

# Fundamentos de la Ciberseguridad Industrial

Seminario ARPEL

---

Agosto 2017

PUBLICACIÓN ARPEL N° EV04-2017



INFORMES DE EVENTOS

# YPF desarrolló jornadas de concientización sobre Ciberseguridad

Siguiendo con el compromiso de difundir y concientizar sobre la importancia de la Ciberseguridad, la **Gerencia de Seguridad de la Información de YPF** llevó a cabo junto a la **Asociación Regional de Empresas del Sector Petróleo, Gas y Biocombustibles en Latinoamérica y el Caribe (ARPEL)** un seminario abierto y tres talleres privados para profesionales y altos ejecutivos de la compañía, los cuales tuvieron lugar del 31 de julio al 2 de agosto en Torre Madero.

La acelerada incorporación de la cuarta revolución industrial y de los productos y/o servicios digitalmente modificados, establecen retos no solamente para las naciones, sino que también para las organizaciones.

Se ponen a prueba los modelos de riesgos y controles en medio de un entorno volátil, incierto, complejo y ambiguo, ahora frente al reto de la resiliencia digital como nuevo normal de las empresas del siglo XXI.

En este escenario, dichas actividades tuvieron como objetivo concretar un entendimiento base sobre el reto que demanda la Ciberseguridad para las organizaciones que aspiran a ser protagonistas de las nuevas exigencias de los negocios digitales.

Durante las tres jornadas fueron abordadas distintas temáticas como ser:

- Presentación del white paper de ARPEL titulado “**Ruta estratégica de la ciberseguridad empresarial**”.
- **Marcos de trabajo actuales en ciberseguridad:** NIST, ISA/IEC 62443, ISO27000, CCDCOE, etc.
- **Riesgos claves** relevantes para la ciberseguridad empresarial.
- **Prácticas emergentes** en ciberseguridad empresarial.
- **Ciber-Resiliencia** en las organizaciones.
- El riesgo de Cyber en los **mercados internacionales** de reaseguro, tratamiento y tendencias de cobertura.



Los **talleres internos** realizados los dos primeros días fueron liderados por el experto **Jeimy Cano**, Profesor Asociado en la Escuela de Administración de la Universidad del Rosario, Bogotá, Colombia. Cano es Ingeniero y Magíster en Ingeniería de Sistemas y Computación por la Universidad de los Andes, y cuenta con más de 20 años de experiencia como académico y profesional en seguridad de la información, auditoría de TI, delitos informáticos, privacidad y temas convergentes en Colombia y Latinoamérica.

Asimismo, es autor del documento de ARPEL “**Ruta estratégica de la ciberseguridad empresarial**”.



**Descargue el documento**

La actividad del primer día tuvo como fin reflexionar e indagar sobre la **práctica actual de la Ciberseguridad Industrial en YPF**, y contó con la participación de los responsables técnicos de la operación de activos industriales de distintos negocios además de integrantes de la **Gerencia de Seguridad de la Información**.

En este primer taller se realizaron dos sesiones de trabajo (mañana y tarde) y se armaron equipos de cinco personas cada uno. Al finalizar, tuvo lugar una puesta en común de las principales ideas trabajadas, motivando un análisis detallado que permitió obtener conclusiones concretas y prácticas.

Al día siguiente, se llevó a cabo el taller dirigido al **CEO, Vicepresidentes de la compañía y Gerentes Ejecutivos** bajo el nombre “**Fundamentos, responsabilidad y riesgos clave de la ciberseguridad empresarial en la industria de petróleo y gas**”.

En tanto, en la tarde se desarrolló el tercer taller orientado al **Comité de Auditoría, Comité de Riesgos y Directores**. En este caso los temas abordados fueron: Convergencia tecnológica de los mundos IT y OT; Fundamentos, responsabilidad y riesgos clave de la ciberseguridad, y Ciber riesgos.

SEMINARIO

# Fundamentos de la Ciberseguridad Industrial

2 de agosto de 2017 | Buenos Aires, Argentina



PATROCINAN



ANFITRIÓN



Como cierre de las actividades realizadas con el fin de concientizar y al mismo tiempo promover un mayor entendimiento sobre la Ciberseguridad, se realizó el 2 de agosto el **Seminario “Fundamentos de la Ciberseguridad Industrial”**, el cual contó con la asistencia de más de 100 profesionales del sector y autoridades gubernamentales locales.

La jornada, que contó con el apoyo de **Kaspersky Lab** y **Honeywell**, comenzó con la charla titulada **“Prácticas emergentes en ciberseguridad empresarial y la importancia en la agenda de la alta dirección”**, a cargo de **Jeimy Cano**.

La agenda continuó con las siguientes exposiciones:  
-**“Ciber-Resiliencia en las Organizaciones”**, por **Julio Ardita**, fundador y Director de Tecnología de CYBSEC desde 1996. Ardita posee más de 22 años de experiencia práctica en seguridad de la información.

-**“Evaluación de situación inicial – cómo elegir un ciber estándar”**, por **Francisco Souto**, Gerente de Desarrollo de Negocios para Ciberseguridad en Honeywell.

-**“Ciberseguridad Industrial: nuevos riesgos y**

**desafíos estratégicos”**, por **Andrés Giarletta**, responsable de Ingeniería para el Cono-Sur en Kaspersky Lab.

-**“El riesgo de Cyber en los mercados internacionales de reaseguro, tratamiento y tendencias de cobertura”**, por **Natalia Char**, Gerente Regional Latinoamérica para productos de Líneas Financieras en Willis Towers Watson, y **Jesús González**, de Cyber Aon Risk Solutions, enfocado exclusivamente en cobertura de riesgos cibernéticos.

El panel de cierre titulado **“Aceptando el cambio industrial 4.0. Prevención y Proactividad”** estuvo a cargo de **Hernán Vázquez**, Gerente de Informática de ARPEL; Ph.D, CFE **Jeimy Cano**, y **Brian O’Durnin**, CISO de YPF.



## RESUMEN DE JEIMY CANO SOBRE ACTIVIDAD EN YPF Y CONTENIDOS DESTACADOS DE ORADORES DEL SEMINARIO

A continuación compartimos un breve resumen elaborado por Jeimy Cano acerca de las actividades realizadas en YPF.

Luego, le sigue una selección de los contenidos expuestos por los disertantes del Seminario **“Fundamentos de la Ciberseguridad Industrial”**.

### RESUMEN DE TALLERES Y PRESENTACIÓN EN EL EVENTO

Por **Jeimy Cano**

La realización de los talleres realizados en YPF sobre ciberseguridad empresarial, establecen un marco de reflexión para los participantes, habida cuenta que permite fundar un lenguaje común que habilita conectar diferentes vistas e intereses de los negocios de la cadena de la industria de petróleo y gas.

Durante el desarrollo de los talleres se presentaron los fundamentos de la ciberseguridad empresarial, concretando tanto la vista del concepto de “Security”, así como el de “Safety”, para introducir el reto de la resiliencia como nueva frontera de la práctica de la ciberseguridad en las empresas. Mientras en la actualidad, la seguridad de la información se concentra en la protección de los activos de información, la ciberseguridad empresarial se concentra en el negocio y su capacidad para sobrevivir a interrupciones conocidas e inesperadas, con el fin de salvaguardar la continuidad de las operaciones y la reputación de la organización.

En este ejercicio la perspectiva del riesgo frente a la protección bien sea de la información o el negocio, se actualiza. Se pasa de un entendimiento natural del riesgo como situación a controlar y mitigar, a una donde el riesgo se debe comprender, con el fin de abrirse a

posibilidades para capitalizar las oportunidades que subyacen en este. Es una apuesta para concretar acciones diferentes desde el entendimiento de los umbrales de riesgo acordados con los ejecutivos de la empresa y movilizar acciones que creen valor en lugares antes inexplorados.

Asumir la incertidumbre de los nuevos escenarios y retos empresariales de la industria de petróleo y gas, supone adelantar simulaciones, prototipos y escenarios con el fin de acelerar los entornos inciertos y aprender rápidamente de lo que estos ejercicios sugieren tanto a la organización como a los participantes de los talleres. De igual forma, con la presentación de los marcos actuales de gestión de la ciberseguridad disponibles, se establecieron referentes base de análisis y revisión que permiten a los participantes comparar sus prácticas actuales para advertir como pueden enriquecer sus apuestas actuales.

Un programa de ciberseguridad empresarial debe estar concebido desde cuatro axiomas de diseño, los cuales deben nutrir cada una de las actividades planteadas, para corresponder con el desafío de

la resiliencia, como objetivo final del ejercicio de la ciberseguridad en las empresas. Los principios de diseño son:

- Asuma que un atacante inteligente podría superar todas las medidas defensivas
- Diseñe defensas para detectar y demorar los ataques
- Incluya niveles de defensa para contener los ataques y proveer redundancia en la protección
- Use defensas activas para capturar y repeler los ataques después que inician y antes que tengan éxito

Seguidamente, se presentan los **cinco riesgos estratégicos claves de la ciberseguridad empresarial** (geopolítico, regulatorio, reputación, crimen organizado,

discontinuidad tecnológica), detallados en el “White Paper” de ARPEL denominado “Ruta estratégica de la ciberseguridad empresarial. Un marco de orientación directiva”, los cuales son desarrollados y comentados como fundamento de la manera como la organización debe asumir el reto de alcanzar la resiliencia digital en el contexto de un mundo volátil, incierto, complejo y ambiguo.

Finalmente, la presentación efectuada en el evento abierto al público sobre ciberseguridad empresarial organizado por ARPEL, se desarrollan tres momentos claves uno de tendencias a la fecha donde introduce el concepto de “densidad digital”, otro de conceptos básicos y finalmente uno adicional de actualización de “herramientas metodológicas” requeridas para explorar y retar el ejercicio de construir una distinción de ciberseguridad empresarial novedosa y ajustada a la inestabilidad de los cambios actuales y futuros.

## Selección de contenidos del Seminario “Fundamentos de la Ciberseguridad Industrial”

### Prácticas emergentes en ciberseguridad empresarial y la importancia en la agenda de la alta dirección

Ph.D, CFE **Jeimy Cano**

**Elementos conceptuales de la ciberseguridad empresarial**

Asuma que un atacante inteligente podría superar todas las medidas defensivas

Diseñe defensas para detectar y demorar los ataques

Incluya niveles de defensa para contener los ataques y proveer redundancia en la protección.

Use defensas activas para capturar y repeler los ataques después que inician y antes que tengan éxito.

**Axiomas para el diseño**

Atacante inteligente

Defensa activa

Detectar y demorar

Repeler y capturar

Adaptado de: Donaldson, S., Segel, S., Williams, C., y Ailam, A. (2018) Enterprise Security: How to build a successful cyberdefense program against advanced threats. Wiley John, USA. Arpeel, P. 22

ARPEL - Fundamentos Ciberseguridad Empresarial

**Ingeniería de ciberresiliencia**

ANTICIPAR

Mantenerse informado de las tendencias del entorno y sus potenciales condiciones adversas

PROTECCIÓN DE DATOS

Productos y servicios digitalmente modificados

MANTENER

Conservar y custodiar la esencia de los controles vigentes a pesar de las condiciones adversas

RECUPERAR

Restaurar los fundamentos de la seguridad y operación durante y después del incidente

EVOLUCIONAR

Ajustar y actualizar los fundamentos de seguridad y privacidad frente a las condiciones adversas actuales o futuras

México tomado de: Brinko, G. y Gresham, R. (2012) Cyber Resiliency and MIT Special Publication 800-63 Rev-4 Corros: Mitre Technical Report, MITR13051. Recuperado de: <https://www.mitre.org/publications/800-63-rev-4-corros>

ARPEL - Fundamentos Ciberseguridad Empresarial

**Resiliencia digital**

Inventario de datos y riesgos	Priorice el inventario de datos y riesgos de negocio, que involucre el nivel ejecutivo de la empresa.
Empleados de primera línea	Móvilice a los empleados de primera línea demostrando el valor de los inventarios de datos.
Integración a procesos	Integre la resiliencia a los ataques a través de todos los procesos de la empresa.
Respuesta a incidentes	Incorpore los mecanismos de respuesta a incidentes en todos los funciones de negocio y mejore éstos con la ejecución de pruebas reales.
Funciones de seguridad	Asegure la integración de las funciones de seguridad en las TICs para incrementar la escalabilidad.
Aseguramiento diferenciado	Implemente la estrategia de seguridad basado en la importancia de los activos más sensibles.
Protección activa	Despliegue los sistemas de protección activa para habilitar la respuesta a los posibles ataques en tiempo real.

México tomado de: McPhee, J. y Swaminathan, A. (2017) Digital @Scale: The playbook you need to transform your company. Hoboken, NJ, USA: John Wiley & Sons, P.244

ARPEL - Fundamentos Ciberseguridad Empresarial



# Ciber-Resiliencia en las Organizaciones

Julio Ardita | CYBSEC



Ciber-Resiliencia en las Organizaciones

Gestión de ciberincidentes

¿Estamos preparados para responder a un incidente de seguridad?  
La respuesta es NO.

Are you prepared to respond to a security breach?

- Hay poca interacción entre SI y OT.
- En el mejor de los casos tenemos CSIRT internos con bajo nivel de madurez y llegada.
- Hay pocos registros con información y casi siempre están implementados por defecto.
- Hay desconocimiento técnico de seguridad informática entre los ingenieros.
- Hay desconocimiento técnico de sistemas OT entre el personal de SI.

Cyber

Ciber-Resiliencia en las Organizaciones

Conclusiones

Nuestra organización debe ser ciber-resiliente para sobrevivir.

Hay que construir puentes con las áreas industriales y concientizar sobre ciberseguridad.

Debemos implementar medidas preventivas para protegernos de ciber incidentes.

Tenemos que estar preparados para gestionar los incidentes de ciberseguridad que vendrán.

Cyber

# Evaluación de situación inicial - como elegir un ciber estándar

Francisco Souto | HONEYWELL

**Failed to Operationalize Cyber Security**

**Did not Change Staffing Levels or Training**

- Did not identify cyber security tasks, activities, and man-hours required to maintain new infrastructure
- Cyber security has its own O&M costs

**Did not Follow Policy**

- Did not audit or enforce their own ICS security policy
- Cyber security requires compliance

**Did not Change Control System Engineering or Maintenance Practices**

- Did not implement security requirements in product selection, design, implementation, testing
- Cyber security must be part of every project (i.e., turnarounds, upgrades, greenfield design)

**Did not Establish a Cyber Security Governance Committee**

- Senior and middle management was unaware and not a priority
- The most effective cyber steering committee I've seen had Senior Managers from each part of the organization. They are informed of cyber security initiatives, projects, progress, audit results, and roadblocks.

EXECUTIVE FORUM

Cyber Security: Governance, Enforcement, Engineering, & Maintenance

**Closing Points**

**As dependence on IT/OT increases, cyber security becomes a business enabler**

**Measuring Performance**

- Do security audits drive your security spending (reacting to risk)?
- Reconsider the framework used for your cyber security program and how you show progress
- The security profiling method shown was effective in showing gaps at a site and enterprise level

**Operationalizing Cyber Security**

- Does it have its own O&M line item?
- Is it part of your engineering and maintenance practices?

**Evaluating Cyber Risk**

- Understanding threats to your business help determine appropriate safeguards

EXECUTIVE FORUM

Cyber Security is a Business Enabler

# Ciberseguridad Industrial: nuevos riesgos y desafíos estratégicos

Andres P Giarletta | KASPERSKY LAB

**ATENCIÓN A LA BRECHA: CIBERSEGURIDAD INDUSTRIAL CON KASPERSKY LAB**



MOTIVACIONES: CIBER RIESGOS Y AMENAZAS

ACCIONES DESTRUCTIVAS

- Impacto no intencional debido a falta de conciencia de ciber seguridad;
- Sabotaje

FRAUDE INDUSTRIAL

- Espionaje industrial
- Fraude operacional del staff

CIBERARMAS

- Algunas soportadas por gobiernos
- Competencia desleal
- Ciber Hoolliganism

KASPERSKY

QUE DIFICULTA LA PROTECCIÓN HOY EN DÍA

- Mezcla de aquí no pasa nada con no nos van a atacar
- Falta de habilidades de ciber seguridad y de practica de ciber seguridad industrial
- La seguridad típica de IT no se puede aplicar en ambientes industriales
- Falta de un dueño de ciber seguridad en el área de OT
- La mayoría de objetivos de los ataques: sistemas viejos, no actualizados difíciles de actualizar, inseguros

KASPERSKY

# El riesgo de Cyber en los mercados internacionales de reaseguro, tratamiento y tendencias de cobertura

Natalia Char | WILLIS GROUP

Jesús González | CYBER AON RISK SOLUTIONS



Andrea Baldassarre | Gerente de Gestión del Riesgo, YPF

### Donde estamos con Cyber?

- La seguridad cibernética es vista como un desafío fundamental y una de las prioridades de las organizaciones.
- Muchas compañías sienten que están en el camino correcto en términos de protección de datos y del manejo de la seguridad de la información.
- Pero la mayoría reconoce que este es un viaje y muchos están mirando como crear una cultura de seguridad cibernética en su organización.
- Muchas amenazas existen alrededor de las conductas de los empleados, y las vulnerabilidades que ellos crean serán una prioridad en los próximos 3 años.
- Las prioridades inmediatas son:
  - Entrenamiento para empleados y contratistas
  - Revisar los gaps de cobertura y considerar comprar amparos

Willis Towers Watson LLP 7

Natalia Char | WILLIS GROUP

### La falta de conciencia de los empleados, procesos ineficientes y falta de presupuesto son los riesgos clave de Cyber

¿En qué medida las siguientes barreras impiden a su organización gestionar eficazmente sus riesgos cibernéticos?

Barrera	La mayoría de las veces / Siempre	En una medida moderada	Hasta cierto punto	Para nada
Comprensión insuficiente de los Riesgos cibernéticos	13%	21%	40%	
Procesos y estructuras ineficientes	7%	25%	29%	
Presupuesto insuficiente	5%	24%	40%	
Entrenamiento insuficiente en riesgos cibernéticos	10%	17%	38%	
Falta de claridad en la estrategia de riesgos cibernéticos	13%	13%	33%	
Falta de experiencia interna	7%	18%	32%	
Falta de compromiso de la dirección en la agenda de Cyber	8%	17%	23%	
Coberturas insuficientes para riesgos cibernéticos	4%	12%	26%	

Willis Towers Watson LLP 11

### Contexto cibernético en evolución

Una mayor aplicación y dependencia sobre tecnologías digitales ha creado exposiciones a eventos cibernéticos para las empresas, que son más complejos, de mayor impacto y exposición.

Dinamizadores tecnológicos → Dinamizadores comerciales → Amenazas estratégicas

Aon Cyber Solutions Group | Proprietary & Confidential

Jesús González | CYBER AON RISK SOLUTIONS

### Evaluar | Evaluar el desempeño de Tecnologías Operativas (TO)

Comprendiendo la efectividad de exposiciones y control para Tecnologías Operativas

Aon utiliza nuestros equipos especialistas en Ingeniería de Riesgos para determinar las exposiciones relacionadas con seguridad

La metodología para evaluar riesgos propiedad de Aon, brinda percepciones granulares a un nivel operativo en el marco de Aon Cyber 360®, permitiendo a los clientes realizar ejercicios de benchmarking sobre sus perfiles de riesgo, promoviendo mejoras continuas e incrementales

Los Elementos Clave de Riesgo Operativo incluyen:

- Protecciones de Activos del Centro de Datos
- Medidas de Protección
- Seguridad Física y Ambiental
- Medidas de Acceso al Control
- Respuesta ante Emergencias

Aon Cyber Solutions Group | Proprietary & Confidential





INFORMES DE EVENTOS

# Fundamentos de la Ciberseguridad Industrial



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.



**Sede Regional:**

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

[www.arpel.org](http://www.arpel.org)