



# OBSERVATORIO ARGENTINO DEL CIBERESPACIO

Director del Proyecto: BM (R) Alejandro Moresi  
Codirector: TC (R) Ing Carlos Amaya

ISSN: en trámite  
<http://www.esgcffaa.edu.ar/obsiber/>

AÑO 3 N° 20  
Enero-Febrero 2020

## OAC Boletín de Enero Febrero 2020

*“En un estudio reciente, el 58% de los encuestados en los Estados Unidos y el 50% en el Reino Unido citaron la tecnología como la principal causa de soledad y aislamiento social”.*

<http://reports.weforum.org/global-risks-2019/heads-and-hearts/#view/fn-41>

### Tabla de Contenidos

<b>ESTRATEGIA</b> .....	2
<u><a href="#">Cumbre de Inteligencia Artificial Latinoamericana en MIT 21 al 23 de enero de 2020</a></u> .....	2
<u><a href="#">La IA y el debate formal sobre los sistemas de armas letales autónomas</a></u> .....	2
<u><a href="#">Rusia logró desconectarse de internet para probar su propia red Runet</a></u> .....	3
<b>CIBERSEGURIDAD</b> .....	3
<u><a href="#">La batalla legal por el control del ciberespacio</a></u> .....	3
<u><a href="#">Anonymous hackeó correos del Ejército de Chile</a></u> .....	3
<u><a href="#">Estados Unidos prohíbe el empleo de ciertas apps a sus soldados</a></u> .....	3
<b>CIBERDEFENSA</b> .....	3
<u><a href="#">Departamento de Interior de EU pone en tierra 810 drones</a></u> .....	3
<u><a href="#">Ataques Cibernéticos y respuesta ciber</a></u> .....	4
<b>CIBERGUERRA</b> .....	4
<u><a href="#">Informe sobre ciberataques de diciembre de 2019</a></u> .....	4
<u><a href="#">La desinformación como arma de combate</a></u> .....	4
<b>CIBERCONFIANZA</b> .....	4
<u><a href="#">Los riesgos cibernéticos en operaciones bancarias se vuelcan a Latinoamérica</a></u> .....	4
<u><a href="#">La Inteligencia Artificial que puede reconocer y responder a las emociones</a></u> .....	5
<b>CIBERFORENSIA</b> .....	5
<u><a href="#">La Agencia Nacional de Seguridad de EEUU advierte sobre vulnerabilidades de Microsoft</a></u> .....	5



<a href="#">Vulnerabilidad en el soporte a clientes de Microsoft</a> .....	5
<b>CIBERDELITO</b> .....	5
<a href="#">La internet de la cosas, un área donde prospera el ciberdelito</a> .....	5
<a href="#">Los Ransomware vuelven al ataque</a> .....	5
<b>NOVEDADES</b> .....	6
<a href="#">El gobierno de datos eficaz</a> .....	6
<a href="#">Informe de perspectivas de ciberseguridad 2020</a> .....	6

---

**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

### Cumbre de Inteligencia Artificial Latinoamericana en MIT

Del 21 al 23 de enero en el MIT, Cambridge EE.UU, se realizó la Cumbre de Inteligencia Artificial de América Latina que convocó a líderes de gobierno, industria, academia y de empresas sin fines de lucro, a través de América Latina y el Caribe, con el fin de identificar oportunidades y riesgos que los países latinoamericanos puedan enfrentar a medida que comiencen a adoptar la inteligencia artificial en diferentes facetas de la sociedad.

<http://ailatinsum.mit.edu/>

[http://52.15.240.241/es/onepage\\_es\\_update/](http://52.15.240.241/es/onepage_es_update/)

### La Inteligencia Artificial y el debate formal sobre los sistemas letales de armas autónomas.

Una nota de Arthur Holland Michel a cerca de los algoritmos asesinos de los que nadie habla y algunas formas de inteligencia artificial que en realidad no aprietan el gatillo podrían ser una pesadilla

<https://foreignpolicy.com/2020/01/20/ai-autonomous-weapons-artificial-intelligence-the-killer-algorithms-nobodys-talking-about/>



### **La computación cuántica hace obsoleta la criptografía actual**

Cuando los enormes recursos que se dedican a la investigación cuántica conducen a la computación cuántica a gran escala, muchas de las herramientas que forman la base de la criptografía digital actual quedarán obsoletas. Los algoritmos de clave pública, en particular, serán fáciles de descifrar. Quantum también promete nuevos modos de encriptación, pero para cuando se hayan implementado nuevas protecciones, es posible que muchos secretos ya se hayan perdido para intrusos, estados y competidores

<http://reports.weforum.org/global-risks-2019/future-shocks/open-secrets/>

### **Rusia logró desconectarse de Internet para probar su propia red Runet**

El Gobierno ruso anunció este lunes que logró desconectar con éxito al país de Internet global para probar la efectividad de Runet, el proyecto de una red de tecnología con la suficiente infraestructura independiente que pueda mantener operativo al país en caso de amenazas externas. .

<https://techcrunch.com/2019/12/26/russia-starts-testing-its-own-internal-internet/>

### **Otra cara de la competencia por las redes de 5 G**

Reino Unido, Huawei y 5G: seis mitos desmentidos, un debate sobre el uso potencial de los equipos de Huawei en las redes 5G del Reino Unido, el riesgo significativamente mayor de seguridad cibernética se destaca. Marcus Willett desafía este pensamiento.

[https://www.iiss.org/blogs/analysis/2020/01/csfc-uk-huawei-and-5g-six-myths-debunked?\\_cldee=YW1vcnVzaTUxQGdtYWlsLmNvbQ%3d%3d&recipientid=contact-a5e4c470e59de911a97d000d3a233b72-af94cc6b63c343dbb37007dca62a13b3&esid=c7e0ee90-ba42-ea11-a812-000d3a44a8e9](https://www.iiss.org/blogs/analysis/2020/01/csfc-uk-huawei-and-5g-six-myths-debunked?_cldee=YW1vcnVzaTUxQGdtYWlsLmNvbQ%3d%3d&recipientid=contact-a5e4c470e59de911a97d000d3a233b72-af94cc6b63c343dbb37007dca62a13b3&esid=c7e0ee90-ba42-ea11-a812-000d3a44a8e9)

---

## **CIBERSEGURIDAD**

### **La batalla legal por el control del Ciberespacio**

El soñado paraíso del conocimiento que se pensó sería internet, hoy es un mundo caótico donde diferentes fuerzas intentan ejercer el poder sobre el individuo, y los estados no son ajenos a esta disputa, a que deben agregar también la protección de los intereses, la seguridad y la libertad de sus ciudadanos

<https://www.lavanguardia.com/internacional/20200119/472962041548/internet-redes-sociales-ciberseguridad-gobiernos-iran-china-rusia-corea-del-norte.html>

### **Anonymous hackeo correos del Ejército de Chile**

Infodefensa ha informado que el grupo de hackers Anonymous, accedió a cuentas del correo electrónico del Ejército de Chile

<https://www.infodefensa.com/latam/2019/12/16/noticia-grupo-hacker-anonymous-filtra-informacion-correos-ejercito-chile.html>

### **EE.UU. prohíbe el empleo de ciertas apps a sus soldados**

Los Estados Unidos ha prohibido el uso de la red social china TikTok, a sus soldados y la misma no podrá ser instalada en teléfonos celulares proporcionados por el gobierno.

<https://edition.cnn.com/2019/12/30/politics/army-tiktok-banned/index.html>



## CIBERDEFENSA

### Departamento de Interior de EEUU pone en Tierra 810 drones

El Departamento del Interior de EE. UU. (DOI) ha puesto a tierra su flota de 810 drones por temor a que los drones de la flota fabricados en China puedan brindar información sensible que dejen al descubierto vulnerables del sistema.

<https://sputniknews.com/science/202001301078182945-us-interior-dept-grounds-drone-fleet-over-cybersecurity-fears-in-chinese-made-uavs/>

### Ataques Cinéticos y respuestas Ciber

Christopher C. Krebs, Director de la Agencia de Seguridad de Ciberseguridad e Infraestructura emitió una advertencia sobre una posible nueva ola de ciberataques iraníes sobre activos estadounidenses después de que el general Qassim Suleimani fuera muerto por un ataque aéreo estadounidense en el aeropuerto de Bagdad en Irak.

<https://www.bleepingcomputer.com/news/security/us-government-issues-warning-about-possible-iranian-cyberattacks/>

## CIBERGUERRA

### Informe sobre Ciberataques de Diciembre de 2019

La revista digital Thiber Digest (<http://www.thiber.org/>), en su número de enero del 2020 presenta un interesante reporte producido por Adolfo Hernandez, sobre sobre ciberataques ocurridos en diciembre de 2019

[http://www.thiber.org/wp-content/uploads/2020/01/Numero\\_16\\_Enero\\_Ciberataques.pdf](http://www.thiber.org/wp-content/uploads/2020/01/Numero_16_Enero_Ciberataques.pdf)

### La desinformación como arma de combate

Es una presentación con una mirada diferente sobre la guerra actual, la misma fue realizada por la Dirección de Investigación y desarrollo de la Fuerza Aérea en el marco del XXX Seminario Internacional de Defensa y Seguridad

<https://www.argentina.gob.ar/fuerzaaerea/direccion-general-de-investigacion-y-desarrollo/centro-de-simulacion-y-juegos-de-guerra-csjg>

## CIBERCONFIANZA

### Los riesgos cibernéticos en operaciones bancarias se vuelcan a Latinoamérica

Así lo muestra bajo el Título III.5. Otros riesgos para el sistema financiero III.5.1. Riesgos cibernéticos e informáticos, *“En México, durante ...De un promedio de 1 reporte por trimestre en 2018, la estadística aumentó a un promedio de 4 reportes por trimestre en 2019. ... mayor número de ataques, se observó que los servicios afectados fueron más diversos, desde transferencias electrónicas hasta cajeros automáticos...”*



<https://www.banxico.org.mx/publicaciones-y-prensa/reportes-sobre-el-sistema-financiero/%7B04E197EE-B6FC-7BA1-72A0-32D3E6C9BF28%7D.pdf>

### **La inteligencia artificial que puede reconocer y responder a las emociones**

A medida que se entrelaza la tecnología con la vida humana, es probable que la "informática afectiva", el uso de algoritmos que pueden leer las emociones humanas o predecir nuestras respuestas emocionales, sea cada vez más frecuente. Con el tiempo, el advenimiento de los "woebots" de inteligencia artificial (IA) y herramientas similares podría transformar la entrega de atención emocional y psicológica, análoga a los monitores cardíacos y los contadores de pasos. Pero las consecuencias adversas, ya sean accidentales o intencionales, del código emocionalmente "inteligente" podrían ser profundas.

<http://reports.weforum.org/global-risks-2019/future-shocks/emotional-disruption/>

---

## **CIBERFORENSIA**

### **La Agencia Nacional de Seguridad de Estados Unidos advierte sobre vulnerabilidades de Microsoft**

Si bien la empresa Microsoft corrige de manera periódica sus vulnerabilidades, en esta oportunidad el reporte se originó en la Agencia de Seguridad Nacional estadounidense (NSA). La vulnerabilidad afecta a un componente criptográfico ampliamente usado en Windows 10, Windows Server 2016 y Windows Server 2019.

<https://media.defense.gov/2020/Jan/14/2002234275/-1/-1/0/CSA-WINDOWS-10-CRYPT-LIB-20190114.PDF>

### **Vulnerabilidad en el soporte a clientes de Microsoft**

Si se ha puesto en contacto con Microsoft para solicitar asistencia técnica en los últimos 14 años, su consulta técnica, junto con alguna información personal identificable, puede haber estado en peligro. Microsoft ha admitido hoy un incidente de seguridad que ha puesto al descubierto casi 250 millones de registros de «Servicio y soporte técnico al cliente» en Internet debido a un servidor mal configurado que contiene registros de conversaciones entre su equipo de soporte técnico y los clientes.

<https://msrc-blog.microsoft.com/2020/01/22/access-misconfiguration-for-customer-support-database/>

---

## **CIBERDELITO**

### **La Internet de las cosas un área donde prospera el ciberdelito**

Un hacker ha publicado esta semana una lista masiva de credenciales de Telnet para más de 515,000 servidores, enrutadores domésticos y dispositivos "inteligentes" de IoT (Internet de las cosas). La lista, que se publicó en un foro de piratería popular, incluye la dirección IP de cada dispositivo, junto con un nombre de usuario y contraseña para el servicio Telnet, un protocolo de acceso remoto que se puede utilizar para controlar dispositivos a través de Internet.

<https://www.zdnet.com/article/hacker-leaks-passwords-for-more-than-500000-servers-routers-and-iot-devices/>



## Los Ransomware vuelven al ataque

Defensa.com, ha publicado un informe del Coronel del Ejército del Aire Español *D. Fernando Antonio Acero Martín*, acerca de la fuerte ofensiva de ransomware que se está produciendo en el nivel internacional, aquí el artículo y otros sitios de interés mencionados

<https://www.defensa.com/cyberseguridad/escalada-ataques-mediante-ransomware-como-defendernos-esta-grave>

<https://www.ccn-cert.cni.es/seguridad-al-dia/alertas-ccn-cert/9403-ccn-cert-al-02-20-repunte-de-la-campana-de-emotet.html>

<https://www.us-cert.gov/ncas/current-activity/2020/01/22/increased-emotet-malware-activity>

<https://www.pandasecurity.com/spain/mediacenter/empresas/ciberseguridad-pymes-ransomware/>

## NOVEDADES

### Documento de Interés

#### *El gobierno de datos eficaz:*

Este breve documento de 15 páginas que ofrece “PowerData” es una guía para minimizar errores y alcanzar objetivos de gobernanza de datos, entre los aspectos destacables incluye: ¿Qué es la gobernanza de datos?, Metas y principios de la gobernanza de datos, ¿Cómo implementar una gobernanza de datos efectiva?, El programa de gobierno datos: estrategia, políticas, arquitectura, estándares y cumplimiento, El checklist de la gobernanza de datos, Gobernanza de datos: mejores prácticas.

[https://landings.powerdata.es/gobierno-de-datos-eficaz-guia-gratuita?utm\\_campaign=Data%20Governance&utm\\_source=hs\\_email&utm\\_medium=email&utm\\_content=82986413&hsenc=p2ANqtz-8fv3wnAkTBNDZQAMW\\_FG2UDKkjrTntPX8p6xfMjPmJlKf3skEpgyTkQmi-iKSsrt35A0JFF2-MQiX0on\\_jGMq9eHCEGuQ6LWlGTJDgWrPSubEBbc&hsmi=82986413](https://landings.powerdata.es/gobierno-de-datos-eficaz-guia-gratuita?utm_campaign=Data%20Governance&utm_source=hs_email&utm_medium=email&utm_content=82986413&hsenc=p2ANqtz-8fv3wnAkTBNDZQAMW_FG2UDKkjrTntPX8p6xfMjPmJlKf3skEpgyTkQmi-iKSsrt35A0JFF2-MQiX0on_jGMq9eHCEGuQ6LWlGTJDgWrPSubEBbc&hsmi=82986413)

#### *Informe de perspectivas de ciberseguridad 2020*

En este informe 20 carillas de “carbon black” (cdn. [www.carbonblack.com](http://www.carbonblack.com) – Carbon Black, Inc. Waltham, Massachusets. US), se incluyen interesantes datos de ataques ciber tomados de fuentes disponibles públicamente y la web oscura para 2020.

El objetivo propuesto por el autor es ofrecer una visión holística de cómo han evolucionado los atacantes, qué están haciendo los defensores para mantener el ritmo y cómo los equipos de seguridad y de TI pueden trabajar juntos en 2020 y más allá en la batalla interminable del “bien contra el mal”.

<https://cdn.www.carbonblack.com/wp-content/uploads/2020/02/VMware-Carbon-Black-2020-Cybersecurity-Outlook-Report-022620.pdf>