arpel Asociación Regional de Empresas del Sector Petróleo, Gas y Biocombustibles en Latinoamérica y el Caribe.

Organización de los Estados Americanos | Más derechos para más gente

Ministerio de Modernización
Presidencia de la Nación

Ministerio de Relaciones Exteriores y Culto
República Argentina

Ciberseguridad, aspecto clave en un mundo hiperconectado

Seminario ARPEL

Diciembre 2016

PUBLICACIÓN ARPEL N° EV03-2016

INFORMES DE EVENTOS

// Contenidos

Introducción

El evento “La ciberseguridad en infraestructuras críticas frente a un mundo tecnológicamente dependiente e interconectado” se llevó a cabo en el Palacio San Martín de Buenos Aires, los días 18 y 19 de octubre de 2016.

Organizado por **ARPEL** (a través de su Grupo de Trabajo en Ciberseguridad), la **Organización de Estados Americanos (OEA)** y los ministerios de **Modernización y de Relaciones Exteriores y Culto de la República Argentina**, el evento congregó cerca de 200 profesionales de los sectores de Tecnologías de la Información (TI) y Tecnologías de la Operación (OT)

Durante dos jornadas de trabajo junto a expertos y autoridades gubernamentales de alto nivel, se analizaron los desafíos que plantea la ciberseguridad para la integridad de las infraestructuras, así como también las más recientes tecnologías, metodologías, sistemas de gestión y estudios de caso.

Las principales conclusiones de dicho evento fueron sintetizadas en este informe, con el fin de lograr una mejor preparación por parte de las empresas y gobiernos ante las nuevas amenazas, emergentes y crecientes que plantea la ciberseguridad.

01 //
Nuevos Riesgos y Amenazas de la Ciberseguridad

La hiperconexión, el nuevo contexto

La acelerada evolución y difusión que han tenido las tecnologías de la información principalmente en los últimos 20 han delineado un mundo completamente diferente al que conocíamos hace una generación atrás. Actualmente es posible difundir y validar una noticia a todo el planeta en segundos, sin necesidad de teletipos, faxes, llamadas internacionales –operador mediante- o intermediarios. Este proceso de profundización de la comunicación no solo es irreversible, sino que también es deseable ya que tiene un rol democratizador, igualador, de libertad de acceso a la información y mejora de la calidad de vida. Como bien planteó **José Hirschson**, representante del Ministerio de Modernización de Argentina, el desafío que surge para los Estados es cómo garantizar la seguridad, a la vez que se aumenta el acceso a la red para generar igualdad.

Por otra parte, las nuevas posibilidades que se ofrecen a nivel de comunicación han modificado sustancialmente la actividad productiva y los canales de comercialización, generando nuevos negocios, pero también deshaciendo otros, en un típico proceso de innovación y destrucción creadora. Esto ha permitido aumentar la productividad de las empresas industriales, por ejemplo, a través del monitoreo en tiempo real de los procesos de trabajo o el control remoto de unidades, pero, a su vez, han hecho emerger una serie de nuevos riesgos para las infraestructuras. Diciendo esto

”

"En los últimos 40 años, el ciberespacio ha traído a una nueva era con nuevos desafíos –ventas, redes sociales, comunicación virtualmente infinita"

José Hirschson
Ministerio de Modernización

último en pocas palabras, hoy en día todo está conectado, y todo lo que esté conectado es controlable de manera remota.
En este contexto de hiperconexión, en el que las áreas operativas ya no pueden manejar la información operativa como compartimentos estancos dentro de la organización, es que se materializan nuevos riesgos de penetración en las redes operativas a través de las redes corporativas.

“Debemos trabajar en conjunto, no se puede superar este desafío individualmente”

“El desafío es mejorar la seguridad, sabiendo que se debe seguir aumentando el acceso para generar igualdad”

José Hirschson
Ministerio de Modernización

Nuevas Amenazas

Según datos del Departamento de Seguridad Nacional de Estados Unidos, en 2015 se reportaron 245 ciberataques a infraestructuras críticas. Ese número es mucho mayor cuando se trata de ataques no vinculados a infraestructuras críticas.
Al asunto ya destacado de la hiperconexión y al almacenamiento de información crítica en la nube –plataforma de servicios informáticos a través de una red, usualmente Internet-, se suma otro que tenderá a crecer exponencialmente en los próximos años e incrementará la vulnerabilidad, el internet de las cosas (IoT por sus siglas en inglés), es decir, a la interconexión de objetos de la vida cotidiana con internet, para lograr su control remoto. El tema fue abordado en detalle por **Erik de Pablo**, consultor español, y también por **Pablo Vaquero**, **Yeffry el Jammal** y **Federico Tandeter**, especialistas de Accenture.
Internet de las cosas industrial (IIoT) es visto como una tendencia con una inmensa potencialidad ya que establece un puente entre los diferentes niveles de información de

“Si la ciberseguridad plantea amenazas, el internet de las cosas pone las cosas mucho peor”

Erik de Pablo
Director de Investigación - ISACA Madrid

“…lo que necesitamos es generar una nueva capacidad adaptativa, ésa es la nueva frontera que tenemos ahora precisamente en ciberseguridad”

Jeimy Cano
M., Ph.D, CFE, Ed.D (c) Profesor Distinguido e Investigador Facultad de Derecho GECTI Uniandes

las compañías, a lo largo de toda la organización y la cadena de valor, permitiendo establecer el monitoreo de indicadores en tiempo real, pero es en este flujo de información que emergen una serie de nuevos riesgos. Controlar remotamente desde luminarias, cámaras o puertas, un auto, una instalación industrial o hasta un marcapasos, son todas situaciones de las que existen ejemplos reales. Por otra parte, **Jeimy Cano,** M., Ph.D, CFE, Ed.D (c) Profesor Distinguido e Investigador Facultad de Derecho GECTI Uniandes, e investigador sobre la temática, hizo una caracterización de los ciberataques y de su entorno, destacando el aumento de la exposición o de la superficie de contacto, no solo debido a lo que refiere a internet de las cosas, sino también a otros ámbitos que aumentan la vulnerabilidad como la computación en la nube, computación móvil, redes sociales, big data y, finalmente, la computación cognitiva, es decir, la inteligencia artificial. Añadió también que los datos son “el petróleo del siglo XXI”, en los que se basa una nueva era industrial y digital, enmarcados en lo que se llama hoy en día la Economía Digital.

Mayor conectividad, mayor dependencia digital, usuarios más dispersos, móviles y menos preparados, y la facilidad de acceso a la tecnología y al conocimiento por parte de los ciberdelincuentes, configuran el escenario de creciente vulnerabilidad de la seguridad personal y de las instalaciones. En el cuadro adjunto se pueden visualizar algunos ejemplos de ataques cibernéticos.

2010

Irán – Nuclear – A través de un gusano informático se logran destruir alrededor de 1.000 centrifugadores enriquecedores de uranio.

2015

Ucrania – Red eléctrica – 30 subestaciones fueron deshabilitadas, alrededor de 230.000 personas quedaron sin energía eléctrica durante un período de entre 1 y 6 horas. Los atacantes estuvieron meses ingresando al sistema operativo para comprender su funcionamiento, y ejecutaron un ataque por varios vectores, que logró apagar las subestaciones, cambiar la visualización de los operarios de control, y bloquear todas las contingencias previstas.

2016

Reino Unido – Potabilizadora de Agua – Una planta potabilizadora de agua para el consumo humano, fue hackeada desde la red corporativa y los parámetros químicos del agua modificados mediante el control remoto de válvulas. A su vez la información personal de 2.5 millones de clientes quedó expuesta. Afortunadamente no hubo consecuencias para la salud de la comunidad.

Bangladesh – Banco – Un ciberataque a través del sistema SWIFT de transferencias internacionales, intentando desviar U$S 951 millones.

Coche autónomo – Un coche autónomo es hackeado a través de un dispositivo de U$S 70, que logra generar falsos obstáculos en los visores láser y hacer que el coche realice maniobras inadecuadas.

Marcapasos – También fue demostrado que el ritmo de un marcapasos puede ser alterado mediante el control remoto a través de un ciberataque.

Una vulnerabilidad adicional que se añade a este nuevo escenario, y que también fue destacada por Jeimy Cano, es la cuestión de los ciberseguros. Citando a la empresa Lloyd´s planteó que el costo de asegurar, por ejemplo, la red eléctrica de EEUU sería de 80 trillones de dólares.

https://www.lloyds.com/news-and-insight/risk-insight/library/society-and-security/business-blackout

Nueva lógica delictiva

La ciberdelincuencia no solo cambia el perfil de los delincuentes, sino también el perfil del delito. Es decir que hoy se pueden desviar fondos de un banco o afectar la operativa de un centro industrial desde la comodidad de un sillón, algo que en otro momento hubiera sido imposible.
Otro aspecto clave del modus-operandi de ataques a las infraestructuras críticas es que el móvil no necesariamente es afectar a la empresa, sino a la comunidad.

Por este motivo también es que el abordaje de la defensa de las infraestructuras debe realizarse con una visión integral que excede los límites de la empresa y que tiene como finalidad la conservación del bien común.
La dificultad de detección, la malicia, la cooperación entre los ciberdelincuentes y la evolución constante de la tecnología son también otros desafíos que propone la nueva lógica de la ciberdelincuencia.

"¿Estamos bajo ataque? Sí, lo vemos permanentemente (…) los gobiernos y las infraestructuras críticas somos objetivos"

Óscar Morotti
Coordinador de Operaciones de la Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad - Ministerio de Modernización de la República Argentina

02 //
OT vs IT
un puente necesario entre dos mundos no tan interconectados

Paradójicamente, uno de los puntos más destacados entre los diferentes presentadores, fue la necesidad de tener una mayor conexión entre lo que refiere a la gestión integrada de IT y OT. Como se explicó anteriormente, la conexión entre estos dos mundos, es decir, entre las redes industriales y las corporativas, se está dando a nivel de sistemas informáticos; las nuevas necesidades de las empresas hacen que esta sea la tendencia, pero genera a su paso nuevas vulnerabilidades.

Un ejemplo claro que dio al respecto **Julio Ardita,** director de CYBSEC, es que en la investigación de incidentes que vulneraron la red industrial, se ha detectado que en muchos casos la intromisión a la red industrial se dio a través de la red corporativa. Una de las principales vulnerabilidades existentes en la protección efectiva ante ciberataques es precisamente la falta de coordinación entre las áreas de IT y OT. Si bien en todos los casos se coincidió en la necesidad de una

"Una buena seguridad es un buen negocio, no un costo"

Julio Ardita
Director de CYBSEC

“Entre tanto no se sepa cuáles son los límites de cada modelo (IT/OT), va a ser difícil poder desarrollar juntos las convergencias”

Maximilian Kon
Director de Wiseplant

gestión más integrada, no se deja de reconocer que estos dos “mundos” tienen sus características particulares y diferenciadoras, lo cual plantea un desafío para la armonización.
Sobre este punto, **Maximilian Kon** de Wiseplant, en su disertación “¿Qué hay de cierto, aciertos y desaciertos cuando se habla de IT/OT?” fue particularmente claro en su caracterización de estos dos “mundos” en cuanto a las políticas aplicadas, los riesgos a considerar, las prioridades y las acciones de mitigación, detección y protección. Las conclusiones se resumen en el siguiente cuadro:

IT	OT
Usuarios dispersos, información concentrada en bases de datos y mayor estandarización	Usuarios concentrados (ej. SCADA), información dispersa, tomada de campo por diferentes sensores desde las capas más bajas, menor estandarización de protocolos, tiempos, etc.
Trabajan sobre la seguridad de la información, y que esta no caiga en las manos equivocadas. El valor más protegido es la confidencialidad	Trabaja sobre la seguridad de activos físicos, es la integridad de la instalación y la vida y la salud de los trabajadores y la comunidad lo que está en juego. El valor más importante es garantizar la disponibilidad y la seguridad física.
Ciclo de vida corto de la tecnología	El ciclo de vida de la tecnología es más largo (equipos de 15-20 años)
Respuesta más rápida a las amenazas, más factible realizar parches.	Respuesta más lenta a las amenazas por la dificultad de realizar parches que surge de la propia operativa

A su vez, por las propias características de estos dos “mundos”, se planteó que concretar un ataque exitoso a una infraestructura industrial es más complejo porque se deben conocer otras tecnologías y protocolos, se deben pasar medidas de seguridad más sólidas y se debe tener conocimiento de cómo operar los sistemas de control y monitoreo, por lo que se necesita mucho más tiempo

Como bien planteó **Santiago Paz** de Agesic, cuando alguien concreta un ataque a una infraestructura, es probable que ya haya entrado a la red y violado la seguridad desde hace ya algún tiempo y que las contingencias también hayan sido vulneradas. Un ejemplo ilustrativo es el ataque realizado en la red eléctrica de Ucrania, en el que los atacantes entraron al sistema durante varios meses para poder aprender a operarlo y comprender sus contingencias también.

Tender puentes entre las áreas de IT y OT es una necesidad, pero a la vez un gran desafío en el que no se deben dejar de lado las cuestiones institucionales y culturales de cada uno de estos mundos, con sus prioridades y características diferenciadoras.

03 //
La respuesta a los incidentes

Los riesgos a los que se está expuesto en cuestiones de ciberseguridad evolucionan permanentemente y solo tenderán a crecer, en función de que las conexiones a la red seguirán creciendo e integrándose cada vez más, aumentando así la superficie de ataque. La nueva lógica delictiva delinea una serie de necesidades diferentes a la hora de responder a la emergencia.

Como bien planteó **Marcos G. Salt**, Director del Programa Nacional sobre Criminalidad Informática, Ministerio de Justicia y DD.HH de la República Argentina, lo que se debe generar contra el ciberdelito, es un frente común entre todos los actores involucrados. Este llamado a la cooperación, y a la alianza público-privada contra el ciberdelito, es un mensaje reiterado en las diferentes sesiones a lo largo de todo el evento.

La cooperación es entonces un aspecto fundamental en la respuesta ante incidentes, y organizaciones como **ARPEL** y **OEA** ya están trabajando en el asunto, dado que son organismos que tienen capacidad de nuclear a los diferentes actores e impulsar esa cooperación a nivel regional.

Entre los actores más importantes para generar ese frente contra el ciberdelito al que hace referencia Marcos G. Salt, se encuentra el Centro de Respuesta a Incidentes de Seguridad Informática (CERT) nacional, el poder ejecutivo a través de sus ministerios, el poder judicial, las instituciones de defensa nacional, el sector privado, las empresas públicas y la academia. Cada uno en su rol y con un fuerte liderazgo desde el Estado, es que se logrará neutralizar los riesgos de la mejor manera posible.

”

“Al final es la inestabilidad que eso (un ciberataque) produce, la incertidumbre que eso produce, lo que finalmente afecta a las organizaciones (…) entonces la ciberseguridad al final lo que está buscando es asegurar la resiliencia organizacional”

Jeimy Cano
M., Ph.D, CFE, Ed.D (c) Profesor Distinguido e Investigador Facultad de Derecho GECTI Uniandes

”

“(la ciberseguridad) Debe ser parte de una Política de Estado, coordinada, que permita establecer un frente común contra el ciberdelito”

Marcos G. Salt
Director del Programa Nacional sobre Criminalidad Informática, Ministerio de Justicia y DD.HH de la República Argentina

El rol de los CERTs

Santiago Paz, Director de Seguridad de la Información en AGESIC , y fundador del Centro Nacional de Respuesta a Incidentes de Seguridad Informática de Uruguay, realizó una elocuente presentación sobre el rol que deben tener los Equipos de Respuesta ante Emergencias Informáticas (CERT, por sus siglas en inglés), en la que quedó de manifiesto la necesidad de cooperación, pragmatismo, agilidad y flexibilidad para hacer frente a las amenazas e incidentes de seguridad de la información. También mencionó algunas buenas prácticas como la aplicación sistemática y coherente de auditorías para implementar las oportunidades de mejora detectadas. Destacó que coordinar y ejecutar actividades de prevención y respuesta a incidentes es el leitmotiv de un CERT y puso énfasis en que se aplique un modelo “agile” de gestión de la respuesta. Es decir, que el CERT sea un facilitador capaz de liderar la respuesta a la emergencia, a través de la formación de equipos ágiles de profesionales de diferentes disciplinas, organismos y ámbitos, con capacidad de autogestión. No todo el conocimiento debe estar en el CERT sencillamente porque no sería lo más eficiente ni costo-efectivo, pero sí deben existir formas de que el CERT acceda rápidamente al conocimiento mediante arreglos preestablecidos con diferentes actores, pudiendo activar así una respuesta eficaz.

“El rol clave del CERT es ser el líder a nivel nacional, ser el articulador que pone a la persona indicada en el lugar indicado para hacer frente a una respuesta”

Santiago Paz
Agesic, Uruguay
Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (Uruguay)

El buen funcionamiento de este tipo de equipos requiere de un “ecosistema de respuesta” bien definido y organizado, en el que cada actor esté capacitado para cumplir su rol. El cuerpo de Policía, el Ministerio de Defensa, el Ministerio de Industria, la Universidad, el Sector Privado, los Proveedores de Servicios Informáticos y las Empresas Públicas son algunos de los actores principales que conforman ese ecosistema en Uruguay.

La ciberseguridad es una amenaza emergente, no tradicional, por lo que para ser exitosos en la prevención, la respuesta también debe salirse de la gestión tradicional de la seguridad.

La necesidad de regulación y el rol de poder judicial

Durante el segundo día del evento se llevó a cabo el panel “La necesidad de un marco normativo para la ciberseguridad industrial” en el que participaron **Raúl Palenque**, consultor del Ministerio de Relaciones Exteriores y Culto y **Marcelo Temperini**, abogado especialista en derecho informático. En dicho panel se discutieron algunas características deseables para que los marcos normativos sean eficientes para hacer frente a los asuntos de ciberseguridad, en un escenario de mayor vulnerabilidad derivada de la incorporación de tecnología al sistema productivo y a la vida cotidiana.

Se estableció que es necesario avanzar en establecer una normativa para la protección de las infraestructuras críticas, de forma que se sienten las bases para el liderazgo del Estado en esa necesaria alianza público-privada para abordar este asunto, aunque la regulación por sí misma no será suficiente.

Por otra parte, **Marcelo Temperini**, que tituló su presentación “El derecho como herramienta”, fue muy enfático en el hecho de que la regulación debe ser pragmática y eficiente. Luego de repasar la situación y los avances logrados en Argentina al respecto,

> “Más allá de los marcos normativos, la primera trinchera en la lucha por la seguridad es la técnica”
>
> **Raúl Palenque**
> Consultor del Ministerio de Relaciones Exteriores y Culto de la República Argentina

planteó que para lograr una regulación útil, en primer lugar se deben tomar los buenos ejemplos existentes a nivel mundial, como el español, el cual fue presentado por **Manuel Sicilia**, jefe de sección de análisis del servicio de cibereguridad de CNPIC, durante el primer día del evento. A su vez, puso énfasis en la necesidad de que el sector público mantenga un fuerte liderazgo en la implementación, acompañando al sector privado pero que defina roles claros, obligaciones y que castigue los incumplimientos ya que un asunto de estas características no debe ser librado a la buena voluntad de actores dispersos, que seguramente sea muy difícil de lograr, y en donde no existe una conciencia real del riesgo que presenta la ciberseguridad para las empresas o individuos.
También fue destacado por él y otros disertantes, el hecho de que una regulación no debe ahondar en la definición de nuevos delitos que añadan redundancias y absorban recursos. Si bien en algunos casos sería estrictamente necesario, la realidad es que los códigos vigentes ya permiten tipificar varias de las situaciones derivadas de los ciberataques. Es decir, en muchos casos lo que cambia no es el tipo de delito, el acto generador, sino el medio utilizado para realizarlo. Un hacker que desvía fondos de un banco a través de la red o que accede al control de una planta industrial, es perfectamente punible desde las leyes vigentes, más allá de cuál haya sido el medio utilizado. Claro está que el asunto de la atribución es uno de los desafíos adicionales que establece la ciberdelincuencia.
En lo que también fueron enfáticos los presentadores durante las dos jornadas fue en el hecho de que se debe trabajar fuertemente en la capacitación del Poder Judicial, algo en lo que ya han avanzado algunos países. Desde esta perspectiva, los jueces deben ser entrenados debidamente para que puedan comprender e interpretar adecuadamente las acciones delictivas perpetradas a través de la red, siendo este otro punto de cooperación necesaria entre el sector público y el privado.
Para finalizar, también se estableció que una buena regulación, si bien es necesaria, no es suficiente para el abordaje de la temática, ya que el desafío es demasiado amplio y se encuentra en constante evolución. En última instancia, será la capacidad de los actores para actuar coordinadamente ante las amenazas lo que permitirá proteger a las infraestructuras del cibercrimen, y la regulación es solo un aspecto fundamental de ese proceso.

Respuesta a los incidentes

“No les estoy diciendo que de la noche a la mañana tiene que estar todo bien (...) Sean selectivos, traten de identificar los riesgos, de priorizar cuáles van a ser los requerimientos y empiecen, empiecen a hacerlo (...) crezcan, definan, empiecen a crear los procedimientos, eduquen y empiecen a practicarlo. Ése es el camino.”

“Sepan que se puede, sepan que es gradual y tengan capacidad de frustración. Ése es mi mejor consejo”

Gabriel Faifman
Director de Programas Estratégicos de Wurldtech

Gabriel Faifman, Director de Programas Estratégicos de Wurldtech, subsidiaria de GENERAL ELECTRIC, realizó su disertación presentando las bondades del estándar 62443 para implementar la ciberseguridad en una empresa industrial y remarcó una serie de recomendaciones para avanzar en la temática.

El estándar 62443 se compone de 13 documentos o guías de buenas prácticas para la implementación de la seguridad informática en toda su extensión. Es un paraguas que establece los requerimientos y las áreas funcionales a proteger. A pesar de la existencia del estándar, mencionó que el 66% de las empresas internacionales encuestadas en el Informe “2015 Global Megatrends in Cybersecurity” de Raytheon and Ponemon, no estaría preparada para gestionar un ciberataque. Destacó que la vulnerabilidad no es una cuestión particular ni de Argentina ni de América Latina, sino que lo es a nivel internacional. Por otra parte destacó la oportunidad que esto representa para Argentina, ya que al momento de actualizar sus sistemas de producción, podría incluir los criterios de ciberseguridad, ya que hoy es posible, debido al estado del arte actual, existiendo el potencial para liderar la temática.

Entre sus principales mensajes para abordar la preparación ante ciberataques, destacó el hecho de que los estándares se basan en modelos de madurez, por lo que insistió en la gradualidad necesaria en la implementación, pero que se debe avanzar sin pausa. Realizar los análisis de riesgos, priorizar, diseñar los procedimientos y capacitar es el camino para avanzar en la implementación de la ciberseguridad, y estas son cosas que hoy se pueden hacer. Por último fue enfático en la necesidad de involucrar a los proveedores de tecnología y ser exigentes, para obtener mejores soluciones y servicios.

¿Qué tan preparados estamos?

Durante el panel “El estado de la ciberseguridad en Latinoamérica”, **Claudio Caracciolo** y **Nora Azúa**, coordinadores del Centro de Ciberseguridad Industrial (CCI), presentaron los resultados preliminares de un estudio realizado recientemente en Argentina por dicha organización. El mismo está basado en una encuesta de la cual participaron 18 empresas de diferentes sectores y que arrojó algunos resultados interesantes, a la vez que desafiantes en cuanto a la preparación ante ciberataques. Se exhiben a continuación algunos resultados destacados:

“Estamos un paso detrás, siempre estuvimos y siempre vamos a estar (..) los hackers tienen la ventaja (…) Es un mito que el sector energético es y será el más atacado. El sector más atacado será el más fácil de atacar, el que tenga menor protección para comprometer equipos”

Claudio Caracciolo
Coordinador del Centro de Ciberseguridad Industrial (CCI)

“Vemos que las empresas están respondiendo de forma reactiva”

Pablo Vaquero
Gerente de Seguridad, Accenture

- En el 42% de los casos, el responsable de la ciberseguridad era el área de TI.
- Se detectó un grado aceptable de capacitación en las áreas de TI, aunque bajo en otras áreas como recursos humanos, calidad, compras, seguridad.
- 41% de las empresas no había realizado formalmente un análisis de riesgos de ciberseguridad.
- En los nuevos proyectos suelen pedirse requisitos de ciberseguridad, pero en general muy básicos y en algunos casos se delega al proveedor.
- En más del 50% de los casos no existe proceso de gestión de incidentes, o su gestión se hizo de forma reactiva.
- El estudio también deja en evidencia muchas veces el desconocimiento que se tiene desde el sector privado de las iniciativas que se impulsan desde el sector público.

Si bien el estudio no puede ser considerado estadísticamente significativo, provee algunas tendencias interesantes en las que valdría la pena profundizar. Es pertinente suponer que existen brechas en lo que respecta a concientización y conocimiento de las amenazas, capacitación, análisis de riesgos y gestión de incidentes.

Claudio Caracciolo, en su segunda disertación, titulada "¿Control y monitoreo o simplemente descontrol?" planteó una máxima sobre protección ante ciberataques, y es el hecho de que serán las empresas e infraestructuras más vulnerables las que serán atacadas y afectadas, y no un sector en particular. Según el estudio del Departamento de Seguridad Nacional de EEUU correspondiente al año 2015 el sector energético contaba con 16% de los ataques registrados, un gran desafío para la industria en su conjunto.

Ser abiertos, cooperativos y compartir información sobre los incidentes fue uno de los puntos más destacados del seminario, como una de esas buenas prácticas que aceleran la curva de aprendizaje y mejoran la preparación ante incidentes. En EEUU, este ha sido el punto clave de la regulación y de la articulación de la cooperación público-privada en ciberseguridad, un ejemplo sin dudas a seguir en nuestra región.

Por otra parte, **Julio Ardita**, Director de CYBSEC, durante la mesa redonda "Casos de ciberataques a infraestructuras críticas" presentó un análisis de diferentes casos reales que fueron estudiados en América Latina y se apoyó en un caso hipotético tipo para extraer algunas conclusiones generales del status de la respuesta a emergencias en nuestra región.

Entre las principales brechas encontradas en las investigaciones de incidentes que ha realizado en la región, se encuentran que existen pocos registros (logs o bitácoras) de lo acontecido, el desconocimiento del tema

"Si se siguen todas las buenas prácticas recomendadas, la probabilidad de ataque es muy baja"

Julio Ardita
Director de CYBSEC

por parte de los ingenieros responsables de la operación, y la escasa conexión entre las áreas de IT corporativas, de seguridad de la información y las áreas operativas (OT vs IT).
Para cerrar su disertación, planteó que los ataques no son solo externos, sino que también pueden venir desde dentro de la organización y en estos casos resulta mucho más complejo el abordaje, y que si bien la ciberseguridad plantea desafíos y una lógica algo diferente a la seguridad tradicional, también existen buenas prácticas y estándares internacionales que, de ser aplicados efectivamente, reducen al mínimo las vulnerabilidades ante los ciberataques.
Concientizar, entrenar, aportar el software adecuado, compartir información y actuar cooperativamente fueron los principales mensajes que surgen del taller para mejorar la protección ante ciberataques.
Por otra parte, **Jeimy Cano**, manifestó la importancia de pensar los riesgos en función de escenarios construidos entre varios miembros y áreas de la organización, que permitan expandir la percepción de lo posible, para actuar en consecuencia. En la misma línea **Erik de Pablo** planteó la necesidad de pensar de forma no lineal los riesgos en ciberseguridad, a diferencia de la forma en que se piensan los riesgos en HSE; porque eso llevaría a la subestimación de costes, ya que existen otros vectores de ataque, como la malicia, o la nueva lógica que plantea la ciberdelincuencia. Pensar distinto, ante una amenaza distinta, es una necesidad para aumentar los niveles de preparación y, finalmente, la resiliencia de la organización.

> “….tenemos que acercarnos al negocio para explicarles la realidad de lo que puede suceder, porque son diferentes tomadores de desiciones..”

Daniel Molina
Director General para los Mercados Estratégicos de América Latina, Karspersky Lab

04 //
Mensajes clave

A modo de conclusión, se destacan a continuación los mensajes clave que emergieron de las dos jornadas de trabajo.

1

La ciberseguridad es una amenaza emergente y creciente ya que está correlacionada al aumento de la conectividad a la red, la cual tenderá a aumentar dadas las posibilidades que ofrece para mejorar la productividad y la calidad de vida de las personas.

2

La ciberseguridad es una amenaza latente, permanente y real de la que nadie está exento y que puede traer consecuencias de altísimo impacto para las infraestructuras, las empresas y la comunidad.

3

La ciberseguridad cambia la lógica de la seguridad y para ser exitosa debe ser abordada desde una perspectiva ágil, pragmática e integral de cooperación entre agentes públicos y privados. Se debe generar un frente común contra el ciberdelito, liderado por el Estado. La regulación es una herramienta necesaria pero no suficiente dentro de ese proceso.

4

Concientizar, entrenar, aplicar las herramientas informáticas adecuadas, compartir información y ser cooperativos y abiertos dentro de ese frente común es una necesidad para generar un nivel de prevención y respuesta eficaces.

5

A pesar de que existen brechas y de que hay mucho trabajo por hacer en cada uno de los países de la región, ya existen estándares, conocimiento, buenas prácticas y herramientas disponibles que permiten reducir al mínimo la posibilidad de un ciberataque. Es decir, que es una amenaza gestionable, en donde la clave para estar preparados radica en poder realizar una correcta implementación de dichos estándares y buenas prácticas.

Haga clik en los títulos o lea los códigos QR con su dispositivo móvil para acceder a los vídeos de las disertaciones.

Descargue la aplicación según el sistema operativo de su dispositivo.

ANDROID

iOS
APPLE

Ceremonia de Apertura

José Hirschson | Subsecretario de Tecnología y Ciberseguridad - Ministerio de Modernización
Francisco Laines | Asesor de la Secretaría Multidimensión de la Secretaría General de la OEA
Jorge Ciacciarelli | Secretario Ejecutivo - ARPEL

La importancia de los CERTs nacionales

Santiago Paz | Director de Seguridad de la Información - AGESIC
Moderador: Mariana Galán | Asesora Legal Experta del Subsecretario de Tecnología y Ciberseguridad del Ministerio de Modernización

Panel: Estado de Ciberseguridad Industrial en Latinoamérica

Nora Alzua | Coordinadora - CCI en Argentina
Claudio Caracciolo | Coordinador - CCI en Argentina
Moderador: Juan J. Dell'Aqua | Director Ejecutivo - Usuaria

Panel: Norma IEC 62443

Gabriel Faifman | Director de Programas Estratégicos - Wurldtech
Andre Ristaino | Director General - ISASecure
Moderador: Gerardo González | Centro de Ciberseguridad Industrial e IC - YPF

Infraestructuras Críticas

Erik De Pablo | Director de Investigación - ISACA Madrid

La protección de las infraestructuras críticas: el caso de España

Manuel Sicilia San José | Jefe de Sección de Análisis del Servicio de Cibereguridad - CNPIC

Convergencia IT/OT: ¿Qué hay de cierto, aciertos y desaciertos cuando se habla de IT/OT?

Maximillian G. Kon | Director Gerente, WisePlant

Panel: Perspectivas de la protección del ciberespacio: iniciativas del Estado Nacional Argentino

Leandro de la Colina | Subsecretaría de Ciberdefensa - Ministerio de Defensa
Marcos G. Salt | Director, Programa Nacional sobre Criminalidad Informática - Ministerio de Justicia y DD.HH (no utilizó ppt)
Jorge A. Teodoro | Director de Tecnología - Ministerio de Seguridad
Moderador: Eduardo Martino | Director Nacional, Infraestructuras Críticas y Ciberseguridad - Ministerio de Modernización

El uso de la ciber resiliencia en la siempre activa empresa

John Duronio | Arquitecto de Seguridad Senior - Intel

Los riesgos de las nuevas tecnologías de operación inteligentes: Industrial Internet of Things

Pablo Vaquero | Gerente de Seguridad - Accenture
Yeffry El Jammal | Gerente Senior de Consultoría - Accenture
Federico Tandeter | Gerente Senior de Seguridad - Accenture
Moderador: Oscar Morotti | Coordinador de Operaciones de la Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad - Ministerio de Modernización

¿Control y monitoreo o simplemente descontrol?

Claudio Caracciolo | Chief Security Ambassador - Eleven Paths

Mesa Redonda: Casos de ciberataques a infraestructuras críticas

Julio Ardita | Director - CYBSEC
Daniel Molina | Director General para los Mercados Estratégicos de América Latina - Karspersky Lab
Moderador: Patricia Prandini - Ministerio de Modernización

Panel: La necesidad de un marco normativo para la ciberseguridad industrial

Raúl Palenque | Consultor - Ministerio de Relaciones Exteriores y Culto
Marcelo Temperini | Abogado Especialista en Derecho Informático - Consultora AsegurarTe
Moderador: Oscar Morotti | Coordinador de Operaciones de la Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad - Ministerio de Modernización

Panel: La importancia de la protección de las infraestructuras críticas y la defensa nacional

Aristides Sebastião Lopes Carneiro | Asesor - Cyber Comando Brasil
Daniel Henao | Cyber Comando Colombia
Oscar Mato | Representante - Cyber Comando Argentina
Ricardo Uquillas Soto | Cyber Comando Ecuador
Moderador: Leandro de la Colina | Subsecretaría de Ciberdefensa - Ministerio de Defensa

Panel: La justicia frente a los ataques de las infraestructuras

Horacio Azzolin | Fiscal de la Procuración General de la Nación - Ministerio Público Fiscal
Daniela Dupuy | Fiscal del Ministerio Público Fiscal de la Ciudad Autónoma de Buenos Aires
Moderadora: Mónica Abalo Laforgia | Asesora Legal - Ministerio de Modernización

Desarrollo y Análisis de escenarios en ciberseguridad

Jeimy Cano | Profesor Distinguido - Facultad de Derecho - GECTI - Universidad de los Andes

Panel: Seguridad sobre infraestructuras críticas

Juan Camilo Reyes | Líder Regional de Servicios de Seguridad - IBM
Walter E. Riveros | Director de Seguridad Ofensiva - Deloitte
Pablo M. Almada | Gerente, Asesoría de TI - KPMG
Hernando Castiglioni | Gerente Ingeniería de Sistemas - Fortinet
Moderador: Gonzalo García-Belenguer | Oficial de Proyecto - OEA

Ciberseguridad Industrial

Francisco Souto | Gerente de Desarrollo de Negocios para Ciberseguridad - Honeywell

Mesa de cierre y reflexión: Construcción de una cultura de ciberseguridad para la protección de infraestructuras críticas

Eduardo Martino | Director Nacional, Infraestructuras Críticas y Ciberseguridad - Ministerio de Modernización
Francisco Laines | Asesor de la Secretaría Multidimensión de la Secretaría General de la OEA
Brian O´Durnin | Gerente de Seguridad de la Información - YPF
Hernán Vázquez | Gerente de TI - ARPEL

Clip general del evento

INFORMES DE EVENTOS

Ciberseguridad, aspecto clave en un mundo hiperconectado

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 más del 90% de las actividades del upstream y downstream en la región e incluyen a empresas operadoras nacionales, internacionales e independientes, a proveedoras de tecnología, bienes y servicios para la cadena de valor, y a instituciones nacionales e internacionales del sector.

Este informe fue patrocinado por

Sede Regional:
Javier de Viana 1018. CP 11200, Montevideo, Uruguay
Tel.: +(598) 2410 6993 | info@arpel.org.uy

www.arpel.org