"Evolución del Malware y Defensa ante Ataques Dirigidos a Infraestructuras Críticas"

Tutor: Jorge Alejandro Kamlofsky

Tesista: Mariano Alberto Pozzi

Trabajo Final de Carrera Presentado para Obtener el Título de Licenciado en Gestión de Tecnología Informática

Octubre, 2020

Resumen

Es sabido que los ataques informáticos a distintas organizaciones a través del tiempo han tenido graves consecuencias en las mismas, sobre todo cuando han existido motivos bélicos y otros intereses políticos. La información es el activo más importante que maneja toda empresa y como tal, es necesario que se resguarde correctamente. Sin embargo, es incierta la relación que hay entre la materialización de estos incidentes y el seguimiento de buenas prácticas de gestión de las vulnerabilidades que todo sistema va presentando debido al inevitable paso del tiempo. Por lo tanto, ha surgido la necesidad de profundizar y estudiar la correspondencia entre estas variables.

Esta tesis de grado fue realizada para presentar al lector cuál ha sido la evolución de los ataques informáticos más trascendentes, ejecutados de manera dirigida en infraestructuras críticas durante la última década, es decir, correspondiendo al período 2009-2019. Esto se ha logrado mediante el análisis de la perspectiva defensiva, haciendo foco en los controles y normativas de mayor importancia surgidas globalmente y, por otro lado, en cómo se relacionan estos con los sistemas implementados en las organizaciones.

Trabajando en profundidad con esta información, se logró obtener una guía orientada a unificar las buenas prácticas preventivas para robustecer las infraestructuras.

Por otra parte, se ha obtenido conocimiento sobre la relación existente entre los ataques informáticos, explotadores de vulnerabilidades por su naturaleza y la aplicación de políticas y estándares de Seguridad Informática.

Palabras Clave[1]:

seguridad informática, malware, seguridad de redes, ciberguerra, seguridad de sistemas energéticos

[1] *https://www.ieee.org/content/dam/ieee-org/ieee/web/org/pubs/ieee-taxonomy.pdf*

Abstract

It is known that computer attacks have had serious consequences on different organizations over time, especially when there have been military motives and other political interests. Information is the most important asset that every company manages and as such, it needs to be properly safeguarded. However, the relationship between the materialization of these incidents and the follow-up of good practices for managing the vulnerabilities that every system has as time goes by, is uncertain. Therefore, there is a need to get deeper and study the correspondence between these variables.

This thesis was carried out to present to the reader how has been the evolution of the most transcendent computer attacks, carried out in targeted critical infrastructures during the period corresponding to 2009-2019. This was achieved by analysing the defensive perspective and focusing on which have been the most important controls and regulations that have emerged in the world and on the other hand, how they are related to the involved companies' systems.

Working in depth with this information, it was possible to obtain a guide directed to unify good preventive practices to strengthen infrastructures.

On the other hand, it has been obtained knowledge about the relationship between computer attacks, exploiters of vulnerabilities by their nature, and the application of Information Security policies and standards.

Keywords[2]:

information security, malware, network security, cyber warfare, power system security

[2] *https://www.ieee.org/content/dam/ieee-org/ieee/web/org/pubs/ieee-taxonomy.pdf*

Reconocimientos

Existen varios profesionales que aportaron testimonios meritorios para la realización de la investigación, a quienes se desea agradecer. Las participaciones intelectuales de Christina Kubecka e Igor Lukic resultaron de gran contribución para recorrer con sus experiencias, el abordaje del virus Shamoon. Por otro lado, el rigor académico de Juan Ignacio Alberdi para describir el comportamiento y tratamiento del ransomware WannaCry, tiene vital importancia para dicha sección en este trabajo.

Asimismo, se desea reconocer a modo de mención especial al tutor de tesis, Jorge Kamlofsky, quien ha dedicado valioso tiempo como guía y mentor, habiendo compartido muchos de sus conocimientos.

Por último, resulta muy importante agradecer y dedicar el trabajo especialmente a Laura y Mateo, por su soporte y amor incondicional en las largas jornadas brindadas a la elaboración de la tesis, así como a mi familia y amigos más cercanos.

Índice General

Índice de Ilustraciones

Índice de Tablas

Capítulo 1

Introducción

1.1 Problemas y Soluciones

El problema principal que se plantea en este trabajo es conocer si existe una relación entre el impacto del malware de ciberguerra dirigido a Infraestructuras Críticas en contraposición con la aplicación de controles pertenecientes a las normativas existentes más reconocidas. Resulta trascendental para esta investigación el apoyo del Lic. Jorge Kamlofsky, quien cuenta con una amplia trayectoria en diversos tópicos de Seguridad Informática, Criptografía, Cibercrimen y Redes Industriales.

Cualquier empresa que maneje activos, sistemas y redes, físicos o virtuales de envergadura, maneja muy probablemente diversas conexiones a una o más redes que se encuentran accesibles desde Internet. Estas pueden ser: instalaciones químicas, instalaciones comerciales, comunicaciones, fabricación, represas, bases industriales de defensa, servicios de emergencia, energía, servicios financieros, alimentación, agricultura, instalaciones gubernamentales o transporte. Por esto mismo, potencialmente se encuentran en riesgo y debe aplicarse un seguimiento protocolar de prácticas conscientes, para evitar ser objetivo de ataques dirigidos con fines malintencionados, como robo de información y espionaje, fraude o sabotaje, los cuales podrían tener un resultado de debilitación sobre la seguridad pública, económica o física.

1.2 Propuesta

Las infraestructuras críticas existen a nivel global, por lo que las consecuencias de no tratar su administración con la requerida responsabilidad profesional, ya sea por negligencia u otras cuestiones, pueden ser muy graves, como la ocurrencia de accidentes fatales que podrían involucrar gran cantidad de personas. Más allá de las enormes pérdidas potenciales económicas, como veremos en los casos que se tratarán, está en juego la vida humana misma.

Es en este contexto en el cual se expone que la aplicación correcta de controles y estándares de seguridad mitiga o reduce el impacto de ataques de ciberguerra dirigidos a infraestructuras críticas.

1.3 Objetivo General y Objetivos Específicos

A continuación, se procede a mencionar el objetivo general que da origen a este trabajo con los respectivos objetivos de índole específicos que tiene asociados.

1.3.1 Objetivo General

El objetivo general de este trabajo final es comprender cuál es la relación entre la aplicación de buenas prácticas y procedimientos de ciberseguridad y la mitigación de ataques de ciberguerra dirigidos a infraestructuras críticas durante los años 2009-2019.

1.3.2 Objetivos Específicos

A partir del objetivo general anteriormente expuesto, contamos también con un primer gran objetivo específico, que es analizar los ataques más significativos en cuanto a impacto, ya sea por pérdidas económicas o cantidad de equipamiento afectado, de la última década. Ejemplos de estos han sido Stuxnet, en el SCADA marca Siemens de la planta de enriquecimiento de uranio iraní de Natanz y Shamoon, en la red de computadoras de la mayor petrolera del mundo Saudi Aramco, como gusanos y virus industriales, o WannaCry, como un ransomware que afectó industrias y empresas globales como Telefónica o Fedex, oficinas de gobierno y servicios de salud en todo el mundo.

En esta investigación se procuró presentar al lector cómo han evolucionado los principales ataques informáticos que se fueron llevando a cabo de manera dirigida en infraestructuras considerables como “críticas” a lo largo de los años. Para poder comprender esta evolución, se expone un segundo objetivo específico, el cual es establecer la relación entre la aplicación de parches y remediación de vulnerabilidades en dichas infraestructuras críticas con la mitigación del impacto.

Por último, también se menciona un tercer objetivo específico, de aporte destacado para la comunidad de profesionales de ciberseguridad: analizar cuáles son las prácticas preventivas más relevantes para robustecer infraestructuras críticas de posibles ataques ya que en algún momento, todas serán afectadas por la problemática.

1.4 Contribuciones Principales

Debe comprenderse que, si bien existe un marco normativo estricto en algunas partes del mundo, como en Europa o Estados Unidos, la legislación en los tipos de sistemas planteados aún es muy confusa y se encuentra en proceso de desarrollo. Por esto, ha sido un gran desafío recorrer íntegra y exhaustivamente el estado del arte de estándares y recomendaciones vigentes, para comprender las problemáticas y contribuir con aportes que sean de utilidad en entornos profesionales para la toma de decisiones de robustecimiento de las Infraestructuras y redes Industriales.

Además, resultó de mucha utilidad, la comprensión de las técnicas que realizaron los especialistas para remediar los ataques mencionados y cuáles hubieran sido las buenas prácticas ya mencionadas que hubieran mitigado estos ataques dirigidos.

Por otro lado, este trabajo también pretende alentar a los profesionales de IT para que implementen los estándares normativos vigentes al momento de desempeñar sus labores habituales, comprendiendo su magnitud, ya que en algunos casos corre riesgo la vida de las personas.

1.5 Metodología de la Investigación

Para corroborar empíricamente la hipótesis, la cual postula que la aplicación de controles y estándares de seguridad reduce o mitiga el impacto de ataques de ciberguerra dirigidos a infraestructuras críticas, se realiza un relevamiento de la población de ataques registrados durante el período 2009-2019, que recolecta información de la base de datos *RISI* (The Repository of Industrial Security Incidents). El conjunto de datos de este repositorio es uno de los más ricos hasta ahora para comprender la contabilización histórica de los ataques cibernéticos en las infraestructuras críticas y los sistemas de control industrial en todo el mundo. Al momento de realizar este trabajo, la base de datos contiene 242 incidentes de seguridad, confirmados como correctos. En esta fuente, sumada a otras reportadas con posterioridad a 2015 en las investigaciones citadas, se basa este trabajo para seleccionar las muestras a analizar minuciosamente en los próximos subapartados.

De acuerdo con las definiciones de malware que se detallan en el *Capítulo 3*, se toma una muestra de cada conjunto teniendo en cuenta cuáles han tenido el impacto más significativo, ya sea por cantidad de equipos infectados, personas involucradas o pérdidas económicas medidas en dólares estadounidenses. Para dichos casos, se analizan los focos y vulnerabilidades que han explotado los atacantes y qué estándares y políticas se han llevado a cabo.

Por último, es mostrada la relación entre las variables de aplicación de controles de Seguridad Informática y el impacto que tienen los ataques dirigidos a infraestructuras críticas.

Esta metodología será retomada en el apartado 4.1, donde tiene un mayor sentido al haber sido recorrido ya el marco teórico.

1.6 Estructura General de la Tesis

1.6.1 Capítulos

El marco teórico y conceptual estará ubicado en el *Capítulo 3*. En el apartado 3.1 se abordará en detalle qué diferentes tipos de redes existen. De esta manera se comprenderá la diferencia entre redes de Tecnología de la Información (IT) y redes de Tecnología Operacional (OT)

para poder establecer la convergencia entre ambos mundos, opuestos pero complementarios, hacia el final del capítulo.

También se mencionará el concepto de “infraestructuras críticas”, marco que pretende recortar la investigación: se explicará cómo funciona un PLC y cómo lo hace un dispositivo SCADA. Estos sistemas serán objetivos de hackers en los ataques que se describirán en el apartado 3.3.

Posteriormente, se abordará en el apartado 3.2, cuál es el marco normativo vigente y referencial a nivel mundial para unificar los criterios del estado del arte.

Se comenzará con la referencia a los diversos estándares ISO: 22301 y toda la serie 27000, incluyendo 27001, 27002 y 27010. También se mencionará COBIT, ITIL, CIS y los estándares más importantes de NIST, como 800-30 y su derivado 800-55, 800-53 y 800-82, específico para sistemas industriales. Para todos estos, se nombrarán cuáles son los conceptos y controles claves, detallados en el *Anexo II*.

En el apartado 3.3, por ser de especial relevancia en la investigación, se ahondará en profundidad en la evolución del malware.

Se comenzará describiendo los tipos y herramientas de malware existentes y su ciclo de vida, así como también las técnicas empleadas por los atacantes, a partir de las cuales quedará evidenciada la importancia de comprender cuándo la Seguridad de una infraestructura crítica está siendo probada, vulnerada e incluso penetrada intencionalmente. Cuando esto sucede, cabe mencionar en qué repositorios de alcance público son documentados los incidentes.

En este apartado también se describe cómo se manejan en los mercados negros, como el de la Deep Web, las ventas de vulnerabilidades zero day.

A partir de este desarrollo conceptual, el lector tendrá un panorama general de los vectores de amenazas en sistemas de control industrial y la evolución que ha tenido el malware, en donde se detallarán las diferencias entre gusanos informáticos, virus y ransomware, siendo los utilizados para perpetrar los ataques con mayor nivel de impacto. Para esto, se analizarán en profundidad, los tres casos más significativos respectivamente.

Por último, se pondrán a la luz las tendencias en los ataques y qué técnicas efectivas se siguen reutilizando al día de la fecha.

Más adelante, en el apartado 3.4, se definirá cómo se desarrolla la ciberseguridad en las infraestructuras críticas.

Entender cómo se le debe brindar respuesta a los incidentes, el monitoreo de eventos con herramientas tales como los SIEM, la aplicación de controles asociados a las normativas referenciadas y las buenas prácticas de seguridad en general, otorgarán las herramientas más adecuadas para robustecer las infraestructuras. Para los incidentes ya materializados, se desarrollará cómo planificar la continuidad del negocio.

Sobre la base de todos los conceptos que se fueron recorriendo anteriormente, se formulará en el *Capítulo 4* la propuesta técnica del prototipo de investigación, poniendo foco en la especificación de la hipótesis y detallando cuál es la delimitación del marco seleccionado para el trabajo.

Por último, en el *Capítulo 5* se realizará la corroboración empírica de la hipótesis central de este trabajo. Este capítulo es netamente de índole experimental, ya que se enfocará en el análisis e interpretación del material informativo relevado, como ataques informáticos y controles de los marcos normativos, para exponer luego los resultados obtenidos.

1.6.2 Anexos

En el *Anexo I*, se incluyen las preguntas de la entrevista realizada a Christina Kubecka, quien ha logrado reconocimiento en el ambiente de ciberseguridad por restablecer las redes comerciales internacionales de la empresa petrolera Saudi Aramco y su seguridad en general, después del ataque cibernético Shamoon. Kubecka es autora, investigadora de seguridad y oradora americana, CEO en HypaSec NL.

Por otro lado, este anexo también contiene las preguntas de la entrevista realizada sobre el ataque WannaCry a Telefónica, principalmente en España, pero también teniendo impacto en Argentina en 2017. Juan Ignacio Alberdi, quien trabajó arduamente en el tema, es

Ingeniero en Informática de la Universidad FASTA e investigador del Infolab[3], docente e investigador graduado del Grupo de Investigación en Sistemas Operativos e Informática Forense y docente en Sistemas Distribuidos en la carrera de Ingeniería en Informática. Coautor de BIP-M Framework, un software para el análisis forense de memoria principal, ha presentado trabajos en múltiples congresos nacionales e internacionales. Ha participado también en la presentación del paper "Windows Malware: Traces in the Host" para el CIBSI 2017.

Como se ha mencionado, en el *Anexo II*, se encuentra el resumen de los controles evocados para sustentar la comprobación empírica de la hipótesis. En esta parte, el lector podrá contar con el detalle completo de los mismos, dentro de los marcos normativos COBIT, ISO/IEC 27001, ISO/IEC 27002, NIST SP 800-53, ITIL, CIS, NIST SP 800-82, ISO/IEC 27010, ISO/IEC 27032 e ISO 22301, respectivamente.

[3] *Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense. Sitio web: https://info-lab.org.ar/*

Capítulo 2

Trabajos Relacionados

2.1 Disparadores de Investigación

A partir de diversos enfoques abordados por autores que han estudiado en profundidad el comportamiento de las redes industriales, la Seguridad Informática, las características del ciberterrorismo y ciberespionaje y los eventos más relevantes en cuanto a ataques informáticos, todavía resta unir la relación entre todas estas variables que, parecen sencillas a simple vista, pero no lo son. La investigación sobre la disminución de los efectos de los Ciberataques a las Infraestructuras Críticas (Kamlofsky, *et al*, 2015), ha evidenciado una relación entre lo considerado como buenas prácticas de seguir los lineamientos de una red correctamente segmentada y de manera lógica para constituir la topología corporativa y la mitigación del impacto de ataques dirigidos, en entornos que se ven fortalecidos por estar basados en estándares robustos como las normas ISO 27001.

Se ve en esta relación, una implícita línea de investigación, que abre la puerta a la temática abordada en este trabajo y pretenderá sumar conocimiento a la comunidad científica desde una perspectiva equidistante entre aspectos técnico-evolutivos y normativos. Es lógicamente sustentable el hecho de que puedan surgir ideas fructíferas, si tomamos los casos de incidentes de mayor impacto presentes en la base de datos RISI hasta 2015, junto con los casos posteriormente reportados y los analizamos en profundidad contraponiéndolos con las normativas existentes al momento de su ocurrencia y las últimas al día de la fecha, luego de haber investigado el estado del arte.

2.2 Aporte a la Comunidad

En el presente trabajo abordado, se hace hincapié en el valor agregado que delinea el vínculo exhaustivo de los ciberataques dirigidos más relevantes y las normativas y estándares informáticos contextualmente referentes.

En el estado del arte, se han encontrado trabajos que aportan buenos juicios de valor: lógicos, por cierto, aunque no presentan ni pretenden como objetivo abordar la correlación entre las variables detectadas.

En el trabajo citado en el punto anterior, por otro lado, se llegan a enumerar los ataques más significativos hasta 2015. Sin embargo, es a partir de ese momento cuando en el mundo comienzan a evidenciarse eventos de ransomware, siendo esta una amenaza esencial para incluir en el análisis, si se desea tener una noción completa del escenario de ciber-guerra hoy.

De esta manera, el análisis en profundidad de los casos relevantes en contraposición con el marco teórico normativo y evolutivo, nos permitirá sustentar científicamente si efectivamente se comprueba la existencia de una correspondencia entre la mitigación de los ataques crecientes en complejidad, con la aplicación de correctas prácticas basadas en estándares cada vez más completos en cuanto a robustez. Para todos estos puntos, es necesario conocer cuál ha sido su evolución en el tiempo.

Capítulo 3

Marco Teórico

3.1 Tipos de Redes

3.1.1 Tecnologías de la Información (IT)

Se puede afirmar que Tecnologías de la Información o IT son: “el conjunto completo de tecnologías, incluidas la infraestructura de hardware y las aplicaciones de software, utilizadas para transformar los datos. Por lo tanto, un sistema de IT se puede definir como un motor que acepta flujos de datos como entrada para entregar un nuevo flujo de datos, pero que no interfiere con el mundo físico” (Atos, 2012, p.4). De esta manera, IT es un sistema de información cuya función es recopilar y procesar información. Los sistemas de información se utilizan para diversas tareas comerciales, como marketing, ventas, fabricación, logística, compras, finanzas o recursos humanos. Ejemplos de sistemas de IT relacionados incluyen sistemas Enterprise Resource Planning o *ERP*, o aplicaciones Customer Relationship Management o *CRM* (Bonnetto, *et al*, 2017).

El perfeccionamiento en IT ha impactado notablemente durante la última década sobre el mercado empresarial. Las organizaciones más tradicionales, jerárquicamente verticalistas, presentan dificultades en este contexto para responder a los exigentes cambios del mercado y han surgido paulatinamente procesos horizontales, brindando un creciente poder de decisión a los empleados. Es entonces cuando surgen procesos de trabajo soportados en el uso de servicios. En la actualidad, las IT han pasado a formar parte de muchos de los ámbitos de la vida de las organizaciones y también de las personas. Su impacto ha sido, y continuará

siendo considerable, incluyendo en el ámbito de la gestión organizacional (Meza Medellín, 2015).

3.1.2 Tecnología Operacional (OT)

La Tecnología Operacional u *OT*, le brinda soporte tanto a la creación de valor físico como a los procesos de fabricación. Estas redes reciben un tratamiento muy diferente a las mencionadas en el punto anterior: se refieren al hardware y software utilizado en los sistemas de controles de automatización de infraestructura, incluyendo a los sistemas de control industrial o *ICS*, como se verá más adelante, o su monitoreo y supervisión. Las industrias forman parte de las infraestructuras críticas, sin las cuales la sociedad y la economía fracasarían. Los sistemas OT fueron diseñados para integrar sistemas de adquisición de datos, sistemas de recolección y transmisión de datos y sistemas de Interfaz Hombre-Máquina o *HMI* para crear una solución centralizada de control y supervisión. En consecuencia, permiten que un operador interprete visualmente el estado de la planta para fines de control y monitoreo (Shahzad, *et al*, 2015). Es decir, se trata de sistemas compuestos de comando y control, de hardware y software, destinados a monitorear y controlar plantas y equipos, cuya función principal será enviar órdenes hacia los medios de producción para accionarlos y recopilar información sobre el progreso de los procesos industriales que efectúan.

Atos define OT como: “el conjunto de dispositivos y procesos que actúan en tiempo real en sistemas operativos físicos, como redes de distribución de electricidad, instalaciones o plantas de producción de vehículos” (Atos, *Op.cit*, 2012, p.4). Un gran porcentaje de los sistemas OT que están en vigencia es bastante antiguo, remontándonos para su implementación a varios años hacia atrás. Usualmente, son minuciosamente diseñados para satisfacer su propósito y utilizan protocolos que son específicos para los requisitos del proyecto. Esto conlleva a mencionar una fuerte debilidad: existe un soporte limitado para estos sistemas, lo que consecuentemente los expone como objetivos, ya que no requieren mayores esfuerzos para ser explotados, más que la destreza por parte del atacante.

Como se explicará más adelante, las amenazas a los sistemas OT se encuentran en constante evaluación y los ataques cibernéticos están aumentando tanto en periodicidad, impacto y complejidad. Las consecuencias de un ciberataque en sistemas OT de infraestructura crítica

implican no sólo perjuicio financiero sino también interrupciones prolongadas de servicios críticos esenciales para el ser humano impacto en su propia vida como lo son, por ejemplo, el agua, la salud o la energía eléctrica (Murray, *et al*, 2017).

El ámbito de aplicación de las tecnologías OT es vasto: desde diversos tipos de industrias, como energía, agua, monitoreo del tránsito, refrigeración, calefacción, petroquímica, gas, logística, hasta aplicación para defensa. Algunos ejemplos de elementos OT e ICS son los sistemas de ejecución de fabricación o *MES*, válvulas, motores, medidores y sensores, entre los que destacan los controladores de automatización programable o *PAC* , los controladores lógicos programables o *PLC* y los sistemas de control de supervisión y adquisición de datos o *SCADA*. Cabe destacar que en este trabajo se ahondará principalmente en los dos últimos, teniendo en cuenta que son los más importantes por su implicancia productiva además de ser los más frecuentemente elegidos como objetivos de ataques. Por esto mismo hablaremos de Sistemas de Control Industrial o *ICS* y OT de manera análoga, puesto que como se ve en el siguiente gráfico, PLC y SCADA forman parte de ambos universos.

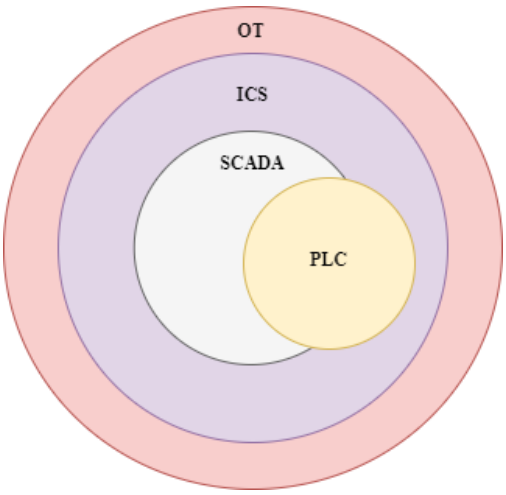


Ilustración 1: Composición conceptual del conjunto de elementos más comunes de la red OT y sus relaciones

PLC

El estudio del procesamiento automatizado es una cuestión muy extensa, que refiere a los transmisores de campo, a la instrumentación industrial con los sensores, a los sistemas de transmisión, sistemas de recolección de datos, sistemas de supervisión y control y todas aquellas aplicaciones de software que supervisan, operan y controlan las plantas y sus procesos industriales en tiempo real. Por este motivo, se ahondará en este tema que será de especial atención para el objetivo de este trabajo.

A continuación, se detallan las definiciones del concepto de automatización más relevantes: "La automatización es un sistema donde se trasfieren tareas de producción, realizadas habitualmente por operadores humanos a un conjunto de elementos tecnológicos. Un sistema automatizado consta de dos partes principales: parte de operativa y parte mando" (Aguilera Martínez, 2002, p.7). En el ámbito de la industria, la automatización implica "usar tecnología que integre un proceso de control a través de dispositivos capaces de tomar decisiones e interactuar con otros, basándose en un programa establecido por el integrador para el manejo de algunas variables, mediante su monitoreo y comparación con un valor esperado del proceso; esto se realiza de manera automática, generando en el sistema mayor productividad, confiabilidad, estabilidad y calidad en sus resultados" (Castro Lugo, *et al*, 2005).

Existen varias metas que persigue el proceso de automatización, entre las cuales se encuentran la mejora de la productividad de una compañía mediante la reducción de costos productivos y mejor de la calidad, la mejora de condiciones del trabajo personal mediante la supresión de trabajos pesados e incremento de las cuestiones de seguridad, la realización de operaciones complejas intelectual y manualmente, la mejora de la disponibilidad de productos a partir de la proveeduría de cantidades justas y oportunas, la simplificación del proceso de mantenimiento reduciendo la cantidad de conocimiento requerido por parte del operador y por último, la integración de los procesos de fabricación y producción (Aguilera Martínez, *Op.cit*, 2002).

"La automatización de los procesos productivos se establece como una herramienta fundamental que permite a las empresas un desarrollo propio, dinámico y competitivo,

facilitando la relación entre las diferentes áreas de la organización o empresa" (Castro Lugo, *et al*, 2005).

Del otro lado de la automatización, aparece el concepto de automatismo, es decir: "[…] dispositivo eléctrico, electrónico, hidráulico, neumáticos, etc. en una máquina o dispositivo, para lograr que funcione de forma automática" (Vallejo, 1999). Actualmente, para realizar dicha tarea, se utiliza el PLC. Básicamente, dicho dispositivo es un aparato electrónico creado con el objetivo de controlar procesos secuenciales, y su lenguaje aglutina contactos serie, en paralelo, contadores, desplazamientos, temporizadores, y otras funciones más complejas (*Ídem*).

Como solución al control de circuitos complejos de automatización, surgió el Autómata Programable Industrial o *API*. Por lo tanto, un API es un aparato electrónico que sustituye los circuitos auxiliares o de mando de los sistemas automáticos. Al mismo le son conectados los captadores o botones transductores, por un lado, y también los actuadores o bobinas de contactores (Aguilera Martínez, *Op.cit*, 2002).

El Controlador Lógico Programable

"Los PLC son dispositivos electrónicos robustos utilizados para gobernar uno o varios procesos en la industria; debido a su flexibilidad tecnológica pueden ser compatibles con los nuevos dispositivos que se van adicionando al sistema y las comunicaciones entre procesos [...]." (Quintero Ruíz, *et al*, 2006). También se define de esta manera a todo dispositivo electrónico creado con el objetivo de controlar, en el ámbito industrial, procesos secuenciales en tiempo real. De todas maneras, este último concepto está sufriendo cambios, debido a que hoy en día existen los micro-PLC, que se utilizan para satisfacer necesidades pequeñas y están al alcance de cualquier persona (Aguilera Martínez, *Op.cit*, 2002).

Un PLC tiene varias funciones, entre las que se encuentran: *a- la detección*, o lectura de la señal de los captadores distribuidos por el sistema de fabricación; *b- el mando*, o elaboración y envío de las acciones al sistema mediante accionadores o pre accionadores; *c- el diálogo hombre-máquina*, obedeciendo y retroalimentando el status, a partir de las consignas de los operadores; *d- la programación*, donde a partir de la lógica del desarrollo del programa de

aplicación del autómata, el diálogo debería permitir modificar el programa incluso con el autómata en pleno proceso de control de la máquina (*Ídem*).

Es importante destacar la importancia del cálculo matemático dentro de todo proceso industrial. El mismo "[…]permite evaluar y medir variables indirectas del proceso. En los diferentes lenguajes de programación de PLC, es posible insertar un cálculo matemático. Sin embargo, esta tarea puede resultar compleja según el número de variables de la ecuación y las capacidades del lenguaje. El lenguaje empleado puede variar la dificultad de inserción e interpretación de ecuaciones matemáticas en los bloques del programa. Insertar una ecuación matemática en un proceso empleando un software de cálculo matemático, […] facilita la programación de un bloque de función para el cálculo del volumen y nivel de un tanque" (Páez Logreira, *et al,* 2015).

Los sistemas PLC tienen muchos espacios de aplicación, sobre todo teniendo en cuenta la constante evolución del hardware y software. Se utilizan "en aquellas instalaciones en donde es necesario un proceso de maniobra, control, señalización, etc. Por lo tanto, su aplicación abarca desde procesos de fabricación industriales de cualquier tipo a transformaciones industriales, control de instalaciones, etc" (Aguilera Martínez, 2002, p.16).

Debido a sus dimensiones minúsculas, su simplicidad de acoplamiento y la capacidad de almacenar programas para su utilización posterior y rápida son muy eficaces en procesos en los que el espacio es reducido, los procesos productivos cambian periódicamente o son secuenciales, existe maquinaria de procesos inconstantes, complejos o amplios y también si se requiere chequear centralizadamente la programación de cada fragmento del proceso. Existen otras ventajas que se pueden observar utilizando PLC. En primer lugar, no es necesario esquematizar los contactos. Tampoco es excluyente que se simplifiquen las ecuaciones lógicas, porque tienen gran capacidad de almacenamiento en el módulo de memoria. Los PLC permiten realizar modificaciones sin tener que modificar el cableado previo, ni agregar dispositivos adicionales. Por esto, tienen un menor costo de mano de obra en la instalación y, en general, son económicos en cuanto al mantenimiento. Adicionalmente, aumentan la confiabilidad del sistema al eliminar contactos móviles. También pueden detectar e indicar averías y administrando múltiples máquinas simultáneamente.

Como se mencionó anteriormente, la programación de PLC es utilizada en la automatización de algún proceso electromecánico, como lo es controlar las máquinas que forman parte de algún proceso productivo industrial. Estos sistemas se utilizan en todo tipo de proyectos: simples u otros con sistemas de control más complejos (*Ídem*).

Una de las desventajas, que se presenta a partir de la utilización de estos controladores, desde el punto de vista económico, es la necesidad de la presencia de un programador. Para ello se debe capacitar a algún técnico o contratar un especialista. El alto costo inicial también suele ser una desventaja (*Ídem*). Por otro lado, también es importante que se haga un correcto uso de estas tecnologías, ya que los PLC podrían verse infectados por algún tipo de malware si no se toman los recaudos necesarios.

Elementos del PLC

Externamente, el PLC es robusto dado que debe desempeñarse adecuadamente en situaciones industriales extremas. Visualmente, se suelen diferenciar marcadamente los terminales de entradas y salidas, que son donde recibe y brinda la información necesaria (*Ídem*). "Existen dos tipos de formato, los compactos y los modulares. Los compactos se utilizan generalmente, en instalaciones pequeñas que requieran pocas señales. Los modulares son conexionados entre sí, mediante cables especiales, conectores o a través de un chasis, quedando bien diferenciado todos los componentes que lo forman, como pueden ser la fuente de alimentación, la unidad central de proceso, los módulos de entradas y salidas digitales, analógicas, de comunicación, especiales, etc." (Vallejo, *Op.cit, Ibidem,* 1999, p.4). Los elementos fundamentales, que forman parte de cualquier autómata programable son: *a-sección de entradas*, líneas de entrada digitales o analógicas donde se conectan los sensores; *b-sección de salidas*, línea de salida digital o analógica donde se conectan los actuadores*; c-unidad central de proceso o CPU*, donde se procesa el programa de usuario mediante zonas de memoria, registros e instrucciones; *d-integrados*, como reguladores PID, control de posición, etc. Las entradas y salidas se encuentran separadas de la Unidad Central del Proceso, según el tipo de autómata utilizado. También pueden formar parte de estos sistemas otras *unidades* como la de alimentación, de comunicación en red, consola de programación, periféricos (de entrada y salida), etc. e *interfaces*, que ayudan en la comunicación del autómata mediante enlace serie con otros dispositivos. (Aguilera Martínez, *Op.cit*, 2002).

La CPU es el corazón del autómata programable, que cumple la tarea de ejecutar el programa de usuario por medio del programa del sistema: en otras palabras, el programa de usuario es interpretado por el programa del sistema. Las funciones de la CPU son: vigilar el tiempo máximo (o ciclo) de ejecución del programa de usuario, ejecutar el programa de usuario, generar una imagen de las entradas para que el programa de usuario no las acceda de manera directa, renovar el estado de las salidas y monitorear el sistema (*Ídem*).

SCADA

El paulatino predominio de los sistemas SCADA en diferentes tipos de infraestructuras es la consecuencia de la gran cantidad de ventajas que estos pueden facilitar a las compañías que los manipulan, realizando tareas que pueden lograrse ágilmente, con un menor costo y con mayor eficiencia, como sucedía en los años ’30. Solamente quienes tenían acceso a las instalaciones podían obtener los datos, lo que hacía de la seguridad informática un tema secundario. Luego, durante los cincuenta años posteriores, estos sistemas manejarán cada vez más datos y de mayor complejidad, por lo cual surgirá la necesidad de optimizar su rendimiento. Ya la década de ‘90, las mejoras en conexiones remotas y la ampliación de las redes informáticas en cuanto a su ancho de banda, facilitaron a estos sistemas las comunicaciones con equipo distantes. La convergencia de las redes industriales con las redes IT, que será tratada en el próximo apartado, ha activado nuevas formas de acceso, lo que abre nuevas posibilidades a los atacantes.

No es una tarea sencilla la obtención de documentación detallada de ataques a sistemas SCADA, puesto que las empresas que padecen estos incidentes no los suelen informar por razones de riesgo reputacional. Sin embargo, por mencionar uno de los casos que oficiará de hilo conductor para este trabajo, en 2010 se hizo público el acontecimiento en Siemens (Stuxnet), el cual se trató de un complejo gusano informático que marcó un antes y un después en referencia con la seguridad en SCADA, debido a que entró en juego la posibilidad de la guerra cibernética. El resultado de un ataque intencional hacia uno de estos sistemas sería devastador, ya que podría tratarse de un primer objetivo de acceso para los ciberterroristas en cuestiones de ciberguerra (Estudios de Seguridad y Defensa, 2014).

Los sistemas SCADA "se idearon para controlar sistemas industriales, conectando PC y redes de autómatas industriales; conformando la interfaz hombre máquina" (Kamlofsky, *et al*, 2015, p.883). Se trata de tipos de ICS que se distribuyen geográficamente en un territorio extenso y usualmente se controlan y gestionan centralizadamente. Los sistemas SCADA se implementan en sectores de infraestructura con necesidades en tiempo real, como es el caso de sistemas de distribución de agua potable y recolección de aguas residuales, oleoductos y gasoductos, distribución y servicio de energía eléctrica o sistemas ferroviarios y de transporte público.

Adicionalmente, posibilitan el control y la gestión de todo sistema local o remoto mediante una interfaz gráfica, que oficia de nexo entre el usuario y el sistema. La misma puede ser una aplicación o varias, creadas con el propósito de ejecutarse sobre equipos que permitan controlar la producción, contando con permisos de acceso a la planta mediante comunicación digital utilizando instrumentos y actuadores, e interfaz gráfica de alto nivel para el operador (Rodríguez Penín, 2007). Deben facilitar indicadores del funcionamiento del sistema, útiles para que los operadores puedan controlarlo de forma remota y distribuida y dar respuesta eficaz a las modificaciones que puedan ir surgiendo. También deben adecuarse a las condiciones de trabajo dadas, condiciones físicas y a la evolución de objetivos de producción y modificaciones en las órdenes corporativas requeridas.

Este tipo de redes, tal como se observa en la *Ilustración 2*, se compone de los siguientes elementos con sus respectivas funciones operativas:

Servidor SCADA: Para llevar a cabo el monitoreo y la gestión de los componentes del sistema.

Servidor Histórico: Para almacenar y consolidar la información recolectada por los sensores del sistema SCADA.

Equipos de comunicación: Enrutadores, para reenvío de los paquetes entre distintas redes y conmutadores o *switches*, creando un canal de comunicación exclusivo entre el origen y el destino.

Estaciones de trabajo: Para ser utilizados por los operadores del sistema y así poder interactuar con los sistemas remotos.

HMI: Para ser utilizadas por los operadores para interpretación de los datos de los sistemas PLC y Unidades Terminales Remotas o *UTR*, mediante los cuales se supervisan los equipos y se pueden modificar los valores de sus variables. Otorgan al operador las funciones de control y supervisión. El proceso para supervisar se simboliza a través de gráficos sinópticos almacenados en la computadora, que son generados desde el editor incorporado en el sistema SCADA o invocados desde una aplicación tercera, cuando el paquete es configurado. La HMI, es la sección del sistema SCADA que proporciona interacción entre los operadores y los sistemas. Son interfaces pragmáticamente diseñadas y basadas en gráficos. Los operadores las utilizan para administrar la estructura general de la red y la comunicación generalmente se representa con símbolos gráficos secuenciales.

Protocolos: Las UTR junto con otros dispositivos de campo transmiten los datos a la red SCADA mediante protocolos ModBUS, como DNP3 o PLC (Estudios de Seguridad y Defensa, *Op.cit*, 2014).

Unidades Terminales Maestras o *MTU*: Para recopilar periódicamente datos de los PLC, procesarlos para extraer información útil, almacenar datos en el disco, disparar alarmas, seleccionar pantallas y visualizar datos históricos y actuales gráficamente y también para enviar la información seleccionada a los sistemas de información corporativos.

Sensores o actuadores: Para realizar mediciones y/o modificar cantidades físicas en el sistema.

Microcontroladores: PLC o microordenadores como, por ejemplo, Raspberry Pi, para realizar mediciones utilizando los mencionados sensores y almacenar los valores medidos en una memoria local.

Desde el punto de vista de Gómez Sarduy (2008), a estos elementos mencionados se les suman los siguientes módulos:

De Configuración: Es en donde el usuario define el entorno de trabajo de la aplicación según la necesidad de pantallas y los niveles de acceso para los distintos usuarios, importándolas desde otra aplicación o generándolas en el propio SCADA.

De Proceso: A partir de los valores vigentes de lectura de variables, es el que ejecuta los trabajos de mando preprogramados. En cada pantalla se pueden programar, en algún lenguaje de alto nivel, las relaciones entre variables de la computadora o del autómata que se ejecutan continuamente. Pueden ser acciones de mando automáticas preprogramadas dependientes de valores de señales de entrada, salida o combinaciones de éstas; maniobras o secuencias de acciones de mando; animación de figuras y dibujos; o una gestión de procedimientos para modificar los parámetros de producción dinámicamente.

De Gestión y archivo de datos: Es el que se encarga del almacenamiento, procesamiento y ordenamiento de los datos, según formatos comprensibles por periféricos de hardware o software del sistema: de esta forma, podrán ser accesibles por otra aplicación. Pueden seleccionarse datos de planta para ser capturados en intervalos periódicos y almacenados como un registro histórico de actividad, o para ser procesados inmediatamente por alguna aplicación de software estadística, de mantenimiento o de análisis de calidad (Gómez Sarduy, *et al*, 2008).

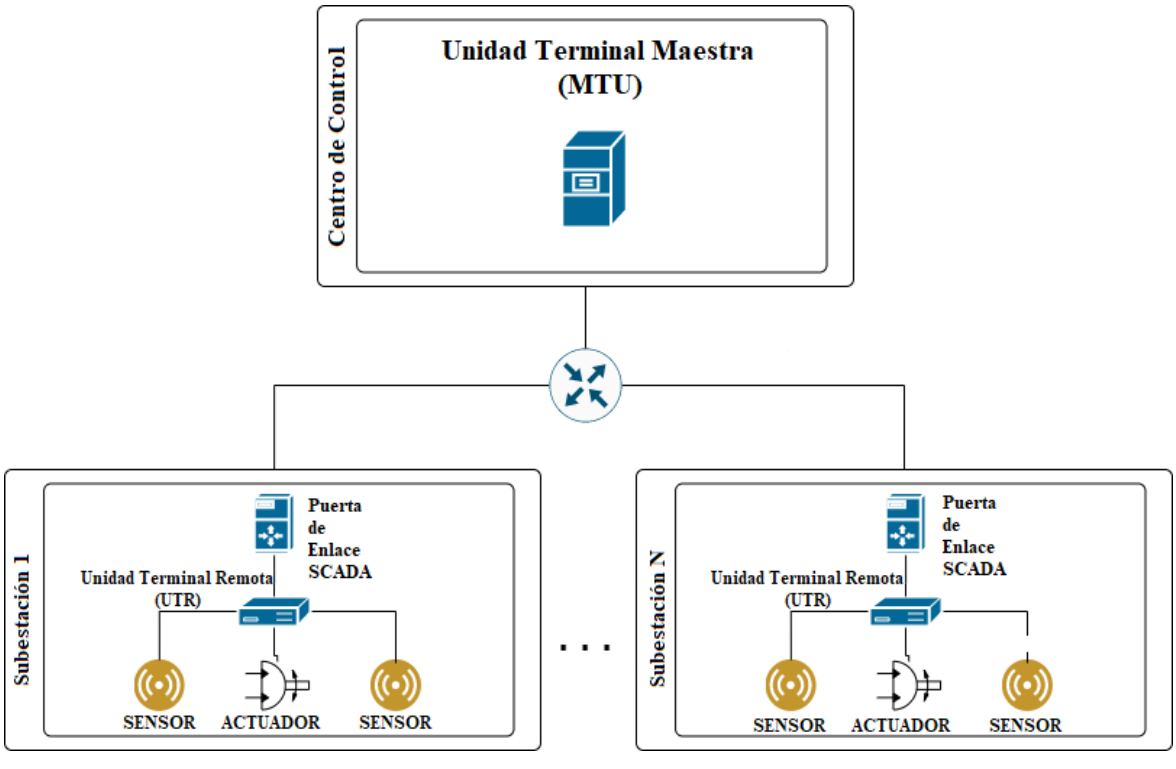


Ilustración 2: Esquema típico de una red SCADA

Ámbito de Aplicación

Los sistemas SCADA, generalmente se encuentran marcadamente presentes en el sector de la generación de la energía. Es primaria su utilización en plantas de generación de energía termoeléctrica o hidráulica y, en menor proporción, energía eólica.

Un segundo ámbito, pero no menor, es el de distribución y transmisión de la energía. En los primeros, los SCADA se hallan considerablemente extendidos, aunque ambos tienen alta dependencia de esta tecnología, debido a que deben ser controlados y monitoreados remotamente (Estudios de Seguridad y Defensa, *Op.cit*, 2014).

En general, son utilizados también en plantas químicas, industrias de petróleo y gas y plantas nucleares, para monitorear temperaturas y presiones, digitalizar y automatizar tareas tales como abrir y cerrar válvulas en tuberías y disyuntores o administrar la maquinaria de la línea de ensamblaje productiva.

La ventaja principal que tiene la utilización de sistemas SCADA, es que los mismos son sistemas automáticos y especializados que reducen los conflictos de gestión y otorgan una reacción rápida dadas las cambiantes condiciones abruptas de un proceso. La rapidez que proporcionan los SCADA, puede colaborar con el mejoramiento de la robustez y vida útil de los componentes del sistema de producción. Por otra parte, permiten también responder de forma ágil para que los operadores pueden realizar mantenimientos tempranos, cuando haga falta (*Ídem*).

Además, gracias a la adquisición de datos se puede observar la evolución del proceso controlado y la gestión de las transiciones entre los estados, la cual resulta ser una columna vertebral para las funciones de supervisión y control, permitiendo conocer el estado en el que se encuentran el proceso y la acción de control y brindando la posibilidad de cambiar los parámetros del proceso. Es importante mencionar que la adquisición de datos, en realidad consiste en el intercambio de estos bidireccionalmente: desde el proceso hasta el sistema y viceversa.

Amenazas a la Seguridad SCADA

Como ya se ha remarcado en este trabajo, los sistemas SCADA se han estado utilizando desde hace más de 50 años. No obstante, solo recientemente los investigadores y desarrolladores de sistemas han comenzado a prestar atención seriamente a la seguridad cibernética de los mismos, luego de haber acontecido varios incidentes y ataques ligados a estos. Como se detallará más adelante, muchas organizaciones han ido implementando estándares y normativas de ciberseguridad para los SCADA utilizados en las industrias ya mencionadas. Por otra parte, los desarrolladores dedicados, han estado tratando de mejorar su seguridad incorporando algunas nuevas características (Aghajanzadeh, *et al*, 2015).

A medida que estos sistemas se conectan a redes corporativas y que esas redes corporativas poseen conexión a Internet o utilizan tecnología inalámbrica, empiezan a hacerse evidentes más vulnerabilidades. Por ejemplo, una red eléctrica podría derribarse, los sistemas telefónicos de emergencia podrían quedar inutilizables o las compuertas de una presa podrían ser desactivadas. Esto sucede, en parte, debido a que estos sistemas de control no han sido diseñados y desarrollados en favor de la seguridad, sino para la eficiencia y la fiabilidad.

También sucede que una gran parte de los sistemas de control heredados no pueden adaptarse a tecnologías de seguridad más modernas como el cifrado y existen típicos problemas de gestión y culturales, de brindar atención nula a temáticas de ciberseguridad.

Por otro lado, el auge de sistemas SCADA abarcando amplias áreas geográficas de distribución de petróleo o electricidad, suele denotar la presencia de muchos sistemas maestros comunicándose con dispositivos remotos mediante Internet, radio inalámbrica, redes privadas de microondas y fibra óptica o sistemas públicos de telefonía. Las UTR no solo son controladas por su maestro, sino que también envían datos en tiempo real.

Las redes SCADA generalmente son muy dependientes de las telecomunicaciones y redes que las respaldan, lo que también las hace vulnerables debido al medio de transporte: las transmisiones podrían ser interceptadas, alteradas, redirigidas o destruidas. La utilización de módems de acceso telefónico, con precarios mecanismos autenticación, suma otra vulnerabilidad. Hoy en día, las empresas manejan cortafuegos y Sistemas de detección de

Intrusión o *IDS* en sus redes corporativas, pero muy pocas los tienen en sus redes de control, más aún, sabiendo que estas utilizan distintos protocolos (Waters, *et al*, 2008).

A partir de un potencial ciberataque a una red OT podrían ocurrir las siguientes consecuencias:

• Retraso en la comunicación entre una UTR y un MTU SCADA, lo cual podría poner vidas humanas en peligro, debido a que la información en cuestión podría ser la velocidad de una turbina, un sensor de nivel, alarmas, actuadores, etc.

• Pérdida o modificación de los valores recibidos por un MTU, pudiendo disparar una respuesta automática no deseada.

• Cambio de los valores ajustables de las UTR, que podría hacer que un recipiente se desborde, al modificar los parámetros de los sensores.

• Cambio o modificación en el funcionamiento de los sistemas de protección del equipo como, por ejemplo, la velocidad de rotación de una turbina (Murray, *et al*, *Op.cit*, 2017).

Clasificación de Ciberataques a SCADA

Dentro de los sistemas SCADA, puede haber vulnerabilidades plausibles de explotación a través de varios vectores de ataque. A saber:

• Puertas traseras y brechas en el perímetro de la red.

• Debilidades en protocolos comunes.

• Ataques a PLC y otros dispositivos de campo remotos.

• Ataques a bases de datos.

• Robo de sesiones y ataques de "Hombre en el Medio" (Estudios de Seguridad y Defensa, *Op.cit,* 2014).

Por otro lado, desde la perspectiva de un Ingeniero de control, los ataques podrían corresponder a la siguiente taxonomía:

"Manipulación de datos de entrada introducidos a través de sensores comprometidos y/o explotación de enlaces de red entre sensores y controladores; manipulación de datos de salida de sensores y controladores; controlar archivos históricos; o ataques de Denegación De Servicio […]" (*Ibídem,* p.145). Todos estos tipos de ataques serán explicados más adelante.

Como últimos comentarios sobre sistemas históricos implementados en ICS, estos solamente proporcionan un control reactivo a las fallas y no se implementan medidas proactivas para aumentar su confiabilidad. Por esto, surge la necesidad de una búsqueda de nuevas formas de gestionar los riesgos de seguridad en estas infraestructuras críticas.

El tratamiento de logs de un sistema SCADA, representa el complemento ineludible de las estrategias de gestión de seguridad tradicionales. Por lo tanto, surgirán necesidades tales como la correlación en tiempo real de información SCADA con algoritmos de detección de intrusos, la gestión del riesgo online con algoritmos de mitigación para las vulnerabilidades del sistema, técnicas de modelado avanzado para capturar la naturaleza dinámica del comportamiento del atacante, así como el comportamiento del sistema y/o modelos avanzados que hagan cuantificables los impactos (*Ídem*).

3.1.3 Infraestructuras Críticas

Las infraestructuras críticas o *IICC* son sistemas que forman parte de nuestra cotidianeidad y que requieren que se focalice fuertemente en su robustecimiento para poder ser preservadas eficientemente. La mayor parte de los servicios vitales de un país están sostenidos por infraestructuras críticas, las cuales están formadas por activos críticos conectados a diversas redes de computación, por lo cual deben ser protegidos.

Entendiendo al ciberespacio como servicios y sistemas conectados a Internet o a otras redes de datos y telecomunicaciones, las amenazas que existen en este son muchas, tal como se explicará más adelante. Los activos críticos pueden sufrir incidentes de ciberseguridad. Un potencial incidente de seguridad en las infraestructuras críticas podría tener impacto en la vida de las personas que habitan un país, afectando directamente a los sistemas físicos de este tipo como los financieros, salud, energéticos, transporte, comercio, alimentación, agua, administración, industriales, militares o de comunicaciones.

Las infraestructuras críticas "son sistemas físicos y sistemas basados en sistemas computacionales complejos que forman parte importante en una sociedad moderna y su funcionamiento fiable y seguro es de suma importancia para la vida económica y la seguridad nacional" (Ten, *et al*, 2010, p.853). A partir de su interacción, darán servicios trascendentales a las personas que habitan un país.

El término "infraestructura crítica" es usado también gubernamentalmente para describir "el conjunto de activos, sistemas y redes, sean físicas o virtuales, que resultan vitales para un país, dado que su incapacitación o destrucción debilitarían la seguridad económica nacional, la salud pública, la seguridad en general, o una combinación de ellas" (Sánchez Fernández, 2013, p.31). Estos activos pueden ser ICS para procesos automatizados, sistemas de información o bases de datos, redes de datos o industriales, instalaciones virtuales o físicas, u otros componentes de tecnología que colaboren para brindar o monitorear servicios esenciales para el bienestar de la población y la sustentabilidad de la economía de un país.

Luego de haber definido conceptualmente a las IC, se debe remarcar la importancia de su seguridad física en plantas industriales, subestaciones o plantas de gas para evitar vandalismo u otros atentados. Por esto mismo, la seguridad de estas redes es tan importante como su

resguardo patrimonial físico teniendo en cuenta el impacto que podría ocasionar su manipulación.

Según Aguirre Ponce (2014), de acuerdo con su prestación, las infraestructuras críticas pueden clasificarse como:

- De información: son las que almacenan, procesan o transmiten información confidencial o sensible. Su propietario puede ser una organización proveedora de servicios vitales, instituciones públicas o privadas o un ciudadano civil. Se debe garantizar la disponibilidad, confidencialidad e integridad de la información. Este tipo de infraestructuras suele estar a merced de fraudes, robos de información confidencial y malware dedicado a secuestrar la información sensible.

- De servicio: son las que proveen servicios vitales a un país, teniendo su indisponibilidad un impacto crítico en la población civil. Las amenazas más grandes que tienen son los ataques de denegación de servicio distribuidos y el malware que tenga como objetivo alterar el funcionamiento de los sistemas principales.

Las infraestructuras críticas industriales, para poder ser protegidas, deben ser identificadas y posteriormente clasificadas en:

- Aisladas: se organizan en redes privadas, las cuales no tienen interconexión con redes públicas ni con la red LAN corporativa, abarcando generalmente solo un área local. Se componen de software específico desarrollado especialmente para su propósito y procesos complejos encargados de su monitoreo y administración. Usualmente no es posible realizar tareas de administración en estas de manera remota y su mantenimiento es más costoso.

- Digitales: emplean redes de datos públicas y privadas. Poseen sistemas de información y procesos automatizados implementados mediante Controladores Lógicos Programables o *PLC*. El monitoreo y administración son realizados remotamente utilizando redes de Supervisión, Control y Adquisición de Datos o *SCADA*. Se conectan a redes corporativas para el análisis de información en tiempo real y la posterior toma de decisiones. Estas redes pueden abarcar extensos territorios geográficos (Aguirre Ponce, 2014).

3.1.4 Convergencia de los Mundos: IT/OT

Las redes de las compañías industriales más importantes, en la actualidad están compuestas por dos segmentos principales: la red LAN Corporativa o *IT* y la red de ICS propiamente, que usualmente se compone de varios PLC y SCADA. Si bien históricamente han estado separados completamente, los mismos pueden interconectarse operativamente para optimizar las funcionalidades propias de cada mundo, proporcionando información en tiempo real para la toma de decisiones, mediante la facilidad en la comunicación entre las dos partes delimitadas de la organización y tomando en cuenta las medidas de seguridad necesarias.

De todas maneras, la gran mayoría de los sistemas OT vigentes, aún continúa trabajando de manera relativamente aislada respecto de los sistemas y la infraestructura de IT y ni siquiera está contemplada la posibilidad de un ciberataque, tanto desde una perspectiva de detección como de defensa. Esto termina siendo un punto débil transcendental, por ejemplo, en períodos de mantenimiento, donde los contratistas utilizan dispositivos multimedia como notebooks, discos duros portátiles, unidades flash USB (pendrives), etc. como soporte dentro de la infraestructura industrial.

Por esto, se ahondará en las cuestiones más importantes necesarias a la hora de hacer convivir y trabajar cooperativamente a ambos mundos.

Modelo de Convergencia entre Redes

Como se ha mencionado en los apartados anteriores, las OT son sistemas de control y comando compuestos por hardware y software, que monitorean y controlan plantas industriales y sus equipos asociados. Comprenden, entre otros, sensores, PAC, PLC y otras unidades. Estas redes tienen como objetivo principal enviar órdenes para accionar los medios productivos y compilar eventos sobre el progreso de los procesos industriales.

Por otra parte, también se ha descripto que las IT son sistemas de información orientados hacia el recabado y procesamiento de la información corporativa. Son utilizados para satisfacer la necesidad de tareas de los diferentes departamentos de una compañía: abastecimiento, logística, finanzas, recursos humanos, etc.

La convergencia IT/OT corresponde a una tendencia creciente al entrelazamiento entre ambos mundos, que permite a IT hacer que datos tales como pedidos productivos o cantidad de stock de materiales, estén disponibles en tiempo real para las máquinas para así poder optimizar la producción. Actualmente, los conceptos de productos o servicios contribuyen a esta convergencia, haciendo partícipes a las diferentes áreas interesadas según cuáles sean las soluciones propuestas (Bonnetto, *et al*, *Op.cit*, 2017). Esto significa, entonces, que las estrategias de las áreas deben armonizarse, instalándose modelos comunes de procesos y de gobierno, así como la seguridad y los datos deben administrarse centralizadamente y los recursos humanos deben capacitarse para conocer y sobre todo comprender, los requisitos de ambas disciplinas. En la *Ilustración 3*, se puede observar un típico esquema de convergencia.

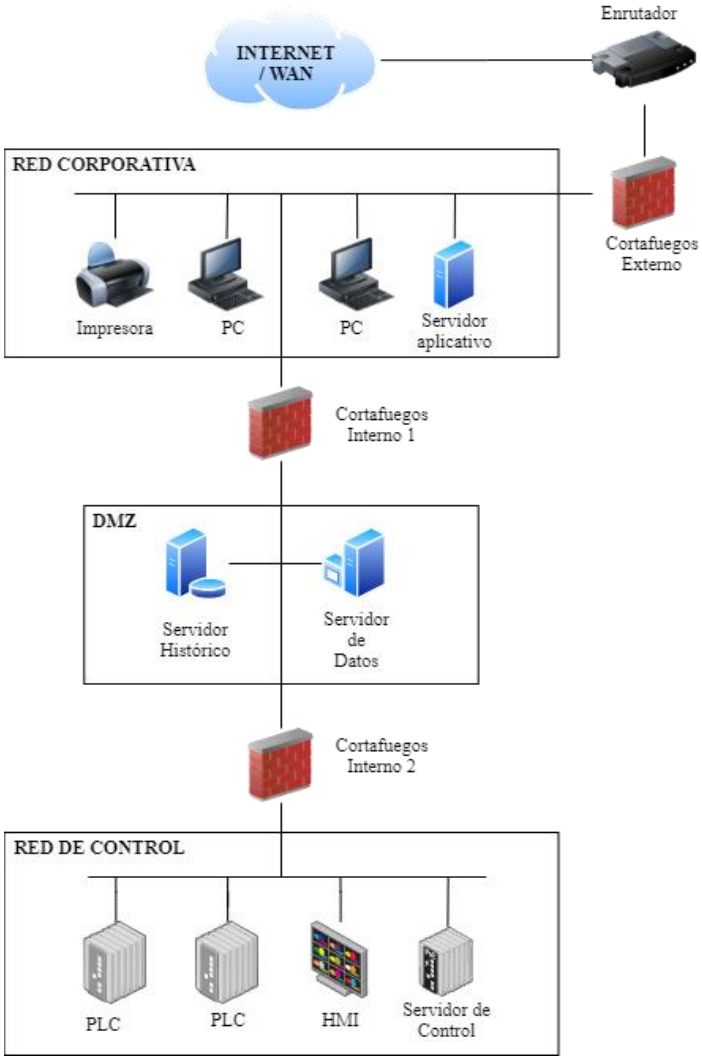


Ilustración 3: Esquema sugerido por NIST para la convergencia, con cortafuegos emparejados entre ambas redes

Diferencias Principales de Abordaje de Ambas Orientaciones

La convergencia está siendo impulsada por la creciente necesidad de informes de gestión cuantitativos, asistidos por big data, inteligencia artificial, automatización, operaciones remotas, computación en la nube, análisis, etc. (Shahzad, *et al*, *Op.cit*, 2016).

La *Tabla 1* revela algunas de las diferencias notables entre los mundos IT y OT. Si bien se dejan en evidencia cuáles son las prioridades de cada uno, será necesario poder interconectar instalaciones para que exista la posibilidad de acceder a los datos en tiempo real y así administrarlos de manera eficiente.

Tabla 1: Principales diferencias entre las redes IT y OT

Dimensiones	**IT**	**OT**
Individualismo o Colectivismo	*Colectivista*	*Colectivista*
Protocolos	*Estandarizados*	*Propietarios*
Foco de Protección	*Datos*	*Activos físicos*
Ambiente	*Físico controlado*	*Físico geográficamente disperso*
Orden de prioridades	*1) Confidencialidad →* *2) Integridad →* *3) Disponibilidad*	*1) Disponibilidad →* *2) Integridad →* *3) Confidencialidad*
Frecuencia de aplicación de actualizaciones	*Alta*	*Baja*
Orientación a largo plazo	*No*	*Sí*
Tipo de sistema operativo	*Estandarizado*	*Propietario*
Motivación del cibercriminal	*Monetaria*	*Ruptura*

Por un lado, la seguridad de IT se centra en preocupaciones que pueden asociarse frecuentemente con la integridad financiera, la degradación del servicio o la pérdida de

información. Las propiedades pueden agruparse y priorizarse, en orden, en confidencialidad, integridad y disponibilidad, tal como sucede en el mundo de la ciberseguridad.

La prioridad de IT es proteger los datos, por lo tanto, su evolución se ha apoyado en herramientas y procedimientos pragmáticos que los intentan preservar de las amenazas cibernéticas.

En contraposición con lo mencionado, para el entorno OT la seguridad y el riesgo operativo son críticos, cambiando el orden de las prioridades: disponibilidad de los datos para mantener la producción de forma segura, integridad y, por último, confidencialidad.

Para este espacio, el objetivo es proteger al conjunto de activos físicos y su producción. Esto se ha traducido en un esfuerzo mínimo para cambios y actualizaciones, debido a que es casi seguro que la producción tenga que desconectarse para lograr los objetivos de mejoras. Este freno potencial de producción y su pérdida de ingresos asociada, sumada a los costes de diseñar e implementar las soluciones, han dado como resultado que los sistemas OT se retrasen de manera significativa con respecto al abordaje de ciber-amenazas de los sistemas de IT (Murray, *et al*, *Op.cit*, 2017).

Ambos mundos, en conjunto, son necesarios para llevar a cabo las operaciones en un sitio industrial, requiriendo dos tipos diferentes de actores para usar o configurar ambas tecnologías, como se ve en la *Ilustración 4*.

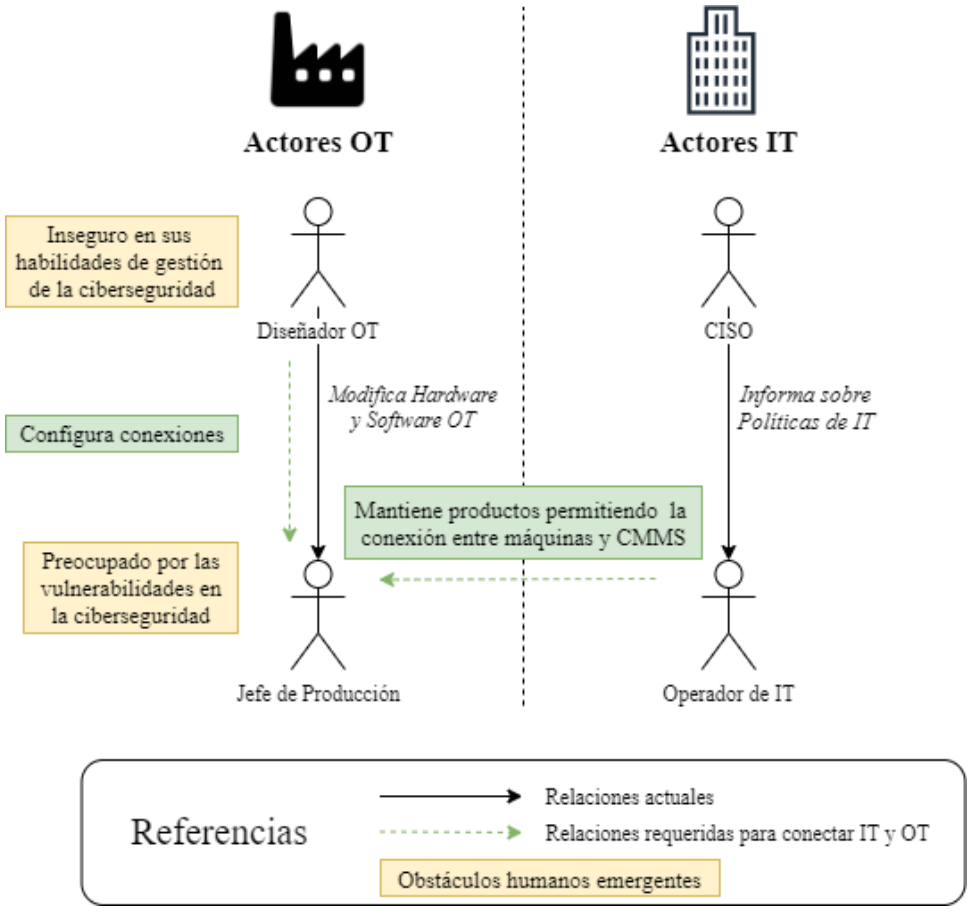


Ilustración 4: Interacción entre actores IT y OT

Enfoques para la Aplicación

Según Cisco (2008), existen 4 enfoques que rodean al universo de la convergencia IT/OT y apoyan su implementación.

I- Aplicar computación de niebla para permitir la toma de decisiones en tiempo real

Este enfoque conserva el ancho de banda, filtrando cuándo y cómo se utilizan los recursos del centro de datos. Para ello, se crea un sistema más escalable y mejora la seguridad general del sistema con la computación de niebla o *fog computing*. Así, el área de IT puede contar así con una certera taxonomía de datos: los datos que son sensibles al tiempo pueden analizarse en el nodo más cercano al dispositivo que genera los datos, los datos que pueden esperar segundos o minutos se pueden pasar a un nodo intermediario que vigile los datos operativos y los datos menos sensibles al tiempo se envían a la nube para su análisis histórico y almacenamiento.

II- Eliminar el tiempo ocioso a través del mantenimiento predictivo

La convergencia IT/OT está creando un cambio de paradigma en el mantenimiento de la fábrica. Los equipos de operaciones planifican y realizan mantenimiento preventivo en entornos de fabricación, en un horario determinado para disminuir la probabilidad de averías en los equipos. Este enfoque requiere que una planta mantenga una base de datos de sus activos, que realice el seguimiento de su estado y confíe en las recomendaciones de los fabricantes para determinar cuándo y cómo mantenerlos. Estos sistemas utilizan inteligencia de datos reales de la fábrica, en lugar de usar meras estimaciones o conjeturas. El cambio a un enfoque de mantenimiento predictivo mejora significativamente los tiempos de actividad y es compatible con la convergencia IT/OT: operaciones recopila en fábrica datos claves de sensores, máquinas y PLC, mientras que IT brinda el análisis de datos y otras herramientas para darles significado a los mismos.

III- Implementación de tecnología inalámbrica en la fábrica

La utilización de la tecnología inalámbrica agrega valor a la tarea de numerosas máquinas, sensores y PLC, además de las plataformas de análisis y las tecnologías auxiliares ya mencionadas, que son ejecutadas en paralelo. Sin embargo, hasta hace no mucho tiempo atrás, la implementación inalámbrica en toda la planta era una opción poco plausible. No obstante, en los últimos años se han presentado grandes avances en la tecnología inalámbrica, ahora con una mayor capacidad de recuperación, lo que la hace más asequible y práctica para entornos industriales y más rápida de implementar, sin importar las conexiones físicas y edilicias de las plantas.

En resumen, la tecnología inalámbrica permite una mayor flexibilidad y adaptabilidad para el monitoreo remoto, cambios de línea de montaje e iniciativas de calidad o cadena de suministro, mientras que también puede generar importantes ahorros económicos.

IV- Garantizar la ciberseguridad para todo el universo de equipos conectados

Proteger la propiedad intelectual y la información del cliente son tareas primordiales para la viabilidad a largo plazo y la reputación de una empresa, y muestran cómo la ciberseguridad es una misión crítica dentro de los procesos de fabricación. Los sistemas de producción comprometidos podrían verse afectados en cuanto a su calidad, rentabilidad e incluso seguridad física. Sin embargo, es necesario comprender cómo el hecho de vincular las máquinas a la red corporativa puede traer múltiples ventajas, como se ha detallado en los tres puntos anteriores. Las soluciones actuales deben conectar redes y permitir la supervisión y el flujo seguro de datos, siendo implementables en entornos preexistentes y en dispositivos heredados. Además, deben ofrecer características de defensa en profundidad para organizar, fortalecer, defender y responder a las amenazas.

La implementación de este nuevo enfoque de ciberseguridad en la fabricación requiere la colaboración y trabajo conjunto tanto de IT como de las operaciones. Para esta segregación de tareas, IT brinda una comprensión profunda de los protocolos y políticas de ciberseguridad, así como experiencia en la administración de la implementación y la garantía del cumplimiento. Pero para que la ciberseguridad logre implementarse en la fabricación, entrará en juego la experiencia de los equipos de operaciones, que desempeñan un papel fundamental en el proceso en cuestión (IT/OT Convergence: Moving Digital Manufacturing Forward, 2018).

Beneficios de la Convergencia IT/OT

Más allá de los problemas que se han expuesto existentes en ambos mundos, sin dudas ha sido posible dejar en evidencia las ventajas tangibles y claras para las empresas. Estas incluyen reducciones de riesgos y costos, tanto como notables mejoras de flexibilidad, optimización y rendimiento. Es importante destacar que previamente se deben dominar los desafíos estratégicos, organizativos y tecnológicos planteados en los subapartados anteriores. Adicionalmente, debe emplearse la gestión del cambio para garantizar que el proceso de implementación funcione sin problemas.

Si se construye sobre estos cimientos esenciales de la convergencia de IT/OT exitosa, las empresas serán capaces de marcar la diferencia a la hora de la competencia, permitiéndoles

explotar capacidades no evidentes en su cadena de suministro agilizando los procesos, aumentando la transparencia de los datos y permitiendo una mejor y más rápida toma de decisiones.

3.2 Marco Normativo Vigente

3.2.1 ISO/IEC 27000-SERIES

International Organization for Standards o *ISO*, es el mayor editor y desarrollador de estándares existente, pudiéndose encontrar presente en más de 150 países. Se trata de un organismo conformado por una red de institutos nacionales de normalización, que promocionan el desarrollo de normas internacionales de cumplimiento voluntario. Las mismas aplican a diferentes ámbitos como las comunicaciones, el comercio y la fabricación industrial, exceptuando los rubros electrónico y eléctrico.

La serie ISO 27000 se publicó originalmente en 2000, reemplazando a la norma ISO 17799 de 1995, sobre todo con el contenido superador de la 27002 aunque manteniendo su estructura. Previamente, la ISO 17799 dividía el universo de seguridad en diez jerarquías de materias principales que contenían treinta y seis controles en el nivel superior, con casi doscientas políticas recomendadas (Jaquith, 2007).

Particularmente, la serie 27000 compone un conjunto de guías y estándares de seguridad, que contienen las mejores prácticas recomendadas en el ámbito de Seguridad Informática para el desarrollo, la implementación y la gestión de un Sistema de Gestión de Seguridad de la Información o *SGSI*, gracias a quien una organización está en condiciones certificar sus prácticas de seguridad (The Standard of Good Practice for Information Security, 2014).

ISO/IEC 27000 está compuesta por los siguientes documentos, entre los más importantes para mencionar:

ISO/IEC 27000: brinda el panorama general con el vocabulario y los términos asociados al SGSI.

ISO/IEC 27001: contiene los requisitos para implantar un SGSI válido.

ISO/IEC 27002: es el código de prácticas correctas para los controles de ciberseguridad.

ISO/IEC 27003: guía de orientación para implementar la gestión de un SGSI.

ISO/IEC 27004: colabora con el seguimiento, medición, análisis y evaluación de un SGSI, para poder medir según el grado de implantación, la eficacia y eficiencia de este.

ISO/IEC 27005: brinda recomendaciones sobre cómo gestionar los riesgos de ciberseguridad.

ISO/IEC 27006: contiene los requisitos de certificación de SGSI para conseguir la acreditación como organización certificadora.

ISO/IEC 27007: es un conjunto de pautas para la auditoría de SGSI.

ISO/IEC 27035: documento de gestión de incidentes ciberseguridad.

ISO/IEC 27799: indica el marco de implementación de la mencionada ISO/IEC 27002 en la industria de la salud (Sánchez Fernández, *Op.cit*, 2013).

De acuerdo con el foco de nuestro estudio, las regulaciones más importantes en las que se hará hincapié serán la ISO/IEC 27001 y ISO/IEC 27002.

ISO/IEC 27001

La ISO/IEC 27001 es el único estándar aceptado internacionalmente para la certificación de la gestión de la ciberseguridad: reúne los requisitos para la evaluación, implantación, operación y para el tratamiento de sus riesgos, los cuales están adecuados a los requisitos genéricos de las organizaciones. El mismo ha sido publicado como tal por la ISO y por la comisión International Electrotechnical Commission o *IEC* en octubre del año 2005, habiendo tenido importantes actualizaciones en la posterioridad, entre las que se destacan la 2013 y la 2018. Para los fines de este trabajo, las actualizaciones que se han realizado sobre los controles con posterioridad a la versión 2013, no tienen impacto adicional.

Esta norma está basada en la BS7799-1 y la BS7799 de *British Standards Institution* y es para la norma principal de la serie 27000. Contiene el conjunto formal de especificaciones para establecer, implementar, monitorear, revisar, mantener y mejorar un SGSI en una organización y así poder obtener la acreditación correspondiente.

El estándar se puede aplicar en cualquier tamaño y tipo de organización y se basa en el *ciclo de Deming* que, en español es, “Planificar, Hacer, Verificar y Actuar”, utilizado en distintos ámbitos.

La norma se divide en varias secciones y tres apéndices, que presentan las bases y los diferentes aspectos de un SGSI. A continuación, se resumirán las secciones y el anexo más importantes.

Sección 4: el SGSI compone la mayoría de la sección, basada en las actividades requeridas por el ciclo PDCA como pruebas de la operación. Primero, *planificar* para poder comprender requisitos, evaluar riesgos, decidir qué controles serán las aplicables. Luego *hacer*: implementar y posteriormente operar el SGSI realizando todos los controles definidos hasta el momento. En tercer lugar, *verificar*, para el monitoreo y revisión del SGSI. Por último, *actuar*: para el mantenimiento y la mejora continua del SGSI.

Sección 5: indica la responsabilidad y compromiso de la Dirección para con el SGSI.

Sección 6: especificación para auditorías internas periódicas en el SGSI para asegurar la eficiencia de los controles.

Sección 7: detalla la revisión a realizar por parte de la Dirección, al menos anualmente, para hallar oportunidades de mejora y la necesidad de cambios.

Sección 8: indica las mejoras continuas en el SGSI utilizando la evaluación como instrumento, tratando la no conformidad (Sánchez Fernández, *Op.cit*, 2013).

Adicionalmente, también presenta un Anexo A, el cual sintetiza los controles y objetivos que se desarrollarán en la norma ISO/IEC 27002 para que contribuyan al robustecimiento de los SGSI de las distintas organizaciones. Si bien, todos estos controles no son necesariamente obligatorios, sí lo es la justificación de no aplicarlos.

ISO/IEC 27002

La ISO/IEC 27002 es un documento que reúne buenas prácticas respecto a técnicas de ciberseguridad, utilizado por las organizaciones como guía para implementar controles que permitan seguir la norma 27001, con el objetivo de obtener la certificación pertinente para el SGSI en cuestión.

En el mismo, se detallan 133 controles y 33 objetivos de control. Para todos, se presenta una descripción, guías para la implementación e información asociada, agrupada en diversas categorías. Las principales son: "Evaluación y tratamiento del riesgo", "Política de ciberseguridad", "Aspectos organizativos de los sistemas de información", "Gestión de activos", "Seguridad ligada a los recursos humanos", "Seguridad física y del entorno", "Gestión de las comunicaciones y operaciones", "Control de acceso" y "Adquisición, desarrollo y mantenimiento de los sistemas de información". Sobre los mencionados activos, se puede observar su taxonomía en la *Ilustración 5* (*Ídem*).

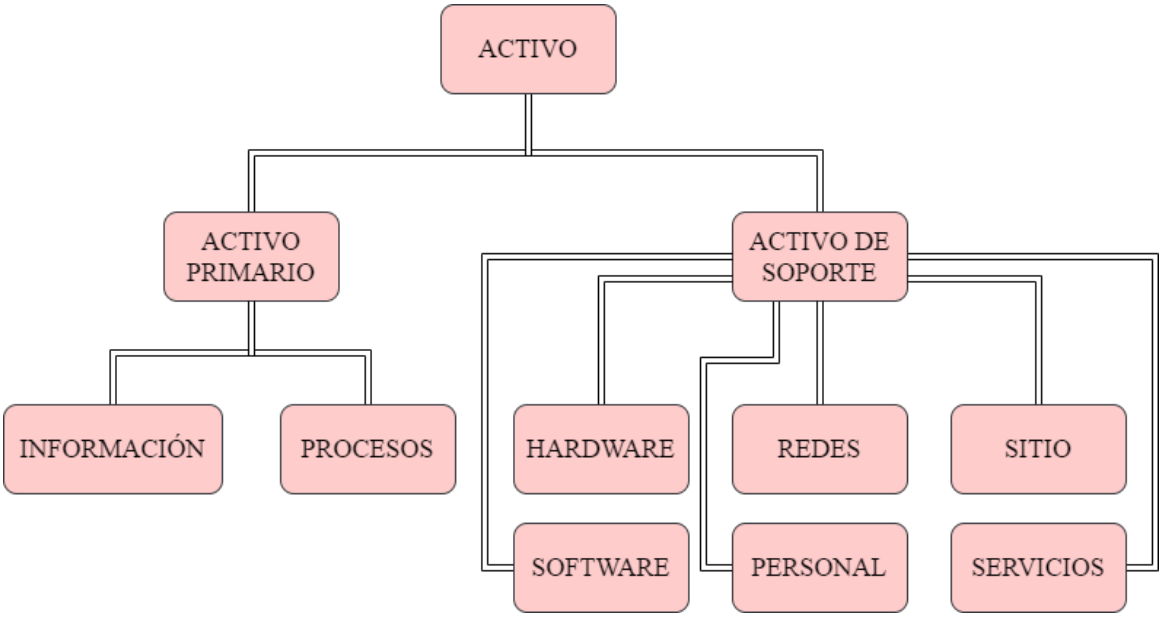


Ilustración 5: Taxonomía de los activos en ISO/IEC 27002

ISO/IEC 27010

La norma ISO/IEC 27010 se publicó el 20 de octubre de 2012. Está compuesta por una guía para la gestión de la seguridad de la información, cubriendo los casos en que esta sea

compartida entre distintas organizaciones o áreas. Por lo tanto, puede aplicarse para participaciones e intercambios de información relacionados con el suministro, protección y mantenimiento de una organización pública o privada, o bien, de infraestructuras críticas de los estados y naciones, en el ámbito nacional e internacional. ISO/IEC 27010 puede ser aplicada en organizaciones de industrias o sectores productivos similares o diversos (Suárez, *et al*, 2012).

ISO/IEC 27032

La norma ISO/IEC 27032 entró en vigor el 16 de Julio de 2012. Se trata de una guía orientativa para mejorar el estado de la ciberseguridad, obteniendo sus aspectos únicos y de sus actividades dependientes, como la seguridad en Internet, la seguridad de las redes y la seguridad de infraestructuras críticas. Esta norma está basada en una descripción general de la ciberseguridad, una definición de las partes interesadas con su descripción según su función, los alineamientos para enfrentar los problemas más comunes en el ámbito de la ciberseguridad y un marco que ayuda a que las partes interesadas puedan colaborar en conjunto con el objetivo común de la solución de problemas en el ámbito de la ciberseguridad (*Ídem*).

3.2.2 ISO 22301

Se trata una norma de carácter internacional, publicada en mayo de 2012, empleada para gestionar la continuidad del negocio, por lo cual se deja evidencia y documentación de los requisitos para la planificación, establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora continua de un SGSI para la protección y reducción de la probabilidad de ocurrencia de las interrupciones del servicio debido al surgimiento de incidentes, así como también su restablecimiento rápido. De manera similar a la ISO/IEC 27001, también presenta requisitos genéricos aplicables transversalmente a todas las organizaciones (International Organization for Standardization, 2012).

3.2.3 COBIT

La guía de Objetivos de Control para la Tecnología de la Información o, simplemente *COBIT*, ha sido desarrollada como un estándar internacional de controles generalmente aplicables y

aceptados para buenas prácticas de seguridad IT, es decir, aceptadas por la comunidad de expertos. Se publicó por primera vez por la Asociación de Auditoría y Control de Sistemas de Información, conocida por sus siglas como *ISACA*, en el año 1996 y presenta actualizaciones frecuentemente.

Su objetivo es investigar, publicar y promover con autoridad objetivos de control en IT.

Si bien se trata de un estándar relativamente breve en tamaño, su finalidad es la practicidad para atender las necesidades del negocio, manteniendo al mismo tiempo una independencia con respecto a las plataformas técnicas de IT adoptadas en una organización (Castello, 2006).

Está basada en cinco principios clave para el gobierno y la gestión corporativa de IT:

Principio 1: satisfacer las necesidades de las partes interesadas equilibrando beneficios, optimización del riesgo y uso de los recursos.

Principio 2: cubrir a la empresa de extremo a extremo, integrando la gobernanza de IT empresarial con la gobernanza de la empresa. No se focaliza solamente en la función de IT, sino que trata la información y las tecnologías relacionadas a estas como activos igualmente importantes.

Principio 3: aplicar un marco único e integrado. COBIT se alinea con otros estándares y marcos relevantes a alto nivel y, por lo tanto, puede servir como marco general para el gobierno y la gestión de IT empresarial.

Principio 4: habilitar un enfoque holístico, teniendo en cuenta a todas las categorías de componentes que interactúan. Estas incluyen principios, políticas, marcos, procesos, estructuras organizativas, cultura, ética, comportamiento, información, servicios, infraestructura, aplicaciones, personas, habilidades y competencias.

Principio 5: separar la gobernanza de la administración. La gobernanza avala que los requerimientos, opciones y escenarios de las partes involucradas puedan evaluarse para delimitar cuáles serán los objetivos empresariales equilibrados y consensuados que deberán alcanzarse. También ayuda a precisar la dirección mediante priorización y toma de decisiones y a monitorear desempeño y cumplimiento de estos objetivos. La administración, por otra parte, planea, construye, hace y monitorea las actividades que están alineadas con la dirección

establecida por el órgano de gobierno. En la mayoría de las empresas, la administración es responsabilidad del director ejecutivo o *CEO*.

Juntos, estos principios que se detallaron le sirven a la empresa para elaborar un marco efectivo de gobierno y gestión que sea capaz de optimizar la inversión y el uso de la información y la tecnología en beneficio de las áreas participantes (ISACA, 2012).

Según Andrew Jaquith (2007), COBIT se aplica en organizaciones que deseen implementar programas de gobierno. Para ello, define treinta y cuatro objetivos de control observables en la *Tabla 2*, agrupados en los siguientes dominios:

- Planificación y organización: son procesos para definir planes estratégicos de ciberseguridad, determinando los presupuestos generales del programa y los niveles de inversión, evaluando el riesgo y administrando los recursos humanos y organizacionales.
- Entrega y soporte: son procesos para definir niveles de servicio, gestión de accesos internos y de terceros, formación de usuarios finales, manejo de incidentes y programas operativos para asegurar datos, instalaciones y operaciones.
- Adquisición e implementación: son procesos para identificar, adquirir, desarrollar e instalar soluciones de seguridad.
- Monitoreo: son procesos que permiten realizar el monitoreo de los sistemas, evaluando la efectividad de los controles de seguridad y respaldando los procesos de auditoría (Jaquith, *Op.cit,* 2007).

Tabla 2: Objetivos de control de COBIT

Planificación y organización	**Entrega y soporte**	**Adquisición e Implementación**	**Monitoreo y evaluación**
PO1: Definir un plan estratégico de IT	**DS1:** Definir y gestionar los niveles de servicio	**AI1:** Identificar soluciones automatizadas	**M1:** Supervisar y evaluar el rendimiento de IT
PO2: Definir la arquitectura de la información	**DS2:** Administrar los servicios de terceros	**AI2**: Adquirir y mantener el software de aplicación	**M2:** Supervisar y evaluar el control interno
PO3: Determinar la dirección tecnológica	**DS3:** Gestionar el rendimiento y la capacidad	**AI3:** Adquirir y mantener infraestructura tecnológica	**M3:** Garantizar el cumplimiento normativo
PO4: Definir los procesos, la organización y las relaciones de IT	**DS4:** Garantizar un servicio continuo	**AI4:** Habilitar la operación y el uso	**M4:** Proporcionar gobierno de IT
PO5: Gestionar la inversión en IT	**DS5:** Garantizar la seguridad de los sistemas	**AI5:** Gestionar los recursos de IT	
PO6: Comunicar objetivos de gestión y dirección	**DS6:** Identificar y asignar costos	**AI6:** Gestionar cambios	
PO7: Gestionar recursos humanos de IT	**DS7:** Educar y capacitar a los usuarios	**AI7:** Instalar y acreditar soluciones y cambios	
PO8: Gestionar la calidad	**DS8:** Administrar la mesa de servicio e incidentes		
PO9: Evaluar y gestionar los riesgos de IT	**DS9:** Administrar la configuración		

PO10: Gestionar proyectos	**DS10:** Gestionar problemas		
	DS11: Administrar datos		
	DS12: Gestionar el entorno físico		
	DS13: Administrar operaciones		

COBIT fue originalmente pensada como un marco formal para poder alinear los requisitos comerciales, los procesos y los recursos de IT. Está basada y extiende:

- Principios de calidad: costo, calidad y cumplimiento de entrega.
- Principios fiduciarios: efectividad y eficiencia en operaciones, confiabilidad de información y cumplimiento de regulaciones.
- Requisitos de seguridad: confidencialidad, integridad y disponibilidad (*Ídem*).

3.2.4 NIST

El sistema de calidad NIST respalda la prestación de servicios de medición: mediciones y pruebas especiales, materiales de referencia estándar y productos de datos de referencia estándar. El sistema de calidad NIST para servicios de medición es reconocido internacionalmente y cumple con los requisitos del Acuerdo de Reconocimiento Mutuo o *MRA* del Comité Internacional para Pesos y Medidas o *CIPM* (Aguirre Ponce, *Op.cit*, 2014).

El enfoque del marco NIST para incrementar la ciberseguridad en infraestructuras críticas, se focaliza en los riesgos, siendo utilizado principalmente para colaborar en la identificación y priorización de operaciones que los reduzcan.

Las cinco categorías de controles NIST abarcan tareas elementales y de alto nivel en el ámbito de la ciberseguridad, alineadas con las técnicas vigentes de gestión de incidentes, para comprender fácilmente por qué debe invertirse, en términos económicos, en ella. A saber:

- Identificar: consiste en otorgar una mirada de concientización respecto a la gestión del riesgo sobre activos de información y sistemas, en el ámbito de la ciberseguridad que pudieran afectarlos. Identificar, propiamente hablando, abarca actividades como comprender el contexto, los riesgos en la ciberseguridad y los recursos que dan soporte a servicios críticos, para permitir a la organización focalizarse en priorizar esfuerzos.
- Proteger: está orientada hacia el desarrollo de mecanismos adecuados que aseguren la continuidad en la prestación de servicios críticos. Para ello, será necesario desarrollar procesos que aseguren la contención del impacto de un potencial ciberataque.
- Detectar: radica en la implementación de procesos adecuados para la identificación oportuna de eventos relacionados con ciberataques.
- Responder: se orienta hacia desarrollar e implementar procesos que, en caso de presentarse un evento de seguridad, sean útiles para la toma de decisiones.
- Recuperar: consiste en el desarrollo e implementación de procedimientos de resiliencia y restauración oportuna de los servicios y operaciones con afectación debido a un potencial evento de ciberseguridad (*Ídem*).

SP 800-30

La normativa NIST SP 800-30 se creó en Estados Unidos en septiembre de 2012 con el propósito de establecer una metodología para evaluar los riesgos en IT, desde el punto de vista gubernamental, corporativo, con el objetivo de garantizar la toma de decisiones, para llevar a cabo tareas de protección de la Ciberseguridad y así poder alcanzar niveles de riesgo aceptables para los estándares de la organización. Esta normativa tiene en cuenta particularmente las ciber-amenazas de IT, es decir tipos de ataques con la capacidad de perjudicar los intereses de la seguridad nacional, especialmente las infraestructuras críticas de las áreas importantes que se han mencionado en el apartado 3.3. El informe SP 800-30 brinda también recomendaciones de comunicación para terceros: compartirles a estos las vulnerabilidades, amenazas y riesgos en los propios activos y servicios de IT, de forma tal de poder prevenir propagaciones que puedan perturbar las actividades de otras organizaciones y su personal.

Otro tema que también es tenido en cuenta es la manifestación de nuevas amenazas, vulnerabilidades y riesgos, poniendo el foco en los servicios en la nube y dispositivos móviles propios: Bring Your Own Device o *BYOD*.

Es importante destacar que la guía NIST SP 800-30, no fundamenta indicadores o métricas. Para esto, se dispone de otra publicación de la serie que se tratará a continuación. (Suárez*, et al*, *Op.cit*, 2015).

SP 800-55

El documento NIST SP 800-55 o "Guía de métricas de seguridad para sistemas de tecnología de la información", amplía el trabajo previo de NIST en el campo de medidas de seguridad de la información para proporcionar pautas adicionales a nivel de programa para cuantificar el rendimiento de la seguridad de la información en apoyo de los objetivos estratégicos de la organización.

Esta publicación especial, se creó en julio de 2008 y es una guía para el desarrollo específico, selección e implementación de medidas a nivel de sistema de información y a nivel de programa para indicar la implementación, impacto, eficiencia y efectividad de los controles de seguridad. Provee pautas sobre cómo una organización, mediante el uso de medidas, identificación de controles de seguridad, políticas y procedimientos en el lugar, puede ayudar a los rangos más altos a decidir dónde invertir en recursos adicionales de seguridad de la información, así como poder evaluar controles no productivos y priorizar controles de seguridad para monitoreo continuo y supervisión.

Es importante utilizar medidas adecuadas y presentar los resultados para poder preparar correctos informes de rendimiento (National Institute of Standards and Technology, 2008).

SP 800-53

La guía SP 800-53, publicada por primera vez en febrero de 2005, representa a un conjunto de controles agrupados en 18 familias: controles para gestión de la respuesta ante incidentes, protección de los sistemas, protección de los activos de comunicación, continuidad del negocio, etc. La misma, tiene una orientación holística de la seguridad de la información,

gracias al mencionado conjunto de controles, lo cual permite enfrentar todo tipo de ciber-amenazas a las que se exponen los gobiernos y las organizaciones privadas.

Cabe destacar que con esta guía se dispone adicionalmente de técnicas de evaluación sobre los controles para determinar su eficacia, para asegurar su robustez, comparabilidad y repetitividad. En la norma está contemplado el reporte de resultados de estas evaluaciones, para poder presentarlos ante las autoridades referentes (National Institute of Standards and Technology, 2020).

SP 800-82

El documento *"Guía de control de supervisión y adquisición de datos (SCADA) y seguridad de sistemas de control industrial"*, publicado por primera vez en enero de 2011, brinda un enfoque para avalar sistemas seguros de control industrial.

Como se ha explicado en el punto 3.1.2, los ICS, que están compuestos por SCADA, sistemas de control distribuido o *DCS* y otros tipos de configuraciones de sistemas de control menos relevantes en tamaño, son hallados habitualmente en sectores de control industrial.

Se ha aclarado ya que los ICS se usan generalmente en industrias tales como petróleo, agua, gas, electricidad, química, alimentos, transporte, farmacéutica, etc. y es común que se usen SCADA para controlar los activos dispersos mediante la adquisición centralizada de datos y el control de la supervisión. Los DCS, por lo general son usados para controlar los sistemas de producción en un rango local y los PLC suelen abarcar el control discreto para aplicaciones específicas. Estos sistemas de control son críticos para el funcionamiento de las infraestructuras críticas.

Esta guía brinda una visión general de los sistemas de control industrial mencionados y sus topologías típicas, detectando las vulnerabilidades y amenazas más comunes y proporcionando contramedidas de seguridad recomendadas para mitigar los riesgos ligados.

Retomando el contenido del apartado 3.1.4, con el auge de la convergencia IT/OT los dispositivos IP ahora están reemplazando las soluciones patentadas, lo cual aumenta considerablemente la probabilidad de aparición de vulnerabilidades y la manifestación de incidentes de ciberseguridad. Los ICS presentan requisitos únicos de rendimiento y

confiabilidad y a menudo usan sistemas operativos y aplicaciones propietarios. Sin embargo, paulatinamente están utilizando cada vez más soluciones IT y paulatinamente se van asemejando a estos sistemas. Al ser diseñados e implementados utilizando computadoras, protocolos de red estándar de la industria y sistemas operativos, con el objetivo de garantizar la conectividad y el acceso remoto, se empiezan a requerir nuevas soluciones de seguridad que sean adaptables al entorno ICS (National Institute of Standards and Technology, 2006).

El objetivo de esta guía es brindar las mejores prácticas de protección, restricción y mantenimiento para considerar en una implementación ICS. Por otra parte, también pone énfasis en las características y grado de *expertise* que debe poseer el equipo de ciberseguridad, teniendo en cuenta sus responsabilidades y aspectos que involucren a los proveedores de servicios ICS. El programa ideal de ciberseguridad deberá adoptar la estrategia de "*defensa en profundidad*", de manera tal de minimizar el impacto de las potenciales fallas, para garantizar la continuidad del negocio y velar por la integridad de los datos. Todos estos aspectos, se detallarán en el subapartado 3.4.6.

3.2.5 ITIL

IT Infrastructure Library o *ITIL* es el enfoque que está mayormente aceptado para la gestión de servicios de IT en todo el mundo. Surgido en 2006 formalmente como ITIL 2, proporciona un compendio de buenas prácticas, que se han extraído de los sectores público y privado a nivel internacional. Está respaldado por un esquema integral de calificaciones, organizaciones de capacitación acreditadas y herramientas de implementación y evaluación.

Beneficios del Diseño y la Gestión de los Servicios IT

La característica más relevante de ITIL es exponer cuáles son las mejores prácticas de Gestión de Servicios de IT en relación con el enfoque de los procesos, los cuales tienen como objetivo satisfacer los servicios los requerimientos del negocio desde el lado de IT, conllevando a varios beneficios.

Por un lado, surge un notable incremento de la calidad del servicio mismo, materializado en un mejor servicio de soporte IT para el negocio. Consecuentemente, como los proveedores

de IT entienden las necesidades de las áreas y se encargan de velar por entrega de lo que se espera de ellos, también habrá un incremento en la satisfacción del cliente.

Todo este círculo virtuoso desemboca en mejoras en cuanto a flexibilidad para atender las necesidades del negocio y capacidad de adaptabilidad a los procesos.

Con todos estos beneficios anteriores, quedan realizados los cimientos para visualizar mejoras en términos de seguridad, precisión, velocidad y disponibilidad según los niveles de servicio acordado (Meza Medellín, *Op.cit*, 2015).

Diseño y Gestión de los Servicios de IT

El objetivo de ITIL es diseñar servicios IT adecuados que satisfagan los requerimientos de la organización, tanto para la actualidad como en el plano futuro. Este enfoque facilita las pautas para diseñar y aplicar los procesos de gestión del servicio, teniendo en consideración tanto los requerimientos del servicio propiamente, como los recursos humanos y sus capacidades.

Con respecto a la gestión de servicios IT, está centrada en la gestión de los recursos, procesos y tecnologías que colaboran para asegurar la calidad de los servicios IT y su alineamiento con las perspectivas presentes y próximas de la empresa y sus clientes. El objetivo entonces será asegurar e incrementar la calidad de los servicios, reduciendo su costo.

La gestión de servicios de IT es un área avocada a que los procesos orientados a los servicios de IT se integren con el negocio, siguiendo una serie de pautas como la calidad, relaciones con clientes y que las operaciones de IT tengan valor agregado. Los actores que participan entonces son: los clientes, especializados en su negocio; los proveedores, especializados en el servicio y los agentes, nexo entre el usuario/cliente y el proveedor, con la obligación de actuar según lo que el cliente ordene, para cuidar sus intereses (*Ídem*).

3.2.6 CIS

Los controles de Center for Internet Security o *CIS*, son aquellas acciones que de forma conjunta predican la excelencia en las prácticas de defensa en profundidad, para reducir el impacto de los ciberataques en las redes y los sistemas.

Estos controles son desarrollados y perfeccionados por una importante comunidad de expertos en IT provenientes de diversos sectores, tales como fabricación, salud, educación, defensa, comercio o gobierno, por lo cual son muy prestigiosos globalmente.

Justificación de Incorporación

Su desarrollo fue iniciado por la Agencia de Seguridad Nacional o *NSA* de Estados Unidos para el Departamento de Defensa, en el año 2008.

Los tipos de problemas que alentaron la creación de los controles CIS, están asociados a un momento histórico-tecnológico confuso en el que las empresas deben tomar decisiones acertadas y focalizadas. Es entonces cuando los datos y el conocimiento toman un papel predominante en la actualidad de las empresas, brindando el potencial para la prevención, la alerta y la respuesta ante los ciberataques que las afectan.

Como se ha antedicho, los controles CIS han sido desarrollados por una comunidad prestigiosa internacional de instituciones e individuos que:

- Realizan acciones defensivas a partir del estudio exhaustivo de ataques y atacantes, hallando las causas fundamentales de los mismos.
- Utilizan y comparten herramientas con el objetivo de solucionar problemas, a partir del conocimiento de sus potenciales.
- Realizan un minucioso seguimiento de la evolución de las ciber-amenazas, las técnicas de los atacantes y los vectores de intrusiones.
- Detectan patrones de problemas y los resuelven como comunidad.
- Asocian los controles a las regulaciones de cumplimiento, priorizando el análisis colectivo (Center for Internet Security, 2019).

Clasificación de las Organizaciones según CIS

Para poder aplicar eficazmente estos controles, se sugiere clasificar a las organizaciones en alguno de los tres posibles Grupos de Implementación o *IG*:

- IG1: Empresa familiar con menos de 10 empleados.
- IG2: Organización regional que brinda un servicio.
- IG3: Gran organización con miles de empleados.

Luego de realizar la clasificación, las organizaciones deberán focalizarse en los subcontroles CIS, de acuerdo con su correspondiente IG. Los criterios para clasificarse en alguno de los grupos por parte de las empresas son:

- Sensibilidad de los datos y criticidad de los servicios: son las organizaciones que prestan servicios esenciales que demandan alta disponibilidad, como es el caso de las mencionadas infraestructuras críticas, o aquellas trabajan con datos sensibles, como por ejemplo las legislaturas.
- Nivel esperado del grado de *seniority* del personal: son las organizaciones que requieren algún grado específico de conocimiento y competencias de IT.
- Recursos disponibles para ciberseguridad: son las empresas que pueden dedicar tiempo, dinero y personal a la ciberseguridad, para contar con una mejor defensa ante ciberataques. (*Ídem*).

3.3 Evolución del Malware

3.3.1 Tipos, Técnicas y Herramientas de Malware

El malware puede ser definido como un "software malicioso diseñado para llevar a cabo acciones molestas o perjudiciales". (Waters, *et al*, *Op.cit*, 2008, p.48). Según Villegas López (2018), el concepto de Malware es demasiado amplio, existiendo la obligación de realizar una segmentación de las diferentes tipologías que existen según su función, objetivos y características. En los próximos subapartados, se definen los tipos, técnicas de ataque y herramientas más importantes utilizados por los atacantes desde la perspectiva de este autor.

Gusano

Waters (2008) define al *gusano* como un "programa de computadora independiente que se reproduce al copiarse de un sistema a otro a través de una red" (Waters, *et al*, *Op.cit*, 2008, p.48).

Se trata de un tipo de malware distinguido por la capacidad de propagación automática a través de una red y dentro de un sistema. Un gusano consume la CPU, memoria y el ancho de banda que le sea útil para su propia difusión, del equipo infectado.

Resumiendo lo expuesto anteriormente, el gusano no requiere dañar los archivos del sistema, así como tampoco la intervención del usuario víctima, a diferencia de otros programas malignos que se pueden replicar a sí mismos (Villegas López, 2018). Cuando se aborde el caso *Stuxnet*, se observarán en detalle las características de los gusanos.

Troyano

El *troyano* es un tipo de malware que hace referencia al caballo de Troya utilizado por los griegos para infiltrar tropas durante la invasión a esta ciudad. Se trata de un programa espía que se oculta sin ser desenmascarado, haciéndose pasar por un programa útil que un usuario tiene intenciones de ejecutar, y se comunica con el exterior escondiendo el código malicioso. Ha sido diseñado así para poder evitar las prácticas de seguridad comunes que bloquean las comunicaciones desde el exterior con la red interna del sistema. De esta manera, la conexión comienza desde el nivel interno, eludiendo todo tipo de barreras y permitiéndole al atacante el robo de información, el control del sistema infectado y la posibilidad de infiltrar otros tipos de malware más destructivos (*Ídem*).

Ransomware

Un *ransomware* se utiliza para a la extorsionar y robar o privar de la información con el objetivo de obtener réditos económicos. Su modus operandi más habitual es infectar un conjunto de sistemas, como pueden ser equipos personales, laborales, o servidores de compañías, para poder secuestrar sus documentos y datos, solicitando un rescate para su recuperación. Este secuestro virtual asociado a la propagación de una infección se implementa utilizando algoritmos criptográficos que cifran los archivos o una parte de estos,

haciéndolos no legibles e incluso permitiendo enviar una copia al atacante para extorsionar a la víctima a cambio de descifrar sus archivos, devolverlos y en ciertos casos no publicarlos en Internet o compartirlos con sus contactos. Es muy común que este pago se gestione mediante una suma de dinero de alguna *criptomoneda,* para desorientar el seguimiento transaccional (*Ídem*).

Próximamente, se analizará el caso *WannaCry,* el cual ha sido un hito en la historia de la ciberseguridad.

Bomba

Una *bomba* es un tipo de malware que espera pasivamente e invisible hasta ciertas condiciones finales hayan sido cumplidas, desencadenando así su efecto. Existen tres tipos:

A) Fork: basadas en una condición lógica siempre verdadera, es decir, una tautología. Un caso de este tipo podría ser la creación indiscriminada de procesos que se reproducen indefinida y exponencialmente, los cuales no causan obligatoriamente un perjuicio en el sistema, pero sí lo bloquea cuando se llega al límite de procesos manejables en simultáneo. En esta instancia, sólo funcionará el reinicio manual.
B) Lógica: suceden cuando su condición de ejecución está supeditada a un evento lógico referente al cumplimiento de un estado determinado: cantidad de uso de memoria, ancho de banda en la red, etc.
C) Temporal: su condición para ejecutar un ataque es una medida de tiempo, como la fecha/hora o contar unidades temporales (*Ídem*).

Adware

Su etimología proviene de la unión de las dos palabras "*Advertisement*" (anuncio) y "Software". Tienen como meta exhibir al usuario publicidad y anuncios, que podrían ser tanto genuinos como malintencionados. En este último caso se trata de software considerablemente peligroso, ya que podría ofuscarse dentro de un anuncio para luego proseguir con el robo de contraseñas, datos y documentación variada de carácter más relevante (*Ídem*).

Spyware

Se denomina así a un software espía instalado sin consentimiento en un sistema de manera automática, el cual le brinda información a una unidad externa o tercero no autorizado acerca de su uso, mediante el rastreo encubierto. Normalmente, este tipo de programa malicioso se puede encontrar en páginas web de índole comercial o búsqueda de servicios, para luego monitorear el perfil del usuario y así desplegarle anuncios dirigidos de acuerdo con sus preferencias, dentro de un marco legal. No obstante, este tipo de programa malicioso podría utilizarse también para robarle a este documentación y credenciales, así a las empresas: todo esto, desde el punto de vista ilegal (*Ídem*).

Rootkit

Más que un tipo concreto de programa malicioso, un *rootkit* representa un compendio de herramientas que colectivamente facilitan accesibilidad con los privilegios más elevados, de manera continua y oculta, a un determinado sistema de información. La palabra "*rootkit*" procede de "*root*", concerniente al usuario raíz del sistema, y "*kit*", debido al conjunto de herramientas componentes que se utilizan generalmente para ocultar archivos, otros programas, rutas y backdoors en los sistemas de las víctimas. Por este motivo, se simplifica considerablemente la posibilidad de regresar a estos equipos más adelante, para utilizarlo prácticamente para cualquier finalidad de manera encubierta para el usuario (*Ídem*).

Virus

Un *virus* puede definirse como "un malware que, cuando se ejecuta, intenta replicarse en otro código ejecutable; cuando tiene éxito, se dice que el código está infectado. Cuando se ejecuta el código infectado, el virus también se ejecuta" (Stallings, 2011, p.357). Se puede afirmar que es uno de los malware que representan mayor peligro. Habitualmente se dispersan y ocultan aglutinándose en otros segmentos de programa, insertándoles una copia de sí mismo: de esta manera, al ejecutarse estos, el virus también lo hará. Posteriormente se reproducirá por el sistema y repetirá el proceso de ocultamiento y propagación utilizando otros segmentos de programas o archivos para consolidar su expansión. Sus objetivos son ilimitados, siendo estos, además, muy dificultosos para su detección (*Ídem*). Las copias, por lo general se

ejecutan cuando el archivo comprometido es cargado en memoria y esto es lo que permite al virus infectar otros archivos.

Un virus requiere la participación humana, generalmente involuntaria, para propagarse (Waters, *et al*, *Op.cit*, 2008).

Un tipo específico de virus, son los *wiper*, que simplemente están orientado a eliminar y destruir todos los archivos de un disco, generalmente para sabotaje.

A partir de lo que se mencionó, se detallará el comportamiento de un virus, evidenciando su capacidad nociva con el caso *Shamoon*, categorizado por su naturaleza como wiper.

Keylogger

Los *keylogger* son malware específicos que almacenan toda pulsación que se realice en un teclado conectado al equipo con el objetivo de monitorear los valores introducidos en cada momento, siendo el robo de credenciales de usuario su principal aplicación. Hay dos tipos de keylogger diferentes:

- Por Software: conforma el programa malicioso que infecta el sistema y envía al atacante toda la información recolectada de accesos a cuentas personales.
- Por Hardware: tiene el único requerimiento de estar ubicado delante de la computadora. Se conecta el dispositivo entre el teclado y el equipo.

La utilización de estos no siempre ingresa en el plano ilegal. Pueden ser establecidos por políticas de seguridad, auditoría o análisis forense (Villegas López, *Op.cit*, 2018).

Rogue Security Software

El malware *Rogue Security*, utiliza la ingeniería social como recurso para engañar personas fingiendo ser una herramienta antivirus, aparentando su comportamiento, pero realizando en realidad tareas como desactivar las configuraciones seguras e infectar el objetivo, sin el discernimiento por parte de la víctima (*Ídem*).

Browser Hijacker

Un *Browser Hijacker* es un tipo de malware que habitualmente es instalado en el navegador como un complemento que promete realizar una mejora en la experiencia de navegación por diversas páginas web, pero que realmente supone una grave amenaza de seguridad. Este malware puede modificar las configuraciones del navegador, dejando vulnerable al sistema soporte, alterando el contenido de lo que se visualiza en la interfaz gráfica y robando datos privados de la víctima. Por todo esto, se dice que "secuestra" al navegador (*Ídem*).

Botnet

Existen una serie de redes de computadoras interconectadas para realizar tareas iterativas, cuyo objetivo es mantener los portales web en funcionamiento y mejorar la experiencia del usuario. Estas se denominan *botnet* y son indiscutiblemente legales. Sin embargo, también existen botnet ilegales: estas son a las que se hace referencia principalmente en este subapartado. Las botnet maliciosas, son redes de sistemas controlados remotamente que se utilizan para coordinar ataques y distribuir malware, spam y realizar estafas de phishing. La palabra "*bot*" es una abreviatura de "*robot*" y define a programas que se instalan de manera oculta en un sistema específico que permite a un usuario no autorizado controlar de forma remota la computadora comprometida para una variedad de propósitos ilegales (Waters, *et al*, *Op.cit,* 2008).

En algunos casos, los equipos son hackeados directamente, mientras que en otros esto se realiza de manera automática mediante piezas de software que escanean Internet, para hallar vulnerabilidades en la seguridad de distintos sistemas y así comprometerlos.

Spamming

Se denomina *spamming* al procedimiento de envío de propaganda no solicitada, de sitios web, productos o servicios, mediante el correo electrónico. El spamming también se puede emplear como procedimiento para entregar malware y/u otras amenazas cibernéticas, ya que es una potente puerta de entrada (*Ídem*).

Phishing

Phishing es el tipo de robo que emplea tecnologías como spam o mensajes de recuadros emergentes en los sitios web y cuyo objetivo es timar a los usuarios para sonsacarles información privada y confidencial. Entre estos datos: información de sus cuentas bancarias, números de seguro social, números de tarjeta de crédito, contraseñas, etc. En Internet, los estafadores utilizan masivamente cebos como correos electrónicos para el phishing de contraseñas y datos financieros (*Ídem*).

Spoofing

El *spoofing* es una técnica empleada para la creación de sitios web falsos con el fin de copiar el look and feel de un sitio web real y conocido. Para esto, comúnmente se usan técnicas como la suplantación de identidad del correo electrónico, la cual se produce cuando la dirección del remitente y otras partes de un encabezado se modifican para que parezca que el correo electrónico se originó en una fuente diferente, y así dar soporte al fraude. La suplantación de los encabezados oculta el origen de un mensaje de correo electrónico (*Ídem*).

Otra técnica para llevar a cabo ataques de spoofing, consiste en cargar los links a los sitios falsos en las redes sociales, usualmente también empleando un perfil de usuario también falso.

Ataque de denegación de servicios

En un ataque de denegación de servicios o *DoS*, un usuario toma todos los recursos compartidos posibles, de manera tal de agotarlos para que no queden recursos disponibles para los usuarios previstos. Por esto, los ataques de DoS afectan la disponibilidad de los recursos (*Ídem*).

Al atacar una computadora y su conexión de red, o las computadoras y la red de los sitios que las personas están tratando de utilizar, un atacante puede evitar que los usuarios accedan a correos electrónicos, sitios web, cuentas en línea u otros servicios que deba disponibilizar el equipo afectado, siendo este generalmente un servidor.

El tipo más común de ataque de DoS ocurre cuando un atacante "inunda" una red con información y solicita visualizar el sitio web o acceder a sus servicios. Todo servidor solo puede procesar hasta una cierta cantidad de solicitudes a la vez. Por lo tanto, si el atacante sobrepasa este umbral de solicitudes, sobrecargará al servidor con peticiones generadas ilegalmente y el servidor no podrá procesar las de los usuarios legítimos (Tropina, 2013).

Ataque Distribuido de Denegación de Servicios

Una variante del ataque de DoS es el ataque distribuido de denegación de servicio o *DDoS*, que corresponde a un ataque coordinado desde un sistema distribuido de equipos en lugar de desde una sola fuente. A menudo, suele utilizar gusanos para propagarse a múltiples computadoras, que luego podrían atacar al objetivo (Waters, *et al*, *Op.cit*, 2008).

Pharming

El *pharming*, es una técnica que radica en reemplazar el sistema de resolución de nombres de dominio o *DNS*, con el objetivo de dirigir a la víctima hacia un sitio web falso (Fuentes, 2008).

3.3.2 Ciclo de Vida del Malware

Como todo programa, el malware también tiene su propio ciclo de vida, compuesto por ocho fases, tal como se observa en la *Ilustración* 6 (Villegas López, *Op.cit*, 2018).

A continuación, se explicará qué sucede en cada una de ellas.

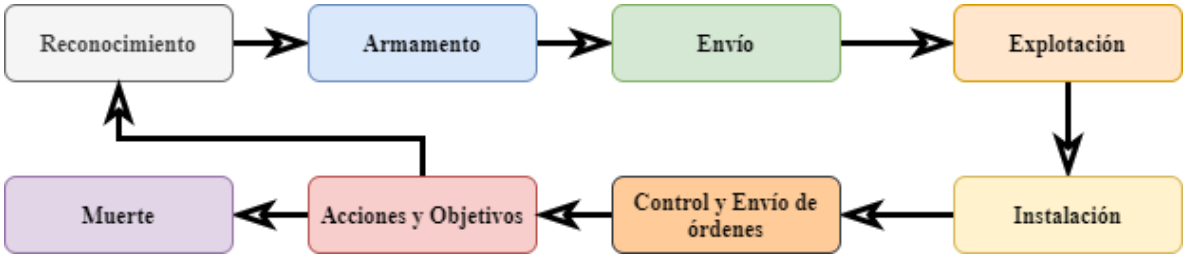


Ilustración 6: Las 8 fases del ciclo de vida del malware

- Reconocimiento: un malware, en primer lugar, realiza la tarea de reconocer los sistemas que va a atacar para hallar estrategias, vulnerabilidades y recursos que pueda explotar para empezar a codificar.

- Armamento: luego de reconocido el ambiente a atacar y recolectadas sus vulnerabilidades, deben obtenerse los recursos para lograr su explotación por medio de la construcción del malware. Este último deberá poder ocultarse, propagarse, escalar privilegios, robar información, etc.
- Envío: una vez creado el malware, es difundido en un medio de propagación adecuado, factor clave para que pueda infectar y replicarse. Uno muy común y útil para los atacantes hoy en día, puede ser la nube.
- Explotación: luego de la difusión exitosa del malware, se podrán aprovechar las vulnerabilidades de software o errores humanos mediante ingeniería social y tomar control del código que se ejecuta en la máquina y todo el sistema.
- Instalación: Luego de que el sistema haya sido infectado y explotado, se intentará controlarlo mediante una conexión, que comúnmente se implementa mediante la utilización de algún troyano o canal encubierto.
- Control y envío de órdenes: en esta etapa la comunicación está establecida y el malware ya se ha instalado. Por lo tanto, el atacante toma control absoluto sobre el sistema y opera sobre él, introduciendo programas maliciosos.
- Acciones y objetivos: aquí se empiezan a explotar los recursos del sistema, como sus datos o capacidad de cómputo. Esto es algo muy habitual en tipos de malware que ejecutan operaciones de minería de criptomonedas, es decir, monedas digitales que utilizan criptografía y se caracterizan por su anonimato y, generalmente, por su descentralización. Al atacante le es útil para obtener un rédito económico mediante el proceso de *blockchain*. También, como se ha mencionado en las técnicas y tipos de ataque del subapartado 3.3.1, se pueden orquestar grandes botnet que permiten ejecutar ataques DDoS sofisticados.
- Muerte: en esta última fase, el programa malicioso queda totalmente obsoleto. Podría volverse a la fase de reconocimiento, solo en el caso de requerir una nueva adaptación (*Ídem*).

3.3.3 Fuentes para la Documentación de Incidentes

Por varias razones mencionadas anteriormente, como riesgo reputacional y cierto recelo en las empresas que son víctimas, es muy difícil contabilizar precisamente los incidentes cibernéticos en los sistemas de control.

Sin embargo, quienes han dedicado valioso tiempo a investigar este tema ven tendencias de crecimiento similares entre las vulnerabilidades expuestas en los sistemas de IT tradicionales y las que se encuentran en los sistemas de control. Existe una base de datos de incidentes de seguridad industrial, conocida en un primer momento como *ISID*, que está diseñada con la finalidad de rastrear incidentes de naturaleza de seguridad cibernética que afecten directamente a los ICS y sus procesos. Esto incluye eventos como incidentes accidentales relacionados aspectos de ciberseguridad, así como eventos deliberados como acceso remoto no autorizado, ataques DoS e infiltraciones de malware. Los datos se recopilan mediante la investigación de incidentes conocidos públicamente y de informes privados de miembros que desean tener acceso a la base de datos. Cada incidente se investiga y luego se clasifica de acuerdo con una categoría que indica grado de confiabilidad. Se incluyen los campos: Título del incidente, Fecha del incidente, Fiabilidad del informe, Tipo de incidente, Industria, Punto de entrada, Autor, Tipo de sistema y hardware afectado, Breve descripción del incidente, Impacto en la organización, Medidas para prevenir la recurrencia y Referencias (National Institute of Standards and Technology, *Op.cit*, 2006).

La información contenida en ISID, fue absorbida por la *RISI Online Incident Database*, retroalimentándola. RISI son las siglas que referencian a Repositorio de Incidentes de Seguridad Industrial.

El espíritu de esta última siempre se ha centrado en la investigación y el intercambio de información en el ámbito de una comunidad de personas para quienes estos datos son relevantes. Para preservar esto, se ha creado la "Security Incidents Organization", la cual es una organización autosuficiente enfocada en realizar investigaciones de interés público y hacer que los resultados de esa investigación estén disponibles para todo el público. Su éxito depende no solo del apoyo financiero de las compañías miembro, sino más importante de la

disposición de los afectados por incidentes de seguridad industrial para compartir sus experiencias en beneficio de la comunidad.

3.3.4 Ataques Informáticos en Ciberguerra

Los ataques y defensas cibernéticos pueden ser realizados a nivel estatal por militares o a nivel personal, por un individuo particular. Podrían englobar un simple ataque de hackers, o una operación compleja a largo plazo, en gran escala y lanzada por el estado de un país con el objetivo específico de dañar la infraestructura de un estado enemigo para lograr el propósito estratégico de paralizar el funcionamiento de ese estado.

Otro objetivo puede ser puramente realizar algún tipo de espionaje. Generalmente, los ciberataques se refieren a la intrusión no autorizada en una computadora o una red informática en formas tales como manipulación, denegación de servicio, robo de datos e infiltración de algún servidor. El surgimiento y desarrollo de los cibergrupos no estatales que poseen una orientación política, como Anonymous y otros grupos de ciberdelitos, añaden complejidad a este análisis (Gazula, 2017).

La guerra cibernética se fundamenta en la ejecución y preparación de operaciones militares que implican interrumpir o destruir los sistemas de información y comunicación mediante los que un adversario lleva a cabo sus estrategias. El motivo principal será intentar adquirir todo el conocimiento posible sobre el otro, mientras que al mismo tiempo se intenta que se sepa muy poco sobre uno mismo. Esta táctica, equilibra con información y conocimiento las desventajas en el plano de las fuerzas (Arquilla, *et al*, 1997).

En el último tiempo, han irrumpido en la escena distintas sociedades perpetradoras de ataques terroristas a través de Internet y las redes sociales, incentivados por temas de índole política o movimientos ciudadanos en los que tienen algún interés. Como ya se ha ido mencionando parcialmente, se han confirmado además ataques informáticos contra ICS críticos, financiados por naciones extranjeras contrarias a los intereses del país que oficia de víctima. Esto se abordará nuevamente más adelante.

Está más claro hoy en día que Internet puede utilizarse para la propaganda terrorista y sus actividades derivadas, difundidas por sitios y redes sociales: reclutar, radicalizar, incitar,

financiar, formar, planificar, ejecutar y, en última instancia, atacar. La propaganda es realizada por medio de comunicaciones multimedia, en las cuales se puede instruir, explicar, promover y justificar las actividades terroristas. Generalmente se utiliza la difusión de mensajes, presentaciones, revistas online, normativas, archivos multimedia y hasta videojuegos, los cuales desarrollan las agrupaciones terroristas.

Por otro lado, quien financia el ciberterrorismo hoy en día tiene la posibilidad de hacerlo vía convocatorias directas de *e-commerce*, realizando pagos en línea o a través de organizaciones de beneficencia, por lo cual se dificulta su seguimiento. Para otras tareas más específicas, la disponibilidad de recursos como herramientas de logística y mapas facilitan su planificación.

Con toda esta preparación, podrá finalmente perpetrarse el ataque planificado de manera anónima: amenazas relacionadas con la utilización de armas, inducción de ansiedad o miedo colectivo en una población o subconjunto, etc. Por lo tanto, un ciberataque se ejecuta habitualmente para alterar el correcto funcionamiento o anular un sistema de información, equipos servidores, redes de computación u otros componentes.

Adicionalmente, la puesta en marcha de un ciberataque a las IICC de un país puede ir más allá del interés de alguna organización terrorista: puede ser relevante para los intereses hegemónicos de otra nación. En este sentido, cobra relevancia las constantes actividades hostiles que han realizado los países, unos contra otros. Varios de estos tienen agencias gubernamentales y departamentos que recolectan información del ciberespacio con el objetivo o justificación de prevenir posibles ciberataques (Estudios de Seguridad y Defensa, *Op.cit,* 2014).

3.3.5 Tipos de Incidentes de Ataques Dirigidos a ICS

La complejidad de los ICS modernos evidencia muchas vulnerabilidades y vectores de ataque, los cuales pueden provenir de muchos lugares, incluso indirectamente a través de la red corporativa o directamente a través de Internet, redes privadas virtuales (VPN), redes inalámbricas, etc. Existen tres categorías amplias de incidentes en ICS:

- Ataques intencionales dirigidos: obtener acceso no autorizado a archivos, realizar un ataque DoS o falsificar la identidad del remitente para un correo electrónico.

- Consecuencias involuntarias o daños colaterales: de gusanos, virus o fallas del ICS.
- Consecuencias de seguridad interna: pruebas negligentes de sistemas operativos o cambios no autorizados en la configuración del sistema. También abarcan casos de ataques perpetrados por empleados descontentos o exempleados.

Cabe destacar que, de los tres, los ataques dirigidos son los menos frecuentes. Sin embargo, potencialmente son los más dañinos, pero también requieren un conocimiento detallado del sistema y la infraestructura de soporte. El agente de amenaza más probable es la no intencional o interna (National Institute of Standards and Technology, *Op.cit*, 2006).

3.3.6 Mercados Negros: Deep, Dark Web y Darknet

Más allá de los objetivos de la ciberguerra, existen mercados negros en los que se comercializan las vulnerabilidades y la información robada, entre otros delitos.

Según L. Ablon (2014), la madurez de estos mercados puede comprenderse a partir de factores como la sofisticación, donde el mercado muta y se va adaptando a las necesidades; la fiabilidad e integridad, ya que las personas y los productos son lo que dicen que son; la accesibilidad, porque es sencillo ingresar a bajo nivel; la especialización, debido a que existen productos, roles y lugares entre los partícipes; y la resiliencia, donde los acontecimientos del exterior no tienen impacto en el mercado (Ablon, *et al*, 2014).

Se puede acceder al contenido de estos mercados realizando conexiones hacia la *Deep* y *Dark Web* y en los mismos es posible adquirir, por ejemplo, vulnerabilidades de día cero o *Zero-Day*. Como es muy común que se nombren los términos Deep Web, Dark Web y Darknets como sinónimos, es importante diferenciarlos correctamente.

La Deep Web abarca el contenido web que no puede ser indexado por buscadores convencionales, es decir, contenido que se encuentra a un nivel inferior al de la *Clearnet*, que es la parte indexable de Internet: la capa navegada habitualmente por la extensa mayoría de usuarios, que usualmente se denomina World Wide Web (Villegas López, *Op.cit*, 2018).

Por lo tanto, al no poder accederse mediante estos navegadores, se puede utilizar entonces algún cliente como The Onion Router o *Tor*, que permitirá visitar los sitios ".onion", propios de esta red. El anonimato de Tor se basa en retransmisiones, es decir, computadoras aleatorias

denominadas enrutadores o nodos, entre las cuales rebota la comunicación, para ofuscar la ruta. Esto permite ocultar de una manera bastante eficiente las direcciones de origen y destino y salvaguardando la privacidad del usuario. El problema surge a partir de las vulnerabilidades inherentes a Tor, que son las mismas que pueden encontrarse en cualquier tecnología o programa (Retzkin, 2018).

La Dark Web forma parte de la Deep Web, y para poder accederla de manera segura hay que tomar los recaudos necesarios, porque es allí en donde se realizan la mayoría de las actividades ilegales. El término tiene dos vertientes principales: se utiliza para referirse a su contenido, mientras que, por otra parte, habla también del plano cultural que implica.

Por último, existen también las Dark Nets, que son subredes aisladas y ocultamente dispersas dentro de la Dark Web (Villegas López, *Op.cit*, 2018). Es importante detenerse en este punto para señalar las diferencias especiales entre Dark Web y Dark Net. Dark Net fue un término utilizado en la década de 1970, para redes aisladas de ARPANET, para la aplicación de seguridad en compartimientos. Estas redes se configuraron para poder recibir datos externos, pero estaban ocultas de los listados de red de ARPANET y no respondían a las solicitudes de red, como *ping*. Con el paso del tiempo, el término también se usó para redes superpuestas, que son esencialmente redes que utilizan software y hardware para crear múltiples capas de abstracción. Estas capas en redes separadas o en una red común superpuesta, accesible solo mediante navegadores especiales, ya que sus direcciones IP no son enrutables globalmente, tal como se ha mencionado para el caso de Tor. Por lo tanto, se puede entender al término Dark Net como la infraestructura debajo de la Dark Web, que es sólo el contenido y los sitios web a los que solamente se puede acceder con el software especializado indicado (Retzkin, *Op.cit*, 2018).

En la *Ilustración 7* (Ídem), se puede apreciar una anatomía de Internet: cómo se relacionan entre sí las capas y sus características en común, a pesar de estar contenidas cada una dentro de otra.

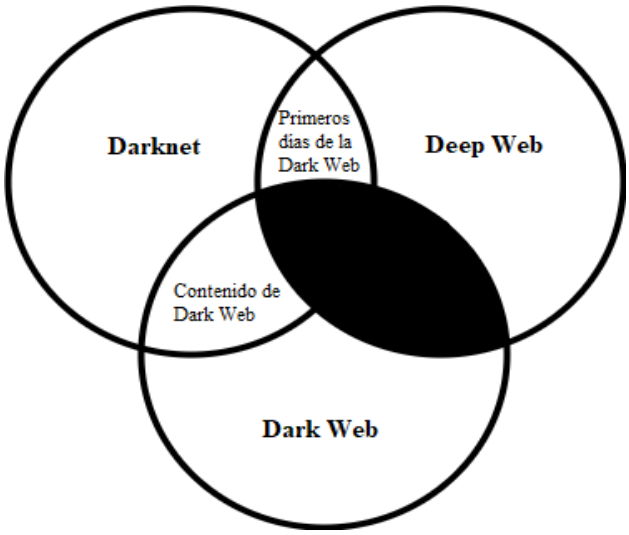


Ilustración 7: Espacio lógico y relación entre Darknet, Deep Web y Dark Web

Para comprender la magnitud, se estima que alrededor del 90% del contenido de Internet, se encuentra dividido entre estos tres espacios, con su gran mayoría en Deep Web. El volumen de información de la Dark Web es despreciable en comparación: alrededor del 0,1%.

En estos niveles, los desarrolladores de malware y otros ciberdelincuentes ofrecen sus servicios y productos de manera remunerada, lo que ha contribuido notablemente a su distribución masiva. Los costos pueden variar debido al sistema operativo o navegador afectados, cantidad de usuarios involucrados o a la gravedad de la vulnerabilidad explotada (Villegas López, *Op.cit,* 2018). Por ejemplo, como se verá más adelante, si se trata de una vulnerabilidad Zero Day el precio puede ser muy elevado.

3.3.7 Vectores de Amenazas en Sistemas de Control Industrial

Las amenazas que afectan los sistemas ICS pueden provenir de numerosas fuentes, tales como gobiernos hostiles, grupos terroristas, espías industriales, empleados descontentos, intrusos maliciosos y, por otro lado, la complejidad propia de los sistemas, errores humanos y accidentes, fallas de equipos o desastres naturales. Para protegerse contra estas, es preciso crear una estrategia de defensa en profundidad para el ICS.

En los próximos subapartados se mencionarán los vectores de amenazas, según la normativa NIST SP 800-82 (National Institute of Standards and Technology, *Op.cit,* 2006).

Atacantes

Los atacantes invaden las redes por el desafío mismo o por temas ligados los derechos de la comunidad de atacantes. Si bien las técnicas de hacking alguna vez requirieron una buena base de conocimiento informático, los atacantes ahora pueden descargar scripts de ataque y lanzarlos contra los sitios de las víctimas. Por lo tanto, si bien las herramientas de ataque se han vuelto más sofisticadas, también se han vuelto más fáciles de usar. Hoy en día, la comunidad mundial de ciberatacantes plantea la amenaza relativamente alta de una interrupción aislada o breve que pudiera ocasionar daños graves (*Ídem*).

Operadores de Redes Bot

Los operadores de redes bot son atacantes que, en lugar de irrumpir en sistemas solamente por el desafío, controlan múltiples sistemas para coordinar ataques y distribuir phishing, spam y ataques de malware. Los servicios de estas redes a veces están disponibles para su adquisición en los mercados negros, como se ha mencionado en el subapartado 3.3.6. Casos típicos de estos pueden ser la compra de un ataque de denegación de servicio o el uso de servidores para transmitir ataques de spam o phishing (*Ídem*).

Grupos Criminales

Los grupos criminales organizados, que incluyen espías corporativos, buscan atacar los sistemas para obtener ganancias económicas. Específicamente, utilizan spam, phishing y spyware como malware para cometer robos de identidades y fraude en línea, para llevar a cabo espionaje industrial, robo monetario a gran escala y para contratar o desarrollar talento para ataque (*Ídem*).

Servicios de Inteligencia Extranjeros

Los servicios de inteligencia extranjeros utilizan herramientas cibernéticas como parte de sus actividades de recopilación de información y espionaje. Además, varias naciones están trabajando arduamente para desarrollar doctrinas, programas y capacidades de ciberguerra, con el objetivo de interrumpir el suministro energético, las comunicaciones y las infraestructuras económicas que respaldan el poder militar de otros países (*Ídem*).

Amenazas Internas

En una empresa, empleados descontentos pueden volverse una potencial fuente del delito informático. Es posible que no necesiten una gran cantidad de conocimiento sobre cómo ingresar como intruso en una computadora, ya que su conocimiento operativo a menudo les permite obtener acceso sin restricciones y así causar daños o robar datos. La amenaza interna también incluye a proveedores externos, así como a empleados que accidentalmente introducen malware en los sistemas corporativos e industriales.

Políticas, pruebas, y procedimientos inadecuados pueden provocar impactos en el ICS y dispositivos de campo, variando desde daños triviales hasta significativos. Los impactos no intencionales de personas de adentro son algunos de los casos con mayor probabilidad de ocurrencia (*Ídem*).

Phishers

Los phishers son individuos o pequeños grupos que ejecutan esquemas de phishing y spear phishing, como se mencionó en el apartado 3.3.1, en un intento de robar credenciales de identidad o información para obtener ganancias económicas. Los phishers también pueden usar malware como spam y spyware para lograr sus objetivos (*Ídem*).

Spammers

Se denomina así a los individuos u organizaciones que distribuyen correos electrónicos no solicitados con información oculta o falsa con el objetivo de vender productos, comenzar esquemas de phishing, distribuir spyware o atacar organizaciones (*Ídem*).

Terroristas

Los terroristas buscan destruir, detener los servicios o explotar las infraestructuras críticas para amenazar la seguridad nacional de un país, causando bajas masivas, debilitando su economía y dañando la moral y la confianza del público. Pueden usar esquemas de phishing o spyware para generar fondos económicos o recopilar información confidencial. También es común que los terroristas ataquen a un objetivo para desviar la atención o los recursos de otros (*Ídem*).

Espías Industriales

El espionaje industrial busca adquirir propiedad intelectual y conocimiento sobre adversarios por métodos clandestinos o no legales (*Ídem*).

3.3.8 Evolución de los Ataques con Malware

En líneas generales, los ataques que incluyen malware derivan luego en otros tales como DDoS, extensión de botnets, fraude bancario, pharming, spamming, gusanos, virus, phishing, etc. Estos son cada vez más complejos y, por lo tanto, muchas medidas preventivas como la utilización de programas antivirus o antispyware, no son suficientes dado al tiempo de respuesta a estas amenazas.

Desde julio de 2007 en adelante, se ha empezado a detectar malware dirigido, empleando técnicas de pharming, a partir de la alteración de los datos del archivo “hosts” del sistema atacado, para luego conducir a las víctimas hacia webs bancarias falsas.

Luego, se empezaron a explotar otras vulnerabilidades mediante estas técnicas de alteración de las tablas DNS mediante enrutadores, como la combinación de pharming con la usurpación del sitio web bancario en la misma computadora comprometida para que el usuario efectúe transacciones allí y los datos personales sean redirigidos hacia algún servidor remotamente (Fuentes, *Op.cit*, 2008).

Los virus evolucionan aprovechando las ventajas que brindan las distintas tecnologías para poder ser dañinos, veloces y sutiles en la forma de engañar a sus víctimas y actuar.

Por otro lado, el espionaje se está volviendo cada vez más común. Las amenazas son reales y muchos actores intentan ingresar a sistemas del sector energético protegidos con buenas prácticas. Entre 2009 y 2017, las observaciones indican que el sector energético ha pasado de estar en la parte inferior de la lista a convertirse en el segundo sector más atacado.

En India, por ejemplo, el sector energético es muy vulnerable. La mayoría de los ataques de energía se traducen en recopilar información valiosa en lugar de ser un acto de ciberguerra o ciberterrorismo. Aunque en la mayoría de los casos los atacantes se han centrado solamente en recopilar información y sin motivos evidentes, en un tiempo cercano, los ataques serán en su mayoría de sabotaje, provocando enormes pérdidas financieras que paralizarán la

economía o llevarán al sector de servicios públicos al límite del colapso. Los impactos económicos en un país pequeño podrían traducirse en un efecto dominó que afectaría a otras empresas de energía a nivel mundial. Por esto, estas empresas deben ser conscientes de estos riesgos para proteger su valiosa información, tanto como sus ICS y SCADA (Venkatachary, *et al*, 2017).

Se observa que existe una evolución del tipo de software malicioso empleado en los últimos años. A partir de 2017, por ejemplo, se incrementó el uso de código dañino, kits de explotación, publicidad dañina, ataques de denegación de servicio y aplicaciones web y ocultación del atacante. Sin embargo, luego se observa que a partir de 2018 han predominado ataques con software para ciberespionaje, ransomware, phishing y spamming, código dañino y kits de explotación, ataques contra la industria de la publicidad, ataques web, ataques de denegación de servicios, IoT e IIoT.

En reglas generales, se están manteniendo en los ataques orientados a la disrupción de los sistemas, ciberespionaje y delincuencia en general. Pero, por otro lado, la tipología de los incidentes presenta nuevos objetivos asociados, como generar influencia en la opinión pública y ciberguerra. Estos últimos casos han afectado políticamente a países como Alemania y Francia, quienes han sufrido el robo de información en sus partidos políticos, mediante técnicas como phishing y spear phishing (Gil, 2018).

En la *Tabla 3*, se extrajeron del artículo "*Economic Impacts of Cyber Security in Energy Sector: A Review*" (Venkatachary, *et al*, *Op.cit*, 2017), los eventos que corresponden a la década que se está analizando en este trabajo. Aquí se pueden visualizar cronológicamente, los hitos de ataques más relevantes dirigidos a las infraestructuras críticas, dado su impacto.

Tabla 3: Evolución del malware dirigido a infraestructuras críticas, en 2009-217

Año	Objetivo	Región	Agente	Tipo	Impacto	Algoritmo	Vector
2009	Aviación civil	Estados Unidos	Desconocido	Malware desconocido	Compromiso de datos; apagado de sistemas	Desconocido	Desconocido
2010	Planta nuclear de Natanz-Irán (centrifuga-doras)	Irán	Stuxnet	Gusano	Las centrifugadoras nucleares de Irán fueron modificadas. El impacto de este ataque fue mundial.	MD5, AES	MS10-046 (0-day); MS10-061 (0-day); MS08-067 (0-day remediada); CVE-2010-2568 (0-day)
2011	No específico; plantas nucleares de Irán	Irán	DuQu	Malware desconocido	Desconocido	Camellia, AES, XTEA, RC4, different multibyte XOR-based encryption	CVE-2011-3402
2012	Saudi Aramco (UAE)	Arabia Saudita	Shamoon	Virus	35.000 equipos	MD5, SHA-256	Desconocido
2012	Varias plantas nucleares	Irán, Líbano, Siria, Sudán, Egipto	Flame *aka* Flamer	Troyano	1.000 equipos	MD5, SHA-256	MS10-061, MS10-046; MS09-025
2013	Compañías de energía	Norteamé-rica - Europa	Dragonfly	Troyano	Más de 1.000 compañías de energía en Norteamérica y Europa	SHA-1, SHA-256, MD5	CVE-2011-0611; CVE-2012-1723, CVE-2013-2465; Spear Phishing, Herramien-tas de acceso remoto
2014	SCADA/ ICS	Francia, Alemania, Rumania, Grecia	Havex	Troyano	146 servidores con comando y control	RAT (nuevo en 2014)	CoInitialize Ex, CoCreate InstanceEx; COM

2015	RasGas	Qatar	Shamoon	Virus	Ataque DDoS	MD5, SHA-256	Desconocido
2015	Kyivoblenergo	Ucrania	Black Energy 3	Troyano	225.000 clientes sin energía durante 6 horas	AES	CVE-2014-751; server blocks
2015	Polish Airlines	Polonia	Desconocido	Malware desconocido	1.400 pasajeros afectados por demoras y cancelaciones	Desconocido	Desconocido
2016	Planta nuclear Gundre-mmingen	Alemania	W32.RAMNIT; Conficker	Malware desconocido	Incidente aislado, que afectó a 1.7 millones de personas	SHA-1#, RC4, RSA	CVE-2014-4113; TA08-297A, CVE-2008-4250, VU827267, Win32/ Conficker.A (CA), Mal/ Conficker-A (Sophos), Trojan.Win32. Agent.bccs (Kaspersky), W32. Downadup.B (Symantec), Confickr
2017	Dispersión mundial	India, Rusia, China, Taiwán, UK y luego resto del mundo	WannaCry	Ransomware	En todo el mundo; 200.000 computadoras incluyendo escáneres de resonancia magnética en el NHS, Reino Unido. Los países más afectados fueron Rusia, India, Taiwán y Ucrania.	RSA, AES	MS17-010: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147 y CVE-2017-0148

3.3.9 Gusano Informático Stuxnet: Ataque Dirigido a Siemens

Stuxnet fue uno de los casos más importantes en la historia de los ataques dirigidos, en lo respectivo a ciberguerra, realizado para afectar el programa nuclear de Irán.

En 2010, para contextualizar el marco geopolítico, el gobierno de Irán confirmó su intención de continuar con el programa nuclear de explotación de uranio que ya llevaba en curso. Pero previamente, los Estados Unidos y determinados países de la Organización del Tratado del Atlántico Norte (OTAN), habían manifestado su discrepancia, con la justificación de que Irán estaba llevando a cabo una carrera armamentista nuclear. El programa instalaba centrifugadoras de enriquecimiento de uranio subterráneas y por ello, la probabilidad de un impacto con un ataque aéreo tenía menor posibilidad de ser exitosa. Por lo tanto, se planeó y logró propagar este gusano informático mediante una memoria flash USB. Alguien, a quien hasta el momento no se pudo identificar, conectó dicho dispositivo en PC de una planta y el virus comenzó a propagarse (Aguirre Ponce, *Op.cit*, 2014).

Es importante remarcar que, si bien habitualmente se ha asociado a Stuxnet únicamente la red ICS de la marca Siemens, de la central nuclear iraní en Natanz, los objetivos de la utilización del gusano han sido variados, como se explicará a continuación.

Características Relevantes de Stuxnet

El gusano de Windows Stuxnet fue descubierto en julio de 2010 por la empresa VirusBlokAda en Bielorrusia. No obstante, se cree que se extendió durante varios meses antes del descubrimiento, incluyendo parte de 2009, y que para ese entonces ya había comprometido su objetivo previsto.

Como se visualiza en la *Tabla 4* (Chen, *et al*, 2011), Stuxnet difiere del malware conocido hasta el momento de su descubrimiento en varias formas.

En primer lugar, la mayoría del malware intenta infectar tantas computadoras como sea posible, mientras que Stuxnet apunta solamente a ICS y entrega su carga en condiciones muy específicas.

En segundo lugar, Stuxnet es más grande y complejo que cualquier otro malware y contiene exploits para varias vulnerabilidades no parcheadas, entre las cuales se encontraban *Zero-Day*, concepto a abordar en el próximo apartado. Su código fuente es de aproximadamente 500 KB y está escrito en varios lenguajes de programación. Respecto al tamaño, todos los gusanos creados hasta el momento oscilaban entre 4 y 150 KB, como referencia (Chen, *et al*, *Op.cit*, 2011).

Tabla 4: Comparación de Stuxnet con otros malware existentes hasta 2010

Aspecto	Stuxnet	Malware común
Orientación	Extremadamente selectivo	Indiscriminado
Tipo de objetivo	ICS	Computadoras
Tamaño	500 KB	< 150 KB
Probable vector inicial de infección	Unidad flash extraíble	Internet y otras redes
Explotación	4 Zero-Day	Posiblemente 1 Zero-Day

Modo de Operación de Stuxnet

A diferencia de la mayoría de los programas maliciosos, Stuxnet se dirige a ICS objetivamente: ataca a equipos con Windows que programan PLC específicos de Siemens o computadoras especializadas que controlan procesos físicos automatizados en ICS.

Stuxnet se dirige a computadoras vulnerables que ejecutan el software de control WinCC/Step 7, que normalmente se utiliza para programar PLC. Cuando una computadora infectada se conecta a un PLC Siemens Simatic, Stuxnet instala un archivo .dll malicioso, reemplazando el archivo .dll original del PLC. El archivo .dll malicioso permite a Stuxnet monitorear e interceptar toda comunicación entre la computadora y el PLC.

Stuxnet está diseñado para infectar y esconderse en unidades extraíbles, utilizando un rootkit de Windows para evitar que el propietario de una PC descubra archivos Stuxnet. La unidad flash solo permite tres infecciones, que intentarán extenderse durante 21 días. Esto sugiere una intención de limitar la velocidad de propagación, tal vez para mantener el sigilo.

Una vez instalado en una red local, Stuxnet intenta encontrar equipos vulnerables y se propaga a través de recursos compartidos de red. Se copia en otros equipos con Windows a través de la vulnerabilidad de cola de impresión “MS10-061” y se conecta a otras computadoras a través del protocolo Server Message Block, explotando una vulnerabilidad de llamada a procedimiento remoto o *RPC* de Windows Server Service “MS08-067”.

Además, busca servidores que ejecuten el software de base de datos Siemens WinCC, que tiene una contraseña codificada que no se puede cambiar ni eliminar. Stuxnet se copia en el servidor mediante inyección SQL.

Mientras que la mayoría de las cargas útiles de malware tienen un propósito claro, como el spam o el robo de datos, se desconoce el objetivo previsto de Stuxnet. Los investigadores han llegado a la conclusión de que parte del código inyectado está destinado a afectar la velocidad de las unidades de los convertidores de frecuencia: el código parece alternar entre desacelerar y acelerar la frecuencia normal. Si el PLC objetivo se conecta a una centrífuga nuclear, utilizada para enriquecer uranio, las fluctuaciones de velocidad podrían hacer que la centrífuga se separe. Sin embargo, el resultado del mundo real es difícil de predecir debido a que los PLC pueden conectarse a una amplia variedad de equipos (*Ídem*).

Tipo de Incidente y Consideraciones sobre Stuxnet

Según las mediciones de tráfico hacia los servidores de comando y control, Stuxnet ha infectado entre 50.000 y 100.000 computadoras, principalmente en Irán (58%), Indonesia, India y Azerbaiyán. Irán también tuvo un 67% de hosts infectados, que ejecutaron el software "Siemens Step 7". El porcentaje refleja un valor alto en comparación con otros países, donde la tasa de infección fue inferior al 13%: esta alta tasa de infección de Irán sugiere un motivo político.

El investigador Ralph Langner ha realizado la disección del código fuente de Stuxnet y, basado en sus pruebas, ha sugerido que su objetivo principal era la planta nuclear de Bushehr en Irán. Por su parte, los funcionarios iraníes han negado que Stuxnet haya causado daños a los principales sistemas de dicha planta nuclear, aunque sí han admitido que algunas PC del personal fueron infectadas. Otros investigadores, han especulado con que el objetivo principal era la instalación de enriquecimiento de uranio Natanz de Irán, siendo esta la teoría más difundida. La producción del sitio cayó un 15% en 2009, cuando se cree que verdaderamente Stuxnet comenzó a difundirse. En noviembre de 2010, el presidente de Irán confirmó que varias centrifugadoras fueron golpeadas por malware, lo que respalda la teoría de que Stuxnet apuntó al programa nuclear de Irán (*Ídem*).

El ataque con Stuxnet requirió conocimientos previos, detallados y confidenciales de PLC e ICS: Siemens WinCC / Step 7. Sus creadores estaban al tanto de que su objetivo no sería accesible a través de Internet, por lo que el vector de infección inicial fue una unidad flash extraíble. Los creadores de Stuxnet habrían necesitado conocer la configuración del PLC de destino, y probablemente necesitaron un hardware similar para desarrollar y probar el código de malware.

Según Porche (2011), la gran complejidad de Stuxnet requeriría importantes recursos para desarrollarse. La especulación sobre lo que se necesitaba para desplegar y llevar a cabo un ataque de tal magnitud incluye lo siguiente, de parte de los desarrolladores:

- Pudieron acceder a los documentos técnicos y de diseño del ICS: controladores Siemens con sus respectivas versiones, sistemas operativos, actualizaciones de seguridad, etc.
- Pudieron adquirir centrifugadoras similares a las de las instalaciones iraníes.
- Obtuvieron conocimiento del entorno informático en la instalación.
- Es probable que hayan establecido un entorno similar que incluyera los controladores industriales necesarios y algún otro hardware de control para probar el gusano.
- Habrían necesitado obtener al menos dos certificados digitales comprometidos. Stuxnet está firmado digitalmente por dos certificados para aparentar la legitimidad. Inicialmente, utilizó un certificado robado de “Realtek Semiconductor”, pero VeriSign revocó el certificado el 16 de julio de 2010. Al día siguiente, se descubrió que Stuxnet estaba usando un certificado robado de “JMicron Technology”, que posteriormente se revocó el 22 de julio de 2010. Dado que las dos compañías están situadas una cerca de la otra, se sugiere la hipótesis de un robo físico en esos lugares.
- Necesitaban conocimientos de exploits desconocidos o no publicados: es decir, Zero-Day en el software de Microsoft.
- Desarrollaron un medio para implantar el gusano en computadoras o unidades flash portátiles que eventualmente podrían conectarse a los sistemas de control.

También está implícita la necesidad de recursos financieros relevantes para adquirir controladores industriales y generar un ambiente de prueba de tal magnitud, así como el acceso al personal para proporcionar la amplia experiencia técnica requerida.

Los análisis posteriores de código abierto sugieren que entre 5 y 10 ingenieros de software con un rango de habilidades variado tardaron al menos 6 meses en desarrollar Stuxnet (Porche, 2011).

Todos los informes que examinan Stuxnet han acordado la probabilidad de que al menos un gobierno haya participado en su desarrollo.

Chen (2011) agrega que, además del conocimiento interno detallado del objetivo, otros aspectos sugieren que los creadores de Stuxnet gastaron considerables recursos, debido a que las cuatro vulnerabilidades Zero-Day de Windows representaron una inversión inusualmente alta.

Por otra parte, los creadores de Stuxnet sabían específicamente que la vulnerabilidad RPC del servicio de Windows Server mencionada, a pesar de tener un parche publicado por Microsoft desde 2008, no había sido remediada. Los atacantes sabían esto y utilizaron el gusano *Conficker* para explotarla.

Las técnicas mencionadas no son novedosas para este contexto. Stuxnet evitó las soluciones de seguridad más populares, inyectándose en un proceso reconocido, para luego instalar un rootkit de Windows y esconderse en el equipo infectado.

Este gusano, puede actualizarse de dos maneras, desde el equipo infectado:

- Utilizando la comunicación entre pares o *P2P* para descargar nuevas actualizaciones.
- Intentando conectarse a servidores de comando y control en Malasia y Dinamarca para informar los datos extraídos del sistema infectado y descargar ejecutables arbitrarios (Chen, *et al*, *Op.cit*, 2011). Todo lo expuesto anteriormente implica un caso de espionaje financiado, con cooperación de una posible amenaza interna.

Reflexiones sobre Stuxnet

Aunque los detalles importantes sobre sus creadores, motivos, objetivo continúan siendo especulativos, el caso Stuxnet reavivó en 2010 las preocupaciones sobre la posibilidad de la guerra cibernética. Algunos expertos califican a Stuxnet como la primera arma real para este tipo de guerra.

Luego del descubrimiento de Stuxnet, Irán acusó a la OTAN y los Estados Unidos de estar involucrados en los ataques, pero ambos han negado la responsabilidad. Algunos también han sospechado de la agencia de seguridad de la "Unidad 8200" de Israel, quien no ha realizado públicamente comentarios sobre Stuxnet, pero reconoce que la guerra cibernética es parte de su misión. En el mundo, posteriormente a este ataque, Estados Unidos fortaleció el Comando Cibernético conocido como *USCYBERCOM*, para defender a sus redes militares. Otras naciones, incluido el Reino Unido, China y Rusia, también continúan invirtiendo y mejorando sus capacidades de guerra cibernética.

Por último, Stuxnet fue mucho más sofisticado que un ataque DoS en su selectividad, sigilo, autoprotección y actualización automática. Un malware similar podría ser adecuado hoy en día como arma de primer ataque para comprometer a su objetivo de forma encubierta antes de una ofensiva manifiesta. Ha manifestado a los investigadores de seguridad que el malware no está restringido solamente a las computadoras, sino que puede afectar gravemente las infraestructuras críticas, que en su mayoría son controladas por software. Esto implica que las amenazas pueden extenderse y tener impacto en la vida real (*Ídem*).

Un ciberataque puede tener sencillamente el objetivo de producir perjuicios físicos como ocurrió aquí, en el que un programa malicioso pudo afectar a los sistemas encargados de controlar infraestructuras críticas.

3.3.10 Virus Shamoon: Ataque Dirigido a Saudi Aramco

La empresa petrolera Saudi Aramco, responsable de abastecer el 10% del petróleo del mundo, fue víctima de un ataque masivo conocido como Shamoon, o W32.distract, el cual dejó fuera de servicio aproximadamente 35.000 terminales por varios meses, las cuales tenían sistema operativo Windows. Esta infección se inició cuando un empleado abrió un correo electrónico

fraudulento que encubría un ataque del tipo phishing, ejecutando este virus, cuya principal característica ha sido la supresión indistinta de archivos de los discos rígidos (Kamlofsky, *et al*, 2015).

Christina Kubecka ha trabajado en la remediación de dicho ataque y ha indicado en la entrevista realizada para esta investigación cuáles han sido sus impresiones y puntos de vistas en relación con el estudio de la propagación de la infección.

Características Relevantes de Shamoon

Shamoon fue informado el 16 de agosto de 2012 por Kaspersky Lab, Symantec y Seculert, y posteriormente investigado a fondo por Kubecka y al equipo de *Hypasec*, quienes lograron restablecer el servicio varios meses después en la empresa Saudi Aramco.

El malware fue parte de una progresión de ataques de ciberespionaje y sabotaje en el área de Medio Oriente, tal como en el previamente descripto caso de Stuxnet. Shamoon no se destaca por sus mecanismos de difusión o explotación de las unidades y carpetas compartidas, sino por su carga útil.

La agrupación *Cutting Sword of Justice* finalmente se atribuyó la responsabilidad de la utilización de este virus contra las estaciones de trabajo de la empresa petrolera, provocando una caída del servicio de tal envergadura (Marrocco, 2019).

Modo de Operación de Shamoon

Una vez que un sistema está infectado, Shamoon reúne archivos de diversas ubicaciones específicas en el sistema, envía la información recopilada al atacante y reemplaza los archivos y el registro maestro de arranque del sistema con una imagen recortada de la bandera estadounidense en llamas (*Ídem*).

Según Kubecka, la red de IT y las redes de ICS eran planas, sin segmentación real. Los atacantes pudieron obtener mediante phishing cuentas de administrador de dominio e instalar controladores de dispositivos robados en todos los sistemas. Esto facilitó considerablemente el proceso de propagación de una máquina infectada a otras computadoras.

A continuación, se enumeran los hitos en la cronología del ataque correspondiente a 2012, según Gazula (2017). Este autor, divide al ataque Shamoon en 5 fases bien diferenciadas:

- Fase1 – 2012, “Disputa”: primer ataque conocido hacia la compañía petrolera nacional de Arabia Saudita, Saudi Aramco. Aunque la compañía no anunció oficialmente esto de inmediato, se vieron obligados a aislar su red de computadoras el día 15 de agosto.
- Fase2A - Mediados de 2012, “Reconocimiento”: uno de los empleados del equipo de IT de Saudi Aramco abrió un correo electrónico fraudulento e hizo clic en un enlace incorrecto, habilitando la entrada de los atacantes.
- Fase 2B - Mediados de 2012 hasta el 15 de agosto de 2012, “Replicación”: el código malicioso es transmitido a través de Internet y posteriormente a través de las computadoras de la red, apuntando hacia las computadoras que no están conectadas a Internet. A medida que se eliminan los datos, este código es enviado nuevamente a la computadora central del hacker. El virus posee un componente llamado "dropper", que realiza la réplica mediante una tarea del sistema operativo Windows.
- Fase 3 - 15 de agosto de 2012, “Hostilidades”: el 15 de agosto de 2012, una persona con acceso elevado a los equipos de la compañía, liberó el virus informático para iniciar el acto más destructivo de sabotaje informático en una compañía hasta la fecha. Atacó aproximadamente 35.000 computadoras de Aramco, dejándolas inutilizables y haciendo que la compañía pase meses restaurando sus servicios. La compañía se desconectó después del ataque.
- Fase 4 - agosto de 2012, “Ofuscación”: cuando se completaron las tareas, el atacante ejecutó el módulo de ofuscación, eliminando toda la evidencia del trabajo y del virus mismo.

- Fase 5 - Principios de 2013, "Retirada": seis meses[4] después, con su red informática ya asegurada y un equipo de seguridad cibernética ampliado, Saudi Aramco volvió a poner en línea su sistema (Gazula, *Op.cit*, 2017).

Tipo de Incidente y Consideraciones sobre Shamoon

Shamoon, se ha utilizado para el ciberespionaje en el sector energético. Las firmas que lo han estudiado han destacado las similitudes entre Shamoon y otros malware. Saudi Aramco es de propiedad estatal y el ataque eliminó datos de sus PC corporativas: documentos, hojas de cálculo, correos electrónicos y archivos, reemplazando todo esto con una imagen de una bandera estadounidense en llamas.

Si bien no hay dudas de que se trató de un ataque intencional dirigido con fines de sabotaje, existen diferentes posturas sobre si debería ser interpretado como un caso de guerra cibernética (*Ídem*). Aunque según Kubecka, sí lo fue.

Previamente, Irán había sido golpeado por el malware *FLAME*, también conocido como Da Flame, que afectó las computadoras del Ministerio de Petróleo. FLAME fue un wiper que llevó a que Irán desconecte las terminales petroleras de internet. Partes de Shamoon utilizaron el código de FLAME. En definitiva, ambos eran malware de borrado de información que causan la desconexión.

Paralelamente al ataque de Saudi Aramco, también fue atacada la compañía RasGas en Qatar mediante un modo de operación similar. Sin embargo, había una diferencia muy característica entre ambos ataques: la versión saudita tenía la bandera estadounidense en llamas ya mencionada y no así la de Qatar.

El marco temporal en el que ocurrió el ataque es extremadamente significativo: corresponde al *Laylat al-Qadr*, o "noche del Todopoderoso" en español. Arabia Saudita es sunita, mientras que Irán, musulmán chiita. Los sunitas tienen puntos de vista muy diferentes sobre Laylat al-Qadr. En chiíta es la noche / día más importante del Ramadán, es decir, cuando Ali

[4] *En varias bibliografías se menciona que la restauración total del servicio llevó 6 meses. No obstante, Kubecka ha confirmado que les llevó 8 meses en total, sólo habiendo podido restaurarse efectivamente el 20% de la información.*

ibn Abi Talib fue atacado en la Gran Mezquita y murió días después, producto de sus heridas. Históricamente, la división principal entre sunitas y chiitas provino a partir de las muertes de Mahoma y de Ali ibn Abi Talib, por la sucesión del liderazgo de los musulmanes. Los sunitas creían que Mahoma no nombraba a un sucesor, mientras que los chiitas creían que Mahoma nombró a un sucesor Ali ibn Abi Talib. Este ataque dirigido se llevó a cabo como venganza religiosa, con lo cual también se justificaría el incidente en Qatar, puesto que fue el primer país en el cual se refugiaron los Al-Saud, cuando llegaron al poder. Es necesario recordar que el nombre del grupo que se adjudicó el ataque es *Cutting Sword of Justice*, en clara referencia al asesinato de Ali ibn Abi Talib, ejecutado con una espada.

El ataque apuntó tanto a la red ICS como a la LAN corporativa, pero solamente a componentes Windows, ya que ambas redes los usaban. Muchas redes ICS usan Windows para las interfaces HMI de los sistemas SCADA. Por otro lado, Kubecka ha mencionado que han sido dos las plantas de producción de petróleo que se vieron afectadas.

Los daños producidos por el malware los detuvieron de una manera más efectiva, desconectando directamente el cortafuegos entre las redes de IT e ICS: solo había un cortafuegos, explotable por obsoleto y por listas de control de acceso o *ACL*, incorrectas.

Por último, se destacan algunas cuestiones relacionadas con controles regulatorios internacionales. El Centro de Operaciones de Seguridad o *SOC* de Saudi Aramco, se estableció antes del ataque. Sin embargo, no cumplía con los requisitos necesarios como para ser considerado sustentable. El SOC habían completado su certificación ISO antes del ataque. Sin embargo, varios integrantes del equipo que estuvo trabajando para restablecer el servicio supusieron que el auditor había sido sobornado para aprobar dicha certificación, avalando un área que en realidad era muy débil. Además, el gerente del SOC provenía de una unidad de la empresa cerrada por corrupción, mientras que el personal no estaba lo suficientemente entrenado como para afrontar dicha tarea.

Reflexiones sobre Shamoon

Como resultado del incidente, Saudi Aramco y sus afiliados experimentaron un importante ciberataque que afectó enormemente las operaciones comerciales.

Según Kubecka, a partir de este incidente, se pudo determinar que la cultura corporativa tiene impacto en el ataque y es necesaria la colaboración de parte de diversos participantes, para el trabajo cooperativo, remediación y resiliencia.

Por último, se deja en claro que la aplicación de controles no tiene sentido alguno si lo que está detrás de estos son estándares auto certificados o corrupción.

La recuperación de una empresa tan grande como Saudi Aramco, fue costosa y lenta, por lo que se debe aprender de la experiencia pasada y presente.

3.3.11 Ransomware WannaCry: Ataque Internacional

WannaCry fue un ransomware vinculado a Corea del Norte, según las agencias de defensa de los Estados Unidos y Reino Unido. Resulta de importancia para esta investigación mencionarlo, ya que se trató de una nueva cepa hasta ahora desconocida y de magnitud global, a diferencia de los casos anteriores. Genera la impresión de estar patrocinado por un gobierno para crear caos y lograr estratégicamente algún tipo de meta política.

Retomando lo ya abordado en el punto 3.3.1 con respecto al ransomware, según el informe anual de KnowBe4 (2019), este puede tomar diferentes formas, pero esencialmente niega el acceso a un dispositivo o archivos hasta que un rescate haya ha sido pagado, entendiendo al ransomware como un tipo de software malicioso basado en PC, Mac o dispositivo móvil que encripta los archivos de un usuario o empresa y los obliga a pagar una tarifa al pirata informático para recuperar el acceso a los propios archivos (Ransomware: hostage rescue manual, 2019).

Características Relevantes de WannaCry

Se trata de un ciberataque internacional, dirigido a dispositivos con sistema operativo Windows, que tal como sucede en esta modalidad, cifra archivos y exige pagos para recuperarlos mediante la criptomoneda Bitcoin, tal como se observa en la *Ilustración 8*. El

ataque comenzó en Asia el 12 de mayo de 2017, para luego extenderse por más de 230.000 computadoras en más de 150 países (Manual de supervisión de riesgos cibernéticos para juntas corporativas, 2017).

Ilustración 8: Pantalla principal del ransomware WannaCry

El software malicioso se propaga gracias a *EternalBlue*, una herramienta del tipo exploit que aprovecha una vulnerabilidad en Server Message Block o *SMB*, un protocolo para compartir archivos utilizado por los sistemas Microsoft Windows.

WannaCry se compone de dos componentes principales: un exploit que utiliza la vulnerabilidad de SMB para atacar el sistema de destino y un ransomware que realiza el cifrado de archivos.

Las condiciones posibles para llevar a cabo el ataque pueden ser frecuentemente, correos electrónicos con phishing o bien, el ataque directo a través del protocolo SMB en sistemas que no cuentan con las últimas actualizaciones (Marrocco, *Op.cit,* 2019).

WannaCry causó daños importantes en infraestructuras críticas como hospitales, sistemas ferroviarios y redes de telecomunicaciones distribuidas en todo el mundo (Venkatachary, *et al, Op.cit,* 2017). Una de las infraestructuras críticas más importantes afectadas por este ciberataque, entre otras, fue el Servicio Nacional de Salud del Reino Unido. El ransomware infectó alrededor de 70.000 dispositivos sólo allí, entre los que había computadoras,

escáneres para imagen por resonancia magnética y refrigeradores de almacenamiento de sangre, lo cual conllevó a una interrupción significativa de los servicios de esta entidad.

Nissan Motor debió detener la producción en una de sus plantas, como resultado de las infecciones por el ransomware, el cual también afectó a otras importantes empresas como FedEx. Las pérdidas económicas ligadas a WannaCry se han estimado más de 4 mil millones de dólares estadounidenses en todo el mundo (Manual de supervisión de riesgos cibernéticos para juntas corporativas, *Op.cit,* 2017).

Modo de Operación de WannaCry

Una vez que ingresó a un sistema, WannaCry se propaga automáticamente a otras computadoras, incluso si no está conectado a Internet, a través de los puertos de comunicación 139 y 445, explotando el servicio de uso compartido de red SMB, como se ha mencionado. Luego realiza un cifrado de archivos, utilizando el algoritmo RSA de 2048 bits. Los archivos cifrados se renombran agregando la extensión ".WNCRY" (*Ídem*).

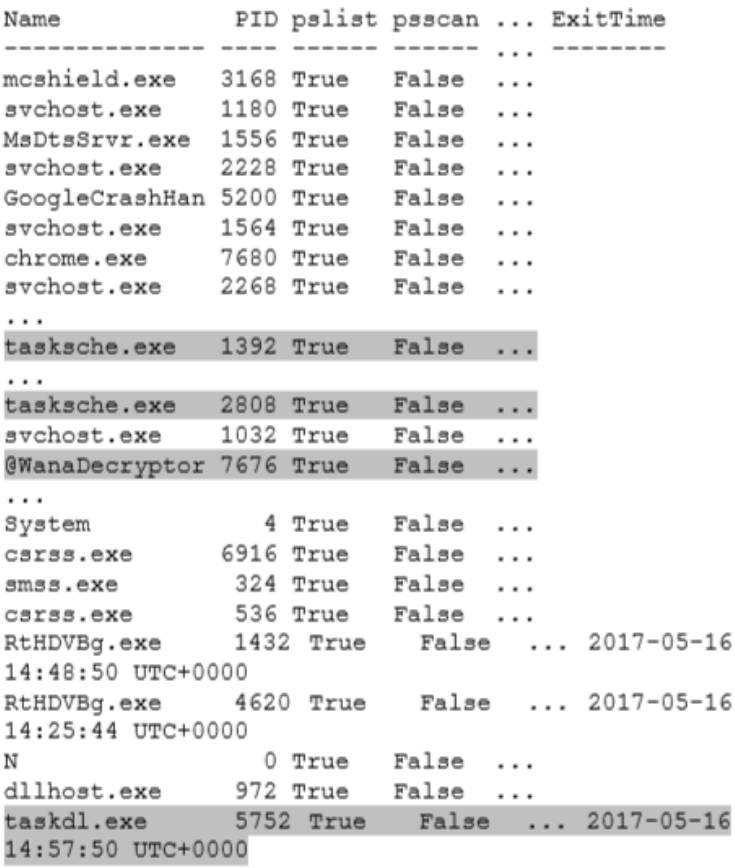
El grupo de investigación de la Universidad FASTA[5] ha realizado el análisis del modo de operación de este ransomware, realizando un volcado en memoria del equipo afectado con la herramienta "Volatility Framework". Con el detalle de esta información, resulta factible la construcción de un indicador de las funciones ejecutadas potencialmente por un proceso.

El análisis del Registro de Windows y de las DLL ayuda a comprender el objetivo de un ataque y cómo un atacante pretende lograrlo. Las DLL pueden permitir que un proceso haga uso de una funcionalidad común sin tener que reescribir código. Por su lado, el análisis del registro de Windows puede detectar la presencia de malware en un equipo. Este repositorio permite definir el alcance de cada entrada en la configuración: si es global y afecta a todos los usuarios o solamente afecta a uno en particular.

Al buscar procesos, han hallado algunos ocultos, como los que se observan resaltados en la *Ilustración 9* (Alberdi, et al, 2017). Dada la forma de proceder de los ransomware, luego de

[5] https://www.ufasta.edu.ar/

haber cifrado los archivos, WannaCry busca llamar la atención del usuario, y por ello, se observan estos nombres particulares para los procesos.



```
Name             PID pslist psscan ... ExitTime
-------------- ---- ------ ------ ... --------
mcshield.exe    3168 True   False  ...
svchost.exe     1180 True   False  ...
MsDtsSrvr.exe   1556 True   False  ...
svchost.exe     2228 True   False  ...
GoogleCrashHan 5200 True   False  ...
svchost.exe     1564 True   False  ...
chrome.exe      7680 True   False  ...
svchost.exe     2268 True   False  ...
...
tasksche.exe    1392 True   False  ...
...
tasksche.exe    2808 True   False  ...
svchost.exe     1032 True   False  ...
@WanaDecryptor 7676 True   False  ...
...
System             4 True   False  ...
csrss.exe       6916 True   False  ...
smss.exe         324 True   False  ...
csrss.exe        536 True   False  ...
RtHDVBg.exe     1432 True   False  ... 2017-05-16
14:48:50 UTC+0000
RtHDVBg.exe     4620 True   False  ... 2017-05-16
14:25:44 UTC+0000
N                  0 True   False  ...
dllhost.exe      972 True   False  ...
taskdl.exe      5752 True   False  ... 2017-05-16
14:57:50 UTC+0000
```

Ilustración 9: Resumen de la salida del comando psxview

En memoria se hallan las librerías CRYPTSP.dll y CRYPTBASE.dll, en las cuales se encuentran las funciones principales.

En particular, la CRYPTSP.dll es la librería que provee la funcionalidad de cifrado al malware: su función "*CryptRandomGen*" crea las claves AES utilizadas para cifrar los archivos. Respecto a los procesos en cuestión:

- "@WannaDecryptor@.exe": es la aplicación encargada de comunicarse con el usuario para pedir el rescate y brindar los datos de pago.
- "tasksche.exe": es el único que utiliza CRYPTSP.dll, ya que es el proceso encargado de cifrar los datos en el equipo (Alberdi, *et al*, *Op.cit*, 2017).

Tipo de Incidente y Consideraciones sobre WannaCry

El efecto de WannaCry ha sido mundial. India fue uno de los países más afectados por WannaCry. Madhya Pradesh fue la región más afectada del mismo, con alrededor del 32,63% del total de ataques de ransomware detectados, seguidos por Maharashtra en 18.84% y Delhi en tercera posición con 8.76% de participación.

También, ha tenido impacto en compañías como FedEx, Nissan, compañías ferroviarias en Alemania y Rusia, el Ministerio del Interior y empresas de telecomunicaciones como Telefónica en la central de España y varias sedes en otros países, 16 organizaciones del Servicio Nacional de Salud del Reino Unido y varias universidades en China (Mohurle, *et al*, 2017).

Como se ha mencionado en el comienzo de esta sección, Estados Unidos y el Reino Unido atribuyeron públicamente este ataque cibernético masivo a Corea del Norte. Microsoft, que fue parte de la investigación, rastreó el ataque hasta llegar hasta los ciberdelincuentes del gobierno de Corea del Norte. El ataque se presentó en un contexto en el cual el país asiático y Estados Unidos presentaban relaciones internacionales tensas, no solo respecto a sus aspiraciones nucleares. Luego, comenzaron a financiarse los ciberataques del lado norcoreano, incentivando comportamiento imprudente y causando interrupciones en todo el mundo.

Es necesario mencionar que, con posterioridad a este incidente, se ordenó desde la presidencia estadounidense la eliminación de todo el software de Kaspersky, empresa rusa, de los sistemas gubernamentales, ya que la misma podría devolver datos al país al que pertenece, representando un nuevo riesgo inaceptable en las redes federales de Estados Unidos. Luego, las principales empresas y minoristas hicieron lo mismo (Bossert, 2017).

El ataque puede ser clasificado como un incidente dirigido, debido a que usualmente comienza por un correo electrónico de phishing o un link malicioso. Por otro lado, también requiere cierta distracción o desconocimiento por parte del usuario como eslabón débil de la cadena y, además, cierta negligencia de parte de las empresas por no llevar a cabo las medidas de seguridad y resguardo de la información necesarias.

Reflexiones sobre WannaCry

WannaCry ha marcado un antes y un después en términos de facilidad para extenderse por todo el mundo y llegar a un gran número de víctimas.

La debilidad que se ha planteado aquí fue que, a pesar de que Microsoft distribuyó rápidamente parches de seguridad capaces de eliminar el exploit EternalBlue, esta actualización no fue instalada por todos, siguiendo las buenas prácticas de seguridad (Manual de supervisión de riesgos cibernéticos para juntas corporativas, *Op.cit,* 2017).

Dentro de estas buenas prácticas, se pueden considerar cuestiones como:

- Tener la última actualización disponible del antivirus.
- Los mensajes de spam no deben abrirse ni responderse.
- Realizar copias de seguridad de los datos.
- Aplicar parches y mantener actualizado el sistema operativo, antivirus, navegadores y otros programas.
- Mantener el cortafuegos de Windows activado y correctamente configurado, deshabilitando los servicios remotos innecesarios y apagar las conexiones inalámbricas no utilizadas, como bluetooth o infrarrojas.
- Filtrar todo tipo de archivos ejecutables en los correos electrónicos.
- Conectarse solamente a redes Wi-Fi seguras.
- No visitar sitios web inseguros y poco confiables.
- Realizar copias de seguridad o respaldo periódicamente y de todos los archivos en otro sistema para evitar la pérdida de datos (Mohurle, *et al*, *Op.cit*, 2017).

Como se ha mencionado, el cifrado del ransomware funciona ocultando el contenido de los archivos del usuario, mediante el uso de algoritmos fuertes. De esta forma, las víctimas no tienen otra alternativa que pagarle al atacante para revertir este proceso, sin la absoluta certeza de que así será. Por esto, es aconsejable implementar las medidas preventivas de seguridad.

3.3.12 Tendencias

En los últimos años se han ido modificando los objetivos de los ataques. Se ha mencionado que hacia 2017, ya predominaban la disrupción de los sistemas y el ciberespionaje y, posteriormente, se agregan objetivos relativos a ciberguerra, influencia de la opinión pública y explotación económica.

Teniendo en cuenta la evolución de los ataques con malware desarrollada, se prevé que los próximos ataques cibernéticos sean más complejos, agresivos y audaces. Gil (2018), enumera las siguientes tendencias a corto y mediano plazo:

1. Incremento de ataques DoS y DDoS: con variantes como la Denegación de Servicio Permanente o *PDoS*. Se esperan complejos ataques DoS de telefonía o *TDoS* y combinación con ransomware o *RansomDoS*, siendo los sistemas vinculados a la salud un posible objetivo.

2. Baja del uso de exploits-kits: solamente se centrarían en ingeniería social.

3. Incremento del ciberespionaje: por razones geopolíticas, económicas o estratégicas. El robo de la propiedad intelectual y de secretos de Estado serán los nuevos objetivos.

4. Incremento de ataques ransomware: contra objetivos concretos, como pueden ser dispositivos sanitarios. También señala la posibilidad de que se realicen campañas de extorsión con la amenaza del uso de ransomware.

5. Acrecentamiento de las brechas de seguridad: orientadas a datos en la nube.

6. Escasez de personal: tendrá impacto en la implantación de reglamentos, normas y estándares de carácter obligatorio.

7. Aumento de tecnologías biométricas: disminución de accesos de usuario y contraseña.

8. Aumento de automatizaciones: inteligencia artificial para enfrentar ciberataques, principalmente debido a la falta de capital humano especializado.

9. Incremento de amenazas a dispositivos móviles: propagación de ransomware.

10. Más regulaciones para IoT e IIoT: a nivel legislativo y aumento del interés de los hackers por controlar estos sistemas.

11. Más complejidad de la ciberdelincuencia: debido a la inteligencia artificial.

12. Perfeccionamiento de ataques contra redes sociales: para actividades de ingeniería social.

13. Aumento de los códigos dañinos sin archivos: debido al uso masivo de criptomonedas, se predicen códigos dañinos dedicados al hurto de información de estas cuentas.

14. Evolución de los proveedores: para servicios gestionados de seguridad de la información (Gil, *Op.cit,* 2018).

La creciente inconsistencia y la falta de especialización del capital humano han alentado a los hackers a explotar las vulnerabilidades en los ICS: se ha observado que los ataques no tienden a disminuir. Es necesario establecer una contraofensiva en respuesta a un ataque cibernético mediante el uso y la adaptación de más dispositivos de tecnología inteligentes.

En muchos casos, la ciberseguridad es un problema de cumplimiento normativo para muchas empresas. Por lo tanto, es fundamental que las empresas entiendan cuáles son sus obligaciones, responsabilidades y que deben cumplir con ellas. Los riesgos de ciberataques deben ser tratados como parte de los riesgos comerciales. Esto puede ayudar a evidenciar qué tan expuesta está una empresa y qué medidas de precaución deben tomarse para protegerla, como así también los intereses de los inversores.

La tendencia de los ciberataques seguirá aumentando a medida que más sistemas se conecten a la red en un modelo distribuido. Proteger estos sistemas será clave para mitigar la indisponibilidad, minimizar las interrupciones y pérdidas, minimizar el tiempo de inactividad, maximizar la disponibilidad y las ganancias (Venkatachary, *et al*, *Op.cit*, 2017).

La mayoría de los ataques cibernéticos se pueden evitar con actualizaciones periódicas y parches impulsados por los proveedores, como se observará en el próximo subapartado.

Se pueden aprender lecciones valiosas de experiencias pasadas y así estar preparados en materia de ciberseguridad, de cara al futuro.

3.4 Ciberseguridad en Infraestructuras Críticas

3.4.1 Vulnerabilidades y Amenazas en Infraestructuras Críticas

La seguridad de las infraestructuras críticas ligadas a ICS no ha sido prioritaria en el pasado, dado que las mismas solían estar organizadas en redes privadas y con programas dedicados exclusivamente para su funcionamiento. Dada la característica de estos sistemas de ser prioritarios, solamente los desarrolladores conocían el código fuente. Además, las amenazas eran sólo locales y por ello más sencillo su tratamiento. Con el tiempo, los administradores de infraestructuras críticas comenzaron a reemplazar estos sistemas, por cuestiones de costos y mantenimiento. Como se ha resaltado en este trabajo desde un principio, la convergencia IT/OT ayudó a evolucionar los sistemas SCADA, permitiendo monitorear y administrar remotamente los ICS, aunque comenzaron a incrementarse nuevos riesgos.

Muchos sistemas SCADA que se encuentran hoy en día en vigencia, son inseguros por utilizar sistemas operativos y programas obsoletos, que carecen de las últimas actualizaciones de seguridad y en la mayoría de los casos, son difíciles de actualizar. Por otra parte, gran parte de las redes SCADA se encuentran conectadas a Internet. En consecuencia, se han reducido las distancias entre atacantes y víctimas (Aguirre Ponce, *Op.cit*, 2014).

En los próximos apartados de este capítulo, se profundizarán los puntos que requieren un mayor análisis asociados a las vulnerabilidades y su gestión.

3.4.2 Vulnerabilidades en ICS según NIST

A continuación, se establecerá un listado no exhaustivo de las amenazas ligadas a infraestructuras críticas, agrupadas de acuerdo con su taxonomía. Se enumerarán las vulnerabilidades que se pueden encontrar comúnmente en los ICS, según la guía “NIST 800-82”. El orden de la descripción de estas vulnerabilidades no refleja necesariamente su prioridad de acuerdo con su probabilidad de ocurrencia o gravedad de impacto. Las vulnerabilidades se agrupan en categorías de políticas y procedimientos, plataformas y redes para ayudar a determinar estrategias de mitigación óptimas. Los ICS típicos exhiben un subconjunto de estas vulnerabilidades, pero también pueden contener vulnerabilidades adicionales exclusivas de su implementación, las cuales no aparecen en esta lista.

De Política y Procedimiento

- Políticas de seguridad inadecuadas o poco específicas para ICS.
- Falta de un programa formal de capacitación y sensibilización sobre seguridad ICS, que concientice sobre seguridad y mantenga al personal actualizado sobre las políticas y procedimientos de seguridad de la organización.
- Arquitectura y diseño de seguridad inadecuados.
- Carencia de procedimientos de seguridad específicos o documentados a partir de la política de seguridad para el ICS.
- Pautas de implementación de equipos ICS ausentes o deficientes y, por lo tanto, falta de procedimientos de seguridad adecuados en caso de un mal funcionamiento de ICS.
- Carencia de mecanismos administrativos para la aplicación de la seguridad.
- Pocas o nulas auditorías de seguridad en el ICS, que revisen y examinen los registros y actividades de un sistema, determinen la idoneidad de los controles, garanticen el cumplimiento de la política y los procedimientos de seguridad de ICS establecidos, detecten infracciones en los servicios de seguridad de ICS y recomienden cambios para robustecer los controles de seguridad.
- Falta de un plan de recuperación ante desastres o *DRP*, lo cual podría afectar la continuidad del negocio debido a tiempos de inactividad prolongados.
- Carencia de procesos de gestión de cambios para configuraciones ICS, que controlen las modificaciones de hardware, firmware, software y documentación, garantizando la protección contra modificaciones inadecuadas (National Institute of Standards and Technology, *Op.cit,* 2006).

De Configuración de Plataforma

- Retardo en el desarrollo de parches de software por parte del proveedor, hasta mucho tiempo después de reportarse las vulnerabilidades de seguridad, debido a la complejidad del software ICS y las posibles modificaciones al SO subyacente.
- Carencia de procedimientos de mantenimiento de parches de seguridad del sistema operativo y las aplicaciones.

- Carencia de pruebas exhaustivas al implementar parches de seguridad del sistema operativo y las aplicaciones.
- Utilización de configuraciones predeterminadas, conduciendo a puertos abiertos inseguros e innecesarios y servicios y aplicaciones explotables que se ejecutan en hosts.
- Falta de almacenamiento o respaldo de configuraciones ICS críticas.
- Falta de políticas, procedimientos y mecanismos para la protección de datos en dispositivos portátiles.
- Falta de una política de contraseña adecuada.
- No utilización de contraseñas, para inicio de sesión del sistema, encendido, protector de pantalla, etc.
- Divulgación de contraseñas.
- Utilización de contraseñas débiles, cortas o predeterminadas, sencillas para la predicción humana o de algoritmos informáticos.
- Aplicación de controles de acceso inadecuados, que puedan dar a un usuario de ICS demasiados o muy pocos privilegios (*Ídem*).

De Hardware de Plataforma

- Pruebas inadecuadas de cambios de seguridad.
- Protección física inadecuada para sistemas críticos.
- Acceso físico al equipamiento ICS por parte del personal no autorizado, que podría llevar a la desconexión, intercepción, robo, daños o cambios no autorizados en los datos o el hardware.
- Acceso remoto inseguro en componentes ICS.
- Activos no documentados.
- Presencia de radio frecuencias y pulsos electromagnéticos, factores que pueden vulnerar un ICS, a partir de la interrupción temporal del comando y el control hasta provocar un daño permanente a las placas de circuito.
- Falta de energía eléctrica de respaldo.
- Pérdida de control ambiental, que pueda sobrecalentar los procesadores.

- Falta de redundancia para componentes críticos (*Ídem*).

De Software de Plataforma

- Desbordamiento de búfer.
- Inhabilitación de características de seguridad predeterminadas.
- Factibilidad de denegación de servicios.
- Mal manejo de condiciones indefinidas, mal definidas o "ilegales", por ejemplo, paquetes que tienen un formato incorrecto o que contienen valores de campo ilegales o inesperados.
- Utilización de protocolos ICS inseguros o que transmitan mensajes en texto plano.
- Ejecución innecesaria de servicios.
- Utilización de software propietario que se haya discutido teóricamente en conferencias informáticas públicas o que persista en manuales de mantenimiento de fácil acceso y gran distribución.
- Autenticación y control de acceso inadecuados para el software de configuración y programación.
- Falta de instalación de software de detección y prevención de intrusiones, como IDS o IPS.
- Carencia de mantenimiento de eventos de seguridad.
- Falta de monitoreo en tiempo real (*Ídem*).

De Protección contra Malware de Plataforma

- Carencia de instalación de protección contra malware, como antivirus, necesario para evitar que los sistemas se infecten con software malicioso.
- Falta de actualización de definiciones y patrones de detección del software de protección contra malware, abriendo la puerta a nuevas amenazas.
- Falta de pruebas exhaustivas para la implementación del software de protección de ICS contra malware (*Ídem*).

De Configuración de Red

- Debilidad en la arquitectura de seguridad de red, desarrollada y modificada en función de los requisitos comerciales y operativos, con poca consideración de los posibles impactos de seguridad de los cambios.
- Falta de controles de flujo de datos, como ACL, para restringir qué sistemas pueden acceder directamente a los dispositivos de red.
- Configuraciones deficientes de equipos de seguridad de IT, conduciendo a puertos abiertos inseguros e innecesarios y servicios de red explotables que puedan ejecutarse en hosts.
- Configuraciones de dispositivos de red no almacenadas o respaldadas.
- Contraseñas no encriptadas en tránsito, susceptibles de ser escuchadas por los adversarios, que podrían reutilizarlas para obtener acceso no autorizado a un dispositivo de red.
- Falta de modificación periódica de contraseñas.
- Aplicación de controles de acceso inadecuados (*Ídem*).

De Hardware de Red

- Protección física inadecuada de los equipos de red para evitar daños o destrucción.
- Puertos físicos sin garantía, como USB, que podrían permitir la conexión no autorizada de unidades de memoria USB, registradores de pulsaciones de teclas, etc.
- Pérdida de control ambiental.
- Personal no autorizado con acceso a equipos y conexiones de red.
- Presencia de servicios de ICS fuera de la red de control, lo que hace que la red de ICS se vuelva dependiente de la red de IT, no teniendo los requisitos de confiabilidad y disponibilidad necesarios.
- Falta de redundancia para redes críticas (*Ídem*).

De Perímetro de Red

- Carencia de un perímetro de seguridad definido, conduciendo a un acceso no autorizado.

- Cortafuegos inexistentes o mal configurados, lo que podría permitir el paso de datos innecesarios entre redes, causando varios problemas, como permitir que los ataques y el malware se propaguen entre las redes, hacer que datos confidenciales sean susceptibles de monitoreo y espionaje o proporcionar a las personas accesos no autorizados a los sistemas.
- Presencia de redes de control utilizadas para tráfico no controlado (*Ídem*).

De Monitoreo y Registro de Red

- Falta de eventos confiables de cortafuegos y enrutadores.
- Falta de monitoreo de seguridad en la red ICS necesario para identificar problemas con los controles de seguridad, tales como configuraciones incorrectas y fallas (*Ídem*).

De Comunicación

- Falta de rutas críticas de monitoreo y control.
- Utilización de texto sin formato por parte de los protocolos de comunicación estándar, lo que hace que los adversarios que pueden monitorear la actividad de la red ICS mediante un analizador de protocolos u otras utilidades para decodificar los datos transferidos por protocolos como telnet, FTP y NFS.
- Deficiente o inexistente autenticación de usuarios, datos o dispositivos.
- Falta de verificación de integridad para las comunicaciones, debido a que no hay controles de integridad asociados a la mayoría de los protocolos industriales: para garantizar la integridad, el ICS puede usar protocolos de capa inferior como IPsec, que ofrecen protección de integridad de datos (*Ídem*).

De Conexión Inalámbrica

- Autenticación inadecuada entre clientes y puntos de acceso.
- Inadecuada protección de datos confidenciales entre clientes inalámbricos y puntos de acceso por la falta de un cifrado seguro (*Ídem*).

3.4.3 Aplicación de Parches de Seguridad

La aplicación de parches en los componentes de un sistema operativo en el entorno de ICS es una tarea en la que se debe tener mucho cuidado. Deben probarse adecuadamente para determinar la aceptación y el impacto de los efectos secundarios.

Es recomendable realizar pruebas de regresión, dado que es común que los parches tengan un efecto adverso en otro software. Un parche puede eliminar una vulnerabilidad, pero también puede presentar un mayor riesgo desde una perspectiva del negocio o seguridad. El parcheo de la vulnerabilidad también puede cambiar la forma en que el sistema operativo o aplicación funciona con las aplicaciones de control, haciendo que esta pueda perder parte de su funcionalidad, o verse afectada.

Una vez que se toma la decisión de implementar un parche, existen otras herramientas que automatizan este proceso desde un servidor centralizado y con la confirmación de que el parche se ha implementado correctamente.

Es importante que se considere la separación del proceso automatizado para la administración de parches ICS del proceso automatizado para aplicaciones de IT. En el primer caso, que es el que se está mencionando, la aplicación de parches debe programarse durante las interrupciones planificadas de los procesos industriales (National Institute of Standards and Technology, *Op.cit*, 2006).

3.4.4 Riesgos

El riesgo es una función que indica la probabilidad de que una fuente de amenaza dada explote una vulnerabilidad potencial y el impacto resultante de explotar dicha vulnerabilidad.

La evaluación es el proceso de identificación de riesgos para las operaciones, activos e individuos de una organización, mediante la determinación de la probabilidad de ocurrencia de que una amenaza identificada explote una vulnerabilidad identificada y el impacto resultante. Una evaluación abarca los controles de seguridad que pueden mitigar cada amenaza y los costos asociados con su implementación. Una evaluación de riesgos también debe comparar el costo de la seguridad con los costos asociados con un incidente (*Ídem*).

Clasificación y Evaluación

Para lograr un nivel de riesgo aceptable, se debe reducir la probabilidad ocurrencia de los incidentes, mitigando o eliminando las vulnerabilidades que pueden explotarse, así como las consecuencias derivadas de los mismos.

La priorización de vulnerabilidades debe basarse en el costo y el beneficio, con el objetivo de proporcionar un conjunto mínimo de requisitos de seguridad del sistema de control para reducir el riesgo a un nivel aceptable. Las vulnerabilidades deben evaluarse y clasificarse de acuerdo con los riesgos antes de intentar seleccionar e implementar controles de seguridad en ellas.

Los controles de seguridad que pertenecen a la mencionada familia "NIST SP 800-53" proporcionan las bases y procedimientos para desarrollar, distribuir y mantener una política de evaluación de riesgos documentada. La misma debe describir su propósito, alcance, roles y responsabilidades.

A todo sistema de información se le debe realizar una evaluación de sus riesgos con el objetivo de comprender la magnitud de potenciales daños, como consecuencia de accesos no autorizados, uso, divulgación, interrupción, modificación o destrucción.

También se incluyen en estos controles los mecanismos para mantener actualizadas las evaluaciones de riesgos y realizar evaluaciones periódicas de vulnerabilidades.

La evaluación de riesgos se realiza en la etapa de refinamiento del control de seguridad para determinar si los controles de seguridad seleccionados deben mejorarse o expandirse.

La norma "NIST SP 800-30", proporciona una guía para la gestión de riesgos de sistemas IT, proporcionando una metodología de evaluación de riesgos, que incluye los siguientes pasos:

1. Caracterización del sistema: demarcar límites.

2. Identificación de amenazas: listar fuentes de amenazas que podrían explotar vulnerabilidades.

3. Identificación de vulnerabilidades: listar las vulnerabilidades del sistema que podrían ser explotadas.

4. Análisis de control: listar controles planificados utilizados para mitigar la probabilidad de que se explote una vulnerabilidad o reducir el impacto.

5. Determinación de probabilidad: calificar la probabilidad en alta, media o baja.

6. Análisis de impacto: medir el impacto de la explotación de la vulnerabilidad en alto, medio o bajo.

7. Determinación del riesgo: medir el riesgo en una escala de alto, medio o bajo.

8. Recomendaciones de control: recomendar controles de seguridad y soluciones alternativas para mitigar el riesgo.

9. Documentación de resultados: realizar un informe de evaluación de riesgos que describa las amenazas y vulnerabilidades, mida el riesgo y proporcione recomendaciones para la implementación del control (*Ídem*).

Marco de Gestión de Riesgos

Para poder realizar un tratamiento eficiente, la primera actividad en el Marco de gestión de los riesgos es categorizar la información y el sistema según el impacto potencial de la pérdida que se esté analizando. Para cada tipo de información y sistema en consideración, los tres objetivos de seguridad definidos por la la Ley Federal de Administración de Seguridad de la Información de 2002 de Estados Unidos o *FISMA* (confidencialidad, integridad y disponibilidad) están asociados con uno de los tres niveles de impacto potencial en caso de incumplimiento de la seguridad. Es importante recordar que, para un ICS, la disponibilidad es generalmente la mayor preocupación.

El formato generalizado para expresar la categoría de seguridad o *SC* es:

$$\text{SC}_{\text{del Tipo de Información o Sistema}} = \{(\text{Confidencialidad, Impacto}), (\text{Integridad, Impacto}), (\text{Disponibilidad, Impacto})\}$$

donde los valores aceptables para el impacto potencial pueden ser: “BAJO”, “MODERADO” o “ALTO”.

Las SC se basan en el impacto potencial en una organización en caso de que ocurran ciertos eventos que pongan en peligro la información y los sistemas de información necesarios para que la organización cumpla su misión asignada, proteja sus activos, cumpla con sus

responsabilidades legales, mantenga sus funciones diarias y proteja la vida de las personas. Las SC se deben utilizar junto con la información de vulnerabilidad y amenaza para evaluar el riesgo para una organización.

El establecimiento de una SC apropiada de un tipo de información requiere esencialmente determinar el impacto potencial para cada objetivo de seguridad asociado con el tipo de información particular. Para comprender este concepto, a continuación, se ejemplificará el caso de una empresa con componentes tanto industriales como administrativos:

$$\text{SC}_{\text{Sensores de la planta}} = \{(\text{Confidencialidad}, \ \text{N/A}), (\text{Integridad}, \text{ALTO}), (\text{Disponibilidad}, \text{ALTO})\}$$

$$\text{SC}_{\text{Información administrativa}} = \{(\text{Confidencialidad}, \text{BAJO}), (\text{Integridad}, \text{BAJO}), (\text{Disponibilidad}, \text{BAJO})\}$$

La categoría de seguridad resultante del SC se expresa inicialmente como:

$$\text{SC}_{\text{Sistema SCADA}} = \{(\text{Confidencialidad}, \text{BAJO}), (\text{Integridad}, \text{ALTO}), (\text{Disponibilidad}, \text{ALTO})\}$$

predominando los valores de impacto potencial máximos para cada objetivo de seguridad.

Dada la SC resultante, si la gerencia de la planta de energía decidiera ajustar el impacto potencial de una pérdida de confidencialidad de "BAJO" a "MODERADO", la SC final del sistema de información se expresaría como:

$$\text{SC}_{\text{Sistema SCADA}} = \{(\text{Confidencialidad}, \text{MODERADO}), (\text{Integridad}, \text{ALTO}), (\text{Disponibilidad}, \text{ALTO})\}$$

3.4.5 Vulnerabilidades de Día Cero

Las vulnerabilidades de día cero o *Zero Day* son "grietas explotables que un proveedor de software desconoce y para el que, aún, no se ha establecido ningún parche" (Ablon, *et al*, *Op.cit*, p.25, 2014). El término "día cero" se utiliza para denominar al malware, sin importar de qué tipo sea, que capaz de operar en un sistema protegido y actualizado a su última versión. Es decir, dicho sistema no dispone hasta el momento de protección alguna para las vulnerabilidades que explota su vector atacante y siendo muy difícil de bloquear. A menudo, se desconocen, hasta que se reporta la incidencia y se crea una actualización o parche de seguridad (Villegas López, *Op.cit*, 2018).

Son las más buscadas por los hackers, porque hacen referencia a tecnologías vulnerables a la explotación: por esto son costosas. Se utilizan para espionaje corporativo o ataques altamente dirigidos, en donde resultan ser la única entrada posible (Ablon, *et al*, *Op.cit,* 2014).

Como se indicó en el punto 3.3.6, las vulnerabilidades de día cero se compran y venden en el mercado negro. De todas maneras, no son tan simples ni frecuentes de encontrar y su aparición es bastante impredecible.

3.4.6 Robustecimiento y Defensa de Infraestructuras Críticas

Así como la tecnología continúa avanzando, las IICC también siguen con su evolución. Para sistemas de información e ICS, se están utilizando redes de datos de amplio alcance dadas sus ventajas en cuanto a economía, implementación sencilla, adaptabilidad frente a cambios y facilidad para monitorear y administrar remotamente: este concepto de crecimiento es irreversible y los esfuerzos deben centrarse en la minimización de los riesgos.

Para seguir reforzando esta idea, la conexión de los ICS con otras redes corporativas y públicas alimenta la necesidad de proteger tanto la información como los sistemas, dada la gran cantidad de nuevos vectores de amenaza que se suman desde Internet.

Como ya se ha mencionado, los ciberataques dirigidos a infraestructuras críticas van teniendo una mayor complejidad y por esto deben extremarse las medidas para prevenirlos o enfrentarlos. Se deberán realizar trabajos conjuntamente entre los gobiernos de los distintos países y también entre responsables de los sectores de un mismo país, con el objetivo de generar una estrategia de ciberseguridad que permita resguardar los activos de información, así como los servicios vitales.

“La ciberseguridad aplicada en las infraestructuras críticas permite reducir los riesgos sobre los activos críticos de una nación, mediante la aplicación de políticas, normas, procedimientos, herramientas y/o buenas prácticas de seguridad en el ciberespacio” (Aguirre Ponce, *Op.cit*, 2014, p.14).

3.4.7 Controles para Ciberseguridad Industrial

A continuación, se mencionarán de forma no exhaustiva las mejores prácticas para el robustecimiento y la defensa de acuerdo con los controles según NIST SP 800-82 mencionados en el subapartado 3.2.4, que son necesarios aplicar para la gestión de la seguridad de los sistemas industriales.

Segmentación y Protección de las Redes

Con respecto a la segmentación de las redes, se deben usar sistemas orientados a la protección como, por ejemplo, dispositivos IPS/IDS, cortafuegos, configurados eficientemente, entre las redes IT y OT. Asimismo, siempre será recomendable la utilización de protocolos web que sean seguros como SFTP o HTTPS.

En referencia con la restricción del acceso lógico a la red ICS, esto incluye el uso de una arquitectura de red de zona desmilitarizada o *DMZ,* con cortafuegos para evitar que el tráfico de red pase directamente entre las redes corporativas e ICS y contar con mecanismos de autenticación y credenciales separados para los usuarios de ambas.

Por último, para el mantenimiento de la funcionalidad en condiciones adversas. Se debe diseñar el ICS para que cada componente crítico tenga una contraparte redundante. Además, si un componente falla, debería hacerlo de una manera que no genere tráfico innecesario en el ICS, o bien, que no cause otro problema en cascada (National Institute of Standards and Technology, *Op.cit,* 2006).

Defensa de Malware (CIS)

Los controles 8 de CIS 7.1, están dedicados a controlar la instalación, propagación y ejecución de código malicioso dentro de varios puntos de la empresa, optimizando la automatización de la defensa a gran escala, la actualización rápida, la integración con procesos como la respuesta a incidentes, la recopilación de datos y las acciones correctivas. El software malicioso se mueve rápidamente, mutando e ingresando mediante diversos puntos como por ejemplo, dispositivos de usuario final, archivos adjuntos de correo electrónico, páginas web, servicios en la nube, acciones del usuario o medios extraíbles.

Como ya se ha resaltado, el malware moderno está diseñado para evadir las defensas y atacarlas o bien deshabilitarlas.

Las defensas deben implementarse en múltiples puntos posibles de ser atacados para detectar, detener el movimiento o controlar la ejecución del software malicioso. Las soluciones *endpoint* de seguridad proporcionan características administrativas para verificar que todas las defensas estén activas y actualizadas en cada sistema administrado.

La automatización se utiliza para garantizar que las firmas antivirus, antispyware e IDS, estén actualizadas y puedan ejecutar evaluaciones automáticas diariamente, revisando los resultados para encontrar y mitigar los sistemas que pudieran haber desactivado tales protecciones, así como los sistemas que no tienen las últimas definiciones de malware. Otra parte de este control está orientada a la recopilación de logs con el objetivo de entender los eventos de seguridad históricos dentro de un entorno, como por ejemplo garantizando que existe un registro habilitado para varias herramientas de línea de comandos, como Microsoft Windows PowerShell y Bash[6]. Habilitar este registro hará que sea mucho más fácil para la organización seguir los eventos para comprender lo que sucedió y por qué sucedió (Center for Internet Security, *Op.cit,* 2019).

Accesos: Cuentas, Autorización y Autenticación

Existen controles NIST 800-82 de seguridad que proporcionan políticas y procedimientos para especificar el uso de los recursos del sistema solo por usuarios, programas, procesos u otros sistemas autorizados. Esta familia de controles ayuda a administrar las cuentas del sistema de información, incluyendo alta, activación, modificación, revisión, desactivación y eliminación de cuentas.

Los controles cubren la separación de tareas, otorgamiento de privilegios mínimos, manejo de intentos de inicio de sesión fallidos, notificaciones de uso del sistema, notificaciones de inicio de sesión anterior, controles de sesión concurrente y bloqueos y finalización de sesión.

---

[6] *Esta información se detalla en el punto "C. Control CIS 7.1-8: Defensa de malware", de la sección de Anexos II.*

Por otro lado, también hay controles para abordar el uso de dispositivos portátiles e implementación de tecnologías inalámbricas.

El acceso puede tomar varias formas, incluyendo la visualización, el uso y la modificación de datos específicos o funciones del dispositivo (National Institute of Standards and Technology, *Op.cit,* 2006).

Seguridad de Recursos Humanos

Para abordar adecuadamente la seguridad en un ICS, es esencial que un equipo de ciberseguridad comparta su conocimiento y experiencia con las demás áreas para colaborar en la evaluación y mitigación de riesgos. Este equipo deberá estar compuesto por un miembro del personal de IT de la organización, un ingeniero con experiencia en seguridad de redes y sistemas, un miembro del personal administrativo y al menos, un miembro del departamento de seguridad física.

Con respecto a la continuidad y la integridad, el equipo de ciberseguridad también deberá realizar consultas periódicas al proveedor del ICS e informar directamente al Gerente de Sistemas quien, a su vez, acepta la responsabilidad completa de la ciberseguridad de las redes corporativas e ICS.

Un programa eficaz de ciberseguridad para un ICS debe aplicar una estrategia conocida como "defensa en profundidad". Esta estrategia significa que los componentes de seguridad están organizados de manera tal que se minimiza el impacto de una falla en cualquier parte del mecanismo (*Ídem*).

Resguardo Patrimonial y Seguridad del Entorno

Existen algunos puntos en la normativa NIST SP 800-82 que están dedicados a la seguridad física de los sistemas. Uno de estos, hace hincapié en que se rastree la localización tanto de los activos físicos como de los empleados.

Es necesario establecer mecanismos que permitan conocer la situación geográfica del personal para aseverar que no hubo accesos a las áreas no autorizadas. La restricción del acceso físico a la red y dispositivos ICS tiene como objetivo evitar las interrupciones serias

que podrían ocurrir en la funcionalidad del ICS. Para ello, se deberán utilizar combinaciones de controles de acceso físico: cerraduras, lectores de tarjetas y protectores.

También es importante conocer la localización de los activos de mayor relevancia que tiene una organización industrial en caso emergencia. Además, estos deben estar protegidos frente a vectores como el calor, el humo o el fuego, la humedad o el agua, el humo u otros posibles daños ambientales.

En la normativa, también se menciona la importancia de la protección de todo el cableado. En primer lugar, protegerlo contra accesos no autorizados del personal propio o externo, por las razones ya mencionadas. Y, en segundo lugar, asegurando su preservación frente al medio físico, típico de una planta industrial: campos electromagnéticos, ondas radiales, altas y bajas temperaturas, polvillo, humedad, etc.

Por último, resulta sustancial que se establezca en una política de carácter general, cuáles son las directivas necesarias para asegurar la utilización de dispositivos electrónicos o computarizados portátiles, utilizados para realizar acciones relacionadas con los ICS. Estos no deberán en ninguna circunstancia salir del área segura de ICS, o bien, hacerlo adecuadamente. Tal es el caso del software para programación de PLC (*Ídem*).

3.4.8 Monitoreo y Respuesta ante Incidentes

Según Sun (2019), el incidente (de ciberseguridad) “se considera un problema potencial e inmediato que exige imperativamente resolverse” (Sun, *et al*, 2019, p.1744).

Por su parte, ITIL define al incidente como “una interrupción no planificada de un servicio o la reducción de la calidad de un servicio” (Gestión de incidentes como una práctica en mi organización, 2018, p.7).

El proceso de gestión de incidentes tiene como finalidad la reducción de su impacto negativo, a partir del restablecimiento del servicio con la mayor celeridad.

En líneas generales, un incidente podría impactar significativamente en el cumplimiento y percepción del servicio por parte del usuario o cliente. Por ello, es necesario que todo incidente se registre, se gestione y se almacene correctamente, para satisfacer las expectativas de estos actores. Para esto pueden utilizarse herramientas dedicadas.

Todo incidente debe tener establecida una prioridad, que asegure que deba resolverse en primer lugar en caso de que tenga un impacto significativo,

Existe una técnica conocida como “enjambre”, que ayuda en la tarea de gestionar los incidentes en las organizaciones. Esta se basa en que las distintas partes interesadas trabajen coordinadamente y en conjunto en un principio, hasta que se establezca con claridad cuál de los equipos está mejor preparado para seguir adelante y cuál podría encarar otras tareas (*Ídem*).

Los programas analíticos como las soluciones SIEM para la revisión de registros pueden proporcionar valor para el monitoreo integral de una red. Algunas de estas herramientas, permiten la correlación de eventos para identificar ataques sutiles. Sin embargo, sigue siendo imperiosa la necesidad de contar con personal calificado de seguridad de la información y administradores de sistemas (Center for Internet Security, *Op.cit*, 2019). Además, tal como se indicó en las normativas ISO 27001 y NIST SP 800-53, la organización debe implementar un plan de respuesta ante incidentes que identifique el personal responsable implicado y defina las acciones a realizar por las personas indicadas.

El plan de respuesta a incidentes es el conjunto de documentos que aglutina instrucciones y procedimientos para detectar, limitar y responder ante las consecuencias de incidentes contra los sistemas de información de una organización. La respuesta debe medirse con respecto al servicio proporcionado y no solo respecto al sistema comprometido. Si se detecta un incidente, debe realizarse una evaluación rápida del riesgo para evaluar el efecto del ataque y las opciones para responder, con sus respectivas consecuencias.

Los controles de seguridad de respuesta a incidentes NIST SP 800-53, proporcionan políticas y procedimientos para su monitoreo, manejo y reporte.

El manejo de un incidente de seguridad incluye las fases de:

- Preparación
- Detección y análisis
- Contención
- Erradicación

- Recuperación

Por su lado, los controles cubren la capacitación de respuesta a incidentes para el personal y la prueba de la capacidad propia de un determinado sistema de información.

La planificación de respuesta a incidentes define los procedimientos a seguir cuando ocurre una intrusión. Solamente a modo de mención breve, el estándar NIST SP 800-61 “Guía de manejo de incidentes de seguridad informática”, proporciona una orientación sobre la planificación de respuesta a incidentes, que puede incluir los siguientes elementos:

- Clasificación de incidentes: según el impacto potencial y la probabilidad de ocurrencia, para que se pueda formular una respuesta adecuada para cada caso.
- Acciones de respuesta: dependiendo del tipo de incidente y su efecto en el sistema y el proceso físico que se controla, puede ser desde no realizar acción alguna, hasta el apagado completo del sistema, poco probable para un ICS.
- Acciones de recuperación: las consecuencias del ataque pueden ser menores o bien, causar muchos problemas en el ICS. Es altamente recomendable un análisis previo para determinar la sensibilidad del sistema físico que se controla a los modos de falla en el ICS. En cada caso, las acciones de recuperación paso a paso deben estar documentadas.

Durante la preparación del plan, se deben obtener aportes de los diversos interesados, los cuales también deberían revisar y aprobar el plan de respuesta ante incidentes dentro de la organización (National Institute of Standards and Technology, *Op.cit,* 2006). Este, en resumen, es necesario para detectar un ataque o que, una vez detectado, se puedan seguir los mejores procedimientos para contener su impacto, anular al atacante y recuperarse del mismo de manera segura.

Si no existe un plan de respuesta eficiente, un eventual atacante podría ocasionar un daño mucho mayor, impactando a más sistemas y extrayendo información confidencial, de manera mucho más efectiva y perjudicial.

3.4.9 Planificación de la Continuidad del Negocio

La planificación de la continuidad del negocio aborda el problema general de mantener o restablecer la producción en caso de una interrupción como, por ejemplo, un desastre natural, un evento no intencional provocado por el hombre, un evento intencional provocado por el hombre o una falla del equipamiento.

Una posible interrupción puede implicar intervalos de tiempo de días, semanas o meses para recuperarse de un desastre natural, o minutos u horas para recuperarse de una infección de malware o una falla mecánica o eléctrica.

A los fines de la ciberseguridad de ICS, deben considerarse tanto las interrupciones a largo plazo de recuperación ante desastres, como las interrupciones a corto plazo de recuperación operativa. Debido a que algunas de estas interrupciones potenciales involucran eventos provocados por el hombre, también es importante trabajar en colaboración con la organización de seguridad física para comprender los riesgos de estos eventos y las contramedidas que existen para prevenirlos en este plano. También es importante que la organización de seguridad física comprenda qué áreas de un sitio de producción albergan sistemas SCADA que pudieran tener riesgos de mayor nivel (*Ídem*).

Plan de Contingencia

Los controles de seguridad que pertenecen a la familia NIST SP 800-53 “Plan de Contingencia”, proporcionan las políticas y procedimientos necesarios para implementar un plan de contingencia especificando roles y responsabilidades, asignando personal y actividades asociadas con la restauración del sistema de información después de una interrupción o falla.

Antes de crearlo, es importante especificar los objetivos de recuperación para los diversos sistemas y subsistemas involucrados en función de las necesidades comerciales típicas, que pueden ser de dos tipos: recuperación del sistema y recuperación de datos. Una vez que se definan, se deberá crear una lista de posibles interrupciones y desarrollar y describir el procedimiento de recuperación.

La recuperación del sistema es el tiempo requerido para recomponer todos los enlaces de comunicación y capacidades de procesamiento, mientras que la recuperación de datos es el período de tiempo más largo durante el cual se puede tolerar la ausencia de datos asociados a las características de producción.

Para la mayoría de las interrupciones a menor escala, las actividades de reparación y reemplazo basadas en un inventario de repuestos críticos serán adecuadas para cumplir con los objetivos de recuperación. Para el resto de las interrupciones, se deberán desarrollar planes de contingencia.

Una vez que se documentan los procedimientos de recuperación, se debe desarrollar un cronograma para probar parte o la totalidad de los procedimientos de recuperación. Se debe prestar especial atención a la verificación de las copias de seguridad de los datos y también revisarse periódicamente que se mantengan en un ambiente seguro y de fácil obtención ante una urgencia (*Ídem*).

Ciber-resiliencia

El uso del ciberespacio ha traído mejoras significativas para los individuos, las empresas y la sociedad en general en numerosas áreas: vida social, servicios públicos, comercio, economía, entretenimiento e infraestructuras críticas. Al mismo tiempo, su uso y dependencia han introducido una serie de nuevas amenazas y vulnerabilidades.

Kott & Linkov (2019) definen a la ciber-resiliencia como la "capacidad de los sistemas para anticipar y adaptarse al potencial de sorpresa y falla, debiendo considerarse en el contexto de sistemas complejos que comprenden no sólo los dominios físicos y de información, sino también los dominios cognitivos y sociales, garantizando que la recuperación del sistema ocurra al considerar el hardware, el software y los componentes de detección interconectados de la infraestructura cibernética" (Kott & Linkov, 2019, p.4). Esto significa que, si un sistema es capaz de soportar presiones externas sin que su comportamiento se modifique, entonces es un sistema robusto. Pero si no es capaz de soportar presiones externas y muta para disminuirlas y continuar operando normalmente, entonces es ciber-resiliente.

El primer paso hacia la ciber-resiliencia en una empresa será traducir y comunicar los riesgos cibernéticos a los directivos, incorporándolos en el registro de riesgos empresariales y alineando esos riesgos con los objetivos estratégicos del negocio y teniendo el mantenimiento de la resiliencia operativa como objetivo final (Cyber Resilience in the electricity ecosystem, 2020).

3.4.10 Políticas y Buenas Prácticas Generales

Las pérdidas masivas de datos, los atentados contra la privacidad, el robo de propiedad intelectual, de tarjetas de crédito, de identidades y la denegación de los servicios son realidades diarias del ciberespacio en el contexto actual.

Para defender las infraestructuras existen varias herramientas y tecnologías de ciberseguridad, estándares, capacitaciones del personal, bases de datos de vulnerabilidades, etc. La protección de los componentes individuales de ICS de su potencial explotación incluye:

- Implementar parches de seguridad de la manera más expedita posible, después de probarlos en condiciones de campo.
- Deshabilitar todos los puertos y servicios no utilizados.
- Restringir los privilegios de usuario de ICS a solo aquellos que sean necesarios para cada rol de cada persona.
- Utilizar pistas de auditoría.
- Utilizar controles de seguridad como el software antivirus y el software de verificación de integridad de archivos donde sea técnicamente factible para prevenir, disuadir, detectar y mitigar el malware (National Institute of Standards and Technology, *Op.cit*, 2006).

Estandarizaciones en Redes OT

De la gestión de IT se puede tomar una vasta experiencia, fruto de varios años y aplicarla en los sistemas OT, a pesar de las diferencias existentes. En este ámbito, la estandarización y homogeneización influye sobre las buenas prácticas en la gestión de procesos y servicios.

La gestión de IT ha ido perfeccionando con el correr de los años distintos procesos y estándares generalizados, cuya implementación en el ciclo de vida de los sistemas de operaciones ayuda a la homogeneización de las arquitecturas, procesos y tecnologías.

Para la gestión OT, dada la característica dispersa sus sistemas, no es sencillo contar con ese grado de estandarización. Implementar la estandarización en todas sus capas: servicios, procesos, competencia o gestión, va a permitir que una empresa preste servicios de excelencia en calidad. A la vez puede impactar de manera positiva en cuanto a la disminución de costos (Altran, 2017).

Confianza Cero

Una buena práctica que viene creciendo en cuanto a tendencia en estos últimos años, apoyada en fundamentos auspiciados por NIST, es el modelo de confianza cero o *zero trust*. Este implica no asumir la confianza en ninguna entidad: usuarios, dispositivos, aplicaciones o paquetes, sin importar si dichas entidades están dentro o fuera de una red segura. Este enfoque se basa en tres principios clave.

En primer lugar, elimina todas las zonas de confianza. Dentro de esta arquitectura; se debe acceder a todos los recursos existentes de forma segura, independientemente de la ubicación.

Segundo, las políticas de control de acceso son estrictamente aplicadas, en algunos casos en múltiples ubicaciones en el diseño incluidas puertas de enlace y cortafuegos, siguiendo el enfoque de privilegios mínimos.

En tercer y último lugar, todo el tráfico de red debe registrarse, inspeccionarse y analizarse independientemente de su origen (Eidle, *et al*, 2017). Es cierto que, si bien esto no deja de ser una abstracción teórica y muchos de los elementos descritos en este marco pueden no ser

factibles en términos comerciales por el momento, se ha ido progresando significativamente en el desarrollo de tecnologías que soporten arquitecturas de confianza cero.

Este modelo tiene como objetivo proporcionar una infraestructura de seguridad escalable que pueda aplicarse en muchos tipos diferentes de organizaciones. Los modelos de seguridad tradicionales se basan en un modelo de seguridad perimetral, en el que toda la comunicación es confiable entre dispositivos dentro de un grupo específico. Este modelo se basa en el supuesto de que la red está segmentada y que existe una DMZ entre las partes confiables y no confiables. Este enfoque relativamente estático de la seguridad, basado en perímetros físicos o virtuales, se rompe en los entornos modernos de computación en la nube y dispositivos móviles, donde las características dinámicas hacen que el concepto de DMZ tradicional sea obsoleto. La nube es ahora el nuevo borde de la red y no se puede defender adecuadamente utilizando un enfoque de confianza tradicional.

Por el contrario, tal como se ha mencionado en los tres principios, una arquitectura de confianza cero incorpora una política de seguridad dinámica y automatizada que se extiende a través de los límites de seguridad convencionales pero que ofrece una segmentación de granularidad fina y aislamiento de recursos críticos. Este enfoque se basa en el modelo de confianza explícito, que verifica todo. En otras palabras, todo el tráfico debe ser validado.

La seguridad explícita es parte de un enfoque de defensa en profundidad en capas, que evita que puntos únicos de falla comprometan todo el sistema de defensa. La segmentación de "grano fino" mejora la visibilidad de la gestión y hace posible interrumpir los ataques a la red rápidamente, para evitar que las técnicas de reconocimiento de datos identifiquen incluso estos recursos que están siendo protegidos (De Cusatis, *et al*, 2016).

Capítulo 4

Propuesta Técnica

4.1 Delimitación del Marco de Investigación

Luego de haber realizado un repaso en profundidad del conocimiento expresado en el *Capítulo 3* de este trabajo, es importante explicar también cuál es la justificación sobre la delimitación de la investigación.

Con respecto al foco en la década 2009-2019, es en esta en donde se han registrado los ataques dirigidos de mayor impacto, los cuales coinciden con los casos aquí estudiados. Por otro lado, dada la complejidad de estos ataques en cuanto a innovación de tecnologías y técnicas, son muy similares a los que se siguen utilizando en la actualidad.

Dado que la cantidad de ataques registrados en la última década es bastante extensa, resulta importante reducir esta complejidad para llevar el problema de investigación a una realidad concreta y más sencilla de manipular. De hecho, solamente en la base de datos RISI se han relevado 81 incidentes de seguridad vinculados a sistemas industriales, para el período abarcado entre 2009 y 2014 inclusive. Por esto, es muy recomendable delimitar concretamente el marco de trabajo.

En el apartado 3.3 se han presentado tres de los casos de estudio más representativos para representar el tema principal aquí abordado, los cuales resultan a los criterios de este trabajo, sensatamente ejemplares para ser estudiados sumado a la variedad de las tipologías: un gusano informático, un virus y un ransomware. Adicionalmente, se los ha considerado de acuerdo con su magnitud de impacto, en diversos términos como el económico, social y político. Los tres ataques han presentado un antes y un después en la lucha contra el

cibercrimen, como se ha concluido en sus respectivos apartados sobre las reflexiones finales que han dejado.

Con respecto a Stuxnet, algunos expertos lo califican como la primera arma real de este tipo de guerra, por su clara intención de sabotaje a Irán, agregando otra razón más para que su análisis resulte imprescindible. El impacto de este gusano fue de casi 100.000 equipos, explotando en simultáneo 4 vulnerabilidades de día cero, cifras desmesuradas para el año 2010.

En segundo lugar, el caso del virus Shamoon no afecto tantos equipos como Stuxnet, aunque su resultado se materializó en importantes pérdidas económicas por detener la operatoria de Saudi Aramco durante casi seis meses. También tuvo connotaciones religiosas en una región caracterizada históricamente por los conflictos, lo que agrega una nueva característica que lo distingue de los demás. Shamoon impactó en una cantidad de pérdida de información sin precedentes, dado que se perdió el 80% de la información.

Por último, WannaCry ha sido el más importante caso de ransomware hasta el momento, con una dispersión mundial. Aquí, la variable económica ha sido preponderante, habiendo ocasionado un total de pérdidas que ascendió a más de 4 mil millones de dólares estadounidenses, afectando tanto redes IT como OT.

Además de haber sido mencionados en las bases de datos de público conocimiento, otra razón para la elección de estos tres casos ha sido su recurrente cita en trabajos de investigación prestigiosos. Dentro de la bibliografía que abordó sendos casos, se encuentran:

- *"Economic Impacts of Cyber Security in Energy Sector: A Review. International Journal of Energy Economics and Policy"*, de Venkatachary y otros (2017), en donde se abordan desde el punto de vista del enfoque económico de sus consecuencias.
- *"Cyber Warfare Conflict Analysis and Case Studies"*, de Gazula (2017), que los incluye en una enumeración de diferentes ataques relevantes, focalizado en aspectos de ciberguerra.
- *"Design and Deployment of a virtual environment to emulate a SCADA network within cyber ranges"*, de Marrocco (2019), citándolos como ejemplos de ataques contra comunicaciones e infraestructuras de servicio.

Respecto a las normativas seleccionadas, se han seleccionado las de aplicación internacional mencionadas en los papers “Ciberdefensa en Redes Industriales”, de Kamlofsky y otros (2015) e “International Journal of Computer Applications” de Aghajanzadeh y otros (2015). En estas publicaciones se han nombrado las regulaciones y controles que se han detallado en el *Capítulo 3*, siendo estas las guías principales a abordar ante topologías de red que incluyan segmentos de control industrial y corporativos.

Todos estos aspectos, refuerzan el foco de trabajo sobre Stuxnet, Shamoon y WannaCry en contraposición con los estándares ISO, COBIT, NIST, ITIL y CIS, como elementos ejemplares para corroborar el postulado contiguo. Para ampliar el conocimiento sobre los controles investigados, se puede obtener más información en el *Anexo II* – Detalle de Controles.

4.2 Especificación de la Hipótesis

4.2.1 Presentación

A partir del análisis de los tres casos más relevantes indicados en los subapartados 3.3.9, 3.3.10 y 3.3.11 del *Capítulo 3* y, adicionalmente, del conocimiento adquirido en el apartado 3.2 sobre normativas y subapartados 3.4.7 al 3.4.10 sobre buenas prácticas, en el próximo subapartado se expone la hipótesis central de este trabajo de investigación.

4.2.2 La Hipótesis

Se puede suponer que, si se hubieran aplicado algunos controles de los estándares NIST, CIS, ISO, COBIT o ITIL sobre las infraestructuras críticas en las empresas que han recibido los ataques mencionados, no hubieran tenido impacto alguno en las mismas o, al menos, se hubieran podido mitigar con mayor facilidad.

Capítulo 5

Corroboración Empírica

5.1 Caso Stuxnet

Con respecto a una falencia en la aplicación del control 800-82 3.3.3 de NIST para vulnerabilidades en el hardware de red, se debe tener en cuenta que Stuxnet pudo infectar Natanz, debido a que había puertos USB no asegurados. Alguien pudo introducir una unidad flash extraíble sin restricciones.

El control pone énfasis en que esto debe estar severamente restringido, sobre todo tratándose de equipos conectados a los PLC. De todas maneras, debe destacarse que el ataque dirigido pudo haberse efectuado entre fines de 2009 y principios de 2010 y, por otro lado, esta normativa fue publicada recientemente en 2011 y teniendo en cuenta varias consideraciones del caso Stuxnet para su armado. Este caso deja en evidencia que el aislamiento de Internet no resulta ser una maniobra defensiva eficiente, dado que un eventual atacante podría poseer una cantidad notable de conocimiento interno, capacidades avanzadas y diferentes recursos. Con toda esta combinación de tecnologías, cualquier organización tendría dificultades para llevar a cabo una ciberdefensa adecuada.

Por otro lado, tampoco fue preservado el perímetro del sector industrial o las barreras fueron evadidas, de forma contraria a lo que sugiere el comentario sobre áreas seguras que se realiza en el control ISO/IEC 27002, para Seguridad física y ambiental en la Sección 11.

En las infraestructuras críticas ha habido un antes y un después a partir del caso de Stuxnet, en los procesos de monitoreo para la gestión de servicios ITIL. Desde entonces se ha

introducido que, a partir de haberse detectado el incidente en los controladores afectados, deberá verificarse la integridad del código. Esto se puede realizar monitoreando cambios a través de la red, pero sin utilizar la DLL propia del controlador del proveedor, que podría estar afectada. Si la solución de monitoreo utiliza un controlador independiente, se pueden verificar sin problemas los cambios mediante la toma de huellas digitales de la configuración de los controladores. Una vez que se detecta un cambio, el operador o ingeniero de mantenimiento pueden determinar si el cambio es legítimo. Así, se podrían detectar también cambios originados en estaciones de ingeniería autorizadas, pero que pudieran haber ocurrido accidentalmente o no haberse informado, lo cual constituye una falta grave y frecuente de los contratistas en los entornos de producción. En definitiva, la tarea realizada es la comparación por integridad entre dos estados del mismo componente informático, disparando las alarmas al verificar cambios.

Luego, con respecto a los controles CIS 7.1-8 (ver *Anexo II*), existen dos subcontroles con especial importancia para un caso como Stuxnet, enfocados en su vector de entrada. La función de seguridad del subcontrol 8.4 es detectar ataques a partir de la configuración del escaneo antimalware para medios extraíbles. Para ello se deben configurar las soluciones antimalware para que realicen automáticamente un análisis sobre estos cuando se insertan o conectan. El segundo subcontrol de esta familia es el 8.5, cuya función es proteger a los activos a partir de configuraciones que impidan directamente ejecutar automáticamente el contenido de los medios extraíbles.

5.2 Caso Shamoon

Si bien cabe destacar que en este trabajo no se califica la calidad de implementación de estos estándares (si la hubo) sino en establecer claramente los conceptos que tienen estrecha relación con la defensa ante los ciberataques, para el caso de Shamoon hay un factor adicional. Para el control 9.2 C de ISO 27001, que recomienda la importancia y características que debe tener una auditoría interna, se debe mencionar que la empresa Saudi Aramco estaba certificada internacionalmente para dicha normativa. Sin embargo, en este caso se dio el peor escenario posible, considerando amenazas internas: esta certificación carecía de legitimidad, puesto que el auditor que la validó con su firma había sido sobornado.

Por ello, una vez más se enfatiza el hecho de tener una correcta y válida documentación de las actividades de Auditoría Interna.

Con respecto al control DS7 de COBIT, entendiendo que Shamoon se originó por la apertura de un correo electrónico con phishing por parte de un empleado, preventivamente se podrían haber efectuado capacitaciones y campañas de concientización en las que se informe al personal sobre este tipo de técnicas. Un procedimiento muy común hoy en día consiste en el simulacro del envío de estos correos de manera controlada de parte de los equipos de Seguridad de la Información hacia todos los empleados, para recabar datos estadísticos sobre el grado de concientización que posee una organización y reforzarla eficientemente.

La correcta implementación de la gestión de servicios ITIL para el monitoreo de los correos electrónicos mediante alguna tecnología de seguridad perimetral, hubiese mejorado la capacidad de detección y mitigación de riesgos tales como el phishing. El monitoreo puede ayudar a garantizar el cumplimiento de las estrategias de servicio una vez implementadas, como puede ser la utilización del correo electrónico como herramienta corporativa para gestionar sus diversas tareas. Habiendo mencionado la importancia que tiene para el cumplimiento de las obligaciones diarias, debe filtrarse correctamente su contenido y bloquear correos que contengan enlaces maliciosos.

En lo que concierne a los controles CIS 7.1-8, existe el subcontrol 8.3 de detección, aplicable a empresas grandes como Saudi Aramco, el cual consiste en habilitar características defensivas contra la explotación del sistema operativo, como la prevención de ejecución de datos y la aleatorización del diseño del espacio de direcciones o la implementación de kits de herramientas que se puedan configurar para proteger aplicaciones y archivos ejecutables. De alguna manera, si existe una vulnerabilidad de día cero, estas configuraciones podrían funcionar como cortafuegos para los servicios o puertos que afecten dicha vulnerabilidad.

La sección 12 de la normativa ISO/IEC 27032 para controles de ciberseguridad en servidores, fomenta la implementación de mecanismos de análisis de los datos que son almacenados o transferidos a los servidores. En este caso ejemplar, el borrado de información crítica se debió a la propagación horizontal del virus Shamoon, abarcando la red de servidores. Un control

de este estilo es útil para mitigar la presencia de software malicioso que pudiera llegar a comprometer la información almacenada en los servidores de archivos.

Otro control importante de esta normativa y relativo a la información, sugiere tener en cuenta la clasificación determinada por cada uno de los procesos y su segmentación, para atenuar la exposición accidental o accesos no autorizados. Como ha sido precisado, los datos de la red IT y las redes de ICS eran transmitidos en texto plano y tampoco existía una segmentación real entre las mismas. Así, los atacantes pudieron obtener diversas cuentas de administrador de dominio e instalar controladores de dispositivos robados en todos los sistemas. El ataque apuntó tanto a la red ICS como a la LAN corporativa, pero solamente a componentes Windows, ya que ambas redes los usaban. Muchas redes ICS utilizan Windows para las interfaces HMI de los sistemas SCADA.

De todas formas, esta normativa fue instaurada el mismo año del incidente. Por lo tanto, no hubiera existido la posibilidad de implementar este control por limitaciones temporales.

Por último, es necesario hacer una referencia al control NIST 800-53 IR7, sobre la gestión de respuesta ante incidentes y la protección de activos. En la entrevista, Kubecka ha mencionado que los daños producidos por el malware finalmente fueron detenidos por el equipo de contingencia de una manera drástica pero efectiva, desconectando directamente el cortafuegos entre las redes de IT e ICS. Solo existía uno solo y era explotable debido a su obsolescencia y a las ACL incorrectas que tenía implementadas. Con una política coherente y periódica para el resguardo de los activos importantes, se podría haber recuperado un porcentaje mucho mayor al 20% que finalmente pudo restablecerse, y esto mismo en un tiempo no mayor a un mes. En este caso, los beneficios de esta práctica son mucho más evidentes.

5.3 Caso WannaCry

Con respecto a DS7 de COBIT, una de las variantes estudiadas de WannaCry es la apertura de correos electrónicos con phishing. De la misma manera observada en el caso anterior, la capacitación y concientización del personal como eslabón débil en la cadena de seguridad, resulta ser el pilar de prevención para este tipo de ataques.

En referencia al control NIST 800-53 IR7 para efectuar un plan de respuesta ante incidentes, se trata de un control que podría haber incrementado la capacidad de mitigación de este ataque por parte de las empresas afectadas. Si bien en 2017, no se habían dado ataques de tales proporciones, con una eficiente hoja de ruta en la cual se detallen los pasos a seguir, se hubiera podido intercambiar de información entre las organizaciones afectadas, para avanzar rápidamente con la remediación. Parte de la capacidad de reducción del impacto de un ransomware, se encuentra supeditada a las buenas políticas de resguardo de información. Habiendo realizado el correspondiente respaldo de la información, no será necesario tener que pagar un rescate a cambio de una clave de desencriptación de los archivos afectados.

Al igual que para el caso Shamoon, las herramientas de análisis perimetral del correo electrónico satisfacen los estándares para el monitoreo de eventos correspondiente a la gestión de servicios ITIL. Uno de los focos de WannaCry, ha sido la recepción de links maliciosos. El monitoreo del correo hubiera sido un importante primer paso para filtrarlo posteriormente con políticas de detección de antispam, antigrayware y sobre todo de antiphishing. Así, se podrían bloquear correos maliciosos antes de llegar al buzón del usuario final.

Por otro lado, ya que EternalBlue explotaba una vulnerabilidad en SMB, el monitoreo de las conexiones mediante este servicio hubiera colaborado en detectar direcciones IP no conocidas desde las cuales se descargó el ransomware finalmente en los equipos afectados. Como se ha mencionado en el subapartado 3.4.8, el monitoreo de eventos con una herramienta SIEM y la creación de alertas para estos eventos, constituyen buenas prácticas de prevención de ciberataques.

Para la administración de soluciones endpoint antimalware, es decir herramientas destinadas a la protección de los equipos finales desde los cuales se propagó WannaCry, el control CIS 7.1-8 presenta el subcontrol 2. Este tiene como objetivo asegurar que el software y las firmas antimalware de la organización tengan actualizadas su motor de escaneo y su base de datos de firmas de manera regular. Este subcontrol, es aplicable a empresas de todo tipo de envergadura y es una buena práctica ya que al reportarse una amenaza los distintos vendors de antivirus actualizan rápidamente sus bases de datos, desde las cuales se nutren estas herramientas mediante la conexión a Internet.

Otro problema que ha presentado el caso de WannaCry es su rápida y sofisticada capacidad de propagación dentro de un mismo conjunto de redes interconectadas. Tal es el caso de la práctica P2P de conexión entre clientes y proveedores, generalmente mediante el uso de un túnel. Se han reportado muchos casos en los que la propagación del ransomware dentro de una empresa se extendió posteriormente a otras con las cuales existían accesos compartidos. Con el objetivo de preservar la seguridad de los datos transferidos estableciendo el alcance de las conexiones punto a punto, es aconsejable el seguimiento de la Sección 13.2 de la normativa ISO/IEC 27010 que ya se ha analizado, para el intercambio de información con partes externas. Para concluir con este control, la implementación de una métrica como la cuantificación de enlaces de terceros para los que se hayan definido e implementado correctamente los requisitos de ciberseguridad resulta imprescindible para proteger los datos en tránsito y el canal de comunicación de fallas técnicas, compromisos de funciones y acciones no autorizadas.

Para finalizar el análisis, la normativa ISO/IEC 27032 en su sección 12 para controles de ciberseguridad en servidores, también fomenta la aplicación de técnicas para monitorear los sistemas y sus vulnerabilidades, así como la publicación de actualizaciones para mitigarlas. La CVE-2017-0143 ha sido una vulnerabilidad en el protocolo SMB reportada por Microsoft, quien lanzó actualizaciones críticas para el sistema operativo Windows. Las empresas que no las aplicaron, quedaron expuestas al ataque con la herramienta ya descripta, EternalBlue.

5.4 Análisis de los Resultados Obtenidos

Para poder resumir el impacto de los controles analizados sobre los casos de estudio, se confeccionó la *Tabla 5*. Además de haberse analizado estas dos dimensiones, se contempló el año de publicación de la normativa. De esta manera, es más exacto el análisis de la factibilidad de haber aplicado correctamente el estándar.

Tabla 5: Relación entre las normativas relacionadas con ICS y el impacto de los casos estudiados

Normativas más importantes analizadas			**Impacto directo según la naturaleza del ataque**			
Nombre	**Año de publicación original**	**Temas principales abordados**	**Controles relacionados**	**Caso 1: Stuxnet (2010)**	**Caso 2: Shamoon (2012)**	**Caso 3: WannaCry (2017)**
COBIT	1996	Equilibrio de beneficios, optimización del riesgo y uso de recursos para integrar la gobernanza IT con la empresa.	*DS7: Educar y capacitar a los usuarios*	N/A	**Sí**	**Sí**
ISO/IEC 27001	2005	Requisitos para implantar un SGSI válido: monitoreo, evaluación, implantación, operación, tratamiento de riesgos y realización de auditorías internas.	*Sección 9.2 C: Auditoría Interna*	N/A	**Sí**	N/A
ISO/IEC 27002	2005	Buenas prácticas para implementar los controles de 27001. Política de ciberseguridad. Evaluación y tratamiento del riesgo. Aspectos organizativos de los sistemas de información. Gestión de activos. Seguridad de RRHH. Seguridad física. Gestión de las comunicaciones.	*Sección 11: Seguridad física y ambiental*	**Sí**	N/A	N/A
NIST SP 800-53	2005	Gestión de Respuesta ante incidentes y protección de activos.	*IR7: Plan de respuesta ante incidentes*	N/A	**Sí**	**Sí**
ITIL	2006	Buenas prácticas de gestión del servicio IT. Monitoreo y respuesta ante incidentes.	*Monitoreo*	**Sí**	**Sí**	**Sí**
CIS	2008	Prácticas de defensa para atenuar el impacto de la explotación de malware.	*Control 8*	**Sí**	**Sí**	**Sí**
NIST SP 800-82	2011	Vulnerabilidades en SCADA y mejores prácticas para la convergencia IT/OT.	*Control 3.3.3 – Vulnerabilidades de red*	**Sí**	N/A	N/A
ISO/IEC 27010	2012	Participaciones e intercambios de información relacionados con el suministro, protección y mantenimiento de una organización pública o privada, o bien, de infraestructuras	*Sección 13.2: Intercambio de información*	N/A	N/A	**Sí**

		críticas de los estados y naciones, con terceros.	*con partes externas*			
ISO/IEC 27032	2012	Seguridad en Internet, seguridad de las redes y seguridad de infraestructuras críticas	*Sección 12: Controles de Cibersegu-ridad*	N/A	**Sí**	**Sí**
ISO 22301	2012	Continuidad del negocio y restablecimiento rápido. Planificación, establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora continua de un SGSI.	*Sección 8.4.4: Planes de continuidad del negocio y Sección 8.4.5: Recuperación*	**Sí**	**Sí**	**Sí**
NIST SP 800-30	2012	Recomendaciones para resguardar los intereses de seguridad nacional (IICC) y prevención de la propagación.	*Las métricas las aplica 800-55*	N/A	N/A	N/A

Referencias:

Normativa previa al ataque: *controles críticos no aplicados o aplicados deficientemente*

Normativa posterior al ataque: *controles críticos deseables*

Se pudo determinar, tal como se detalló en los últimos 3 apartados, que existe una estrecha relación entre el seguimiento de algunas buenas prácticas de robustecimiento de la seguridad en las infraestructuras críticas y remediación de vulnerabilidades con la mitigación de ataques dirigidos hacia las mismas. Para cada uno de los casos estudiados, se han hallado varios controles críticos que, de haberse implementado, pudieron haber prevenido o mitigado el impacto de los ataques informáticos más relevantes.

Caso 1 → "Stuxnet" (2010): 3 controles críticos no aplicados o aplicados deficientemente y 2 controles críticos deseables.

Caso 2 → "Shamoon" (2012): 3 controles críticos no aplicados o aplicados deficientemente y 2 controles críticos deseables.

Caso 3 → "WannaCry" (2017): 7 controles críticos no aplicados o aplicados deficientemente.

Existen dos controles adicionales pertenecientes a la normativa ISO 22301, que tienen estrecha relación con los 3 casos y, en líneas generales, con cualquier incidente en infraestructuras críticas. Estos son los controles de las secciones 8.4.4 de planes de continuidad del negocio y 8.4.5, para recuperación.

Los planes de continuidad tienen definidos los alcances, objetivos, criterios y procedimientos de activación e implementación. Además, establecen los compromisos y roles de los actores y de las autoridades, así como las instrucciones de comunicación del incidente, dependencias e interacciones y requerimientos de recursos. Con respecto a la recuperación, se debe contar con instructivos formales para restaurar y retomar las actividades comerciales luego de manifestarse el incidente. Para el caso 2, se han mencionado los largos meses requeridos para el recupero de la información sensible, lo cual implicó la detención total de la producción de una de las empresas petroleras más importantes del mundo. La creación y aplicación de este documento fue mérito de la empresa que trabajó en la contingencia del incidente, cuando hubiera sido útil considerarlo previamente al ataque para contar con valioso tiempo a favor.

La normativa corresponde al año 2012, por lo tanto, es posterior a Stuxnet, aunque aplicable en este, y contemporánea a Shamoon. Aquí, resultaría poco factible el hecho de evaluarse e implementarse en el mismo año a su publicación. Sin embargo, estas prácticas sí pudieron haberse implementado en las empresas afectadas por WannaCry. Un claro lineamiento de continuidad del negocio y recuperación ante casos de ransomware, como ya se ha afirmado, implica contar con políticas claras de resguardo de la información para su restauración.

A continuación, en la sección de Conclusiones se generalizarán todas estas cuestiones.

Conclusiones

A partir del material presentado y analizado en el desarrollo de esta tesis, se puede aseverar que la aplicación de los controles pertenecientes a las normativas más importantes ligadas a infraestructuras IT, hubiera permitido reducir marcadamente el grado de impacto de los ciberataques dirigidos hacia las mismas. De esta forma, queda evidenciada la asociación directa entre las dos variables.

Casi todos estos documentos se encontraban en vigencia al momento de haber ocurrido estos ciberataques notables a infraestructuras críticas y, de haberse aplicado correctamente, pudieron haber tenido un papel fundamental en la mitigación de los impactos.

Asimismo, se destaca la importancia de aplicar las normativas que fueron emergiendo con posterioridad a estos hechos, con el objetivo de proteger este tipo de sistemas, aprendiendo de los errores pasados para no repetirlos en el futuro.

En segundo lugar, se observan dos finalidades recurrentes e implícitas para todo ciberataque. Por un lado, la extrapolación de información y, por el otro, sencillamente el objetivo de ocasionar daños.

Otra importante observación para mencionar, resulta ser la tendencia de los tipos de grupos de ataque. Al principio de la década anterior, un ciberataque dirigido de envergadura requería del apoyo logístico y la participación de varios desarrolladores con distintos conocimientos, así como la posibilidad de contar con la complicidad de empleados directos, tercerizados o proveedores de la organización a la que se pretende atacar, como vector o amenaza interna. A partir de WannaCry, a estos se les suman los ataques individuales. Un desarrollador con conocimientos avanzados y cierta destreza en la explotación de vulnerabilidades críticas puede perpetrar un importante ataque forma aislada, utilizando kits herramientas fácilmente conseguibles, los cuales están publicados en sitios web con fines didácticos o educacionales.

Los atacantes optimizan y mejoran cada vez más sus técnicas. Como se ha mencionado, existen individuos que se desempeñan en equipos bien organizados, por lo que es muy importante seguir sus pasos, estudiar detalladamente sus técnicas y comprender los códigos fuente que utilizan, para neutralizar el impacto de sus ataques e intentar prever cuáles serán

sus tendencias. Es importante reflexionar en que si se ignora cómo actúa un invasor, no se tendrá la destreza necesaria para enfrentarlo.

Adicionalmente, resulta fundamental infundir una cultura de seguridad, concientizando a los miembros de las organizaciones y empleando técnicas preventivas que promuevan la protección de los sistemas de información.

El surgimiento y adopción de las últimas tecnologías viene asociado con un crecimiento potencial de nuevos vectores de amenazas. Es en este contexto, en el que diariamente son explotadas las vulnerabilidades y se realizan ciberataques para obtener accesos no autorizados y manipular los sistemas, arriesgando los intereses de las naciones. Las infraestructuras y servicios críticos, especialmente los del sector industrial, se ven amenazados por las mismas vulnerabilidades que afectan a los ambientes corporativos. Por lo tanto, se les debe brindar un tratamiento correcto para la reducción de sus riesgos, debido a que las amenazas intentan explotar debilidades, ante la falta de controles en los sistemas.

Por otra parte, habiendo abordado el problema del tratamiento de las vulnerabilidades de día cero, se expone una gran limitación, como lo es su carácter impredecible. Estos ataques, aprovechan vulnerabilidades de software desconocidas por los desarrolladores. Por lo tanto, no resulta posible pronosticar con total certeza en qué momento se podrá materializar un incidente en una infraestructura crítica que explote este tipo de amenazas. Estos tipos de ataques requieren respuestas en cuestión de horas o días, a más tardar.

Finalmente, tal como se menciona en las normas, existen varias actividades en los cuales puede ser muy útil invertir tiempo y esfuerzo, para obtener beneficios significativos en la gestión de los riesgos de las infraestructuras críticas. En líneas generales:

- Determinar qué partes son las interesadas.
- Identificar los líderes.
- Concientizar a los usuarios.
- Comunicar correctamente los incidentes.
- Comprender las capacidades de los riesgos.
- Definir quiénes serán los propietarios de los riesgos.
- Realizar un inventario de los activos de la organización.

- Realizar el tratamiento de los riesgos.
- Identificar las oportunidades de mejora.

Sobre la base de que no se puede garantizar la seguridad absoluta de un sistema, si se dispusiera de controles bien implementados y de sistemas de protección de software y hardware, quien se perfila como el principal factor de riesgo es el humano, como eslabón débil en la cadena de la seguridad. Por esto mismo, es imprescindible que, en todo ambiente tecnológico, se trabaje enérgicamente en la concientización. Las acciones de capacitación deben realizarse para todos los niveles del organigrama, comenzando por los superiores hasta los inferiores.

En líneas generales, es deseable que las nociones de ciberseguridad, con sus potenciales riesgos y resguardos sean enseñadas desde edades muy tempranas y en todos los ámbitos de educación.

Líneas Futuras de Investigación

A partir de algunas ideas expresadas en las conclusiones, surgen las posibles líneas de investigación que podrá encarar el lector como líneas de continuación de este trabajo, en donde se podría focalizar en comprender cuáles son las directrices de las vulnerabilidades Zero Day, si existen patrones que permitan comprender cuáles son los objetivos de los hackers según los diversos contextos políticos, sociales y económicos y si se podrá realizar un seguimiento de las tendencias en la Deep Web, etc. Todos estos tópicos serán completamente enriquecedores y complementarán las metas de este trabajo, extendiendo sus límites.

Por otro lado, tal como se ha mencionado en este trabajo, no ha habido gestión de actualizaciones de la base de datos RISI desde 2015 en adelante. Al no existir una base de datos adecuada que cubra todos los incidentes de seguridad, resultaría fundamental construir un repositorio global y unificado para todos estos, el cual se encuentre a disposición del público para que los investigadores puedan analizar los ataques. Por otro lado, las industrias también deberían informar los ataques en sus IICC y a partir de esta nueva base de datos, se podrían documentar rápidamente las vulnerabilidades de día cero, minimizando notablemente su diseminación masiva.

Las crecientes amenazas de ciberseguridad ameritan rediseñar arquitectónicamente las redes, basándose en los principios z*ero trust*. Esta tendencia aplicable a los esquemas topológicos proporciona mejoramientos en la seguridad, tanto en redes corporativas como en entornos de nube, como parte de una estrategia de defensa en profundidad, evitando huellas digitales no deseadas para los recursos protegidos. Una potencial línea de investigación futura podría orientarse en la práctica de confianza cero, optimizada para redes industriales, beneficiándose con las ventajas que ofrece gracias a la automatización.

Asimismo, otra idea que viene cobrando relevancia en los últimos años es el programa de recompensas de errores llamado “Bug Bounty”, en el cual ciertas compañías de software y hardware premian con recompensas monetarias, puntajes y/o reconocimientos a quienes logren encontrar errores de programación y vulnerabilidades en sus tecnologías, dentro de un marco delimitado y controlado. Si bien estos portales son muy comunes hoy en día, poco se ha hablado de su aplicación en ICS.

Existen algunas pocas empresas que ofrecen estos programas para redes industriales, sin embargo, a esta idea todavía le falta madurez para convertirse en una realidad masiva, a la par de los programas de análisis de sitios web. Plantear ventajas y desventajas de esta práctica y evaluar posibles escenarios, incluyendo los riesgos de irrumpir en ambientes industriales no autorizados para los participantes, puede formar parte de trabajos dedicados a esta problemática.

Por último, el período de culminación de este trabajo coincidió con la pandemia COVID-19. Seguramente en los próximos meses, se estará hablando de temas ligados a ataques a infraestructuras críticas de la salud y espionaje afianzado por la declaración implícita de guerra al menos, económica, entre Estados Unidos y China.

Anexo I – Entrevistas Realizadas

A. Listado de Preguntas Realizadas a Christina Kubecka para la Sección 5.4.8, "Virus Shamoon: Ataque Dirigido a Saudi Aramco"

- From your in-depth analysis: was the virus destined for cyber warfare crime?
- Would you agree that it was a targeted attack, considering that most of Saudi Aramco's staff was on vacation?
- How was the process of propagation from an infected machine to other computers?
- From your point of view, do you think it was directed to the ICS network or to the corporate LAN?
- What were the components of the virus that most caught your attention?
- What was the major difficulty in the restoration process?
- Do you think that the attack could have been prevented if at that time international regulatory controls (ISO, COBIT, ITIL, CIS, NIST, etc) had been efficiently implemented? Could any control of the aforementioned regulations have mitigated the cyber-attack?
- In terms of personal emotions, what did you feel when you were progressing with your achievements?

B. Listado de Preguntas Realizadas a Juan Ignacio Alberdi para la Sección 5.4.8, "Ransomware WannaCry: Ataque Internacional"

- (Sobre WannaCry en el caso "Telefónica") […] Aunque se haya tratado de un ataque hasta entonces sin precedentes: en el caso de que no los hubiera, ¿Piensa que podría haberse evitado o mitigado si se hubieran aplicado eficientemente controles regulatorios internacionales?

- Caso contrario, ¿qué pudo haber fallado para que se propagara el ataque?
- ¿Qué otros factores pudieron haber facilitado el éxito del ataque? ¿Qué actividad/es se podría/n haber realizado preventivamente para atenuarlo?
- ¿Hubiera sido importante la aplicación de controles NIST 800-82, asociados a la segmentación correcta de las redes IT y OT para evitar la propagación?
- Desde su punto de vista, ¿pudieron haber ayudado los controles CIS 7.1-8, que tienen como objetivo la automatización de la defensa al detectarse el código malicioso?

Anexo II – Resumen de Puntos Relevantes en los Controles

C. Control CIS 7.1-8: Defensa de Malware

Tabla 6: Descripción de los subcontroles CIS 7.1-8

Sub-Control	Tipo de activo	Función de seguridad	Control	Descripción	Grupos de imple-menta-ción
8.1	Dispositivos	Proteger	**Utilizar software antimalware administrado centralmente**	Utilizar software antimalware administrado centralmente para monitorear y defender continuamente cada una de las estaciones de trabajo y servidores de la organización.	*2-3*
8.2	Dispositivos	Proteger	**Asegurar que el software y las firmas antimalware se actualicen**	Asegurar que el software antimalware de la organización actualice su motor de escaneo y su base de datos de firmas de manera regular.	*1-2-3*
8.3	Dispositivos	Detectar	**Habilitar las características de Anti-Explotación del Sistema Operativo para poder implementar tecnologías AntiExploit**	Habilitar funciones contra la explotación, como la prevención de ejecución de datos y la aleatorización del diseño del espacio de direcciones, que están disponibles en un sistema operativo, o implementar kits de herramientas que se pueden configurar para aplicar protección a un conjunto más amplio de aplicaciones y archivos ejecutables.	*2-3*
8.4	Dispositivos	Detectar	**Configurar el escaneo antimalware para medios extraíbles**	Configurar los dispositivos para que realicen automáticamente un análisis antimalware de los medios extraíbles cuando se insertan o conectan.	*1-2-3*

8.5	Dispositivos	Proteger	**Configurar dispositivos para que no ejecuten automáticamente el contenido**	Configurar los dispositivos para que no se ejecuten automáticamente contenidos desde medios extraíbles.	*1-2-3*
8.6	Dispositivos	Detectar	**Centralizar el registro antimalware**	Enviar todos los eventos de detección de malware a las herramientas de administración antimalware de la empresa y a los servidores de registro de eventos para análisis y alertas.	*2-3*
8.7	Redes	Detectar	**Habilitar el registro de consultas DNS**	Habilitar el registro de consultas DNS para detectar búsquedas de nombres de host para dominios maliciosos conocidos.	*2-3*
8.8	Dispositivos	Detectar	**Habilitar el registro de auditoría por la línea de comandos**	Habilitar el registro de auditoría de línea de comandos para consolas como Microsoft PowerShell y Bash.	*2-3*

Referencias:

Grupo de implementación 1: Una organización con recursos limitados y experiencia en ciberseguridad para implementar los subcontroles.

Grupo de implementación 2: Una organización con recursos moderados y experiencia en ciberseguridad para implementar los subcontroles.

Grupo de implementación 3: Una organización madura con recursos significativos y experiencia en ciberseguridad para implementar los subcontroles.

D. Control COBIT DS7: Educación y Entrenamiento de Usuarios

En este trabajo, se hizo foco en el control “DS7”, para la educación y entrenamiento de usuarios, cuyo fin es certificar que los usuarios estén utilizando efectivamente la tecnología a su disposición y que estén concientizados sobre las responsabilidades y riesgos que existen. Las herramientas de este control son planes de capacitación apropiados para la

organización, como procedimientos para detectar las necesidades de instruir al personal para que este utilice correctamente los servicios de la información, así como la difusión de las campañas de concientización que abarcan cuestiones éticas de la función de estos (Castello, *Op.cit*, 2006).

E. Control NIST 800-82 3.3.3 – Vulnerabilidades en el Hardware de Red

Tabla 7: Detalle del control NIST 800-82 3.3.3

Vulnerabilidad	Descripción
Inadecuada protección física de los equipos de red	El acceso al equipamiento de red debe controlarse para impedir su destrucción o daño.
Puertos físicos no seguros	El no aseguramiento del bus universal en serie o USB y puertos PS/2 podría permitir la conexión no autorizada de unidades de memoria USB, registradores de pulsaciones de teclas, etc.
Pérdida del control ambiental	La pérdida del control ambiental podría provocar el sobrecalentamiento de los procesadores. Algunos procesadores pueden apagarse para protegerse y otros derretirse si se sobrecalientan.
Acceso a equipos y conexiones de red por parte del personal no crítico	El acceso físico a los equipos de red debe restringirse solo al personal necesario. El acceso inadecuado a los equipos de red puede llevar al robo físico, daño o destrucción de datos y hardware, a cambios no autorizados en el entorno de seguridad, a la intercepción y manipulación no autorizada de la actividad de la red y a la desconexión de enlaces de datos físicos.
Servicios de red de control que no están dentro de la red de control	Cuando las redes de control utilizan servicios de IT como DNS y DHCP, a menudo se implementan del lado de IT, lo que hace que la red de ICS se vuelva dependiente de esta red, que puede no tener los requisitos de confiabilidad y disponibilidad que necesita el ICS.
Falta de redundancia para redes críticas	La falta de redundancia en redes críticas podría reducir el tráfico a un único punto de posibilidades de falla.

F. Control ISO/IEC 27001 – Auditoría Interna: 9.2 C

El objetivo de este control será proporcionar información sobre el SGSI, tomando como referencia las necesidades de la empresa y de la normativa ISO 27001.

Los objetivos de la organización serán entonces:

- Evidenciar el plan de auditoría interna incluyendo su periodicidad y funciones, los métodos por los cuales se realizará y la asignación de responsabilidades para planificación, rendimiento y exposición de los informes de los resultados obtenidos.
- Establecer los puntos de vista y el alcance de cada auditoría.
- Elegir a los auditores considerando sus criterios objetivos e imparciales.
- Asegurar el informe de resultados a las áreas que corresponda.
- Documentar las evidencias de información sobre la implementación del programa de auditoría y sus resultados (Sánchez Fernández, *Op.cit,* 2013).

G. Control ISO/IEC 27002 – Seguridad Física y Ambiental: Sección 11

Este control presenta dos partes principales a resguardar:

- Áreas seguras: los perímetros y barreras que se han definido con controles de entrada física y procedimientos de trabajo deben proteger las instalaciones contra accesos no autorizados. También se debe tener en cuenta la protección contra desastres naturales.
- Equipamiento: El equipamiento y el cableado, sumado a las herramientas de apoyo, como energía y aire acondicionado deben asegurarse y mantenerse. El equipo y la información no deben llevarse fuera del sitio a menos que estén autorizados, y deben protegerse adecuadamente tanto dentro como fuera del sitio. La información debe destruirse antes de eliminar o reutilizar los medios de almacenamiento (*Ídem*).

H. Control NIST 800-53 IR7 – Plan de Respuesta ante Incidentes

Este control se aplica para desarrollar un plan de respuesta a incidentes que:

- Brinde a la organización una hoja de ruta para la respuesta ante incidentes.
- Facilite un enfoque de alto nivel sobre cómo la estructura de la gestión de respuesta a incidentes se adapta a la organización general.
- Cumpla con los requisitos únicos de la organización, que se relacionan con la misión, el tamaño, la estructura y las funciones.
- Precise cuáles son los incidentes reportables.
- Provea métricas que permitan medir la capacidad de respuesta a incidentes dentro de la organización.
- Defina los recursos y el soporte de gestión necesarios para mantener y hacer madurar efectivamente el proceso de respuesta ante incidentes.
- Sea chequeado y aprobado.
- Designe explícitamente la responsabilidad de la respuesta a incidentes a entidades o personal.
- Sea protegido contra la divulgación no autorizada.

Como parte de las capacidades de respuesta a incidentes, las organizaciones consideran la coordinación y el intercambio de información con organizaciones externas, incluidos los proveedores de servicios externos y otras organizaciones involucradas en la cadena de suministro (National Institute of Standards and Technology, *Op.cit*, 2006).

I. Control ISO/IEC 27010 – Intercambio de Información con Partes Externas: Sección A.13.2

El Anexo A.13.2 se refiere a la forma en que las organizaciones protegen su información en las redes. Trata de la seguridad de la información en tránsito, ya sea que vaya a una parte diferente de la organización, a un tercero, a un cliente u otra parte interesada. Los subcontroles que lo componen son:

- 13.2.1 Procedimientos de intercambio de información y políticas para la protección de los datos en tránsito.
- 13.2.2 Acuerdos de intercambio para gestionar la transmisión segura de información confidencial entre las partes.
- 13.2.3 Mensajería electrónica.
- 13.2.4 Acuerdos de confidencialidad y secreto para los acuerdos de confidencialidad y "no divulgación" (Sánchez Fernández, *Op.cit*, 2013).

J. Control ISO/IEC 27032 – Controles de Ciberseguridad: Sección 12

Luego de que los riesgos de ciberseguridad sean identificados y se escriben los lineamientos adecuados, se podrán seleccionar e implementar estos controles.

En primer lugar, se definirán las políticas que regularizarán crear, recolectar, almacenar, trasmitir, distribuir, procesar y utilizar información que se comparta o administre en el ciberespacio: actualizaciones de seguridad, clasificación y categorización adecuada de la información, concientización sobre riesgos, evaluación de aplicaciones y monitoreo de la información transmitida y de los accesos a aplicaciones y servidores.

Los siguientes aspectos deben ser tenidos en cuenta en los controles.

Aplicaciones:

- Aplicar controles que ayuden a proteger la información compartida entre las aplicaciones.
- Proteger el manejo de las sesiones web.
- Instituir los lineamientos que garanticen desarrollos seguros y mitiguen ataques que puedan comprometer la información crítica de la empresa, dentro de los desarrollos propios o de terceros.

Servidores:

- Configurar tipos de autenticación que impidan accesos no autorizados.

- Aplicar técnicas para el análisis de la información almacenada para mitigar la presencia de software malicioso.
- Definir y aplicar las técnicas para monitorear los sistemas con el objetivo de hallar vulnerabilidades y monitorear la implementación de actualizaciones periódicas para mitigar problemas de seguridad.

Dispositivos y mecanismos de conexión:

- Mermar las amenazas asociadas con la utilización de redes inalámbricas, públicas o no seguras.

Información:

- Controlar de acuerdo con la clasificación determinada por cada uno de los procesos, para atenuar la exposición accidental o accesos no autorizados (Guzmán Solano, 2019).

K. Control ISO 22301 – Planes de Continuidad del Negocio: Sección 8.4.4 y Recuperación: 8.4.5

La organización debe documentar planes de continuidad del negocio, que no son más que procedimientos para responder ante un incidente disruptivo y detallar cómo retomará sus actividades dentro de un plazo determinado. Estos, estarán conformados por:

- Responsabilidades y roles de los actores principales durante y después de un incidente, es decir, equipos y personas.
- Un proceso que disparará respuestas.
- Datos para tratar las consecuencias de un incidente disruptivo preservando el bienestar de las personas y estrategias para responder a la interrupción y prevención de otros nuevos incidentes.
- Datos sobre la gestión de la comunicación con los empleados, comunidad y contactos de emergencia en general.
- Detalles de cómo se cumplirá con los plazos para la recuperación de las actividades principales.
- Una estrategia de comunicación sobre el incidente.

Respecto a recuperación, la organización debe contar con procedimientos documentados para restaurar y retomar las actividades comerciales con posterioridad a la ocurrencia de un incidente (International Organization for Standardization, *Op.cit, 2012*).

Acrónimos

ACL ***Access Control List***

Regla o filtro de tráfico de red que puede controlar el tráfico entrante o saliente, definiendo cómo se reenvían o bloquean paquetes en una interfaz.

AES ***Advanced Encryption Standard***

Cifrado iterativo basado en la red de sustitución/permutación. Está compuesto por una serie de operaciones vinculadas entre sí, tales como reemplazar entradas por salidas específicas y barajar bits.

AKA ***As-known-as***

En español, “también conocido/s como”.

ARPANET ***Advanced Research Projects Agency Network***

La Red de Agencias de Proyectos de Investigación Avanzada fue una de las primeras redes informáticas de área amplia, creada por el Departamento de Defensa de Estados Unidos. Fue también una de las primeras redes informáticas en ofrecer conmutación de paquetes, tal como funciona Internet, y por esto es vista como su precursora.

Backdoor ***Backdoor***

Tipo de malware que otorga acceso remoto a los recursos dentro de una aplicación, base de datos o servidor de archivos, lo que brinda a los atacantes la capacidad de emitir comandos y actualizar dicho malware.

Blockchain ***Cadena de Bloques***

Tecnología de libro mayor distribuido, basada en una topología punto a punto que permite que los datos se almacenen globalmente en miles de servidores, al tiempo que cualquier persona en la red ve todas las entradas en tiempo real.

BYOD ***Bring Your Own Device***

Tendencia en evolución de los empleados de utilizar sus dispositivos personales para fines laborales, como computadora portátil, teléfono inteligente, tableta o disco duro portátil.

CIS ***Center for Internet Security***

Organización sin fines de lucro cuya misión es identificar, desarrollar, validar, promover y mantener soluciones de mejores prácticas para la defensa cibernética y construir y liderar comunidades para permitir un entorno de confianza en el ciberespacio.

CISO ***Chief Information Security Officer***

Director de Seguridad de la Información, responsable de establecer una estrategia de seguridad y garantizar que los activos de datos estén protegidos.

CMMS ***Computerized Maintenance Management System***

Solución de software que mejora la forma en que los líderes administran las operaciones de mantenimiento, los flujos de trabajo, los equipos, el cumplimiento, el inventario y otros procesos o actividades.

COBIT ***Control Objectives for Information and Related Technology***

Documento de buenas prácticas presentado como un marco de trabajo, orientado al control y supervisión de IT.

CRM ***Customer Relationship Management***

Combinación de estrategias, tecnologías y prácticas que las empresas utilizan para analizar y gestionar las interacciones y los datos de los clientes a lo largo de su ciclo de vida, para mejorar la calidad del servicio y colaborar con su retención, con el objetivo de impulsar el crecimiento de las ventas.

CS ***Ciberseguridad***

Práctica de aseguramiento de la privacidad, exactitud, disponibilidad, integridad y confidencialidad de la información. Está compuesta por un grupo de herramientas en evolución, guías para gestionar riesgos, buenas prácticas, tecnologías y capacitaciones, creadas para proteger los programas, las redes, los datos y los dispositivos de ataques de accesos no autorizados.

DLL ***Dynamic-link Library***

Biblioteca de funciones ejecutables o datos que puede utilizar una aplicación de Windows.

DNS ***Domain Name System***

Sistema que asigna nombres de dominio legibles por humanos, por ejemplo, en URL, a direcciones IP.

E-commerce ***Comercio Electrónico***

Negocio de comprar y vender bienes y servicios en internet.

Endpoint ***Punto Final***

Dispositivo que es físicamente un punto final en una red: computadoras portátiles, de escritorio, virtuales, servidores, móviles, tabletas, etc.

ERP ***Enterprise Resource Planning***

Sistema que consta de componentes de software llamados módulos, centrados en una funcionalidad comercial básica, como finanzas, contabilidad, producción, administración de recursos humanos, gestión de materiales, etc.

FTP ***File Transfer Protocol***

Método básico para mover archivos de una ubicación en una red a otra.

ICS ***Industrial Control Systems***

Distintos tipos de sistemas de control e instrumentación, que abarcan las redes, sistemas, dispositivos y controles usados para operar y automatizar los procesos industriales.

IDS ***Intrusion Detection System***

Sistema que monitorea y analiza el tráfico de la red en búsqueda de comportamientos de ataques materializados en amenazas cibernéticas conocidas, existentes en una base de datos, y los bloquea o previene, para evitar que se infiltren o sustraigan información.

IICC ***Infraestructuras Críticas***

Sistemas vitales para un país, dado que su interrupción o destrucción debilitarían su seguridad nacional, salud o economía.

IIoT ***Industrial Internet of Things***

Extensión y uso de internet de las cosas en sectores y aplicaciones industriales.

IoT ***Internet of Things***

Interconexión digital de objetos cotidianos con internet.

IPS ***Intrusion Prevention System***

Sistema ubicado en el mismo sitio lógico que un cortafuegos, entre el exterior y la red interna, y bloquea proactivamente el tráfico en función de un perfil de seguridad, en caso de que un paquete represente una amenaza conocida.

IPSec ***Internet Protocol Security***

Conjunto de protocolos que garantizan la autenticación, integridad y confidencialidad de las comunicaciones de datos en una red IP.

IRT ***Incident Response Team***

Equipo cuyo objetivo es responder, respetando los estándares definidos, a partir de la materialización de un incidente informático.

IT ***Information Technology***

Empleo de sistemas electrónicos para remitir, guardar, procesar y retomar datos.

ITIL ***IT Infrastructure Library***

Marco de referencia que describe un conjunto de mejores prácticas y recomendaciones para la administración de servicios de IT, con un enfoque de administración de procesos.

L&F ***Look-and-Feel***

Sensación del usuario ante las interacciones con la interfaz de un sistema operativo, sitio web o aplicación, respecto a la disposición de los logotipos, gráficos, menús y otros y la forma en que se opera con sus funciones.

MD5 ***Message-Digest Algorithm 5***

Algoritmo hash criptográfico que se puede utilizar para crear un valor de cadena de 128 bits a partir de una cadena de longitud arbitraria.

NFS ***Network File System***

Tipo de mecanismo de sistema de archivos desarrollado por Sun Microsystems, que permite el almacenamiento y la recuperación de datos de múltiples discos y directorios a través de una red compartida.

NIST ***National Institute of Standards and Technology***

Academia voluntaria creada en Estados Unidos para fomentar la innovación, promover la competitividad en la industria y reducir los riesgos de ciberseguridad.

OT ***Operational Technology***

Tecnologías orientadas al control de procesos tecnológicos o al cambio de estos mediante la monitorización y control de dispositivos de uso industrial.

P2P ***Peer-to-Peer***

Plataforma descentralizada mediante la cual dos nodos interactúan directamente entre sí, sin la intermediación de un tercero.

PLC ***Programmable Logic Controller***

Computador empleado para la automatización industrial de los procesos electromecánicos.

RAT ***Radio Access Technologies***

Método de conexión física subyacente para una red de comunicación móvil, basado en radio, como Wi-Fi, 3G, 4G, LTE y Bluetooth.

RC4 ***Rivest Cipher 4***

Cifrado de flujo utilizado en protocolos como SSL, para proteger el tráfico de Internet y WEP, para asegurar redes inalámbricas. Presenta muchas debilidades en cuanto a seguridad, pero se destaca en cuanto a velocidad.

RPC ***Remote Procedure Call***

Técnica para la construcción de aplicaciones distribuidas basadas en cliente-servidor. Extiende la llamada al procedimiento local convencional para que el procedimiento llamado no necesite existir en el mismo espacio de direcciones.

RSA ***Rivest, Shamir y Adieman***

Interconexión digital de objetos cotidianos con internet.

SCADA ***Supervisory Control and Data Acquisition***

Software utilizado para fiscalizar e inspeccionar procesos industriales en tiempo real y remotamente, mediante la utilización de actuadores y sensores, facilitando la retroalimentación.

SE ***Social Engineering***

Técnica de manipulación que explota el error humano y su falta de prevención, para obtener información privada, acceso u objetos de valor.

SGSI ***Sistema de Gestión de la Seguridad de la Información***

Herramienta utilizada para el conocimiento, gestión y minimización de los potenciales riesgos que atentan contra la seguridad de la información de una nuestra empresa.

SHA-1 ***Secure Hash Algorithm 1***

Hash de 160 bits, susceptible a ataques, creado en 1993

SHA-256 ***Secure Hash Algorithm 256***

Hash de 256 bits perteneciente a la familia de SHA-2, que tiene la misma estructura subyacente y mismo tipo de operaciones binarias lógicas y aritméticas modulares que SHA-1, aunque es más seguro.

SIEM ***Security Information and Event Management***

Solución informática que combina la gestión de eventos de seguridad y datos de registro en tiempo real proporcionando correlación de eventos, monitoreo de amenazas y respuesta ante incidentes, con la gestión de seguridad de la información, que recupera y analiza datos de registro y genera informes.

SMB ***Service Message Block***

Organización sin fines de lucro cuya misión es identificar, desarrollar, validar, promover y mantener soluciones de mejores prácticas para la defensa cibernética y construir y liderar comunidades para permitir un entorno de confianza en el ciberespacio.

TELNET ***Teletype Network***

Protocolo de red no seguro para acceso remoto a un terminal, generalmente mediante el puerto 23.

UScybercom ***United States Cyber Command***

Comando cibernético de Estados Unidos que dirige, sincroniza y coordina la planificación y las operaciones del ciberespacio en defensa de los intereses de dicho país.

VULN ***Vulnerability***

Relacionada con el riesgo y la amenaza, se puede definir como la debilidad o grado de exposición de un sujeto, objeto o sistema, así como fallas, omisiones o deficiencias de seguridad que puedan ser aprovechadas por los delincuentes.

XTEA ***eXtended Tiny Encryption Algorithm***

Interconexión digital de objetos cotidianos con internet.

Referencias

ABLON, Lillian; LIBICKI, Martin & GOLAY, Andrea. Are Hacker Black Markets Mature?. En: Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar. 1ra. Ed. Santa Mónica: RAND Corporation, 2014. pp. 29-30.

ABLON, Lillian; LIBICKI, Martin & GOLAY, Andrea. Projections and Predictions for the Black Market. En: Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar. 1ra. Ed. Santa Mónica: RAND Corporation, 2014. pp. 31-38.

ABLON, Lillian; LIBICKI, Martin & GOLAY, Andrea. Zero-Day Vulnerabilities in the Black and Gray Markets. En: Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar. 1ra. Ed. Santa Mónica: RAND Corporation, 2014. pp. 25-28.

AGHAJANZADEH, Nasser & KESHAVARZ-HADDAD, Alireza. A Concise Model to Evaluate Security of SCADA Systems based on Security Standards. *International Journal of Computer Applications*, 111 (14): pp. 1-9, 2015.

AGUILERA MARTÍNEZ, Patricia. (2002) "Programación de PLCs". Director, Mg. GARZA, Juan Ángel. Tesis de Maestría. Universidad Autónoma de Nuevo León. Facultad de Ingeniería Mecánica y Eléctrica.

AGUIRRE PONCE, Arsenio. (2014) "Ciberseguridad en Infraestructuras Críticas de Información". Directora, Mg. PRANDINI, Patricia. Tesis de Maestría. Universidad de Buenos Aires. Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería.

ALBERDI, Juan Ignacio; RUÍZ DE ANGELI, Gonzalo; CONSTANZO, Bruno; CURTI, Hugo; DI IORIO, Ana Haydée. Windows Malware: Traces in the Host. 9no Congreso Iberoamericano de Seguridad Informática; 2017 Nov 1-3. Buenos Aires, Argentina. CIBSI. 2017.

ARQUILLA John & RONFELDT David. Cyberwar is coming!. En: Athena's Camp: Preparing for Conflict in the Information Age. 1ra. Ed. Santa Mónica: RAND Corporation, 1993. pp. 23-60.

BONNETTO, Emilie; YANNOU, Bernard; BERTOLUCI, Gwenola; BOLY, Vincent & ÁLVAREZ, Jorge. A categorization of customer concerns for an OT front-end of innovation process in an IT/OT convergence context. International Design Conference, 2016 May 16-19. Dubrovnik, Croacia. Hal, 2017.

BOSSERT, Thomas. It's Official: North Korea Is Behind WannaCry [En línea]. Nueva York: Wall Street Journal, 2017. Disponible en: https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537.

CASTELLO, Ricardo. Auditoría en entornos informático. 1ra. Ed. Córdoba: Creative Commons, 2006. 294 p.

CASTRO LUGO, José; PADILLA YBARRA, Juan & ROMERO, Eduardo. Metodología para realizar una automatización utilizando PLC. *Impulso*, 1 (1): pp. 18-21, 2005.

CHEN, Thomas & ABU-NIMEH, Saeed. Lessons from Stuxnet. En: Computer, Vol. 44, Nro. 4. Washington: IEEE Computer Society, 2011. pp. 91-93.

CIS CONTROLS (Center for Internet Security). Version 7.1. East Greenbush: CIS, 2019. 72 p.

CONVERGENCIA ENTRE IT Y OT: Resultado del estudio sobre el estado de la Tecnología de Operaciones y su convergencia con las Tecnologías de la Información [Reporte]. Altran. Madrid: 2017.

CYBER RESILIENCE IN THE ELECTRICITY ECOSYSTEM [Reporte en línea]. World Economic Forum. Ginebra: 2020.

DE CUSATIS, Casimer; LIENGTIRAPHAN, Piradon; SAGER, Anthony & PINELLI, Mark. Implementing Zero Trust Cloud Networks with Transport Access Control and First Packet Authentication [En línea]. Nueva York: SmartCloud, 2016. Disponible en: https://www.blackridge.us/sites/default/files/IEEE-Implementing-Zero-Trust-Cloud-Networks-with-Transport-Access-Control.pdf

EIDLE, Dayna; NI, Si Ya; DE CUSATIS, Casimer & SAGER, Anthony. Autonomic security for zero trust networks. 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference; 2017 Oct 19-21. Nueva York, Estados Unidos.UEMCON. 2017

ESD. ESTUDIOS DE SEGURIDAD Y DEFENSA. Santiago, 1 (3). Junio 2014.

FUENTES, Luis. Malware, una amenaza de internet. *Revista Digital Universitaria*, 9 (4): pp. 2-9, 2008.

GAZULA, Mohan. (2017) "Cyber Warfare Conflict Analysis and Case Studies". Directores, Prof. MADNICK, Stuart & Prof. MOULTON, Allen. Tesis de Maestría. Massachusetts Institute of Technology. M.S., Computer Science Boston University.

GESTIÓN DE INCIDENTES COMO UNA PRÁCTICA EN MI ORGANIZACIÓN [Presentación en línea]. BPGurus-ManageEngine. México DF: 2018.

GIL, Javier. La evolución de las ciberamenazas (SIC) y sus tendencias [En línea]. Granada: Centro Criptológico Nacional, 2017. Disponible en: http://www.seguridadinternacional.es/?q=es/print/1481

GÓMEZ SARDUY, Julio; REYES CALVO, Roy & GUZMÁN DEL RÍO, Daniel. Temas especiales de instrumentación y control. 1ra. Ed. La Habana: Félix Varela, 2008. 164 p.

GUZMÁN SOLANO, Sandra. (2019) "Guía para la implementación de la norma ISO 27032". Tesis de Grado. Universidad Católica de Colombia. Facultad de Ingeniería.

ISACA. COBIT 5: A business Framework for the Governance and Management of Enterprise IT. Rolling Meadows: ISACA, 2012. 94 p.

ISO (International Organization for Standardization). ISO/IEC 22301:2012(en). Ginebra: ISO, 2012. 33 p.

ISO (International Organization for Standardization). ISO/IEC 27000:2018(en). Ginebra: ISO, 2018. 233 p.

IT/OT CONVERGENCE: Moving Digital Manufacturing Forward [Paper]. Cisco. San José: 2018.

JAQUITH, Andrew. Security Metrics: Replacing fear, Uncertainty, and Doubt. 1ra. Ed. Upper Saddle River: Pearson Education, 2007. 335 p.

KAMLOFSKY, Jorge & MIERES, Jorge. Un enfoque de teoría de grafos para mejorar la clasificación y el análisis de crimeware. 9no Congreso Iberoamericano de Seguridad Informática; 2017 Nov 1-3. Buenos Aires, Argentina. CIBSI. 2017.

KAMLOFSKY, Jorge; ABDEL MASIH, Samira; COLOMBO, Hugo; VEIGA, Daniel & HECHT, Pedro. Ciberdefensa en Redes Industriales. 17mo Workshop de Investigadores en Ciencias de la Computación; 2015 Abr 16-17. Salta, Argentina. RedUNCI. 2015.

KAMLOFSKY, Jorge; COLOMBO, Hugo; SLIAFERTAS, Matías & PEDERNERA, Juan. Un Enfoque para Disminuir los Efectos de los Ciber-ataques a las Infraestructuras Críticas. 3er Congreso Nacional de Ingeniería Informática / Sistemas de Información; 2015 Nov 19-20. Buenos Aires, Argentina. CONAIISI. 2015.

KOTT Alexander & LINKOV, Igor. Cyber Resilience of Systems and Networks. 1ra. Ed. Nueva York: Springer Nature, 2018. 475 p.

MANUAL DE SUPERVISIÓN DE RIESGOS CIBERNÉTICOS PARA JUNTAS CORPORATIVAS [Manual en línea]. Organización de los Estados Americanos (OEA). Columbia: 2017.

MARROCCO, Daniele. (2019). "Design and Deployment of a virtual environment to emulate a SCADA network within cyber ranges". Director, Prof. PRINETTO, Paolo. Tesis de Grado. Politecnico di Torino. Corso di Laurea in Ingegneria Informatica.

MEZA-MEDELLÍN, Guillermo. La gestión de servicios: un enfoque de gestión de ITIL y su importancia para la organización. *Revista de Tecnologías de la Información*, 2 (3): pp. 137-145, 2015.

MOHURLE, Savita & PATIL, Manisha. A brief study of WannaCry Threat: Ransomware Attack 2017. *International Journal of Advanced Research in Computer Science*, 8 (5): pp. 1938-1940, 2017.

MURRAY, Glenn; JOHNSTONE, Michael &VALLI, Craig. The convergence of IT and OT in Critical Infrastructure. 15th Australian Information Security Management Conference, 2017 Dic 5-6. Perth, Australia. Edith Cowan University. 2017.

NIST (National Institute of Standards and Technology). Special Publication 800-30: Guide for Conducting Risk Assessments. Gaithersburg: NIST, 2012. 95 p.

NIST (National Institute of Standards and Technology). Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations. Gaithersburg: NIST, 2020. 480 p.

NIST (National Institute of Standards and Technology). Special Publication 800-55: Performance Measurement Guide for Information Security. Gaithersburg: NIST, 2008. 80 p.

NIST (National Institute of Standards and Technology). Special Publication 800-82: Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security. Gaithersburg: NIST, 2006. 164 p.

PÁEZ LOGREIRA, Heyder David; ZAMORA MUSA, Ronald & BOHÓRQUEZ PÉREZ, José. Programación de Controladores Lógicos (PLC) mediante Ladder y Lenguaje de Control Estructurado (SCL) en MATLAB. *Revista Facultad de Ingeniería (Fac. Ing.)*, 24 (39): pp. 109-119, 2015.

PORCHE, Isaac. A cyberworm that knows no boundaries. 1ra. Ed. Santa Mónica: RAND Corporation, 2011. 19 p.

QUINTERO RUÍZ, Alexander; SÁNCHEZ PÉREZ, César & CHIO CHO, Nayibe. Diseño e implementación de prácticas de redes industriales usando controladores lógicos programables. *Revista Educación en Ingeniería*, 1 (2): pp. 52-61, 2006.

RANSOMWARE: HOSTAGE RESCUE MANUAL [Reporte en línea]. KnowBe4. Clearwater: 2019.

RETZKIN, Sion. Hands-On Dark Web Analysis. 1ra. Ed. Birmingham: Packt, 2018. 199 p.

RODRÍGUEZ PENÍN, Aquilino. Sistemas SCADA. 2 Ed. Barcelona: Marcombo, 2007. 448 p.

SÁNCHEZ FERNÁNDEZ, Pablo. (2013) "Sistema de Gestión de la Ciberseguridad Industrial". Director, Prof. GARCÍA, Daniel. Tesis de Maestría. Universidad de Oviedo. Escuela Politécnica de Ingeniería de Gijón.

SHAHZAD, Aamir; LEE, Malrey; XIONG, Neal; JEONG, Gisung; LEE, Young-Keun; CHOI, Jae-Young; MAHESAR, Abdul & AHMAD, Iftikhar. A Secure, Intelligent, and Smart-Sensing Approach for Industrial System Automation and Transmission over Unsecured Wireless Networks. *Revista Sensors*, 16 (332): pp. 2-18, 2016.

STALLINGS, William. Network Security Essentials. 4ta. Ed.. New Jearsey: Prentice Hall, 2011. 432 p.

SUÁREZ, Héctor & PELÁEZ ÁLVAREZ, Juan. Ciber-Resiliencia: aproximación a un marco de medición [En línea]. León: Insituto Nacional de Tecnologías de la Comunicación, 2015. Disponible en: https://www.incibe.es/extfrontinteco/img/File/Estudios/int_ciber_resiliencia_marco_medicion.pdf

SUN, Nan; ZHANG, Jun; RIMBA, Paul; GAO, Shang & YU ZHANG, Leo. Data-Driven Cybersecurity Incident Prediction: A Survey. *IEEE Communications Surveys & Tutorial*s, 21(2): pp. 1744-1772, 2019.

TEN, Chee-Wooi; MANIMARAN, Govindarasu & LIU, Chen-Ching. Cybersecurity for Critical Infrastructures: Attack and Defense Modeling. En: IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans. Vol. 40, Nro 4. Washington: IEEE Computer Society, 2010. pp. 853-865.

THE CONVERGENCE OF IT AND OPERATIONAL TECHNOLOGY [Paper en línea]. Atos. Bezons: 2012.

THE STANDARD OF GOOD PRACTICE FOR INFORMATION SECURITY [Presentación en línea]. Information Security Forum. Londres: 2014.

VALLEJO, Horacio. Los controladores lógicos programables. *Saber Electrónica*, 1 (166): pp. 3-11, 1999.

VENKATACHARY, Sampath; PRASAD, Jagdish & SAMIKANNU, Ravi. Economic Impacts of Cyber Security in Energy Sector: A Review. *International Journal of Energy Economics and Policy*, 1 (7): pp. 250-262, 2017.

VILLEGAS LÓPEZ, Alejandro. (2018) "Aplicación de los principios de la Ingeniería del Malware al contexto del Pentesting". Director: Prof. ARROYO GUARDEÑO, David. Tesis de Maestría. Universidad Autónoma de Madrid. Escuela Politécnica Superior.

WATERS, Gary; BALL, Desmond & DUDGEON, Ian. Protecting Information Infrastructures. En: Australia and Cyber-warfare. 1ra. Ed. Acton ACT: ANU Press, 2008. pp. 85-118.

WATERS, Gary; BALL, Desmond & DUDGEON, Ian. Information Warfare Attack and Defence. En: Australia and Cyber-warfare. 1ra. Ed. Acton ACT: ANU Press, 2008. pp. 33-58.