Vol. Nº 12
Septiembre/2021
www.csirt.gob.cl

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CIBER SUCESOS

Investigación, Tendencia y Concientización

¿QUÉ ES LA CIBERSEGURIDAD INDUSTRIAL Y POR QUÉ ES IMPORTANTE?

CIBERSEGURIDAD INDUSTRIAL

Resguardando
el puente entre IT y OT

Cooperación Internacional
CCI de España

Tendencias
Cadena de suministros,
miel para ciberdelincuentes

Comunidades Nacionales
La labor de IoTSI

Legal
Normas al servicio
de la ciberseguridad
industrial

CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

145 8712 7864
096 4321 5541

CSIRT es el Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile. Su misión es reducir los riesgos de la ciberseguridad en las redes del Gobierno de Chile, asesorando a las diferentes organizaciones que lo componen, actuando como socio estratégico en la defensa de las amenazas y colaborando para brindar mayor seguridad y robustez a las infraestructuras del Estado.

¿Cómo lo **hacemos?**

Contamos con un equipo multidisciplinario de profesionales y las tecnologías para proveer de asistencia técnica y logística a nuestros beneficiarios, así como prevenir la explotación de vulnerabilidades y actuar oportunamente frente a amenazas y ciberataques.

- MONITOREO DE LAS PLATAFORMAS DE INTERNET DE ORGANISMOS PÚBLICOS Y PRIVADOS **24/7**
- INVESTIGACIÓN Y CAPACITACIÓN PARA ENFRENTAR LAS AMENAZAS DEL FUTURO
- DETECCIÓN DE VULNERABILIDADES DE SITIOS Y SISTEMAS WEB DEL ESTADO
- GESTIÓN DE INCIDENTES Y DIFUSIÓN DE MEDIDAS PREVENTIVAS
- INCORPORACIÓN DE NUEVAS TECNOLOGÍAS Y HERRAMIENTAS DE SEGURIDAD INFORMÁTICA
- MEJORA CONTINUA DE LOS ESTÁNDARES DE CIBERSEGURIDAD DEL PAÍS

Alianza del Pacífico · FIRST · CSIRTamericas.org · MERIDIAN Connecting and Protecting

ÍNDICE

pag. **04** Editorial

pag. **05** ¿Qué es la ciberseguridad industrial y por qué es importante?

pag. **09** Ciberseguridad industrial. Resguardando el puente entre IT y OT

pag. **13** Cooperación internacional: CCI de España

pag. **17** Tendencias: Cadena de suministros, miel para ciberdelincuentes

pag. **21** Comunidades nacionales: La labor de IoTSI

pag. **25** Legal: Normas al serviciode la ciberseguridad industrial

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CIBER SUCESOS
Investigación, Tendencia y Concientización

cibersucesos@interior.gob.cl

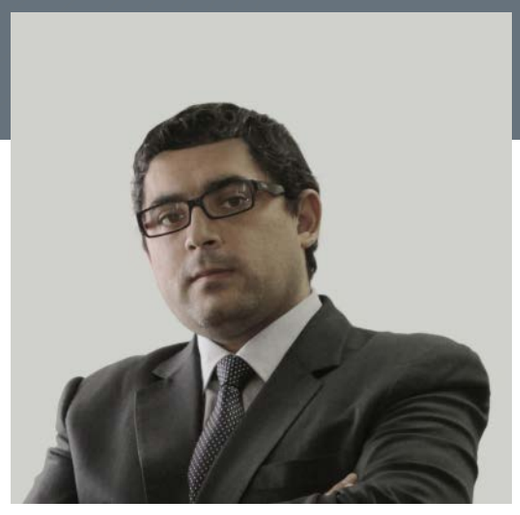
Director: Carlos Landeros Cartes

Jefa de contenidos y edición:
Katherina Canales Madrid

Colaboradores equipo CSIRT:
Ramón Rivera,
Hernán Espinoza,
Carlos Silva
Cristobal Hammersley

Diseño y diagramación: Jaime Millán

EDITORIAL



Carlos Landeros Cartes
Director Nacional
CSIRT de Gobierno

Quienes navegamos día a día la creciente convergencia existente entre lo virtual y lo real, con todas las ventajas e incertidumbres que plantea, debemos también tomar conciencia de que a medida de que la realidad se digitaliza, cada vez más elementos físicos y tangibles de nuestro diario vivir quedan a merced de amenazas cibernéticas que antes quedaban circunscritas a lo virtual.

Es por esto que el presente número de CiberSucesos decidimos dedicarlo a la ciberseguridad industrial, que se ocupa de proteger tanto las tecnologías de la información (IT), el campo tradicional de la ciberseguridad, como las tecnologías de las operaciones (OT), ya que, como señalábamos, cada vez están más entrelazadas e inseparables. Son ejemplos de aquella "convergencia", como se le denomina, entre ambas tecnologías, los principales componentes de la llamada Industria 4.0, como el internet operacional de las cosas (IIoT), sistemas de control industrial (ICS), sensores inteligentes, robots, controladores lógicos programables (PLC) y los sistemas de supervisión, control y adquisición de datos (SCADA), entre otros.

Así, un actor malicioso que logre entrar a los sistemas de una industria moderna puede causar graves daños a su infraestructura física, dañando líneas de producción, pudiendo generar productos peligrosos o nocivos, e incluso hiriendo directamente a personas. Famosos son ejemplos como el ataque que, accediendo remotamente a las redes SCADA de distribución eléctrica en Ucrania dejaron a cientos de miles de personas sin luz, o el gusano Stuxnet, con el que se cree que Israel logró sabotear el programa nuclear iraní.

En definitiva, la ciberseguridad hoy debe contemplar esta integración digital e industrial, y es por eso que nuestras notas principales se dedican a explicar qué es la ciberseguridad industrial, cuáles son sus alcances y cómo protegerla. En la misma línea, la sección Tendencias explica los ataques a la cadena de suministro, una forma de infectar a múltiples organizaciones con solo acceder a una de sus proveedoras.

En el apartado de Comunidades Nacionales contamos con la experiencia de Freddy Macho, presidente del IoT Security Institute Chile (IoTSI), que se ocupa de promover la ciberseguridad industrial en nuestro país, y como parte de la Cooperación Internacional, el ejemplo que desde España supone en Centro de Ciberseguridad Industrial (CCI). Y para cerrar, en la sección Legal, delineamos las principales normas que el CSIRT de Gobierno ha impulsado de la mano de distintas superintendencias para mejorar los estándares de ciberseguridad en varias industrias del país, como la generación y distribución eléctrica, las aguas y las telecomunicaciones.

QUÉ ES LA CIBERSEGURIDAD INDUSTRIAL Y PORQUÉ ES IMPORTANTE

En las economías que buscan lograr el desarrollo, las labores industriales necesitan crecer, expandirse y beneficiarse de la transformación digital de la denominada industria 4.0, internet industrial o industria conectada 4.0. Hablamos de digitalización, de conectar y controlar máquinas, integrar sistemas, incorporar software y hardware de automatización, y recoger grandes cantidades de datos, para tomar decisiones mejores y más rápidas e incrementar la productividad de las organizaciones, resultando así más competitivas.

Entre las nuevas técnicas implementadas (en un proceso acelerado por la pandemia) se cuentan la operación a distancia de las máquinas, el internet de las cosas (IoT) y el almacenamiento cloud, convergiendo de esta manera las redes IT (Tecnologías de Información) y OT (Tecnología de las Operaciones) con el objeto de automatizar, monitorear y gestionar de mejor manera los sistemas.

Se complejiza **la protección**

Este aumento de los aparatos y procesos inteligentes es particularmente crucial cuando se trata de infraestructuras críticas, sectores esenciales para una sociedad, ya que su interrupción puede traducirse en un severo daño a la economía, a la continuidad de los servicios y a la seguridad de la población. Ejemplos son industrias como la sanitaria, combustibles, eléctricas y transporte público, las que deben poner especial atención en considerar la ciberseguridad al incorporar nuevas tecnologías y automatizar procesos.

Es así como la integración de los mundos OT e IT, además de traer consigo beneficios conlleva nuevos riesgos: los ataques cibernéticos. Más aún, las líneas de protección se vuelven más complejas, ya que usuarios de redes IT se conectan a equipos de la red OT para la visualización de la planta, obtención de datos y para optimizar procesos. Esta conexión facilita la implantación de malware en la red OT, por mucho que se pretenda mantener ambos mundos separados físicamente, ya que los propios trabajadores pueden llevar el malware de manera consciente o no.

Es así como la seguridad, confiabilidad y disponibilidad en las industrias modernas se pone en riesgo con la explosión de la conectividad de los sistemas OT como PLC, ICS y SCADA con el mundo IT. La complejidad aumenta ya que cada sistema, sensor y red debe evaluarse y protegerse de ciberataques. Desde el punto de vista de los agentes maliciosos, los ataques cibernéticos industriales suelen buscar la interrupción operativa, la destrucción física o el daño a las personas que usan sus productos o servicios, con fines terroristas o como componente de un ataque de ransomware.

Una mirada **integral**

El enfoque meramente técnico del problema ya ha demostrado no ser suficiente en los otros ámbitos donde la ciberseguridad se ha instalado como un eje fundamental para la sobrevivencia de la empresa. Por esta razón, han emergido importantes directivas orientadas a fortalecer otros pilares de la ciberseguridad industrial que pueden llegar a ser tan importantes como los técnicos, como por ejemplo, las personas.

En el ámbito TI se está buscando aceleradamente intentar convertir a las personas del eslabón más débil en la cadena a ser importantes actores en el esquema de ciberseguridad, actuando como sensores y cuidando sus acciones, aportando alertas y señales tempranas de intentos de ataques por phishing, por ejemplo.

La ciberseguridad industrial tiene así un alcance mucho mayor que solo la seguridad SCADA o la seguridad de los sistemas de control industrial, pues incluye la definición de los Procesos, Personas y Tecnologías necesarias para la protección de las organizaciones e infraestructuras industriales. Por lo tanto, se debe considerar que en ciberseguridad industrial se han de abarcar al menos los siguientes aquellos pilares, con el objetivo de dar cobertura integral y recibir las lecciones aprendidas desde el mundo TIC:

SISTEMAS

Deben incorporar a los entornos OT, sistemas específicos de la segmentación de redes, con el análisis y gestión de eventos relacionados con la seguridad, entre otros.

PROCESOS

Deben establecerse políticas, procedimientos y programas que ayuden a fortalecer los entornos industriales y de infraestructuras.

PERSONAS

Es necesario crear equipos multidisciplinares que sean capaces de identificar posibles amenazas y vulnerabilidades, de gestionar los Sistema de Gestión de Seguridad de la Información (SGSI) y de adaptar los procesos propuestos en las normativas y documentos de referencia a cada planta concreta.

Riesgos de la **industria**

Las ventajas de la digitalización y la conectividad son enormes, pero han aumentado la superficie de exposición de las empresas a ciberataques, y ampliado las posibles consecuencias de un ciberataque, que pueden incluir, por ejemplo, el secuestro de datos, el robo de propiedad industrial y la interrupción o alteración de las operaciones hasta una modificación de valores prefijados (setpoints) que hagan que el producto fabricado no tenga las propiedades esperadas (incluyendo la calidad sanitaria) o que se tomen decisiones equivocadas. Sus consecuencias pueden ser, además de económicas, medioambientales e incluso provocar lesiones o muerte a las personas, todo lo que afectará obviamente además la reputación de la empresa.

La industria es vulnerable fundamentalmente a dos grupos de amenazas informáticas.

1. El primero son las amenazas a las tecnologías de la información (TI), que se utilizan para fines comerciales y administrativos. Estos son los ataques sobre los cuales se escucha en los medios con mayor frecuencia y en los que se infectan equipos de oficina para el robo o destrucción de datos. Este grupo de amenazas está relativamente bien entendido y existen soluciones avanzadas de protección, en forma de aplicaciones antivirus o para la detección y prevención de intrusiones (IDS / IPS).

2. El segundo grupo de amenazas, que tiene como objetivo la tecnología operacional (OT), como son los sistemas de producción y control, están viendo una respuesta, en términos de ciberseguridad, con un notable retraso. Peor aún, la gran mayoría de los sistemas industriales en uso fueron desarrollados hace muchos años, cuando la ciberseguridad no tenía el impacto y conocimiento que tiene actualmente.

En vista de esta situación, es clave que la industria se informe periódicamente de las vulnerabilidades reportadas por los fabricantes de sus equipos industriales, las medidas de mitigación que esos proveedores sugieren y en qué plazo plantean resolver esas vulnerabilidades y cómo.

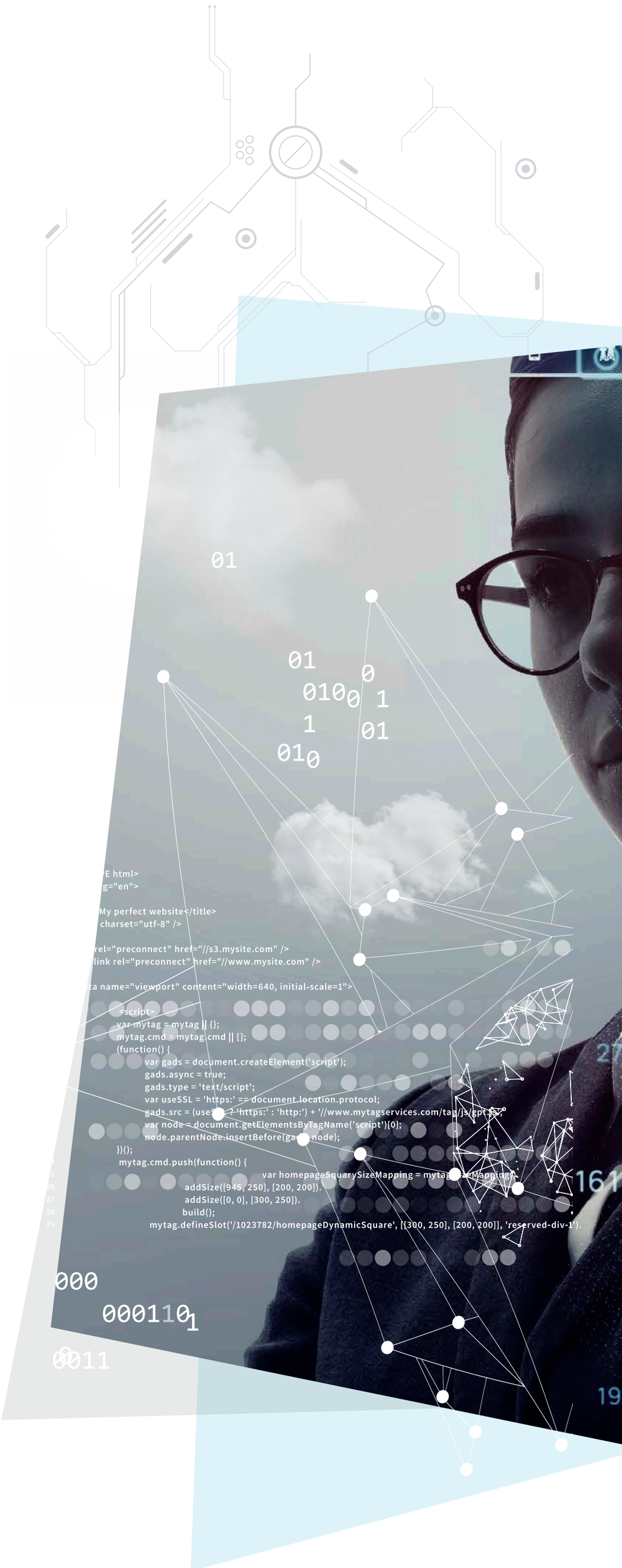
Afortunadamente, cada vez más fabricantes de sistemas y equipamientos industriales disponen de departamentos especializados en la ciberseguridad de sus productos, para identificar sus vulnerabilidades, resolverlas, informar sobre ellas y asesorar a sus clientes sobre cómo solucionarlas, además de diseñar sus nuevos sistemas de una forma más cibersegura.

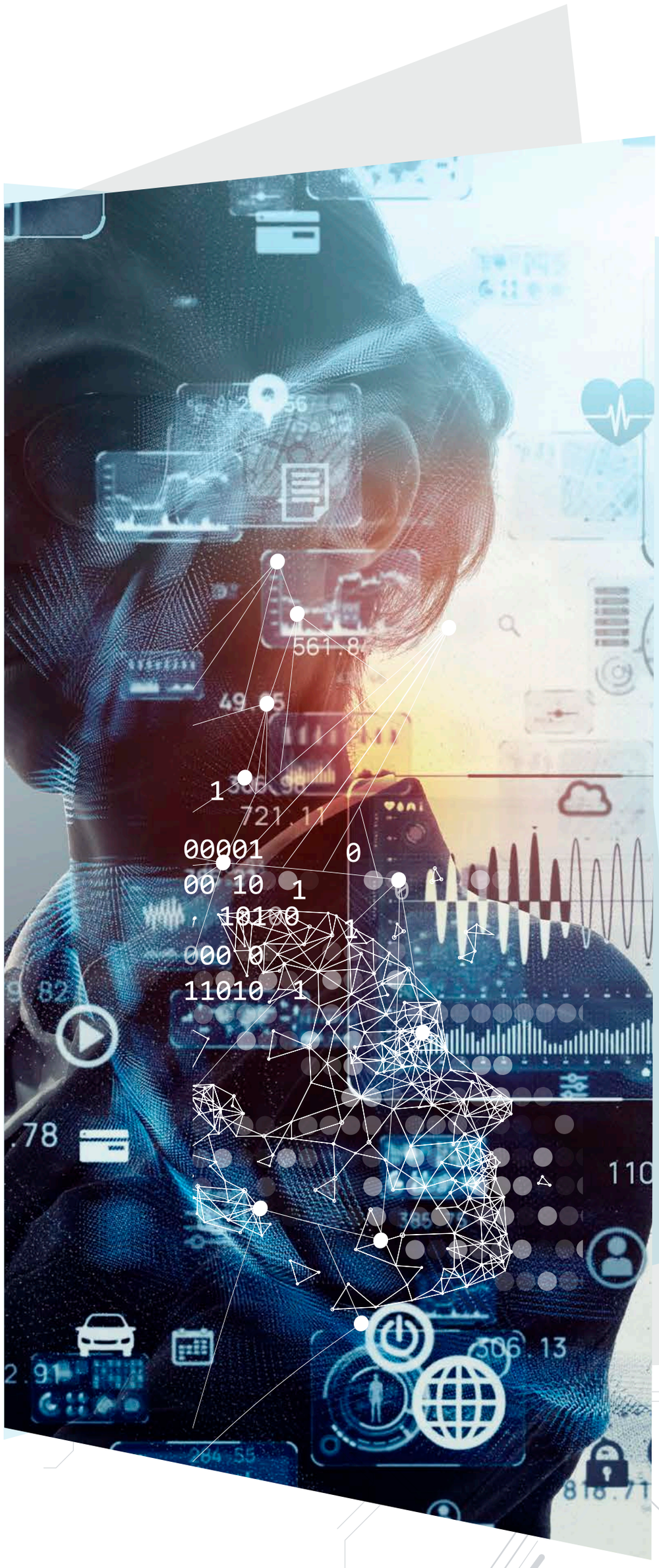
Tal como para el mundo TI la experiencia ha demostrado que es fundamental contar con un directorio informado y responsable de la seguridad de la empresa, expresando su voluntad, estrategia y directivas a través de una política general, es sumamente importante que en el ámbito industrial también se pueda desarrollar y aplicar una estrategia desde el más alto nivel de autoridad en la empresa.

Las fases fundamentales **para contar con una estrategia**

Es necesario, entonces, definir una estrategia de ciberseguridad industrial que abarque y establezca los objetivos de alto nivel:

- Establecer un Sistema de Gestión de Riesgos para la ciberseguridad industrial.
- Establecer un programa de promoción de una cultura de la ciberseguridad industrial.
- Establecer de un programa de medidas de ciberprotección para las instalaciones industriales.
- Establecer objetivos y metas específicas de garantía de resiliencia y continuidad de los sistemas de operación.





Se debe así establecer un objetivo final de gestión, que asegure que la ciberseguridad industrial está siendo gestionada, revisada, mejorada y sostenida a través de un Sistema de Gestión de Seguridad de la Información (SGSI).

Para que las empresas que han incorporado sistemas y dispositivos de OT, IoT, o sistemas y hardware de automatización avanzados puedan mantenerse vigentes y no ser golpeados por los ciberdelincuentes, necesitan apostar por la ciberseguridad. Ciertamente hay dificultades, tales como la de aplicar actualizaciones y mantenimiento en los sistemas de automatización y control industrial, dada la alta exigencia de disponibilidad, el menor grado de concienciación en ciberseguridad de los entornos industriales en comparación con la seguridad física, y la falta de conocimiento en cuanto a normas o buenas prácticas aplicables a las empresas del sector.

Pero con un trabajo integral de implementación de ciberseguridad, a través de un SGSI, y no descuidando los otros pilares (sistemas, procesos y personas) se logrará mejorar notablemente la postura de la organización ante las amenazas que se ciernen sobre sus activos, procesos industriales, sus trabajadores y sus clientes y consumidores.

Fases de una estrategia de **ciberseguridad industrial**

D1 Definición de una Estrategia de Ciberseguridad Industrial

- **D2**: Gestión de los Riesgos para la Ciberseguridad Industrial
- **D3:** Promoción de una Cultura de la Ciberseguridad Industrial
- **D4:** Establecimiento de Medida de Ciberprotección en instalaciones industriales
- **D5:** Garantía de Resiliencia y Continuidad de los Sistemas de Operación
- **D6:** Gestión, Revisión, Mejora y Sostenibilidad del SGCI

Fuente: "Guía SGCI", CCI, ISA Sección Española y Centro Vasco de Ciberseguridad

CIBERSEGURIDAD **INDUSTRIAL**

Resguardando el puente entre IT y OT

La integración de las tecnologías operativas (OT) y de la información (IT) no es algo nuevo. De hecho, el fenómeno se encuentra descrito en la pirámide de automatización industrial. Pero en los tiempos que estamos viviendo y dado el avance de la denominada revolución industrial 4.0, cada día más industrias están realizando la convergencia de sus redes IT y OT. Con ello, el mundo físico y el mundo digital se integran para mejorar el flujo de datos entre departamentos, los procesos productivos y con ello cumplir con los objetivos de la empresa de forma más eficiente.

Este fenómeno llama la atención dado que, históricamente, en la mayoría de las firmas industriales estos sistemas se encontraban separados, islas conviviendo en una misma organización. Por un lado, los sistemas IT tradicionales que funcionan sobre bases de datos, servidores de aplicaciones y servidores web, y por el otro, los sistemas OT, basados en redes de campo, redes de control, redes de supervisión y redes de operación.

Más aún, esta evolución de las tecnologías del Internet Industrial de las Cosas (IIoT) ha representado un desafío y una oportunidad para grandes compañías de IT como Microsoft, Intel, HP y Red Hat, las cuales se encuentran desarrollando nuevos productos para integrar tecnologías OT e IT utilizando software estándar.

IMPLICANCIAS PARA **LA CIBERSEGURIDAD**

A medida que los sistemas IT y OT se integran, el manejo de la ciberseguridad en una compañía con operaciones industriales se hace más desafiante. Hablamos de empresas que complementan sus procesos fabriles con entornos en la nube, pudiendo enviar información a servidores externos para facilitar la gestión, registrar datos, visualizar información, realizar análisis o alimentar modelos de inteligencia artificial, pudiendo llegar a desarrollar infraestructuras virtuales y entornos para sistemas de comunicación híbridos.

Por supuesto, un efecto de estos fenómenos es hacer de los sistemas de control industrial (ICS), esenciales hoy para el manejo de infraestructura crítica, un blanco cada día más atractivo para los ciberataques. Así, la Agencia de Ciberseguridad y Seguridad de la Infraestructura de los Estados Unidos (CISA) ha informado tan solo este año más de 300 alertas sobre información de problemas de seguridad, vulnerabilidades que afectan a los proveedores de infraestructura industrial (de 1770 alertas realizadas desde 2010)[1] .

Según la firma de ciberseguridad Kaspersky[2] , por ejemplo, en el segundo semestre del 2020 un 33,4% de los computadores ICS fueron atacados, lo que significó un alza contra los números registrados un año antes para el 62% de los países investigados.

(1) ICS-CERT Advisories | CISA
(2) Threats against industrial control systems on the rise in H2 2020, growing by nearly 8 percentage points in the engineering sector | Kaspersky

Según ese estudio, la industria con más computadores ICS con objetos maliciosos detectados fue Petróleo y Gas, con 46,7%, seguida de Ingeniería e Integración ICS, con 44%, y Energía, con 39,3%.

La misma Kaspersky entrega[3] además el panorama de las amenazas detectadas y bloqueadas por sus productos según el origen de la infección. Según estos datos, un 20,5% de las amenazas provienen de internet, un 7% de medios removibles y 4,4% de correo electrónico.

Indicator	H1 2020	H2 2020	2020
Global percentage of attacked ICS computers	32.60%	33.42%	38.55%
Percentage of attacked ICS computers by region			
Northern Europe	10.1%	11.5%	12.3%
Western Europe	15.1%	14.8%	17.6%
Australia	16.3%	17.0%	18.9%
United States and Canada	17.2%	16.5%	19.6%
Eastern Europe	26.4%	28.0%	30.5%
Southern Europe	27.6%	29.6%	33.1%
Latin America	33.6%	34.3%	38.8%
Russia	32.2%	34.6%	39.5%
Middle East	34.0%	34.6%	40.2%
East Asia	42.9%	41.8%	46.3%
South Asia	38.8%	41.3%	47.0%
Central Asia	43.7%	43.9%	48.8%
Africa	45.6%	46.4%	51.2%
Southeast Asia	49.8%	47.5%	53.9%
Main threat sources globally			
Internet	16.7%	16.7%	20.5%
Removable media	5.8%	5.4%	7.0%
Email clients	3.4%	4.1%	4.4%

(3) Threat landscape for industrial automation systems. Statistics for H2 2020 | Kaspersky ICS CERT

PRINCIPALES **RECOMENDACIONES**

Para poder proteger las redes convergentes que emplean IIoT, es necesario establecer protecciones multicapa que cubran tanto las redes de TI como las de OT. Además, los sistemas OT deben actualizarse de igual forma que los sistemas IT, pero debido al poco dinamismo de los sistemas y la necesidad de estar siempre funcionando, los proveedores realizan menos actualizaciones y las compañías muchas veces no las implementan a tiempo, ya que en muchos casos para realizarlo deben detener sus procesos productivos. Y es que mientras en los sistemas TI se da prioridad a la confidencialidad, la disponibilidad es lo más importante cuando se trata de equipos OT.

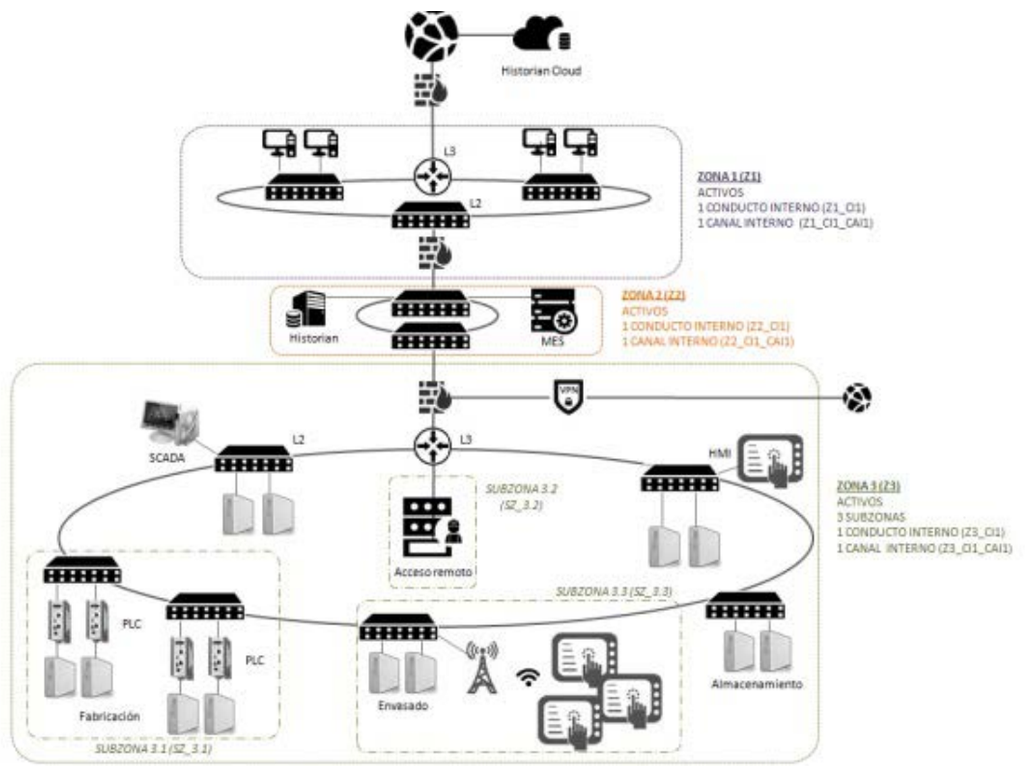
Por otro lado, hardware y software deben, en su conjunto, hacer posible una defensa que permita lo siguiente:

- Integrar tecnologías actuales y futuras.
- Detectar cambios no intencionados o no autorizados.
- Restaurar o volver a un modo seguro para continuar el funcionamiento después de un ataque.
- Proteger toda comunicación mediante canales cifrados y que pueda enviar alertas o logs a los concentradores, los cuales deben ser monitoreados por un equipo de respuesta ante incidentes de seguridad informática o por un centro de operaciones de Seguridad OT/IT.

Las estaciones que monitorean las operaciones industriales como computadores y servidores deben, por supuesto, estar protegidas por agentes antimalware y anti-cryptor, para prevenir los ransomware. Y las redes o infraestructura que soportan la OT deben igualmente estar en constante monitoreo, identificando los activos que se detecten (versiones de firmware y de software), verificando la integridad de comunicación entre dispositivos y midiendo la telemetría en tiempo con historial de flujo.

También es recomendable implementar las mejorar prácticas de seguridad industrial internacional, como aquellas incluidas por la norma IEC 62443, conjunto de estándares que a su vez se basa en los conceptos definidos por la noma ISA99. Estas normativas proponen lo que llaman zonas, conductos y canales de seguridad.

Las zonas de seguridad son agrupaciones de activos físicos o lógicos, que lleva un borde, podrían existir subzonas. Los conductos son zonas de seguridad que agrupan activos vinculados a la electrónica de red, como por ejemplo switches, routers, firewall y cables. Y los canales son la forma lógica de comunicar diferentes zonas, asociadas físicamente con un conducto.



En definitiva, las compañías deben considerar la ciberseguridad en los procesos operativos y de producción como un solo modelo, para englobar e identificar la mayor cantidad de riegos y amenazas posible. Y hacerlo siempre de acuerdo a estrategias definidas incorporando los puntos listados en este artículo, que recoge las mejores prácticas para conseguir mejorar la ciberseguridad de las organizaciones industriales.

LOS MAYORES ATAQUES A ICS DE 2020

de acuerdo con **Kaspersky**

- APT 33/APT 34
- Sofacy
- APT41/BARIUM/Winnti
- PoetRAT
- Ataques a los sistemas de aguas de Israel
- Mikroceen
- Chafer/APT39/Remix Kitten
- TA410
- Lazarus
- Gorgon APTCactusPete
- Palmerworm/BlackTech
- IAmTheKing
- MontysThree
- MuddyWater
- Cicada/APT10
- SolarWinds

Centro de Ciberseguridad Industrial

LA INICIATIVA ESPAÑOLA QUE CONECTA EXPERTOS Y DIFUNDE CONOCIMIENTOS **EN CIBERSEGURIDAD INDUSTRIAL**

El Centro de Ciberseguridad Industrial (CCI) es una asociación privada fundada en España, sin fines de lucro, y con capítulos en varios países del mundo. Su objetivo es, como dice su nombre, promover la seguridad informática en la industria, principalmente a través de la creación del que denomina el mayor ecosistema que reúne a industrias (usuarios finales), proveedores de servicios, profesionales, integradores, y organizaciones públicas.

Es cada día más claro que la importancia de la misión del Centro de Ciberseguridad Industrial (CCI) es clave, en vista de la progresiva automatización e incorporación tecnológica de los procesos productivos, siendo su cara más visible, probablemente, la proliferación del internet industrial de las cosas (IIoT).

Resulta útil, en vista de este escenario, conocer algunas de las formas en que podemos beneficiarnos de las plataformas de la CCI para mejorar la ciberseguridad de nuestras industrias, incluso si optamos por unirnos la entidad a través de su membresía gratuita.

FOCO EN LA DISEMINACIÓN **DE CONOCIMIENTO**

Para lograr sus objetivos de mejora permanente de la ciberseguridad industrial, la CCI se basa en tres principales grupos de actividades:

1. FACILITAR INSTANCIAS DE NETWORKING (generación de redes) entre expertos de diversos países, contando ya con más de 3 mil miembros en el mundo. Esto lógicamente dependía de foros y eventos, los que ahora han sido traspasados al mundo online. Además, la CCI provee de un catálogo de profesionales y empresas proveedoras, que permite fácilmente contactar expertos.

2. COMPARTIR CONOCIMIENTOS, a través de cursos y una plataforma donde los miembros pueden acceder a guías e información, muchos de ellos disponibles incluso bajo el registro gratuito. La CCI también entrega un boletín semanal a todos quienes se registren con ella, también incluido con la membresía sin costo.

3. INTERCAMBIAR EXPERIENCIAS, al conectar miles de profesionales de la ciberseguridad industrial. No por nada la CCI está presente hoy en 22 países de América y Europa, incluyendo España, además de contar con un equipo que lo representa en el Medio Oriente.

Dentro del segundo pilar, el educacional, se encuentra la Plataforma de Conocimiento del CCI, que reúne los documentos, publicaciones y herramientas sencillas de mejoramiento de la ciberseguridad industrial, además de ser el portal de acceso para los socios a la Escuela Profesional del CCI, los Equipos de Conocimiento del CCI, y el Programa de Reconocimiento del CCI.

— Esta escuela consta de cursos prácticos, dirigidos principalmente a encargados de ciberseguridad en organizaciones industriales, con descuentos para socios, además de poner a la venta guías con los temas más importantes que deben dominar.

— También cuentan con talleres y un Máster. Algunos ejemplos de talleres son: ciberseguridad en sistemas de automatización y control industrial (IACS), gestión de incidentes de ciberseguridad industrial y análisis forense en un entorno de automatización industrial.

— Su equipo docente y de compartición de conocimiento se divide asimismo en tres áreas de experiencia:

- **Infraestructuras críticas industriales:** enfocados en la protección de infraestructura crítica para el funcionamiento del negocio y la prestación de servicios, o perteneciente a sectores estratégicos como el energético, el agua, el transporte, el químico y el nuclear.
- **Digitalización industrial:** cuya especialidad son los proyectos de ingeniería e industria 4.0, ciudades inteligentes o salud inteligente, además de departamentos de instrumentación y control.
- **Buen gobierno y compliance:** Dedicados a asegurar el cumplimiento de las regulaciones y normativas que regulan a la industria y su ciberseguridad.

Además, entre las formas en las que la CCI promueve la ciberseguridad industrial se encuentra su constante impulso de la adopción de estrategias de ciberseguridad que incorporen las tecnologías operacionales (OT).

Finalmente, es importante recordar que si bien la mayor parte de los miembros y actividades de la CCI están en su origen, España, en Chile cuenta con Gabriel Bergel y Jesús Peña Martinez como coordinadores, y Freddy Macho, presidente y fundador del capítulo chileno del IoTSI participa igualmente como coordinador, pero para Venezuela.

01

```
<!DOCTYPE html>
<html lang="en">
<head>
  <title>My perfect website</title>
  <meta charset="utf-8" />

  <link rel="preconnect" href="//s3.mysite.com" />
  <link rel="preconnect" href="//www.mysite.com" />

  <meta name="viewport" content="width=640, initial-scale=1">

   <script>
  var mytag = mytag || {};
  mytag.cmd = mytag.cmd || [];
  (function() {
        var gads = document.createElement('script');
        gads.async = true;
        gads.type = 'text/script';
        var useSSL = 'https:' == document.location.protocol;
        gads.src = (useSSL ? 'https:' : 'http:') + '//www.mytagservices.com/tag/js/gpt.js';
        var node = document.getElementsByTagName('script')[0];
        node.parentNode.insertBefore(gads, node);
  })();
   mytag.cmd.push(function() {
                var homepageSquarySizeMapping = mytag.sizeMapping().
          addSize([945, 250], [200, 200]).
          addSize([0, 0], [300, 250]).
         build();
    mytag.defineSlot('/1023782/homepageDynamicSquare', [[300, 250], [200, 200]], 'reserved-div-1').
```

CADENA DE **SUMINISTROS** MIEL PARA CIBERDELINCUENTES

La cadena de suministro en el campo de las tecnologías de la información y comunicación (IT) es un ecosistema complejo e interconectado a nivel mundial, que abarca todo el ciclo de vida del hardware, el software y los servicios que gestionan. Desde dispositivos de telefonía móvil hasta software de intercambio de información, el Estado y la industria compran estos productos y servicios y los utilizan para alimentar y habilitar sus sistemas. Dada su importancia, debemos tener claro que una cadena de suministro es tan fuerte como su eslabón más débil.

Los ciberdelincuentes que buscan robar, comprometer o alterar y destruir información sensible pueden atacar al Gobierno y a la industria a través de sus contratistas, subcontratistas y proveedores en todos los niveles de la cadena de suministro IT. La complejidad de la seguridad de la cadena de suministro se ve elevada por el hecho de que las amenazas y vulnerabilidades pueden introducirse durante cualquier fase del ciclo de vida del producto: diseño, desarrollo y producción, distribución, adquisición y despliegue, mantenimiento y eliminación. Estas alteraciones pueden incluir la incorporación de software malicioso, hardware y componentes falsificados; el diseño de productos defectuosos y procesos de fabricación y procedimientos de mantenimiento deficientes.

Es así como un ataque a la cadena de suministro (en inglés: supply chain attack), también llamado ataque a la cadena de valor o ataque de terceros, ocurre cuando un actor de amenazas cibernéticas se infiltra en la red de un proveedor de servicios y emplea código malicioso para comprometer uno o más activos o bien la incorporación de hardware o software malicioso en un servicio o producto contratado al proveedor.

Este tipo de ataques tienen un gran potencial destructivo, debido a que un proveedor puede dar servicio a muchos clientes, los cuales pueden ser a su vez proveedores de otras empresas, existiendo además una relación de confianza entre cliente y proveedor que muchas veces implica la existencia de menos controles de seguridad. De esta forma, en una sola operación pueden infectarse o comprometerse a todos los clientes, o bien solo a algunos específicos, a través, por ejemplo, un APT (en inglés: Advanced Persistent Threat).

ALGUNAS TÉCNICAS **EMPLEADAS**

en el ámbito de la industria de la cadena de suministro de software

Los ataques a la cadena de suministro de software suelen requerir gran aptitud técnica y compromiso a largo plazo, siendo a menudo difíciles de ejecutar.

En general, es más probable que los actores maliciosos del tipo amenazas persistentes avanzadas (APT) tengan tanto la intención como la capacidad para llevar a cabo este tipo de ataques, mediante campañas que pueden dañar la seguridad nacional. Los actores maliciosos emplean diferentes técnicas para ejecutar los ataques a la cadena de suministro de software, siendo estas algunas de las más comúnmente utilizadas:

- Secuestro de actualizaciones.
- Ataque a la firma de códigos.
- Compromiso del código de fuente abierta (opensource).

Estas técnicas no son mutuamente excluyentes y los actores maliciosos a menudo las aprovechan simultáneamente.

CONSECUENCIAS DE UN ATAQUE A LA CADENA DE **SUMINISTRO DE SOFTWARE**

Un ataque a la cadena de suministro de software puede tener severas consecuencias. Primero, los actores maliciosos utilizan un proveedor de software comprometido para obtener privilegios y acceso persistente a una red de víctimas. Al comprometer un proveedor de software, evitan las medidas de seguridad perimetral tales como routers de borde y cortafuegos, obteniendo así su acceso primario. Si un actor malicioso pierde el acceso a la red, pueden volver a entrar en una red utilizando el proveedor comprometido. Dependiendo de la intención del actor malicioso y su capacidad, este malware adicional puede permitir que el actor lleve a cabo diversas actividades maliciosas, que pueden incluir el robo de datos personales o financieros, el seguimiento de organizaciones o individuos, la inhabilitación de redes y sistemas, e incluso causar daños físicos o la muerte.

RECOMEN**DACIONES**

1. Política de seguridad de la información para las relaciones con los proveedores

Las instituciones necesitan identificar e imponer controles de seguridad de la información para mitigar los riesgos asociados al acceso de los proveedores, en una política que debe contemplar:

a. La identificación y la documentación de los tipos de proveedores, y a quiénes autorizará la organización para acceder a su información.

b. Un proceso y ciclo de vida estandarizado para administrar las relaciones con los proveedores.

c. La definición de los tipos de acceso a la información que se permitirá a los distintos tipos de proveedores y el monitoreo y control del acceso.

d. Requisitos mínimos de seguridad de la información para cada tipo de información.

e. Procesos y procedimientos para monitorear la adherencia a los requisitos de seguridad de información establecidos para cada tipo de proveedor.

f. Controles de precisión y nivel de detalles para garantizar la integridad de la información o el procesamiento de información que entrega cualquiera de las partes.

g. Tipos de obligaciones aplicables a los proveedores para proteger la información de la información.

h. Manejo de incidentes y contingencias asociadas con el acceso a los proveedores.

i. Resiliencia y, en caso de ser necesario, disposiciones de recuperación y contingencia para garantizar la disponibilidad de la información.

j. Capacitación de concientización para el personal de la organización involucrado en las adquisiciones sobre políticas, procesos y procedimientos correspondientes.

k. Capacitación de concientización también para el personal de la organización que interactúa con el personal de los proveedores.

l. Administración de las transiciones necesarias de información.

2. Abordar la seguridad dentro de los acuerdos con los proveedores

Las instituciones deben establecer y acordar los requisitos de seguridad de la información pertinentes con cada proveedor que puede acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI de la organización.

Se debería incluir en los acuerdos los siguientes términos para satisfacer los requisitos de seguridad:

a. Descripción de la información.

b. Clasificación de la información.

c. Requisitos legales y normativos, incluida la protección de datos, los derechos de propiedad intelectual y derechos de autor.

d. Reglas de uso aceptable de la información, incluido uso inaceptable de ser necesario.

e. Una lista explícita del personal autorizado para acceder a o recibir la información.

f. Requisitos y procedimientos de la administración de incidentes.

g. Normativas pertinentes para la subcontratación, incluidos los controles que se deberían implementar.

h. Derecho a auditar los procesos y los controles del proveedor relacionados al acuerdo.

i. Obligaciones del proveedor de cumplir con los requisitos de seguridad de la organización.

3. Monitoreo y revisión de los servicios del proveedor

Las instituciones deben monitorear y auditar la prestación de servicios del proveedor regularmente para garantizar que los términos y condiciones de seguridad de la información de se respeten y que los incidentes y de seguridad de la información se gestionen correctamente.
La organización debe retener la visibilidad en las actividades de seguridad como la administración del cambio, la identificación de vulnerabilidades y los informes y respuestas ante incidentes a través de un proceso de informes definido.

4. Administración de cambios en los servicios del proveedor

Las instituciones deben administrar los cambios a la provisión de servicios de parte de los proveedores, manteniendo y mejorando las políticas de seguridad de la información, los procedimientos y controles específicos, considerando la criticidad de la información comercial, los sistemas y procesos involucrados y la reevaluación de riesgos.

a. Cambios a los acuerdos del proveedor.

b. Los cambios realizados por la organización.

c. Cambios en los servicios del proveedor a implementarse.

d. Uso de nuevas tecnologías.

e. Adopción de nuevos productos o nuevas versiones.

f. Nuevas herramientas y entornos de desarrollo.

g. Cambios en la ubicación física de las instalaciones de servicios.

h. Subcontratación a otro proveedor.

En el contexto del importante proceso que está llevando la transformación digital del Estado y la profundización de la industria 4.0, junto a los potentes procesos integradores que vienen de la mano con las tecnologías IoT y las redes móviles de transporte de datos y servicios (5G), recordamos cuán importante es mantener informados y entrenados a nuestros colaboradores en estas materias con el objetivo de transformar a dicho recurso humano, actualmente considerado uno de los eslabones más débiles en la cadena, en un activo fundamental del esquema de ciberseguridad, pasando entonces de tener "n" puertas de entrada vulnerables a tener "n" redes neuronales biológicas al servicio de la ciberseguridad corporativa o institucional.

Ciertamente el contexto actual de globalización, tanto de proveedores como de clientes, sobre todo para un Chile que está inmerso profundamente en el sistema de comercio internacional, hacen de la trazabilidad de la ciberseguridad un aspecto crítico en lo relacionado con los ataques a la cadena de suministro, y nos desafían a implementar controles suficientes para mantener la cadena de seguridad de cada uno de los componentes, tanto hardware como software, que utilizamos como suministros para producir nuestros bienes y servicios, sin que se rompan los cibersellos de seguridad en el camino. Solo así podremos aventurar algún grado de confianza en estos escenarios e implementar exitosamente arquitecturas Zero Trust.

IoTSI

La labor de IoTSI para reforzar la ciberseguridad de la industria en un entorno cada día más conectado

Freddy macho
Presidente de IoT Security Institute Chile (IoTSI)

Freddy Macho es el presidente de IoT Security Institute Chile (IoTSI) y coordinador regional del Centro de Ciberseguridad Industrial (CCI), además de presidente del Centro de Investigación de Ciberseguridad IoT-IIoT y también del Comité IoT-IIoT del Laboratorio de Ciberseguridad de la Organización de los Estados Americanos (OEA). Consiguientemente, este experto en ciberseguridad y seguridad de la información está íntimamente involucrado en esfuerzos por mejorar los estándares de seguridad de las empresas en nuestro país, y aquí nos informa de su trabajo para lograrlo de la mano de IoTSI.

Hoy en día, los procesos industriales en Chile y el mundo tienen un alto componente automatizado, o al menos electrónico, lo que se ve ejemplificado por los sistemas de control industrial (ICS —aparatos, programas, redes y sistemas usados para operar o automatizar procesos industriales), parte del denominado Internet Industrial de las Cosas (IIoT). “Muchos aspectos de la vida moderna dependen del funcionamiento ininterrumpido de los ICS”, explica Freddy Macho, presidente del CCI en Chile, ya que, añade, un ataque a los ICS puede sumar a los efectos de un ciberataque tradicional, graves efectos concretos sobre el mundo físico, como la interrupción de servicios básicos y el daño al medioambiente.

TENDENCIAS EN CHILE QUE IMPULSAN AL IIOT DE ACUERDO CON FREDDY MACHO

Electricidad
- Desarrollo del uso del hidrogeno verde.
- Impulso de la generación de eléctrica por medio de parques eólicos y centrales solares.
- Desarrollo e impulso de la medición de consumo eléctrico inteligente.
- Mantenimiento de entornos sostenibles.

Transporte
- Desarrollo e impulso de la electromovilidad.
- Seguimiento automatizado de la localización de vehículos

Minería
- Uso de Hidrogeno verde en la movilización de vehículos de carga.
- Automatización de centros de control.

Petróleo y gas
- Supervisión y monitoreo de oleoductos y gasoductos conectados.
- Seguimiento y gestión remota de activos.

Agua
- Controladores del flujo de agua
- Tratamiento de aguas residuales
- Gestión inteligente del consumo de agua

Es en medio de esta proliferación del IIoT que, para Macho, la protección de sensores, instrumentos y dispositivos autónomos conectados con aplicaciones industriales a través de internet se torna más desafiante, ya que "el aumento de habilidades tales como el machine learning, la inteligencia artificial, el big data y el 5G amplían los posibles vectores de ataque".

CÓMO **MEJORAR**

En este contexto, es claro que las organizaciones deben redoblar sus esfuerzos. De acuerdo con Macho, hay que combinar adecuadamente estrategia, recursos humanos capacitados y tecnología: "Se necesita generar estructuras organizacionales especializadas en la ciberseguridad industrial, creando líneas de trabajo estratégicas dirigidas de manera exclusiva al resguardo de las redes industriales y las infraestructuras críticas", explica el especialista. Así, "a corto plazo se identifica la necesidad de generar una estrategia de ciberseguridad industrial que plantee de manera robusta la defensa de los sistemas industriales, las infraestructuras críticas y los ambientes hiperconvergentes", señala

"La ciberseguridad en el mundo OT (tecnología operativa, o de operaciones) no puede basarse en los mismos criterios y enfoques del mundo IT (tecnologías de información)", asegura el experto, ya que mientras en el contexto IT la información es lo central, cuando se trata de OT, lo clave son los procesos. Del mismo modo, resulta imperativo que exista comunicación entre los encargados de ciberseguridad y los ingenieros de planta, que son quienes conocen a fondo el funcionamiento de sus procesos productivos.

PRINCIPALES AMENAZAS **Y DESAFÍOS**

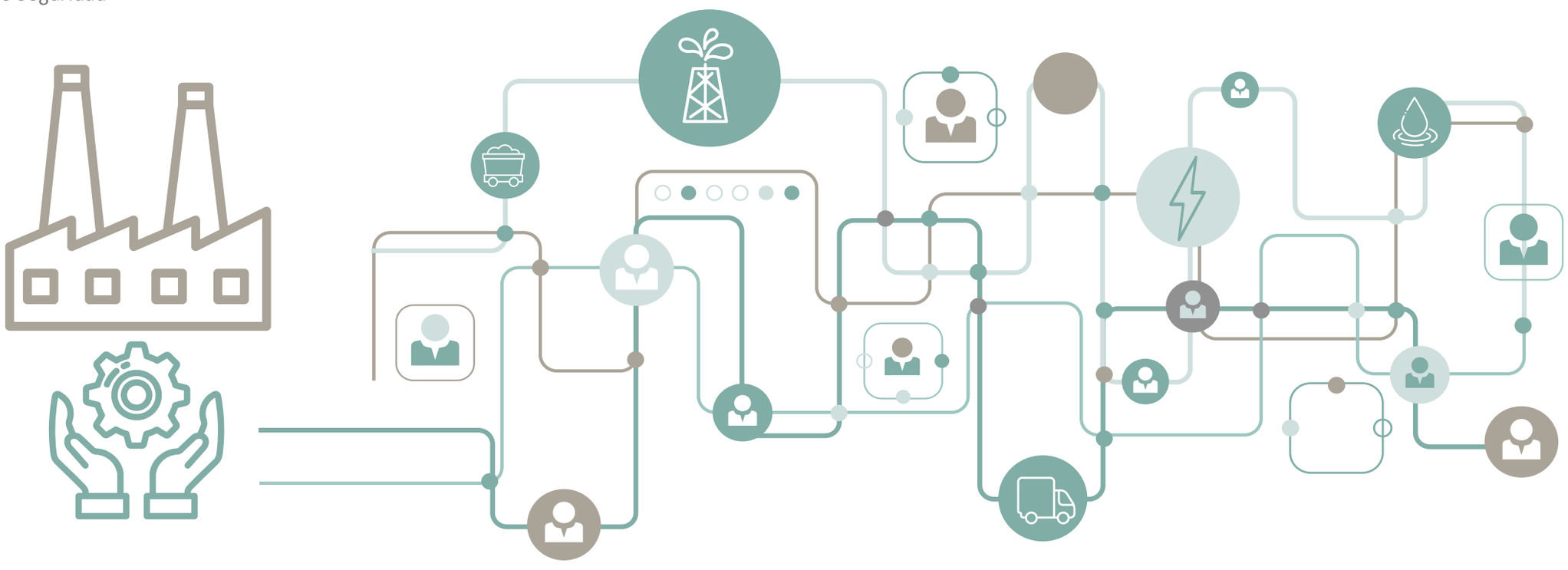
Macho explica que los dispositivos del denominado internet de las cosas industrial (IIoT) se ven afectados por las mismas amenazas que el resto de los dispositivos, pero con consideraciones adicionales, como tener que "adoptar algoritmos criptográficos ligeros, en términos de requisitos de procesamiento y memoria, el uso de protocolos estándar y la necesidad de minimizar la cantidad de datos intercambiados entre nodos".

Y es que la integración del mundo físico en el tejido de la web, "impone requisitos de seguridad avanzados que deben satisfacerse para garantizar un control estricto sobre la interacción del servicio de IIoT.

Todo esto, en luz de una falta de normativas técnicas y regulación en Iberoamérica, señala Macho, quien resume de la siguiente forma los principales desafíos de ciberseguridad en el contexto OT.

Desafíos de **ciberseguridad OT**

Tema de seguridad	Tecnología operativa (OT)
Antivirus y códigos móviles	' Los requisitos de memoria pueden afectar a los ICS. ' Las organizaciones solo pueden proteger los sistemas heredados con soluciones posventa. ' Generalmente se requiere carpetas de "exclusión" para evitar que los programas pongan en cuarentena archivos críticos.
Administración de parches	' Hay una larga línea de tiempo para la instalación exitosa del parche. ' Son específicos de cada proveedor. ' Pueden "romper" la funcionalidad del ICS.
Tecnología Soporte	' Durante 10 o 20 años se mantiene un mismo proveedor. ' El final de la vida útil del producto crea nuevos problemas de seguridad.
Pruebas y Métodos de auditoría	' Se debe sintonizar las pruebas con el sistema. ' Los métodos modernos pueden ser inapropiados. ' El equipo puede ser susceptible a fallas durante la prueba.
Administración de cambios	' Programación estratégica. ' El proceso no es trivial debido al impacto en la producción
Clasificación de activos	' Solo se realiza cuando está obligado ' Inventarios precisos son poco comunes para activos no vitales ' Hay desconexión entre el valor de los activos y contramedidas apropiadas.
Respuesta al incidente y análisis forense	' Está centrada en las actividades de reanudación del sistema. ' Procedimientos forenses inmaduros (más allá del evento recreación). ' Se requiere buenas de relaciones entre TI y ICS.
Seguridad Física y Ambiental	' Por lo general, es excelente para áreas críticas, pero la madurez varía para las instalaciones del sitio según la criticidad y la cultura.
Desarrollo de Sistemas seguros	' Históricamente no es una parte integral del proceso de desarrollo. ' Los proveedores están madurando pero a un ritmo más lento que el de TI. ' Soluciones ICS centrales o emblemáticas son difíciles de actualizar con seguridad.
Cumplimiento de Seguridad	' La orientación regulatoria es específica según el sector.



EL TRABAJO DE **IoTSI EN CHILE**

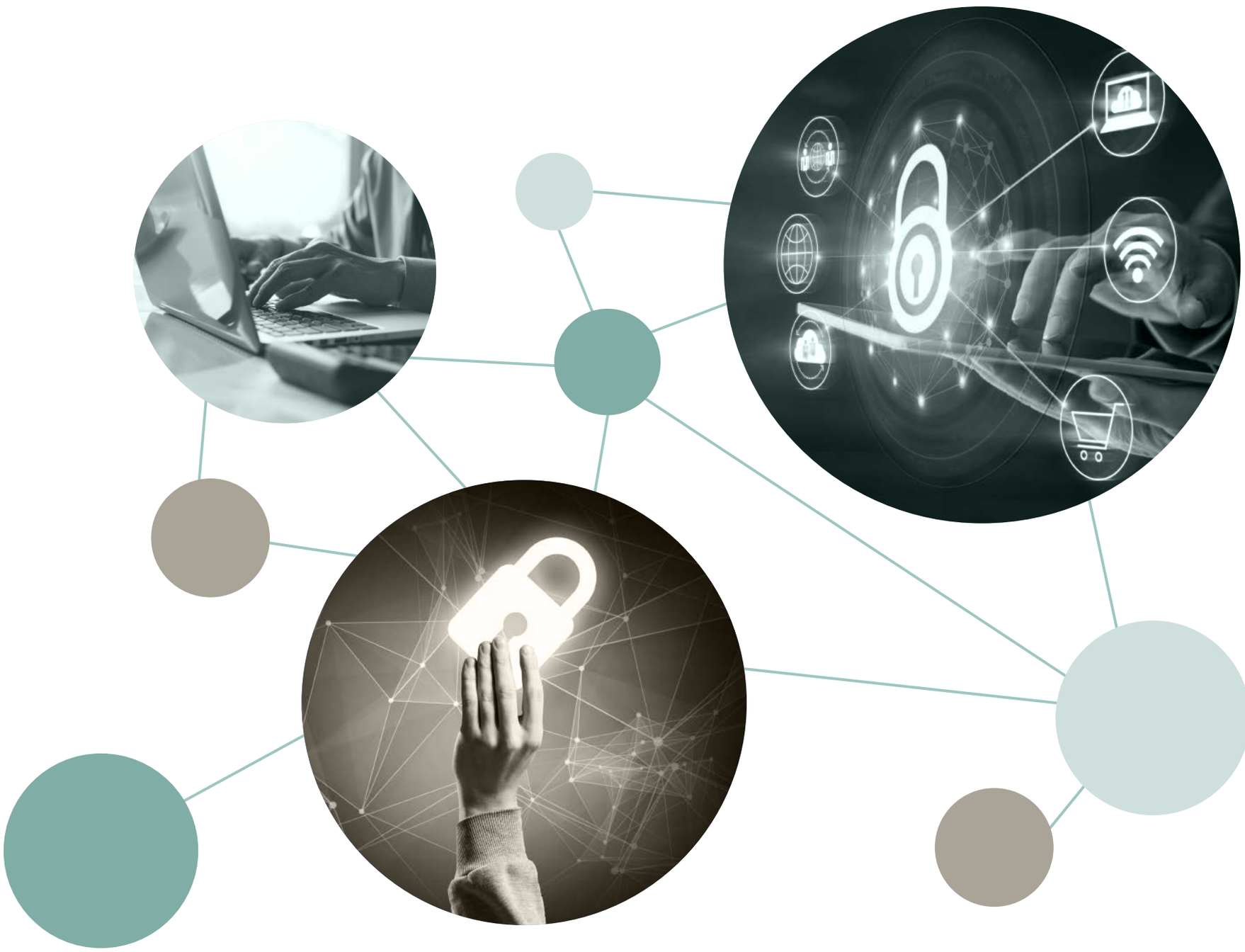
Finalmente, Freddy Macho explica que: "el IoTSI es un organismo académico e industrial dedicado a proporcionar marcos de referencia, servicios calificados y desarrollo educativo para evaluar, gestionar y resguardar la ciberseguridad dentro de los ecosistemas de IoT, IIoT y los ambientes hiperconvergentes".

El especialista resalta asimismo que el IoTSI es el único organismo que entrega una certificación profesional con foco en el diseño e implementación de la ciberseguridad en ciudades inteligentes e infraestructura crítica, conocida como SCCISP. "El IoTSI tiene presencia en más de 25 países, y en Chile cuenta con más de 1.100 miembros en todo el país", añade Macho.

- La presentación del primer documento de trabajo para Chile y la región con las principales definiciones relacionadas con la ciberseguridad en ambientes hiperconvergentes IoT e IIoT.

- El desarrollo del primer diplomado de Ciberseguridad Industrial de Chile.

- La creación de la mesa de trabajo del Comité de Ciberseguridad de la OEA, centrada en ambientes hiperconvergentes IoT e IIoT.



NORMAS AL SERVICIO DE LA CIBERSEGURIDAD INDUSTRIAL

Este año 2021 ha sido la mayor prueba de ciberseguridad industrial de la historia. Muchas empresas ya están disfrutando de los frutos de la conexión de una mayor cantidad de dispositivos a internet y de la convergencia de la tecnología operativa u OT bajo la gestión de los sistemas de TI. Sin embargo, ese impulso también ha sido un atractivo para los ciberdelincuentes, en particular aquellos cuyo empleo es la extorsión y el lucro mal habido. Los activos de numerosas instituciones están expuestos en línea en un número récord, y junto con ellos, todos sus defectos: vulnerabilidades sin parches, credenciales sin protección, configuraciones débiles y el uso de protocolos industriales obsoletos.

En los primeros seis meses del año, toda esta combinación de factores conspiró para traernos ataques de ransomware en el sector industrial de alta notoriedad, como lo fueron los casos de los oleoductos de la firma Colonial Pipeline y el gigante de distribución de carne JBS en Estados Unidos, así como la intrusión en una planta de tratamiento en el estado de Florida con el fin de envenenar el agua que entrega a la población.

Aquella situación de vulnerabilidad cibernética del sector industrial no se aleja mucho de lo sucedido en Chile entre 2020 y 2021, periodo en el que como CSIRT de Gobierno hemos tenido que lidiar con ataques cibernéticos emblemáticos a instituciones tanto públicas como privadas en sectores críticos para el país, como el financiero, alimenticio, forestal, energético y de salud.

La relevancia de estos últimos ataques cibernéticos no solo radica en las pérdidas económicas directas producidas por estos, sino que también por el hecho de haber logrado, en muchos casos, la interrupción en la prestación del servicio, afectando el normal desarrollo de la vida de los ciudadanos del país.

Es así como, en un contexto donde la transformación digital y la industria 4.0 son protagonistas de la modernización de las instituciones, la tendencia es a que los ciberataques al sector industrial sigan proliferando, y cabe esperar que tendrán cada vez mayores y perniciosas consecuencias

Conscientes de este problema resulta urgente fijar lineamientos con el objeto de prevenir el éxito de este tipo de ataques, hemos trabajado con los reguladores sectoriales de salud, energía, aguas y otros en el desarrollo de normas estándar de ciberseguridad con una base común para sus regulados, a fin de aumentar sus exigencias en esta materia.

Legal

UN NUEVO ESTÁNDAR **DE CIBERSEGURIDAD**

A partir de las directrices establecidas por el CSIRT de Gobierno en materia de ciberseguridad, la norma estándar que es trabajada en conjunto y dictada por cada uno de los reguladores tiene por objeto establecer lineamientos mínimos a cumplir por las instituciones reguladas para la gestión de la ciberseguridad.

En ese sentido, la norma tiene dos pilares fundamentales que son transversales: el establecimiento de medidas técnicas y de organización, así como también de medidas de comunicación y reporte de ciberincidentes. Las primeras buscan identificar tanto el análisis de impacto operacional como los riesgos y controles mitigantes, así como la gestión del ciclo de vida de un ciberincidente, considerando la prevención, detección, análisis, notificación, contención, erradicación, respuesta, recuperación y documentación a su respecto.

En tanto que con las segundas se busca instruir sobre los reportes de ciberincidentes que las instituciones reguladas deben enviar a su regulador o fiscalizador para establecer las acciones orientadas a mitigar sus efectos e impactos y contribuir a una oportuna normalización y estabilización de los servicios afectados.

PRINCIPAL CONTENIDO **DE LA NORMA**

Los pilares de la norma se desarrollan mediante el establecimiento de distintas obligaciones, entre las principales se encuentran:

DEFINICIONES: Con el fin de estandarizar conceptos y procedimientos propiciando el uso de un lenguaje común en la materia, el estándar establece definiciones ampliamente aceptadas nacional e internacionalmente.

OBLIGACIONES GENERALES DE CIBERSEGURIDAD: Se establecen obligaciones generales de ciberseguridad aplicables a todos los regulados, tales como medidas de gestión, seguridad por diseño y planes de gestión de riesgo.

UNIDADES DE CIBERSEGURIDAD: Cada una con las competencias suficientes para velar por la observancia de las obligaciones del estándar, identificar los riesgos de afectación de los servicios por causa de ciberincidentes, verificar el cumplimiento eficaz de los respectivos planes de gestión, reportar los ciberincidentes y coordinar la gestión de ciberseguridad en general.

REPORTE OBLIGATORIO DE CIBERINCIDENTES: Se establece la obligación para los regulados de reportar a la Superintendencia, y en caso de estimarlo necesario al CSIRT de Gobierno, acerca de todos los ciberincidentes que alcancen los niveles de peligrosidad e impacto establecidos en la norma, los que van desde un nivel Bajo a Crítico.

PROTOCOLO DE COMUNICACIÓN: Se establece la obligación para todo regulado de cumplir con el estándar internacional "Traffic Light Protocol" o TLP para el intercambio de información en el reporte de ciberincidentes.

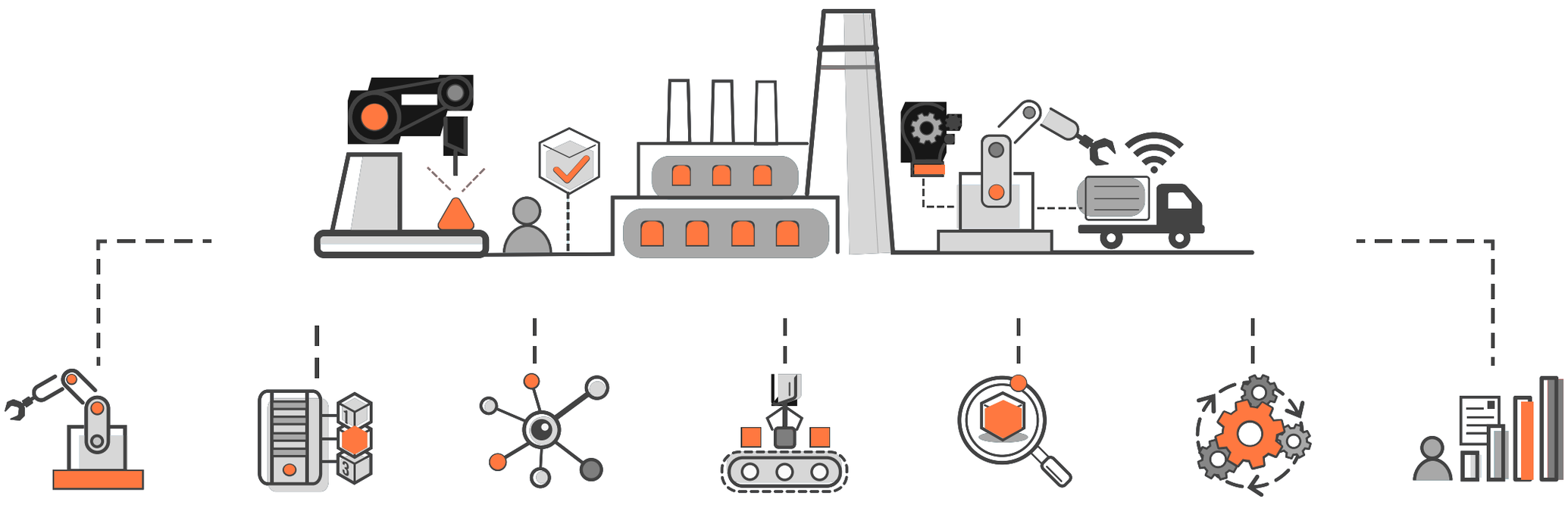
OBLIGACIÓN DE RESOLUCIÓN DE CIBERINCIDENTES: Detectado un ciberincidente, el regulado deberá efectuar todas las gestiones necesarias para su resolución en base a su plan de gestión de riesgo, priorizando aquellas que reduzcan el impacto en los clientes.

ANÁLISIS FORENSE: Se recomienda como una mejor práctica que el regulado contrate un análisis forense independiente luego de finalizado un incidente.

OBLIGACIÓN DE DENUNCIAR: El regulado que detecte que sus redes, equipos y sistemas fueron utilizados para la comisión de un delito informático, y de estimarlo necesario, deberá propender a formular las denuncias ante los órganos competentes y ejercer las acciones judiciales pertinentes.

OBLIGACIÓN DE SUPERVICIÓN DE CIBERSEGURIDAD: Se establece la obligación para los regulados de someter (según la regularidad señalada en su plan de gestión de riesgo) sus redes, equipos y sistemas a pruebas y simulacros de ciberseguridad.

ESTANDAR DE NOTIFICACIÓN: Se establece un marco de referencia en el ámbito de la notificación y gestión de incidentes de ciberseguridad. Esto incluye la definición de una serie de criterios mínimos exigibles y de obligaciones de reporte.



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

CSIRT
https://www.csirt.gob.cl/

Teatinos 92 piso 6
Santiago, Chile

CONTÁCTANOS

+(562) 2486 3850

registra un incidente

Síguenos

Twitter de CSIRT
https://twitter.com/csirtgob/

LinkedIn
https://www.linkedin.com/company/csirt-gob/

Youtube
https://www.youtube.com/channel/UCua0E5Jz9V1Rn-VtLHPP4Nw/

Instagram
https://www.instagram.com/csirtgobcl

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

Teatinos 92 piso 6
Santiago, Chile
www.csirt.gob.cl