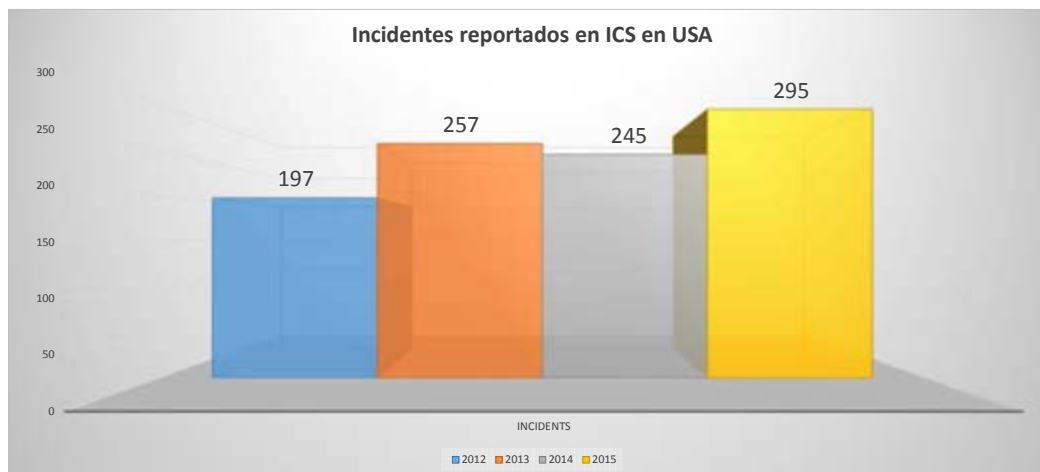


Seguridad sobre infraestructuras críticas

Juan Camilo Reyes Fierro, CISSP
Security Services Leader, SSA Region



Las estadísticas y noticias nos muestran que los ataques a ICS son una realidad creciente.

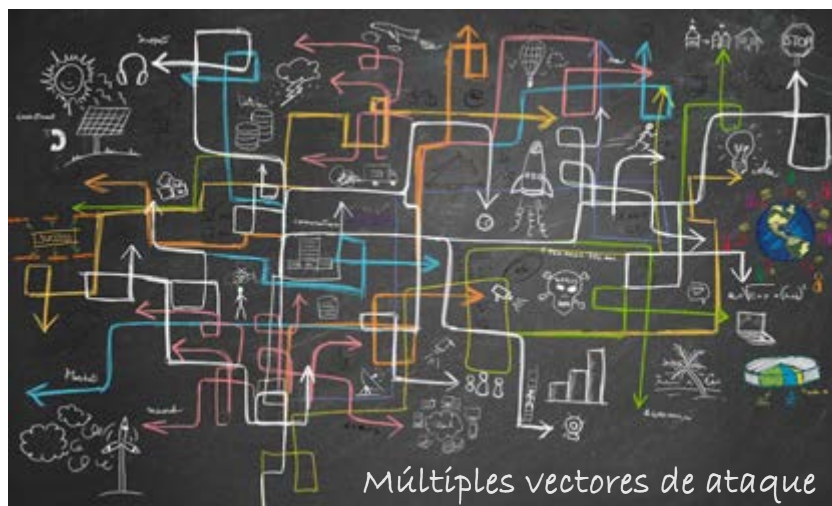


Fuente: NCCIC/ICS – CERT Year in review – FY2015

Qué podemos concluir de los casos más representativos



Qué podemos concluir de los casos más representativos



SEMINARIO LA CIBERSEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS
frente a un mundo tecnológicamente dependiente e interconectado

Logos: aspel, Organización de los Estados Americanos, No brechas por no gobernar, Ministerio de Modernización y Presidencia de la Nación, Ministerio de Economía y Finanzas Públicas, República Argentina

Logos: Kaspersky, Veeva, IBM, SAP, Xerox, Deloitte, EY, Fortinet, Honeywell, Accenture, Microsoft

¡¡¡No existen las tecnologías milagrosas!!!

SEMINARIO LA CIBERSEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS
frente a un mundo tecnológicamente dependiente e interconectado

Logos: aspel, Organización de los Estados Americanos, No brechas por no gobernar, Ministerio de Modernización y Presidencia de la Nación, Ministerio de Economía y Finanzas Públicas, República Argentina

Logos: Kaspersky, Veeva, IBM, SAP, Xerox, Deloitte, EY, Fortinet, Honeywell, Accenture, Microsoft

La seguridad no se logra únicamente con tecnologías

SEMINARIO LA CIBERSEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS
frente a un mundo tecnológicamente dependiente e interconectado

Eliminar los silos entre IT y OT

Figure 1. Stage 1: Cyber Intrusion Preparation and Execution

Figure 2. Stage 2: ICS Attack Development and Execution

Fuente: Sans Institute - The Industrial Control System Cyber Kill Chain

SEMINARIO LA CIBERSEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS
frente a un mundo tecnológicamente dependiente e interconectado

“Considere los riesgos de ciberseguridad en ICS como parte de los procesos de gestión de riesgo organizacional.”

SEMINARIO LA CIBERSEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS
frente a un mundo tecnológicamente dependiente e interconectado

Organización de los Estados Americanos | No Discriminación por Género | Ministerio de Modernización y Presidencia de la Nación | Ministerio de Economía y Finanzas Públicas | República Argentina

KAPROCKY | VFP | IBM | KPMG | xforce | Deloitte | EY | FORTINET | Honeywell | acronis | WatchGuard

10 practicas esenciales para una postura de seguridad robusta

Entender la parte esencial de la seguridad

GOAL:
Intelligent cyber threat protection and risk management

- 1 Construir una cultura basada en riesgo y Sistema de gestión
- 2 Establecer operaciones de seguridad inteligentes y respuesta rápida a incidentes
- 3 Colaboración segura en el sitio de trabajo móvil y social
- 4 Desarrollo de productos seguros, desde el diseño
- 5 Gestión de TI higiénica
- 6 Crear redes seguras y resilientes
- 7 Manejar la complejidad de seguridad de la nube y virtualización
- 8 Gestionar el cumplimiento de seguridad con terceros
- 9 Asegurar la privacidad y seguridad de la información
- 10 Gestionar el ciclo de vida de la identidad digital

SEMINARIO LA CIBERSEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS
frente a un mundo tecnológicamente dependiente e interconectado

Organización de los Estados Americanos | No Discriminación por Género | Ministerio de Modernización y Presidencia de la Nación | Ministerio de Economía y Finanzas Públicas | República Argentina

KAPROCKY | VFP | IBM | KPMG | xforce | Deloitte | EY | FORTINET | Honeywell | acronis | WatchGuard

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- [@ibmsecurity](https://twitter.com/ibmsecurity)
- youtube/user/ibmsecuritysolutions

IBM Security

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

IBM.