impacto Alto: El impacto queda acotado a los privilegios de la cuenta que tiene la potencialidad de ser comprometida. El caso de mayor impacto es el acceso con intención hostil.

[4] *Fuente: https://attack.mitre.org/techniques/T1195/*

Riesgo Medio: Implementar políticas muy estrictas respecto al alta y baja de vías de acceso, así como también el ajuste riguroso de sus privilegios, puede resultar en la práctica una dificultad para la disponibilidad de dichos recursos. El nivel de seguridad debe incrementarse rápidamente en la medida en que la probabilidad de la existencia de empleados o exempleados infieles deje de ser despreciable.

El acceso a los recursos puede generar varios conflictos en la organización. En estas, se suele conceder acceso elevado a personal para administrar redes, accesos, etc. y, por ejemplo, al momento de terminar de trabajar en la planta, todo ese conocimiento puede ser buscado por un atacante para realizar actividades en contra de la empresa. Además, podríamos hablar del empleado infiel, quien podría brindar información estando dentro de la misma o bien, un malware podría aprovecharse de los débiles o inadecuados controles de permisos a los recursos y, con el usuario comprometido, también podría obtener información confidencial[5].

AP02 - Gestión de los activos: inventario, configuración y comportamiento de los activos.

Dominio: Gestión de activos.

Amenaza: Pérdida de la disponibilidad, integridad y confidencialidad de la información.

Vulnerabilidad: Desconocimiento de un activo existente, su configuración y comportamiento previsto.

Medidas de protección: Documentación de activos.

Impacto Alto: La falta de control sobre los activos no tiene una cota de daño estimable, pudiendo llegarse a pérdidas económicas o de tiempo muy altas.

Riesgo Bajo: En general, es relativamente sencillo implementar mínimas medidas de control que ofrecen una protección razonable, y el riesgo se reduce rápidamente conforme aumenta el nivel de control implementado.

El conocimiento de los activos es fundamental para asegurar la infraestructura del SCI de una organización ya que los riesgos asociados a vulnerabilidades de los activos son inherentes a cada activo en particular. Algunos riesgos que surgen son la pérdida de disponibilidad, integridad y confidencialidad de información, y que reflejan potenciales impactos adversos en las operaciones de la organización. Esto se debe a que, al no conocer un activo en detalle, además de perjudicar a los procesos en los que éste tenga participación (ya que si no se sabe mucho acerca de él, no puede

[5] *Ver tabla MITRE columna "Initial Access":* https://attack.mitre.org/tactics/TA0001/

ser monitoreado con eficacia, por ejemplo), puede derivar en algún tipo de amenaza que ponga en peligro la integridad del sistema de la organización.

De todos los activos presentes en una organización se deben conocer sus características fundamentales, esto forma parte del inventario en el cual todos los activos deben estar debidamente registrados. Este inventario se traduce en conocimiento por parte del personal que administra el sistema acerca de qué función cumple cada activo, su configuración, quiénes son los autorizados a tener acceso a ellos, tarea que desempeñan, resultados esperados, entre otras características, para que en caso de una falla en el sistema, ya sea tráfico anómalo de red, perdida de datos o cualquier otra inconsistencia, ésta pueda ser detectada y así conocer de qué proceso y activo proviene, permitiendo tomar las acciones correspondientes para su corrección.

La documentación de una organización tiene una gran relevancia en el ámbito de la gestión, representan los conocimientos adquiridos con el tiempo que, si no se preservan adecuadamente, pueden perderse. La estandarización de los procesos sirve para que todo proceso se desarrolle de manera disciplinada y sistemática, asegurando su correcto funcionamiento y un flujo adecuado de la información. Por otra parte, los planes de seguridad y privacidad describen la aplicación prevista de cada control seleccionado en el contexto del sistema, con un nivel de detalle suficiente para implementar correctamente el control y evaluar posteriormente su eficacia. La documentación de control describe cómo se implementan los controles del sistema y los planes con respecto a la funcionalidad del mismo[6].

AP03 - Definición de procesos asociados a la visualización y análisis de flujos de datos, que ayuden a los analistas en seguridad a detectar eventos o incidentes del dispositivo e infraestructura.

Dominio: Gestión de las operaciones; Política y Marco Normativo.

Amenaza: No detección de flujos de datos anómalos.

Vulnerabilidad: Capacidades deficientes de análisis y visualización de datos para una correcta monitorización de los procesos en la organización.

Medidas de protección: Implementación o mejoras de la vulnerabilidad mencionada para la detección inmediata de cualquier falla o comportamiento anómalo en el sistema.

[6] *Fuente: NIST SP 800-37, página 54: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf*

Impacto Medio: En general el tiempo que se tarda en detectar una situación anómala guarda una relación directa con el impacto que la misma puede producir.

Riesgo Medio: Implementar medidas de monitoreo permiten reducir rápidamente las pérdidas ante anomalías a un costo razonable. El mayor riesgo se halla en una tendencia a descuidar este tipo de medidas.

La visualización de datos y resultados que arrojan los procesos llevados a cabo por los activos permiten la monitorización de toda la actividad del sistema. Además de que estas capacidades estén implementadas, el personal que administra los datos debe tener una forma rápida y eficaz para poder realizar su tarea y que cualquier flujo de datos irregular pueda detectarse con rapidez permitiendo examinar a qué se debe el mismo.

AP04 - Personal con roles específicos en Ciberseguridad.

Dominio: Administración de personal propio.

Amenaza: Aprovechamiento de la falta de inversión en ciberseguridad.

Vulnerabilidad: Inexistencia de personal y roles específicos en Ciberseguridad.

Medidas de protección: Contar con el personal capacitado para realizar estas tareas.

Impacto Muy Alto: El impacto de la falta de un análisis adecuado de riesgos no tiene cota teórica.

Riesgo Medio: Dado un análisis de riesgos adecuado, para un nivel de seguridad medio o superior, es recomendable contar con personal especializado que pueda garantizar la sostenibilidad del nivel de seguridad requerido.

Con el aumento de los ciberataques, es prioritario contar con personal que tenga conocimiento en ciberseguridad para hacer frente a los ataques a los que se exponen a diario. Este personal es el encargado de minimizar el nivel de riesgo al que está expuesta la información ante amenazas, y en caso de no poder prevenirlas, son quienes están capacitados para poder recuperar el control de la situación en el menor tiempo minimizando el impacto.

AP05 - Respuesta ante incidentes y simulaciones de ataque.

Dominio: Respuesta a incidentes y Gestión de amenazas y vulnerabilidades; Política y Marco Normativo.

Amenaza: Respuesta inadecuada frente a un incidente.

Vulnerabilidad: Procesos inexistentes o deficientes de respuesta ante incidentes.

Medidas de protección: Es importante contar con revisiones periódicas de simulaciones de ataque, como así también elaborar métodos, procesos y mecanismos para dar respuesta ante un evento indeseado en la organización.

Impacto Muy Alto: El impacto de la falta o deficiencia de procesos o mecanismos de respuesta ante incidentes no tiene cota teórica.

Riesgo Alto: El diseño, prueba y actualización continua de procesos o mecanismos de respuesta ante incidentes comunes es algo que habitualmente se subestima hasta tanto se produce un incidente. La simulación de incidentes en general, y ataques en particular, es una herramienta muy efectiva para mantener vigentes los procesos y mecanismos de respuesta ante incidentes.

AP06 - Auditorías en Seguridad Informática en la organización.

Dominio: Gestión de las operaciones; Política y Marco Normativo.

Amenaza: Explotación de fallas en la seguridad.

Vulnerabilidad: Auditorías en seguridad informática inexistentes o deficientes.

Medidas de protección: Implementación de auditorías y monitoreo de eventos de seguridad para evaluar el estado del nivel de seguridad de un ecosistema ante todo tipo de problemas y realizar cualquier análisis forense necesario.

Impacto Muy Alto: El impacto de la falta o deficiencia de auditorías en seguridad informática no tiene cota teórica.

Riesgo Alto: La implementación y actualización de políticas de auditoría de seguridad informática es algo que habitualmente se subestima hasta tanto se produce una contingencia.

La seguridad de un SCI debe incorporar mecanismos para monitorear, registrar y auditar actividades que ocurren en el sistema y las redes. Estos mecanismos son importantes para comprender el estado actual del sistema, validar que el mismo está funcionando según lo previsto y que no haya violaciones a las políticas o incidentes cibernéticos obstaculizando el correcto funcionamiento de los procesos; además son importantes para caracterizar el estado normal del SCI y puede proporcionar indicaciones de sistemas comprometidos cuando algo falla[7].

[7] *Fuente: NIST SP 800-82, páginas 5-25: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.*

AP07 - Planes de resguardo de la información.

Dominio: Gestión de las operaciones; Política y Marco Normativo.

Amenaza: Pérdida de información importante para los procesos y la organización en sí.

Vulnerabilidad: Inexistente o deficiente plan de resguardo de la información.

Medidas de protección: Implementación de planes de resguardo que permitan recuperar información en caso de una pérdida y políticas que aseguren un buen uso de las mismas, que se mantengan seguras, con restricción de acceso a ellas para personal autorizado, etc.

Impacto Muy Alto: El impacto de la falta o deficiencia de planes de resguardo de información no tiene cota teórica.

Riesgo Alto: Si bien existe, en general, conciencia sobre la importancia de las copias de respaldo, los mecanismos suelen ser deficientes o incompletos, resultando en copias de seguridad ineficaces al producirse una contingencia. En particular, es común que el acceso a la copia de seguridad sea equivalente al acceso a la información, por lo que un ataque efectivo puede comprometer tanto la información como su copia de seguridad.

Una copia de seguridad o resguardo, también llamada *back-up*, hace referencia a la copia de todo tipo de datos de un sistema de modo tal que puede utilizarse para restaurar la información original en caso de sufrir una pérdida de datos por cualquier tipo de ataque. Estos ataques abarcan desde un ransomware hasta un desastre natural que afecte a equipos con información indispensable para el funcionamiento del sistema. Disponer de estas copias de seguridad es imprescindible para evitar el vacío de información, así como el costo y tiempo de reconstrucción de datos[8].

Cuando se implementa una copia de seguridad, hay varios factores que se deben tener en cuenta para su gestión y buen uso de las mismas. Uno de los puntos más importantes para que estas sean eficientes en un escenario de ataque a la integridad del sistema, es que esta copia de seguridad esté actualizada. Es posible que a una pyme le baste con una copia de seguridad diaria al no tener la misma actividad administrativa y cuyos datos tampoco tienen la misma importancia e impacto que una empresa potabilizadora de agua, por ejemplo. Es decir que la periodicidad de su actualización depende de la magnitud de la problemática que está en juego. Además, no solo es necesario que la copia de seguridad se mantenga actualizada, sino que la información debe ser

[8] *Fuente: https://www.deycosat.com/la-importancia-de-las-copias-de-seguridad-en-las-empresas/*

resguardada de forma segura y su recuperación debe ser rápida, para no impactar sobre la disponibilidad de la planta.

AP08 - Política de claves en sistemas y/o dispositivos.

Dominio: Control de acceso y gestión de Identidades; Política y Marco Normativo.

Amenaza: Accesos no autorizados a los activos de la organización.

Vulnerabilidad: Política inexistente o deficiente de claves de acceso que provoca que las claves utilizadas sean predecibles, por defecto o ya hayan sido vulneradas.

Medidas de protección: Revisar el proceso de generación de claves automático, cambio periódico, robustez de claves y confidencialidad en la comunicación de las mismas.

Impacto Alto: El impacto de un acceso no autorizado está acotado por los privilegios de la cuenta comprometida. Es natural proteger con más fuerza las cuentas con mayores privilegios.

Riesgo Medio: La implementación de políticas de claves de acceso deben tener en cuenta la disponibilidad de los recursos. La utilización de claves demasiado aleatorias o la imposición de cambio en períodos cortos puede tener un impacto negativo en la disponibilidad y por lo tanto también en la seguridad, generando el efecto contrario al buscado. Es de vital importancia ajustar adecuadamente la fortaleza de las políticas de establecimiento y cambio de claves de acceso para reducir este riesgo.

Mantener una adecuada política de seguridad de gestión de contraseñas es un punto crítico para resguardar la seguridad y privacidad. Si, por ejemplo, las claves generadas son como mínimo de 12 caracteres de longitud, se tardarían años en probar todas las combinaciones hasta dar con la clave. Justamente, los ataques de fuerza bruta utilizan el método de prueba y error para adivinar información de inicio de sesión y claves de cifrado o encontrar una página web oculta. Los ciberdelincuentes prueban todas las combinaciones posibles con la esperanza de adivinar la combinación correcta[9]. Para mitigar el ataque de fuerza bruta es necesario implementar bloqueos de intentos repetitivos sin éxito u otras técnicas que permitan identificar que se está tratando de realizar un acceso automático (o de tipo robot).

Este proceso de ingreso por clave de acceso puede ser robustecido utilizando múltiples factores de autenticación.

[9] Fuente: https://latam.kaspersky.com/resource-center/definitions/brute-force-attack

4.1.3. Ataque a los protocolos de comunicación (APC)

APC01 - Diseño de redes.

Dominio: Intercambio de información, comunicaciones.

Amenaza: Aprovechamiento de redes no correctamente segmentadas.

Vulnerabilidad: Datos concentrados en una red física compacta donde, al acceder a un dispositivo, se posee visibilidad de los demás dispositivos de la red.

Medidas de protección: Implementación de segmentación de las redes que contengan la información más importante del sistema, garantizando el acceso únicamente a quienes tengan permisos y teniendo en cuenta el impacto sobre la disponibilidad.

Impacto Alto: Una vez que un usuario, autorizado o no, tenga acceso a una red, la protección de los equipos conectados a ella es mucho más baja que si no se tuviera acceso. Conectarse a una red implica pasar por un mecanismo de seguridad. Es decir, una vez que se accedió a la red, el impacto de una conexión hostil es mucho mayor sobre los equipos conectados a esa red. Si en vez de tener una única red, ésta estuviera segmentada en varias, los demás segmentos de red estarían aislados de la conexión hostil que pudiera provocarse en algún segmento.

Riesgo Alto: El correcto diseño de la arquitectura y topología de una red requiere conocimiento experto que muchas veces no está disponible, por lo que su diseño y posterior ejecución no alcanza los estándares mínimos deseables.

Con esto, se refiere a la partición de la red en redes más pequeñas. La segmentación y segregación de una red son dos de los conceptos arquitectónicos más efectivos que se pueden implementar para proteger el sistema de control industrial, y permite a los administradores de red aplicar políticas detalladas para el control de flujo de tráfico entre las distintas subredes. El objetivo de la segmentación de redes es minimizar el acceso a información crítica para aquellos sistemas y personas que no lo necesitan. La seguridad debe estar siempre dada desde el diseño para lograr una mayor efectividad[10].

[10] *Fuente: NIST SP 800-82, páginas 5-2.*

APC02 - Gestión de redes.

Dominio: Gestión de las operaciones.

Amenaza: Acceso no autorizado a la red de la planta. Manipulación de tráfico de red, recolección de datos confidenciales.

Vulnerabilidad: Deficiente o inexistente configuración de seguridad de las redes.

Medidas de protección: Configuración en base a estándares recomendados de los dispositivos, usar segmentación de redes de acuerdo a mejores prácticas (o aisladas si fuera necesario) y canales cifrados cuando fuere necesario.

Impacto Alto: La conexión desde la red interna permite traspasar la seguridad del perímetro. El impacto de una conexión hostil desde la red interna depende fuertemente de la robustez de la configuración de seguridad de cada equipo de la red por separado.

Riesgo Alto: En general, la configuración de seguridad de los equipos de la red interna suele tener baja robustez, por lo que la seguridad se suele concentrar en el perímetro.

Se abarcan varios aspectos referidos a la configuración de redes. Uno de ellos es que, a pesar de que éstas no se encuentren aisladas, las redes deben ser seguras evitando que un atacante se posicione entre dos dispositivos, capturando el tráfico de datos y pudiendo obtener detalles de la red, identificadores de usuarios, direcciones IP, características de configuraciones, etc. También estos pueden manipular tanto datos transmitidos como colocar en la red datos que no deberían estar allí. De la misma forma, podrían lograr acceso a la configuración de equipos y aprovechar puertos abiertos para persistir de forma maliciosa en la red; esto se puede llevar a cabo a través del uso de librerías o aprovechando la imagen del sistema de parches[11]. Además, se puede evitar la intercepción de información sensible por parte de agentes maliciosos utilizando una conexión cifrada.

APC03 - Acceso remoto a los dispositivos de la organización.

Dominio: Intercambio de información, comunicaciones; Gestión de las operaciones; Control de Acceso y Gestión de Identidades.

Amenaza: Aprovechamiento de escasos controles o exposición de los recursos hacia Internet para su acceso.

[11] *Ver tabla MITRE columnas "Collection y Command and Control":* https://attack.mitre.org/matrices/ics/.

Vulnerabilidad: Políticas inexistentes o deficientes con respecto al control de accesos remotos y configuración de las redes.

Medidas de protección: Revisar periódicamente las políticas de accesos remotos respecto de cómo se da acceso, configuración de claves, monitorización de flujo y usuarios que participan o están dentro, etc.

Impacto Muy Alto: El impacto de la exposición hacia la Internet de recursos no preparados para tal fin no tiene cota teórica.

Riesgo Medio: En muchas ocasiones es relativamente simple y económico establecer una protección en el perímetro para evitar la exposición de recursos internos.

Se hace referencia a que los atacantes pueden aprovechar los servicios de acceso remoto externos para acceder inicialmente y/o persistir dentro de una red. Servicios remotos como las VPN, por ejemplo, permiten a los usuarios conectarse a los recursos de red de una empresa desde ubicaciones externas. Para implementarlos, los usuarios autorizados tienen credenciales de autenticación. Esta condición suele ser un requisito fundamental para el manejo de estos accesos, y de no ser implementada de la manera correcta puede facilitar el ingreso de un atacante a una red[12]. Otra medida a implementar es que solamente los recursos que lo requieran deberían estar expuestos a Internet para minimizar la superficie de ataque.

APC04 - Detección de tráfico de red anómalo.

Dominio: Intercambio de información, comunicaciones; Gestión de las operaciones.

Amenaza: Ataques al sistema no detectados en tiempo y forma.

Vulnerabilidad: Falta de capacidades de monitorización y alertas para detectar tráfico de red anómalo en tiempo real.

Medidas de protección: Monitorización adecuada de los protocolos de las redes informáticas y flujos habituales de tráfico, tanto en volumen como dirección, para así poder detectar con mayor facilidad la aparición de algún cambio repentino que puede derivar en una intrusión.

Impacto Alto: La falta o deficiencia de monitoreo y alertas permite que una intrusión o una anomalía pase desapercibida, aumentando notoriamente el posible impacto del daño provocado.

Riesgo Medio: En muchas ocasiones es económico implementar un sistema de monitorización de tráfico de red, y anomalías en protocolos de red.

[12] *Fuente: https://attack.mitre.org/techniques/T1133/*

El conocimiento de la ubicación de un activo y la línea base de su comportamiento permiten la detección de comportamientos anómalos que pueden ser el resultado de una vulnerabilidad explotada con éxito, si se implementa una supervisión de la red adecuada. La capacidad de detectar de manera confiable cambios en el comportamiento de los activos y conocer los atributos de estos es clave para responder a posibles incidentes de ciberseguridad[13].

APC05 - Protocolos de cifrado de las comunicaciones.

Dominio: Intercambio de información, comunicaciones.

Amenaza: Interceptación y visualización de la información que circula dentro de la organización por parte de un usuario no autorizado.

Vulnerabilidad: Protocolos de cifrado inexistentes o deficientes.

Medidas de protección: Idear políticas e implementar mecanismos para estos protocolos de cifrado teniendo en cuenta aspectos tales como la facilidad de violar el cifrado, uso de claves, etc.

Impacto Alto: Un cifrado obsoleto o mal implementado puede ser vulnerado con facilidad, luego de lo cual la confidencialidad de la información queda comprometida.

Riesgo Medio: Los ataques por reducción de nivel de seguridad de los protocolos son en general difíciles de implementar.

La capacidad de cifrado de un dispositivo de red puede ser comprometida. Este cifrado se puede utilizar para proteger el tráfico de red transmitido para mantener su confidencialidad (protección contra divulgación no autorizada) e integridad (protección contra cambios no autorizados). Los atacantes también pueden poner en peligro y manipular los dispositivos que realizan el cifrado del tráfico de red, lo cual plantea un mayor riesgo de divulgación no autorizada y puede ayudar a facilitar la manipulación de datos, el acceso a credenciales o los esfuerzos de recopilación[14]. No obstante, es crucial asegurarse de que el cifrado interfiera en la menor medida posible con el funcionamiento de la red ya que, por ejemplo, un aumento de la latencia podría ocasionar problemas en la disponibilidad o incluso integridad del sistema.

[13] *Fuente: NIST SP 800-23, página 12: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-23.pdf*

[14] *Fuente: https://attack.mitre.org/techniques/T1600/*

4.1.4. Ataque al sistema operativo (ASO)

ASO01 - Estado de actualización del software (o nivel de obsolescencia).

Dominio: Gestión de Activos y cambios.

Amenaza: Aprovechamiento de brechas de seguridad conocidas en software desactualizado u obsoleto.

Vulnerabilidad: Software desactualizado u obsoleto.

Medidas de protección: Implementar un proceso para la actualización periódica de software y firmware de los equipos de la organización, de modo que los cambios sean planificados, programados y probados antes de ser desplegados.

Impacto Alto: Cuando las vulnerabilidades encontradas en los sistemas se hacen públicas, también se publican los vectores de ataque, por lo que un sistema no actualizado con el parche adecuado queda sujeto al impacto de la explotación de la brecha de seguridad.

Riesgo Medio: En muchas ocasiones es relativamente simple implementar medidas de actualización periódica de Software. Sin embargo, en infraestructuras críticas se suele evitar la actualización, perjudicando severamente el nivel de seguridad de las mismas.

Actualizar el software del sistema en una organización es indispensable y no contar con ello puede conllevar varios riesgos que pueden poner en peligro la integridad del sistema. Las versiones obsoletas pueden convertirse en grietas que permiten a atacantes una facilidad para llevar a cabo su ingreso al sistema para realizar lo que deseen. Estas actualizaciones de software, que incluyen parches de seguridad, se aplican basándose en políticas y procedimientos de seguridad a menudo automatizados con herramientas basadas en servidores. No obstante, es fundamental que todo cambio sea planificado, programado y probado antes de ser implementado en los sistemas productivos de la organización.

En la SCI, una solución de compromiso puede lograrse proponiendo el despliegue de todas las actualizaciones durante los períodos de parada programada de planta por mantenimiento, con un minucioso control posterior del correcto funcionamiento de dispositivos y variables del sistema, y la posibilidad de recuperación al valor anterior, en caso de detectarse fallos en la operación. Se recomienda armar un **plan de actualización de software** continuo basado en migraciones y pruebas sobre simuladores cuando es posible, o con equipo auxiliar cuando no lo es.

ASO02 - Estado de software EDR (Endpoint Detection and Response) de los dispositivos.

Dominio: Gestión de Activos y cambios.

Amenaza: Infección de dispositivos con algún tipo de malware.

Vulnerabilidad: Implementación de EDR inexistentes o desactualizados.

Medidas de protección: Contar con software EDR actualizado y con control y gestión centralizado de dispositivos.

Impacto Alto: Un ataque de malware puede llegar a comprometer todos los datos de uno o más equipos y, ante la falta de un sistema de respaldo efectivo, puede generar un daño muy grande.

Riesgo Medio: Es relativamente sencilla la implementación de una solución EDR, siendo hoy una herramienta necesaria que complementa al antivirus para contar con una protección más completa en los endpoints.

EDR es una herramienta de software que proporciona monitorización y análisis continuo de la red y sus endpoints, es decir, los dispositivos conectados a ella. Cuenta con más herramientas que las de un antivirus tradicional en cuanto al análisis de la red y de los dispositivos, utilizando inteligencia artificial para la detección y bloqueos avanzados para la respuesta[15].

Un dispositivo que no cuente con software EDR actualizado, se encuentra más propenso a ser infectado por cualquier tipo de malware, desde un adware hasta un ransomware. Las soluciones para empresas, además, permiten una gestión integral y visualización de amenazas y estado de los dispositivos de toda una organización. No contar con este tipo de soluciones, podría dejar a toda una organización expuesta frente a diversos tipos de ataques.

4.1.5. Ataque a las aplicaciones s/sistema operativo (AAS)

AAS01 - Aplicaciones web de la organización.

Dominio: Gestión del desarrollo de software; Intercambio de información, comunicaciones.

Amenaza: Robo, daño o pérdida de la información a través de un ataque web.

Vulnerabilidad: Fallas en las aplicaciones web, tanto de diseño como por la carencia o inexistencia de seguridad de los datos de sus usuarios.

Medidas de protección: Implementar parches que solucionen las fallas de las aplicaciones web y conseguir un mayor nivel de seguridad de almacenamiento y tratamiento de la información.

[15]Fuente: https://latam.kaspersky.com/resource-center/preemptive-safety/endpoint-detection-and-response

Las aplicaciones web pueden protegerse también por fuera de la propia aplicación, tomando medidas de seguridad por capas, protegiendo perímetros por fuera de la misma como ser la utilización de WAF.

Impacto Muy Alto: Un ataque sobre un sistema Web permite generar daños a causa de los muy elevados privilegios de los procesos del servidor Web respecto al acceso a los datos.

Riesgo Crítico: Actualmente el desarrollo de aplicaciones Web suele ser bastante inmaduro respecto de la seguridad. La seguridad todavía debe ser incorporada desde afuera a las aplicaciones, cuando ya debería estar incorporada en su diseño.

Al igual que cualquier tecnología nueva, la gran mayoría de aplicaciones web vienen acompañadas de una variedad de vulnerabilidades de seguridad que no suelen identificarse a la hora del desarrollo. Por lo tanto, deben estudiarse las formas y posibilidades de explotación para poder implementar los parches correspondientes.

La seguridad en las aplicaciones web es un tema de interés que implica tanto a las organizaciones que les pertenecen como a los usuarios que hacen uso de las mismas. Muchas de ellas implementan estas aplicaciones para expandir e incrementar sus ganancias con el comercio a través de Internet. De acuerdo a la organización OWASP[16], según su reporte de vulnerabilidades clásicas en el 2021, estos son los posibles riesgos presentes en aplicaciones web a considerar:

- *Broken Access Control*: este se refiere a la mala implementación y configuración de las restricciones sobre las funciones que los usuarios autenticados pueden operar. Los atacantes pueden aprovechar estas fallas para realizar operaciones tales como acceder a cuentas de otros usuarios, visualizar archivos confidenciales, modificar datos de otros usuarios, cambiar derechos de acceso, etc.
- *Cryptographic Failures*: muchas aplicaciones web no encriptan adecuadamente los datos confidenciales para protegerlos. Por ende, los atacantes pueden robar o modificar esos datos para cometer fraude mediante robo de identidad, tarjetas de crédito, etc.
- I*njection*: la inyección de código es la explotación de un error de un sistema causado por el procesamiento de datos no válidos. El atacante usa la inyección para introducir código en un programa informático vulnerable y cambiar el curso de ejecución. El resultado de una

[16] *Vínculo al sitio del reporte de OWASP: https://owasp.org/Top10/es/A00_2021_Introduction/*

inyección de código exitosa puede ser caótico, por ejemplo, permitir a gusanos propagarse en uno o varios sistemas.

- *Insecure Design*: el diseño inseguro es una categoría amplia que representa diferentes debilidades, expresadas como "diseño de control faltante o ineficaz". Un diseño seguro aún puede tener defectos de implementación que conduzcan a vulnerabilidades que pueden explotarse. Un diseño inseguro no se puede arreglar con una implementación perfecta ya que, por definición, los controles de seguridad necesarios nunca se crearon para defenderse de ataques específicos.
- *Security Misconfiguration*: este suele ser el resultado de configuraciones predeterminadas inseguras o incompletas, almacenamiento abierto en la nube, mensajes de error que contengan información confidencial, entre otros. Éste es un problema muy común en aplicaciones web.
- *Vulnerable and Outdated Components*: establece algunas causas para ser vulnerable. La primera es software no compatible o no actualizado. La segunda, tiene que ver con la ausencia de búsquedas de vulnerabilidades con regularidad y de informes acerca de la seguridad relacionada con los componentes que se utilizan. En tercer lugar, la falta de testeo de compatibilidad de actualizaciones y parches en bibliotecas por parte de los desarrolladores de software. La cuarta causa tiene que ver con el no aseguramiento de las configuraciones de los componentes.
- *Identification and Authentication Failures*: se refiere a la confirmación de la identidad, autenticación y sesión del usuario. La gestión es fundamental para protegerse contra los ataques relacionados a la autenticación.
- *Software and Data Integrity Failures*: las fallas en la integridad del software y los datos se relacionan con el código y la infraestructura que no protegen contra las violaciones a la integridad. Muchas aplicaciones ahora incluyen la función de actualización automática, donde las actualizaciones se descargan sin una verificación de integridad suficiente y aplicado a la aplicación de confianza anterior.
- *Security Logging and Monitoring Failures*: esta categoría es para ayudar a detectar y responder a las infracciones activas. Sin registro y monitoreo, las infracciones no se pueden detectar. Un registro insuficiente, la detección, el seguimiento y la respuesta activa se producen en cualquier momento.

- *Server-Side Request Forgery*: las fallas de SSRF ocurren cuando una aplicación web está obteniendo un recurso remoto sin validar la URL proporcionada por el usuario. Permite que un atacante coaccione a la aplicación para que envíe una solicitud diseñada a un destino inesperado, incluso cuando está protegido por un firewall, VPN u otro tipo de lista de control de acceso a la red (ACL).

4.1.6. Ataque a las personas (APP)

APP01 - Identidad Digital.

Dominio: Control de acceso y gestión de Identidades; Plan de concientización y capacitación al personal.

Amenaza: Un atacante que obtenga, mediante técnicas de ingeniería social, información, acceso o privilegios en sistemas de información que les permitan realizar actos que perjudiquen la integridad de la organización.

Vulnerabilidad: Desconocimiento por parte del personal acerca de estas técnicas, sus variantes y como se llevan a cabo.

Medidas de protección: Capacitación con una visión de todas las formas en las que se implementa la ingeniería social para que el personal tenga el mayor recaudo posible en estos aspectos.

Impacto Alto: El daño que puede provocarse mediante una suplantación de identidad aumenta con el nivel de privilegios que posea la persona engañada.

Riesgo Medio: En general las personas que tienen más privilegios suelen estar más preparadas para detectar suplantaciones de identidad.

Se basa en el concepto de ingeniería social en el sentido de práctica para obtener información confidencial a través de la manipulación de usuarios legítimos. Esta técnica es usada por personas con el fin de obtener información, acceso o privilegios en sistemas de información que les permitan realizar actos que perjudiquen la integridad de la organización comprometida. Un tipo de ingeniería social y una de las más usadas es la suplantación de identidad, la cual es una actividad malintencionada que consiste en hacerse pasar por otra persona u organismo cometiendo algún tipo de fraude. Esta suplantación implica abusos informáticos cometidos por delincuentes para estafar, obtener información personal, contraseñas, etc. de forma ilegal.

APP02 - Capacitación del personal de la organización sobre el uso responsable de las nuevas tecnologías.

Dominio: Plan de concientización y capacitación del personal.

Amenaza: Aprovechamiento del desconocimiento del personal sobre uso responsable de los activos digitales.

Vulnerabilidad: Débil o inexistente plan de capacitación del personal de la organización.

Medidas de protección: Se requiere entrenar al personal de acuerdo al área en la que se desenvuelve para poder desempeñar su trabajo de forma correcta y segura, esto implica conocer los detalles de manejo del sistema con el que está operando a diario.

Impacto Medio: El daño que puede provocar el desconocimiento de los protocolos de seguridad o de uso de los activos digitales está acotado por los privilegios de los usuarios.

Riesgo Medio: Con el paso del tiempo cada vez hay más conciencia sobre la necesidad de capacitarse para el correcto uso de los activos digitales, lo que hace que el riesgo se reduzca.

En las organizaciones la capacitación del personal es un aspecto muy importante, al terminar su capacitación y poder convertirse en profesional en constante aprendizaje, el personal puede centrarse en las tareas que debe hacer y ofrecer una mejora continua en su desempeño, aumentando así la seguridad con la que los dispositivos tecnológicos son manejados y aumentando la experiencia que se traduce en agilidad y eficiencia[17].

Siempre la cadena de seguridad se corta por el eslabón más débil, y este usualmente es el usuario. Es importante robustecer sus conocimientos en cuanto al uso responsable, para lograr un ecosistema digital más seguro dentro de la organización.

4.2. Amenazas y Dominios

En la Tabla 1 se presenta, en modo de gráfico, el cruce entre dominios y categorías de amenazas detectadas para poder representar, de una forma más sintética, la amenazas que podrían entrar presentes según los dominios previamente identificados.

[17] *Fuente: https://www.scandepot.com.mx/blog/la-importancia-de-la-capacitacin-de-personal/.*

Amenaza/Dominio	Seguridad Física	Gestión de las operaciones	Gestión de Activos y cambios	Gestión del desarrollo de software	Control de acceso y Gestión de identidades	Intercambio de información, comunicaciones	Respuesta a incidentes y Gestión de amenazas y vulnerabilidades	Plan de concientización y capacitación al personal	Cadena de suministro y gestión de 3ras partes	Administración de personal propio	Políticas y marco normativo
Ataque físico a los equipos (AFE)	X		X						X		
Ataque a los procesos (AP)		X	X		X		X		X	X	X
Ataque a los protocolos de comunicación (APC)		X			X	X					
Ataque al sistema operativo (ASO)			X								
Ataque a las aplicaciones s/sistema operativo (ASS)				X		X					
Ataque a las personas (APP)					X			X			

Tabla 2: Matriz Amenaza / Dominio (Fuente: Elaboración propia)

4.3. Matriz de Riesgos

Como se mencionó anteriormente, desde el punto de vista de la ecuación, podemos decir que un riesgo es un número, el resultado de una multiplicación. El riesgo es el producto entre la probabilidad de ocurrencia y el impacto que genera una amenaza que explota una vulnerabilidad en la organización.

Se lo definió: $R_A = P_A.I_A R_A = P_A.I_A$

Tanto para la probabilidad como para el impacto se definen escalas y valores para cada una de ellas. Donde las probabilidades pueden ser "1 vez al año, 2 veces al mes, etc." Y el impacto puede estar definido como "Bajo, Medio o Alto", como, también, de forma cuantitativa. Una vez definidas estas escalas y valores como resultado se generará una matriz de riesgos.

De esta manera, según el resultado de la matriz, se establecerá el riesgo y las acciones correspondientes a tomar para cada caso. Aquí es donde se observa que los riesgos son particulares para cada organización ya que las probabilidades e impactos tendrán diferentes significados dependiendo de la importancia que ese activo digital afectado tenga en la organización. Esto es lo que denominamos el "apetito de riesgo" o "tolerancia al riesgo" de una organización.

Se diseñó, a fines orientativos, la siguiente matriz de riesgos que es habitual encontrar en organizaciones de infraestructuras críticas industriales.

Tabla 3: Matriz de riesgos (Fuente: Elaboración propia)

Probabilidad *¿Cuál es la probabilidad de que ocurra la vulnerabilidad?*	Impacto ¿Qué tan severo sería el riesgo si ocurriera la vulnerabilidad?			
	Bajo	Medio	Alto	Muy Alto
Muy Alta	Medio	Alto	Muy Alto	Crítico
Alta	Bajo	Medio	Alto	Muy Alto
Media	Bajo	Medio	Medio	Alto
Baja	Bajo	Bajo	Bajo	Medio

Donde:

El resultado del producto, en este ejemplo, nos da 5 valores posibles, que son: Bajo, Medio, Alto, Muy alto y Crítico. Esta segmentación es propia de cada empresa y por lo general encontramos entre 4 y 6 valores. Incluso el primer valor puede ser "Insignificante" en lugar de "Muy Bajo".

Para cada sección (definida en diferente color) podemos tomar acciones Preventivas, Correctivas, Reactivas y Resilientes.

El objetivo es tener a los riesgos contenidos dentro de la zona verde y para ello debemos implementar contramedidas con el fin de mitigar el riesgo existente hasta alcanzar dicha zona.

De acuerdo a esto, se procedió a realizar una matriz de riesgos, a nivel general, sobre los diferentes tipos de procesos detectados en el apartado anterior, dando como resultado la siguiente tabla:

Tabla 4: Matriz de riesgos generalizada (Fuente: Elaboración propia)

PROCESO - ACTIVIDAD	EVALUACIÓN DEL RIESGO		VALORACIÓN DEL RIESGO
	PROBABILIDAD OCURRENCIA	IMPACTO	PRIORIDAD DE TRATAMIENTO DEL RIESGO
AFE01	BAJA	MUY ALTO	MEDIO
AFE02	MEDIA	MEDIO	MEDIO
AFE03	BAJA	ALTO	BAJO
AP01	MEDIA	ALTO	MEDIO
AP02	BAJA	ALTO	BAJO
AP03	MEDIA	MEDIO	MEDIO

AP04	BAJA	MUY ALTO	MEDIO
AP05	MEDIA	MUY ALTO	ALTO
AP06	MEDIA	MUY ALTO	ALTO
AP07	MEDIA	MUY ALTO	ALTO
AP08	MEDIA	ALTO	MEDIO
APC01	ALTA	ALTO	ALTO
APC02	ALTA	ALTO	ALTO
APC03	BAJA	MUY ALTO	MEDIO
APC04	MEDIA	ALTO	MEDIO
APC05	MEDIA	ALTO	MEDIO
ASO01	MEDIA	ALTO	MEDIO
ASO02	MEDIA	ALTO	MEDIO
AAS01	MUY ALTA	MUY ALTO	CRÍTICO
APP01	MEDIA	ALTO	MEDIO
APP02	MEDIA	MEDIO	MEDIO

Para una mejor comprensión de lo aquí expuesto, a continuación, se adjuntan dos matrices modelo pero teniendo en cuenta el análisis para los sistemas SCADA y los PLC presentes en la mayoría de las organizaciones de control industrial:

Tabla 5: Matriz de riesgos PLC (Fuente: Elaboración propia)

ACTIVO PLC	PROCESO - ACTIVIDAD	EVALUACIÓN DEL RIESGO		VALORACIÓN DEL RIESGO
		PROBABILIDAD	GRAVEDAD / IMPACTO	PRIORIDAD DE TRATAMIENTO DEL RIESGO
	AFE01	BAJA	MUY ALTO	MEDIO
	AFE02	MEDIA	MEDIO	MEDIO
	AFE03	MEDIA	ALTO	MEDIO
	AP01	MEDIA	ALTO	MEDIO
	AP02	MEDIA	ALTO	MEDIO
	AP03	ALTA	ALTO	ALTO
	AP04	ALTA	ALTO	ALTO
	AP05	MUY ALTA	MUY ALTO	CRÍTICO
	AP06	MEDIA	ALTO	MEDIO
	AP07	MEDIA	MUY ALTO	ALTO
	AP08	MUY ALTA	MUY ALTO	CRÍTICO
	APC01	ALTA	ALTO	ALTO
	APC02	ALTA	ALTO	ALTO
	APC03	MEDIA	ALTO	MEDIO
	APC04	NO APLICA	NO APLICA	NO APLICA
	APC05	MUY ALTA	MUY ALTO	CRÍTICO
	ASO01	MUY ALTA	MUY ALTO	CRÍTICO
	ASO02	NO APLICA	NO APLICA	NO APLICA
	AAS01	NO APLICA	NO APLICA	NO APLICA
	APP01	MEDIA	ALTO	MEDIO
	APP02	MEDIA	MEDIO	MEDIO

Tabla 6: Matriz de riesgos SCADA (Fuente: Elaboración propia)

ACTIVO SCADA	PROCESO - ACTIVIDAD	EVALUACIÓN DEL RIESGO		VALORACIÓN DEL RIESGO
		PROBABILIDAD	GRAVEDAD / IMPACTO	PRIORIDAD DE TRATAMIENTO DEL RIESGO
	AFE01	BAJA	MUY ALTO	MEDIO
	AFE02	MEDIA	ALTO	MEDIO
	AFE03	NO APLICA	NO APLICA	NO APLICA
	AP01	MEDIA	ALTO	MEDIO

	AP02	NO APLICA	NO APLICA	NO APLICA
	AP03	NO APLICA	NO APLICA	NO APLICA
	AP04	ALTA	ALTO	ALTO
	AP05	ALTA	MUY ALTO	MUY ALTO
	AP06	ALTA	MUY ALTO	MUY ALTO
	AP07	MEDIA	MUY ALTO	ALTO
	AP08	MUY ALTA	MUY ALTO	CRÍTICO
	APC01	MUY ALTA	MUY ALTO	CRÍTICO
	APC02	NO APLICA	NO APLICA	NO APLICA
	APC03	MEDIA	ALTO	MEDIO
	APC04	NO APLICA	NO APLICA	NO APLICA
	APC05	NO APLICA	NO APLICA	NO APLICA
	ASO01	ALTA	MUY ALTO	MUY ALTO
	ASO02	ALTA	MUY ALTO	MUY ALTO
	AAS01	ALTA	MUY ALTO	CRÍTICO
	APP01	MEDIA	ALTO	MEDIO
	APP02	MEDIA	ALTO	MEDIO

4.3.1. Descripción de Riesgos

Un **riesgo trivial** se refiere a un riesgo extremadamente bajo o insignificante. En otras palabras, es un riesgo que tiene una probabilidad muy baja de ocurrencia y, si llegara a ocurrir, su impacto sería mínimo o prácticamente nulo.

Este tipo de riesgo generalmente no requiere una atención o preocupación significativa y no representa una amenaza significativa para la seguridad, la salud o los intereses de las personas/organizaciones involucradas.

Un **riesgo bajo** se refiere a una situación en la que la probabilidad de que ocurra un evento adverso o no deseado es mínima. Esto implica que hay una baja posibilidad de que se materialice un peligro y que, incluso si llegara a suceder, es poco probable que tenga un impacto significativo o perjudicial. Cuando se evalúa un riesgo como bajo, se considera que las medidas de control existentes son efectivas para mitigar o prevenir la ocurrencia del evento negativo. Además, es probable que existan salvaguardias y mecanismos de protección adecuados para reducir cualquier posible impacto a un nivel insignificante o manejable. Sin embargo, es importante monitorear continuamente estos riesgos para asegurarse de que sigan siendo bajos y tomar medidas adicionales si cambian las circunstancias o se identifican nuevas amenazas.

Un **riesgo medio** se refiere a un nivel de riesgo que se sitúa entre un riesgo bajo y un riesgo alto. Indica que existe una probabilidad moderada de que ocurra un evento adverso o no deseado, y que este evento puede tener un impacto de magnitud o gravedad también moderada.

En términos de evaluación de riesgos, un riesgo medio implica que hay una posibilidad razonable de que ocurra un evento negativo, pero no es tan alta como para considerarlo inminente o muy probable. Además, el impacto del evento, aunque no es insignificante, tampoco es extremadamente grave o catastrófico.

Un riesgo medio generalmente requiere una atención y consideración adecuadas, ya que puede tener consecuencias significativas si no se gestionan adecuadamente. Puede ser necesario implementar medidas de mitigación, controles o estrategias de manejo de riesgos para reducir la probabilidad de ocurrencia o limitar el impacto en caso de que ocurra.

Cuando se evalúa un **riesgo como alto**, significa que hay una probabilidad elevada de que se produzca un evento no deseado, lo cual puede tener consecuencias significativas en términos de pérdidas financieras, daños a la propiedad, lesiones a las personas o cualquier otro impacto negativo relevante.

Los riesgos altos, generalmente, requieren una atención y una gestión prioritaria, ya que pueden tener efectos adversos significativos en las personas, organizaciones o comunidades involucradas. Es fundamental implementar medidas de control, estrategias de mitigación y acciones preventivas para reducir la probabilidad de ocurrencia del evento o limitar su impacto en caso de que se produzca.

Un **riesgo crítico** es el nivel más alto de riesgo en la evaluación de riesgos. Representa una amenaza grave y significativa con una alta probabilidad de ocurrencia de un evento adverso o no deseado, y cuyo impacto potencial es de gran magnitud y puede tener consecuencias catastróficas.

Cuando se considera un riesgo como crítico, implica que existe una alta certeza de que se producirá un evento negativo y que este evento puede tener consecuencias extremadamente graves, tanto en términos de pérdidas materiales como en términos de daño a la vida humana, el medio ambiente o la integridad de una organización.

Los riesgos críticos requieren una atención inmediata y una gestión urgente. Es fundamental implementar medidas de mitigación, controles y estrategias de respuesta para reducir la probabilidad de ocurrencia del evento o para minimizar su impacto en caso de que se produzca.

Dada la naturaleza y gravedad de los riesgos críticos, su identificación y gestión adecuadas son esenciales para garantizar la seguridad, la continuidad del negocio y la protección de los intereses de las personas y las organizaciones afectadas.

5. Vulnerabilidades presentes en ICIs

En la Tabla 7 pueden observarse las vulnerabilidades habituales en este tipo de infraestructuras para que se tenga una referencia al respecto de cuáles serían los principales focos de atención.

Tabla 7: Vulnerabilidades (Fuente: Elaboración propia)

Vulnerabilidades de políticas y procedimientos	Mitigante
Política de seguridad inadecuada para el SCI	Las vulnerabilidades a menudo se introducen en SCI debido a políticas inadecuadas o la falta de políticas específicas para la seguridad del sistema de control.
No hay programa formal de capacitación en seguridad y concientización	Un programa documentado de capacitación y concientización formal de seguridad está diseñado para mantener al personal actualizado sobre las políticas y procedimientos de seguridad organizacionales, así como los estándares de seguridad cibernética de la industria y las prácticas recomendadas. Sin capacitación en políticas y procedimientos específicos de SCI, no se puede esperar que el personal mantenga un entorno de SCI seguro.
Arquitectura y diseño de seguridad inadecuados	Históricamente, los ingenieros de control han recibido capacitación mínima en seguridad y hasta hace poco, los proveedores no han incluido características de seguridad en sus productos.
No se desarrollaron procedimientos de seguridad específicos o documentados a partir de la política de seguridad para el SCI	Se deben desarrollar procedimientos de seguridad específicos y los empleados ser capacitados para el SCI. Son las raíces de un programa de seguridad sólido.
Guías de implementación de equipos de SCI ausentes o deficientes	Los lineamientos de implementación del equipamiento deben mantenerse actualizados y fácilmente disponibles. Estos lineamientos son una parte integral de los procedimientos de seguridad en caso de un mal funcionamiento de SCI.
Falta de mecanismos administrativos para la aplicación de seguridad	El personal responsable de hacer cumplir la seguridad debe ser responsable de la administración de políticas y procedimientos de seguridad.
Pocas o ninguna auditoría de seguridad en el SCI	Las auditorías de seguridad independientes deben revisar y examinar los registros y actividades de un sistema para determinar la adecuación de los controles del sistema y garantizar el cumplimiento de las políticas y procedimientos de seguridad del SCI establecidos. Las auditorías también deben usarse para detectar violaciones en los servicios de seguridad del SCI y recomendar cambios, que pueden incluir, hacer que los controles de seguridad existentes sean más robustos y/o agregar nuevos controles de seguridad.

No hay planes de continuidad de las operaciones o de recuperación ante desastres específicos para SCI	Se debe preparar, probar y disponibilizar un plan de recuperación ante desastres (DRP) en caso de una falla importante de hardware o software o destrucción de las instalaciones. La falta de un DRP específico para el SCI podría conducir a tiempos de inactividad extendidos y pérdidas de producción.
Falta de gestión de cambios de configuración específica para SCI	Se debe implementar un proceso para controlar modificaciones al hardware, el firmware, el software y la documentación, para garantizar que un SCI esté protegido contra modificaciones inadecuadas o inapropiadas antes, durante y después de la implementación del sistema. La falta de procedimientos de gestión del cambio de configuración puede conducir a errores de seguridad, exposiciones y riesgos.
Vulnerabilidades de configuración de la plataforma	**Mitigante**
Los parches en el sistema operativo y en software de proveedores no pueden aplicarse hasta significativamente después del descubrimiento de la vulnerabilidad de seguridad	Debido a la complejidad del software SCI y las posibles modificaciones al sistema operativo subyacente, los cambios deben sufrir pruebas de regresión integrales. El tiempo transcurrido para dichas pruebas y la distribución posterior de software actualizado proporciona una larga ventana de vulnerabilidad
Los parches de seguridad del SO y de las aplicaciones no son mantenidos	SO y aplicaciones desactualizadas pueden contener vulnerabilidades recién descubiertas que podrían explotarse. Se deben desarrollar procedimientos documentados sobre cómo se mantendrán los parches de seguridad. El soporte de parches de seguridad puede no estar disponible para SCI que usan SO obsoletos.
Los parches de seguridad del SO y de las aplicaciones se implementan sin pruebas exhaustivas	Los parches del sistema operativo y de la aplicación implementados sin pruebas podrían comprometer el funcionamiento normal del SCI. Se deben desarrollar procedimientos documentados para probar nuevos parches de seguridad.
Se utilizan configuraciones predeterminadas	El uso de configuraciones predeterminadas a menudo conduce a puertos abiertos inseguros e innecesarios y servicios y aplicaciones explotables que se ejecutan en el dispositivo.
Las configuraciones críticas no están almacenadas ni respaldadas	Los procedimientos deben estar disponibles para restaurar la configuración del SCI en caso de cambios de configuración accidentales o iniciados por un adversario para mantener la disponibilidad del sistema y evitar la pérdida de datos. Se deben desarrollar procedimientos documentados para mantener la configuración de los SCI.

Datos sin protección en el dispositivo portátil	Si los datos confidenciales (por ejemplo, contraseñas, números de acceso telefónico) se almacenan en los dispositivos portátiles, como computadoras portátiles y tablets y estos dispositivos se pierden o se roban, la seguridad del sistema podría verse comprometida. Se requieren políticas, procedimientos y mecanismos para la protección.
Falta de política de contraseña adecuada	Se necesitan políticas de contraseña para definir cuándo deben usarse las contraseñas, qué tan fuertes deben ser y cómo deben mantenerse. Sin una política de contraseña, los sistemas pueden no tener controles de contraseña apropiados, lo que hace que el acceso no autorizado a los sistemas sea más probable. Las políticas de contraseña deben desarrollarse como parte de un programa general de seguridad del SCI teniendo en cuenta las capacidades del SCI y su personal para manejar contraseñas más complejas.
No se usa contraseña	Las contraseñas deben implementarse en componentes SCI para evitar el acceso no autorizado. Las vulnerabilidades relacionadas con la contraseña incluyen no tener contraseña para: • Inicio de sesión del sistema (si el sistema tiene cuentas de usuario) • Encendido del sistema (si el sistema no tiene cuentas de usuario) • Protector de pantalla del sistema (si un componente SCI está desatendido con el tiempo) La autenticación de contraseña no debe obstaculizar ni interferir con las acciones de emergencia para los SCI.
Divulgación de contraseña	Las contraseñas deben mantenerse confidenciales para evitar el acceso no autorizado. Ejemplos de divulgaciones de contraseña incluyen: • Publicar contraseñas a simple vista, local a un sistema • Compartir contraseñas de cuentas de usuarios individuales con asociados • Comunicar las contraseñas a los adversarios a través de la ingeniería social • Enviar contraseñas que no están encriptadas a través de comunicaciones sin protección

Adivinación de contraseña	Las contraseñas débiles pueden ser adivinadas por los humanos o algoritmos de computadora fácilmente para obtener acceso no autorizado. Los ejemplos incluyen: • Las contraseñas que son cortas, simples (por ejemplo, todas las letras en minúsculas) o no cumplen con los requisitos de resistencia típicos. La fuerza de la contraseña también depende de la capacidad de SCI específica para manejar contraseñas más complejas. • Contraseñas que se dejan con el valor suministrado por el proveedor. • Contraseñas que no se cambian en un intervalo de tiempo especificado
Controles de acceso inadecuados	Los controles de acceso mal especificados pueden dar a un usuario de SCI demasiados o muy pocos privilegios. Lo siguiente ejemplifica cada caso: • Sistema configurado por defecto proporciona a un operador privilegios administrativos • Sistema configurado incorrectamente impide que un operador tome medidas correctivas en una situación de emergencia Las políticas de control de acceso deben desarrollarse como parte de un programa de seguridad SCI.
Vulnerabilidades de hardware de la plataforma	**Mitigante**
Pruebas inadecuadas de cambios de seguridad	Muchas instalaciones de SCI, especialmente las instalaciones más pequeñas, no tienen instalaciones de prueba, por lo que se deben implementar cambios de seguridad utilizando los sistemas operativos en producción
Protección física inadecuada para sistemas críticos	El acceso al centro de control, los dispositivos de campo, los dispositivos portátiles, los medios y otros componentes SCI deben controlarse. Muchos sitios remotos de campo a menudo no tienen personal y puede no ser factible monitorearlos físicamente.

El personal no autorizado tiene acceso físico al equipo	El acceso físico al equipo SCI debe restringirse solo al personal necesario, teniendo en cuenta los requisitos de seguridad, como el cierre de emergencia o los reinicios. El acceso inadecuado al equipo SCI puede conducir a cualquiera de los siguientes casos: • Robo físico de datos y hardware • Daño físico o destrucción de datos y hardware • Cambios no autorizados en el entorno funcional (por ejemplo, conexiones de datos, uso no autorizado de medios extraíbles, agregar/eliminar recursos) • Desconexión de enlaces de datos físicos • Interceptación indetectable de datos (pulsación de teclas y otros registros de entrada)
Acceso remoto inseguro en componentes SCI	Los módems y otras capacidades de acceso remoto que permiten a los ingenieros y proveedores de control conectarse remotamente a los sistemas, deben ser implementados con controles de seguridad para evitar que las personas no autorizadas obtengan acceso al SCI.
Tarjetas de interfaz de red duales (NIC) para conectar redes	Las máquinas con NIC duales conectadas a diferentes redes podrían permitir el acceso no autorizado y el paso de datos de una red a otra.
Activos indocumentados	Para asegurar adecuadamente un SCI, debe haber una lista precisa de los activos en el sistema. Una representación inexacta del sistema de control y sus componentes podrían dejar un punto de acceso no autorizado o puerta trasera al SCI.
Radiofrecuencia y pulso electromagnético (EMP)	El hardware utilizado para los sistemas de control es vulnerable a la radiofrecuencia y los pulsos electromagnéticos (EMP). El impacto puede variar desde la interrupción temporal del comando y el control hasta el daño permanente a las placas de circuito.

Falta de energía de respaldo	Sin poder de respaldo a los activos críticos, una pérdida general de energía apagará el SCI y podría crear una situación insegura. La pérdida de energía también podría conducir a una configuración predeterminada insegura.
Pérdida del control ambiental	La pérdida del control ambiental podría conducir al sobrecalentamiento de los procesadores. Algunos procesadores se apagarán para auto-protegerse; algunos pueden continuar operando pero en una capacidad mínima, produciendo errores intermitentes; y algunos casos simplemente se derriten si se sobrecalientan.
Falta de redundancia para componentes críticos	La falta de redundancia en los componentes críticos podría generar posibilidades de falla de un solo punto
Vulnerabilidades de software de plataforma	**Mitigante**
Desbordamiento del búfer	El software utilizado para implementar un SCI podría ser vulnerable a los desbordamientos del búfer; los adversarios podrían explotarlos para realizar varios ataques.
Capacidades de seguridad instaladas no están habilitadas de forma predeterminada	Las capacidades de seguridad que se instalaron con el producto son inútiles si no están habilitadas o al menos identificadas como deshabilitadas.
Denegación de servicio (DOS)	El software SCI podría ser vulnerable a los ataques de DOS, lo que resulta en la incapacidad del acceso autorizado a un recurso del sistema o retrasando las operaciones y funciones del sistema.
Mal manejo de condiciones indefinidas, mal definidas o "ilegales"	Algunas implementaciones de SCI son vulnerables a los paquetes que están malformados o contienen valores de campo ilegales o inesperados.
OLE para el control de procesos (OPC) se basa en la llamada de procedimiento remoto (RPC) y el modelo de objetos de componentes distribuidos (DCOM)	Sin parches actualizados, OPC es vulnerable a las vulnerabilidades RPC/DCOM conocidas.

Uso de protocolos industriales inseguros	El protocolo de red distribuido (DNP) 3.0, Modbus, Profibus y otros protocolos son comunes en varias industrias y la información sobre el protocolo está disponible gratuitamente. Estos protocolos a menudo tienen pocas o ninguna capacidad de seguridad incorporadas.
Uso de texto claro	Muchos protocolos de SCI transmiten mensajes en texto claro a través de los medios de transmisión, posibilitando al adversario leer los mensajes.
Servicios innecesarios ejecutándose	Muchas plataformas tienen una amplia variedad de servicios de procesadores y redes definidas para operar con valores predeterminados. Los servicios innecesarios rara vez están deshabilitados y podrían explotarse.
Uso de software patentado que se ha discutido en conferencias y en publicaciones periódicas	Los problemas de software propietario se discuten en las conferencias internacionales de TI, SCI y "sombrero negro" y están disponibles a través de documentos técnicos, publicaciones periódicas y servidores de listados. Además, los manuales de mantenimiento del SCI están disponibles en los proveedores. Esta información puede ayudar a los adversarios a crear ataques exitosos contra SCI.
Autenticación inadecuada y control de acceso para el software de configuración y programación	El acceso no autorizado a la configuración y el software de programación podría proporcionar la capacidad de corromper un dispositivo.
Software de detección/prevención de intrusos no instalado	Los incidentes pueden dar lugar a la pérdida de disponibilidad del sistema; la captura, modificación y eliminación de datos; y ejecución incorrecta de comandos de control. El software IDS/IPS puede detener o prevenir varios tipos de ataques, incluidos los ataques DOS, y también identificar hosts internos atacados, como los infectados con gusanos. El software IDS/IPS debe probarse antes de la implementación para determinar que no comprometa el funcionamiento normal del SCI.
Registros no mantenidos	Sin registros adecuados y precisos, podría ser imposible determinar qué causó que ocurriera un evento de seguridad.
No se detectan incidentes	Cuando se instalan registros y otros sensores de seguridad, pueden no ser

	monitoreados en tiempo real y, por lo tanto, los incidentes de seguridad no pueden detectarse y remediarse rápidamente.
Vulnerabilidades de protección de malware de la plataforma	**Mitigante**
Software de protección de malware no instalado	El software malicioso puede provocar la degradación del rendimiento, la pérdida de disponibilidad del sistema y la captura, modificación o eliminación de datos. Se necesita software de protección de malware, como el software antivirus, para evitar que los sistemas sean infectados por software malicioso.
Software de protección o definiciones de malware no actualizadas	El software y las definiciones de protección de malware anticuadas dejan el sistema abierto a nuevas amenazas de malware.
Software de protección de malware implementado sin pruebas exhaustivas	El software de protección de malware implementado sin pruebas podría afectar el funcionamiento normal del SCI.
Vulnerabilidades de configuración de red	**Mitigante**
Arquitectura de seguridad de red débil	El entorno de infraestructura de red dentro del SCI a menudo se ha desarrollado y modificado en función de los requisitos comerciales y operativos, con poca consideración para los posibles impactos de seguridad de los cambios. Con el tiempo, las brechas de seguridad pueden haberse introducido inadvertidamente en partes particulares de la infraestructura. Sin remediación, estos huecos pueden representar puertas traseras en el SCI.
Controles de flujo de datos no empleados	Se necesitan controles de flujo de datos, como listas de control de acceso (ACL), para restringir qué sistemas pueden acceder directamente a los dispositivos de red. En general, solo los administradores de red designados deberían poder acceder directamente a dichos dispositivos. Los controles de flujo de datos deben garantizar que otros sistemas no puedan acceder directamente a los dispositivos.

Equipamiento con seguridad mal configurada	El uso de configuraciones predeterminadas a menudo conduce a puertos abiertos inseguros e innecesarios y servicios de red explotables que se ejecutan en los hosts. Las reglas de firewall y las ACL configuradas incorrectamente en el enrutador pueden permitir un tráfico innecesario.
Configuraciones del dispositivo de red no almacenadas ni respaldadas	Los procedimientos deben estar disponibles para restaurar la configuración del dispositivo de red en caso de cambios de configuración accidentales o iniciados por adversarios para mantener la disponibilidad del sistema y evitar la pérdida de datos. Se deben desarrollar procedimientos documentados para mantener la configuración del dispositivo de red.
Las contraseñas no están encriptadas en tránsito	Las contraseñas transmitidas en texto transparente a través de los medios de transmisión son susceptibles a ser leídas por los adversarios, quienes podrían utilizarlas para obtener acceso no autorizado a un dispositivo de red. Dicho acceso podría permitir que un adversario interrumpa las operaciones de SCI o monitoree la actividad de la red SCI.
Las contraseñas no se cambian en los dispositivos de red	Las contraseñas deben cambiarse regularmente para que si una es conocida por una parte no autorizada, esta tiene acceso no autorizado al dispositivo de red solo por un corto tiempo. Dicho acceso podría permitir que un adversario interrumpa las operaciones de SCI o monitoree la actividad de la red SCI.
Controles de acceso inadecuados	El acceso no autorizado a dispositivos de red y funciones administrativas podría permitir que un usuario interrumpa las operaciones de SCI o monitoree la actividad de la red SCI.
Vulnerabilidades de hardware de red	**Mitigante**
Protección física inadecuada de los equipos de red	El acceso al equipo de red debe controlarse para evitar daños o destrucción.
Puertos físicos inseguros	Los puertos USB y los puertos PS/2 inseguros podrían permitir una conexión no autorizada de unidades de almacenamiento portátil, registradores de pulsaciones de teclas, etc.

Pérdida del control ambiental	La pérdida del control ambiental podría conducir al sobrecalentamiento de los procesadores. Algunos procesadores se apagarán para auto-protegerse, y otros simplemente se derriten si se sobrecalientan.
El personal no crítico tiene acceso a equipos y conexión de redes	El acceso físico al equipo de red debe restringirse solo al personal necesario. El acceso inadecuado al equipo de red puede conducir a cualquiera de los siguientes casos: • Robo físico de datos y hardware • Daño físico o destrucción de datos y hardware • Cambios no autorizados en el entorno de seguridad (por ejemplo, alterar las ACL para permitir que los ataques ingresen a una red) • Intercepción y manipulación no autorizadas de la actividad de la red • Desconexión de enlaces de datos físicos o conexión de enlaces de datos no autorizados
Falta de redundancia para redes críticas	La falta de redundancia en redes críticas podría proporcionar posibilidades de falla de un solo punto
Vulnerabilidades del perímetro de red	**Mitigante**
Sin perímetro de seguridad definido	Si la red de control no tiene un perímetro de seguridad claramente definido, entonces no es posible asegurarse de que los controles de seguridad necesarios se implementen y configuren correctamente. Esto puede conducir a un acceso no autorizado a sistemas y datos, así como a otros problemas.
Firewalls inexistentes o configurados incorrectamente	La falta de firewalls adecuadamente configurados podría permitir que datos innecesarios pasen entre redes, como el control y las redes corporativas. Esto podría causar varios problemas, permitiendo que los ataques y malware que se propaguen entre redes, hacer que los datos confidenciales sean susceptibles a monitoreo/escucha en la otra red y proporcionando a las personas acceso no

	autorizado a los sistemas.
Redes de control utilizadas para el tráfico no controlado	El tráfico de control y de otro tipo tienen diferentes requisitos, como el determinismo y la confiabilidad, por lo que tener ambos tipos de tráfico en una sola red hace que sea más difícil configurar la red para que cumpla con los requisitos del tráfico de control. Por ejemplo, el tráfico que no es de control podría consumir inadvertidamente recursos que el tráfico de control necesita, causando interrupciones en las funciones de SCI.
Los servicios de la red de control no están dentro de la red de control	Los servicios de TI como el sistema de nombres de dominio (DNS) y/o el protocolo de configuración de host dinámico (DHCP) que son utilizados por redes de control, a menudo se implementan en la red de TI, lo que hace que la red SCI se vuelva dependiente de la red de TI que puede no tener los requisitos de confiabilidad y disponibilidad que necesitan el SCI.
Vulnerabilidades de monitoreo y registro de redes	**Mitigante**
Inadecuados registros (logs) de firewalls y de enrutadores	Sin registros adecuados y precisos, podría ser imposible determinar qué causó que ocurriera un incidente de seguridad.
Sin monitoreo de seguridad en la red SCI	Sin un monitoreo de seguridad regular, los incidentes pueden pasar desapercibidos, lo que provoca daños y/o interrupciones adicionales. También se necesita un monitoreo de seguridad regular para identificar problemas con los controles de seguridad, como configuraciones erróneas y fallos.
Vulnerabilidades de comunicación	**Mitigante**
No se identifican las rutas de control y el monitoreo críticos	Las conexiones falsas y/o desconocidas en el SCI pueden dejar una puerta trasera para ataques.

Estándar, bien documentado sobre los protocolos de comunicación se utilizan en texto plano	Los adversarios que pueden monitorear la actividad de la red SCI pueden usar un analizador de protocolo u otras utilidades para decodificar los datos transferidos por protocolos como Telnet, Protocolo de transferencia de archivos (FTP) y sistema de archivos de red (NFS). El uso de tales protocolos también facilita a los adversarios realizar ataques contra el SCI y manipular la actividad de la red SCI.
La autenticación de usuarios, datos o dispositivos es deficiente o inexistente	Muchos protocolos de SCI no tienen autenticación en ningún nivel. Sin autenticación, existe el potencial de reproducir, modificar o falsificar datos o falsificar dispositivos, como sensores e identidades de usuario.
Falta de comprobación de integridad para las comunicaciones	No hay verificaciones de integridad en la mayoría de los protocolos de control industrial; los adversarios podrían manipular las comunicaciones sin ser detectados. Para garantizar la integridad, el SCI puede usar protocolos de capa inferior (por ejemplo, IPSEC) que ofrecen protección contra la integridad de datos.
Vulnerabilidades de conexión inalámbrica	**Mitigante**
Autenticación inadecuada entre clientes y puntos de acceso	Se necesita una fuerte autenticación mutua entre clientes inalámbricos y puntos de acceso para garantizar que los clientes no se conecten a un punto de acceso falso implementado por un adversario, y también para garantizar que los adversarios no se conecten a ninguna de las redes inalámbricas del SCI.
Protección de datos inadecuada entre clientes y puntos de acceso	Los datos confidenciales entre clientes inalámbricos y puntos de acceso deben protegerse utilizando un cifrado fuerte para garantizar que los adversarios no puedan obtener acceso no autorizado a los datos no cifrados.

6. Incidentes habituales en ICIs

Al igual que en el apartado anterior, en el cual se detallaron las vulnerabilidades habituales en ICIs, es importante hacer una breve mención a los incidentes que podrían suscitarse como consecuencia de una explotación de las vulnerabilidades mencionadas:

Tabla 8: Incidentes de seguridad (Fuente: Elaboración propia)

Incidentes de Seguridad	Descripción
Denegación de acciones de control	La operación de los sistemas de control es interrumpida por retraso o bloqueo del flujo de información, denegando así la disponibilidad de las redes a los operadores de los sistemas de control o causando cuellos de botella en la transferencia de información o denegando servicios de TI (como DNS).
Dispositivos de control reprogramados	Cambios no autorizados realizados en instrucciones programadas en PLC, RTU, DCS o controladores SCADA, umbrales de alarma cambiados o comandos no autorizados emitidos para controlar equipamientos, lo que podría dar lugar a daños a los equipos (si se excede las tolerancias), el cierre prematuro de los procesos (tales como cierre prematuro de las líneas de transmisión), causando un incidente ambiental o incluso deshabilitando el equipo de control.
Información falsa de estado del sistema	Información falsa enviada a los operadores del sistema de control para ocultar los cambios no autorizados o para iniciar acciones inapropiadas por parte de los operadores del sistema
Manipulación de la lógica de control de los sistemas de seguridad	Modificación del software o de las configuraciones del sistema de control, produciendo resultados impredecibles.
Malware en sistemas de control	El software malicioso (por ejemplo, Virus, Worm, Troyano) introducido en el sistema.
Sistemas de seguridad modificados	La operación de los sistemas de seguridad se manipula de tal manera que no funcionan cuando es necesario o realizan acciones de control incorrectas que dañan el SCI
Interrupción del proceso	Se evalúa el impacto que tendría la explotación de una vulnerabilidad en la interrupción del proceso y en la continuidad de la producción.
Potencial de daño físico	Se evalúa el impacto que tendría la explotación de una vulnerabilidad en la seguridad física de las personas, en caso de que se produzca un daño físico a causa de la vulnerabilidad.
Costo económico y de reputación	Pérdidas económicas que podrían implicar una explotación exitosa de la vulnerabilidad. Y la pérdida de confianza por parte de clientes y accionistas
Pérdida de integridad y confidencialidad de los datos	Se evalúa el impacto que tendría la explotación de una vulnerabilidad en la pérdida de integridad y confidencialidad de los datos del sistema.

Seguridad Funcional	Impacto en la seguridad funcional del sistema si la vulnerabilidad es explotada. Algunos ejemplos de seguridad funcional son: la capacidad de un atacante para manipular los sistemas de seguridad, para desactivarlos, o para interferir con sistemas críticos, entre otros.

7. Guía de recomendaciones en ICIs

Una vez identificados los problemas que puedan llegar a coexistir en infraestructuras tan complejas como las de este caso de estudio, es necesario implementar acciones para afrontar todos los riesgos y, de esta manera, intentar reducir su probabilidad de ocurrencia y/o el daño que podrían ocasionar a la organización en el caso de que surjan incidentes relacionados a ellos.

7.1. Recomendaciones generales

A continuación, se presentan ciertas acciones generales posibles para mitigar los riesgos identificados, los cuales serán categorizados según los enfoques mencionados en el apartado *"Clasificación de Medidas de Seguridad"* y los códigos de categorías de ataques mencionados en el apartado *"Guía de Identificación de Riesgos en ICIs"*:

AFE01 - Control de ingreso y egreso a la planta operacional.

- **Precaución**: evitar que personal no autorizado ingrese a la planta.
- **Prevención**: implementar un sistema de identificación y autenticación para el personal que ingresa a la planta.
- **Reacción**: vigilar por presencia de personas no autorizadas en la planta y detenerlas.

AFE02 - Control de ingreso de dispositivos

- **Precaución**: permitir solo el ingreso y egreso de los dispositivos estrictamente autorizados y en posesión del personal con permisos para tal fin.
- **Prevención**: implementar un sistema de escaneo de dispositivos electrónicos y posterior verificación de su correspondiente autorización. Homologar una lista de dispositivos autorizados (lista blanca).
- **Reacción**: implementar identificación automatizada y decomisar todo dispositivo no autorizado que se conecte en cualquier sistema o red.

AFE03 - Control/gestión de ubicación física

- **Precaución**: llevar un registro de todos los activos desde el momento que se adquieren. (inventarios y ciclo de vida de ciber activos)
- **Prevención**: realizar auditorías sorpresivas para detectar posibles desvíos.

- **Reacción**: realizar correcciones sobre el inventario en caso de ser necesario.

AP01 - Acceso a los recursos de la organización por parte de los empleados o terceros.

- **Precaución**: clasificar la información como confidencial, restringida, de uso interno, pública o sensible; contar con una adecuada herramienta de DLP y directivas de acceso a la información, además de un plan de gestión de fuga de información, con responsables del equipo de gestión bien identificados.
- **Prevención**: limitar el acceso a la información confidencial, monitoreando su acceso y cifrado la misma.
- **Reacción**: convocar al Comité de crisis para ejecutar el plan correspondiente.

AP02 - Gestión de los activos: inventario, configuración y comportamiento de los activos

- **Precaución**: llevar un registro de todos los activos desde el momento que se adquieren.
- **Prevención**: implementar buenos mecanismos de actualización de los inventarios, para mantener la información vigente.
- **Reacción**: disparar algún protocolo de comprobación y ajuste rápido del inventario.

AP03 - Definición de procesos asociados a la visualización y análisis de flujos de datos, que ayuden a los analistas en seguridad a detectar eventos o incidentes del dispositivo e infraestructura

- **Precaución**: toda medida de precaución de incidentes:
    - Físicos: medidas de precaución con respecto a inundación, incendios o corte de suministro energético.
    - Lógicos: medidas de precaución con la implementación de IDS, por ejemplo.
- **Prevención**: diseñar alarmas que alerten de manera temprana ante posibles incidentes a partir de la disponibilidad de los datos del monitoreo.
- **Reacción**: disparar un protocolo de respuesta ante incidentes.

AP04 - Personal con roles específicos en Ciberseguridad

- **Precaución**: contar con personal con roles específicos en ciberseguridad dentro de la organización y mantener el "la caza de talentos" de estos roles.
- **Prevención**: capacitar en ciberseguridad a las personas que integran la organización para formar roles en la disciplina.
- **Reacción**: contar con mecanismos de fidelización y de retención de personal (bonos, acciones, etc.).

AP05 - Respuesta ante incidentes y simulaciones de ataque

- **Precaución**: contar con un IDS y un firewall.
- **Prevención**: capacitar al personal de la organización para evitar ataques asociados con el phishing.
- **Reacción**: contar con un equipo de respuesta ante incidentes para poder reaccionar a un ataque real.

AP06 - Auditorías en Seguridad Informática en la organización

- **Precaución**: Implementar un SGSI alineado con las normativas y regulaciones del negocio.
- **Prevención**: ejecutar evaluaciones de seguridad, auditorías y certificaciones con la frecuencia correspondiente, que incrementen el nivel de madurez de seguridad y mejoren la postura de seguridad de la organización.
- **Reacción**: implementar proceso de sanción ante el incumplimiento de las políticas o normativas.

AP07 - Planes de resguardo de la información

- **Precaución**: contar con un sistema de resguardo de información con las características necesarias que permitan asegurar la continuidad del negocio de una forma rápida, minimizando impactos negativos.
- **Prevención**: implementar políticas de resguardo adecuadas de acuerdo con la criticidad de la información y RPO correspondiente, con planes de pruebas de restauración que validen periódicamente la integridad de la información.

- **Reacción**: restaurar el último resguardo íntegro y viable disponible.

AP08 - Política de claves en sistemas y/o dispositivos

- **Precaución**: contar con un sistema de gestión de las contraseñas y políticas adecuadas.
- **Prevención**: capacitar a los empleados en el adecuado uso de las contraseñas, generando conciencia sobre los riesgos de una gestión inadecuada de las mismas.
- **Reacción**: realizar el bloqueo urgente de las cuentas comprometidas y bloquear el acceso a él o a los sistemas involucrados.

APC01 - Diseño de redes

- **Precaución**: contar con un diseño seguro de redes a nivel físico y lógico en base a estándares.
- **Prevención**: monitorear eventos de tráfico de redes, contando con alertas ante correlación de eventos.
- **Reacción**: aislar la subred comprometida para un análisis y evitar propagación del problema a otras redes.

APC02 - Gestión de redes

- **Precaución**: implementar medidas de autorización y autenticación de acceso según estándares, además de separar las redes por zonas
- **Prevención**: contar con monitoreo y alertas ante eventos de intrusión en el acceso a recursos o eventos de tráfico anormal u otras alertas.
- **Reacción**: aislar los recursos comprometidos para un análisis y replanteamiento de las medidas de seguridad a mejorar.

APC03 - Acceso remoto a los dispositivos de la organización

- **Precaución**: implementar un sistema de control de dispositivos y aplicar políticas de seguridad.
- **Prevención**: implementar un sistema de monitoreo en cada dispositivo que permita alertas en tiempo real sobre eventos sospechosos.

- **Reacción**: aislar dispositivos involucrados en la red y realizar una auditoría forense para determinar el origen del incidente e implementar controles de mitigación.

APC04 - Detección de tráfico de red anómalo

- **Precaución**: implementar un sistema de monitoreo de eventos de seguridad con posibilidad de reacción y alerta ante eventos anómalos.
- **Prevención**: contar con monitoreo en tiempo real y configuración de alertas, además de respuesta automática ante un evento anómalo.
- **Reacción**: aislamiento de la red comprometida y posterior análisis forense.

APC05 - Protocolos de cifrado de las comunicaciones

- **Precaución**: realizar hardening de dispositivos implementados para mejorar el nivel de seguridad.
- **Prevención**: monitoreo y análisis de configuración de dispositivos con periodicidad.
- **Reacción**: aplicar robustecimiento de sistema operativo y aplicaciones (Hardenning) en los dispositivos detectados.

ASO01 - Estado de actualización del software (o nivel de obsolescencia)

- **Precaución**: mantener un sistema de actualización de software y firmware de los dispositivos que actúe en forma periódica.
- **Prevención**: monitorear periódicamente el estado del software de los dispositivos implementados.
- **Reacción**: actualizar el software obsoleto y analizar el impacto.

ASO02 - Estado de software EDR (Endpoint Detection and Response) de los dispositivos

- **Precaución**: implementar un EDR (o XDR) en cada dispositivo que permita acciones en forma automática cuando se detecta un evento anómalo.
- **Prevención**: contar con monitoreo en tiempo real de los dispositivos con un EDR (o XDR) y revisar alertas.
- **Reacción**: aislar el dispositivo y realizar un análisis forense.

AAS01 - Aplicaciones web de la organización

- **Precaución**: implementar controles de seguridad en diferentes capas, como por ejemplo un Web Application Firewall y testear periódicamente el plan de resguardo y recuperación de información.
- **Prevención**: monitorear los eventos de seguridad en las aplicaciones publicadas de la organización.
- **Reacción**: analizar el ataque y ajustar los controles para mitigar el impacto.

APP01 - Identidad Digital

- **Precaución**: implementar un sistema de control de accesos que contemple datos que solamente el usuario conoce, qué tiene o qué es.
- **Prevención**: monitorear intentos de acceso y alertas.
- **Reacción**: aislar la identidad digital y denegar acceso para auditar qué impacto tuvo.

APP02 - Capacitación del personal de la organización sobre el uso responsable de las nuevas tecnologías

- **Precaución**: Brindar entrenamiento a los usuarios en el uso adecuado de la tecnología y sus riesgos.
- **Prevención**: monitorear los activos digitales y controlar las políticas de acceso.

7.2. Recomendaciones específicas

A continuación, se desarrollarán algunas acciones particulares y recomendaciones para gestionar distintos activos de una organización. Se aclara que son recomendaciones, cada organización optará por implementarlas, mejorarlas, adaptarlas a su situación particular o descartarlas.

7.2.1. Inventario de Activos OT[18]

En este capítulo se ofrece una guía completa junto con los pasos esenciales para llevar a cabo un inventario de activos en un entorno industrial. Se exploran distintos métodos potenciales para la preparación del inventario, así como la clasificación de los diversos tipos de bienes que pueden encontrarse en dicho inventario. Además, se presenta un repertorio tanto de herramientas de código abierto como propietarias que pueden emplearse para llevar a cabo el inventario.

El contenido aborda los siguientes aspectos:

- Tipos de Inventario de Activos en SCI: Se detallan los tipos de inventario que pueden ser implementados. Esta sección analiza los distintos enfoques de implementación y metodología del inventario.
- Gestión de Activos: Se expone una clasificación de los activos según su naturaleza, junto con la descripción de la información relevante que se almacena en el inventario para cada tipo de activo.
- Clasificación de Herramientas de Inventario de Activos: Se proporciona un compendio de herramientas que pueden utilizarse para llevar a cabo el inventario de activos, tomando ejemplos tanto de herramientas gratuitas como de pago. Se detalla su funcionalidad y utilidad dentro del proceso de inventario.
- Pasos para la Creación Correcta del Inventario de Activos en SCI: Se establecen los pasos necesarios para llevar a cabo el inventario de activos de manera adecuada, asegurando la precisión y eficiencia del proceso.
- Mantenimiento del Inventario: Se resalta la importancia de mantener actualizado el inventario y se explica por qué no hacerlo puede resultar en una depreciación del valor de los activos.

  Conclusiones: Se sintetizan los puntos clave que destacan la relevancia y los beneficios de realizar un inventario de activos en los sistemas de control industrial, subrayando su valor para la gestión eficaz de los recursos y la toma de decisiones informada.

[18] Esta sección ha sido tomada, y brevemente adaptada, del documento elaborado por el Instituto Nacional de Ciberseguridad de España – INCIBE , *"Guía para la gestión de un inventario de activos en sistemas de control industrial". Fuente:* https://www.incibe.es/sites/default/files/contenidos/guias/doc/incibe-cert_guia_inventario_de_activos_2020_v1.pdf

Introducción al Inventario de Activos

En los últimos años, la creciente vulnerabilidad de los sistemas de control industrial (SCI) ante los incidentes de ciberseguridad es innegable. En este sentido, el primer paso crucial para garantizar la seguridad de un sistema de control industrial es llevar a cabo un exhaustivo inventario que abarque todos los activos involucrados en el proceso.

Cuando este inventario se realiza de manera precisa y completa, se obtienen detalles específicos de cada activo, incluyendo información sobre la versión del software o firmware instalado. Esta recopilación detallada de datos proporciona una lista de verificación que resulta fundamental para gestionar de forma efectiva las vulnerabilidades presentes en el sistema.

Gracias a esta información detallada, se pueden aplicar soluciones y medidas de mitigación de manera precisa y oportuna. Esta lista de verificación se convierte así en una herramienta invaluable para identificar y abordar las vulnerabilidades, contribuyendo así a reforzar la seguridad del sistema de control industrial.

¿Para qué sirve el Inventario de Activos?

Contar con un inventario de activos en un sistema de control industrial proporciona una visión completa de todos los componentes involucrados en su funcionamiento, lo cual conlleva numerosas ventajas, entre las que se incluyen:

- Gestión de Vulnerabilidades Simplificada: Al disponer de un inventario actualizado, es fácil identificar las versiones de software o firmware presentes en el sistema en cualquier momento, lo que facilita la gestión de vulnerabilidades y la aplicación de parches o actualizaciones necesarias.
- Respuesta Efectiva a Incidentes: Conocer todos los activos del sistema permite una respuesta más rápida y organizada ante incidentes de seguridad, ya que se comprende mejor el alcance del incidente y se agiliza la implementación de medidas correctivas.
- Detección de Fallas Operativas: Los inventarios de activos no solo benefician la ciberseguridad, sino que también ayudan a identificar fallos en los procesos operativos, lo que contribuye a mejorar la eficiencia general de la operación.
- Reducción de Costos: Todas estas ventajas se traducen en una mayor seguridad y un conocimiento más completo de los activos, lo que a su vez conduce a una reducción de costos asociados a posibles incidentes de seguridad o interrupciones operativas.

Incluir la realización de un inventario de activos como uno de los primeros pasos en la implementación de un plan de gestión de ciberseguridad es fundamental para garantizar la protección de los activos y descubrir posibles riesgos desconocidos previamente.

Tipos de Implementación de Inventario

Es prudente que el inventario de activos se ajuste a los lineamientos establecidos para el inventario general de la infraestructura de control industrial. No obstante, también puede adaptarse específicamente para estas capas. A continuación, se ofrece una clasificación.

Inventario Manual

Un inventario manual implica la recopilación de datos por parte de responsables designados, prescindiendo del uso de software auxiliar. Aunque esta metodología garantiza acceso a la información necesaria sobre cada activo, se recomienda únicamente cuando la cantidad de activos es reducida debido al tiempo requerido para su ejecución y actualización.

Inventario Automático

Por otro lado, un inventario automático se lleva a cabo mediante herramientas que agilizan la recopilación de datos de cada activo de manera automática. Esta metodología resulta especialmente beneficiosa en organizaciones con un gran número de activos. Sin embargo, puede presentar un desafío en términos de obtención de información detallada sobre cada activo.

Inventario Mixto

Los inventarios mixtos combinan el uso de herramientas automatizadas y técnicas manuales para alcanzar la mayor precisión posible. Esta metodología permite una gestión más completa de activos, ya que se recopilan todos los activos posibles utilizando herramientas automatizadas y se complementan manualmente con información adicional. Se recomienda esta implementación cuando el número de activos es intermedio, ya que si es muy alto, el esfuerzo requerido puede ser considerable.

Por lo tanto, la selección del método de inventario depende del tamaño y la complejidad de la infraestructura de control industrial, así como de la cantidad de activos a gestionar. Es crucial considerar estos factores para determinar la metodología más adecuada que garantice la precisión y eficiencia del inventario de activos.

Tipos de Inventario

Según la metodología empleada para llevar a cabo el inventario, pueden distinguirse dos tipos principales: activos y pasivos.

Inventario Activo

Los inventarios activos requieren una interacción directa con los activos, lo que implica revisar sus configuraciones o ejecutar scripts para obtener detalles, con el riesgo potencial de afectarlos. Este enfoque puede involucrar el escaneo activo de redes o la inspección física de activos. Por ejemplo, el escaneo activo en redes representa una implementación automatizada, mientras que la inspección física de activos es un método manual.

Inventario Pasivo

Por su parte, un inventario pasivo se caracteriza por no interactuar directamente con los activos, siendo menos intrusivo que el enfoque activo. Aunque proporciona información menos precisa, no afecta a los activos. Este tipo de inventario puede incluir análisis de tráfico de red o inspección de archivos de configuración de los activos. Por ejemplo, el análisis de red puede ser una combinación de herramientas automáticas y análisis manual, mientras que la revisión de archivos de configuración es un proceso puramente pasivo y manual.

La elección entre un inventario activo y uno pasivo depende de los objetivos del inventario y del nivel de intrusión aceptable. Ambos enfoques tienen sus ventajas y limitaciones, y pueden ser complementarios en algunos casos, según las necesidades específicas de la organización.

Clasificación de Activos

Con el fin de realizar una gestión adecuada de los activos, es posible categorizarlos según su naturaleza. Así, se puede contar con uno o varios inventarios que contengan todos los activos posibles de la organización. A su vez, es fundamental almacenar información suficiente sobre cada activo para que el inventario tenga un valor significativo.

A continuación, se presenta una posible clasificación de los activos según su naturaleza.

Hardware: Incluye todos los equipos físicos utilizados en el desarrollo del proceso industrial, como PLC, RTU, IED y servidores.

Software: Engloba las aplicaciones empleadas para la gestión del proceso, como SCADA, sistemas operativos, firmware y herramientas de desarrollo.

Personal: Hace referencia al personal que trabaja en la organización, ya sea fijo o subcontratado.

Información: Comprende los datos generados, recogidos, gestionados, transmitidos y destruidos, independientemente de su formato, como bases de datos, documentación y manuales.

Red: Involucra los dispositivos de conectividad de red, como routers, switches y cortafuegos.

Tecnología: Incluye los equipos necesarios para gestionar personas y el negocio de la empresa, como computadoras, teléfonos, impresoras y cableado.

Equipamiento Auxiliar: Abarca activos que no pertenecen a ninguna de las categorías anteriores y que brindan soporte a los demás sistemas, como climatización, iluminación e instalaciones.

Instalaciones: Hace referencia a los lugares donde se alojan los equipos relevantes de la empresa, como oficinas y edificios.

Información referente de los activos

Para que el inventario sea efectivo en términos de seguridad y gestión de riesgos, es necesario almacenar información detallada sobre cada activo registrado. Algunos de los campos relevantes a completar para cada activo incluyen:

- Identificador: Código único que identifica a cada activo.
- Nombre: Puede incorporar el modelo, marca, versión, entre otros detalles.
- Fabricante: En el caso de activos software, se refiere al fabricante o desarrollador, pudiendo incluirse también en el campo "nombre".
- Descripción: Debe proporcionar información sobre el uso del activo.
- Tipo: La clasificación del activo.
- Propietario: Persona encargada de tomar decisiones respecto al activo.
- Responsable: Persona encargada de garantizar la operatividad del activo y gestionar el acceso al mismo, pudiendo coincidir con el propietario.

- Ubicación: El lugar físico donde se encuentra el activo; para activos lógicos, la ubicación será un activo físico.
- Versiones de software: En el caso de activos físicos, se puede incluir un resumen breve del software presente, incluyendo sus versiones.
- Valoración del activo: Permite evaluar su impacto y criticidad en el sistema, considerando aspectos como:
    - Disponibilidad: Importancia de la presencia del activo, valorada cualitativa o cuantitativamente.
    - Integridad: Repercusiones para el negocio ante modificaciones no autorizadas al activo, valoradas cualitativa o cuantitativamente.
    - Confidencialidad: Grado de confidencialidad necesario para el activo, valorado cualitativa o cuantitativamente.
    - Criticidad: Dependencia del proceso respecto al activo, donde un mayor valor de criticidad implica mayores consecuencias para el negocio ante la pérdida del activo.
    - Costo: Valor económico asociado al activo.

Clasificación de herramientas para el inventariado de Activos

Dentro de las herramientas utilizadas para realizar un inventariado de activos, se pueden distinguir principalmente dos tipos: las herramientas gratuitas (open source y libres) y las herramientas propietarias o comerciales, que también pueden considerarse libres. Las herramientas open source son aquellas que se pueden utilizar de forma gratuita y cuyo código fuente está disponible para todos, lo que permite realizar cambios y modificaciones según sea necesario. Por otro lado, las herramientas libres también están disponibles de forma gratuita, pero su código fuente no se proporciona.

Las herramientas comerciales son propietarias y requieren la compra de una licencia o registro para su uso, aunque algunas ofrecen versiones de prueba limitadas en tiempo o funcionalidades. En algunos casos, estas herramientas comerciales también pueden clasificarse como libres, ya que sus desarrolladores pueden proporcionarlas a los usuarios sin acceso al código fuente.

A continuación, se mencionan algunos ejemplos tanto de herramientas open source y libres como de herramientas comerciales. Dado el alcance del documento, no se incluyen todas las

herramientas disponibles, sino ejemplos representativos de cada categoría, especialmente aquellas que permiten un inventariado detallado de activos de red.

Herramientas Open Source y Libres

Wireshark

Wireshark [19] es una herramienta de código abierto desarrollada para el análisis de protocolos de red. Permite la realización de un inventario al identificar los equipos involucrados en las comunicaciones de forma pasiva, mediante la captura de tráfico de red.

Nmap

Nmap[20] es una herramienta utilizada para el descubrimiento de activos de red y auditorías de seguridad. Permite identificar servicios presentes en los mismos, asociados a puertos de red abiertos o en escucha. Su tipo de inventariado es activo, lo que implica un escaneo directo sobre los activos de la red. Por tanto, es crucial estudiar cuidadosamente sus resultados para evitar posibles impactos negativos. Estos podrían incluir un aumento en el consumo de recursos de los equipos, saturación de la red, mal funcionamiento de los dispositivos e incluso condiciones de denegación de servicio.

OpenVAS

OpenVAS[21] es una herramienta destinada a la identificación y gestión de vulnerabilidades en los activos. Permite obtener información detallada, como versiones de software y vulnerabilidades asociadas. La herramienta realiza un inventario de manera activa, escaneando los activos de la red. Es importante estudiar cuidadosamente los resultados para evitar posibles impactos negativos, similares a los que podría causar Nmap. La ejecución de scripts NVT para identificar vulnerabilidades de seguridad puede ocasionar problemas en la actividad de los equipos.

[19] Sitio oficial: https://www.wireshark.org/

[20] Sitio oficial: https://nmap.org/

[21] Sitio oficial: https://openvas.org/

Herramientas Comerciales

OT-Base

OT-Base, desarrollada por la empresa Langner[22], es una solución de seguridad diseñada específicamente para equipos y redes TO. Ofrece capacidades como el descubrimiento de activos de la red y la gestión de un inventario TO. Utiliza escaneos activos que emplean protocolos de comunicación industriales, como Modbus, y otros protocolos de ámbito TI, con una metodología menos intrusiva que otras soluciones, lo que garantiza que no afecte negativamente a la operación.

EyeSight

EyeSight[23], desarrollada por la empresa Forescout, es una herramienta multifuncional para el descubrimiento y clasificación de activos de la red. Ofrece la capacidad de descubrir activos tanto en redes TI como en redes TO, permitiendo la creación de un inventario completo de todos los activos. Esta herramienta posibilita el descubrimiento de activos tanto de forma pasiva, mediante la captura de tráfico de red, como de forma activa, mediante el uso de comandos Nmap y consultas HTTP y SNMP.

Pasos para la creación de un Inventario de Activos de un SCI

Una herramienta fundamental en el trabajo con sistemas de control industrial (SCI) es contar con un inventario de activos que facilite la gestión de todos los dispositivos de TO disponibles. Esto garantiza un control exhaustivo de los equipos, mejorando tanto la seguridad como la eficiencia al buscar dispositivos específicos. Para lograrlo, es crucial seguir ciertos pasos al crear el inventario desde cero. Dada la gran cantidad de dispositivos conectados posibles, realizar esta tarea sin un orden y pautas establecidas puede resultar bastante difícil.

A continuación se detallan los pasos necesarios para la creación de un inventario de activos.

Definir el alcance

Inicialmente, es necesario definir el alcance del inventario, que no se refiere a la cantidad de activos a incluir (que deberán ser todos), sino a la profundidad de la información a recopilar de cada uno. Esto implica una revisión exhaustiva del alcance de los dispositivos, pudiendo requerir varios inventarios o su clasificación en distintos grupos debido a la diversidad y cantidad de

[22] Sitio oficial: https://www.langner.com/

[23] Datasheet: https://forescouttechnologies.es/resources/eyesight-datasheet/

dispositivos a gestionar. La importancia de un inventario de activos sólido en proyectos de ciberseguridad es fundamental, ya que contribuye a realizar un trabajo efectivo. Además, al definir adecuadamente el alcance de la información de los activos a incluir, se puede protegerlos de manera más eficiente ante posibles vulnerabilidades.

Definir el tipo de inventario

Una vez que se ha definido el alcance del inventario, es necesario determinar el tipo de implementación a utilizar para su creación (manual, automática o mixta). Esta elección dependerá de la infraestructura y topología de los dispositivos existentes, ya que ciertos métodos serán más convenientes que otros en función de estas características. Lo mismo sucede al elegir el tipo de inventariado (activo o pasivo), ya que esto tendrá un impacto variable en la infraestructura o topología de los dispositivos en funcionamiento.

Búsqueda de activos y creación del inventario

La creación inicial de un inventario de activos de calidad demanda tiempo para su implementación, aunque esto puede ser desafiante debido a otros factores como costos y proyectos en curso. Además, es crucial realizar revisiones periódicas para garantizar su actualización constante.

Es recomendable dedicar todo el tiempo necesario para crear un inventario que cumpla con requisitos mínimos, ya que disponer de información detallada sobre los activos mejora la seguridad.

Las técnicas empleadas para recopilar dispositivos en el inventario dependen del tipo de implementación o inventariado seleccionado, adaptándose a la estructura y distribución de la planta.

Es esencial asegurar que todos los equipos estén incluidos en el inventario y clasificados de manera adecuada.

Revisión del inventario y copias de seguridad

Una vez creado el inventario o inventarios, es fundamental mantenerlos actualizados constantemente; de lo contrario, se volverán obsoletos y no proporcionarán la información necesaria, lo que puede conducir a una gestión deficiente de la seguridad.

Es crucial revisar los inventarios no solo cuando se añadan nuevos activos, sino de manera periódica, para asegurarse de que estén siempre al día.

Realizar copias de seguridad del inventario principal ayuda a prevenir desastres, ya sean causados por terceros o por personal interno, que puedan resultar en robo o eliminación de datos. Así, en caso de incidentes, se puede restaurar la copia de seguridad sin perder información. Es recomendable mantener una copia actualizada para garantizar la recuperación de la versión más reciente del inventario en caso de pérdida de datos.

Mantenimiento de Inventarios

Para que el inventario de activos sea efectivo en términos de seguridad, debe ser dinámico y actualizarse continuamente, con revisiones que respondan a cualquier cambio en el sistema, como la adición de nuevos dispositivos o la eliminación de equipos obsoletos. Aunque la ideal es mantener una actualización constante, en la práctica se suelen establecer revisiones trimestrales, anuales o según la conveniencia de la organización.

Es esencial establecer una periodicidad adecuada para la actualización del inventario, que puede variar según el tipo de activo o la información que se desea actualizar. Por ejemplo, los cambios en el personal pueden requerir actualizaciones manuales inmediatas, mientras que los cambios en el software instalado pueden ser monitoreados periódicamente con herramientas automáticas.

El control de accesos al inventario debe ser supervisado para limitar los cambios solo a usuarios autorizados. Normalmente, el personal de sistemas es el propietario del inventario, pero ciertos perfiles de otros departamentos pueden tener acceso limitado para realizar modificaciones. Se recomienda permitir el acceso de lectura a cualquier usuario para que estén informados de los activos identificados y puedan proponer cambios si detectan errores.

En cuanto a las copias de seguridad del inventario, son esenciales para ayudar en la resolución de incidentes y proteger los datos contra ciberataques o errores. Se sugiere realizar copias de seguridad regularmente, con especial atención a los cambios significativos en su contenido, independientemente de cuándo se haya realizado la última copia de seguridad.

Formulario de ejemplo para toma de inventario de activos

A continuación, se presenta un ejemplo de formulario sugerido para la realización de toma de inventario manual.

Tabla 9: Formulario propuesto para toma de inventario (Fuente: INCIBE)

Inventario				Responsable			Fecha:				
Fabricante	Descripción	Tipo	Versión de software	Estado	Responsable	Ubicación	Valoración del activo				
							Disponibilidad	Integridad	Confidencialidad	Criticidad	Costo
	Firma del Responsable:			Fecha:		Hora:					

7.2.2. Ciberseguridad de Red[24]

El crecimiento de Internet y la llegada de innumerables dispositivos con conectividad y posibilidades de procesamiento razonables ha creado nuevos desafíos de seguridad que también afectan a las infraestructuras críticas.

Estas infraestructuras suelen estar gestionadas por sistemas de control industrial específicos que se utilizan para supervisar y gestionar procesos industriales típicos, y están cada vez más expuestas a interacciones con otros sistemas en el entorno de Internet.

Las tendencias observadas en la detección de amenazas indican que la infraestructura industrial se ha convertido en un objetivo importante para los ataques que involucran a actores como el terrorismo, el gobierno o el espionaje industrial, entre otros. Así lo evidencia el creciente número de eventos e incidentes relacionados con este tipo de infraestructura.

Todo esto hace que una comprensión detallada de los protocolos involucrados en los procesos industriales sea crucial para comprender las posibles debilidades, los vectores de ataque y las posibles defensas que deben tenerse en cuenta al implementar o fortalecer los sistemas de control industrial.

Seguridad en el Diseño de una Red SCI

La seguridad básica comienza con una arquitectura de red separada por zonas, según la cantidad de segmentos de red necesarios para poder diferenciar y proporcionar las medidas de seguridad y control de tráfico adecuadas para cada zona. Esta separación es un concepto fundamental en la planificación de cualquier arquitectura de red y también se aplica a SCI. Este tipo de diseño, combinado con el control del flujo de datos entre dominios definidos, minimizará el daño causado por el posible compromiso de los dispositivos en el dominio.

Este objetivo se puede lograr mediante la incorporación de soluciones diseñadas para la segmentación y protección de segmentos de red, donde:

[24] Esta sección ha sido tomada, y brevemente adaptada, del documento elaborado por el Instituto Nacional de Ciberseguridad de España – INCIBE , *"Protocolos de seguridad en redes de control industrial.". Fuente:* https://www.incibe.es/sites/default/files/contenidos/guias/doc/incibe_protocolos_seguridad_red_sci.pdf

Segmentación

Dividir la arquitectura de red en diferentes áreas según funciones, lo más cerca posible a la propuesta de referencia ISA-95, como se muestra en la siguiente figura. Debe haber al menos tres áreas para separar la zona de control, DMZ y LAN empresarial. Esta simple división permite contener una infección dentro de una misma zona, dificultando el salto hacia otras zonas.

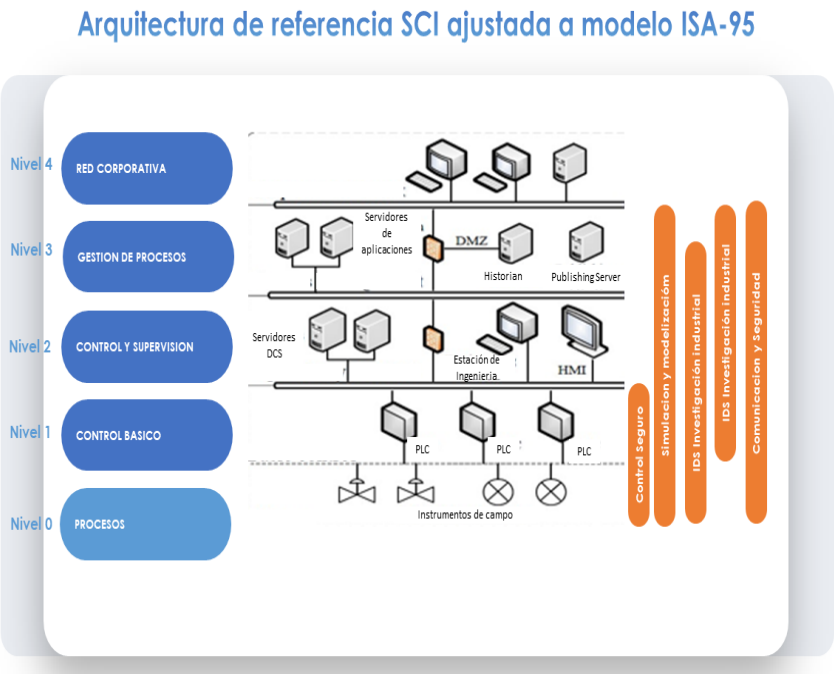


Figura 6: Arquitectura de SCI ajustada a modelo ISA-95 (Fuente: INCIBE)

Cifrado y separación lógica de comunicaciones entre segmentos de red

Mediante el uso de tecnologías VLAN y VPN. Esta medida también se utiliza para evitar que la infección salte entre capas.

Control y filtrado

El tráfico pasa a través de firewalls, proxies y elementos diseñados para identificar y separar al tráfico y a las comunicaciones tanto a nivel de red (IP, enrutamiento) como por puerto/protocolo y a nivel de aplicación. Esto ayuda a detectar infecciones cuando intenten cambiar de área. Si se agregan elementos como IDS o SIEM a la red para control de eventos, alertas de intrusión y registro, la red resultante se parecerá a la red del diagrama.

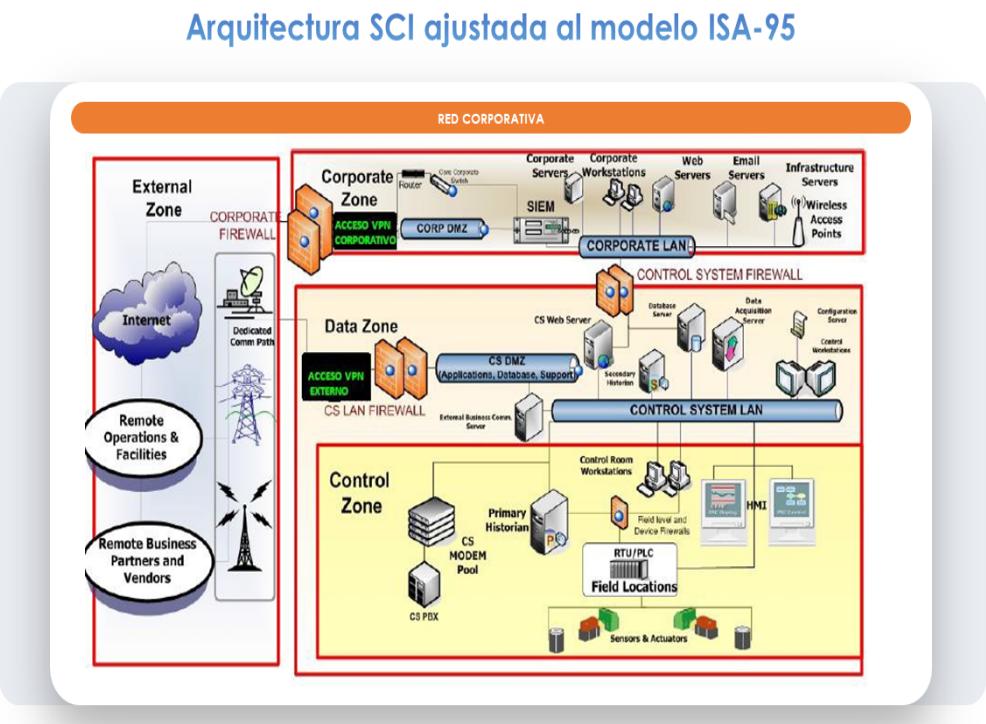


Figura 7: Arquitectura de SCI ajustada a modelo pirámide ISA (Fuente: INCIBE)

Extensión de Seguridad

Extender la seguridad a las capas de enlace y aplicación. Ampliar la seguridad en la capa de enlace con controles de acceso como 802.1x y filtrado de direcciones MAC, y en el nivel de aplicación con firewalls de aplicación (WAF).

Control de acceso

Controlar el tráfico con ayuda de un mecanismo de listas blancas (whitelisting), implementando reglas de acceso basadas en elementos conocidos negando el acceso a todo lo demás.

Redes inalámbricas

Las redes inalámbricas conllevan un riesgo adicional, por lo que deben implementarse únicamente bajo necesidad o decisión particular de la organización y siempre bajo condiciones justificadas. En su caso, se utilizarán mecanismos IEEE 802.1x para la autenticación haciendo uso de protocolos EAP-TLS que autentican clientes con certificados o haciendo uso de un servidor RADIUS. Los puntos de acceso se situarán en redes aisladas o con mínimos puntos de interconexión a la red de control SCI (evitándolo si es posible). Utilizar un protocolo robusto para las

comunicaciones inalámbricas como WPA2, adicionalmente usar un SSID característico y único, desactivando su broadcast e igualmente habilitar filtrado por dirección MAC.

Cifrado de las Comunicaciones

La mayoría de los protocolos de control industrial no incorporan cifrado en su implementación. Así, cualquier acceso no autorizado a la red permitiría a un atacante inspeccionar y manipular el tráfico. De esta forma el uso de HTTPS, SSH, SNMP v3 en la medida que sea posible es altamente recomendado para la autenticación y el acceso a servicios de la red o los dispositivos de la misma.

Autenticación y Control de Acceso.

Una adecuada gestión de privilegios basados en roles (RBAC) es una medida que aporta seguridad en el aspecto de las restricciones relativas a cada perfil. Por ello, crear distintos perfiles de usuario diferenciados y asignar un rol operativo a cada uno, dependiendo de sus funciones, resultará un complemento favorable. También se recomienda añadir medidas adicionales como mensajes de advertencia que ayuden a identificar el servicio al que se accede en previsión de posibles errores no intencionados.

Acceso Remoto.

En caso de ser necesario el acceso desde infraestructuras externas a la red de control, la utilización de soluciones VPN aportará el cifrado y autenticación necesarios para proteger la conexión. Se recomienda el uso de un software y/o hardware especializado para acceso remoto, así como una adecuada política de seguridad relativa al mantenimiento de actualizaciones, de gestión de acceso y usuarios.

Disponibilidad.

En los sistemas de control de procesos, la latencia y la velocidad de transmisión de mensajes son críticas, por lo que son los factores determinantes en la preparación del diseño de una red de control para enfrentar posibles problemas de congestión o pérdida de conexión. Las recomendaciones para mejorar la resiliencia cibernética frente a estos problemas son:

- Utilización de conmutadores que brinden capacidades de red para dividirlos en VLAN y utilización de criterios de calidad de servicio para priorizar diferentes tipos de tráfico.

- Utilización de topologías redundantes para mejorar la disponibilidad e implementación STP (Protocolo de árbol de expansión) para controlar la formación de bucles de red.
- Utilización del protocolo IGMP con VLAN para brindar un mejor rendimiento y restricción de mensajes de multidifusión según el tipo de tráfico y los dispositivos asociados.

Recomendaciones para cortafuegos (Firewalls)

Complementando las recomendaciones propuestas para la arquitectura de red que se describen en este apartado, las siguientes reglas de carácter general pueden aplicarse:

- El conjunto de reglas de base debe ser denegar todo e ir permitiendo comunicaciones o servicios según necesidades (listas blancas).
- Los puertos y servicios entre el entorno de red de control y la red de la corporativa deben ser habilitados y permitidos de manera específica, según las necesidades de cada caso. Debe haber una justificación documentada con el análisis de riesgos y una persona responsable de cada flujo de datos entrante o saliente permitido.
- Todas las reglas de «acceso permitido» deben fijarse con una dirección IP y puerto TCP/UDP específico con control de estado.
- Todas las reglas deben definirse para restringir el tráfico solo a una dirección IP específica o a un rango de direcciones.
- Denegar tráfico directamente desde la red de control a la red corporativa. Todo el tráfico de control debe terminar en la zona DMZ.
- Todo protocolo permitido entre la red de control y DMZ no debe permitirse explícitamente entre la DMZ y las redes corporativas (y viceversa).
- Todo el tráfico saliente de la red de control de la red corporativa debe estar estrictamente restringido por fuente y destino, así como el servicio y el puerto.
- Los paquetes salientes desde la red de control o DMZ solo deben ser autorizados si los paquetes tienen una dirección IP de origen correcta asignada a la red de control o dispositivos de la red DMZ.
- No se debe permitir el acceso a Internet a dispositivos de la red de control.
- Las redes de control no deben conectarse directamente a Internet, aunque estén protegidas por un firewall.
- Todo el tráfico de administración de firewall debe realizarse en cualquiera de una red separada, asegurado gestión (por ejemplo, fuera de banda) o en una red cifrada con

autenticación de múltiples factores. El tráfico también debe ser restringido por dirección IP a las estaciones de gestión específicas.

- Todas las políticas de firewall deben probarse periódicamente.
- Todos los firewalls deben ser respaldados (copia de respaldo de reglas y configuración en general) inmediatamente antes de la puesta en marcha.

Recomendaciones generales sobre servicios TCP

Sumando a las reglas generales descriptas, se proponen las siguientes reglas de cortafuegos (firewalls) genéricas según el servicio o protocolo:

Tabla 10: Recomendaciones sobre TCP (Fuente: INCIBE)

SERVICIO	RECOMENDACIÓN
DNS	Hacer un uso de un servidor DNS local interno restringido para la red de control. En casos de elementos limitados puede hacerse uso de archivos locales de hosts.
HTTP	El protocolo utilizado para acceso web con navegadores es muy útil y cómodo. No obstante, si no se usa HTTPS cuyas transmisiones son cifradas debe ser denegado desde la red corporativa o pública a la red de control. Adicionalmente: ✓ Hacer uso de listas blancas (filtrado IP) para los accesos web a servicios en la red de control o física. ✓ Control de acceso tanto a orígenes como destinos ✓ Implementación de autorización a nivel aplicación ✓ Restringir el número de tecnologías soportadas para disminuir la superficie de vulnerabilidades Registrar y monitorizar tanto el uso como los intentos o accesos al servicio
FTP Y TFTP	Estos dos protocolos de transmisión de archivos son de uso común en sistemas SCI. Sin embargo, la ausencia de cifrado los hace vulnerables a robo de credenciales e información. Debe evitarse en la medida de lo posible y sustituir de versiones cifradas como SCP o SFTP. En caso estrictamente necesario utilizar únicamente bajo un túnel cifrado o restringir su uso a transmisiones no críticas.
TELNET	Este protocolo de acceso y comunicación no cuenta con cifrado lo que desaconseja su uso. En caso de necesidad utilizar una red privada o VPN para proteger la transmisión.
DHCP	Este protocolo diseñado para la configuración automática de red de dispositivos es de gran utilidad, pero entraña riesgos de seguridad al poderse utilizar para ataques MITM e interceptar tráfico. En la medida de lo posible evitar su utilización o, en caso necesario implementar reglas de inspección de tráfico para evitar falsos servidores DHCP (*rogue servers*) así como medidas anti *spoofing* de ARP e IP.
SSH	Una correcta utilización de SSH debe considerarse como una medida eficaz para establecer comunicación segura entre segmentos o elementos de red con tráfico sensible. Debe permitirse y sustituir a FTP, TELNET, RCP y otros protocolos inseguros.
SOAP	SOAP (Simple Object Acess Protocol) utiliza una sintaxis XML para intercambiar mensajes. Es un mecanismo sin control de estado y por ello bastante vulnerable a falsificación e interceptación. En este sentido reglas de inspección de tráfico a nivel de aplicación son aconsejables para controlar el contenido de los mensajes.
SMTP	Este protocolo utilizado en el correo electrónico debe ser denegado en la red de control. Tráfico SMTP saliente desde la red de control a la corporativa puede permitirse para envió de alertas por correo electrónico.
SNMP	SNMP es el protocolo utilizado para el control y monitorización entre elementos de red siendo de gran utilidad. No obstante en sus versiones 1 y 2 hace uso de comunicaciones no cifradas y contraseñas genéricas. SNMP versión 3 ya soluciona estos problemas pero no siempre es compatible con todos los dispositivos. En caso de contar con el uso de las versiones anteriores a v3 se recomienda separar el tráfico SNMP en una red de gestión.
DCOM	DCOM, del inglés Distributed Component Object Model es el protocolo sobre el que se apoya OPC (OLE for Process Control. Hace uso de RPC (Remote Procedure Call) servicio que debe ser convenientemente parcheado por contar con múltiples vulnerabilidades. Además OPC a través de DCOM, hace uso de puertos dinámicos (desde 1024-65535) lo que incrementa la dificultad de establecer una regla concreta de firewall. El tráfico de este protocolo debe permitirse únicamente entre las redes de control y DMZ. Adicionalmente se recomienda aplicar configuraciones de DCOM en los dispositivos para reducir el rango de puertos dinámicos disponibles.

8. Análisis Forense en SCADA (caso de estudio)

En el marco del Trabajo Final de Carrera del Lic. Raúl Oscar Romero[25], perteneciente al grupo de investigación que desarrolló el presente trabajo, se elaboró una metodología de trabajo para disminuir la brecha de seguridad que actualmente existe en los sistemas SCADA. Éstos permiten controlar de manera remota una instalación recolectando e integrando información desde distintos sensores y autómatas industriales (PLCs o RTUs) por intermedio de diferentes protocolos desde ambos dispositivos. Desde el punto de vista del software se instala y cumple con los requerimientos específicos para ello.

Esta metodología de trabajo se desarrolló ante la falta de aplicación de estándares a redes industriales críticas que puedan establecer seguridad en esta infraestructura. Se llevó a cabo mediante la realización de la estructura topológica como una solución de laboratorio, simulando un entorno industrial real. Se seleccionó para esta investigación una empresa que produce y comercializa productos plásticos.

El resultado alcanzado, la aplicación de normativas y estándares y de regulaciones aplicadas en países del primer mundo genera la adquisición de nuevas tecnologías de hardware y software relevantes para las redes industriales críticas que ya desde su diseño y fabricación permiten disminuir las brechas e incidentes de seguridad en la industria. Demostraron ser efectivas y/o asertivas a la hora de minimizar la inseguridad en la infraestructura.

Por lo antes mencionado será importante la concientización y capacitación de todos los usuarios interactuantes con los sistemas críticos industriales.

A continuación, se mencionarán las particularidades a tener en cuenta al realizar un análisis forense en este tipo de situaciones y los resultados de este trabajo.

8.1. Características de los sistemas SCADA

Muchas veces, de forma errónea, al conjunto de los sistemas de campo, control y supervisión se lo denomina como SCADA. SCADA, es un acrónimo de Supervisory Control And Data

[25] Romero Raul Oscar. “Informática Forense, Seguridad y Estándares en Sistemas Industriales e Infraestructuras Críticas”, Universidad Abierta Interamericana, (2021).

Acquisition (Control Supervisor y Adquisición de Datos) y es un concepto que se emplea para realizar un software para ordenadores que permite controlar y supervisar procesos industriales a distancia.

La primera generación de SCADA presenta tres niveles: El nivel de campo, el nivel de control y el de supervisión.

En el nivel de campo se puede hallar a los diferentes equipos que intervienen directamente en el proceso de producción: sensores analógicos como ser: de temperatura y/o nivel en tanques, caudalímetros, sensores de presión (que en general por su confiabilidad usan el estándar 4 – 20mA[26]); o sensores digitales (que usan diferencias de potencial) como ser: micro-switches, sensores de fin de carrera, sensores ópticos, actuadores para encendido de motores o bombas, apertura o cierre de válvulas, etc. que generalmente se conectan a relés.

En el nivel de control se encuentra principalmente a los dispositivos de control (básicamente PLC y RTU) e interfaces hombre-máquina (HMI según sus siglas en inglés). Estos elementos se encuentran distribuidos dentro de la planta de producción, y conectados entre sí mediante una red de comunicaciones. Un PLC es una computadora industrial que usa la ingeniería para la automatización de procesos. Controlan las entradas y salidas de manera segura, poseen una programación compatible con distintos lenguajes, una interfaz amigable que facilita la comunicación con el usuario, conexión a sistemas de supervisión y ejecutan la programación de forma continuada. Un HMI, por otro lado, es un software diseñado específicamente para SCI. Utiliza datos en red para proporcionar a los operadores una interfaz gráfica que permite monitorear el rendimiento de muchas partes y equipos y emitir comandos y configuraciones de proceso desde una pantalla.

El nivel de supervisión se compone por equipos de cómputo con software específico. Allí puede hallarse el software SCADA de supervisión, terminales de ingeniería y mantenimiento. Los SCADA permiten que los operadores de los ambientes de producción tengan un informe resumido de cada uno de los equipos conectados a la red. Las soluciones SCADA permiten monitorear con precisión, controlar y visualizar cada aspecto de la operación de manera centralizada. Así, a simple

[26] Control para la Industria S.A. "¿Porqué 4 – 20 mA?". En línea: https://www.cpi.com.ar/notas/por-que-4-20-ma/. Consultado 01/07/2022

vista, el operador puede visualizar qué es lo importante que necesita conocer. Los SCADA tradicionales no se conectaban con otros sistemas ni otras redes de computadoras. Sus mecanismos de comunicación y protocolos se acercaron a esquemas del tipo propietario. Los últimos productos se han desarrollado para el protocolo Modbus (uno de los más usados en los SCADA).

La segunda generación de sistemas SCADA integró los sistemas de gestión con los sistemas de control conectando así las redes de IT con las OT dentro de lo que es la Intranet de una empresa. A esta generación de SCADA se lo llama sistema MES (iniciales en inglés de Administración de Sistemas de Ejecución). Gracias a los sistemas MES se pueden conectar todas las áreas de trabajo de una empresa y gestionarla de forma integral. Los sistemas MES agregan las siguientes funcionalidades: proporcionar ordenes de producción ayudando a su eficiencia, calcular el rendimiento y buscar su eficiencia, medir y reducir los costos de producción y anticipar los posibles imprevistos y/o errores. Puede datarse el inicio de esta generación de SCADA a fines de la década de 1990.

Los sistemas SCADA de hoy integran los MES a Internet. Se corresponden con la denominada tercera generación de SCADA o SCADA basados en Internet. Se integran los SCADA con el sistema ERP (iniciales en inglés de planificación de recursos empresariales). Los SCADA de tercera generación tienen una integración total con las redes corporativas que están interconectadas con Internet. Para este nivel de integración se requiere la apertura de los SCADA lo que se manifiesta en las técnicas comunes adoptadas, plataformas, instalaciones, software, etc. En los sistemas SCADA de tercera generación, los datos en tiempo real de los sistemas de control y monitoreo se transfieren a través de Intranet o incluso Internet. Puede situarse el inicio de la tercera generación de SCADA a inicios de la década pasada (es decir a inicios de 2010).

Hoy, el concepto de Industria 4.0 propone la interconexión de los SCADA de tercera generación con otros sistemas y otras tecnologías.

8.2. Ciberseguridad en las Tecnologías de Operación

Los SCADA se diseñaron para supervisar y actuar sobre los procesos industriales. No se diseñaron para ser seguros. El aislamiento de los procesos de producción les dio por muchos años una sensación de seguridad ilusoria gracias al ocultamiento. Con el tiempo surgió la necesidad de vincularlos a la red corporativa e incluso a internet. Su interconexión dejó a los SCI expuestos a

amenazas y riesgos, lo que supone serias consecuencias. Los casos documentados de ataques a sistemas SCADA comenzaron a incrementarse significativamente desde 1998, coincidiendo con la evolución de los SCADA a su segunda generación y su interconexión con la red corporativa.

En el año 2010 las plantas nucleares de Irán fueron atacadas por un virus informático llamado Stuxnet, lo que desconcertó a analistas estratégicos de todo el mundo. La comunidad internacional mostró preocupación por la seguridad. Desde esa fecha fueron varios los ataques documentados contra sistemas SCI. Muchos de ellos pueden consultarse en las bases de datos públicas RISI y en las del SCI Cert de EEUU.

En el ámbito IT, se posee conocimientos amplios y experiencias en ciberseguridad. Se destacan las normas ISO/IEC 27000:2018 y la NIST SP800-128. Entre otras cosas, en ellas se presentan definiciones y propuestas de buenas prácticas que ayudan a evitar incidentes y/o ataques cibernéticos. Componen un ambiente completo de ciberseguridad. Se dispone también de dispositivos y equipos y su uso práctico para la defensa contra el cibercrimen: antivirus, sistemas de detección de intrusiones, firewalls, entre otros.

Sin embargo, en el ámbito OT también se dispone de amplia y completa normativa específica de ciberseguridad, entre ellas se destacan: ISO/IEC 62443 y NIST SP 800-82. Sin embargo, en OT la prioridad se centra en la disponibilidad de los sistemas, los cuales deben funcionar en forma continua. La seguridad de la información no es prioridad. Es por ello, quizás, que habiendo normativa completa y de gran calidad, sus recomendaciones no se despliegan en todo el mundo OT.

La forensia informática brinda herramientas para la identificación y el estudio de ataques informáticos. En el ámbito IT la informática forense posee varios estándares que las regula. Entre ellas: NIST SP800-86, ISO / IEC 27037:2012, ISO / IEC 27042:2015, RFC 3227, RFC 4810, RFC 4998, RFC 6283. Sin embargo, en el ambiente OT no se presenta normativa específica de Informática Forense para SCI / SCADA.

8.3. Limitaciones del uso de la forensia tradicional en los Sistemas SCADA

Con la creciente amenaza de ataques sofisticados en infraestructuras críticas, es vital que las investigaciones forenses tengan lugar inmediatamente después de un incidente de seguridad. Este trabajo presenta y propone un modelo de proceso forense SCADA estructurado para llevar

fuera de las investigaciones forenses, una discusión sobre las limitaciones del uso forense tradicional, de los procesos de investigación y los desafíos que enfrentan los investigadores forenses, además de fallas en las investigaciones existentes para proporcionar capacidad forense en los sistemas SCADA que se examinan en detalle.

8.4. Motivos para hacer un análisis forense

El análisis forense permite, mediante la utilización de software y hardware, identificar y luego verificar situaciones de fraude, visualizar funcionamiento de procesos y procedimientos, fuga de información y otros incidentes de seguridad. En este trabajo el análisis forense será utilizado para visualizar las brechas de seguridad de los sistemas industriales.

Hoy en día, el análisis forense está siendo pensado como parte del área de Seguridad de la información en las organizaciones; otras lo ofrecen como un servicio privado, ya sea como parte de un juicio o investigación. En ambos casos participan: las partes interesadas, letrados de ambas partes, Escribanos, Peritos Informáticos Forenses, Auxiliares Forenses Informáticos, entre otros.

8.4.1. Tipos de análisis forense

Existen varias modalidades para realizar un análisis forense informático, de los cuales se pueden mencionar algunos de ellos:

- Análisis Forense de Equipos de Cómputo: computadoras personales, notebooks, netbooks, memoria RAM.
- Análisis Forense de Dispositivos Móviles: teléfonos celulares, Smartphones, tablets.
- Análisis Forense de Software: software enlatado, software a medida, sistemas operativos.
- Análisis Forense de Dispositivos Extraíbles: disco rígido magnético, disco de estado sólido, pendrive, memorias flash, medios ópticos (CD, DVD, Blue Ray, Mini-Disc), medios magnéticos (Tape BackUp).
- Análisis Forense de Redes: redes alámbricas e inalámbricas.

8.4.2. Limitaciones del análisis forense para sistemas industriales

Al centrarse en las redes industriales, hoy en día no es frecuente la ejecución de un análisis forense. Uno de los motivos se debe a su funcionamiento operativo de 7x24, dado que no es posible detener el proceso de producción de la empresa.

El proceso de producción continua impide la interrupción del servidor lo cual no permite el reinicio del equipo ante la instalación de actualizaciones del sistema operativo o en su defecto la instalación de un sistema operativo más reciente. Esto hace que el sistema operativo se mantenga desactualizado y vulnerable ante cualquier tipo de ataque por parte de los ciberdelincuentes. Lo mismo sucede para los sistemas operativos que ya no cuentan con soporte por parte del fabricante. Esto también limita las actualizaciones de hardware haciendo que las mismas se vuelvan vulnerables y obsoletas permitiendo el acceso de los ciberdelincuentes.

Esta situación de no actualización del sistema operativo hace que no se puedan instalar nuevas versiones de los sistemas industriales. Lo mismo sucede al momento de la utilización de las herramientas forenses impidiendo el acceso a las herramientas más sofisticadas en lo que a tecnologías se refiere.

Otro motivo de la desactualización de hardware (no solo equipos de cómputo sino también la infraestructura) y software se debe, en ocasiones, a la negación al cambio, falta de concientización, temas económicos, entre otros, por parte de la organización.

8.5. Desarrollo Experimental

El estudio concluye con una experimentación de una arquitectura de capacidad forense SCADA propuesta en un DELTA DVP-12SP[27].

Para el desarrollo técnico de este trabajo se toma como escenario industrial o SCADA, un PLC portátil debido a las limitaciones de movilidad por la pandemia, lo cual no permite tener acceso a un escenario industrial o SCADA real.

La industria elegida para la programación del PLC es una fábrica que comercializa artículos plásticos. Para esta tarea se contó con el soporte de la empresa Trend Ingeniería[28].

[27] Sitio oficial: https://www.deltaww.com/en-us/products/PLC-Programmable-Logic-Controllers/ALL/
[28] Sitio oficial: http://www.trendingenieria.com.ar/

8.5.1. Preparación del escenario

La preparación del escenario experimental consta de varias etapas:

- Preparación y armado del tablero PLC portátil
- Instalación de Sistema Operativo Windows[29] 7 Starter
- Instalación de la aplicación Wonderware[30]
- Selección de herramientas forenses
- Programación del PLC portátil

El SCADA posee las siguientes pantallas: Carátula, Menú, Producción, Totales, CNC's, Inyectora 1, como muestra la siguiente figura.

Figura 8: Tablero Comando PLC (Fuente: Trabajo Final Romero)

El PLC habilita el funcionamiento de la inyectora para cada uno de los turnos. La siguiente figura presenta el programa del PLC (en lenguaje Ladder).

En el laboratorio, la obtención de la información se realizó en vivo (live) tanto al equipo de cómputo como a la red en base a: Características del terminal PC, red y tráfico de red y actividades del PLC.

[29] Sitio oficial: https://www.microsoft.com/es-ar/windows
[30] Sitio oficial: https://www.wonderware.es/hmi-scada/intouch/

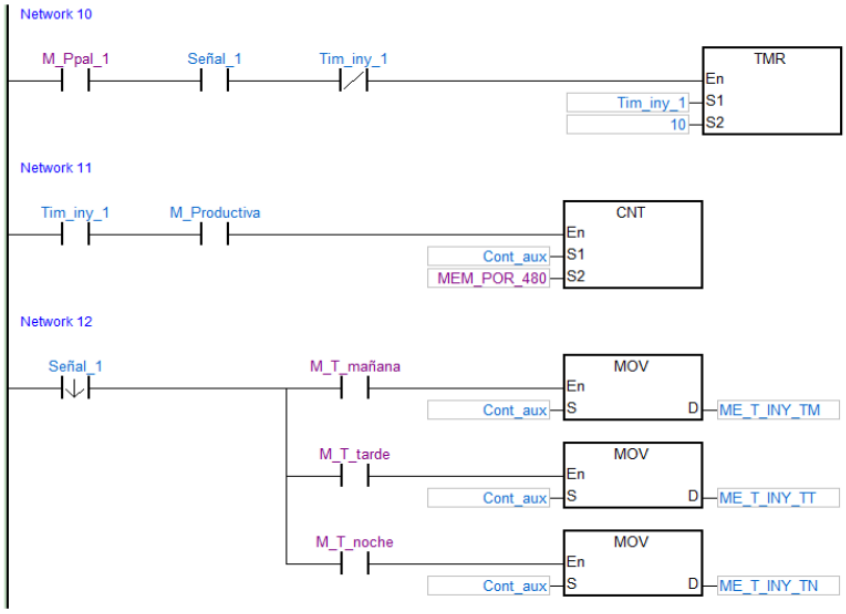


Figura 9: Circuito (Fuente: Trabajo Final Romero)

8.5.2. Sistema Operativo y Aplicaciones instaladas en Terminal SCADA

La obtención de la información se inicia con un análisis de auditoría del sistema operativo para lo cual se utilizó la aplicación WinAudit, ejecutada desde la herramienta Bento. De la misma se obtiene una completa información del equipo de cómputo. La información obtenida se refiere tanto al Sistema Operativo como otras aplicaciones instaladas, puertos de comunicaciones, entre otros.

Se presentaron los siguientes reportes:

- Vista General.
- Sistema Operativo.
- Grupos Relevantes.
- Grupos Miembro.
- Derechos de Usuarios.
- Usuarios Relevantes.
- Aplicaciones instaladas Relevantes (COMMGR 1.11, DAServer Runtime Components Upgrade, DCISoft 1.22, HWCONFIG 4.00, ISPSoft 3.10, Modicon MODBUS Plus. Sentinel Protection Installer 7.5.0, SuiteLink, Virtual COM, Wonderware Alarm2U DAServer, Wonderware Common Components, Wonderware Compact Panel DAServer. Wonderware FactorySuite Gateway,

Wonderware InTouch, Wonderware Kontron DAServer, Wonderware MBSerial DAServer, Wonderware MBTCP DAServer, Wonderware Modicon MODBUS Ethernet, WonderwareTSInfoTool, WPLSoft 2.49).

- Dispositivos de Red.
- Puertos de comunicación.
- Puertos Abiertos Relevantes.
- Tabla de Ruteo.
- Configuración de Seguridad.

En la siguiente Tabla se presenta el reporte de la aplicación “ISPSoft 3.10”.

Tabla 11: Reporte Aplicación ISPSoft 3.10 (Fuente:Trabajo Final Romero)

Item	*Value*
Name	*ISPSoft 3.10*
Vendor	*DELTA ELECTRONICS,INC.*
Version	*3.10*
Product Language	*English*
Install Date	*20200410*
Install Location	
Install Source	*C:\Users\SCADA\AppData\Local\Temp_isE30F*
Install State	*The product is installed for the current user.*
Assignment Type	*Per Machine*
Package Code	*{071AB193-12AA-45A3-A62F-AC8CE890F911}*
Package Name	*ISPSoft 3.10.msi*
Local Package	*C:\Windows\Installer\83fb2.msi*
Product ID	*None*
Registered Owner	*SCADA*
Software ID	*{8E89EEE3-D05E-4C02-B52A-A31FEABAEE9C}*

8.5.3. Análisis de Red

Para lectura del tráfico de red y captura de paquetes se utilizaron las aplicaciones NetworkTrafficViewer y SmartSnif respectivamente, ejecutadas desde Bento. Para el tráfico de red se capturan las direcciones IP de los dispositivos conectados a la red. Mientras que para la captura

de paquetes se captura el paquete de información que se transmite desde el equipo de cómputo al PLC y viceversa.

La lectura del tráfico de red, a través de la aplicación NetworkTrafficViewer, arrojó resultados satisfactorios de comunicación recíproca entre el equipo de cómputo y el PLC. Las direcciones IP del equipo de cómputo es 192.168.1.2 y el PLC es 192.168.1.5. Los reportes presentados por la aplicación son:

- Visualización de comunicación entre el equipo de cómputo y el PLC.
- Captura de paquetes de datos en modo Automático.
- Captura de paquetes de datos en modo Ascii (notar que los datos viajan en claro).
- Captura de paquetes de datos en modo Hex Dump.

En la siguiente figura se presenta la pantalla Captura de paquetes de datos en modo ASCII de NetworkTrafficViewer.

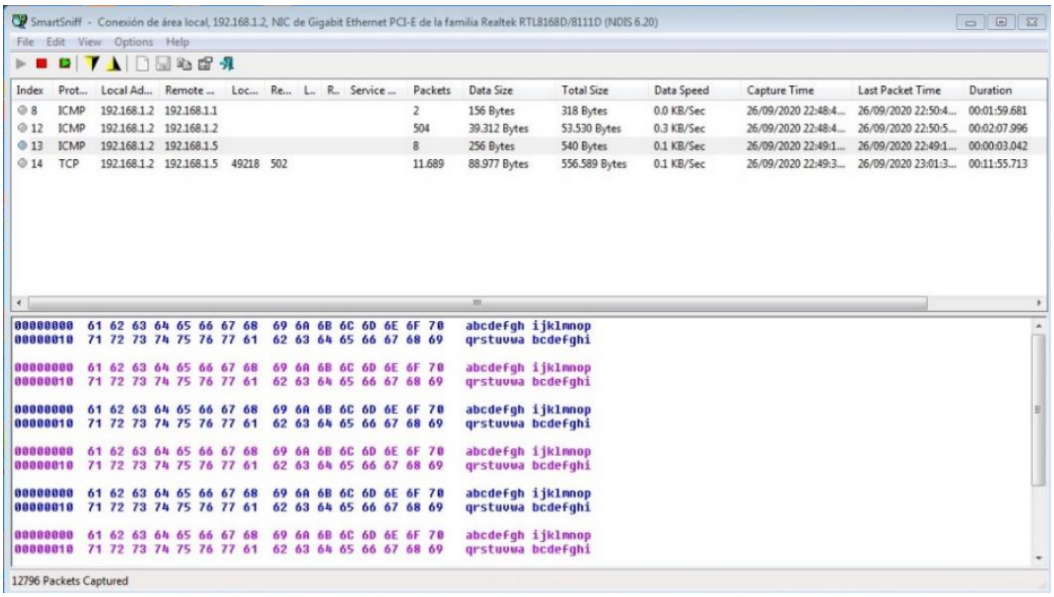


Figura 10: Captura de paquetes de datos en modo ASCII de NetworkTrafficViewer (Fuente:Trabajo Final Romero)

Observar que el mensaje “abcdefghijklmnop” viaja en claro (sin encriptar) en la red desde el SCADA hacia el PLC.

8.5.4. Huellas de los Dispositivos de Control Industrial

Para leer la trazabilidad de actividades realizadas por el PLC se utilizó la aplicación SMC de la herramienta Wonderware InTouch. En dicha aplicación se visualizan los eventos satisfactorios y no satisfactorios que ocurren en el PLC.

Las pantallas obtenidas son: Visor de Eventos de actividad del software Intouch Wonderware – Licenciamiento y Visor de Eventos de actividad del software Intouch Wonderware – Conexión.

A continuación, se presenta el Visor de Eventos de actividad del software Intouch Wonderware – Conexión.

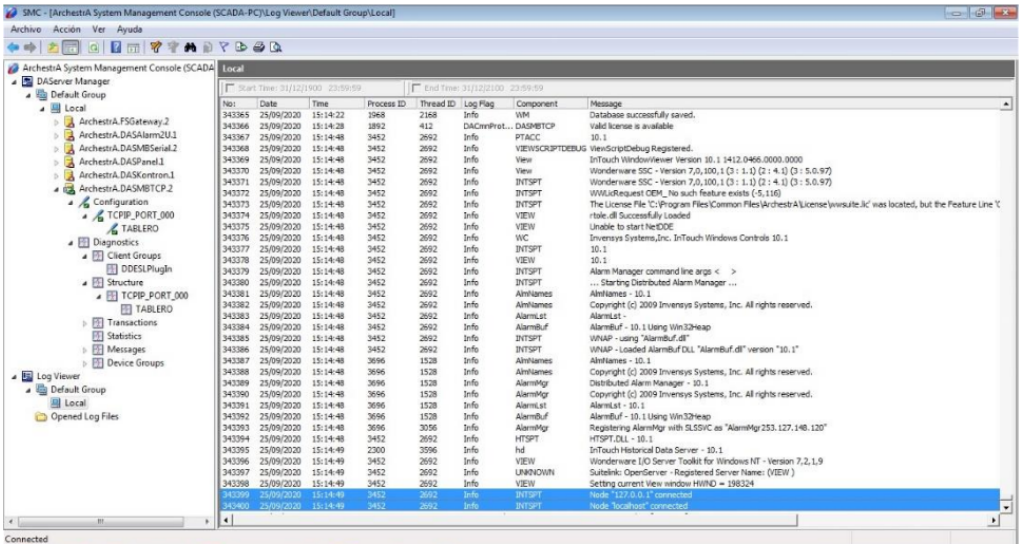


Figura 11: Visor de Eventos software InTouch Wonderware (Fuente: Trabajo Final Romero)

8.5.5. Análisis de los resultados

Para el análisis del Sistema Operativo y Aplicaciones Instaladas en el Terminal SCADA, la herramienta Bento ejecutó la aplicación WinAudit. De la misma se obtuvieron reportes con información detallada de las características del equipo, aplicaciones instaladas, usuarios y configuraciones de seguridad.

Para el caso del tráfico de red se verificó que existe comunicación recíproca entre el equipo de cómputo y el PLC. En el mismo proceso se visualizaron las direcciones IP de ambos dispositivos.

En el caso de las actividades registradas en el PLC, se puede verificar actividades que se realizaron en el PLC y se registran en el software Intouch Wonderware.

Para información detallada de los reportes se recomienda obtenerlos del trabajo de Romero donde originalmente se presentaron los resultados de esta experiencia.

8.6. Conclusiones

Con la herramienta Bento se realizó una adquisición en vivo de un SCI / SCADA en funcionamiento, sin detenerlo. De la imagen adquirida pudo obtenerse evidencias forenses tanto del terminal SCADA, de la red de comunicaciones entre el PLC y la PC con el SCADA y de las actividades del PLC registradas en la PC.

Una primera conclusión de esto es que el método de adquisición forense en vivo puede ser adecuado para adquirir evidencias de un SCI / SCADA sin necesidad de detener el funcionamiento de la planta.

Una segunda conclusión se refiere al detalle de la evidencia: si bien podría decirse que el análisis del terminal SCADA brinda información equivalente a un análisis de una adquisición fría, el resultado de los demás análisis (tráfico de red y actividad del PLC) brindan información adicional muy relevante.

9. Bibliografía

- Boletín Oficial de la República Argentina. “Definición de Infraestructuras Críticas y de Infraestructuras Críticas de Información”, 2019. https://www.boletinoficial.gob.ar/detalleAviso/primera/216860/20190918
- International Society of Automation. (n.d.). “ISA-95: Enterprise-Control System Integration”, 2000.
- International Organization for Standardization. “ISO/IEC 27001:2021 - Information technology - Security techniques - Information security management systems - Requirements.”, 2021 https://www.iso.org/standard/27001
- U.S. Department of Energy. (n.d.). “Cybersecurity Capability Maturity Model (C2M2)”. Office of Cybersecurity, Energy Security, and Emergency Response, 2022, https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2.
- MITRE. (n.d.). “MITRE ATT&CK”, 2024. https://attack.mitre.org/
- Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2022). “Guide to Industrial Control Systems (ICS) Security (NIST Special Publication 800-82 Revision 3)”, National Institute of Standards and Technology, 2023. https://csrc.nist.gov/pubs/sp/800/82/r3/final.
- International Society of Automation. (n.d.). “ISA/IEC 62443 Series of Standards”, 2018. https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.
- Instituto Nacional de Ciberseguridad de España (INCIBE). “*Guía para la Gestión de un Inventario de Activos en Sistemas de Control Industrial”*. 2020. https://www.incibe.es/sites/default/files/contenidos/guias/doc/incibe-cert_guia_inventario_de_activos_2020_v1.pdf
- Instituto Nacional de Ciberseguridad de España (INCIBE). “*Protocolos y seguridad de red en Infraestructuras SCI”*, 2017. https://www.incibe.es/sites/default/files/contenidos/guias/doc/incibe_protocolos_seguridad_red_sci.pdf
- James McCarthy et al. (2020). “Energy Sector Asset Management For Electric Utilities, Oil & Gas Industry”. NIST. Link: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-23.pdf.

- JOINT TASK FORCE (2018). “Risk Management Framework for Information Systems and Organizations”. NIST. Link: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.
- Cai, N., Wang, J., & Yu, X. (2008, July). SCADA system security: Complexity, history and new developments. In 2008 6th IEEE International Conference on Industrial Informatics (pp. 569-574). IEEE.
- WICC – 2019: Kamlofsky, Jorge, et al. "Ciberseguridad en los sistemas de control industrial: clave para la ciberdefensa de las infraestructuras críticas." XXI Workshop de Investigadores en Ciencias de la Computación (WICC 2019, Universidad Nacional de San Juan), 2019.
- Mardones, Hernán Díaz. "Infraestructura crítica vulnerable a la ciberguerra." En “La Ciberguerra: Sus Impactos y Desafíos”. Centro de Estudios Estratégicos del Ejército de Chile, 2018.
- TREND Micro: “Mirada sobre los ciberataques en la industria del Gas y petróleo”. Diciembre 2019 - https://www.trendmicro.com/vinfo/es/security/news/internet-of-things/drilling-deep-a-look-at-cyberattacks-on-the-oil-and-gas-industry
- P. Binnar, A. Dalvi, S. Bhirud and F. Kazi, "Cyber Forensic Case Study of Waste Water Treatment Plant". 2021 IEEE Bombay Section Signature Conference (IBSSC), (2021), pp. 1-5, doi: https://doi.org/10.1109/IBSSC53889.2021.9673346.
- Karabiyik, Umit, et al. "Forensic analysis of scada/ics system with security and vulnerability assessment." 2018 ASEE Annual Conference & Exposition, (2018).
- Di Iorio, Ana Haydée, et al. "El rastro digital del delito: Aspectos técnicos, legales y estratégicos de la informática forense." (2017).
- Mahesh Kolhe et al. “Live Vs Dead Computer Forensic Image Acquisition”. International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 8 (3), (2017), 455-457.
- Abdullah, Haris Iskandar Mohd, et al. "Digital Forensics Investigation Procedures of Smart Grid Environment." International Journal of Computing and Digital System. Vol 11, No.1, (2021). DOI: https://dx.doi.org/10.12785/ijcds/110186
- Romero Raul Oscar. “Informática Forense, Seguridad y Estándares en Sistemas Industriales e Infraestructuras Críticas”, (2021).
- Control para la Industria S.A. “¿Porqué 4 – 20 mA?”. En línea: https://www.cpi.com.ar/notas/por-que-4-20-ma/. Consultado 01/07/2022.

- Copa Roman. “Entradas digitales en equipo de control industrial”. Blog Coparoman, (2019). En línea: https://coparoman.blogspot.com/2019/08/entradas-digitales-en-equipo-de-control.html. Consultado: 01/07/2022.
- Blog Enerxia. “Automatismos: Partes de un PLC - Salidas digitales”. En linea: https://www.enerxia.net/portal/index.php/i-auto/941-automatismos-partes-de-un-plc-salidas-digitales. Consultado: 09/07/2022.
- Industrias GSL. “Qué es un PLC y cómo funciona”, (2021). En línea: https://industriasgsl.com/blogs/automatizacion/que-es-un-plc-y-como-funciona. Consultado: 09/07/2022.
- Bernard Cubizolles. “Everything You Need to Know about HMI / SCADA”, (2020). En línea: https://www.ge.com/digital/blog/everything-you-need-know-about-hmi-scada. Consultado: 10/07/2022.
- Modbus Organization. “Modbus News”, (2022). En línea: https://modbus.org/. Consultado: 01/08/2022.
- Nexus Integra. “MES vs SCADA en la Industria 4.0”. En línea: https://nexusintegra.io/es/mes-vs-scada/. Consultado el 01/08/2022.

10. ANEXO I: Detalles de Amenazas

Tabla 12: Vínculo entre identificador y tipo de ataque (Fuente: Elaboración propia)

	Ataques físicos a equipos (AFE)
AFE01	Control de ingreso y egreso a la planta
AFE02	Control de ingreso de dispositivos
AFE03	Control de ubicación física del activo
	Ataques a procesos (AP)
AP01	Acceso a recursos por parte de empleados o terceros
AP02	Gestión de activos, inventario, configuración y comportamiento
AP03	Definición de procesos asociados a visualización y análisis de flujos de datos para detectar eventos
AP04	Personal con roles específicos en ciberseguridad
AP05	Respuesta ante incidentes y simulaciones de ataque
AP06	Auditorías en Seguridad Informática en la organización
AP07	Planes de resguardo de la info.
AP08	Políticas de claves en sistemas y dispositivos
	Ataques a protocolos de comunicación (APC)
APC01	Diseño de redes
APC02	Gestión de redes
APC03	Acceso remoto a dispositivos
APC04	Detección de tráfico de red anómalo
APC05	Protocolos de cifrado de las comunicaciones
	Ataque al sistema operativo (AS)
ASO01	Estado de actualización del software
ASO02	Estado de software EDR de los dispositivos
	Ataque a las aplicaciones s/sistema operativo (AAS)
AAS01	Aplicaciones web de la organización
	Ataque a las personas (APP)
APP01	Identidad Digital
APP02	Capacitación del personal de la organización sobre uso responsable de nuevas tecnologías

Tabla 13: Detalle completo de amenazas (Fuente: Elaboración Propia)

Cod. categoría Amenaza	***Realizar reconocimiento y recopilar información.***	***Descripción***
APC01, APC03	Realizar el reconocimiento/escaneo de la red perimetral.	Un adversario utiliza software comercial o gratuito para escanear perímetros organizacionales y así obtener una mejor comprensión de la infraestructura de tecnología de la información y mejorar la probabilidad de lanzar ataques exitosos.
APC02, APC05	Realizar el análisis de tráfico de redes expuestas.	Un adversario con acceso a canales de datos cableados o inalámbricos expuestos utilizados para transmitir información utiliza el análisis de la red para identificar componentes, recursos y protecciones.
APC03, AAS01	Recopilar información utilizando el descubrimiento de información de código abierto de información organizacional.	Un adversario busca información públicamente accesible para recopilar datos sobre sistemas de información organizacional, procesos comerciales, usuarios o personal, o relaciones externas que el adversario puede emplear posteriormente en apoyo de un ataque.
AAS01	Realizar el reconocimiento y la vigilancia de las organizaciones específicas.	Un adversario utiliza diversos medios (por ejemplo, escaneo, observación física) para examinar y evaluar las organizaciones y determinar puntos de vulnerabilidad.
AP01, APP01	Realizar un reconocimiento interno dirigido por malware.	Un adversario utiliza malware instalado dentro del perímetro organizacional para identificar objetivos potenciales. Debido a que el escaneo, descubrimiento u observación no cruza el perímetro, no se detecta mediante sistemas de detección de intrusos colocados externamente.
	Crear herramientas de ataque.	***Descripción***
APP01, APP02	Ataques de phishing.	El adversario falsifica las comunicaciones de una fuente legítima/confiable para adquirir información confidencial, como nombres de usuario, contraseñas o SSN. Los ataques típicos ocurren por correo electrónico, mensajes instantáneos o medios similares; Comúnmente dirige a los usuarios a sitios web que parecen ser sitios legítimos, al tiempo que roban la información ingresada.
APP01, APP02	Ataques de spear phishing.	El adversario emplea ataques de phishing dirigidos a

		objetivos de alto valor (por ejemplo, líderes/ejecutivos superiores).
ASO01, ASO02	Ataques específicamente basados en el entorno de tecnología de la información implementado.	El adversario desarrolla ataques (por ejemplo, diseña malware dirigido) que aprovechan su conocimiento sobre el entorno de tecnología de la información organizacional.
APP02	Crear sitio web falsificado.	El adversario duplica sitios web legítimos; Cuando los usuarios visitan un sitio falsificado, el sitio puede recopilar información o descargar malware.
APC05	Crear certificados falsificados.	El adversario falsifica o compromete una autoridad de certificado, para que el malware o las conexiones parezcan legítimas.
APP01, APP02	Crear y operar organizaciones falsas para inyectar componentes maliciosos en la cadena de suministro.	El adversario crea organizaciones falsas con la apariencia de proveedores legítimos en el camino crítico del ciclo de vida para luego inyectar componentes del sistema de información corrupto/malicioso en la cadena de suministro organizacional.
	Entregar/insertar/instalar capacidades maliciosas.	***Descripción***
APP02	Entregar malware conocido a los sistemas de información organizacional interna.	El adversario utiliza mecanismos de entrega comunes (por ejemplo, correo electrónico) para instalar/insertar malware conocido (por ejemplo, malware cuya existencia es conocida) en los sistemas de información organizacional.
APP02	Entregar malware modificado a los sistemas de información organizacional internos.	El adversario utiliza mecanismos de entrega más sofisticados que el correo electrónico (por ejemplo, tráfico web, mensajería instantánea, FTP) para entregar malware y posiblemente modificaciones de malware conocido para obtener acceso a los sistemas de información organizacional interna.
APP02, ASO01	Entregar malware dirigido para el control de sistemas internos y exfiltración de datos.	El adversario instala malware que está específicamente diseñado para tomar el control de los sistemas de información organizacional interna, identificar información confidencial, exfiltrar la información al adversario y ocultar estas acciones.
ASO02	Entregar malware a través de medios extraíbles.	El adversario distribuye estratégicamente diversos medios extraíbles (por ejemplo, pendrives) que contienen malware dentro de ubicaciones externas a perímetros físicos organizacionales, pero donde es

		probable que los empleados encuentren los mismos (por ejemplo, estacionamiento de las instalaciones, casillas perimetrales, salas de conferencias, baños, etc.) y asi los introduzcan dentro de los sistemas de información y/o la Red de la empresa.
ASO02, AAS01	Insertar el malware no dirigido en software descargable y/o en productos de tecnología de información comercial.	El adversario corrompe o inserta malware en productos comunes de Freeware, Shareware o Tecnología de la Información Comercial. El adversario no está dirigiendo el ataque a organizaciones específicas, simplemente buscando puntos de entrada en los sistemas de información organizacional interna. Tenga en cuenta que esto es particularmente una preocupación para las aplicaciones móviles.
ASO01, ASO02, AAS01	Insertar el malware dirigido en los sistemas de información organizacional y los componentes del sistema de información.	El adversario inserta malware en sistemas de información organizacional y componentes del sistema de información (por ejemplo, productos de tecnología de información comercial), específicamente dirigido al hardware, el software y el firmware utilizados por las organizaciones (basados en el conocimiento adquirido a través del reconocimiento).
ASO01, ASO02	Insertar el malware especializado en los sistemas de información organizacional en función de las configuraciones del sistema.	El adversario inserta malware especializado, no detectable, en los sistemas de información organizacional basados en configuraciones del sistema, específicamente dirigidos a componentes del sistema crítico de información basados en el reconocimiento y la ubicación dentro de los sistemas de información organizacional.
AFE02	Insertar hardware falsificado o manipulado en la cadena de suministro.	El adversario intercepta hardware de proveedores legítimos. El adversario modifica el hardware o lo reemplaza con hardware defectuoso.
AP01, AP02	Insertar componentes críticos manipulados en los sistemas organizacionales.	El adversario reemplaza, a través de la cadena de suministro, sabotaje interno o alguna combinación de los mismos, componentes del sistema de información crítica con componentes modificados o corruptos.
APC04	Instalar los bisijos de uso general en sistemas o redes de información controlados por la organización.	El adversario instala software de análisis en redes o sistemas de información organizacional interna.
APC04, APC05	Instalar los sniffers persistentes y dirigidos en los sistemas y redes de información organizacional.	El adversario se ubica dentro de los sistemas de información o redes de información organizacional interna diseñada para (durante un período continuo

		de tiempo) recopilar el tráfico de red (sniff).
	Explotación y compromiso.	***Descripción***
AFE01, AP01	Explotar el acceso físico del personal autorizado para obtener acceso a las instalaciones de la organización.	El adversario sigue a las personas autorizadas en ubicaciones seguras/controladas con el objetivo de obtener acceso a las instalaciones, eludiendo los controles de seguridad física, táctica conocida como tailgating.
AAS01	Explote sistemas de información mal configurados o no autorizados expuestos a Internet.	El adversario gana acceso a través de Internet a sistemas de información que no están autorizados para la conectividad a Internet o que no cumplen con los requisitos de configuración organizacional.
AFE02, APC03	Explotación de split tunneling	El adversario aprovecha los sistemas de información organizacionales o personales externos (por ejemplo, computadoras portátiles en ubicaciones remotas) que se conectan simultáneamente de forma segura a sistemas o redes de información organizacional y a conexiones remotas no seguras.
APC03	Explotar multi-tenancy en un entorno de la nube.	El adversario, con procesos ejecutándose en un entorno en la nube de uso organizacional, aprovecha el multi-tenant para observar el comportamiento de los procesos organizacionales, adquirir información organizacional o interferir con el funcionamiento oportuno o correcto de los procesos organizacionales.
ASO01	Explotar vulnerabilidades conocidas en sistemas móviles (por ejemplo, computadoras portátiles, tablets, teléfonos inteligentes).	El adversario aprovecha el hecho de que los sistemas de información transportables están fuera de la protección física de las organizaciones y la protección lógica de los firewalls corporativos, y compromete los sistemas en función de las vulnerabilidades conocidas para recopilar información de esos sistemas.
ASO01	Explotar vulnerabilidades descubiertas recientemente.	El adversario aprovecha las vulnerabilidades descubiertas recientemente en los sistemas de información organizacional en un intento de comprometer los sistemas antes de que estén disponibles medidas de mitigación o aplicadas.
ASO01	Explotar vulnerabilidades en sistemas de información organizacional interna.	El adversario busca vulnerabilidades conocidas en sistemas de información interna organizacional y explota esas vulnerabilidades.
ASO01	Explotar vulnerabilidades utilizando ataques de día cero.	El adversario emplea ataques que explotan vulnerabilidades aún no publicitadas. Los ataques de

		día cero se basan en la perspectiva del adversario sobre los sistemas de información y las aplicaciones utilizadas por las organizaciones, así como el reconocimiento de las organizaciones realizado por el adversario.
ASO01	Explotar las vulnerabilidades en los sistemas de información relacionados con la misión y operaciones comerciales.	El adversario lanza ataques a las organizaciones de manera consistente con las necesidades de la organización para llevar a cabo sus operaciones de negocio.
APC03	Explotar la eliminación de datos insegura o incompleta en un entorno multi-tenant.	El adversario obtiene información no autorizada debido a la eliminación de datos de manera insegura o incompleta en un entorno multi-tenant (por ejemplo, en un entorno de computación en la nube).
APC01	Comprometer el aislamiento en el entorno múltiple.	El adversario evita o burla los mecanismos de aislamiento en un entorno multi-tenant (por ejemplo, en un entorno de computación en la nube) para observar, corromper o negar el servicio a los servicios e información/datos alojados.
AFE01, AFE02	Comprometer los sistemas de información crítica a través del acceso físico.	El adversario obtiene acceso físico a los sistemas de información organizacional y realiza modificaciones.
ASO02	Comprometer los sistemas o dispositivos de información utilizados externamente y reintroducirlos en la empresa.	El adversario instala malware en sistemas o dispositivos de información, mientras los sistemas/dispositivos están fuera de las organizaciones a los efectos de infectar posteriormente las organizaciones cuando se vuelven a conectar.
ASO02	Comprometer el software de los sistemas de información crítica organizacional.	El adversario inserta malware o corrompe los sistemas críticos de información organizacional interna.
ASO02	Comprometer los sistemas de información organizacional para facilitar la exfiltración de datos/información.	El adversario implanta malware en sistemas de información organizacional interna, donde el malware con el tiempo puede identificar y luego exfiltrar información valiosa.
AP02	Compromiso de información de misión crítica.	El adversario compromete la integridad de la información de misión crítica, evitando así la capacidad de las organizaciones a las que se proporciona información, para llevar a cabo operaciones.
AFE01, AFE02	Comprometer el diseño, fabricación y/o distribución de componentes del sistema de información (incluidos hardware, software y firmware).	El adversario compromete el diseño, fabricación y/o distribución de componentes del sistema de información crítica en proveedores seleccionados.

	Realizar un ataque (es decir, herramientas o actividades de ataque directas/coordinadas).	***Descripción***
APC02, APC04, APC05	Realizar ataques de intercepción de comunicaciones.	El adversario aprovecha las comunicaciones que no están cifradas o usan cifrado débil (por ejemplo, cifrado que contiene defectos públicamente conocidos), tiene como blanco esas comunicaciones y gana acceso a la información transmitida y canales.
APC02, APC04	Realizar ataques inalámbricos de interferencia.	El adversario toma medidas para interferir con las comunicaciones inalámbricas para impedir o evitar que las comunicaciones lleguen a los receptores previstos.
APC02, APC04	Realizar ataques utilizando puertos, protocolos y servicios no autorizados.	El adversario realiza ataques utilizando puertos, protocolos y servicios para ingreso y salida que no están autorizados para el uso de las organizaciones.
APC02, APC04	Realizar ataques que aprovechan el movimiento del tráfico/datos permitidos en todo el perímetro.	El adversario utiliza los flujos de información permitidos (por ejemplo, comunicación por correo electrónico, almacenamiento extraíble) para comprometer los sistemas de información interna, lo que permite al adversario obtener y exfiltrar información confidencial a través de los perímetros.
APC02, APC04	Realizar un ataque de denegación simple de servicio (DOS).	El adversario intenta hacer que un recurso accesible a través de Internet, no esté disponible para los usuarios previstos, o evitar que el recurso funcione de manera eficiente, temporalmente o indefinidamente.
APC02, APC04	Realizar ataques de denegación distribuida de servicio (DDoS).	El adversario utiliza múltiples sistemas de información comprometidos para atacar un objetivo único, lo que provoca la denegación del servicio para los usuarios de los sistemas de información específicos.
APC02, APC04	Realizar ataques de denegación de servicio (DOS) dirigidos.	El adversario dirige ataques de DOS a sistemas de información críticos, componentes o infraestructuras de soporte, basadas en el conocimiento adversario de las dependencias.
AFE01	Realizar ataques físicos en instalaciones organizativas.	El adversario realiza un ataque físico contra las instalaciones organizativas (por ejemplo, genera un incendio).
AFE01	Realizar ataques físicos contra infraestructuras que respaldan las instalaciones organizativas.	El adversario realiza un ataque físico contra una o más infraestructuras que respaldan las instalaciones

		de la organización (por ejemplo, rompe una cañería de agua, corta una línea eléctrica).
AFE02, APC03	Realizar ataques ciber-físicos en instalaciones organizativas.	El adversario lleva a cabo un ataque ciber-físico contra las instalaciones organizativas (por ejemplo, cambia de forma remota a la configuración de HVAC).
APC02, APC04	Realizar ataques de recolección de datos en un entorno de nube.	El adversario obtiene datos utilizados y luego eliminados por procesos organizacionales que se ejecutan en un entorno en la nube.
AP08	Realizar intentos de inicio de sesión utilizando ataques de fuerza bruta.	El adversario intenta obtener acceso a los sistemas de información organizacional mediante pruebas aleatorias o sistemáticas de contraseñas, posiblemente soportadas por las utilidades de cracking de contraseña.
ASO01	Realizar ataques de día cero no dirigidos.	El adversario emplea ataques que explotan hasta ahora vulnerabilidades no publicitadas. Los ataques no se basan en ninguna información que el adversario posea sobre vulnerabilidades específicas de las organizaciones.
AAS01	Realizar el secuestro de sesiones externamente.	El adversario toma el control de sesiones de sistemas de información legítimas, ya establecidas entre organizaciones y entidades externas (por ejemplo, usuarios que se conectan desde ubicaciones fuera de la organización). Esto se conoce como hijacking.
AAS01	Realizar el secuestro de sesiones internamente.	El adversario coloca una entidad dentro de las organizaciones para obtener acceso a sistemas o redes de información organizacional con el propósito expreso de tomar el control (hijackig) de una sesión legítima ya establecida entre organizaciones y entidades externas (por ejemplo, usuarios que se conectan desde ubicaciones remotas) o entre dos ubicaciones dentro de las redes internas.
APC02, APC04	Realizar ataques de modificación de tráfico de red externamente (man in the middle).	El adversario, operando fuera de los sistemas organizacionales, intercepta/escucha sesiones entre sistemas organizacionales y externos. El adversario luego transmite mensajes en medio de esa comunicación, haciéndoles creer que están hablando directamente entre sí a través de una conexión privada, cuando, de hecho, la comunicación completa está controlada por el adversario. Tales ataques son de particular

		preocupación por el uso organizacional de nubes comunitarias, híbridas y públicas.
APC02, APC04	Realizar ataques de modificación de tráfico de red internamente (man in the middle).	El adversario operando dentro de la infraestructura organizacional, intercepta y corrompe las sesiones de datos.
APP01	Ingeniería social realizada por personas externas a la organización para obtener información.	El adversario colocado externamente toma acciones (por ejemplo, usar correo electrónico, teléfono) con la intención de persuadir o engañar a las personas dentro de las organizaciones para que revelen información crítica/confidencial (por ejemplo, información de identificación personal).
APP01	Ingeniería social realizada por personas internas de la organización para obtener información.	El adversario colocado internamente toma acciones (por ejemplo, usar correo electrónico, teléfono) para que las personas dentro de las organizaciones revelen información crítica/confidencial (por ejemplo, información de misión crítica).
AP01, ASO02	Realizar ataques orientados a comprometer dispositivos personales de empleados críticos.	El adversario ataca a los empleados claves de la organización colocando malware en sus sistemas y dispositivos de información de propiedad personal (por ejemplo, computadoras portátiles/portátiles, asistentes digitales personales, teléfonos inteligentes). La intención es aprovechar cualquier instancia en la que los empleados usen sistemas o dispositivos de información personal para manejar información crítica/confidencial.
ASO02	Realizar ataques de cadena de suministro dirigidos y explotando hardware crítico, software o firmware.	El adversario ataca y compromete el funcionamiento del software (por ejemplo, a través de inyecciones de malware), firmware y hardware que realiza funciones críticas para las organizaciones. Esto se logra en gran medida como ataques de la cadena de suministro en sistemas y componentes de información personalizados y comerciales.
	Lograr resultados (es decir, causar impactos adversos, obtener información)	***Descripción***
APC02, APC05	Obtener información confidencial a través del análisis de tráfico de redes externas.	El adversario con acceso a canales de datos cableados o inalámbricos expuestos que las organizaciones (o personal organizacional) usan para transmitir información (por ejemplo, quioscos, redes inalámbricas públicas) intercepta las comunicaciones.

ASO02	Obtener información confidencial a través de la exfiltración.	El adversario dirige el malware en los sistemas organizacionales para ubicar y transmitir de manera oculta información confidencial.
APC02, APC04, ASO02	Causar degradación o denegación de los servicios o capacidades seleccionadas por los atacantes.	El adversario dirige el malware sobre los sistemas organizacionales para afectar el correcto y oportuno soporte de las funciones de misión crítica/negocio organizacional.
AFE01, AP01	Causar deterioro/destrucción de componentes y funciones del sistema de información crítica.	El adversario destruye o causa el deterioro de los componentes del sistema de información crítica para impedir o eliminar la capacidad de la organización para llevar a cabo sus misiones o funciones comerciales. La detección de esta acción no es una preocupación.
AAS01	Causar pérdida de integridad mediante la creación, eliminación y/o modificación de datos en sistemas de información accesibles públicamente (por ejemplo, modificación no autorizada a un sitio web).	El adversario vandaliza, o realiza cambios no autorizados en sitios web organizacionales o datos en sitios web.
AP01, AP02	Causar pérdida de integridad al contaminar o corromper datos críticos.	El adversario implanta datos corruptos e incorrectos en datos críticos, lo que resulta en acciones poco óptimas o pérdida de confianza en los datos/servicios organizacionales.
AP01, AP02	Causar pérdida de integridad al inyectar datos falsos pero creíbles en los sistemas de información organizacional.	El adversario inyecta datos falsos pero creíbles en los sistemas de información organizacional, lo que resulta en acciones poco óptimas o pérdida de confianza en los datos/servicios organizacionales.
APP02	Causar divulgación de información crítica y/o confidencial por parte de usuarios autorizados.	El adversario induce (por ejemplo, a través de la ingeniería social) a los usuarios autorizados a exponer, divulgar o manejar información crítica/confidencial de forma inadvertida.
AP02	Causar divulgación y/o falta de disponibilidad al exponer de manera no autorizada información confidencial.	El adversario contamina los sistemas de información organizacional (incluidos los dispositivos y las redes) al hacer que manejen información de una clasificación/sensibilidad para la cual no han sido autorizados. La información está expuesta a las personas que no tienen autorizado el acceso a dicha información, y el sistema de información, el dispositivo o la red no están disponibles, mientras la divulgación se investiga y mitiga.
APC02	Obtener información mediante intercepción externa de la red inalámbrica.	El adversario intercepta las comunicaciones organizacionales sobre las redes inalámbricas. Los ejemplos incluyen atacar el acceso público inalámbrico o conexiones de redes de hoteles, y la

		toma de control de los enrutadores inalámbricos del hogar u organizacionales.
AP01	Obtener acceso no autorizado.	El adversario con acceso autorizado a sistemas de información organizacional, gana acceso a recursos que exceden la autorización.
AAS01	Obtener información confidencial públicamente	El adversario escanea o extrae información sobre servidores y páginas web accesibles públicamente con la intención de encontrar información confidencial.
AFE03	Obtener información robando o buscando en los sistemas/componentes de información de manera oportunista.	El adversario roba sistemas o componentes de información (por ejemplo, laptops, medios de almacenamiento de datos) que se dejan desatendidos fuera de los perímetros físicos de las organizaciones, o buscan componentes desechados.
	Mantener una presencia o conjunto de capacidades.	***Descripción***
ASO02	Ofuscar/ocultar acciones de los adversarios.	El adversario toma medidas para inhibir la efectividad de los sistemas de detección de intrusos o las capacidades de auditoría dentro de las organizaciones.
AP06	Adaptar los ataques cibernéticos basados en la vigilancia detallada.	El adversario adapta el comportamiento en respuesta a la vigilancia y las medidas de seguridad organizacional.
	Coordinar una campaña.	***Descripción***
ASO02	Coordinar una campaña de ataques múltiples (por ejemplo, hopping).	El adversario mueve el origen de la ejecución de comandos o acciones maliciosas de un sistema de información comprometido a otro, lo que dificulta el análisis.
AFE01	Coordinar una campaña que combina ataques internos y externos en múltiples sistemas de información y tecnologías de información.	El adversario combina ataques que requieren presencia física dentro de las instalaciones organizacionales y los métodos cibernéticos para lograr el éxito. Los pasos de ataque físico pueden ser tan simples como convencer al personal de mantenimiento de que deje las puertas o los gabinetes abiertos.
	Coordinar campañas en múltiples organizaciones para adquirir información específica o lograr el resultado deseado.	El adversario no limita la planificación para atacar una organización. El adversario observa múltiples organizaciones para adquirir la información necesaria sobre los objetivos de interés.
ASO02	Coordinar una campaña que extienda los ataques	El adversario utiliza la presencia existente dentro de

	entre los sistemas organizacionales.	los sistemas organizacionales para extender el alcance de control a otros sistemas organizacionales, incluida la infraestructura organizacional. Por lo tanto, el adversario está en posición de socavar aún más la capacidad de la organización para llevar a cabo misiones críticas/funciones comerciales.
AP01	Coordinar una campaña de ataques cibernéticos continuos, adaptativos y cambiantes basados en una vigilancia detallada.	El ataque del adversario cambia continuamente en respuesta a las medidas de vigilancia y seguridad organizacional.
	Coordinar los ataques cibernéticos utilizando vectores de ataque externos (externos), internos (internos) y de la cadena de suministro (proveedor).	El adversario emplea ataques continuos y coordinados, potencialmente utilizando los tres vectores de ataque con el fin de impedir las operaciones organizacionales.
	Eventos de amenaza no generadas por un adversario	***Descripción***
APP02	Divulgar Información confidencial	El usuario autorizado contamina erróneamente un dispositivo, un sistema de información o una red colocando en él o enviando información de una clasificación/sensibilidad que no ha sido autorizada a manejar. La información está expuesta al acceso por personas no autorizadas y, como resultado, el dispositivo, el sistema o la red no están disponibles mientras la divulgación se investiga y mitigan.
APP02	Mala gestión de la información crítica y/o confidencial por usuarios autorizados	El usuario privilegiado y autorizado expone inadvertidamente información crítica/confidencial.
AP02, APP02	Configuración incorrecta de privilegios	El usuario o administrador privilegiado y autorizado asigna erróneamente a un usuario privilegios excepcionales o establece requisitos de privilegio en un recurso demasiado bajo.
AP05	Degradación de comunicaciones	El rendimiento de las comunicaciones es degradado debido a las acciones de contención.
AP02	Pantalla ilegible	Pantalla ilegible debido a la antigüedad del equipamiento.
AFE	Terremoto en la instalación primaria	El terremoto de la magnitud definida por la organización en la instalación primaria hace que la instalación sea inoperable.
AFE	Incendio en la instalación primaria	El fuego (no debido a la actividad de un adversario) en la instalación primaria hace que la instalación sea inoperable.
AFE	Incendio en la instalación de respaldo	El fuego (no debido a la actividad de un adversario) en

		la instalación de respaldo hace que la instalación sea inoperable o destruye las copias de seguridad de software, configuraciones, datos y/o registros.
AFE	Inundación en la instalación primaria	La inundación (no debido a la actividad de un adversario) en la instalación primaria hace que la instalación sea inoperable.
AFE	Inundación en la instalación de respaldo	La inundación (no debido a la actividad de un adversario) en la instalación de respaldo hace que la instalación sea inoperable o destruya las copias de seguridad de software, configuraciones, datos y/o registros.
AFE	Huracán/Tornado en la instalación primaria	El huracán de la fuerza definida por la organización en la instalación primaria hace que la instalación sea inoperable.
AFE	Huracán/Tornado en la instalación de respaldo	El huracán de la fuerza definida por la organización en la instalación de respaldo hace que la instalación sea inoperable o destruye copias de seguridad de software, configuraciones, datos y/o registros.
AP02, AP05	Falta de recursos	Degradación del rendimiento del procesamiento debido al agotamiento de los recursos.
ASO01	Introducción de vulnerabilidades en productos de software	Debido a las debilidades inherentes en los lenguajes de programación y los entornos de desarrollo de software, los errores y las vulnerabilidades se introducen en productos de software de uso común.
AP07	Error de disco	Almacenamiento corrupto debido a un error de disco.
AP07, AP02	Error de disco generalizado	Errores de disco múltiples debido a la antigüedad de un conjunto de dispositivos, todos adquiridos al mismo tiempo, del mismo proveedor.

11. Glosario

11.1. Términos usados popularmente en tecnología

RFC: Es una sigla en inglés (Request For Comments) que significa requerimiento de comentarios, o comentarios requeridos. Se trata de un documento que puede ser escrito por cualquier persona y que contiene una propuesta para una nueva tecnología, información acerca del uso de tecnologías y/o recursos existentes, propuestas para mejoras de tecnologías, proyectos experimentales y demás. Las RFC (pronúnciese "erre-efecé") conforman básicamente la documentación de protocolos y tecnologías de Internet, habiéndose convertido muchas de ellas en estándares. Las mismas son mantenidas por el IETF (Internet Engineering Task Force) y son accesibles por cualquier persona ya que son publicadas de manera online y sin restricciones. Pueden consultarse las mismas en la página de búsqueda de RFCs del IETF.

WWW: Es un sistema de distribución y publicación de documentos de hipertexto interconectados y accesibles a través de Internet. Con un navegador web, un usuario visualiza sitios web compuestos de páginas web que pueden contener textos, imágenes, vídeos u otros contenidos multimediales y navega a través de esas páginas usando enlaces de hipertexto que lo llevan directamente a otras páginas en el mismo sitio u otros. Conocida como "la web", debe su nombre a la sigla de World Wide Web, que en español podemos entender como la telaraña a lo largo del mundo.

GPS: Es la denominación del Sistema de Posicionamiento Global (en inglés, *GPS*; Global Positioning System). Es un sistema que permite determinar en la posición de cualquier objeto dentro del planeta Tierra (una persona, un vehículo o un móvil) con una precisión de hasta centímetros aunque lo habitual son algunos metros de precisión. El sistema fue desarrollado, instalado y empleado por el Departamento de Defensa de los EEUU. Funciona mediante una red de como mínimo 24 satélites en órbita sobre la Tierra, con órbitas distribuidas tal que en todo momento haya al menos 4 satélites visibles en cualquier punto de la tierra. El receptor que se utiliza localiza automáticamente un mínimo de cuatro satélites de la red y con ello obtiene su posición en el planeta. A este proceso se lo denomina geo localización.

Bluetooth: Creado por Bluetooth Special Interest Group, Inc. es un sistema inalámbrico de conectividad entre objetos que posibilita la transmisión de voz y datos entre diferentes dispositivos por un enlace por radiofrecuencia. Los principales objetivos que se pretenden conseguir con esta norma son facilitar las comunicaciones entre equipos móviles, eliminar los cables y conectores y ofrecer la posibilidad de crear pequeñas redes inalámbricas y facilitar la sincronización de datos entre equipos personales. Los dispositivos que con mayor frecuencia utilizan esta tecnología son los teléfonos móviles, las computadoras portátiles, las impresoras, los altavoces inalámbricos y cámaras digitales entre otros.

Arduino: Es una compañía de desarrollo de software y hardware libre y una comunidad internacional que diseña y manufactura placas de desarrollo de hardware para construir dispositivos digitales y dispositivos interactivos. Su objeto es el de acercar y facilitar el uso de la electrónica y programación de sistemas embebidos en proyectos multidisciplinarios. Los diseños de estas placas usan diversos microcontroladores y microprocesadores. El proyecto Arduino tiene sus orígenes en el proyecto Wiring, el cual surge por el año 2003 como una herramienta para estudiantes en el Interaction Design Institute Ivrea en Ivrea, Italia, con el objetivo de proporcionar una forma fácil y económica de que principiantes y profesionales crearan dispositivos que pudieran interactuar con su entorno mediante sensores y actuadores. El nombre *Arduino* viene de un bar en Ivrea, Italia; en donde algunos de los fundadores del proyecto solían reunirse. El bar fue nombrado en honor a Arduino de Ivrea, quien fue el margrave de la Marcha de Ivrea y Rey de Italia desde el año 1002 hasta el año 1014.

Raspberry: Se trata de una computadora de placa única u ordenador de placa simple de bajo costo, desarrollado en el Reino Unido por la Raspberry Pi Foundation, con el objetivo de estimular la enseñanza de informática en las escuelas. El modelo original se convirtió en más popular de lo que se esperaba, hasta incluso vendiéndose afuera del mercado objetivo para usos como robótica. No incluye periféricos (como teclado y ratón) o carcasa.

El software es de código abierto, siendo su sistema operativo oficial una versión adaptada de Debian, denominada Raspbian, aunque permite usar otros sistemas operativos, incluido una versión de Windows 10.

GDPR: Es la sigla del Reglamento General de Protección de Datos (RGPD) por su denominación en inglés, General Data Protection Regulation, y se trata del reglamento europeo relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos. Entró en vigor el 25 de mayo de 2016 y fue de aplicación efectiva el 25 de mayo de 2018. Estos dos años permitió a las empresas, las organizaciones, los organismos y las instituciones que se fueran adaptando para su cumplimiento. Es una normativa a nivel de la Unión Europea, por lo que cualquier empresa de la unión, o aquellas empresas que tengan negocios en la Unión Europea, que manejen información personal de cualquier tipo, deberán acogerse a la misma. Las multas por el no cumplimiento del RGPD pueden llegar a los 20 millones de euros. En España, el RGPD dejó obsoleta la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) de 1999, siendo sustituida el 6 de diciembre de 2018 por la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales, acorde con el RGPD.

Falso positivo: En informática se refiere a la detección de un archivo como virus (o alguna otra clase de malware) por parte de un antivirus, cuando en realidad no es ningún virus o malware. Estos errores suelen ser pocos, aunque dependiendo de algunos factores (como la heurística) puede aumentar la probabilidad de la aparición de estos.

Wifi: Es una tecnología que permite la interconexión inalámbrica de dispositivos electrónicos.

Los dispositivos habilitados con Wifi (tales como computadoras personales, teléfonos móviles, televisores, videoconsolas, reproductores de música, etc.) pueden conectarse entre sí o a internet a través de un punto de acceso de red inalámbrica. Wi-Fi es una marca de la Alianza Wi-Fi, la organización comercial que cumple con los estándares 802.11 relacionados con redes inalámbricas de área local.

SSID: Por su sigla en inglés de Service Set Identifier es la secuencia de caracteres que da nombre a la red Wifi que vemos al buscar las redes disponibles. Uno de los métodos más básicos de proteger una red inalámbrica es desactivar la difusión del SSID, ya que para el usuario medio no aparecerá como una red en uso y no será visible.

Wereable o Vestibles: La tecnología ponible o vestible (del inglés *wearable technology*), que hace referencia también a la tecnología corporal, ropa tecnológica, ropa inteligente son dispositivos electrónicos inteligentes incorporados a la vestimenta o usados corporalmente como implantes o accesorios que pueden actuar como extensión del cuerpo o mente del usuario. Los dispositivos

vestibles como los monitores de actividad son un buen ejemplo del Internet de las cosas, puesto que cosas como la electrónica, software, sensores y conectividad son mecanismos que permiten a los objetos intercambiar información a través de Internet con un fabricante, operador u otros dispositivos conectados, sin necesitar de la intervención humana. La tecnología vestible tiene una variedad de aplicaciones que crece en medida que el campo de conocimiento se expande. Se ha popularizado con el consumo exponencial de los relojes inteligentes.

5G: En telecomunicaciones, son las siglas utilizadas para referirse a la quinta generación de tecnologías de telefonía móvil. Es la sucesora de la tecnología 4G. Actualmente está disponible su primera versión estandarizada aunque las empresas de telecomunicaciones continúan investigando nuevas tecnologías para posteriores versiones. La velocidad a la que permite navegar esta tecnología en dispositivos móviles es de hasta 1.2 gigabits por segundo, muy superior a la que permitía el 4G (100Mbps en movimiento).

Red social: Se denomina así a una estructura social conformada por un conjunto de usuarios (individuos u organizaciones) que se relacionan acorde a algún criterio (relación profesional, amistad, parentesco, hobbie, etc.). Normalmente se representan simbolizando los actores como nodos y las relaciones como líneas que los unen. Las redes sociales se han convertido, en pocos años, en un fenómeno global que se expande como un sistema abierto en constante evolución. Las plataformas de Internet que facilitan la comunicación entre personas con los mismos intereses se denominan servicios de red social y las personas interactúan a través de perfiles creados por ellos mismos, en los que comparten sus fotos, historias, notas, eventos o simplemente pensamiento y opiniones.

RFID: Es la sigla de Identificación por Radio Frecuencia (del inglés Radio Frequency Identification). Se trata de un sistema de almacenamiento y recuperación de datos en forma remota que se utiliza en etiquetas o tarjetas RFID. El propósito fundamental de esta tecnología es transmitir la identidad de un objeto mediante ondas de radio. Las etiquetas RFID son unos pequeños dispositivos que se adhieren, incorporan o enganchan a un producto, a un animal o incluso a una persona. Los locales o lugares de lectura de dichas etiquetas contienen antenas que le permiten recibir y responder a peticiones por radiofrecuencia desde un emisor-receptor RFID. Existen etiquetas pasivas que no necesitan alimentación eléctrica interna, y otras que son activas que sí lo requieren. Una de las ventajas del uso de esta tecnología en lugar de otra, como ser la de rayos infrarrojos, es que no se requiere visión directa entre emisor y receptor.

IPTV: Televisión por Protocolo de Internet, por sus sigla del inglés Internet Protocolo Television. Es un sistema de distribución de señales de TV por suscripción con un pago previo que utiliza conexiones de banda ancha sobre el protocolo IP. No es televisión on line ni tampoco de las hoy denominadas OTT (Over The Top) que realizan streaming de video, por lo que se garantiza calidad por parte de las operadoras reservando parte de su ancho de banda para prestar los servicios de televisión.

TCP/IP: Son los dos protocolos más importantes que componen Internet, fueron de los primeros en definirse, y son los dos más utilizados de la familia. Su nombre viene de TCP: protocolo de control de transmisión (Transmission Control Protocol) y de IP: protocolo de internet (Internet Protocol).

Big Data: Es el proceso de recolección de gran cantidad de datos para analizarlos de forma rápida y eficaz con el fin de obtener conclusiones e información oculta a primera vista, patrones de recurrencia, nuevas correlaciones, etc. Es el proceso mediante el cual se analizan la gran cantidad de datos producidos por las personas, las redes sociales y el IoT.

IoE: Es la sigla de Internet of Everything, es decir, Internet de Todo. Es la evolución natural del IoT. Es un concepto que extiende el alcance de Internet de las cosas (IoT) hacia las comunicaciones de máquina a máquina (M2M, Machine to Machine) para describir un sistema más complejo que también abarca personas y procesos.

CCTV: Es la sigla del inglés de Closed Circuit TeleVisión, que traducido al español es Circuito Cerrado de TeleVisión y su objetivo principal es realizar vigilancia y prevención. Se refiere a un sistema de una o más cámaras de vigilancia conectadas a una aplicación que las opera y controla y a monitores que muestran imágenes en tiempo real. Por tratarse de un sistema cerrado las imágenes grabadas por las cámaras no se transmiten fuera del sistema sino que se almacenan en un dispositivo de almacenamiento a tal fin ya que luego pueden ser usadas como evidencia, por ejemplo en el caso de un robo, o cualquier ilícito. Por lo general las cámaras se encuentran fijas en puntos específicos son operadas desde una sala de control o desde una aplicación de un móvil si se trata de un sistema doméstico. Puede contar con funciones avanzadas como ser enfoque, zoom, panorámica, inclinación, entre otras. Existen modelos que permiten captar imágenes en oscuridad (infrarrojo), realizar análisis de video, y hasta configurar detección de movimiento vía software.

PoE: Se trata de una tecnología de que incorpora alimentación eléctrica utilizando el tendido de cable de red de datos. Viene de la sigla en inglés de ***Power over Ethernet***. Permite que la

alimentación eléctrica llegue a un dispositivo de la red haciendo uso del mismo cable que se utiliza para la conexión de red. Su gran ventaja es que elimina la necesidad de utilizar tomas de corriente en cada una de las ubicaciones del dispositivo alimentado (cámaras, puntos de acceso inalámbrico, sensores, alarmas, etc.).

YouTubers: Se denomina YouTubers a aquellas personas que se dedican a hacer vídeos de todo tipo para contar lo que les gusta, dar un servicio a la comunidad y generar contenido para sus suscriptores. Algunos de ellos ya tienen millones de fan y seguidores. Estos videos los publican en canales propios del sitio YouTube. Se han convertido en una importante fuente de información (y hasta formadores de opinión) y de entretenimiento para las nuevas generaciones así como una parte influyente de la economía de Internet, que tiene impacto en lo que las personas piensan y compran.

11.2. Definiciones del marco normativo

Identidad: Conjunto de rasgos propios o características particulares de una persona o cosa que permiten distinguirla unívocamente de otras en un conjunto. Se denomina **Identidad Digital** al conjunto de informaciones publicadas en Internet sobre una persona y que conforman la imagen que los demás tienen de ella: datos personales, imágenes, noticias, comentarios, gustos, amistades, aficiones, etc.

Privacidad: Es el ámbito de la vida privada de una persona que tiene derecho a proteger de cualquier intromisión exterior no deseada. La declaración Universal de los DDHH establece que el derecho a la privacidad es un derecho humano, definiendo que “Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.”

Confidencialidad: Es la garantía de que la información clasificada de esta manera será protegida para no ser divulgada sin consentimiento del propietario, creador o afectado directamente por la misma. Dicha garantía se lleva a cabo por medio de un grupo de reglas que limitan el acceso a ésta información, dependientes de la plataforma donde se alojen y las formas de transporte.

Servicio esencial: Es el servicio necesario para el normal funcionamiento del negocio de las diversas UUNN y empresas del Grupo.

Sector estratégico: Cada una de las empresas y/o áreas diferenciadas dentro del Grupo que proporciona un servicio esencial o que garantiza la operación y seguridad del mismo.

Subsector estratégico: Cada uno de los ámbitos en los que se dividen los distintos sectores estratégicos.

Infraestructuras Críticas: Conjunto de activos e instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales y no permiten (o poseen) soluciones alternativas para el normal desenvolvimiento del negocio. Cualquier perturbación, avería o destrucción de los mismos podría tener un grave impacto sobre los servicios esenciales, el medio ambiente, la seguridad de las personas e integridad de las instalaciones, afectando la imagen pública de la empresa y/o produciendo una cuantiosa pérdida económica.

PLC: Controlador Lógico Programable, más conocido por sus siglas en inglés PLC (Programmable Logic Controller). Es una computadora utilizada en la ingeniería automática o automatización industrial, para automatizar procesos electromecánicos, tales como el control de la maquinaria de una fábrica en líneas de montaje o en otros procesos industriales de diversas industrias como la petrolera, generación de energía eléctrica, agroindustrias, etc.

Red (o sistema) de Automatización y Control: En forma genérica una Red (o sistema) de Control, automatización, telemedición, etc. Pudiendo ser o no industrial.

Sistemas de Control Industriales: Son aquellos sistemas y/o redes de automatización, monitoreo y control que permiten la operación eficiente, segura y automatizada de los procesos de producción industrial.

Están constituidos por la integración de dispositivos de campo, redes de comunicación de transporte de datos industriales, telemedición, dispositivos de control y sistemas de supervisión, operación y adquisición de datos.

Proceso Industrial: Sucesión de etapas físicas o químicas aplicadas a determinada materia prima con el objeto de obtener, transportar o elaborar un producto final deseado.

Dispositivos de campo: Dentro de este conjunto de elementos tenemos dos grupos: los ***Dispositivos de Entrada*** que son aquellos dispositivos electrónicos, tanto analógicos como

digitales, capaces de censar estados y medir parámetros físicos de un proceso industrial automatizado (también llamados **Instrumentación Industrial)** y los ***Dispositivos de Salida*** que son aquellos que mediante su actuación permiten cambiar estados binarios o modificar variables analógicas haciendo que las mismas aumenten o disminuyan su valor.

Entre los primeros tenemos: Pulsadores y llaves de comando, detectores en general (nivel de líquidos, fuego, humo, movimiento etc.) detectores de finales de carrera en válvulas, sensores de proximidad, termocuplas, instrumentos de medición analógica (temperatura, presión, caudal, vibraciones, mezcla explosiva, corriente, rpm, carga de baterías etc.)

En el segundo grupo tenemos: Actuadores de válvulas, variadores de velocidad de motores, arrancadores suaves, servomotores, dosificadores, sirenas de alarma, balizas de señalización etc.

Dispositivos de control: Son aquellos elementos dentro de una red de control que tienen la función de recibir la información de los estados y variables de un proceso industrial proveniente de los dispositivos de entrada y en función de cierta lógica programada en ellos y los set points, recetas y comandos ingresados por los operadores a través de las terminales de control, actúan sobre los diferentes dispositivos de salida para controlar lazos, accionar válvulas, secuenciar etapas, dosificar sustancias, dar marcha o detener equipos etc.

Dentro de estos dispositivos tenemos a los PLC (Programmable Logic Controllers), RTU (Remote Terminal Units) y DCS (Distributed Control Systems).

Existen numerosos fabricantes y gran variedad de modelos para cada uno de ellos. Es frecuente encontrarlos integrados dentro de un mismo sistema de control, esta diversidad da un marco de complejidad importante al relevamiento de estas redes

Sistemas Industriales: Sistemas de automatización y control utilizados en manufactura y proceso de plantas industriales y facilities, automatización de edificios, aplicaciones distribuidas geográficamente como ser generación distribución de energía, y aguas, poliductos, ductos, producción de petróleo, servicio de transporte con sistemas de control y de supervisión o monitoreo.

Dentro de estos sistemas incluimos:

- Sistemas de Control Distribuido (DCSs), Controladores Lógicos Programables (PLCs), Unidades Terminales Remotas (RTUs), Sistemas de Supervisión, Control y Adquisición de Datos (SCADAs), Redes de Telemedición y Monitoreo de variables.

- Sistemas de Información asociados, como: Sistemas de Control Avanzado o Multivariable, Equipos de Monitoreo Dedicados, Historizadores de eventos y variables de proceso.

- Redes e Interfaces Hombre Máquina (HMIs) destinados a proveer control, seguridad, y funcionalidades de operación en procesos continuos, discretos, por lotes etc.

Zona: Conjunto de activos lógicos o físicos agrupados por requerimientos comunes de seguridad. Los límites de cada zona deben estar claramente establecidos. Las zonas pueden estar organizadas jerárquicamente, es decir una zona puede ser el resultado de una agrupación de sub zonas

Conducto: Es un canal de comunicación entre dos zonas de seguridad. Proporciona las funciones de seguridad que permiten a dos zonas comunicarse de forma segura. Toda comunicación entre diferentes zonas ha de realizarse a través de un conducto.

Facilities: Conjunto de edificios, instalaciones, equipos, sistemas y servicios auxiliares necesarios para el normal desarrollo de las actividades dentro de los mismos.

Información: Conjunto de datos, relacionados y/o procesados de tal manera que pueden ser utilizados para la determinación de acciones y toma de decisiones según el fin previsto.

Datos: Conjunto de valores recabados en un instante dado para un cierto fin pero que no han sido interrelacionados con otros de manera funcional.

Plan de continuidad del negocio: Conjunto de medidas de planificación y prevención tendientes a mantener la continuidad de los procesos industriales mediante la maximización de la disponibilidad de los sistemas que los soportan y su recuperación y/o restauración, acorde a los objetivos de recuperación del negocio, frente a una interrupción parcial o total.

Proceso Industrial: Sucesión de etapas físicas o químicas aplicadas a determinada materia prima con el objeto de obtener, transportar o elaborar un producto final deseado.

Dispositivos de campo: Dentro de este conjunto de elementos tenemos dos grupos: los ***Dispositivos de Entrada*** que son aquellos dispositivos electrónicos, tanto analógicos como digitales, capaces de censar estados y medir parámetros físicos de un proceso industrial automatizado (también llamados **Instrumentación Industrial)** y los ***Dispositivos de Salida*** que son aquellos que mediante su actuación permiten cambiar estados binarios o modificar variables analógicas haciendo que las mismas aumenten o disminuyan su valor.

Entre los primeros tenemos: Pulsadores y llaves de comando, detectores en general (nivel de líquidos, fuego, humo, movimiento etc.) detectores de finales de carrera en válvulas, sensores de proximidad, termocuplas, instrumentos de medición analógica (temperatura, presión, caudal, vibraciones, mezcla explosiva, corriente, rpm, carga de baterías etc.)

En el segundo grupo tenemos: Actuadores de válvulas, variadores de velocidad de motores, arrancadores suaves, servomotores, dosificadores, sirenas de alarma, balizas de señalización etc.

Dispositivos de control: Son aquellos elementos dentro de un sistema de automatización y control que tienen la función de recibir la información de los estados y variables de un proceso industrial proveniente de los dispositivos de entrada y en función de cierta lógica programada en ellos y los set points, recetas y comandos ingresados por los operadores a través de las terminales de control, actúan sobre los diferentes dispositivos de salida para controlar lazos, accionar válvulas, secuenciar etapas, dosificar sustancias, dar marcha o detener equipos etc.

Dentro de estos dispositivos tenemos a los PLC (Programmable Logic Controllers), RTU (Remote Terminal Units) y DCS (Distributed Control Systems).

Sistemas de supervisión, operación y adquisición de datos: Dentro de estos sistemas tenemos los **SCADA** (Supervisory Control And Data Adquisition) y los **HMI** (Human Machine Interface).

Estos sistemas tienen la función fundamental de ser el punto de operación de un sistema de control.

Se comunican con los distintos dispositivos de control (PLC, RTU, DCS) utilizando protocolos de comunicaciones específicos de la actividad industrial. Poseen pantallas con representación gráfica esquemática de los distintos procesos controlados donde el operador puede supervisar y operar en tiempo real, ya sea en forma local o remota, las diferentes etapas del proceso.

Desde estos sistemas se visualizan eventos, curvas de tendencias y permiten el monitoreo y la gestión del reconocimiento y reseteo de alarmas.

Los sistemas SCADA suelen correr sobre PCs industriales instaladas en "Salas de Control" y poseen su propia base de datos.

Los HMI están generalmente al pie de los equipos de campo permitiendo su operación en forma local aunque de una manera algo más limitada. Poseen generalmente paneles táctiles. No poseen base de datos local.

Propietarios y Operadores críticos: Las UUNN y empresas controladas, desde sus áreas responsables de las inversiones y del funcionamiento diario de una instalación, red, sistema, equipo físico o de tecnología de la información designada como infraestructura crítica. Debe existir un único propietario responsable para cada sistema que sea determinado como IC

Catálogo Único de Infraestructuras Críticas (CUIC): Comprende la información completa, actualizada, contrastada e informáticamente sistematizada relativa a las características específicas de cada una de las infraestructuras críticas definidas en el ámbito del Grupo. Incluye anexos con las infraestructuras de sistemas de control y automatización (industriales y no industriales) que no sean declaradas como críticas pero están en funcionamiento en la compañía.

Arquitectura Sencilla: Es aquella que posee un único punto de conexión entre la Red de Automatización y Control y la Red Corporativa.

Arquitectura compleja: Aquella arquitectura de comunicaciones que no permita una segregación con firewalls por no existir un borde de red único (ej. redes en el campo compartiendo enlaces de radio).

Red de Control Industrial: Conjunto de equipos y medio físico o inalámbrico que permiten comunicar grupos de 2 o más computadoras, terminales, periféricos, equipos de control y dispositivos de campo entre otros y que a diferencia de las redes de datos IT utilizan protocolos específicos de la actividad industrial.

Protocolo de comunicaciones: Conjunto de reglas y formatos (semántica y sintaxis) que determina el comportamiento de la comunicación de (N)-Nodos en una red.

Algunos ejemplos de Protocolos industriales de comunicaciones son: Modbus, ControlNet, Ethernet/IP, DH, DH+, RIO etc.

DMZ (Demilitarized Zone): Una zona desmilitarizada (DMZ) es un diseño conceptual de red que nos permite eliminar las comunicaciones directas entre dos o más redes de nivel de seguridad diferente. En esta zona se ubican los servidores que es necesario que sean accedidos desde el exterior, por ejemplo servidores de datos históricos, de actualizaciones/parcheo de aplicaciones, de autenticación, etc.

Protección: Todas las actividades destinadas a garantizar la funcionalidad, continuidad e integridad de las infraestructuras críticas con el fin de prevenir, paliar y neutralizar una amenaza, riesgo o vulnerabilidad.

Evolución del conocimiento: Se refiere al proceso mediante el cual desde la recopilación de datos generamos sabiduría. Conocido como la Jerarquía del Conocimiento o Pirámide del Conocimiento, se define como un conjunto de modelos que representan las relaciones entre Datos, Información, Conocimiento, y Sabiduría. No todas las versiones comprenden estos cuatro componentes y en muchos casos, además de ser considerados en forma jerárquica también se los toma en forma de cadena, o de una plataforma o un continuo.

12. Acrónimos más comunes

ANS	**Acuerdo de Nivel de Servicio**
AyC	**Automatización y Control**
CA	**Control de Acceso**
Cat5	**Categoría 5. Se refiere al tipo de cable de cobre utilizado para las conexiones de red de computadoras.**
Cat6	**Categoría 6. Se refiere al tipo de cable de cobre utilizado para las conexiones de red de computadoras.**
CERT	**(Computer Emergency Response Team) Equipo de respuesta a Incidentes Informáticos. Se trata de un grupo de expertos responsable del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información. Un CERT estudia el estado de seguridad global de redes y ordenadores y proporciona servicios de respuesta ante incidentes a víctimas de ataques en la red, publica alertas relativas a amenazas y vulnerabilidades y ofrece información que ayude a mejorar la seguridad de estos sistemas.**
CSIRT	**(Computer Security Incident Response Team) Equipo de Respuesta ante Incidencias de Ciberseguridad. También se puede utilizarse éste término para referirse al CERT. De hecho el término CSIRT es el que se suele usar en Europa en lugar del término protegido CERT, que está registrado en EEUU.**
DCS	**(Distributed Control System) Sistema de Control Distribuido**
DMZ	**(Demilitarized Zone) - Zona Desmilitarizada.**
FAT	**Ensayos en fábrica**
HMI	**Interfaz Hombre Máquina. Se le indica al Sistema que monitorea y maneja un Operador.**

ICS	**(Industrial Control System) Sistema de Control Industrial**
iFIX:	**Uno de los nombres comerciales de software de Scada**
ISA	**(International Society of Automation) Organización de Ingenieros y Técnicos quienes trabajan en el campo de la instrumentación y control de procesos industriales.**
IT	**(Information Technology) Tecnologías de la información**
LENEL	**Plataforma de software homologada y utilizada en YPF SA para los controles de acceso y presentismo.**
NIST	**(National Institute of Standards and Technology) Instituto Nacional de Estándares y Tecnología.**
OT	**(Operational technology) Tecnologías de dispositivos empleados en los sistemas de control industrial.**
PEM	**Puesta en marcha**
PLC	**(Programmable Logic Controller) Controlador lógico programable.**
RPO	**(Recovery Point Objective) Punto Objetivo de Recuperación.**
RTO	**(Recovery Time Objective) Tiempo Objetivo de Recuperación.**
RTU	**(Remote Terminal Unit) Unidad Terminal Remota**
SAT	**Ensayos en sitio**
SCADA	**(Supervisory Control And Data Acquisition) Supervisión, Control y Adquisición de Datos**
SCADA	**(Supervisory Control And Data Acquisition) Supervisión, Control y Adquisición de Datos.**
SGSI	**Sistema de Gestión de la Seguridad de la Información**

SNMP	**Protocolo de capa de aplicación basado en IP que intercambia información entre una solución de administración de red y cualquier dispositivo habilitado para SNMP**
Switch	**Dispositivo de comunicaciones que permite entregar servicios de red a los puntos de red.**
TIC	**Tecnologías de la Información y las Comunicaciones**
UPS	**(Uninterruptible Power Supply) Sistema de alimentación ininterrumpida**
UUNN	**Unidades de Negocios.**

La guía ofrece un enfoque integral para la gestión de la ciberseguridad en infraestructuras industriales críticas, abordando aspectos conceptuales, prioridades de seguridad y un marco estructurado para la implementación de medidas de ciberseguridad.

Esta guía permitirá trabajar tanto ex ante (prevención) como ex post (actuación, remediación, resiliencia) en el abordaje de incidentes de ciberseguridad en infraestructuras que requieren una gestión de extrema seguridad, por su condición de criticidad para la propia organización y la población en general; especialmente, en instalaciones industriales del Estado o de empresas que brindan servicios esenciales (agua, energía, comunicaciones, combustibles, etc.). Un problema de seguridad en estas instalaciones puede significar el colapso de servicios vitales para la población. De ahí la importancia de desarrollar un producto tecnológico de soporte a la gestión..

UNIVERSIDAD FASTA
FACULTAD DE INGENIERÍA
InFo-Lab
INSTITUTO DE CIENCIAS FORENSES
UNIVERSIDAD FASTA
UNDEF
FACULTAD DE INGENIERÍA DEL EJÉRCITO
UAI
Universidad Abierta Interamericana

ISBN 978-631-90546-3-7