



## OAC Boletín de Julio 2019

Operaciones en el ciberespacio (CO) es el empleo de capacidades del ciberespacio donde el propósito principal es lograr objetivos en o a través del ciberespacio.

Cyberspace Operations Joint Publication 3-12

### Tabla de Contenidos

<b>ESTRATEGIA</b> .....	2
Inteligencia Estratégica desde el foro económico mundial .....	2
La guerra por la tecnología 5G ha llegado a nuestro suelo .....	2
<b>CIBERSEGURIDAD</b> .....	2
Ciberseguridad: OTAN y los activos estratégicos en el espacio .....	2
Documento de Interés.....	3
Código de Derecho en Ciberseguridad.....	3
La Ciberseguridad y el sistema energético .....	3
<b>CIBERDEFENSA</b> .....	3
Documento de Interés.....	3
Los Estados continúan siendo la principal ciberamenaza para la seguridad nacional .....	3
<b>CIBERGUERRA</b> .....	4
Un libro blanco para la cooperación público-privada en ciberseguridad.....	4
<b>CIBERCONFIANZA</b> .....	4
Los cuidados del Estado a los usuario de Redes Sociales.....	4
<b>CIBERFORENSIA</b> .....	4
Bug en una librería de Microsoft.....	4
<b>CIBERCRIMEN</b> .....	4
La internet de las cosas es objeto de ataques.....	4
<b>NOVEDADES Y NOTICIAS</b> .....	5
Firma de convenios de cooperación académica.....	5



**El Observatorio Argentino del Ciberespacio (OAC), micro-sitio de la Escuela Superior de Guerra Conjunta**

URL: <http://www.esgcffaa.edu.ar/esp/oac-boletines.php>.

Es un esfuerzo posible por el financiamiento que el observatorio recibe de la **Universidad de la Defensa Nacional**, a través de los programas UNDEFI y se encuentra inserto en la **Antena Territorial de Defensa y Seguridad** de la Secretaría de Ciencia y Tecnología de la Nación y es administrado por el **Centro de Estudios de Prospectiva Tecnológica Militar "Grl Mosconi" de la Facultad de Ingeniería del Ejército Argentino**

Nuestro objetivo se reafirma en la intención de llevar a la comunidad ciberespacial distintas perspectivas de este nuevo ámbito operacional, aportando novedades reportes e informes que permitan a la comunidad educativa y a la sociedad en general conocer más acerca del mismo

## **ESTRATEGIA**

### **Inteligencia Estratégica desde el foro económico mundial**

El foro económico mundial ha presentado una herramienta interesante para poder armar mapas de situación de diferentes tecnologías, países y capacidades a partir de un sitio interactivo de información estratégica e inteligencia contextual donde se puede explorar y revisar los problemas y las fuerzas que impulsan el cambio de las economías, las industrias y los asuntos globales.

<https://intelligence.weforum.org/>

### **La guerra por la tecnología 5G ha llegado a nuestro suelo**

El periodista Dinatle a través de infobae informa que funcionarios del gobierno de los EEUU han comunicado a la administración Macri su preocupación por el avance chino en el área de la informática

<https://www.infobae.com/politica/2019/06/30/fuertes-advertencias-de-ee-uu-a-la-argentina-por-la-amenaza-de-china-con-huawei-en-la-tecnologia-5g/>

## **CIBERSEGURIDAD**

### **Ciberseguridad: OTAN y los activos estratégicos en el espacio**

Las operaciones militares modernas se basan en activos espaciales, estos medios no se encuentran libres de vulnerabilidades cibernéticas que pueden socavar la confianza en el desempeño de los sistemas estratégicos. Este documento evalúa las amenazas, vulnerabilidades y riesgos cibernéticos para estos sistemas estratégicos.

<https://www.chathamhouse.org/publication/cybersecurity-nato-s-space-based-strategic-assets>



## Documento de Interés

### *Código de Derecho en Ciberseguridad*

El propósito de este documento es el de fijar las directrices generales del uso seguro del ciberespacio a través del impulso de una visión integradora que garantice la seguridad y el progreso de España. Tal objetivo debía alcanzarse a través de la adecuada coordinación y cooperación entre todas las Administraciones Públicas, pero también entre aquellas con el sector privado y con los ciudadanos. Entre los temas tratados en sus 1114 páginas encontramos aspectos referidos a: la normativa de seguridad nacional, infraestructuras críticas, equipos de respuestas frente a incidentes de seguridad, telecomunicaciones y usuarios, ciberdelincuencia, protección de datos, relaciones con la administración, todo ello tratado en detalle.

[https://www.boe.es/legislacion/codigos/codigo.php?id=173\\_Codigo\\_de\\_Derecho\\_de\\_la\\_Ciberseguridad&modo=1](https://www.boe.es/legislacion/codigos/codigo.php?id=173_Codigo_de_Derecho_de_la_Ciberseguridad&modo=1)

### *La Ciberseguridad y el sistema energético*

Si bien el sistema energético es uno de las infraestructuras críticas más cuidadas, donde la Ciberseguridad ha progresado de forma eficiente en razón del alto valor de los activos empresariales a proteger a fin de evitar los ciberataques que tienen al sector en su punto de mira. El Ciberelcano ha realizado una investigación dentro de España, mostrando otros riesgos asociados al sistema energético, más allá de la seguridad cibernética.

[http://www.realinstitutoelcano.org/wps/portal/rielcano\\_es/contenido?WCM\\_GLOBAL\\_CONTEXT=/elcano/elcano\\_es/zonas\\_es/ari83-2019-arteaga-ciberseguridad-y-seguridad-integral-en-el-sector-energetico?utm\\_source=CIBERelcano&utm\\_medium=email&utm\\_campaign=46-julio2019&cldee=YW1vcmVzaTUxQGdtYWlsLmNvbQ%3d%3d&recipientid=contact-a5e4c470e59de911a97d000d3a233b72-4e26c1aa3f424643b7d3e5a40aad4f18&esid=29d520ce-7ba2-e911-a988-000d3a233e06](http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari83-2019-arteaga-ciberseguridad-y-seguridad-integral-en-el-sector-energetico?utm_source=CIBERelcano&utm_medium=email&utm_campaign=46-julio2019&cldee=YW1vcmVzaTUxQGdtYWlsLmNvbQ%3d%3d&recipientid=contact-a5e4c470e59de911a97d000d3a233b72-4e26c1aa3f424643b7d3e5a40aad4f18&esid=29d520ce-7ba2-e911-a988-000d3a233e06)

## CIBERDEFENSA

### Documento de Interés

#### *Los Estados continúan siendo la principal ciberamenaza para la seguridad nacional*

El CCN-CERT IA-13/19 ha publicado la edición 2019 el informe acerca de Ciberamenazas y tendencias. Edición 2019. El documento hace el balance de los principales ciberincidentes registrados el pasado año, los métodos de ataque empleados por los agentes de la amenaza, las múltiples vulnerabilidades explotadas, los objetivos de ataque y las medidas necesarias para mejorar la seguridad en empresas e instituciones. Finalmente da una idea acerca de las tendencias de 2019, donde advierte acerca de los ataques a los datos y el empleo de la Inteligencia artificial en los ataques cibernéticos

<https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3767-ccn-cert-ia-13-19-ciberamenazas-y-tendencias-resumen-ejecutivo-2019/file.html>



## CIBERGUERRA

### **Un libro blanco para la cooperación público-privada en ciberseguridad**

Carlos Galán, Licenciado y doctor en Informática, licenciado en Derecho y abogado especialista en Derecho de las TIC, profesor de la Universidad Carlos III de Madrid, presidente de la Agencia de Tecnología Legal y miembro del Grupo de Trabajo de Ciberpolítica del Real Instituto Elcano y Javier Alonso Lecuit, miembro del Grupo de Trabajo sobre Ciberpolítica del Real Instituto Elcano.

Abordan un interesante punto de vista sobre la imperiosa necesidad de integración de agentes públicos y privados para hacer frente a los desafíos de la ciberseguridad.

[www.realinstitutoelcano.org/wps/portal/rielcano\\_es/contenido?WCM\\_GLOBAL\\_CONTEXT=/elcano/elcano\\_es/zonas\\_es/ari67-2019-galanalonsolecuit-libro-blanco-para-cooperacion-publico-privada-ciberseguridad](http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari67-2019-galanalonsolecuit-libro-blanco-para-cooperacion-publico-privada-ciberseguridad)

## CIBERCONFIANZA

### **Los cuidados del Estado a los usuario de Redes Sociales**

Una de las obligaciones de los estados es cuidar de sus ciudadanos y que ellos dispongan de adecuada seguridad, tanto en el mundo real, como en el virtual y de esto último trata la ciberconfianza, uno de los aspectos más recomendados en la Política que predica la Unión Internacional de Telecomunicaciones. Más allá de que estaba dentro del marco de lo posible se ha concretado la multa a Facebook por los casos de “Cambridge Analytica y el resto de escándalos de privacidad”, ello determinó que Facebook tendrá que pagar 5.000 millones de dólares de multa por no proteger los datos de sus usuarios.

<https://www.nytimes.com/2019/07/12/technology/facebook-ftc-fine.html>

<https://www.wsj.com/articles/ftcs-5-billion-fine-alone-wont-get-facebook-out-of-crosshairs-11563043006>

## CIBERFORENSIA

### **Bug en una librería de Microsoft**

Se considera el bug como una vulnerabilidad de baja ocurrencia. Aunque en ciertos casos, como es el caso de software para servidores como «Internet Information Services», Una vulnerabilidad de denegación de servicio puede ser un problema importante.

<https://bugs.chromium.org/p/project-zero/issues/detail?id=1804>

## CIBERCRIMEN

### **La internet de las cosas es objeto de ataques**

La internet de las cosas (IoT) tiene un nuevo atacante: ‘Silex’, ya ha paralizado más de 2000 dispositivos en pocas horas, ha atacado dispositivos con base GNU/Linux y con las credenciales de acceso por defecto,



aparentemente la única finalidad sería el hacer daño por hacer, ya que no recogen información de las víctimas o piden rescates, afirma el investigador de seguridad Ankit Anubhav (@ankit\_anubhav)

<https://securityaffairs.co/wordpress/87609/iot/silex-malware-bricks-iot-devices.html>

## NOVEDADES y NOTICIAS

### FIRMA DE CONVENIOS DE COOPERACIÓN ACADÉMICA



En el ámbito de la UNIVERSIDAD DE DEFENSA NACIONAL (UNDEF), el 02 de julio de 2019, el DECANO de la FACULTAD DE INGENIERIA DEL EJERCITO (FIE) “GrI Div MANUEL N. SAVIO”, General de Brigada ANIBAL LUIS INTINI, procedió a celebrar dos Convenios de Cooperación Académica.

El primer Convenio se firmó con el DIRECTOR de la ESCUELA SUPERIOR DE GUERRA CONJUNTA DE LAS FUERZAS ARMADAS (ESGC), Coronel Mayor GABRIEL ANIBAL CAMILLI, con el objeto de permitir y estimular el intercambio académico entre la FIE por el **Centro de Estudios de Prospectiva Tecnológica Militar “GrI Mosconi”** y la ESGC por el **“Observatorio Argentino del Ciberespacio”**



El segundo Convenio se firmó con el DECANO de la FACULTAD DE LA FUERZA AÉREA, Brigadier (R) HUGO DI RISIO, con el objeto de permitir y estimular el intercambio académico entre la FIE por el **Centro de Estudios de Prospectiva Tecnológica Militar “GrI Mosconi”** y la ESGA por el **“Observatorio Tecnológico del Aeroespacio”**.

Los acuerdos alcanzados permitirán la realización de actividades conjuntas que promuevan la cooperación y el mejor aprovechamiento de las capacidades disponibles en las áreas de competencia de las partes firmantes.

Cabe destacar que el **CENTRO MOSCONI** ha conformado dentro de su organización la **Antena Territorial de Defensa y Seguridad**, con el apoyo integral del Ministerio de Ciencia y Tecnología (actualmente denominado **Secretaría de Gobierno de Ciencia y Tecnología**), en el marco del **Programa Nacional de Vigilancia e Inteligencia Competitiva**, cuyo propósito es contribuir a que las organizaciones pueden estar atentas a las novedades del entorno para mejorar la gestión del riesgo,



anticiparse a los cambios futuros, detectar tecnologías emergentes y aquellas que van quedando obsoletas, conocer las últimas líneas de investigación, así como los nuevos productos.

**A partir de la firma de estos Convenios, los Observatorios del Ciberespacio y el Aeroespacial serán parte integrante de la Antena Territorial de Defensa y Seguridad.**

Participaron del acto, además las siguientes autoridades:

BM (R) Alejandro Moresi – Director del Observatorio Tecnológico del Aeroespacio.

GB (R) “VGM” Alberto L. M. Corvalán – Director del Centro de Estudios de Prospectiva Tecnológica Militar “Grl Mosconi”.

CM Ángel Rojo - Director de la Escuela Superior de Guerra Aérea.

TC (R) Ing. Carlos F. Amaya – Codirector del Observatorio Argentino del Ciberespacio.

Esp. Lic. Nancy V. Perez – Coordinadora de Estudios Tecnológicos, Vigilancia e Inteligencia Estratégica (Subsecretaría de Estudios y Prospectiva – Secretaría de Gobierno de Ciencia y Tecnología).

Secretarios de Extensión de las Unidades Académicas firmantes



---

Copyright © \*|2018|\*

\*|Escuela Superior de Guerra Conjunta|\*,

All rights reserved.

\*|Observatorio Argentino del Ciberespacio |\*

Nuestra dirección postal es:

\*|Luis María Campos 480 - CABA - República Argentina |\*

Nuestro correo electrónico:

\*|observatorioargentinodelciberespacio@conjunta.undef.edu.ar |\*