

**XIII
JORNADAS
STIC
CCN-CERT**



Ciberseguridad Aeroespacial



**COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD**

#XIIIJORNADASCCNCERT



COL. Fernando A. Acero Martín

Director de Ciberdefensa del EA

JSTCIS / EJÉRCITO DEL AIRE

Índice

- 1. Escenario y amenazas**
- 2. Ejemplos de ciberataques a comunicaciones no protegidas**
- 3. Problemas estructurales del sector**
- 4. Posibles soluciones**

Ciberseguridad Aeroespacial

Escenario y amenazas I/III

- ACTORES QUE COMPARTEN LOS MEDIOS PERO CON DISTINTOS OBJETIVOS Y MOTIVACIONES:
 - HACKTIVISMO
 - CIBERCRIMEN
 - CIBERTERRORISMO
 - CIBERESPIONAJE
 - CIBERGUERRA
- EL MONOPOLIO DE LA VIOLENCIA YA NO ES DE LOS ESTADOS, SE HA ROTO LA PAZ DE WESTFALIA.
- PROBLEMAS COMPARTIDOS CON OTROS SECTORES POR CONVERGENCIA IT/OT.
- EL ECOSISTEMA AEROESPACIAL ES CIBERDEPENDIENTE Y MUY COMPLEJO.



Ciberseguridad Aeroespacial

Escenario y amenazas II/III

EL MUNDO Edición España Versión Móvil

Noticias | Tecnología | Economía | Deportes | Cultura | Opinión | Internacional | Mundo | España | País | Aplicaciones | Opinión

SEGURIDAD Informática

Berlín atribuye a espías extranjeros un 'ciberataque' a su centro aeroespacial

DE - Berlín
Actualizado: 13/03/15 11:08 horas

El Centro Aeroespacial Alemán (DLR) lleva meses defendiéndose de un ciberataque que las autoridades alemanas, por su entidad y complejidad, atribuyen a un servicio secreto extranjero, avanzó el periódico Die Welt.

Noticias Relacionadas

- La jubilación de Windows XP, un gran dolor de cabeza para China
- Así se saltan los filtros de censura en Internet
- No es un pájaro, es un dron
- Símbol, cuatro años marca dentro de una moneda
- La Comunidad de Madrid ahorra 27 millones de euros en medicamentos para hospitales

Más leídas

- Tendrá presencia su arma contra los ataques las

La seguridad aérea amenazada por nuevos riesgos como drones o ciberataques

lainformacion.com
jueves, 04/12/14 - 18:47

Los "exitosos" resultados de la gestión de la seguridad aérea seguirán poniéndose a prueba en el futuro por nuevos casos de riesgo posibles provocados por ciberataques o drones de uso comercial, según un informe de la aseguradora Allianz Global Corporate and Specialty (AGCS), que presta su servicio al sector de la aviación.

Temas Accidentes aéreos y espaciales | América | Asia | Estados Unidos | Europa | Tecnología (general) | Transporte aéreo | África

Madrid, 4 dic.- Los "exitosos" resultados de la gestión de la seguridad aérea seguirán poniéndose a prueba en el futuro por nuevos casos de riesgo posibles provocados por ciberataques o drones de uso comercial, según un informe de la aseguradora Allianz Global Corporate and Specialty (AGCS), que presta su servicio al sector de la aviación.

El estudio señala que la probabilidad de ciberataques va a ser cada vez mayor, porque los aviones de nueva generación están muy expuestos al cibercrimen por el uso generalizado de redes de datos, sistemas informáticos incorporados y sistemas de navegación.

Asimismo, se prevé un aumento de los drones (vehículos aéreos no tripulados o UAV) de uso comercial, la reducción en un futuro de mano de obra cualificada, como son los pilotos, y un incremento de las turbulencias que genera el cambio climático.

comentar

0 0

Twitter 0 0

Recomendar 0 0

La FAA reconoce que fue víctima de un ciberataque a principios de año

Publicado: 7 abr 2015 19:44 GMT



Control aéreo de EEUU es vulnerable a ciberataques

WASHINGTON.- Una de las áreas débiles es la capacidad de prevenir y detectar acceso sin autorización a la amplia red de sistemas de cómputo y comunicación que utiliza la FAA para procesar y rastrear vuelos alrededor del mundo, señala el informe

ALTO PELIGRO | 03 de Marzo de 2015



El sistema para guiar aviones y otras aeronaves en Estados Unidos corre un "riesgo incrementado e innecesario" de sufrir ataques cibernéticos, indica un informe. (AP)

WASHINGTON.- AP

Ciberseguridad Aeroespacial

Escenario y amenazas III/III

INTERCEPTACIÓN DE VÍDEO DE DRONES (IRAK Y AFGANISTÁN 2009).

SPOOFING DE GPS DE UN SENTINEL AMERICANO (2011).

ATAQUE A AERONAVES A TRAVÉS DE INFRAESTRUCTURAS IT (2011) (AUTOMOCIÓN 21,4%).

SPOOFING DE GPS DE DRONES CIVILES (2012).

INFECCIÓN DE SISTEMAS EMBARCADOS A TRAVÉS DE WIRELESS (2012).

SPOOFING DE AERONAVES CON MENSAJES ADS-B (2012).

TRACKING DE AVIONES (BARR) MEDIANTE ADS-B (2012).

ATAQUE A FMS MEDIANTE MENSAJES ADS-B Y ACARS (2013).

ATAQUE A SISTEMAS CRÍTICOS DE MISIÓN MEDIANTE INTERFACES DISPONIBLES.

VULNERABILIDADES DE SISTEMAS COTS (EFB).

SPANAIR 5022 TROYANO EN ORDENADOR DE MANTENIMIENTO (2008).

Ciberseguridad Aeroespacial

Ejemplos de ataques a comunicaciones no protegidas

- PROBLEMA DE FUNCIONALIDAD/COMODIDAD FRENTE A CIBERSEGURIDAD.
- **ADS-B (AUTOMATIC DEPENDENT SURVEILLANCE-BROADCAST):**
 - CREAR UN AVIÓN FANTASMA.
 - CREAR INFORMES METEOROLÓGICOS FALSOS.
 - PERTURBACIÓN (ACCESIBILIDAD).
 - TRANSMITIR INFORMACIÓN MANIPULADA A PILOTOS O CONTROLADORES.
- **ACARS (AIRCRAFT COMMUNICATIONS ADDRESSING AND REPORTING SYSTEM):**
 - ACTUALIZACIÓN MANIPULADA DE PLANES DE VUELO.
 - INFORMACIÓN METEOROLÓGICA FALSA.
 - MENSAJES FALSOS ENTRE EL AVIÓN Y TIERRA.
 - PERTURBACIÓN (ACCESIBILIDAD).



Ciberseguridad Aeroespacial

Problemas estructurales del sector

- DESEQUILIBRIO ENTRE SAFETY Y SECURITY.
- NECESIDAD DE CIBERSEGURIDAD POR DISEÑO Y POR DEFECTO Y MANTENERLA.
- NECESIDAD DE SOLUCIONES Y ESTÁNDARES CIBER PARA EL SECTOR.
- ENSAMBLAJE FRENTE A LA FABRICACIÓN (PARTNERS) COMPLICA EL CONTROL DE LA CADENA DE SUMINISTRO Y GENERA DEPENDENCIA TECNOLÓGICA.
- SHADOW IT (NO SABEMOS LO QUE HAY EN DETERMINADOS EQUIPOS).
- OBSOLESCENCIA (AFECTA A LA INTEROPERABILIDAD Y CIBERSEGURIDAD):
 - PROBLEMA MUY COMPLEJO (MEJOR EVITARLA QUE GESTIONARLA).
 - EFECTO DE ARRASTRE.
 - SOFTWARE, HARDWARE, ESTÁNDARES, ALGORITMOS, PROTOCOLOS E INTERFACES.
 - MANTENIMIENTO PREVENTIVO, CORRECTIVO, PERFECTIVO, EVOLUTIVO ADAPTATIVO Y PREDICTIVO.



Ciberseguridad Aeroespacial

Estrategia de seguridad aeroespacial I/IV



BOLETÍN OFICIAL DEL ESTADO



Núm. 103

Martes 30 de abril de 2019

Sec. I. Pág. 43482

I. DISPOSICIONES GENERALES

MINISTERIO DE LA PRESIDENCIA, RELACIONES CON LAS CORTES E IGUALDAD

6349 *Orden PCI/489/2019, de 26 de abril, por la que se publica la Estrategia de Seguridad Aeroespacial Nacional, aprobada por el Consejo de Seguridad Nacional.*

El Consejo de Seguridad Nacional, en su reunión del día 12 de abril de 2019, ha aprobado la Estrategia de Seguridad Aeroespacial Nacional.

Para general conocimiento se dispone su publicación en el «Boletín Oficial del Estado» como anexo a la presente Orden.

Madrid, 26 de abril de 2019.—La Vicepresidenta del Gobierno y Ministra de la Presidencia, Relaciones con las Cortes e Igualdad, Carmen Calvo Poyato.

ANEXO

Estrategia de Seguridad Aeroespacial Nacional

Sumario

Resumen ejecutivo

Ciberseguridad Aeroespacial

Estrategia de seguridad aeroespacial II/IV

CIBERAMENAZAS:

- ENTORNO MUY TECNIFICADO Y VINCULADO AL DOMINIO CIBERNÉTICO.
- CRECIENTE PESO DE LA INFORMÁTICA EN LOS SISTEMAS EMBARCADOS.
- OBJETIVO DE ELEVADO VALOR ESTRATÉGICO Y DE ALTA RENTABILIDAD.
- OBJETIVOS MUY DIVERSOS Y EFECTOS MUY DIVERSOS.
- NECESIDAD DE ELEVADOS RECURSOS (ESTADOS / AMENAZA DESCONOCIDA).
- PRIORIDAD DE LA SEGURIDAD OPERATIVA Y FUNCIONAL FRENTE A LA SEGURIDAD CIBERNÉTICA. NECESIDAD PREVIA DE SEGURIDAD CIBERNÉTICA PARA LOGRAR LA SEGURIDAD AEROESPACIAL (AERONAVEGABILIDAD).
- TAMBIÉN AERONAVES Y SISTEMAS EMBARCADOS.
- FALLOS DE DISEÑO, PROGRAMACIÓN O FABRICACIÓN, QUE PUEDEN GENERAR VULNERABILIDADES.

Ciberseguridad Aeroespacial

Estrategia de seguridad aeroespacial III/IV

LÍNEAS DE ACCIÓN:

- FORTALECER PREVENCIÓN, DETECCIÓN, VIGILANCIA Y RESPUESTA.
- ADECUAR LOS SISTEMAS AL ESQUEMA NACIONAL DE SEGURIDAD.
- FOMENTAR EL EMPLEO DE PRODUCTOS CERTIFICADOS Y ACREDITADOS.
- CONCIENCIAR EN CIBERSEGURIDAD AL SECTOR.
- ESTABLECER MECANISMOS DE INTELIGENCIA Y CONTRAINTELIGENCIA.
- COOPERAR CON OTROS ESTADOS Y DESARROLLAR LA LEGISLACIÓN.
- IMPLANTAR UNA POLÍTICA DE SEGURIDAD INTEGRAL.

Ciberseguridad Aeroespacial

Estrategia de seguridad aeroespacial IV/IV

CONTENIDO DE LA POLÍTICA DE SEGURIDAD INTEGRAL:

- PROMOVER LA REDUNDANCIA, RESILIENCIA, RESISTENCIA.
- GESTIONAR DE LA OBSOLESCENCIA.
- AUDITAR LA SEGURIDAD DE SISTEMAS CRÍTICOS.
- DETERMINAR LA FORMACIÓN CIBER DEL PERSONAL QUE OPERA Y SOSTIENE SISTEMAS AEROESPACIALES.
- ORGANIZAR EJERCICIOS DE CIBER PARA EVALUAR SISTEMAS Y PERSONAL.

Ciberseguridad Aeroespacial

Posibles soluciones I/II

ESTÁNDARES EUROCAE/EASA

- ED-201 AERONAUTICAL INFORMATION SYSTEM SECURITY (AISS) FRAMEWORK GUIDANCE.
- ED-202A AIRWORTHINESS SECURITY PROCESS SPECIFICATION.
- ED-203/ED-203A (DRAFT) AIR WORTHINESS SECURITY METHODS AND CONSIDERATIONS.
- ED-204 INFORMATION SECURITY GUIDANCE FOR CONTINUING AIRWORTHINESS.
- ED-205 PROCESS STANDARD FOR SECURITY CERTIFICATION AND DECLARATION OF ATM ANS GROUND SYSTEMS.

Ciberseguridad Aeroespacial

Posibles soluciones II/II

- NECESIDAD DE EXPERTOS EN GESTIÓN DE OBSOLESCENCIA (INTEROPERABILIDAD Y CIBERSEGURIDAD), SE REQUIERE UN ENFOQUE HOLÍSTICO Y MULTIDISCIPLINAR.
- ADECUAR EL CICLO DE VIDA DE LOS SISTEMAS CIS/TIC A LOS AEROESPACIALES.
- DISPONER DE UN FRAMEWORK TECNOLÓGICO COMÚN, CERTIFICADO Y ACREDITADO, CON UN CICLO DE VIDA ADECUADO (SISTEMAS ABIERTOS).
- CONTEMPLAR TODOS LOS TIPOS DE MANTENIMIENTO EN OT/IT AEROESPACIAL.
- USAR ARQUITECTURAS Y SISTEMAS RESILIENTES, REDUNDANTES Y RESISTENTES.
- EQUILIBRIO SAFETY & SECURITY (AGILIDAD EN SOLUCIONES CIBER EMBARCADAS).
- CONTROLAR LA CADENA DE SUMINISTRO Y DEPENDENCIA TECNOLÓGICA.
- APLICAR PROGRAMACIÓN SEGURA Y DEFENSIVA.
- CREAR HERRAMIENTAS DE ANÁLISIS DE RIESGOS PARA IT/OT AEROESPACIAL.





COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD

#XIIIJORNADASCNCERT

OC.CCN.CNI.ES

WWW.CCN.CNI.ES

WWW.CCN-CERT.CNI.ES

XIII JORNADAS STIC CCN-CERT

CCN-cert
centro criptológico nacional