



lacnic23

18/22 mayo - lima, Perú



Confianza y valor en los sistemas de información

Lima Chapter

Desarrollo de estrategias de ciberseguridad nacional y protección de infraestructuras críticas

Juan Dávila, MBA, CRISC, CISM, CISA, ISO 27001 LA, ISO 22301 LA, Cobit 5F Acc Trainer

LACSEC 2015



Riesgos y comportamientos

THE INTERNET OF THINGS AT WORK

GLOBAL
WWW.ISACA.ORG/RISK-REWARD-BAROMETER



As wearables and other connected devices increasingly make their way into the workplace, IT professionals still see more risk than benefit. Yet with sound preparation, education and governance, enterprises can be well-positioned to embrace the benefits of the Internet of Things (IoT).

INCREASED SECURITY THREATS



BIG CHALLENGES

DATA PRIVACY

25%

IDENTITY AND ACCESS MANAGEMENT

8%

COMPLIANCE REQUIREMENTS

6%

OWNERSHIP OF TECH AND/OR DATA OUTSIDE OF IT

6%

43%

SAY ORGANIZATION ALREADY HAS OR EXPECTS TO CREATE PLANS FOR INTERNET OF THINGS WITHIN NEXT 12 MONTHS



60%

BELIEVE "BRING YOUR OWN WEARABLE" AND "BRING YOUR OWN DEVICE" ARE EQUALLY RISKY

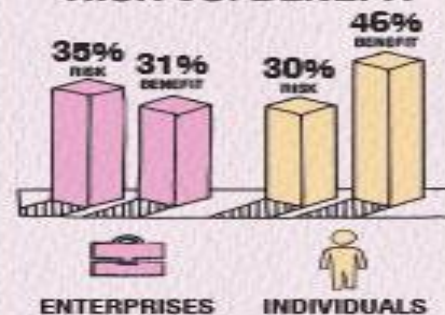


69% VERY CONCERNED
25% SOMEWHAT CONCERNED
4% NOT CONCERNED
2% DON'T BELIEVE IT'S DECREASING

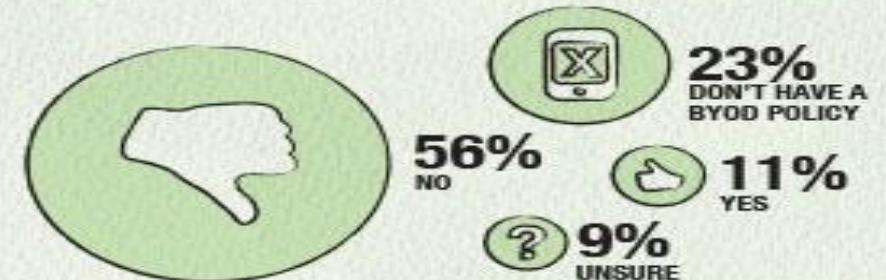
IS PRIVACY DEAD?

Attitude toward decreasing level of personal privacy

INTERNET OF THINGS RISK VS. BENEFIT



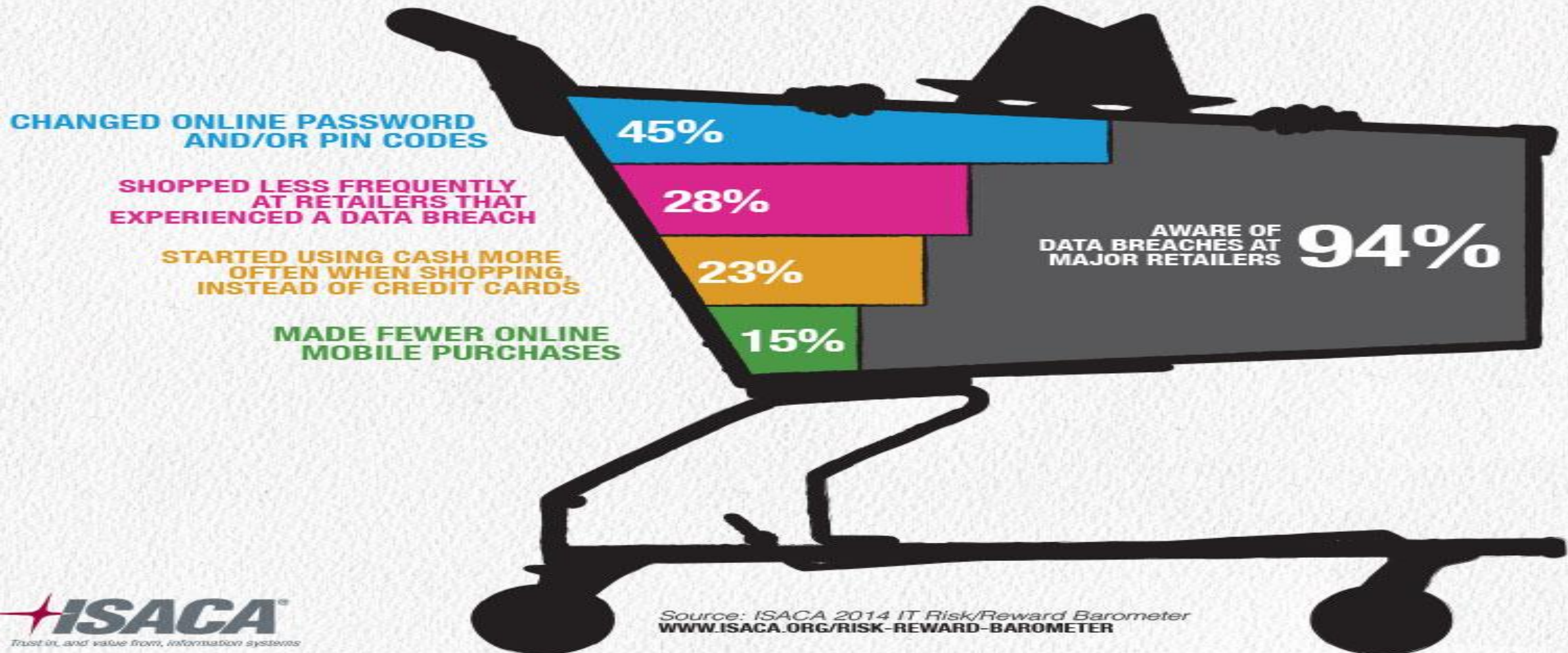
WORKPLACE BYOD POLICY ADDRESSES WEARABLE TECH



Riesgos y comportamientos

DO SHOPPERS CARE ABOUT DATA BREACHES?

Most US consumers are aware of the data breaches at major retailers over the past year. A substantially smaller number changed their shopping behaviors as a result.



Ciber ... qué?



LACSEC 2015

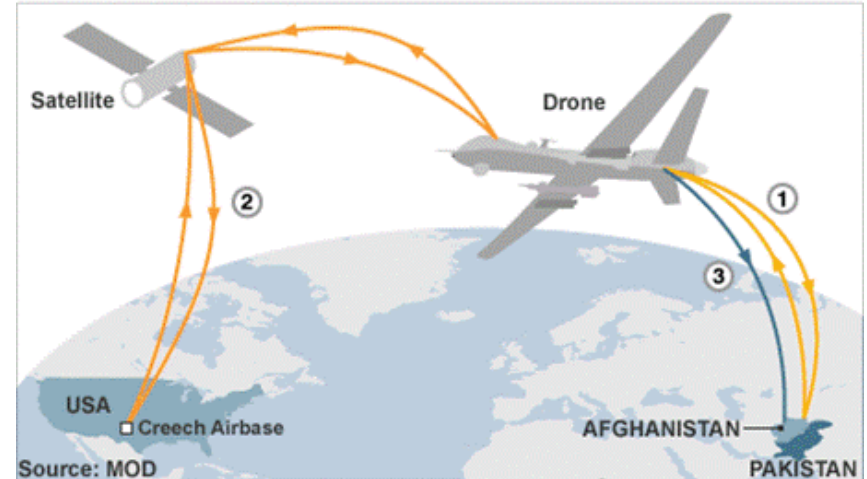
Facts !!!

- “Anyone can simply gather information related to the hacking of drones online with the use of Google” (Esti Peshin, Israel Aerospace Industries Cyber-programs Director).
- El mayor problema con los drones está relacionado con la tecnología obsoleta utilizada en su funcionamiento.
- Todd Humphrey (University of Texas), demostró, con aprox. US\$ 1,000 en equipos y pocos colaboradores, la capacidad de enviar señales al GPS de un drone militar, secuestrarlo en el aire y controlar su ruta.

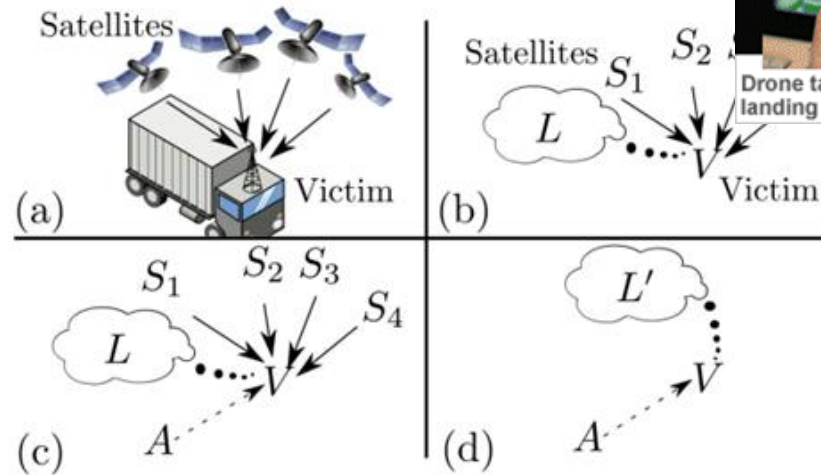
Ciber ... qué?



How drones work



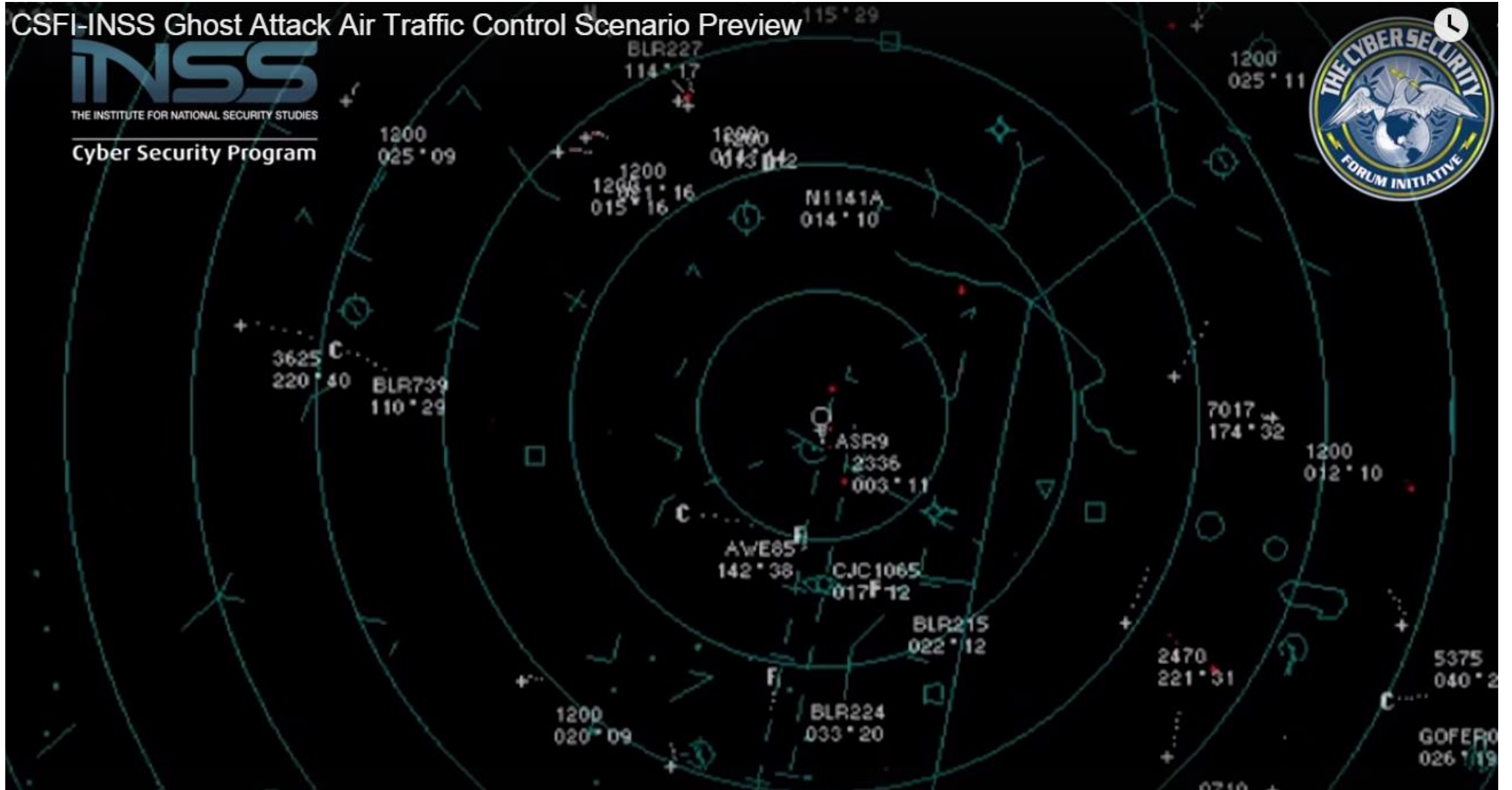
Source: MOD



Ataques y ... más ataques



Ataques y ... más ataques



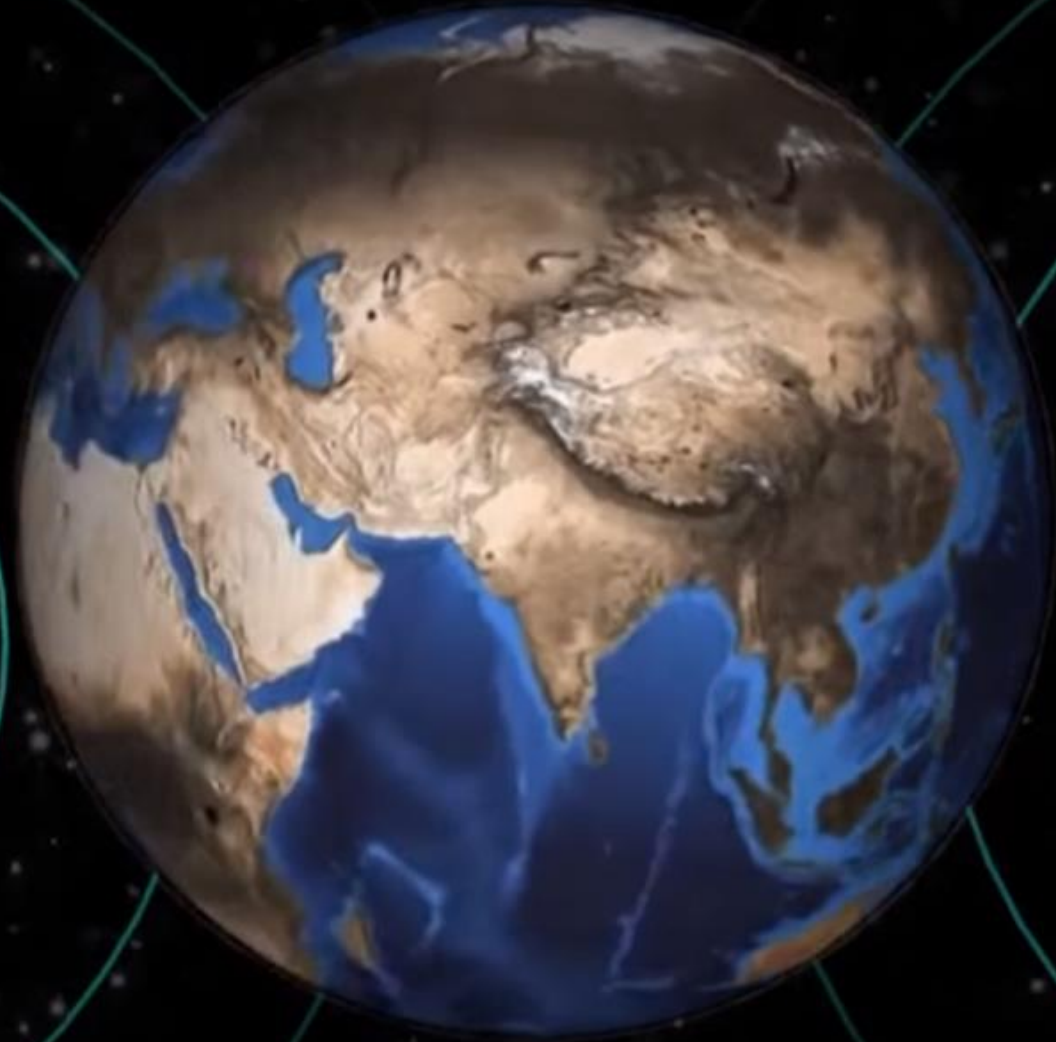
Ataques y ... más ataques

CSFI-INSS Ghost Attack Air Traffic Control Scenario Preview

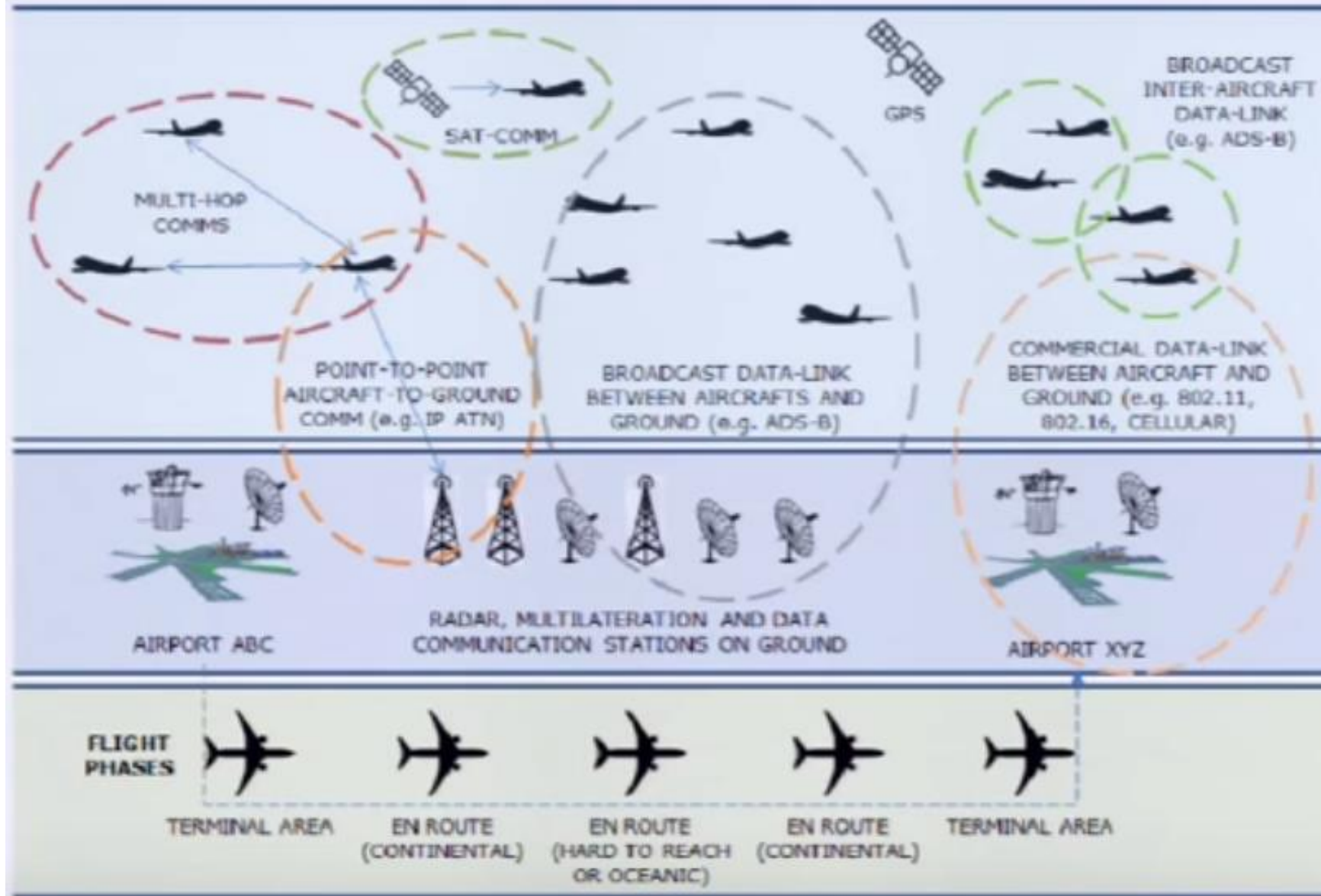
INSS

THE INSTITUTE FOR NATIONAL SECURITY STUDIES

Cyber Security Program



Ataques y ... más ataques



Ataques y ... más ataques

CSFI-INSS Ghost Attack Air Traffic Control Scenario Preview

INSS

THE INSTITUTE FOR NATIONAL SECURITY STUDIES

Cyber Security Program



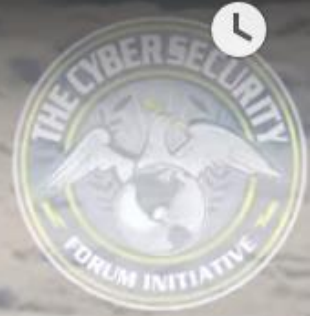
Ataques y ... más ataques

CSFI-INSS Ghost Attack Air Traffic Control Scenario Preview

INSS

THE INSTITUTE FOR NATIONAL SECURITY STUDIES

Cyber Security Program

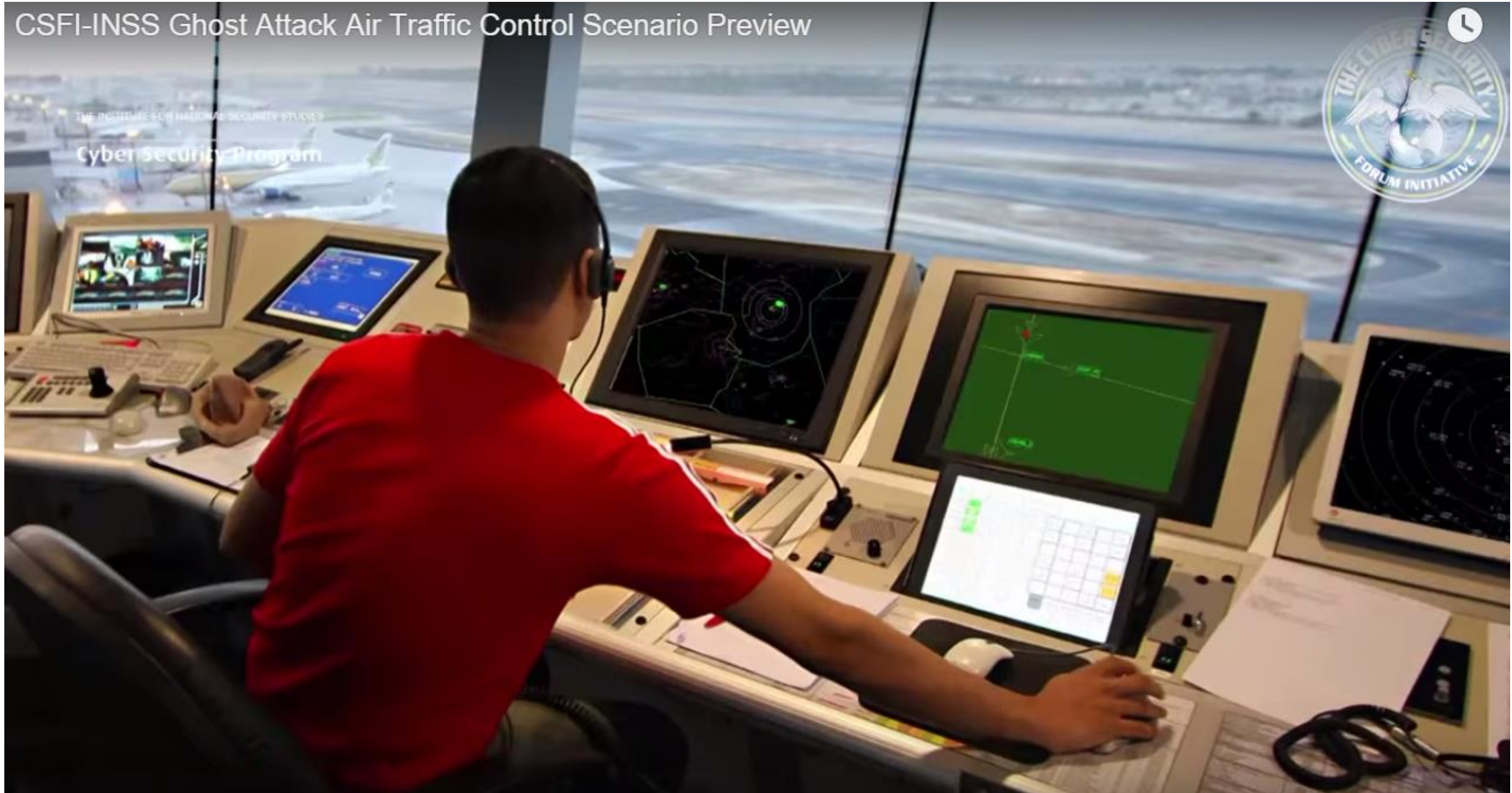


Ataques y ... más ataques

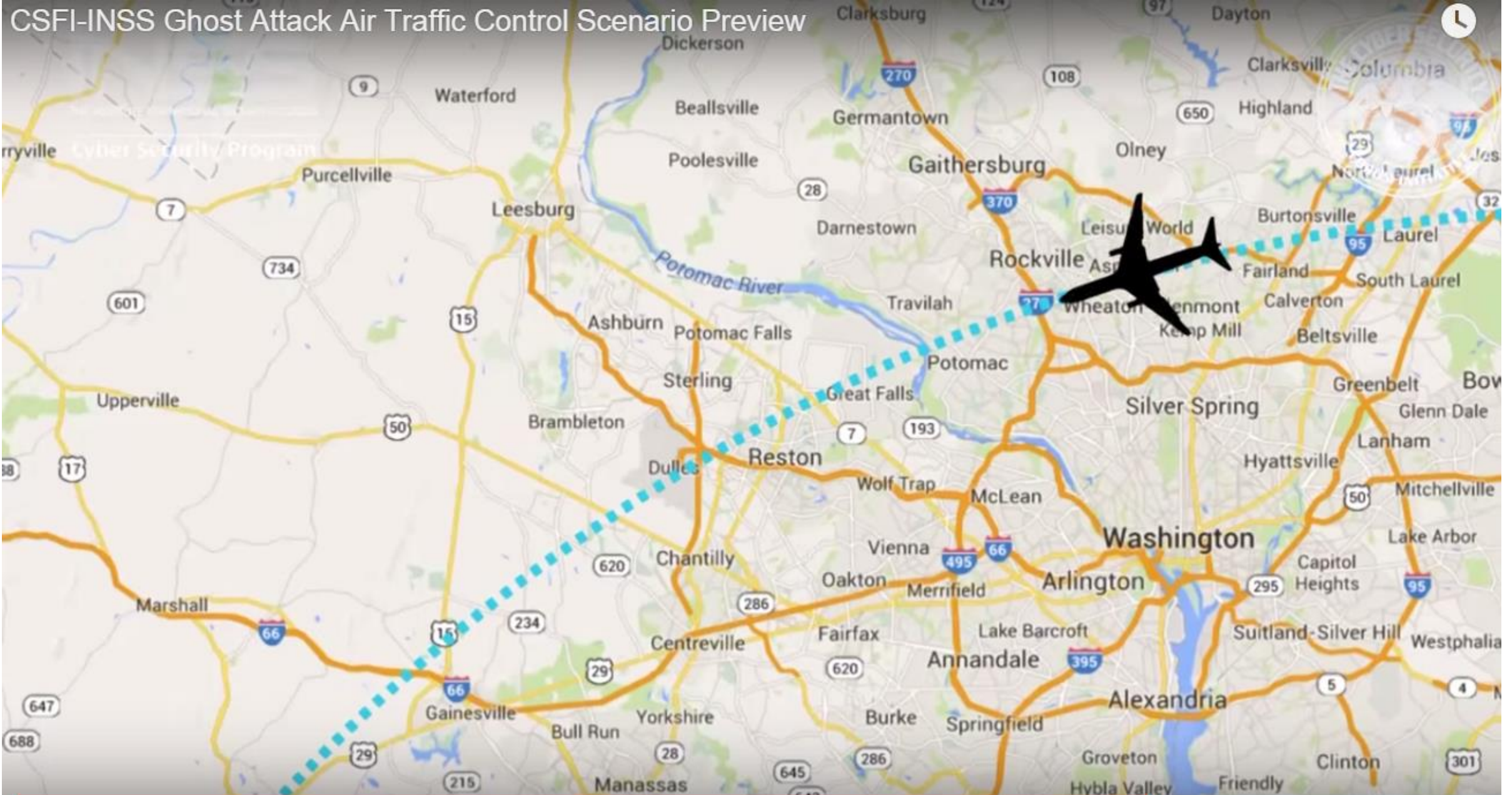
CSFI-INSS Ghost Attack Air Traffic Control Scenario Preview

THE INSTITUTE FOR NATIONAL SECURITY STUDIES

Cyber Security Program



Ataques y ... más ataques



Ataques y ... más ataques

CSFI-INSS Ghost Attack Air Traffic Control Scenario Preview

INSS
THE INSTITUTE FOR NATIONAL SECURITY STUDIES

Cyber Security Program

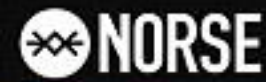


**BREAKING
NEWS**

MID-AIR COLLISION

343 DEATHS

Más hechos !!!



ATTACK ORIGINS

#	Country
907	United States
574	China
77	Netherlands
70	Russia
67	Austria
51	Hong Kong
48	Thailand
47	Taiwan
44	France
38	Mil/Gov

ATTACK TARGETS

#	Country
1371	United States
73	Hong Kong
55	Thailand
39	Netherlands
34	Portugal
32	Turkey
31	Canada
30	Liechtenstein
23	Austria
23	Norway

ATTACKS

Timestamp	Organization	Attacker Location	P	Target Location	Service	Port
2014-06-26 10:57:53.23	TheInfo-RD clients [WebDC]	Moscow, Russia	188.120.225.71	unknown, Austria	http	80
2014-06-26 10:57:54.85	Allyan Computing Co., LTD	Hangzhou, China	182.92.75.26	San Francisco, United States	unknown	33435
2014-06-26 10:57:54.86	N/A	unknown, Chile	190.110.121.93	San Francisco, United States	unknown	33435
2014-06-26 10:57:57.57	TheInfo-RD clients [WebDC]	Moscow, Russia	188.120.225.71	unknown, Austria	http	80
2014-06-26 10:57:57.53	TheInfo-RD clients [WebDC]	Moscow, Russia	188.120.225.71	unknown, Austria	http	80
2014-06-26 10:57:57.53	TheInfo-RD clients [WebDC]	Moscow, Russia	188.120.225.71	unknown, Austria	http	80
2014-06-26 10:57:57.54	TheInfo-RD clients [WebDC]	Moscow, Russia	188.120.225.71	unknown, Austria	http	80
2014-06-26 10:57:57.53	TheInfo-RD clients [WebDC]	Moscow, Russia	188.120.225.71	unknown, Austria	http	80

ATTACK TYPES

#	Service	Port
524	vnc	5900
241	unknown	33435
180	http	80
143	http-alt	8080
126	ssh	22
94	microsoft-ds	445
67	sip	5060
64	telnet	23

Son varios ataques...
bueno, más que varios



Ciberseguridad – Objetivo

- Utilización segura y efectiva de la infraestructura crítica, a través de capacidades nacionales de prevención, identificación, defensa, respuesta y recuperación ante ciberataques.

Protección de infraestructuras críticas



Ciberseguridad

- Desafíos y soluciones para gestionar el ambiente multi-amenazas: Cibertaquas, desastres naturales, escenarios de guerra, cambio climático, ...
- Sector público y privado: centrales hidroeléctricas, Camisea, puertos, bancos, etc.) ¿Cuál es el impacto de esto?
- Probabilidades, amenazas, seguridad, medio ambiente, servicios públicos, etc.
- ¿Cómo es la ciberseguridad ahora?
- Personas – Procesos – Tecnología:
 - Seguridad en 8 capas.
 - ¿Es suficiente?

Cibercrimen

- Se cometen fácilmente.
- Cualquiera es capaz de hacerlo bajo la percepción de anonimato e impunidad.
- Posibilidad de obtención de rápidos beneficios/daños.
- Relación costo/beneficio altamente conveniente
- La ubicuidad genera desafíos jurisdiccionales y legales.
- Costo de un ciberataque: € 435.000 (M.O., Hw, Sw, indemnizaciones. No incluye lucro cesante). Fuente: Symantec – *Costo del Cibercrimen*.

Protección de infraestructuras críticas

- Las ciberamenazas son una realidad latente. En cualquier momento, y sin que lo sepamos, podemos ser objetivos de algún tipo de ciberataque capaz de paralizar las operaciones de las IC.
- Los desafíos, más que técnicos, son estratégicos, políticos, sociales y culturales.
- Resiliencia ante ciberataques a la IC.



Construir ciber-resiliencia

- Respuesta técnica: Backup, redundancia, alta disponibilidad, etc.
- Respuesta estratégica: Política integral de PIC:
 - Aspectos políticos, sociales, económicos, oragnizacionales, respaldados por una autoridad nacional efectiva.
 - Esquemas mixtos y masivos de colaboración, local, nacional, regional y global.
- Complejo????
- Si consideramos el contexto actual de los servicios públicos , el desafío es
- Algunos países ni siquiera pueden defender su orden interno,...
- Se requiere dedicar recursos para proteger el ciberespacio y las IC.

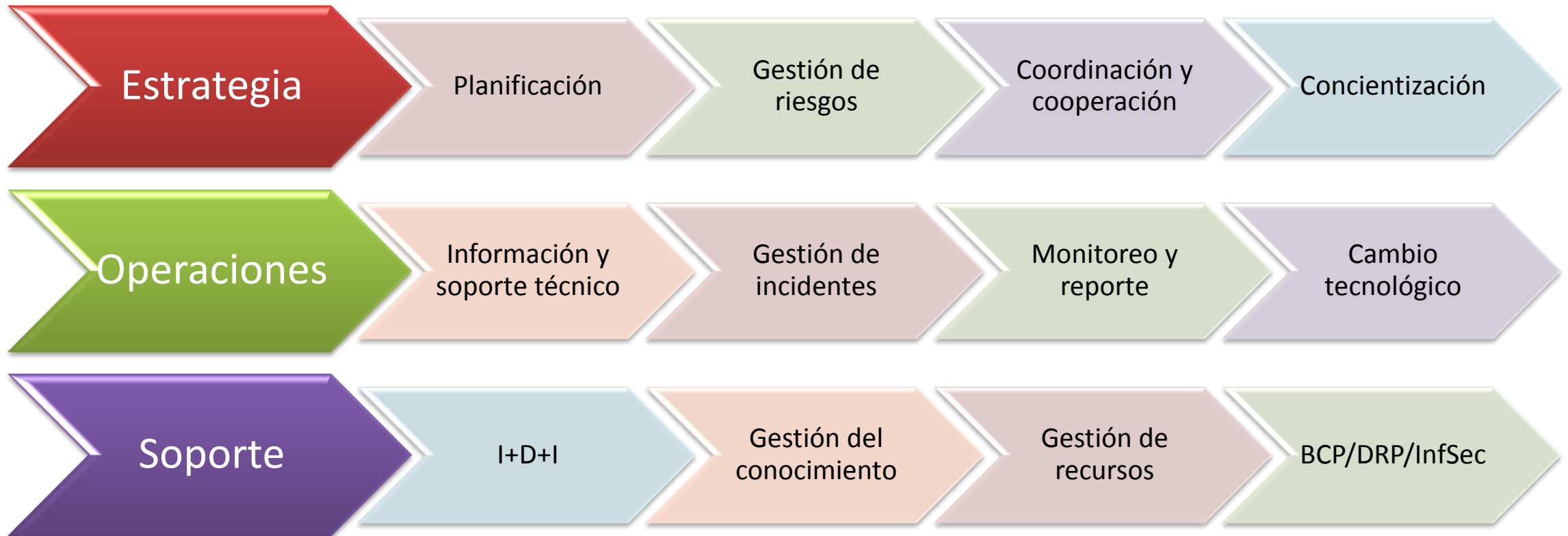


www.ami.com

American Megatrends

Keyboard not found
Press F1 to Resume

Ciberseguridad– Estructuras organizativas



Ciberseguridad – Hacia la sociedad segura !!

- ¿Cómo estiman que será la actitud ciudadana al respecto? ¿En 5 años?
- ¿Hacemos una apuesta?
- Sociedad cibersegura:
 - Cybercrimen, Ciberterrorismo, Privacidad, Confianza.
- Sociedad resiliente.

Ciberseguridad - Awareness



Ciberseguridad – ¿Qué se requiere?

- Definir un marco normativo.
- Definir una estructura organizativa.
- Definir planes estratégicos y operativos.
- Asignar recursos.
- Concientizar !!!
- Medir y mejora continua.

Estrategias ...

- Comando centralizado: Autoridad, coordinación, recursos, ...
 - Equipos multidisciplinarios de apoyo.
 - CERTs.
- Inventario de IC (público y privado).
- Estrategias sectoriales.
- Evaluación de riesgos.
- Planes de acción articulados (público, privado y ciudadanía). Son responsabilidades compartidas.
- Monitoreo y reporte: Verificaciones de efectividad: Testing, auditorías, certificaciones, ...

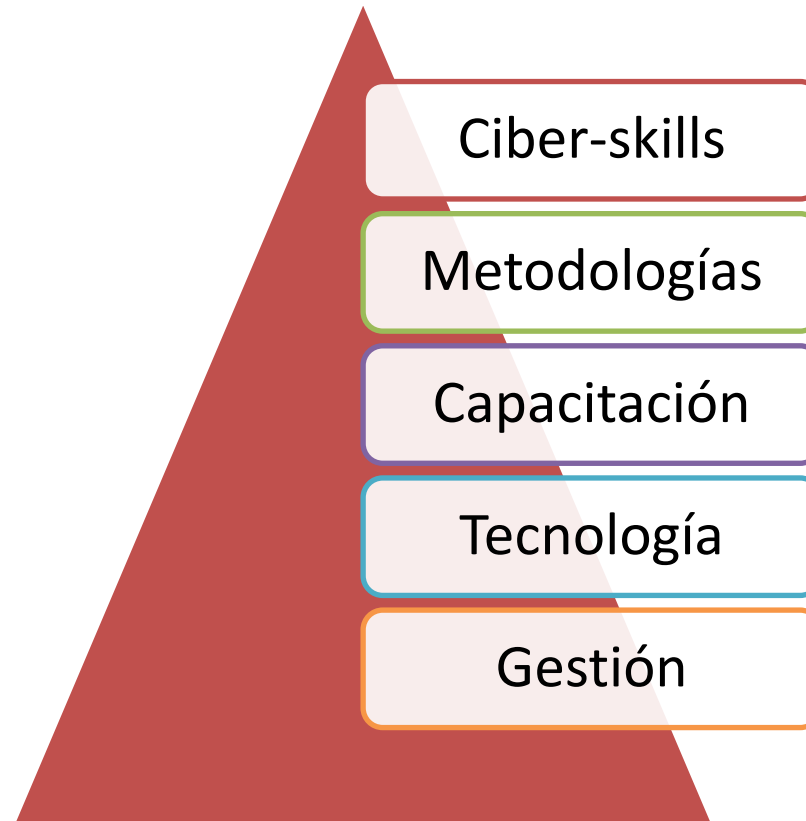


Estrategias de ciberseguridad – Drivers

- Jurisdicción.
- Colaboración.
- Coordinación.
- Autonomía
- Efecto inmediato.
- Marco jurídico.



Ciberseguridad – Competencias





Ciberseguridad – Necesidades

- Pocos expertos
- Amenazas multidireccionales.
- Riesgos cambiantes.
- Privacidad.



Ciberseguridad – Nivel Personal



Ciberseguridad – Nivel organizacional



Ciberseguridad – Nivel global

- Ciber-terrorismo.
- Cooperación internacional.



Ciberseguridad – Nivel cultural

- Es un estilo de vida.
- Todos debemos evangelizar en forma multidireccional.



Aprendamos !!

- La tecnología nos desborda, a nivel personal y a nivel organizacional.
- Al parecer nuestra actitud al respecto es ...
- Realmente pensamos que es un problema de alguien más, y que ese alguien hará algo, y no sabemos qué !!!
- ¿Entonces, el tema es cultural?
- ¿A qué nivel: personal, organizacional, nacional, regional, global?
- Cultivar la conciencia alrededor del riesgo en general, y a los riesgos tecnológicos en forma específica, es
- Y bueno. ¿Qué estamos haciendo al respecto?

Aprendamos a aprender !!

- Reconozcamos el impacto del cibercrimen, en cualquiera de sus formas.
- Las organizaciones cibercriminales son organizadas, especializadas y hasta sofisticadas, por tanto, hay que analizarlas y enfrentarlas como tales (organizaciones con objetivos estratégicos, rentables, con disponibilidad de recursos, etc.)
- En este momento no hay buenas noticias, porque, hagamos lo que hagamos en PIC, ...

Aprendamos a aprender a aprender!!

- El cibercrimen opera en nuestras comunidades, por tanto, están más integrados con nosotros de lo que creemos. La información está disponible para cualquiera...
- Reconozcamos que con nuestro actual enfoque cultural somos cómplices de su acción y crecimiento, y garantizamos su impunidad.
- Se aprovechan de nuestro desconocimiento !!!
- Más aún, saben que no nos involucraremos !!!

¿Entendemos de qué se trata todo esto?

- ¿Estamos seguros de haber entendido el significado de la ciberseguridad y sus desafíos?
- ¿Estamos conscientes del nivel de compromiso que requiere de todos nosotros?
- ¿De qué niveles estamos hablando: Individual, organizacional, institucional, nacional, global?

Desarrollo de estrategias de ciberseguridad y protección de infraestructuras críticas

Ing. Juan Dávila, MBA, CRISC, CISM, CISA, ISO 27001 LA, ISO 22301 LA, Cobit 5F Trainer
jdavilara@gmail.com



LACSEC 2015