ASOCIACIÓN REGIONAL DE EMPRESAS DEL SECTOR
PETRÓLEO, GAS Y BIOCOMBUSTIBLES
EN LATINOAMÉRICA Y EL CARIBE.

Ciberseguridad en Infraestructuras Críticas: Riesgos, Oportunidades y Prioridades

Marzo 2019

PUBLICACIÓN ARPEL N° EV01 – 2019

YPF

INFORMES DE EVENTOS

Introducción

El **Seminario Ciberseguridad en Infraestructuras Críticas: Riesgos, Oportunidades y Prioridades**, se llevó a cabo los días 9 y 10 de octubre en Buenos Aires, Argentina, y fue coorganizado por ARPEL, la Organización de los Estados Americanos (OEA) e YPF con el apoyo del Gobierno Argentino a través de la Secretaría de Modernización y del Ministerio de Relaciones Exteriores y Culto.
El mismo se enmarca dentro de una fuerte línea de trabajo en ciberseguridad que mantienen tanto OEA con los Estados como ARPEL con las empresas de petróleo y gas de América Latina y el Caribe.
El Seminario reunió a más de 200 profesionales y expertos provenientes de más de 60 empresas e instituciones de toda Latinoamérica y Caribe. En el mismo se analizó el escenario actual de la ciberseguridad y sus desafíos, la importancia de la regulación como inductor de la preparación y respuesta ante las amenazas, la relevancia de los análisis de riesgos, así como también se presentaron casos exitosos de implementación.

Las principales conclusiones y mensajes del evento se resumen en este informe, con el fin de apoyar a las compañías, principalmente del sector petróleo y gas, a mejorar sus niveles de protección ante los riesgos del ciberespacio.

El escenario actual

El marco actual de los negocios ha variado sustancialmente en los últimos años, entre otros motivos, por la creciente digitalización. Esto ha traído nuevos modelos de negocio, formas de interacción social y también nuevos riesgos que deben ser gestionados. Las tendencias identificadas en el Informe ARPEL "Ciberseguridad – aspecto clave en un mundo interconectado" no solo se fueron confirmando sino que también acelerando. (https://arpel.org/library/publication/473/)

Riesgo que crece aceleradamente…

El marco actual implica una mayor densidad digital, una mayor superficie de exposición ante las ciberamenazas y, a su vez, una mayor complejidad en los tipos de ataque. Por otra parte, se ha identificado la tendencia de que los ciberataques se direccionan cada vez más al OT (tecnologías de operación).

Algunas cifras presentadas durante el Seminario permiten ilustrar estas tendencias:

Según la consultora internacional McKinsey, el internet industrial de las cosas (IIoT) permitirá desplegar a nivel global unos 6.0 trillones de dólares de impacto económico para 2025.

El Foro Económico Mundial (WEF) identificó a la ciberseguridad como uno de los mayores riesgos actuales a nivel global, con impactos potenciales equiparables a los generados por desastres naturales.

Argentina: En 2017 se detectaron 4.1 millones de incidentes, para lo cual se debieron procesar 5.500 millones de eventos.

Colombia: El sector energético recibió 19.583 ataques por día durante 2017 (16% del total), siendo el tercer sector más afectado detrás de telecomunicaciones (26% de los ataques) y el sector financiero (40% de los ataques).

Según información de la Security Incidents Organization, Repository of Industrial Security Incidents (RISI), un 5% de los ciberataques a la industria en EEUU durante el último año resultó en lesiones o fatalidades.

La densidad digital y el internet de las cosas está haciendo que los ataques cibernéticos se lancen desde heladeras, microondas o hasta peceras y otros dispositivos de uso común que se conectan a internet.

…y aún más para el sector de la energía…

A nivel internacional, tres de cada cuatro compañías de petróleo y gas fueron víctimas de ataques cibernéticos frecuentes y sofisticados, además el 80% de las compañías del sector han visto un incremento en el número de ciberataques durante 2017.

Esto se debe a que algunas características propias del sector energético lo convierten en un blanco ideal para ciberataques industriales.

a.

Existen múltiples actores coordinados y el ajuste entre oferta y demanda es instantáneo (lo cual es más notorio en el caso del sector eléctrico).

b.

Un evento en cualquier eslabón de la cadena afecta a todo el resto, y tiene efectos sobre otros sectores.

c.

Los equipos son costosos y difíciles de reemplazar, por lo que su reparación puede llevar meses e implicar millones de dólares.

En el fondo, es una cuestión de dinero…

El móvil último de los ciberataques es la búsqueda de una ganancia económica, por eso los sectores financieros suelen ser los más atacados, pero también sectores como el de la energía cuyos impactos económicos potenciales son muy grandes.

Encontrar vulnerabilidades en OT que permitan extorsionar, realizar un fraude o sabotaje industrial se puede pagar miles de dólares en el mercado negro, por lo que existe un gran incentivo para lograrlo.

Entonces, la ciberseguridad ya no es un riesgo solo tecnológico…

Elizabeth Gurney de Willis Towers Watson destacó la importancia que tiene ampliar la concepción de los ciber-riesgos, ya no solamente como meros riesgos tecnológicos, debido a que tiene potenciales impactos en el mundo físico. En sus palabras expresó que “los ataques en contra de un sistema pueden involucrar solo los componentes cibernéticos y su operación, pero esos impactos pueden extenderse a los sistemas físicos, comerciales, humanos y ambientales a los que están conectados”. Este hecho, sumado a que “no hay límites en el ciberespacio” y su capacidad de combinarse y potenciar otros riesgos, dificulta su gestión, mitigación y cuantificación.

Elizabeth Gurney | Willis Towers Watson

Mensajes clave

Las nuevas tecnologías digitales seguirán desplegando su potencial y teniendo un impacto económico cada vez mayor.

Sin embargo, esta mayor densidad digital trae aparejada una mayor superficie de ataque y riesgos más complejos para las operaciones.

Hay una tendencia creciente a atacar las infraestructuras y el OT.

El sector energético, por sus características, es un blanco deseable para los ciberatacantes.

El beneficio económico es el driver principal de los ciberataques.

El rol de la regulación

El rol y la importancia de la regulación fue discutido en profundidad durante el panel final de cierre del evento. El mismo fue moderado por **Brian O'Durnin** (YPF) e integrado por **Gabriel Faifman** (BHGE), **Maximilian Kon** (Director General de Wiseplant), **Diego Zuluaga** (ISAGEN), **Claudio Caracciolo** (Eleven Paths) y **Jeimy Cano** (Universidad del Rosario).

El primer punto destacado es que la regulación de la ciberseguridad está aún en un nivel muy incipiente, tanto a nivel internacional como regional, aunque en mayor o menor medida todos los países están avanzando en esa dirección. Sí existen avances más importantes a nivel de estándares técnicos, que sirven como base para las regulaciones.

La regulación establece las expectativas mínimas aceptables para las compañías, por lo cual su existencia es siempre un inductor para movilizar a la acción. En palabras de **Diego Zuluaga** (ISAGEN) "la regulación ayuda a agilizar procesos, a dispararlos y desplegarlos"

Diego Zuluaga | ISAGEN

Si bien se reconoció a la regulación como driver necesario para impulsar la ciberseguridad y dar un marco claro de acción, también se puso énfasis en que la misma no es por sí sola suficiente. En tal sentido, **Maximillian Kon** (Wiseplant) planteó que "la regulación sirve porque habilita cosas, pero no alcanza solo con eso, lo importante es querer hacer las cosas bien". En la misma línea se pronunció Diego Zuluaga (ISAGEN) respecto a la experiencia de la regulación colombiana y la importancia del cambio cultural para que se mejoren los niveles de preparación y respuesta, más allá de la regulación.

A su vez, las características de los ciber-riesgos, implican el mencionado cambio cultural y la necesidad de trabajar en comunidad entre todos los sectores para hacer frente contra los riesgos. Más allá de que la capacidad de coerción de los reguladores, se destacó que es importante poder superar la cultura de actuar simplemente por evitar los castigos y pasar a una cultura proactiva y colaborativa entre los actores.

Maximillian Kon | Wiseplant

Jeimy Cano | Universidad del Rosario

Claudio Caracciolo | Eleven Paths

Por otra parte, la regulación de infraestructuras críticas es naturalmente un asunto complejo y que involucra a muchos actores y a la sociedad en general desde el punto de vista de las consecuencias potenciales, por lo que no se puede esperar a tener una regulación para comenzar a evaluar e implementar la ciberseguridad.

En palabras de **Jeimy Cano** (Universidad del Rosario): "Se debe formar la comunidad y construir propuestas que permitan cambiar las cosas, influenciar a quienes tomen las decisiones (…) construir una regulación entre las partes interesadas, dirigido por el gobierno es el modelo ideal, pero estar organizados en comunidad es lo que permite tener un mejor diálogo".

Diego Zuluaga (ISAGEN) por su parte añadió que "la regulación va a llegar", por lo que es mejor estar preparados desde antes y que esto facilite la implementación de los programas.

En cuanto al cambio cultural, **Claudio Caracciolo** (Eleven Paths) destacó que es fundamental que se incluyan los temas de ciberseguridad en los cursos universitarios de grado y posgrado, que esto ya está empezando a suceder en Argentina y que precisamente éste es un gran logro de la comunidad.

Por último, se conversó sobre cómo poder influenciar a los tomadores de decisión y reguladores (los dueños de los riesgos). En este sentido, **Gabriel Faifman** (BHGE) destacó que las áreas de IT deben estar más involucradas en el negocio para tener una mayor capacidad de influencia, que ya no se las puede considerar como proveedores de servicios dentro de la compañía, sino que son también generadores de valor.

Gabriel Faifman | BHGE

En la misma línea, **Jeimy Cano** (Universidad del Rosario) destacó que hay dos preguntas que las áreas de IT deben poder contestar a los directivos, pero que pocas veces lo logran hacer de manera eficaz:

- ¿Qué va a cambiar?
- ¿Cuál es el modelo de valor de la compañía?

Mensajes clave

La regulación es un driver necesario para inducir las acciones pero no suficiente para establecer una defensa eficaz y resiliente contra los ciber-riesgos.

Crear regulaciones es complejo y vale la pena el esfuerzo, pero se debe formar comunidad entre las partes interesadas para poder mejorar la resiliencia y facilitar los acuerdos y procesos del regulador.

Para ser más influyentes, las áreas de IT deben involucrarse más en el negocio de las compañías, percibirse como un generador de valor y no un proveedor de servicios.

Implementación de los programas de ciberseguridad

Si bien es claro que los ciber-riesgos avanzan rápidamente, la implementación de los sistemas de ciberseguridad para proteger las instalaciones lo hace a un ritmo más lento.

Lucas Siniscalco de ABB Argentina planteó claramente este escenario dual “La nueva disponibilidad de grandes cantidades de datos, junto con las herramientas estadísticas para reducir estos números, ofrece una forma completamente nueva de entender el mundo. La correlación reemplaza la causalidad, y la ciencia puede avanzar incluso sin modelos coherentes, teorías unificadas, o realmente ninguna explicación mecanicista en absoluto”. (Anderson, 2008). Asimismo, enfatizó que hoy en día “tenemos capacidad para hacer análisis de esa información (la que envían los sensores, dispositivos, etc.), pero no tenemos lo principal, es decir, asegurada la instalación”.

Lucas Siniscalco | ABB Argentina

I. El enfoque de la resiliencia

"Resiliencia es planificar cómo prevenir, cómo remediar y cómo recuperarnos después del ataque (…) hay que enfrentar los problemas, este problema es ubicuo".
Mariano Cuadrelli | HONEYWELL

Jeimy Cano (Universidad del Rosario) presentó el enfoque de la resiliencia, como la nueva forma de abordar los ciber-riesgos.

En su visión, el nuevo entorno es volátil, incierto, complejo y ambiguo, y que este es un gran cambio en términos del ecosistema de seguridad.

Además añadió que los saberes están segmentados, por lo que se debe pensar en las prácticas que nos permiten reducir la incertidumbre y generar las capacidades que permitan defender y anticipar.

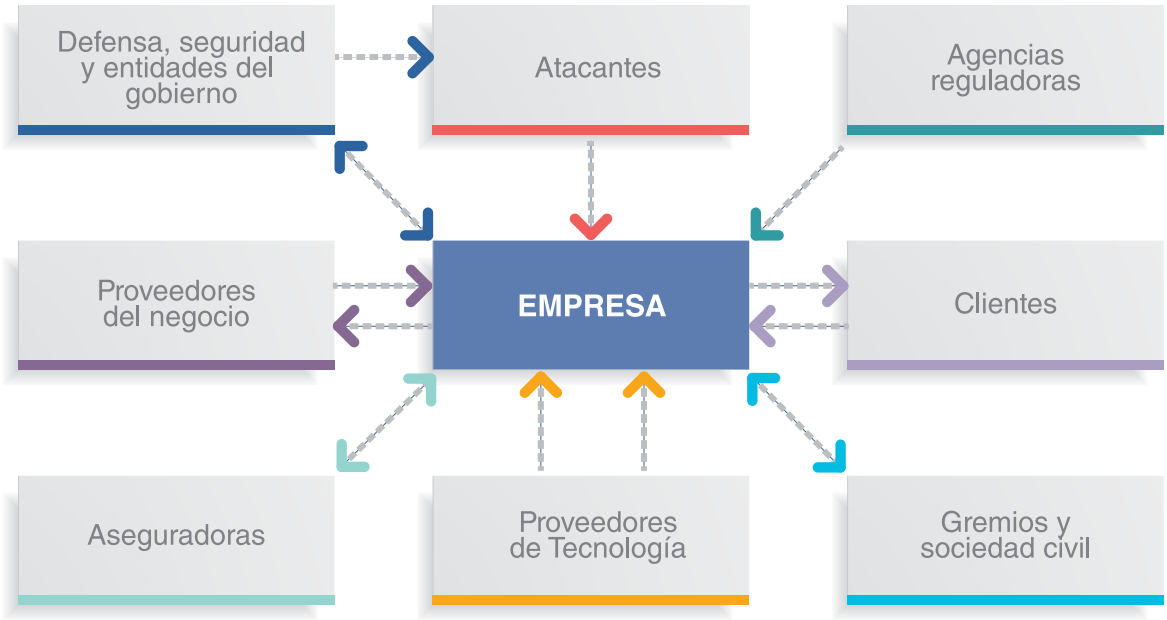
"El ciber riesgo es sistémico y por eso es tan complicado, la conectividad incrementa la superficie de ataque, existen tensiones geo-info-políticas, es sensible al contexto y está supeditado a la convergencia tecnológica (…) Asimetría de la información disponible, vulnerabilidades inciertas y emergentes e impactos difícilmente predecibles o cuantificables".

Puso su énfasis en que el enfoque safety/security debe ser integrado y que se debe lograr que el sistema siga operando a pesar de los ataques, es decir, se debe apuntar a la RESILIENCIA del negocio, lo cual es muy distinto al concepto de continuidad.

Para lograrlo, se deben crear capacidades colectivas, más allá de los saberes especializados, y tener nuevos normales. Además, recordó que "los criminales sí que saben trabajar en equipo".

“La ciberseguridad no es un tema técnico o táctico. Es un imperativo estratégico que navega en el presente, aprendiendo del futuro”, según dijo el experto.

Cano también destacó que las empresas forman parte de un ecosistema de ciberseguridad empresarial, en el que se debe entender cada relación y cómo puede ser implicada y afectar a los demás eslabones.



II. Grado de Madurez

Compromiso, Conocimiento de los riesgos, sentido de la vulnerabilidad y Conciencia de los impactos potenciales fueron las características deseables de una Junta Directiva identificadas por la audiencia en una breve encuesta interactiva realizada durante la presentación de Jeimy Cano.

Julio Ardita | CYBSEC / Deloitte

Varios presentadores mostraron los grados de madurez de la industria respecto a los ciber riesgos:

Mariano Cuadrelli (HONEYWELL) por su parte, presentó un esquema que evalúa entre 0 y 5 los niveles de madurez y manifestó que, en general, las empresas se encuentran todavía en un nivel 1 (seguridad ad-hoc), es decir, un esquema aún reactivo.

Julio Ardita (CYBSEC / Deloitte), en un esquema similar, planteó en base a un estudio de Deloitte que a nivel global se estima que la madurez de la industria de petróleo y gas está en un promedio de 2,2 (ad-hoc con sistematización incipiente); mientras que se tendría que apuntar a tener como mínimo un nivel 4 (gestionada sistemáticamente) .

Cyber Security
Three guiding principles

1.
Reality

There is no such thing as 100% or absolute security

2.
Process

Cyber security is not destination but an envolving target - it is not a product but a process

3.
Balance

Cyber security is about finding the richt balance - risk reduction vs investments needed

III. Los análisis de riesgos

> "El primer paso para todo es generar un análisis de riesgos, entender las vulnerabilidades, qué superficie exponemos y qué tan permeables somos".
> **Óscar Morotti** | Ministerio de Modernización de Argentina

El estudio de benchmarking realizado por el Centro de Ciberseguridad Industrial detectó que en empresas industriales de Latinoamérica, solamente el 30% ha realizado análisis de riesgos en sistemas de automatización y control, 45% no cuenta con un sistema de gestión de incidentes y un 18% no tienen una adecuada segmentación de redes, lo cual es un riesgo mayor ya que los ataques al OT suelen comenzar por brechas en las redes de IT.

Gonzalo García | Fortinet

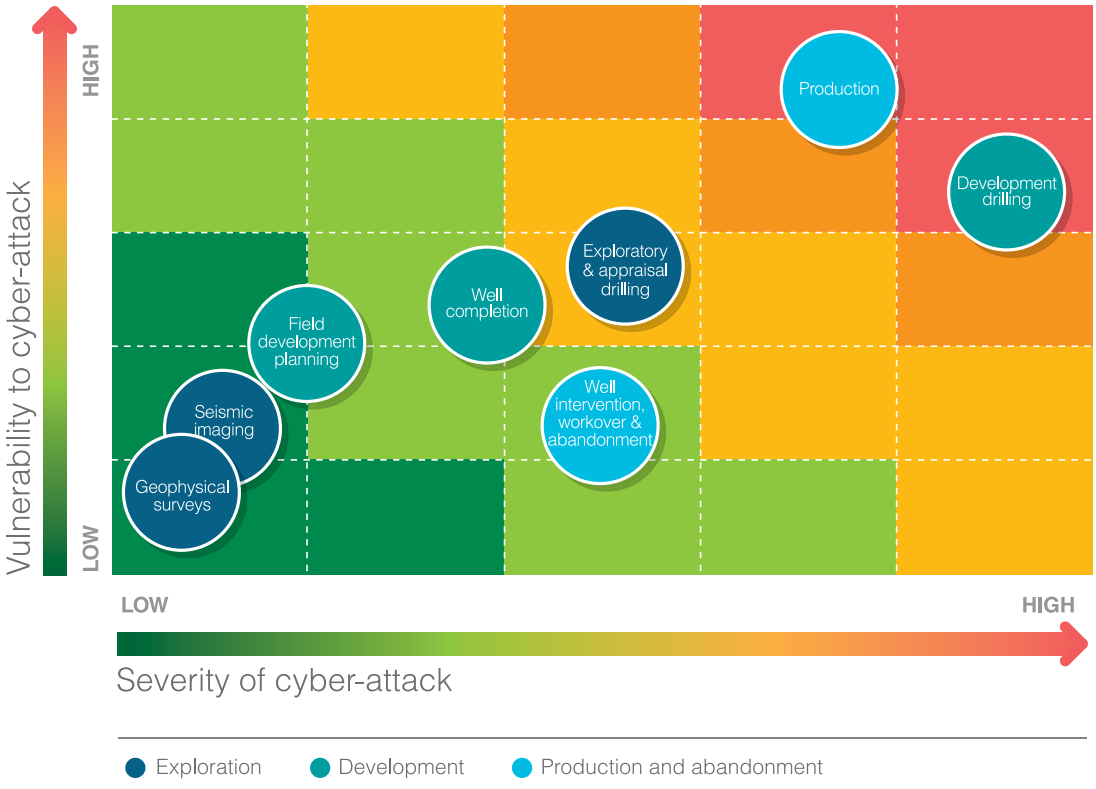
Respecto a este último punto, **Gonzalo García** (Fortinet) mencionó que "el 90% de los ataques dirigidos con amenazas persistentes avanzadas vienen a través de correo electrónico porque es la forma más fácil de que alguien ejecute algo en una computadora" y que "lo normal es que los ataques sean por etapas, van madurando de a poco, no se entra con el tanque, se entra con legos y se arma el tanque adentro".

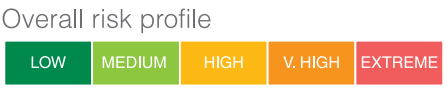
Por su parte, **Mariano Cuadrelli** (Honeywell) añadió que desde su experiencia en más de 30 ejercicios de assessment realizados en Latinoamérica, detectaron brechas en el 100% de los sistemas anti-malware, encontrando muestras de malware en el 20% de los casos. Además, un 83% mostraron deficiencias en seguridad física, 86% de los equipos evaluados mostraron alta vulnerabilidad, 62% de sistemas operativos estaban obsoletos y el 49% de firmwares evidenció vulnerabilidades.

Julio Ardita (Cybseg/Deloitte) mostró cuáles son los principales riesgos identificados en la industria de petróleo y gas, tanto para upstream como para downstream, basados en un estudio de Deloitte (https://www2.deloitte.com/cl/es/pages/risk/articles/cyber-risk-energy.html)

Upstream

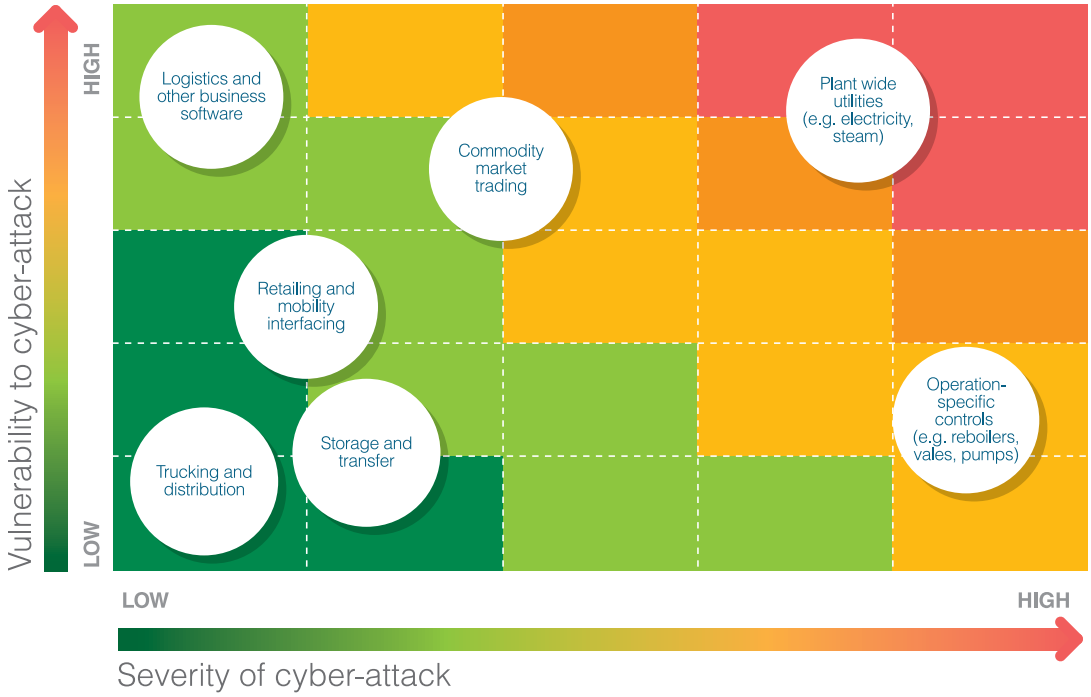
Producción y perforaciones de desarrollo fueron los riesgos identificados como de mayor impacto y vulnerabilidad.





Downstream

En el caso del downstream, los servicios auxiliares (energía, agua, vapor, etc.) fueron identificados como los de mayor vulnerabilidad e impacto.



Ardita además detalló cuáles son los pasos para realizar una correcta evaluación de los riesgos a los cuáles está expuesta una compañía:

i. Conformar un equipo multidisciplinario que inlcuya al negocio, al área de operaciones y a las de seguridad informática.

ii. Realizar un inventario de activo de OT lo más profundo posible

iii. Hacer un ranking por criticidad

iv. Evaluar los controles clave y evaluar la madurez de los mismos

v. Desarrollar un plan de aseguramiento sobre los activos de OT en función de los hallazgos.

Mateo Martínez | KOD

Mateo Martínez (KOD) expresó que las evaluaciones de riesgos se deben pensar desde las amenazas, modelar los escenarios y enfatizó el concepto de "porosidad de las redes", poniendo el foco desde los potenciales puntos de entrada. Durante el Seminario se destacó también la utilidad de algunas metodologías no tradicionales (ej. Hackaton / War Games) para detectar precisamente esas vulnerabilidades.

GOVERNANCE		SECURE		VIGILANT		RESILIENT	
Cyber Security Management	Rick Management & Compliance	Information Protection	Information Lifecycle Management	Threat Management	Cyber Attack Readness Testing	Incident Management	Security Incident Response
	Policies & Standards		Encryption	Security Analytics	Security Event Monitoring		Business Continuity Management
	Training & Awareness	Identity & Access Management	Authentication				
	Vendor Management		Roles & Richts Management				
			Identify Lifecycle Management				
		Infrastrucure Protection	Network Security				
			Physical Security				
			System Security				
			Patch & Vulnerability				
			Malware Protection				

IV. Implementación de la ciberseguridad

> "No existen soluciones mágicas, la seguridad es una cuestión de madurez y requiere tiempo y trabajo".
> **Lucas Siniscalco** | ABB

Uno de los grandes problemas que está enfrentando la parte industrial es que la mayoría de los planes de ciberseguridad son de mediano y largo plazo, ya que rediseñar una red requiere tiempo y hay respuestas y mejoras que se deben realizar en el corto plazo.

Lucas Siniscalco (ABB) expresó que existen tres pilares en la implementación de un programa de ciberseguridad: las personas, los procesos y las tecnologías. Los tres son interdependientes y se deben atacar al mismo tiempo, ya que si la madurez de uno de estos pilares queda rezagada, esto generará una brecha importante a nivel de ciberseguridad sin importar qué tan maduros estén los demás.

Diego Zuluaga (ISAGEN) por su parte, puso énfasis en la dimensión humana y en la necesidad de generar hábitos seguros, para lo cual es necesario tener en cuenta tres elementos:

- Conocer los riesgos (conocimiento)
- Saber qué y cómo enfrentarlos (habilidad)
- Tener voluntad de hacerlo (deseo)

Expresó que el hábito es la intersección entre el conocimiento, la habilidad y el deseo. Este último punto es el que marcó como crítico ya que "el adulto no aprende lo que no le interesa y le interesa solo lo que es necesario para su vida".

Los programas de auditoría y generar un adecuado control es un factor importante ya que genera disciplina, pero es mucho más importante que las personas incorporen los buenos hábitos. Esto no es una tarea sencilla debido a que siempre existe resistencia al cambio, pero también existen personas que participan de manera entusiasta de estos procesos y logran un efecto multiplicador.

La gobernanza y la seguridad en el diseño también se identificaron como dos aspectos clave para lograr una buena protección contra las ciber-amenazas.

Por su parte, **Carlos Buenaño** (Cytric Solutions) expresó que visibilizar las redes, priorizar su segmentación, expandir las reglas al OT y educar operadores, ejecutivos y directivos fueron también algunas de las recomendaciones brindadas durante el Seminario.

Por último, se manifestó que en muchos aspectos la ciber-seguridad no siempre es algo tan sofisticado, sino que se debe comenzar con lo básico y que es un proceso de mejora y madurez continua en el que se va creciendo paso a paso.

Diego Zuluaga | ISAGEN

Carlos Buenaño | Cytric Solutions

Seguridad en el diseño, la clave

> "No es la convergencia de IT/OT, es la convergencia de todo el negocio, no es un camino o una opción, es el único camino posible".
> **Gabriel Faifman** | BHGE

Maximillian Kon | Wiseplant

Maximillian Kon (Wiseplant) destacó que "en el ambiente industrial, la seguridad y la ciberseguridad dependen del diseño".

Por su parte, **Claudio Caracciolo** (Eleven Paths) en su charla "IIoT no tiene por qué ser un problema, aunque a veces lo es…" destacó que uno de los problemas es precisamente que los requeriemientos de ciberseguridad a la hora de adquirir equipos y tecnologías suele ser bajo o inexistente, y que este es un aspecto a mejorar, se debe ser mucho más exigente en los requerimientos para asegurar la instalación desde el diseño.

Sin embargo, claro está que la seguridad en el diseño puede pensarse para tecnología nueva que traiga certificaciones desde fábrica, aunque para tecnologías ya instaladas, con las características intrínsecas del OT, el enfoque debe ser adaptativo. Sin perjuicio de lo anterior, también se manifestó durante el Seminario la existencia de casos en los que los equipos venían modificados de fábrica.

Claudio Caracciolo | Eleven Paths

	Traditional IT	Industrial IOT
What is being Protected	Data	Physical Process
Impact Area	Disclosure of information; Financial loss	Safety, Availabity, Financial, Environment
Security Objective	Confidentiality, Privacy	Availability, Integrity
Operating Systemas	Windows, Linux	Windows at HMI, RTOS at field devices
Availability Requirements	99%	99,9% - 99,999% (downtime pero year: 8,76 hours to 26 min)
System Lifetime	3 - 10 years	5 - 25 years
Logging and forensics	Standard practice	Limited
Patching	Standard schedule; can be expedited	Non-satndard; could be a long time between updates

Gabriela Reynaga | ISACA

La importancia de las auditorías

Gabriela Reynaga (ISACA) durante su charla "Orden dada y no supervisada, no sirve para nada" destacó la importancia de las auditorías para identificar las brechas y puntos de mejora en el proceso de la ciberseguridad y de generar empresas resilientes contra las ciber-amenazas.

Manifestó que suele existir resistencia para la realización de auditorías y que las mismas se realizan, en general, cuando existe una obligación legal de hacerlo. Expresó además que las auditorías más exitosas suelen ser las que se realizan de forma proactiva ya que se le da mayor seguimiento a los hallazgos. Propuso a las auditorías externas como la "4ª línea de defensa" (Gestión Operativa, la Gestión del Riesgo y Funciones de Cumplimiento, Auditoría Interna: https://www.auditool.org/blog/control-interno/1850-sistema-tres-lineas-de-defensa-en-gestion-de-riesgos-y-control), que el gobierno corporativo de la compañía es quien debe liderar el proceso para apalancar los cambios y cerrar las brechas halladas en las auditorías y que, el factor más crítico y vulnerable no son ni los procesos ni las infraestructruras, sino que son las personas.

Las auditorías son útiles, pero deben realizarse no simplemente por el compliance, sino por querer hacer las cosas bien.

Los mercados de seguros

Elizabeth Gurney (WTW) planteó que hoy en día los grandes aseguradores ofrecen productos para lograr cuantificar y poner un precio a los ciber-riesgos. En general se ofrecen pólizas independientes de las pólizas tradicionales que abordan específicamente los ciber-riesgos.

Por otra parte, **Sergio Torres** (AON) planteó algunas estadísticas sobre el dinamismo del mercado de ciber-seguros, lo que pone en evidencia el riesgo creciente y las necesidades de cobertura.

En su presentación planteó que la prima bruta global de ciber-seguros asciende hoy a los 3 mil millones de dólares y que se espera que se multiplique por seis en los próximos 5 años, que el 80% de las empresas Fortune 1000 compran una póliza para cubrirse de los ciber-riesgos y que se espera que el costo de la ciberdelincuencia para la economía mundial alcance los 6 mil trillones de dólares al 2027. (https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/).

El mercado de los ciber-seguros está en pleno desarrollo y aún tiene mucho camino por recorrer, tanto en cuanto a definiciones como en tipos de cobertura y el abordaje de los riesgos. En tal sentido, y como evidencia de la inmadurez del mercado, se planteó durante el Seminario que para que la madurez de las empresas en cuanto a la gestión de los ciber-riesgos se vea reflejada en las primas de riesgos, aún se necesita una mayor competencia y liquidez en el mercado.

Sergio Torres | AON

¿Por qué fallan las compañías?

> "En general, las organizaciones fallan por tres motivos: no conocen los estándares, no los implementan bien o la alta dirección no considera los riesgos de ciberseguridad como parte de los riesgos del negocio".
> **Maximillian Kon** | Wiseplant

Sí se puede!...
Dos casos exitosos de implementación: COGA y YPF

En cuanto a la implementación, **Neptalí Mayorga y Ernesto Landa** (COGA) mostraron las claves para lograr los exitosos avances alcanzados por COGA en la materia.

El gatillo fue que el Análisis FODA corporativo comenzó a incluir los riesgos de ciberseguridad a partir de 2014, por lo que pasó a ser un asunto estratégico de la gestión.

Neptalí Mayorga | COGA

Por otra parte, destacó que el respaldo se ve en los presupuestos y en los recursos destinados y no en los papeles y en las políticas. Destacó además que tuvieron un respaldo consistente en su empresa para llevar adelante los programas de ciberseguridad.

Ernesto Landa | COGA

También expresó que más importante que las políticas, es cómo se están realizando las tareas en campo. En sus palabras: “Más que preocuparnos por redactar, implantar una política, se necesita establecer un sistema de control que nos permita ver que las buenas prácticas se están cumpliendo”.

Brian O’Durnin | YPF

Gerardo González | YPF

La experiencia de YPF fue presentada por **Brian O’Durnin y Gerardo González** (YPF). El punto de inflexión se dio a partir de 2015, cuando el CEO de la compañía tuvo que firmar el reporte 20F (exigido por la NYSE) y ante la necesidad identificada de avanzar en el tema, se convirtió en el principal spónsor e impulsor de la ciberseguridad. También fue importante el apoyo recibido desde las áreas de seguros, ya que esto afecta a las primas pagadas por la compañía.

Fue así que se logró desarrollar la norma, basada en los estándares ISA99-IEC62443. La misma fue relativametne genérica dada la diversidad de negocios de la compañía y se otorgó un plazo de un año y medio para implementar las mejoras propuestas. Éste fue identificado como un gran desafío ya que desde que existe una norma la misma pasa a ser materia auditable.

Reconocieron que para la implementación se tuvieron que romper algunas barreras, en particular se debió entender que el área de IT tiene que formar parte del negocio y no actuar como un agente externo que brinda recomendaciones.

La norma estableció 3 fases de implementación: Evaluación, implementación propiamente dicha y mantenimiento y mejora continua. Actualmente se encuentra en la fase 2.

Carlos Buenaño (Cytric Solutions) planteó que las 5 primeras observaciones que surgen de las implementaciones en campo son:

- Dispositivos no actualizados
- Comunicaciones externas comprometidas
- Protocolos inseguros
- Operaciones de escritura anormales
- Puertos abiertos

Mensajes clave

Los ciber-riesgos son sistémicos y complejos en su abordaje y deben considerarse como una cuestión estratégica y un riesgo para el negocio y gestionarlos como tales, con el apoyo explícito de la Junta Directiva y la asignación de recursos correspondiente.

La ciberseguridad se debe entender como un proceso evolutivo, de aprendizaje constante, en el que el objetivo debe ser la madurez.

La contrapartida de lo anterior es que las áreas de IT deben reconocerse como áreas que agregan valor al negocio y no ya como un proveedor de servicios para otras áreas.

El enfoque actual es el de resiliencia empresarial dentro de un ecosistema de ciberseguridad, que es un concepto mucho más amplio que el de continuidad del negocio.

Conclusiones

Nuevo escenario, riesgos crecientes y en aceleración, digitalización, industria 4.0, etc.

La tendencia hacia la digitalización, que incluye una mayor conectividad y la Internet de las Cosas (IoT, por sus siglas en inglés), está creciendo entre las organizaciones industriales, como es el caso de las centrales eléctricas, las fábricas y los centros de tratamiento de agua, que dependen de los sistemas de control industrial (ICS) para sus operaciones. Es una tendencia que viene con reconocidos peligros de ciberseguridad: el 65% de las empresas cree que los riesgos de seguridad de los ICS son más probables con la IoT. La convergencia de la IT y la OT (tecnología operativa), la mayor conectividad de OT con redes externas y el creciente número de dispositivos de IoT industrial, están ayudando a aumentar la eficiencia de los procesos industriales. Sin embargo, estas tendencias generan riesgos y puntos de vulnerabilidad cada vez mayores, lo que hace que las organizaciones industriales se sientan inseguras: más del 77% de las empresas cree que su organización se convertirá en el blanco de un incidente de ciberseguridad que involucra a sus redes de control industrial.

Trabajar para hacer frente a las ciberamenazas, se debe poner el foco en las personas y en hacer las cosas en forma correcta, en generar comunidad, en desarrollar la regulación y el cambio cultural

Realizar formación para los empleados sobre seguridad. Siempre hemos dado mucha importancia a la formación y capacitación de los empleados, y en temas de seguridad no podía ser diferente. Los empleados deberán recibir la formación necesaria para no cometer errores en la seguridad.

Establecer políticas, normativas y procedimientos de seguridad. La incorporación de un nuevo empleado es el momento ideal para indicar qué puede hacer y qué no puede hacer con el mail, el acceso a Internet, etcétera. Incluso, si hay sanciones por incumplimiento de las normas, es momento de indicarlas.

Supervisar que se cumplen las buenas prácticas en seguridad. Como en todo plan, la supervisión es imprescindible para corregir errores que se puedan estar realizando e implementar mejoras.

Realizar acciones de sensibilización y concienciación en seguridad. Más allá de las formaciones, se propone la realización de acciones dinámicas y entretenidas para que la concienciación sobre la seguridad de la empresa sea efectiva.

La ciberseguridad es una cuestión de madurez, un proceso continuo, existen herramientas y conocimientos

La Ciberseguridad no es un estado, es un proceso continuo que involucra a toda la organización. Si bien no existe seguridad absoluta, los ejecutivos de las empresas, incluyendo los comités directivos y de auditoría, deben comprender el concepto de ciberseguridad, sus alcances y riesgos asociados al negocio, la importancia de encarar dichos riesgos y las posibles implicaciones de no atender el tema. Es esencial establecer un proceso de sensibilización en toda la organización, indicando claramente los roles y responsabilidades que cada área debe tomar para que el modelo de control sea efectivo.

Avances lentos en la implementación pero en la dirección correcta. Ya existen casos exitosos de implementación de programas de ciberseguridad en la industria de petróleo y gas (COGA y YPF)

La estrategia de seguridad debe definir los resultados esperados y los objetivos por alcanzar, por lo que una vez definidos, el siguiente paso consiste en realizar un análisis de brechas. En esta actividad es necesario conocer el estado actual de seguridad y la postura que se desea alcanzar con la ejecución del programa. Una referencia sobre el estado deseado de la seguridad suelen ser las buenas prácticas de la industria, plasmadas en estándares internacionalmente reconocidos.

CEREMONIA DE APERTURA
Oscar Morotti | Director de Infraestructuras Críticas y Ciberseguridad - Secretaria País Digital - Ministerio de Modernización
Gonzalo García Belenguer | OEA
Brian O´Durnin | Gerente de Seguridad de la Información - YPF
Hernán Vázquez | Gerente de TI - ARPEL

CYBERSECURITY ASSESSMENT EN EL CICLO DE VIDA DE DESARROLLO DE PROYECTOS OPERACIONALES
Disertante:
Mariano Cuadrelli | Gerente de Desarrollo de Negocios para América Latina - HONEYWELL

EVALUACIÓN DE RIESGOS PARA TOMAR BUENAS DECISIONES Y SELECCIONAR TECNOLOGÍAS ADECUADAS PARA LA SEGURIDAD CIBERNÉTICA INDUSTRIAL
Disertante:
Maximilliam Kon | Director General - WisePlant

SOPORTE PARA INFRAESTRUCTURAS CRITICAS Y CIBERSEGURIDAD POR PARTE DEL MINISTERIO DE MODERNIZACIÓN
Disertante:
Oscar Morotti | Director de Infraestructuras Críticas y Ciberseguridad - Secretaria País Digital - Ministerio de Modernización

DETECCIÓN PROACTIVA DE AMENAZAS EN AMBIENTES DE INFRAESTRUCTURAS CRÍTICAS E INDUSTRIALES
Disertante:
Pablo Almada | Gerente Senior, KPMG Argentina KPMG

IMPLEMENTANDO UNA ESTRATEGIA DE CIBERSEGURIDAD INDUSTRIAL: UN COMPROMISO MULTIDISCIPLINARIO. DOS CASOS DE ÉXITO
Disertantes:
Brian O'Durnin | CISO - YPF
Gerardo González | Gerencia de Ciberseguridad - YPF
Neptali Mayorga | Gerente de Tecnología e Informática - COGA
Ernesto Landa | CISO - COGA

CIBER-RIESGOS EN LA INDUSTRIA DE PETRÓLEO, GAS Y ENERGÍA
Disertante:
Julio Ardita | Director CYBSEC by DELOITTE

LOS BROKERS DE SEGUROS EN LA CIBERSEGURIDAD
Disertantes:

Qué tan relevante es el cyber seguro como un medio de gestión de riesgos para industrias críticas
Elizabeth Gurney | Cyber Product Champion América Latina - Willis Towers Watson

Cyber Risk: más allá de la perdida de datos
Sergio Torres | Vicepresidente Líneas Financieras - AON

CIBERSEGURIDAD EMPRESARIAL, CAUTIVANDO EL INTERÉS DE LA JUNTA DIRECTIVA
Disertante:
Jeimy Cano | Profesor Asociado - Escuela de Administración, Universidad del Rosario

RELEVAMIENTO DE SEGURIDAD DE TO…Y AHORA QUE?…POR DONDE SIGO? CUANDO PUEDO PARAR?
Disertante:
Gabriel Faifman | Gerente Proncipal de Producto Técnico y Director de Programas Estratégicos - BHGE

ORDEN DADA NO SUPERVISADA NO SIRVE PARA NADA. LA AUDITORÍA DE LA CIBERSEGURIDAD DE INFRAESTRUCTURAS CRÍTICAS COMO ELEMENTO CLAVE PARA LA PREVENCIÓN
Disertante:
Gabriela Reynaga | Miembro del Directorio de ISACA

APRENDIZAJES DEL SECTOR ELÉCTRICO COLOMBIANO EN PROTECCIÓN A LA INFRAESTRUCTURA CRÍTICA
Disertante:
Diego Zuluaga | Especialista Seguridad en Información en ISAGEN

LA CIBERSEGURIDAD COMO PILAR DEL PROCESO DE TRANSFORMACIÓN DIGITAL
Disertante:
Lucas Siniscalo | Gerente de I&D - ABB Argentina

TALES FROM THE FIELD: DISECCIÓN DE EVALUACIONES RECIENTES DE REDES ICS.
Disertante:
Schawn Weishaar | Director de Ventas de Claroty - Cytric Solutions

ESTRATEGIAS DE CYBERSEGURIDAD PARA AMBIENTES INDUSTRIALES
Disertante:
Gonzalo Garcia | Director de Fortinet para Sudamérica - FORTINET / Consulting Services

RESILIENCIA EN INFRAESTRUCTURAS CRÍTICAS: ¿CÓMO LOGRAR UNA CAPACIDAD DE RECUPERACIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS?
Disertantes:
Mateo Martínez | Director Ejecutivo - KOD LATAM SECURITY

IIOT NO TIENE QUE SER UN PROBLEMA, AUNQUE A VECES LO ES
Disertante:
Claudio Caracciolo | Chief Security Ambassador - Eleven Paths

MESA DE CIERRE Y REFLEXIÓN
Brian O'Durnin | YPF
Gabriel Faifman | BHGE
Maximilian Kon | Director General de Wiseplant
Diego Zuluaga | ISAGEN
Claudio Caracciolo | Eleven Paths
Jeimy Cano | Universidad del Rosario

INFORMES DE EVENTOS

Ciberseguridad en Infraestructuras Críticas: Riesgos, Oportunidades y Prioridades

arpel

ASOCIACIÓN REGIONAL DE EMPRESAS DEL SECTOR
PETRÓLEO, GAS Y BIOCOMBUSTIBLES
EN LATINOAMÉRICA Y EL CARIBE.

ARPEL es una asociación sin fines de lucro que nuclea a empresas e instituciones del sector petróleo, gas y biocombustibles en Latinoamérica y el Caribe. Fue fundada en 1965 como un vehículo de cooperación y asistencia recíproca entre empresas del sector, con el propósito principal de contribuir activamente a la integración y crecimiento competitivo de la industria y al desarrollo energético sostenible en la región.
Actualmente sus socios representan un alto porcentaje de las actividades del upstream y downstream en América Latina y el Caribe e incluyen a empresas operadoras nacionales e internacionales, proveedoras de tecnología, bienes y servicios para la cadena de valor, y a instituciones nacionales e internacionales del sector.

Este informe fue patrocinado por

YPF

Sede Regional:
Av. Luis A. de Herrera 1248. WTC. Torre 2. Piso 7. Of. 717.
CP 11300. Montevideo, Uruguay
Tel: (+598) 2623-6993 • info@arpel.org.uy

www.arpel.org