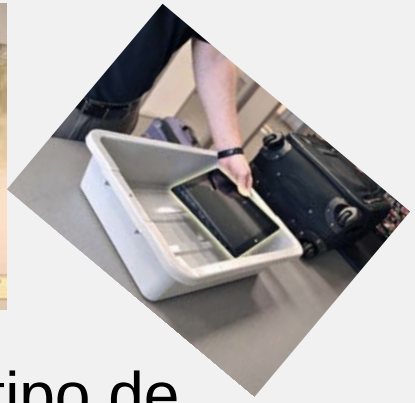
LA CIBERSEGURIDAD EN LA AVIACIÓN CIVIL. Perspectivas desde una aerolínea.

Alicia Sorroza, Subdirectora Security, Grupo Aeroméxico
Gerardo Quintanilla, Gerente de Operaciones de Ciberseguridad, Grupo Aeroméxico

ICAO WORKSHOP
Cybersecurity in Aviation
Mexico City, 4-6 December 2018

HOY…

Acto de interferencia ilícita: enfoque fundamentalmente basado en amenazas fisicamente y tangibles.



Medidas de mitigación basadas en ese tipo de amenazas y en que los autores o responsables están cercanos o involucrados en el vuelo.

Amenaza a la aviación civil es dinámica y cambiante, entre la más alta tecnología
Y artefactos improvisados y “caseros”

La **ciberamenaza** irrumpe en la seguridad de la aviación civil con otras premisas

Debemos estar preparados para **TODO!!**

El GASeP (2017) entre sus acciones globales incorpora identificar y enfrentar las ciberamenazas a la seguridad de la aviación civil.

"*Solo una voluntad política sostenida, especialmente en los más altos niveles de los gobiernos y de la industria, puede asegurar el éxito del GASeP*," Secretaria General, Dra. Liu.

Papel clave del la **INDUSTRIA**

DESAFÍOS

• Estructura y recursos internos diferenciados hacia el interior de los actores.

- Seguridad de la Aviación Civil
- Ciberseguridad, enfoque técnico

ENFOQUES DIFERENTES: UN MISMO OBJETIVO

"La Seguridad es lo primero"

DESAFÍOS

Proceso de Aprendizaje: de todos los stakeholders

DESAFÍOS

•Análisis de riesgo

•Dificultades para compartir información entre los distintos involucrados.

•Nuevas implementaciones y avances tecnologicos para la facilitación, experiencia al cliente, seguridad, eficiencia operativa….

• Cultura de seguridad (falta de…/ insuficiente) necesidad de trabajar la sensibilización y el conocimiento ante ciberamenazas

ALGUNAS INICIATIVAS

- Mejora de capacidades y recursos internos
- Buenas prácticas a nivel industria
- Ser líderes y pioneros en ciberseguridad
- Apoyar la implementación del GASeP
  - Security Focus Group para America Latina (IATA)

IATA AVIATION SECURITY STRATEGY - THE AMERICAS Nov 2017

Purpose

Security is critical for the growth and sustainability of the global aviation industry. There is a need to monitor the security threats to aviation and a need to understand the regional risk picture. The Strategy provides the framework and apparatus (Americas Regional Security Focus Group) to work together to deliver agreed security objectives to meet current and emerging security challenges within the region. These objectives are consistent with the IATA SEG strategy and the ICAO GASeP.

Objective

To establish regional, risk-based security priorities that will
effectiveness of global and regional aviation security by having
measurable outcomes; clear accountabilities; regional inp
commensurate with regional risks.
Ensure a regional voice championing regional needs, highlightin
seeking opportunities and leveraging our strengths.
The Focus Group believes that the five ICAO GASeP priorities
consistent with the regional needs and the IATA SEG priorities. IATA
priorities via the 10 Focus Group Activities to deliver an action or wor
approved by the Chair of the Focus Group. IATA will provide the
support to the Focus Group.

GASeP Priorities - Industry Application

a) **Enhance risk awareness and response**. Understanding risk is essential for policies and measures to be effective, proportionate and sustainable. Undertaking risk assessments will help to identify gaps and vulnerabilities, which can then be addressed in the most practical way possible, and with optimal use of resources.
b) **Develop security culture and human capability**. The promotion of effective security culture is critical to achieve good security outcomes. A strong security culture must be developed from the top management across and within every organization. The existence of a well-trained, motivated and professional work force is a critical prerequisite for effective aviation security.
c) **Improve technological resources and foster innovation**. Promoting and applying better technological solutions and innovative techniques can provide the tools for enhancing security effectiveness while ensuring operational efficiency.
d) **Improve oversight and quality assurance**. Effective quality control and oversight

Focus Group Activities:

1. Monitoring regional threats, challenges and opportu
2. Encouraging and sharing industry best practice;
3. Developing a security culture with all stakeholders
   region;
4. Identifying sustainable (and where possible harmo
   security measures;
5. Encouraging innovation and technology;
6. Balancing facilitation needs;
7. Adhering to risk based methodology to manage risk
8. Coordinating effective regional lobbying;

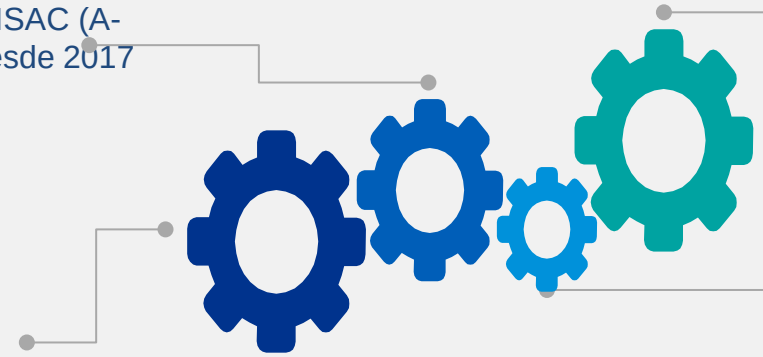
CULTURA DE SEGURIDAD

- Desde una perspectiva integral
- Diagnóstico de la cultura de seguridad: en colaboración con IATA
- Plan de transformación de la cultura de seguridad
- Desarrollo de buenas prácticas y programa piloto dentro del Security Focus Group

Colaboraciones estratégicas

Miembro de Aviation ISAC (A-ISAC) desde 2017

Colaboración táctica con proveedores de servicios del sector y Ciberinteligencia



Colaboración con la Policía Federal -División Científica Participación en la 4ta. Semana de Ciberseguridad: "*Colaboración pública y privada en el sector aeronáutico*"

IATA – Miembro observador de I-SQG (Information Security Quality Group) -2018

Datos Personales / Datos de Tarjeta

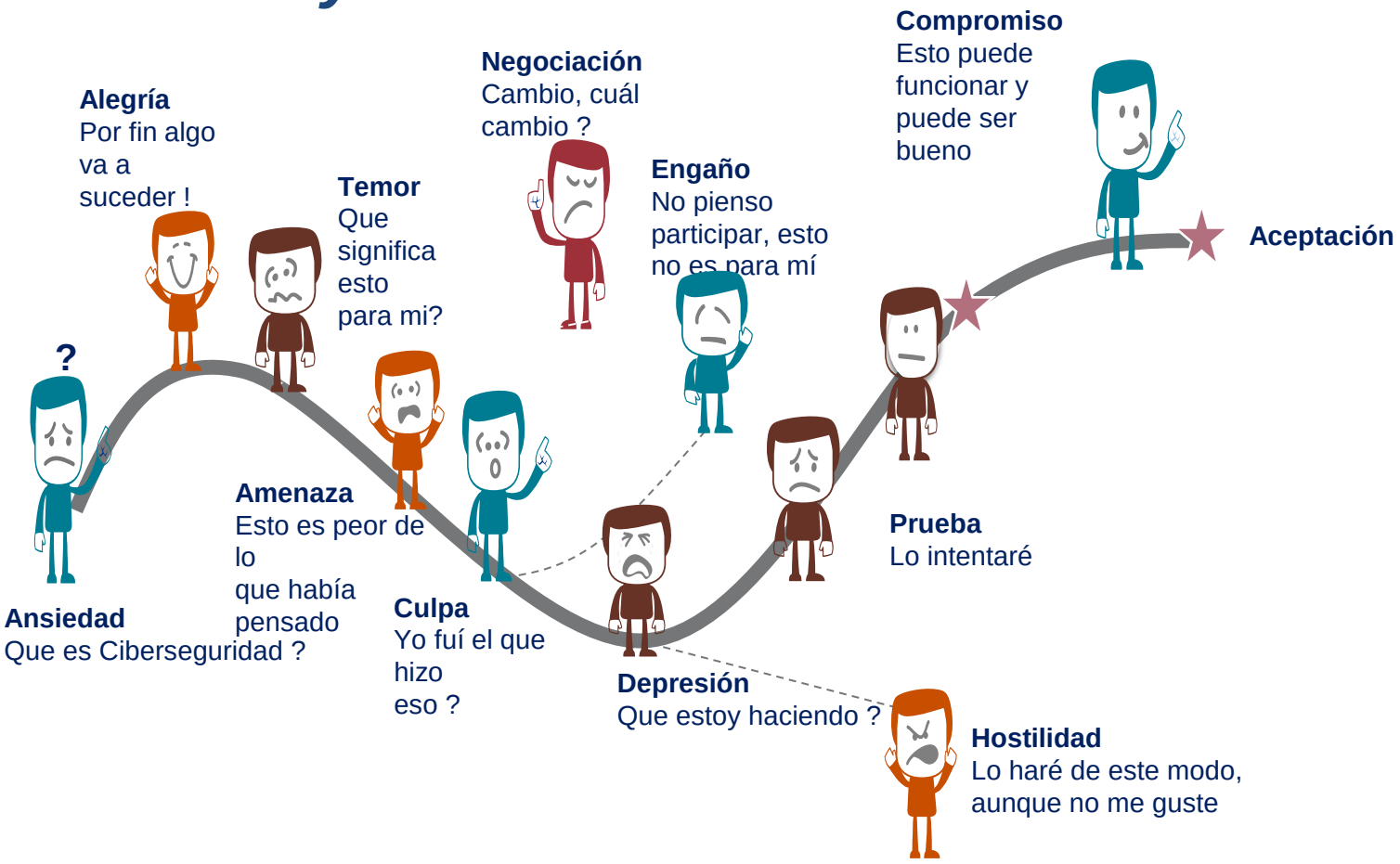
PCI

GDPR

Marco Regulatorio
TI
(ISO 27002)

Gestión de
Terceras
Partes

Programa de Sensibilización y Cultura de Cambio



La actitud de las personas durante un cambio son categorizados dentro del proceso que incluye estos cinco momentos

TLP
GREEN

Un entorno de confianza

De que manera la industria aeronáutica colabora en las mejores prácticas de seguridad relacionadas a las plataformas intermodales, sistemas de pago, marcos de referencia, infraestructura TI e inteligencia de amenazas ?

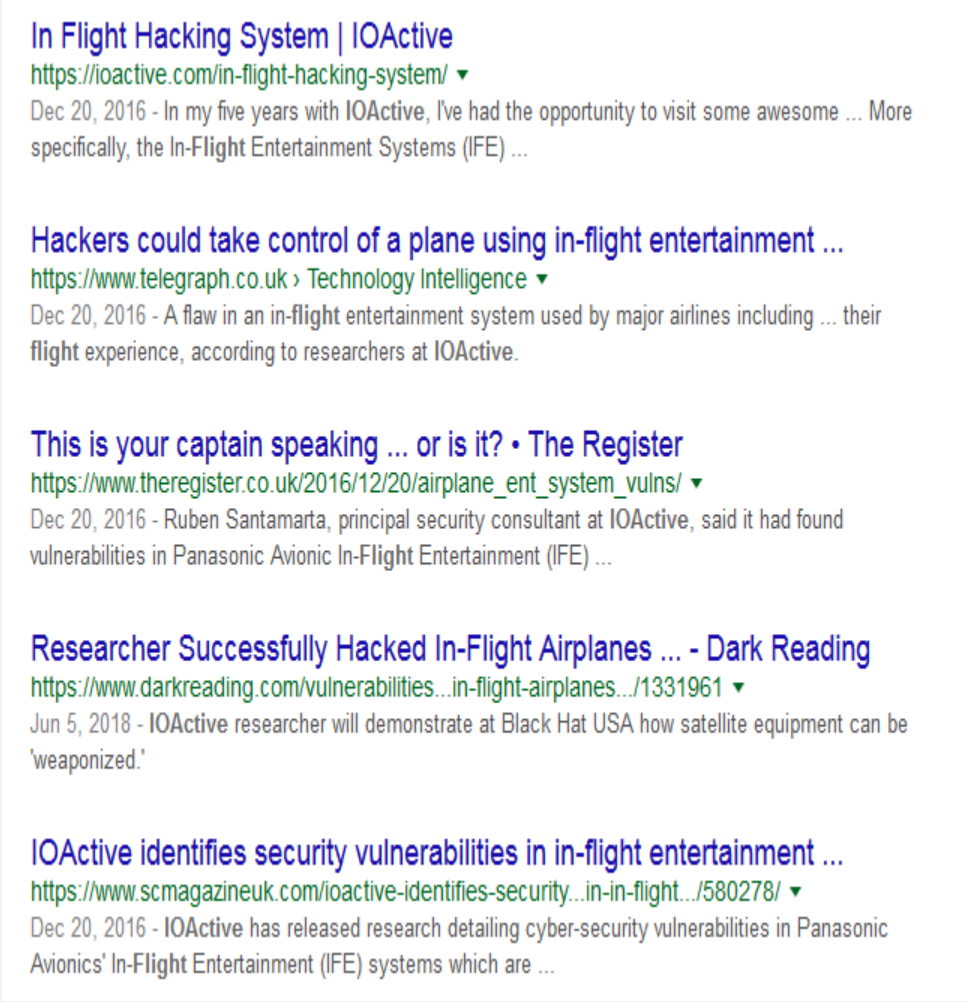
- Areas de interés comunes
- Confianza
- Entorno Seguro
- Colaboración

Antecedentes (Casos teóricos)

IOActive®

2016

Planteamiento Teórico / Hipotético



In Flight Hacking System | IOActive
https://ioactive.com/in-flight-hacking-system/ ▾
Dec 20, 2016 - In my five years with **IOActive**, I've had the opportunity to visit some awesome ... More specifically, the In-**Flight** Entertainment Systems (IFE) ...

Hackers could take control of a plane using in-flight entertainment ...
https://www.telegraph.co.uk › Technology Intelligence ▾
Dec 20, 2016 - A flaw in an in-**flight** entertainment system used by major airlines including ... their **flight** experience, according to researchers at **IOActive**.

This is your captain speaking ... or is it? • The Register
https://www.theregister.co.uk/2016/12/20/airplane_ent_system_vulns/ ▾
Dec 20, 2016 - Ruben Santamarta, principal security consultant at **IOActive**, said it had found vulnerabilities in Panasonic Avionic In-**Flight** Entertainment (IFE) ...

Researcher Successfully Hacked In-Flight Airplanes ... - Dark Reading
https://www.darkreading.com/vulnerabilities...in-flight-airplanes.../1331961 ▾
Jun 5, 2018 - **IOActive** researcher will demonstrate at Black Hat USA how satellite equipment can be 'weaponized.'

IOActive identifies security vulnerabilities in in-flight entertainment ...
https://www.scmagazineuk.com/ioactive-identifies-security...in-in-flight.../580278/ ▾
Dec 20, 2016 - **IOActive** has released research detailing cyber-security vulnerabilities in Panasonic Avionics' In-**Flight** Entertainment (IFE) systems which are ...

Supuestos riesgos (descartados)

IOActive

2018

Documentación Técnica / Propuesta

Attackers may:

- Perform attacks against 3rd party satellites by influencing into the antenna pointing algorithm and other parameters, such as the EIRP, which may cause a disruption of critical communication services

- Perform cyberphysical, by radiating attacks against aircraft actuators, sensors and/or other antennas as long as they're located in the range of the azimuth and the elevation is supported by the Antenna, which are 360º and 0-90º respectively.

This may pose a safety risk.

- Disrupt In-Flight network connectivity
- Inject malicious data into passenger and/or crew's communications.
- Intercept network traffic on-board

"Facilitar la colaboración a través de la industria aeronáutica global para impulsar nuestra habilidad de responder ante vulnerabilidades, incidentes y amenazas, diseminar en tiempo con información oportuna entre los miembros afiliados, y funcionar como un canal de comunicación primario en el sector"

WORK IN PROGRESS!!!

GRACIAS!!